ESET Endpoint Security

คู่มือผู้ใช้

คลิกที่นี่เพื่อแสดงเวอร์ชันออนไลน์ของเอกสารนี้

Digital Security
Progress. Protected.

ESET Endpoint Security ได้รับการพัฒนาจาก ESET, spol. s r.o.

สำหรับข้อมูลเพิ่มเติม โปรดไปที่ https://www.eset.com

ฝ่ายสนับสนุนด้านเทคนิค: https://support.eset.com

REV. 12/4/2024

ESET Endpoint Security

ESET Endpoint Security เป็นวิธีการใหม่ในการรักษาความปลอดภัยคอมพิวเตอร์ที่ผสานรวมอย่างแท้จริง เครื่องมือสแกนเวอร์ชันใหม่ล่าสุดของ ESET LiveGrid® ที่ผสมผสานกับไฟร์วอลล์ที่กำหนดเองและโมดูลการป้องกันสแปมอีเมลไคลเอ็นต์ ใช้ความเร็วและความแม่นยำในการทำให้คอมพิวเตอร์ของคุณปลอดภัยอยู่เสมอ เป็นผลให้เกิดระบบอัจฉริยะที่ตื่นตัวอยู่เสมอต่อการโจมตีและซอฟต์แวร์ที่เป็นอันตรายซึ่งจะก่อให้เกิดอันตรายต่อคอมพิวเตอร์ของคุณ

ESET Endpoint Security 9 เป็นโซลูชันการรักษาความปลอดภัยแบบสมบูรณ์ จากความมุ่งมั่นอันยาวนานในการผสมผสานการป้องกันสูงสุดกับการใช้ทรัพยากรของระบบน้อยที่สุด เทคโนโลยีปัญญาประดิษฐ์ขั้นสูงนี้สามารถกำจัดและแฝงตัวจากไวรัส สปายแวร์ ม้าโทรจัน เวิร์ม แอดแวร์ รูทคิทและ การโจมตีจากอินเทอร์เน็ตในรูปแบบอื่นๆ ในเชิงรุก โดยไม่ขัดขวางประสิทธิภาพการทำงานของระบบหรือรบกวนคอมพิวเตอร์

ESET Endpoint Security ได้รับการออกแบบมาใช้กับเวิร์กสเตชันในสภาพแวดล้อมของธุรกิจขนาดย่อม

ในส่วน การติดตั้ง คุณสามารถค้นหาหัวข้อวิธีใช้ที่แบ่งออกเป็นหลายบทและบทย่อยเพื่อสร้างความเข้าใจและมีบริบท รวมถึง การดาวน์โหลด การติดตั้ง และ การเปิดใช้งาน

การใช้ ESET Endpoint Security พร้อมกับ ESET PROTECT ในสภาพแวดล้อมขององค์กร จะทำให้คุณสามารถจัดการกับเวิร์กสเตชันไคลเอ็นต์จำนวนเท่าใดก็ได้ ใช้นโยบายและกฎ ติดตามการตรวจหา และกำหนดค่าไคลเอ็นต์จากระยะไกลจากคอมพิวเตอร์เครื่องใดก็ได้ในเครือข่ายได้อย่างง่ายดาย

นี้จะครอบคลุมบทคำถามที่พบบ่อยและปัญหาที่พบเกือบทั้งหมด:

คุณลักษณะและคุณประโยชน์

ส่วนติดต่อผู้ใช้รูปแบบใหม่	ส่วนติดต่อผู้ใช้ในเวอร์ชันนี้ ได้รับการปรับรูปแบบใหม่อย่างเห็นได้ชัดและถูกทำให้ใช้ง่ายขึ้นซึ่งเป็นไปตามผลการทดสอบการใช้งาน การใช้คำและการแจ้งเตือนของ GUI ได้รับการทบทวนอย่างระมัดระวังและส่วนติดต่อให้การสนับสนุนภาษาที่อ่านจากขวาไปซ้ายเช่นฮิบรูและอารบิกแล้วในตอนนี้ ตัวช่วยออนไลน์ รวมเข้ากับ ESET Endpoint Security แล้วในตอนนี้และให้เนื้อหาสนับสนุนที่ได้รับการอัพเดทอย่างต่อเนื่อง
โหมดสีเข้ม	ส่วนขยายที่ช่วยให้คุณสลับหน้าจอเป็นธีมสีเข้มได้อย่างรวดเร็ว คุณสามารถเลือกโทนสีที่คุณต้องการใน องค์ประกอบส่วนต่อประสานผู้ใช้ ได้
การป้องกันไวรัสและสปายแวร์	ตรวจหาและกำจัดไวรัส เวิร์ม โทรจัน และรูทคิททั้งที่รู้จักและไม่รู้จักในเชิงรุกได้มากกว่า การวิเคราะห์พฤติกรรมขั้นสูงจะกำหนดสถานะแม้กระทั่งมัลแวร์ที่ไม่เคยพบเห็นมาก่อน ซึ่งจะช่วยป้องกันคุณจากภัยคุกคามที่ไม่รู้จักและลดประสิทธิภาพภัยคุกคามก่อนที่จะก่อให้เกิดอันตราย การป้องกันการเข้าถึงเว็บ และ การป้องกันฟิชชิงทำงานโดยการตรวจสอบการสื่อสารระหว่างเบราว์เซอร์เว็บและเซิร์ฟเวอร์ระยะไกล (รวมถึง SSL) การป้องกันไคลเอ็นต์อีเมล ให้การควบคุมการสื่อสารทางอีเมลที่ได้รับผ่านโปรโตคอล POP3(S) และ IMAP(S)

การอัพเดทเป็นประจำ	การอัพเดทกลไกตรวจหา (ก่อนหน้านี้เรียกว่า "ฐานข้อมูลไวรัส") และโมดูลโปรแกรมเป็นประจำเป็นวิธีที่ดีที่สุดเพื่อให้แน่ใจว่าคอมพิวเตอร์ของคุณจะมีระดับการรักษาความปลอดภัยสูงสุด
ESET LiveGrid® (ความเชื่อถือที่อ้างอิงคลาวด์)	คุณ สามารถตรวจสอบความเชื่อถือของกระบวนการและไฟล์ที่ทำงานอยู่ได้โดยตรงจาก ESET Endpoint Security
การจัดการระยะไกล	ESET PROTECT ช่วยให้คุณจัดการผลิตภัณฑ์ ESET บนเวิร์กสเตชัน เซิร์ฟเวอร์ และอุปกรณ์เคลื่อนที่ในสภาพแวดล้อมการทำงานของเครือข่ายจากจุดศูนย์กลางจุดเดียว ด้วยการใช้เว็บคอนโซล ESET PROTECT (เว็บคอนโซล ESET PROTECT) คุณสามารถปรับใช้โซลูชัน ESET จัดการงาน บังคับใช้นโยบายด้านความปลอดภัย ตรวจสอบสถานะระบบและตอบสนองต่อปัญหาหรือภัยคุกคามบนคอมพิวเตอร์ระยะไกลได้อย่างรวดเร็ว
การป้องกันการโจมตีเครือข่าย	จะวิเคราะห์เนื้อหาของเครือข่ายการรับส่งข้อมูลเครือข่ายและป้องกันการโจมตีเครือข่าย การรับส่งใด ๆ ที่ได้รับพิจารณาว่าเป็นอันตรายจะถูกปิดกั้น
การควบคุมเว็บไซต์ (เฉพาะ ESET Endpoint Security)	การควบคุมการเข้าถึงเว็บไซต์ช่วยให้คุณบล็อกหน้าเว็บที่อาจมีเนื้อหาที่ไม่เหมาะสม นอกจากนี้ นายจ้างหรือผู้ดูแลระบบสามารถห้ามการเข้าถึงเว็บไซต์ที่กำหนดไว้ล่วงหน้าได้มากกว่า 27 ประเภทและกว่า 140 ประเภทย่อย

มีอะไรใหม่

มีอะไรใหม่ใน ESET Endpoint Security เวอร์ชัน 11

เครื่องมือแก้ไขกฎของไฟร์วอลล์ใหม่

เครื่องมือแก้ไข กฎของไฟร์วอลล์ ได้รับการออกแบบใหม่เพื่อให้คุณสามารถกำหนดกฎของไฟร์วอลล์ได้ง่ายขึ้นด้วยตัวเลือกการกำหนดค่าเพิ่มเติม

การจัดการจุดอ่อนและโปรแกรมแก้ไข

ฟีเจอร์ใน ESET PROTECT Cloud ที่จะสแกนเวิร์กสเตชันเป็นประจำเพื่อตรวจหาซอฟต์แวร์ที่ติดตั้งไว้ซึ่งอาจมีความเสี่ยงด้านความปลอดภัย การจัดการแพทช์ ตรวจสอบว่ามีพื้นที่ว่างเพียงพอก่อนเริ่มดาวน์โหลด (ค่าเริ่มต้นและค่าต่ำสุดคือ 2GB) และช่วยปรับปรุงแก้ไขความเสี่ยงเหล่านี้ผ่านการอัพเดทซอฟต์แวร์อัตโนมัติ ทำให้อุปกรณ์มีความปลอดภัยมากขึ้น

สถานะผลิตภัณฑ์ที่สิ้นสุดอายุการใช้งาน

ESET Endpoint Security ในเวอร์ชั่นนี้สามารถแสดง สถานะผลิตภัณฑ์การสิ้นสุดอายุการใช้งานต่างๆ คุณสามารถตั้งค่าสถานะการสิ้นสุดอายุการใช้งานได้ใน การแจ้งเตือน

ความต้องการของระบบ

เพื่อให้การใช้งาน ESET Endpoint Security เป็นไปอย่างราบรื่น ระบบควรเป็นไปตามข้อกำหนดด้านฮาร์ดแวร์และซอฟต์แวร์ต่อไปนี้ (การตั้งค่าผลิตภัณฑ์เริ่มต้น):

ตัวประมวลผลที่รองรับ

ตัวประมวลผล Intel หรือ AMD 32 บิต (x86) พร้อมชุดคำสั่ง SSE2 หรือ 64 บิต (x64), 1 GHz หรือสูงกว่า

ตัวประมวลผล ARM64, 1 GHz หรือสูงกว่า

ระบบปฏิบัติการ

Microsoft® Windows® 11

Microsoft® Windows® 10

สำหรับรายการเวอร์ชันของ Microsoft® Windows® 10 และ Microsoft® Windows® 11 ที่รองรับอย่างละเอียด โปรดดู นโยบายการสนับสนุนระบบปฏิบัติการ Windows

โปรดพยายามอัพเดทระบบปฏิบัติการของคุณให้ทันสมัยเสมอ

จะต้องติดตั้งการสนับสนุนสำหรับ Azure Code Signing บนระบบปฏิบัติการ Windows ทั้งหมดเพื่อติดตั้งหรืออัพเกรดผลิตภัณฑ์ ESET ที่วางจำหน่ายหลังเดือนกรกฎาคม 2023 ข้อมูลเพิ่มเติม

ความต้องการของคุณลักษณะ ESET Endpoint Security

ดูความต้องการของระบบสำหรับคุณลักษณะบางรายการของ ESET Endpoint Security ในตารางด้านล่าง:

คุณลักษณะ	ความต้องการ
Intel® Threat Detection Technology	ดู ตัวประมวลผลที่รองรับ
เบราว์เซอร์ที่ปลอดภัย	ดู เว็บเบราว์เซอร์ที่รองรับ
เครื่องมือทำความสะอาดเฉพาะทาง	ตัวประมวลผลที่ไม่ใช่ ARM64
การป้องกันการโจมตีแบบ Exploit	ตัวประมวลผลที่ไม่ใช่ ARM64
การตรวจสอบการทำงานเชิงลึก	ตัวประมวลผลที่ไม่ใช่ ARM64

ตัวติดตั้ง ESET Endpoint Security ที่สร้างขึ้นใน ESET PROTECT จะรองรับ Windows 10 Enterprise for Virtual Desktops และ Windows 10 โหมดหลายเซสชัน

อื่นๆ

- ระบบปฏิบัติการและซอฟต์แวร์อื่นๆ ที่ติดตั้งอยู่บนคอมพิวเตอร์เป็นไปตามความต้องการของระบบ
- หน่วยความจำระบบว่าง 0.3 GB (ดู หมายเหตุ 1)
- พื้นที่ว่างดิสก์ 1 GB (ดู หมายเหตุ 2)
- ความละเอียดจอแสดงผลต่ำสุด 1024 x 768
- การเชื่อมต่ออินเทอร์เน็ตหรือการเชื่อมต่อเครือข่ายของพื้นที่กับแหล่งที่มา (ดู หมายเหตุ 3) ของการอัพเดทผลิตภัณฑ์
- โปรแกรมป้องกันไวรัสสองโปรแกรมที่ทำงานพร้อมกันบนอุปกรณ์เดียวทำให้เกิดความขัดแย้งของทรัพยากรระบบที่หลีกเลี่ยงไม่ได้ เช่น การชะลอตัวของระบบเพื่อให้ไม่สามารถทำงานได้

แม้ว่าอาจติดตั้งและเรียกใช้ผลิตภัณฑ์บนระบบที่ไม่เป็นไปตามข้อกำหนดเหล่านี้ได้ เราก็ขอแนะนำให้ทดสอบก่อนการใช้งานโดยอิงตามข้อกำหนดด้านประสิทธิภาพ

(1): ผลิตภัณฑ์อาจใช้หน่วยความจำมากขึ้น หากมีหน่วยความจำที่ไม่ได้ใช้บนคอมพิวเตอร์ที่ติดไวรัสอย่างหนัก หรือเมื่อกำลังนำเข้ารายการข้อมูลจำนวนมากเข้าสู่ผลิตภัณฑ์ (เช่น รายชื่อ URL ปลอดภัย)
(2) จำเป็นต้องมีพื้นที่ในดิสก์เพื่อดาวน์โหลดโปรแกรมติดตั้ง ติดตั้งผลิตภัณฑ์ เก็บสำเนาแพ็คเกจการติดตั้งในข้อมูลโปรแกรม และบันทึกข้อมูลสำรองการอัพเดทผลิตภัณฑ์เพื่อรองรับคุณลักษณะการย้อนกลับ ผลิตภัณฑ์อาจใช้พื้นที่ในดิสก์มากขึ้นภายใต้การตั้งค่าที่ต่างกัน (เช่น เมื่อจัดเก็บข้อมูลสำรองของการอัพเดทผลิตภัณฑ์ไว้หลายเวอร์ชันขึ้น ดัมพ์หน่วยความจำ หรือเก็บบันทึกจำนวนมาก) หรือบนคอมพิวเตอร์ที่ติดไวรัส (เช่น เนื่องจากคุณสมบัติการกักเก็บ) เราขอแนะนำให้เก็บพื้นที่ว่างในดิสก์ให้เพียงพอเพื่อรองรับการอัพเดทระบบปฏิบัติการและการอัพเดทผลิตภัณฑ์ ESET
(3) แม้ว่าจะเป็นการดำเนินการที่ไม่แนะนำ แต่คุณก็สามารถอัพเดทผลิตภัณฑ์ด้วยตนเองได้จากสื่อที่ถอดเข้าออกได้

ภาษาที่รองรับ

ESET Endpoint Security พร้อมให้ติดตั้งและดาวน์โหลดในภาษาต่อไปนี้

ภาษา	รหัสภาษา	LCID
ภาษาอังกฤษ (สหรัฐอเมริกา)	en-US	1033
ภาษาอารบิก (อียิปต์)	ar-EG	3073
ภาษาบัลแกเรีย	bg-BG	1026
ภาษาจีนตัวย่อ	zh-CN	2052
ภาษาจีนตัวเต็ม	zh-TW	1028
ภาษาโครเอเชีย	hr-HR	1050
ภาษาเช็ก	cs-CZ	1029
ภาษาเอสโตเนีย	et-EE	1061
ภาษาฟินแลนด์	fi-FI	1035

ภาษา	รหัสภาษา	LCID
ภาษาฝรั่งเศส (ฝรั่งเศส)	fr-FR	1036
ภาษาฝรั่งเศส (แคนาดา)	fr-CA	3084
ภาษาเยอรมัน (เยอรมนี)	de-DE	1031
ภาษากรีก	el-GR	1032
*ภาษาฮิบรู	he-IL	1037
ภาษาฮังการี	hu-HU	1038
*ภาษาอินโดนีเซีย	id-ID	1057
ภาษาอิตาลี	it-IT	1040
ภาษาญี่ปุ่น	ja-JP	1041
ภาษาคาซัค	kk-KZ	1087
ภาษาเกาหลี	ko-KR	1042
*ภาษาลัตเวีย	lv-LV	1062
ภาษาลิธัวเนีย	lt-LT	1063
Nederlands	nl-NL	1043
ภาษานอร์เวย์	nb-NO	1044
ภาษาโปแลนด์	pl-PL	1045
ภาษาโปรตุเกส (บราซิล)	pt-BR	1046
ภาษาโรมาเนีย	ro-RO	1048
ภาษารัสเซีย	ru-RU	1049
ภาษาสเปน (ชิลี)	es-CL	13322
ภาษาสเปน (สเปน)	es-ES	3082
ภาษาสวีเดน (สวีเดน)	sv-SE	1053
ภาษาสโลวัก	sk-SK	1051
ภาษาสโลวีเนีย	sl-SI	1060
ภาษาไทย	th-TH	1054
ภาษาตุรกี	tr-TR	1055
ยูเครเนียน (ยูเครน)	uk-UA	1058
*ภาษาเวียดนาม	vi-VN	1066

* ESET Endpoint Security สามารถใช้งานได้ในภาษาที่ทำเครื่องหมายไว้ แต่คู่มือผู้ใช้แบบออนไลน์จะไม่สามารถใช้งานในภาษาดังกล่าวได้ (เปลี่ยนเส้นทางไปยังเวอร์ชันภาษาอังกฤษ)

หากต้องการเปลี่ยนภาษาของคู่มือผู้ใช้แบบออนไลน์ฉบับนี้ โปรดดูกล่องเลือกภาษา (ที่มุมซ้ายบนที่มุมขวาบน)

บันทึกการเปลี่ยนแปลง

การป้องกัน

เมื่อใช้คอมพิวเตอร์ โดยเฉพาะเมื่อคุณใช้อินเทอร์เน็ต โปรดพึงระลึกไว้ว่าไม่มีระบบป้องกันไวรัสใดที่สามารถกำจัดความเสี่ยงจาก การตรวจหา และ การโจมตีระยะไกล ได้ทั้งหมด หากต้องการเพิ่มการป้องกันและความสะดวกสูงสุด คุณต้องใช้โซลูชันป้องกันไวรัสอย่างถูกต้องและปฏิบัติตามกฎที่มีประโยชน์ต่างๆ:

อัพเดทเป็นประจำ

ตามสถิติจาก ESET LiveGrid® การแฝงตัวแบบใหม่และไม่ซ้ำกันหลายพันแบบจะถูกสร้างขึ้นทุกวันเพื่อให้สามารถผ่านการวัดความปลอดภัยที่มีอยู่และสร้างผลกำไรให้กับผู้เขียนได้ โดยสร้างความเสียหายให้เกิดขึ้นกับผู้ใช้อื่น ผู้เชี่ยวชาญของ ESET Virus Lab วิเคราะห์การคุกคามเหล่านี้ทุกวัน และจัดเตรียมและเผยแพร่การอัพเดทเพื่อปรับปรุงระดับการป้องกันสำหรับผู้ใช้ของเราอย่างต่อเนื่อง เพื่อให้แน่ใจว่าการอัพเดทเหล่านี้มีประสิทธิภาพสูงสุด ต้องมีการกำหนดค่าการอัพเดทอย่างถูกต้องในระบบของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีกำหนดค่าการอัพเดท โปรดดูในบท การตั้งค่าการอัพเดท

ดาวน์โหลดโปรแกรมแก้ไขด้านความปลอดภัย

ผู้เขียนซอฟต์แวร์ที่เป็นอันตรายมักใช้จุดอ่อนของระบบเพื่อเพิ่มประสิทธิภาพของการแพร่โค้ดที่เป็นอันตราย เมื่อทราบเช่นนี้แล้ว บริษัทซอฟต์แวร์จึงต้องติดตามจุดอ่อนต่างๆ อย่างใกล้ชิดในแอพพลิเคชันของตน เพื่อแสดงและเผยแพร่การอัพเดทการรักษาความปลอดภัยที่จะกำจัดการคุกคามที่อาจเกิดขึ้นเป็นประจำ จึงเป็นสิ่งจำเป็นที่ต้องดาวน์โหลดการอัพเดทการรักษาความปลอดภัยเหล่านี้เมื่อมีการเผยแพร่ Microsoft Windows และเว็บเบราว์เซอร์เช่น Microsoft Edge คือตัวอย่างของสองโปรแกรมที่มีการเผยแพร่การอัพเดทการรักษาความปลอดภัยตามกำหนดการเป็นประจำ

การสำรองข้อมูลสำคัญ

ผู้เขียนมัลแวร์จะไม่สนใจความต้องการของผู้ใช้ และการทำงานของโปรแกรมที่เป็นอันตรายมักจะนำไปสู่การทำงานไม่ถูกต้องทั้งหมดของระบบปฏิบัติการและการสูญหายของข้อมูลสำคัญ ดังนั้นจึงต้องสำรองข้อมูลของคุณไว้ในแหล่งที่มาภายนอกอยู่เสมอ เช่น ดีวีดีหรือฮาร์ดไดรฟ์ภายนอก ซึ่งจะทำให้กู้คืนข้อมูลของคุณได้ง่ายดายและรวดเร็ว

ยิ่งขึ้นในกรณีที่ระบบล้มเหลว

สแกนคอมพิวเตอร์เพื่อหาไวรัสเป็นประจำ

การตรวจหาไวรัส เวิร์ม โทรจัน และรูทคิทที่รู้จักและไม่รู้จักได้มากขึ้นจะมีการจัดการโดยโมดูลการป้องกันระบบไฟล์แบบเรียลไทม์ ซึ่งหมายความว่าทุกครั้งที่คุณเข้าถึงหรือเปิดไฟล์ ระบบจะสแกนเพื่อหากิจกรรมของมัลแวร์ เราขอแนะนำให้คุณเรียกใช้การสแกนคอมพิวเตอร์แบบเต็มรูปแบบอย่างน้อยเดือนละครั้ง เนื่องจากฐานข้อมูลมัลแวร์อาจหลากหลายและกลไกตรวจหาจะอัพเดทตัวเองทุกวัน

ปฏิบัติตามกฎการรักษาความปลอดภัยพื้นฐาน

กฎที่มีประโยชน์และมีประสิทธิภาพมากที่สุด คือควรระมัดระวังอยู่เสมอ ในปัจจุบัน การบุกรุกจำนวนมากต้องการการดำเนินการของผู้ใช้เพื่อให้ระบบทำงานและกระจายการบุกรุก หากคุณระมัดระวังเมื่อเปิดไฟล์ใหม่ คุณจะสามารถประหยัดเวลาและความพยายามที่จะต้องใช้ในการกำจัดการบุกรุกได้เป็นอย่างมาก คำแนะนำที่มีประโยชน์มีดังนี้:

- อย่าเข้าชมเว็บไซต์ที่น่าสงสัยที่มีโฆษณาป็อปอัพและแบบแฟลชจำนวนมาก
- ระมัดระวังเมื่อติดตั้งโปรแกรมฟรีแวร์ ชุดเข้ารหัส/ถอดรหัส เป็นต้น โปรดใช้โปรแกรมที่ปลอดภัยและเข้าสู่เว็บไซต์ทางอินเทอร์เน็ตที่ปลอดภัยเท่านั้น
- ระมัดระวังเมื่อเปิดสิ่งที่แนบมาของอีเมล โดยเฉพาะอย่างยิ่งข้อความที่ส่งให้ผู้รับจำนวนมากและข้อความจากผู้ส่งที่ไม่รู้จัก
- อย่าใช้บัญชีผู้ดูแลระบบสำหรับการทำงานประจำวันในคอมพิวเตอร์ของคุณ

สถานะสิ้นสุดอายุการใช้งาน

ESET Endpoint Security สามารถแสดงการแจ้งเตือนหรือส่งคำเตือนโดยอัตโนมัติเพื่อให้คุณทราบเกี่ยวกับข้อมูลสิ้นสุดอายุการใช้งานที่กำลังจะมาถึง ณ ตำแหน่งต่างๆ ในหน้าต่างโปรแกรมหลัก

> อ่านเพิ่มเติมเกี่ยวกับ:
> • นโยบายสิ้นสุดอายุการใช้งาน (ผลิตภัณฑ์ธุรกิจ)
> • การอัพเดทผลิตภัณฑ์
> • ฮอตฟิกซ์เกี่ยวกับความปลอดภัยและความเสถียร
> หากต้องการข้อมูลเพิ่มเติมเกี่ยวกับการเปลี่ยนแปลง ESET Endpoint Security โปรดอ่าน บทความฐานความรู้ ESET

ตารางด้านล่างแสดงตัวอย่างบางส่วนของสถานะผลิตภัณฑ์และการแจ้งเตือนให้ดำเนินการตามประเภทต่อไปนี้:

ประเภท	หน้าต่างการแจ้งเตือนหรือคำเตือน	หน้าอัพเดท	หน้าวิธีใช้และการสนับสนุน
มีฟีเจอร์ใหม่หรือการอัพเดทการให้บริการ	เวอร์ชันใหม่พร้อมให้บริการแล้ว มีการอัพเดทที่มีการแก้ไขการให้บริการที่สำคัญซึ่ง ESET Endpoint Security จำเป็นต้องมี อัพเดทตอนนี้เพื่อรับการป้องกันล่าสุด **การทำงาน**: เรียนรู้เพิ่มเติม	มี ESET Endpoint Security เวอร์ชันใหม่พร้อมให้ใช้งาน มี ESET Endpoint Security เวอร์ชันใหม่พร้อมให้ใช้งาน **การทำงาน**: อัพเดทตอนนี้/เปิดใช้งานการอัพเดทอัตโนมัติ	มี ESET Endpoint Security เวอร์ชันใหม่พร้อมให้ใช้งาน อัพเดทตอนนี้เพื่อรับเวอร์ชั่นล่าสุดพร้อมฟีเจอร์และการปรับปรุงใหม่ๆ รองรับจนถึง: ว/ดด/ปปปป
	มีการอัพเดทซ่อมบำรุงให้ใช้งาน มี ESET Endpoint Security เวอร์ชั่นใหม่พร้อมให้ใช้งาน อัพเดทตอนนี้เพื่อรับเวอร์ชั่นล่าสุดพร้อมฟีเจอร์และการปรับปรุงใหม่ๆ **การทำงาน**: เรียนรู้เพิ่มเติม	มีการอัพเดทซ่อมบำรุงสำหรับ ESET Endpoint Security ให้ใช้งาน หมายเลขเวอร์ชั่นที่ติดตั้ง รองรับจนถึง: ว/ดด/ปปปป **การทำงาน**: เรียนรู้เพิ่มเติม	มีการอัพเดทที่มีการแก้ไขการให้บริการที่สำคัญซึ่ง ESET Endpoint Security จำเป็นต้องมี อัพเดทตอนนี้เพื่อรับการป้องกันล่าสุด รองรับจนถึง: ว/ดด/ปปปป
	ขอแนะนำให้รีสตาร์ทอุปกรณ์ มีการอัพเดทที่มีการแก้ไขการให้บริการที่สำคัญซึ่ง ESET Endpoint Security จำเป็นต้องมี อัพเดทตอนนี้เพื่อรับการป้องกันล่าสุด **การทำงาน**: เรียนรู้เพิ่มเติม		รองรับจนถึง: ว/ดด/ปปปป
	มีการอัพเดทซ่อมบำรุงที่สำคัญอย่างยิ่งให้ใช้งาน มีการอัพเดทที่มีการแก้ไขการให้บริการที่จำเป็นซึ่ง ESET Endpoint Security จำเป็นต้องมี อัพเดทตอนนี้เพื่อรับการป้องกันล่าสุด **การทำงาน**: เรียนรู้เพิ่มเติม	มีการอัพเดทซ่อมบำรุงที่สำคัญอย่างยิ่งสำหรับ ESET Endpoint Security ให้ใช้งาน หมายเลขเวอร์ชั่นที่ติดตั้ง รองรับจนถึง: ว/ดด/ปปปป **การทำงาน**: เรียนรู้เพิ่มเติม	มีการอัพเดทที่มีการแก้ไขการให้บริการที่จำเป็นซึ่ง ESET Endpoint Security จำเป็นต้องมี อัพเดทตอนนี้เพื่อรับการป้องกันล่าสุด รองรับจนถึง: ว/ดด/ปปปป
	ต้องรีสตาร์ทอุปกรณ์ ดาวน์โหลดการอัพเดทเป็นหมายเลขเวอร์ชั่นแล้ว ซึ่งมีการแก้ไขการให้บริการที่สำคัญและการแก้ไขเสถียรภาพที่ ESET Endpoint Security จำเป็นต้องมี อัพเดทตอนนี้เพื่อรับการป้องกันล่าสุด **การทำงาน**: เรียนรู้เพิ่มเติม		รองรับจนถึง: ว/ดด/ปปปป

ประเภท	หน้าต่างการแจ้งเตือนหรือคำเตือน	หน้าอัพเดท	หน้าวิธีใช้และการสนับสนุน
การสนับสนุนสำหรับแอพพลิเคชันที่กำลังจะหมดอายุ	การสนับสนุนแอพพลิเคชันเวอร์ชั่นที่ติดตั้งอยู่จะสิ้นสุดลงในวันที่ วว/ดด/ปปปป และอุปกรณ์ของคุณจะสูญเสียการป้องกันในไม่ช้า อัพเดทตอนนี้เพื่อรับการป้องกันต่อไป **การทำงาน**: อัพเดททันที	หมายเลขเวอร์ชั่นที่ติดตั้ง/รองรับจนถึง: วว/ดด/ปปปป **การทำงาน**: อัพเดทตอนนี้/เปิดใช้งานการอัพเดทอัตโนมัติ	การสนับสนุน ESET Endpoint Security เวอร์ชันที่ติดตั้งอยู่ใกล้สิ้นสุดลงแล้ว ซึ่งจะทำให้คอมพิวเตอร์ของคุณสูญเสียการป้องกัน อัพเดทตอนนี้เพื่อรับการป้องกันต่อไป รองรับจนถึง: วว/ดด/ปปปป
	การสนับสนุนแบบขยายของ ESET สำหรับแอพพลิเคชันเวอร์ชันที่ติดตั้งอยู่จะสิ้นสุดลงในวันที่ วว/ดด/ปปปป และอุปกรณ์ของคุณจะสูญเสียการป้องกันในไม่ช้า อัพเดทตอนนี้เพื่อรับการป้องกันต่อไป **การทำงาน**: อัพเดททันที	หมายเลขเวอร์ชั่นที่ติดตั้ง/รองรับจนถึง: วว/ดด/ปปปป **การทำงาน**: อัพเดทตอนนี้/เปิดใช้งานการอัพเดทอัตโนมัติ	การสนับสนุนแบบขยายของ ESET สำหรับ ESET Endpoint Security เวอร์ชันที่ติดตั้งอยู่ใกล้สิ้นสุดลงแล้ว ซึ่งจะทำให้คอมพิวเตอร์ของคุณสูญเสียการป้องกัน อัพเดทตอนนี้เพื่อรับการป้องกันต่อไป รองรับจนถึง: วว/ดด/ปปปป
	ระบบปฏิบัติการที่ติดตั้งอยู่ล้าสมัยแล้ว และการสนับสนุนสำหรับแอพพลิเคชันเวอร์ชันที่ติดตั้งอยู่จะสิ้นสุดลงในวันที่ วว/ดด/ปปปป โปรดอัพเกรดระบบปฏิบัติการของคุณเพื่อรับการอัพเดทแอพพลิเคชันล่าสุดและให้ได้รับการป้องกันต่อไป **การทำงาน**: เรียนรู้เพิ่มเติม	หมายเลขเวอร์ชั่นที่ติดตั้ง รองรับจนถึง: วว/ดด/ปปปป **การทำงาน**: เรียนรู้เพิ่มเติม	การสนับสนุน ESET Endpoint Security เวอร์ชันที่ติดตั้งอยู่ใกล้สิ้นสุดลงแล้ว ซึ่งจะทำให้คอมพิวเตอร์ของคุณสูญเสียการป้องกัน อัพเดทตอนนี้เพื่อรับการป้องกันต่อไป รองรับจนถึง: วว/ดด/ปปปป
	การสนับสนุนแบบขยายของ ESET สำหรับแอพพลิเคชันเวอร์ชันที่ติดตั้งอยู่ใกล้สิ้นสุดลงแล้ว ระบบปฏิบัติการที่ติดตั้งอยู่ล้าสมัยแล้ว และการสนับสนุนสำหรับแอพพลิเคชันเวอร์ชันที่ติดตั้งอยู่จะสิ้นสุดลงในวันที่ วว/ดด/ปปปป โปรดอัพเกรดระบบปฏิบัติการของคุณเพื่อรับการอัพเดทแอพพลิเคชันล่าสุดและให้ได้รับการป้องกันต่อไป **การทำงาน**: เรียนรู้เพิ่มเติม	การสนับสนุนแบบขยายของ ESET สำหรับ ESET Endpoint Security เวอร์ชันที่ติดตั้งอยู่ใกล้สิ้นสุดลงแล้ว หมายเลขเวอร์ชั่นที่ติดตั้ง รองรับจนถึง: วว/ดด/ปปปป **การทำงาน**: เรียนรู้เพิ่มเติม	การสนับสนุนแบบขยายของ ESET สำหรับ ESET Endpoint Security เวอร์ชันที่ติดตั้งอยู่ใกล้สิ้นสุดลงแล้ว ซึ่งจะทำให้คอมพิวเตอร์ของคุณสูญเสียการป้องกัน อัพเดทตอนนี้เพื่อรับการป้องกันต่อไป รองรับจนถึง: วว/ดด/ปปปป

ประเภท	หน้าต่างการแจ้งเตือนหรือคำเตือน	หน้าอัพเดท	หน้าวิธีใช้และการสนับสนุน
แอพพลิเคชันเวอร์ชันนี้ไม่รองรับอีกต่อไป	⚠ แอพพลิเคชันที่ติดตั้งอยู่ไม่ได้รับการสนับสนุนอีกต่อไปแล้ว การสนับสนุนสำหรับแอพพลิเคชันเวอร์ชันที่ติดตั้งอยู่ของคุณสิ้นสุดลงแล้ว ซึ่งอาจทำให้อุปกรณ์ของคุณไม่ได้รับการป้องกัน อัพเดทตอนนี้เพื่อรับการป้องกัน **การทำงาน**: อัพเดททันที	⚠ ESET Endpoint Security เวอร์ชันที่ติดตั้งอยู่ไม่ได้รับการสนับสนุนอีกต่อไป หมายเลขเวอร์ชั่นที่ติดตั้ง/รองรับจนถึง: ว/ดด/ปปปป **การทำงาน**: อัพเดทตอนนี้/เปิดใช้งานการอัพเดทอัตโนมัติ	⚠ รองรับจนถึง: ว/ดด/ปปปป
	⚠ แอพพลิเคชันที่ติดตั้งอยู่ไม่ได้รับการสนับสนุนอีกต่อไปแล้ว ระบบปฏิบัติการที่ติดตั้งอยู่ล้าสมัยแล้ว และการสนับสนุนสำหรับแอพพลิเคชันเวอร์ชันที่ติดตั้งอยู่จะสิ้นสุดลงในวันที่ คอมพิวเตอร์ของคุณไม่ได้รับการป้องกัน อัพเกรดระบบปฏิบัติการของคุณเพื่อรับการอัพเดทแอพพลิเคชันล่าสุดและรับการป้องกัน **การทำงาน**: เรียนรู้เพิ่มเติม	⚠ ESET Endpoint Security เวอร์ชันที่ติดตั้งอยู่ไม่ได้รับการสนับสนุนอีกต่อไป หมายเลขเวอร์ชั่นที่ติดตั้ง รองรับจนถึง: ว/ดด/ปปปป **การทำงาน**: เรียนรู้เพิ่มเติม	⚠ การสนับสนุน ESET Endpoint Security เวอร์ชันที่ติดตั้งอยู่สิ้นสุดลงแล้ว ซึ่งทำให้คอมพิวเตอร์ของคุณไม่ได้รับการป้องกัน อัพเดทตอนนี้เพื่อรับการป้องกัน รองรับจนถึง: ว/ดด/ปปปป
ต้องมีการอัพเดทระบบปฏิบัติการ	⚠ ระบบปฏิบัติการที่ติดตั้งอยู่ล้าสมัยแล้ว ระบบปฏิบัติการที่ติดตั้งอยู่ล้าสมัยแล้ว โปรดอัพเกรดระบบปฏิบัติการของคุณเพื่อรับการอัพเดทแอพพลิเคชันล่าสุดและให้ได้รับการป้องกันต่อไป **การทำงาน**: เรียนรู้เพิ่มเติม	✔ ESET Endpoint Security หมายเลขเวอร์ชั่นที่ติดตั้ง	รองรับจนถึง: ว/ดด/ปปปป

หน้าวิธีใช้

ยินดีต้อนรับสู่คู่มือผู้ใช้ ESET Endpoint Security ข้อมูลที่ให้ไว้นี้จะแนะนำคุณเกี่ยวกับผลิตภัณฑ์ของคุณและช่วยทำให้คอมพิวเตอร์ของคุณมีความปลอดภัยมากยิ่งขึ้น

การเริ่มต้นใช้งาน

ก่อนที่คุณจะเริ่มใช้ ESET Endpoint Security โปรดทราบว่าผลิตภัณฑ์สามารถ จัดการได้จากระยะไกลโดยใช้ ESET PROTECT เราขอแนะนำให้คุณสร้างความคุ้นเคยกับ ประเภทการตรวจหา และ การโจมตีระยะไกล ที่คุณอาจพบได้เมื่อใช้คอมพิวเตอร์ของคุณ

โปรดดู คุณลักษณะใหม่ เพื่อเรียนรู้เกี่ยวกับคุณลักษณะที่เริ่มใช้ใน ESET Endpoint Security เวอร์ชันนี้ พวกเรายังได้จัดเตรียมคู่มือเพื่อช่วยให้คุณตั้งค่าและปรับแต่งการตั้งค่าพื้นฐานของ ESET Endpoint Security

วิธีใช้หน้าวิธีใช้ของ ESET Endpoint Security

หัวข้อวิธีใช้จะแบ่งออกเป็นหลายบทและบทย่อยเพื่อสร้างความเข้าใจและมีบริบท คุณจะพบข้อมูลที่เกี่ยวข้องได้ด้วยการเรียกดูโครงสร้างของหน้าวิธีใช้

กด **F1** เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับหน้าต่างใดก็ตามในโปรแกรม หน้าวิธีใช้ที่เกี่ยวข้องกับหน้าต่างที่คุณเปิดอยู่จะปรากฏขึ้น

คุณสามารถค้นหาหน้าวิธีใช้ด้วยการใช้คำหลักหรือพิมพ์คำหรือวลีต่างๆ ความแตกต่างระหว่างสองวิธีนี้ก็คือ คำหลักนั้นอาจมีเนื้อหาเกี่ยวข้องกับหน้าวิธีใช้ที่ไม่ได้มีคำหลักนั้นๆ อยู่ในข้อความก็ได้ การค้นหาตามคำและวลีจะค้นหาเนื้อหาของหน้าวิธีใช้ทั้งหมด และแสดงเฉพาะที่มีคำหรือวลีนั้นๆ

เพื่อความสอดคล้องและช่วยป้องกันการสับสน ศัพท์บัญญัติที่ใช้ในคำแนะนำนี้จะไปเป็นตามชื่อศัพท์บัญญัติพารามิเตอร์ของ ESET Endpoint Security นอกจากนี้เรายังใช้ชุดรูปแบบสัญลักษณ์ชุดหนึ่งเพื่อเน้นหัวข้อต่างๆ ที่น่าสนใจเป็นพิเศษหรือมีความสำคัญ

บันทึกย่อเป็นเพียงการสำรวจสั้นๆ เท่านั้น ถึงแม้ว่าคุณจะสามารถข้ามได้ แต่บันทึกย่อมีข้อมูลที่มีประโยชน์อย่างยิ่ง เช่น คุณสมบัติที่เฉพาะเจาะจงหรือลิงก์ไปที่หัวข้อบางหัวข้อ

ซึ่งคุณควรให้ความใส่ใจกับบันทึกนี้ เราจึงขอแนะนำไม่ให้คุณข้าม ปกติแล้ว ในบันทึกจะมีข้อมูลที่ไม่จำเป็นแต่มีความสำคัญ

นี่เป็นข้อมูลที่ต้องให้ความใส่ใจและระมัดระวังเป็นพิเศษ มีการระบุคำเตือนไว้อย่างเจาะจงเพื่อป้องกันไม่ให้คุณทำสิ่งผิดพลาดที่อาจเป็นอันตราย โปรดอ่านและทำความเข้าใจข้อความที่อยู่ในวงเล็บคำเตือน เนื่องจากข้อความเหล่านี้จะพูดถึงระบบที่สำคัญมากหรือสิ่งต่างๆ ที่มีความเสี่ยง

การดำเนินการนี้เป็นรูปแบบการใช้หรือตัวอย่างภาคปฏิบัติซึ่งมีวัตถุประสงค์เพื่อช่วยให้คุณเข้าใจว่าสามารถใช้ฟังก์ชันหรือคุณลักษณะบางอย่างได้อย่างไร

รูปแบบ	ความหมาย
ประเภทตัวหนา	ชื่อของรายการส่วนติดต่อต่างๆ เช่น กล่องและปุ่มตัวเลือก
ประเภทตัวเอียง	ตัวยึดสำหรับข้อมูลที่คุณป้อน ตัวอย่างเช่น ชื่อไฟล์ หรือ พาธ หมายความว่าคุณพิมพ์พาธหรือชื่อไฟล์ดังกล่าว
`Courier New`	ตัวอย่างโค้ดหรือคำสั่งต่างๆ
ไฮเปอร์ลิงค์	มอบเส้นทางที่รวดเร็วและง่ายดายในการข้ามไปสู่หัวข้อที่อ้างถึงหรือตำแหน่งเว็บภายนอก ไฮเปอร์ลิงค์จะถูกไฮไลท์เป็นสีฟ้าและอาจขีดเส้นใต้
%ProgramFiles%	ไดเรกทอรีของระบบ Windows ซึ่งจัดเก็บโปรแกรมที่ติดตั้งลงใน Windows เอาไว้

วิธีใช้ออนไลน์ เป็นแหล่งข้อมูลหลักของเนื้อหาวิธีใช้ วิธีใช้ออนไลน์เวอร์ชันล่าสุดจะแสดงโดยอัตโนมัติเวลาที่คุณมีการเชื่อมต่ออินเทอร์เน็ตที่ใช้งานได้

เอกสารประกอบสำหรับอุปกรณ์ปลายทางที่จัดการจากระยะไกล

ผลิตภัณฑ์ ESET Business เช่นเดียวกับ ESET Endpoint Security สามารถจัดการระยะไกลบนเวิร์กสเตชันไคลเอ็นต์ เซิร์ฟเวอร์ และอุปกรณ์เคลื่อนที่ในสภาพแวดล้อมการทำงานของเครือข่ายจากจุดศูนย์กลางจุดเดียว ผู้ดูแลระบบที่จัดการมากกว่า 10 เวิร์กสเตชันไคลเอ็นต์อาจพิจารณาการปรับใช้หนึ่งในเครื่องมือการจัดการระยะไกลของ ESET เพื่อปรับใช้โซลูชัน ESET จัดการงาน บังคับใช้นโยบายด้านความปลอดภัย ตรวจสอบสถานะระบบและตอบสนองต่อปัญหาหรือภัยคุกคามบนคอมพิวเตอร์ระยะไกลจากจุดศูนย์กลางจุดเดียวได้อย่างรวดเร็ว

เครื่องมือการจัดการระยะไกลของ ESET

ESET Endpoint Security สามารถจัดการจากระยะไกลได้โดยใช้ทั้ง ESET PROTECT หรือ ESET PROTECT Cloud

- บทแนะนำเกี่ยวกับ ESET PROTECT
- บทแนะนำเกี่ยวกับ ESET PROTECT Cloud

- ESET HUB – เกตเวย์กลางไปยัง ESET PROTECT ซึ่งเป็นแพลตฟอร์มการรักษาความปลอดภัยแบบครบวงจร ซึ่งจะมีข้อมูลประจำตัว การสมัครใช้งาน และการจัดการผู้ใช้แบบรวมศูนย์สำหรับโมดูลแพลตฟอร์ม ESET ทั้งหมด ดูคำแนะนำในการเปิดใช้งานผลิตภัณฑ์ของคุณได้ที่ ESET PROTECT การจัดการใบอนุญาต ESET HUB จะแทนที่ ESET Business Account และ ESET MSP Administrator โดยสมบูรณ์

- ESET Business Account – คือพอร์ทัลจัดการใบอนุญาตสำหรับผลิตภัณฑ์ทางธุรกิจของ ESET โปรดดูESET PROTECTการจัดการใบอนุญาต เพื่อดูคำแนะนำในการเปิดใช้งานผลิตภัณฑ์ของคุณ หรือดูESET Business Accountวิธีใช้แบบออนไลน์ เพื่อดูข้อมูลเพิ่มเติมเกี่ยวกับการใช้ ESET Business Account หากคุณมีชื่อผู้ใช้และรหัสผ่านที่ ESET เป็นผู้ออกให้และต้องการแปลงเป็นรหัสใบอนุญาต โปรดดูส่วน แปลงข้อมูลการเข้าสู่ระบบดั้งเดิม

ผลิตภัณฑ์รักษาความปลอดภัยเพิ่มเติม

- ESET Inspect - ระบบ Endpoint Detection and Response แบบครบวงจรซึ่งมีคุณลักษณะ เช่น การตรวจหา การจัดการและการตอบสนองต่อเหตุการณ์ การรวบรวมข้อมูล ตัวชี้วัดการตรวจหาที่ถูกคุกคาม การตรวจหาที่ผิดปกติ การตรวจหาพฤติกรรม และการละเมิดนโยบาย

- ESET Endpoint Encryption – เป็นแอพพลิเคชันด้านความปลอดภัยที่ครอบคลุมซึ่งออกแบบมาเพื่อปกป้องข้อมูลของคุณทั้งในระหว่างที่ใช้งานและไม่ได้ใช้งาน คุณสามารถใช้ ESET Endpoint Encryption เพื่อเข้ารหัสไฟล์ โฟลเดอร์ และอีเมล หรือสร้างดิสก์เสมือนที่เข้ารหัส บีบอัดไฟล์ที่เก็บถาวร ตลอดจนเพิ่มเครื่องทำลายสำหรับเดสก์ท็อปเพื่อให้ลบไฟล์ได้อย่างปลอดภัย

เครื่องมือการจัดการระยะไกลของบริษัทอื่น

- การตรวจสอบและการจัดการระยะไกล (RMM)

แนวทางปฏิบัติ

- เชื่อมต่ออุปกรณ์ปลายทางทั้งหมดด้วย ESET Endpoint Security เข้ากับ ESET PROTECT
- ปกป้องการตั้งค่าขั้นสูงบนคอมพิวเตอร์ไคลเอ็นต์ที่เชื่อมต่อเพื่อหลีกเลี่ยงการแก้ไขโดยไม่ได้รับอนุญาต
- นำนโยบายที่แนะนำไปใช้เพื่อบังคับใช้คุณลักษณะด้านความปลอดภัยที่มีให้ใช้งาน
- ย่อขนาดส่วนติดต่อกับผู้ใช้ – เพื่อลดหรือจำกัดการโต้ตอบของผู้ใช้กับ ESET Endpoint Security

วิธีการแนะนำ

- วิธีการใช้โหมดเขียนทับ
- วิธีปรับใช้ ESET Endpoint Security โดยใช้ GPO หรือ SCCM

บทแนะนำเกี่ยวกับ ESET PROTECT

ESET PROTECT ช่วยให้คุณจัดการผลิตภัณฑ์ ESET บนเวิร์กสเตชัน เซิร์ฟเวอร์ และอุปกรณ์เคลื่อนที่ในสภาพแวดล้อมการทำงานของเครือข่ายจากจุดศูนย์กลางจุดเดียว

ด้วยการใช้เว็บคอนโซล ESET PROTECT คุณสามารถปรับใช้โซลูชัน ESET จัดการงาน บังคับใช้นโยบายด้านความปลอดภัย ตรวจสอบสถานะระบบและตอบสนองต่อปัญหาหรือภัยคุกคามบนคอมพิวเตอร์ระยะไกลได้อย่างรวดเร็ว โปรดดูภาพรวมของสถาปัตยกรรมและองค์ประกอบโครงสร้างพื้นฐานของ ESET PROTECT การเริ่มต้นใช้งานเว็บคอนโซล ESET PROTECT และ สภาพแวดล้อมการจัดเตรียมเดสก์ท็อปที่รองรับ

ESET PROTECT ประกอบด้วยส่วนประกอบต่อไปนี้:

- ESET PROTECT เอเจนท์ - เซิร์ฟเวอร์นี้จัดการการสื่อสารกับตัวแทน แล้วรวบรวมและจัดเก็บข้อมูล

แอพพลิเคชันในฐานข้อมูล เซิร์ฟเวอร์ ESET PROTECT สามารถติดตั้งได้บนเซิร์ฟเวอร์ Windows และ Linux อีกทั้งยังมาในรูปแบบ Virtual Appliance ด้วย

- เว็บคอนโซล ESET PROTECT - เว็บคอนโซล เป็นส่วนติดต่อผู้ใช้บนเว็บที่อนุญาตให้คุณจัดการกับคอมพิวเตอร์ไคลเอ็นต์ในสภาพแวดล้อมของคุณ เว็บคอนโซลนี้จะแสดงภาพรวมสถานะไคลเอ็นต์ในเครือข่ายของคุณและทำให้คุณสามารถปรับใช้โซลูชัน ESET กับคอมพิวเตอร์ที่ไม่ได้รับการจัดการแบบระยะไกล หลังจากคุณติดตั้งเซิร์ฟเวอร์ ESET PROTECT แล้ว คุณจะสามารถเข้าถึงเว็บคอนโซลได้โดยใช้เว็บเบราว์เซอร์ของคุณ หากคุณเลือกทำให้เว็บเซิร์ฟเวอร์สามารถใช้งานได้ผ่านอินเทอร์เน็ต คุณจะสามารถใช้ ESET PROTECT จากสถานที่หรืออุปกรณ์ใดๆ ที่มีการเชื่อมต่ออินเทอร์เน็ตได้
- เอเจนต์ ESET Management - ช่วยอำนวยความสะดวกในการสื่อสารระหว่างเซิร์ฟเวอร์ ESET PROTECT และคอมพิวเตอร์ไคลเอ็นต์ เอเจนต์ต้องถูกติดตั้งบนคอมพิวเตอร์ไคลเอ็นต์เพื่อสร้างการสื่อสารระหว่างคอมพิวเตอร์เครื่องนั้นและเซิร์ฟเวอร์ ESET PROTECT เนื่องจากเอเจนต์อยู่ในคอมพิวเตอร์ไคลเอ็นต์และสามารถจัดเก็บสถานการณ์ของการรักษาความปลอดภัยได้หลายสถานการณ์ การใช้เอเจนต์ ESET Management จะลดเวลาตอบโต้กับภัยคุกคามใหม่ๆ ได้อย่างมาก เมื่อใช้เว็บคอนโซล ESET PROTECT คุณจะสามารถปรับใช้เอเจนต์ ESET Management กับคอมพิวเตอร์ที่ไม่ได้รับการจัดการที่ระบุโดย Active Directory หรือเซนเซอร์ RDของ ESET ได้ คุณยังสามารถติดตั้งเอเจนต์ ESET Management ได้เองบนคอมพิวเตอร์ไคลเอ็นต์ หากจำเป็น
- ESET Rogue Detection Sensor—ตรวจจับคอมพิวเตอร์ที่ไม่ได้รับการจัดการบนเครือข่ายของคุณและส่งข้อมูลของคอมพิวเตอร์เหล่านี้ไปยังเซิร์ฟเวอร์ ESET PROTECT ซึ่งจะช่วยให้คุณจัดการคอมพิวเตอร์ไคลเอนต์ใหม่ใน ESET PROTECT ได้โดยไม่จำเป็นต้องค้นหาและเพิ่มด้วยตนเอง Rogue Detection Sensor จดจำคอมพิวเตอร์ที่ถูกค้นพบและจะไม่ส่งข้อมูลเดิมซ้ำ
- ESET Bridge - คือบริการที่สามารถใช้ร่วมกับ ESET PROTECT เพื่อทำสิ่งต่างๆ ต่อไปนี้:
    - แจกจ่ายอัพเดทไปยังไคลเอ็นต์คอมพิวเตอร์และแพ็คเกจการติดตั้งไปยังตัวแทนESET Management
    - ส่งต่อการสื่อสารจากเอเจนต์ ESET Management ไปยังเซิร์ฟเวอร์ ESET PROTECT
- Mobile Device Connector - คือส่วนประกอบที่อนุญาตสำหรับการจัดการอุปกรณ์เคลื่อนที่ที่มี ESET PROTECT ทำให้คุณสามารถจัดการอุปกรณ์เคลื่อนที่ได้ (Android และ iOS) และดูแล ESET Endpoint Security for Android
- ESET PROTECT Virtual Appliance - มีจุดประสงค์สำหรับผู้ใช้ที่ต้องการใช้ ESET PROTECT ในสภาพแวดล้อมเสมือนจริง
- โฮสต์ตัวแทนเสมือน ESET PROTECT—เป็นส่วนประกอบของ ESET PROTECT ที่จำลองเอนทิตีตัวแทนขึ้นเพื่อจัดการเครื่องเสมือนที่ไม่มีตัวแทน โซลูชันนี้เปิดใช้งานระบบอัตโนมัติ การใช้งานกลุ่มไดนามิค และการจัดการงานในระดับเดียวกันในฐานะตัวแทน ESET Management บนคอมพิวเตอร์เครื่องจริง ตัวแทนเสมือน

รวบรวมข้อมูลจากเครื่องเสมือนและส่งไปยังเซิร์ฟเวอร์ ESET PROTECT

- เครื่องมือมิเรอร์—จำเป็นสำหรับการอัพเดทโมดูลออฟไลน์ หากคอมพิวเตอร์ไคลเอ็นต์ของคุณไม่มีการเชื่อมต่ออินเทอร์เน็ต คุณสามารถใช้เครื่องมือมิเรอร์เพื่อดาวน์โหลดไฟล์การอัพเดทจากเซิร์ฟเวอร์การอัพเดทของ ESET และจัดเก็บไว้ในเครื่องของคุณได้
- ESET Remote Deployment Tool—ปรับใช้แพ็คเกจแบบครบวงจรที่ถูกสร้างในเว็บคอนโซล <%PRODUCT%> ถือเป็นวิธีที่สะดวกในการแจกจ่ายตัวแทน ESET Management ที่มีผลิตภัณฑ์ ESET อยู่บนคอมพิวเตอร์ผ่านเครือข่าย

สำหรับข้อมูลเพิ่มเติม โปรดดู วิธีใช้ออนไลน์ของ ESET PROTECT

บทแนะนำเกี่ยวกับ ESET PROTECT Cloud

ESET PROTECT Cloud ให้คุณจัดการผลิตภัณฑ์ ESET บนเวิร์กสเตชันและเซิร์ฟเวอร์ในสภาพแวดล้อมแบบเครือข่ายจากจุดศูนย์กลางจุดเดียวโดยไม่มีข้อกำหนดให้มีเซิร์ฟเวอร์ทางกายภาพหรือเซิร์ฟเวอร์เสมือนเช่นเดียวกับ ESET PROTECT เมื่อใช้ (เว็บคอนโซล ESET PROTECT Cloud) คุณจะสามารถปรับใช้โซลูชัน ESET, จัดการงาน, บังคับใช้นโยบายความปลอดภัย, ตรวจสอบสถานะระบบและรับมือกับปัญหาหรือภัยคุกคามในคอมพิวเตอร์ระยะไกลได้อย่างรวดเร็ว

ESET PROTECT Cloud ประกอบด้วยส่วนประกอบต่อไปนี้:

- อินสแตนซ์ ESET PROTECT Cloud – ทำหน้าที่จัดการการสื่อสารกับเอเจนท์ จากนั้นรวบรวมและจัดเก็บข้อมูลแอพพลิเคชันในฐานข้อมูล
- เว็บคอนโซล ESET PROTECT Cloud - เว็บคอนโซล เป็นส่วนติดต่อผู้ใช้บนเว็บที่อนุญาตให้คุณจัดการกับคอมพิวเตอร์ไคลเอ็นต์ในสภาพแวดล้อมของคุณ เว็บคอนโซลนี้จะแสดงภาพรวมสถานะไคลเอ็นต์ในเครือข่ายของคุณและทำให้คุณสามารถปรับใช้โซลูชัน ESET กับคอมพิวเตอร์ที่ไม่ได้รับการจัดการแบบระยะไกล คุณสามารถใช้ ESET PROTECT Cloud จากที่ใดก็ได้ด้วยอุปกรณ์ที่มีการเชื่อมต่ออินเทอร์เน็ต
- เอเจนท์ ESET Management – ช่วยอำนวยความสะดวกในการสื่อสารระหว่างเซิร์ฟเวอร์ ESET PROTECT Cloud และคอมพิวเตอร์ไคลเอ็นต์ เอเจนต์ต้องได้รับการติดตั้งบนคอมพิวเตอร์ไคลเอ็นต์เพื่อสร้างการสื่อสารระหว่างคอมพิวเตอร์เครื่องนั้นและ ESET PROTECT Cloud เนื่องจากเอเจนต์อยู่ในคอมพิวเตอร์ไคลเอ็นต์และสามารถจัดเก็บสถานการณ์ของการรักษาความปลอดภัยได้หลายสถานการณ์ การใช้เอเจนต์ ESET Management จะลดเวลาตอบโต้กับภัยคุกคามใหม่ๆ ได้อย่างมาก เมื่อใช้เว็บคอนโซล ESET PROTECT Cloud คุณจะสามารถปรับใช้ESET Managementเอเจนท์กับคอมพิวเตอร์ที่ไม่ได้รับการจัดการ คุณยังสามารถติดตั้งเอเจนต์ ESET Management ได้เองบนคอมพิวเตอร์ไคลเอ็นต์ หากจำเป็น

- ESET Bridge - คือบริการที่สามารถใช้ร่วมกับ ESET PROTECT Cloud เพื่อทำสิ่งต่างๆ ต่อไปนี้:
    - แจกจ่ายอัพเดทไปยังไคลเอ็นต์คอมพิวเตอร์และแพ็คเกจการติดตั้งไปยังตัวแทนESET Management
    - ส่งต่อการสื่อสารจากเอเจนท์ ESET Management ไปยัง ESET PROTECT Cloud
- การจัดการอุปกรณ์เคลื่อนที่ - คือส่วนประกอบที่อนุญาตสำหรับการจัดการอุปกรณ์เคลื่อนที่ที่มี ESET PROTECT Cloud ทำให้คุณสามารถจัดการอุปกรณ์เคลื่อนที่ได้ (Android และ iOS) และดูแล ESET Endpoint Security for Android
- การจัดการจุดอ่อนและแพทช์ – ฟีเจอร์ใน ESET PROTECT Cloud ที่จะสแกนเวิร์กสเตชันเป็นประจำเพื่อตรวจหาซอฟต์แวร์ที่ติดตั้งไว้ซึ่งอาจมีความเสี่ยงด้านความปลอดภัย การจัดการแพทช์ ช่วยแก้ไขความเสี่ยงเหล่านี้ผ่านการอัพเดทซอฟต์แวร์อัตโนมัติ ทำให้อุปกรณ์มีความปลอดภัยมากขึ้น

สำหรับข้อมูลเพิ่มเติม โปรดดู วิธีใช้ออนไลน์ของ ESET PROTECT Cloud

การตั้งค่าที่ป้องกันด้วยรหัสผ่าน

หากต้องการมอบความปลอดภัยสูงสุดให้กับระบบของคุณ ESET Endpoint Security ต้องได้รับการกำหนดค่าให้ถูกต้อง การเปลี่ยนแปลงหรือการตั้งค่าใดๆ ที่ไม่เข้าเกณฑ์อาจทำให้ความปลอดภัยและระดับการป้องกันของลูกค้าลดลง หากต้องการจำกัดไม่ให้ผู้ใช้เข้าถึงการตั้งค่าขั้นสูง ผู้ดูแลระบบสามารถใช้รหัสผ่านป้องกันการตั้งค่าได้

ผู้ดูแลระบบสามารถสร้างนโยบายสำหรับรหัสผ่านเพื่อปกป้องการตั้งค่าขั้นสูงสำหรับ ESET Endpoint Security บนคอมพิวเตอร์ไคลเอ็นต์ที่เชื่อมต่ออยู่ หากต้องการสร้างนโยบายใหม่ให้ทำดังนี้:

1. ในเว็บคอนโซล ESET PROTECT ให้คลิก **นโยบาย** ในเมนูหลักทางซ้าย
2. คลิก **นโยบายใหม่**
3. ตั้งชื่อนโยบายใหม่ของคุณ และใส่รายละเอียดหรือไม่ก็ได้ คลิกปุ่ม **ดำเนินการต่อ**
4. จากรายการผลิตภัณฑ์ ให้เลือก **ESET Endpoint สำหรับ Windows**
5. คลิก **ส่วนติดต่อผู้ใช้** ในส่วน**Settings** แล้วขยาย**การตั้งค่าการเข้าถึง**
6. ให้คลิกปุ่มสลับเพื่อเปิดใช้งาน **รหัสผ่านเพื่อป้องกันการตั้งค่า** ตามเวอร์ชันของ ESET Endpoint Security โปรดระลึกว่าผลิตภัณฑ์ ESET Endpoint เวอร์ชัน 7 มีการป้องกันที่ได้รับการปรับปรุงแล้ว หากคุณมีผลิตภัณฑ์ Endpoint ทั้งเวอร์ชัน 7 และเวอร์ชัน 6 อยู่ในเครือข่าย เราขอแนะนำให้คุณตั้งรหัสผ่านที่แตกต่างกันสำหรับแต่ละเวอร์ชัน
7. ในหน้าต่างการแจ้งเตือน ให้สร้างรหัสผ่านใหม่ ยืนยันรหัสผ่าน แล้วคลิก **ตกลง** คลิก **ดำเนินการต่อ**
8. กำหนดนโยบายให้กับไคลเอ็นต์ ให้คลิก**กำหนด** แล้วเลือกคอมพิวเตอร์หรือกลุ่มของคอมพิวเตอร์เพื่อให้

ป้องกันด้วยรหัสผ่าน คลิก **ตกลง** เพื่อยืนยัน

9. ตรวจสอบว่าคอมพิวเตอร์ไคลเอ็นต์ที่ต้องการทั้งหมดอยู่ในรายการเป้าหมายและคลิก **ดำเนินการต่อ**
10. ตรวจดูการตั้งค่านโยบายในข้อมูลสรุป แล้วคลิก **สิ้นสุด** เพื่อบันทึกนโยบายใหม่

นโยบายคืออะไร

ผู้ดูแลระบบสามารถผลักดันการกำหนดค่าเฉพาะไปที่ผลิตภัณฑ์ ESET ที่กำลังทำงานบนคอมพิวเตอร์ไคลเอ็นต์โดยใช้นโยบายจากเว็บคอนโซล ESET PROTECT สามารถนำนโยบายมาใช้ได้โดยตรงกับคอมพิวเตอร์แต่ละเครื่องและกลุ่มของคอมพิวเตอร์ คุณยังสามารถกำหนดนโยบายหลายนโยบายให้กับคอมพิวเตอร์หนึ่งเครื่องหรือหลายเครื่องได้อีกด้วย

ผู้ใช้ต้องมีสิทธิ์ต่อไปนี้เพื่อสร้างนโยบายใหม่: สิทธิ์ **อ่าน** เพื่ออ่านรายการนโยบาย สิทธิ์ **ใช้** เพื่อกำหนดนโยบายให้กับคอมพิวเตอร์เป้าหมาย และสิทธิ์ **เขียน** เพื่อสร้าง ปรับ หรือแก้ไขนโยบาย

นโยบายจะถูกนำไปใช้ในลำดับของกลุ่มคงที่ สำหรับกลุ่มไดนามิคนั้น นโยบายจะถูกนำไปใช้กับกลุ่มไดนามิคย่อยก่อน การดำเนินการนี้จะทำให้คุณสามารถปรับใช้นโยบายได้โดยส่งผลมากขึ้นต่อด้านบนสุดของโครงกลุ่ม และนำนโยบายที่เฉพาะเจาะจงกว่าไปใช้กับกลุ่มย่อย การใช้ ธง ผู้ใช้ ESET Endpoint Security ที่มีการเข้าถึงกลุ่มที่อยู่ในโครงระดับสูงกว่าสามารถเขียนทับนโยบายของกลุ่มในระดับต่ำกว่าได้ ดูคำอธิบายอัลกอริทึมได้ใน วิธีใช้ออนไลน์ของ ESET PROTECT

> **i** เราแนะนำให้กำหนดนโยบายทั่วไป (ตัวอย่างเช่น นโยบายเซิร์ฟเวอร์การอัพเดท) ไปยังกลุ่มระดับสูงกว่าภายในโครงกลุ่ม) ควรนโยบายที่เฉพาะเจาะจงมากกว่า (ตัวอย่างเช่น การตั้งค่าการควบคุมอุปกรณ์) ให้กับโครงกลุ่มที่อยู่ระดับลึกกว่า นโยบายระดับต่ำมักจะเขียนทับการตั้งค่าของนโยบายในระดับสูงกว่าเมื่อถูกนำมารวมกัน (ยกเว้นระบุไว้เป็นอย่างอื่นโดยใช้ ธงนโยบาย)

การรวมนโยบาย

นโยบายที่นำมาใช้กับไคลเอ็นต์มักเป็นผลมาจากนโยบายหลายนโยบายที่ถูกรวมเข้าด้วยกันเป็นนโยบายสุดท้ายหนึ่งรายการ นโยบายถูกรวมเข้าด้วยกันทีละรายการ เมื่อรวมนโยบาย กฎทั่วไปคือนโยบายหลังสุดจะมาแทนที่ชุดการตั้งค่าโดยนโยบายเก่า หากต้องการเปลี่ยนการทำงานนี้ คุณสามารถใช้ธงนโยบาย (มีให้ใช้งานสำหรับการตั้งค่าแต่ละรายการ)

เมื่อสร้างนโยบาย คุณจะสังเกตว่าการตั้งค่าบางรายการมีกฎเพิ่มเติม (แทนที่/ต่อท้าย/ขึ้นต้น) ซึ่งคุณสามารถกำหนดค่าได้

- **แทนที่** - รายการทั้งหมดจะถูกแทนที่ เพิ่มค่าใหม่ และลบค่าก่อนหน้าออกทั้งหมด
- **ต่อท้าย** - รายการถูกเพิ่มที่ด้านล่างสุดของรายการที่นำมาใช้ในปัจจุบัน (ต้องเป็นนโยบายอื่น รายการในเครื่องจะถูกเขียนทับเสมอ)
- **ขึ้นต้น** - รายการถูกเพิ่มที่ด้านบนสุดของรายการที่นำมาใช้ในปัจจุบัน (รายการในเครื่องจะถูกเขียนทับ)

ESET Endpoint Security รองรับการรวมการตั้งค่าในเครื่องกับนโยบายระยะไกลในรูปแบบใหม่ หากการตั้งค่าเป็นรายการ (ตัวอย่างเช่น รายการของเว็บไซต์ที่ปิดกั้น) และนโยบายระยะไกลขัดแย้งกับการตั้งค่าในเครื่องที่มีอยู่ นโยบายระยะไกลจะเขียนทับการตั้งค่าในเครื่องที่มีอยู่ คุณสามารถเลือกวิธีการรวมรายการในเครื่องและระยะไกลได้โดยเลือกกฎการรวมที่แตกต่างสำหรับ:

- การตั้งค่าการรวมสำหรับนโยบายระยะไกล
- การรวมนโยบายระยะไกลและนโยบายในเครื่อง - การตั้งค่าในเครื่องที่มีนโยบายระยะไกล

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการรวมนโยบาย โปรดดูที่ESET PROTECTคู่มือผู้ใช้ออนไลน์ แล้วดู ตัวอย่าง

ธงทำงานอย่างไร

นโยบายที่นำไปใช้กับคอมพิวเตอร์ไคลเอ็นต์มักจะมาจากนโยบายหลายๆ รายการรวมกันเป็นนโยบายสุดท้ายหนึ่งนโยบาย เมื่อรวมนโยบาย คุณสามารถปรับพฤติกรรมที่คาดหวังของนโยบายสุดท้าย กำหนดการตามลำดับของนโยบายที่นำไปใช้ โดยใช้ธงนโยบาย ธงจะกำหนดวิธีที่นโยบายจะได้รับการจัดการในการตั้งค่าแบบเฉพาะเจาะจง

สำหรับการตั้งค่าแต่ละรายการ คุณสามารถเลือกธงใดธงหนึ่งต่อไปนี้:

ไม่นำไปใช้	การตั้งค่าใดๆ ที่มีธงนี้เป็นการตั้งค่าที่ไม่ได้ตั้งค่าโดยนโยบาย เนื่องจากการตั้งค่าไม่ได้ตั้งโดยนโยบาย การตั้งค่านี้จึงสามารถถูกเปลี่ยนโดยนโยบายอื่นๆ ที่นำมาใช้ภายหลังได้
นำไปใช้	การตั้งค่าที่มีธง**นำไปใช้**จะถูกนำไปใช้ที่คอมพิวเตอร์ไคลเอ็นต์ อย่างไรก็ตามเมื่อรวมนโยบาย การตั้งค่านี้อาจถูกเขียนทับโดยนโยบายอื่นๆ ที่ปรับใช้ภายหลัง เมื่อส่งนโยบายไปยังคอมพิวเตอร์ไคลเอ็นต์ที่มีการตั้งค่าที่ถูกทำเครื่องหมายด้วยธงนี้ การตั้งค่าเหล่านั้นจะเปลี่ยนการกำหนดค่าในเครื่องของคอมพิวเตอร์ไคลเอ็นต์ เนื่องจากการตั้งค่าไม่ได้ถูกบังคับ การตั้งค่ายังสามารถถูกเปลี่ยนโดยนโยบายอื่นๆ ที่นำมาปรับใช้ภายหลังได้
บังคับ	การตั้งค่าที่มีธง**บังคับ**มีความสำคัญที่สุดและไม่สามารถเขียนทับได้โดยนโยบายอื่นๆ ที่นำมาใช้ภายหลัง (แม้จะมีธง**บังคับ** เช่นเดียวกันก็ตาม) นี่จะช่วยทำให้แน่ใจว่านโยบายอื่นๆ ที่นำมาใช้ภายหลังจะไม่ทำให้การตั้งค่านี้เปลี่ยนแปลงระหว่างการรวม เมื่อส่งนโยบายไปยังคอมพิวเตอร์ไคลเอ็นต์ที่มีการตั้งค่าที่มีธงนี้ การตั้งค่าเหล่านั้นจะเปลี่ยนการกำหนดค่าในเครื่องของคอมพิวเตอร์ไคลเอ็นต์

สถานการณ์: ผู้ดูแลระบบ ต้องการอนุญาตให้ผู้ใช้ชื่อ *John* สร้างหรือแก้ไขนโยบายในกลุ่มบ้านของเขาและดูนโยบายทั้งหมดที่สร้างโดยผู้ดูแลระบบ รวมถึงนโยบายที่มี ธงบังคับ ผู้ดูแลระบบ ต้องการให้ *John* สามารถดูนโยบายทั้งหมดได้ แต่ไม่สามารถแก้ไขนโยบายที่มีอยู่ซึ่งสร้างโดย ผู้ดูแลระบบ *John* จึงสามารถสร้างหรือแก้ไขนโยบายภายในกลุ่มบ้านของเขาที่ชื่อว่า San Diego ได้เท่านั้น
วิธีแก้ไขปัญหา:ผู้ดูแลระบบ ต้องทำตามขั้นตอนต่อไปนี้:
สร้างกลุ่มคงที่แบบกำหนดเองและชุดสิทธิ์
1. สร้าง กลุ่มคงที่ ใหม่ชื่อว่า *San Diego*
2. สร้าง ชุดสิทธิ์ ใหม่ชื่อว่า นโยบาย - *John* ทั้งหมด โดยให้มีการเข้าถึงกลุ่มคงที่ ทั้งหมด และมีสิทธิ์ **อ่าน** สำหรับ **นโยบาย**
3. สร้าง ชุดสิทธิ์ ใหม่ชื่อว่า นโยบาย *John* โดยมีการเข้าถึงกลุ่มคงที่ *San Diego* และมีการเข้าถึงฟังก์ชันสิทธิ์ **เขียน** สำหรับ **กลุ่มและคอมพิวเตอร์** และ **นโยบาย** ชุดสิทธิ์นี้อนุญาตให้ *John* สร้างหรือแก้ไขนโยบายในกลุ่มบ้านของเขาที่ชื่อว่า *San Diego*
4. สร้าง ผู้ใช้ ใหม่ชื่อ *John* และในส่วน **ชุดสิทธิ์** ให้เลือก นโยบาย - *John* ทั้งหมด และ นโยบาย *John* **สร้างนโยบาย**
5. สร้าง นโยบาย ใหม่ ไฟร์วอลล์ที่เปิดใช้งานทั้งหมด ขยายส่วน **การตั้งค่า** เลือก **ESET Endpoint สำหรับ Windows** นำทางไปที่ **ไฟร์วอลล์ส่วนบุคคล** > **พื้นฐาน** แล้วนำการตั้งค่าทั้งหมดไปใช้ด้วยธง **บังคับ** ขยายส่วน **กำหนด** และเลือกกลุ่มคงที่ ทั้งหมด
6. สร้างนโยบายใหม่ กลุ่ม *John* - เปิดใช้งานไฟร์วอลล์ ขยายส่วน **การตั้งค่า** เลือก **ESET Endpoint สำหรับ Windows** นำทางไปที่ **ไฟร์วอลล์ส่วนบุคคล** > **พื้นฐาน** และนำการตั้งค่าทั้งหมดไปใช้ด้วยธง **นำไปใช้** ขยายส่วน **กำหนด** และเลือกกลุ่มคงที่ *San Diego*
ผลลัพธ์
นโยบายที่สร้างโดยผู้ดูแลระบบจะถูกนำไปใช้ก่อนเพราะมีธง **บังคับ** ที่การตั้งค่านโยบาย การตั้งค่าที่มีธงบังคับมีความสำคัญที่สุดและไม่สามารถเขียนทับได้โดยนโยบายอื่นที่นำมาใช้ภายหลัง นโยบายที่สร้างโดยผู้ใช้ *John* จะถูกนำมาใช้หลังนโยบายที่สร้างโดยผู้ดูแลระบบ
หากต้องการดูลำดับนโยบายสุดท้าย ให้นำทางไปที่ **เพิ่มเติม** > **กลุ่ม** > **San Diego** เลือกคอมพิวเตอร์และเลือก **แสดงรายละเอียด** ในส่วน **การกำหนดค่า** ให้คลิก **นโยบายที่นำไปใช้**

การติดตั้ง

มีวิธีการติดตั้ง ESET Endpoint Security หลายวิธีบนไคลเอ็นต์เวิร์กสเตชัน ยกเว้น ปรับใช้ESET Endpoint Security ระยะไกลถึงไคลเอ็นต์เวิร์กสเตชันผ่าน ESET PROTECT หรือ ESET PROTECT Cloud

คุณสามารถดาวน์เกรดจาก ESET Endpoint Security ไปเป็น ESET Endpoint Antivirus ผ่านการเรียกใช้โปรแกรมติดตั้ง ESET Endpoint Antivirus โดยต้องติดตั้ง ESET Endpoint Security ไว้แล้ว อย่างไรก็ตามคุณต้องติดตั้งเวอร์ชันเดียวกันหรือเวอร์ชันที่ใหม่กว่า

วิธี	จุดประสงค์	ลิงค์สำหรับดาวน์โหลด
การติดตั้งด้วย ESET AV Remover	เครื่องมือ ESET AV Remover จะช่วยคุณลบซอฟต์แวร์ป้องกันไวรัสเกือบทั้งหมดที่ติดตั้งไว้บนระบบของคุณออก ก่อนที่จะดำเนินการติดตั้ง	
ฉัน การติดตั้ง (.exe)	กระบวนการการติดตั้งที่ไม่มีESET AV Remover	
การติดตั้ง (.msi)	ในสภาพแวดล้อมทางธุรกิจ โปรแกรมติดตั้ง .msi ต้องการแพ็คเกจติดตั้ง เป็นสิ่งหลักเนื่องจากการปรับใช้แบบออฟไลน์และแบบระยะไกลที่ใช้เครื่องมือที่หลากหลาย เช่น ESET PROTECT	
การติดตั้งบรรทัดคำสั่ง	ESET Endpoint Security สามารถติดตั้งภายในเครื่องได้ โดยใช้บรรทัดคำสั่งหรือแบบระยะไกลโดยใช้งานไคลเอ็นต์จากESET PROTECT	N/A

วิธี	จุดประสงค์	ลิงค์สำหรับดาวน์โหลด
การปรับใช้โดยใช้ GPO หรือ SCCM	ใช้เครื่องมือการจัดการ เช่น GPO หรือ SCCM เพื่อปรับใช้ ESET Management Agent และ ESET Endpoint Security ไปยังไคลเอ็นต์เวิร์กสเตชัน	N/A
การปรับใช้โดยใช้เครื่องมือ RMM	ปลั๊กอิน DEM ของ ESET DEM สำหรับเครื่องมือการตรวจสอบและการจัดการระยะไกล (RMM) จะช่วยคุณในการปรับใช้ ESET Endpoint Security ไปยังเวิร์กสเตชันไคลเอ็นต์	N/A

ESET Endpoint Security สามารถใช้งานได้มากกว่า 30 ภาษา

การติดตั้งด้วย ESET AV Remover

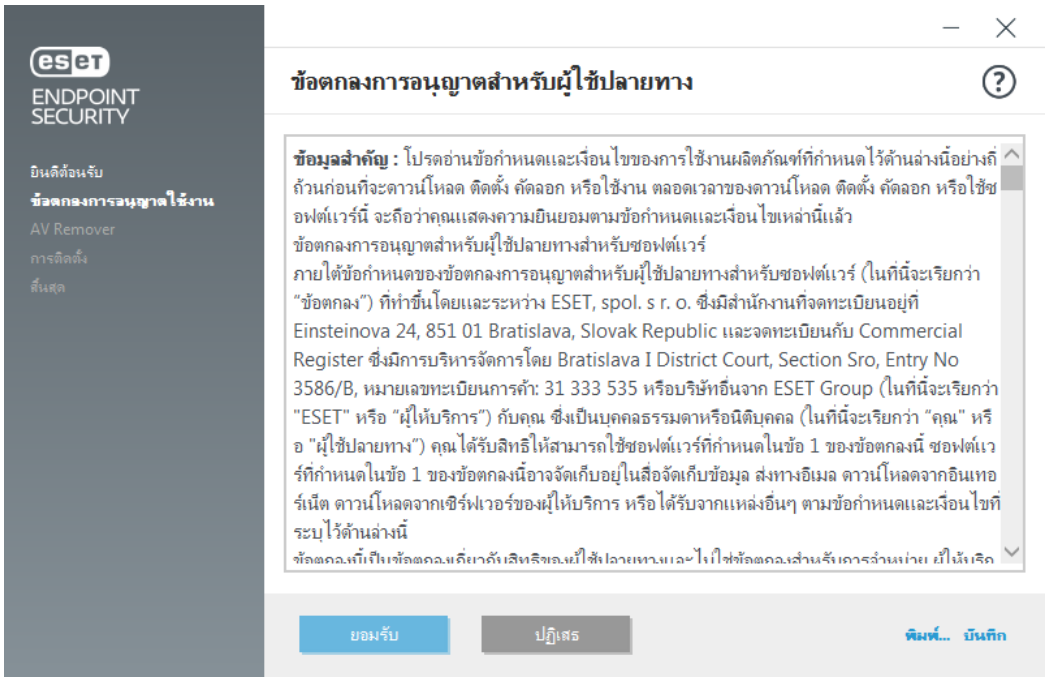
ก่อนดำเนินการติดตั้งต่อ เป็นเรื่องสำคัญที่คุณต้องลบการติดตั้งแอพพลิเคชั่นรักษาความปลอดภัยใด ๆ ที่มีอยู่ในเครื่องคอมพิวเตอร์ เลือกกล่องทำเครื่องหมายหน้า **ฉันต้องการลบแอพพลิเคชั่นป้องกันไวรัสที่ไม่ต้องการโดยใช้ ESET AV Remover** เพื่อให้ ESET AV Remover สแกนระบบของคุณและลบแอปพลิเคนป้องกันไวรัสใดใด ที่รองรับ ไม่เลือกที่กล่องทำเครื่องหมายและคลิกที่**ทำต่อ** เพื่อติดตั้งESET Endpoint Securityโดยไม่เรียกใช้งานESET AV Remover

ESET AV Remover

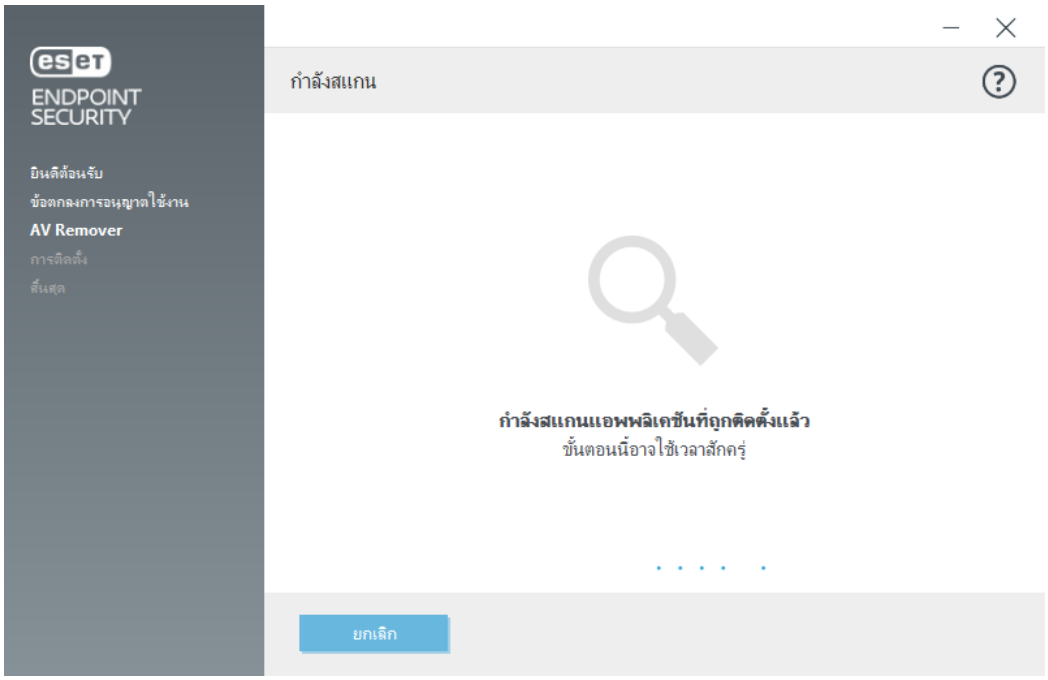
ESET AV Removerเครื่องมือนี้จะช่วยให้คุณลบซอฟต์แวร์ป้องกันไวรัสเกือบทุกตัวที่ติดตั้งไว้ก่อนหน้านี้ในระบบของคุณได้ ทำตามคำแนะนำด้านล่างเพื่อลบโปรแกรมป้องกันไวรัสที่มีอยู่โดยใช้ ESET AV Remover:

1. เพื่อดูรายการของซอฟต์แวร์ป้องกันไวรัสที่ ESET AV Remover สามารถลบได้ [โปรดไปที่บทความฐานความรู้ ESET]

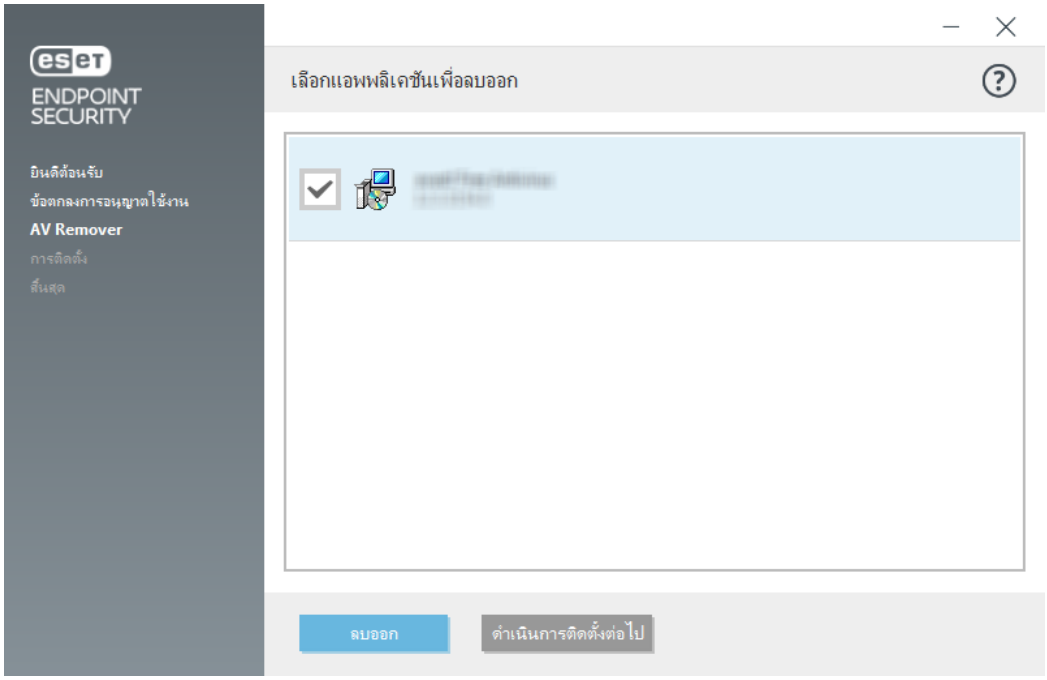
2. อ่านข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง แล้วคลิก **ยอมรับ** เพื่อรับทราบการยอมรับข้อตกลงของคุณ การคลิกที่ **ปฏิเสธ** จะทำการติดตั้ง ESET Endpoint Security โดยไม่ลบแอพพลิเคชั่นรักษาความปลอดภัยที่มีบนเครื่องคอมพิวเตอร์



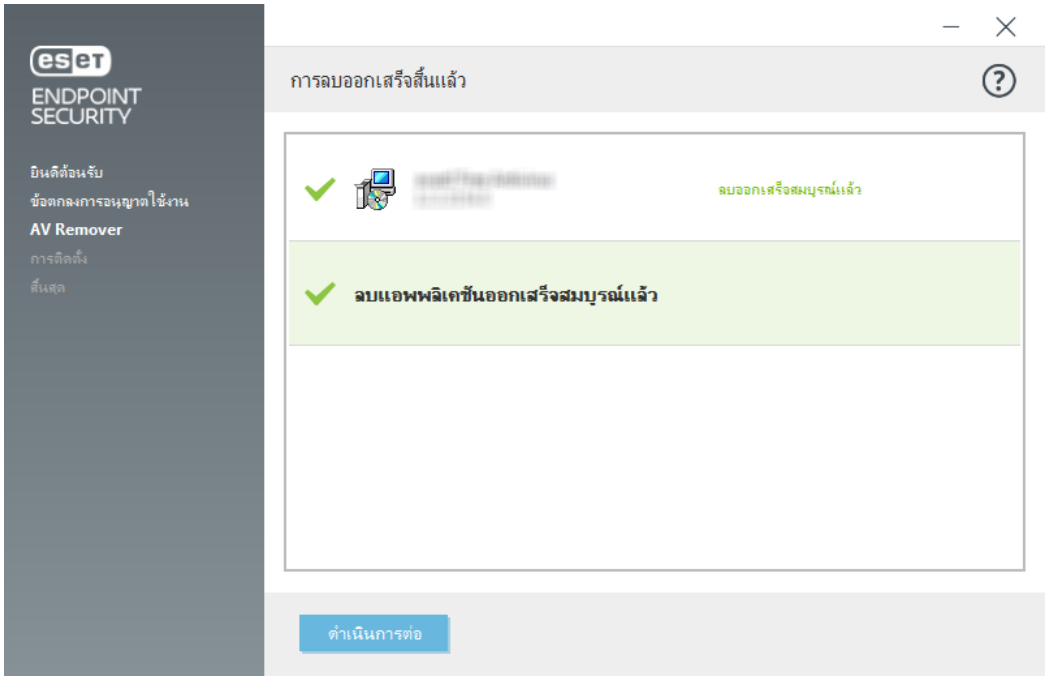
2. ESET AV Remover จะเริ่มการค้นหาซอฟท์แวร์ป้องกันไวรัสในระบบของคุณ



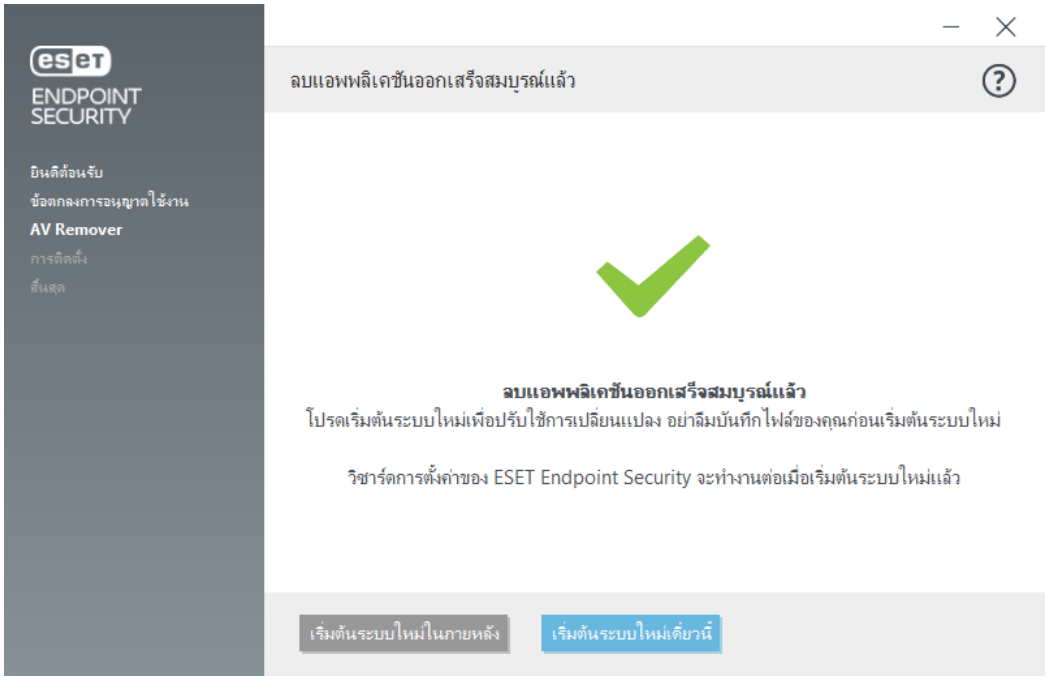
2. เลือกแอพพลิเคชั่นป้องกันไวรัสในรายการและคลิก **ลบออก** การลบอาจใช้เวลาสักครู่



2. เมื่อการลบสำเร็จ ให้คลิกที่ **ทำต่อ**



6. เริ่มต้นคอมพิวเตอร์ของคุณใหม่เพื่อใช้การเปลี่ยนแปลงและทำการติดตั้ง ESET Endpoint Security ต่อ หากการลบการติดตั้งไม่สำเร็จ ให้ดูที่ส่วนการลบการติดตั้งด้วย ESET AV Remover ที่สิ้นสุดด้วยข้อผิดพลาดของคู่มือนี้



ลบการติดตั้งโดยใช้ESET AV Remover ที่สิ้นสุดด้วยข้อผิดพลาด

หากคุณไม่สามารถลบโปรแกมป้องกันไวรัสโดยใช้ESET AV Removerคุณจะได้รับคำเตือนว่าแอพพลิเคชั่นที่คุณกำลังพยายามลบอาจไม่รองรับโดย ESET AV Remover โปรดดูที่ รายการผลิตภัณฑ์ที่รับรอง หรือ ตัวลบการติดตั้งสำหรับซอฟท์แวร์ป้องกันไวรัสวินโดวส์ทั่วไปบนฐานความรู้ของ ESET เพื่อดูว่าอาจสามารถลบโปรแกรมเฉพาะนี้ได้

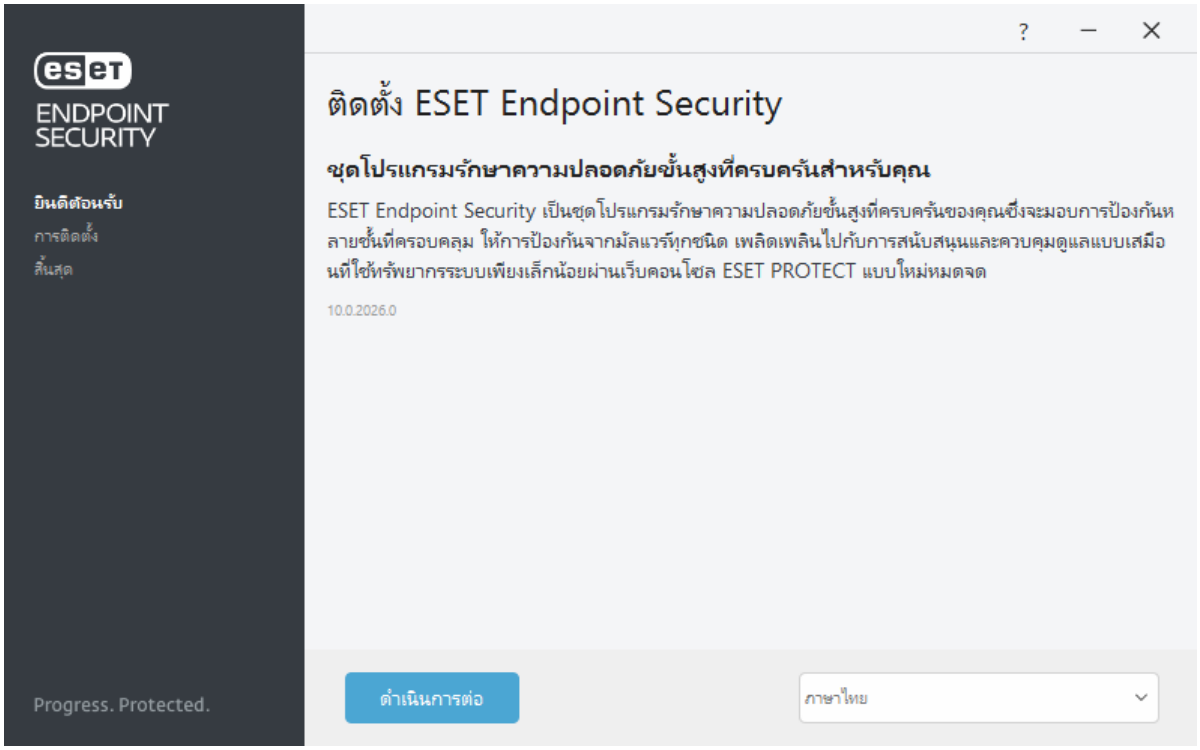
เมื่อลบการติดตั้งของผลิตภัณฑ์การรักษาความปลอดภัยไม่สำเร็จ หรือลบการติดตั้งบางส่วนของโปรแกรม คุณจะได้รับแจ้งเตือนให้ **เริ่มต้นระบบใหม่และสแกนซ้ำ** ยืนยัน UAC หลังจากเริ่มระบบและดำเนินการสแกนและลบการติดตั้งต่อ

หากจำเป็น ให้ติดต่อ ฝ่ายสนับสนุนด้านเทคนิค ESET เพื่อเปิดคำขอการสนับสนุนและมีไฟล์ **AppRemover.log** พร้อม สำหรับการช่วยเหลือช่างเทคนิค ESET ไฟล์**AppRemover.log** อยู่ในโฟลเดอร์ **eset** เรียกดูที่ *%TEMP%* ใน Windows Explorer เพื่อเข้าถึงโฟลเดอร์นี้ ฝ่ายสนับสนุนด้านเทคนิค ESET จะตอบสนองอย่างรวดเร็วทันทีที่ทำได้เพื่อแก้ปัญหาของคุณ

การติดตั้ง (.exe)

เมื่อคุณเริ่มต้นโปรแกรมติดตั้ง .exe วิซาร์ดการติดตั้งจะนำคุณเข้าสู่กระบวนการติดตั้ง

ตรวจสอบว่าไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอื่นในคอมพิวเตอร์ของคุณ ถ้ามีการติดตั้งโซลูชันการป้องกันไวรัสสองชนิดขึ้นไปบนคอมพิวเตอร์เครื่องเดียว อาจมีการทำงานที่ขัดแย้งกัน ขอแนะนำให้คุณลบการติดตั้งโปรแกรมป้องกันไวรัสอื่นในระบบของคุณ ดูบทความฐานความรู้ของคุณเพื่อดูรายการเครื่องมือถอนติดตั้งสำหรับซอฟต์แวร์ป้องกันไวรัสที่ใช้กันทั่วไป (ให้บริการเป็นภาษาอังกฤษและภาษาอื่นๆ อีกมากมาย)



1. เลือกการกำหนดลักษณะของคุณสำหรับคุณลักษณะต่อไปนี้ อ่านข้อตกลงการอนุญาตใช้งานสำหรับผู้ใช้ปลายทางและนโยบายความเป็นส่วนตัว แล้วคลิก **ดำเนินการต่อ** หรือคลิก **อนุญาตทั้งหมดและดำเนินการต่อ** เพื่อเปิดใช้งานคุณลักษณะทั้งหมด:

- ESET LiveGrid® ระบบคำติชม
- การตรวจหาแอพพลิเคชันที่อาจไม่พึงประสงค์

เมื่อคลิก **ดำเนินการต่อ** หรือ **อนุญาตทั้งหมดและดำเนินการต่อ** จะถือว่าคุณยอมรับข้อตกลงการอนุญาตใช้งานสำหรับผู้ใช้ปลายทางและรับทราบนโยบายความเป็นส่วนตัวแล้ว คุณสามารถติดตั้งESET Endpoint Security เพื่อระบุโฟลเดอร์โดยการคลิกเปลี่ยนโฟลเดอร์การติดตั้ง

2. หลังจากที่ติดตั้งเสร็จสมบูรณ์แล้ว คุณจะได้รับข้อความให้ เปิดใช้งาน ESET Endpoint Security

เปลี่ยนโฟลเดอร์การติดตั้ง (.exe)

คุณสามารถ **เปลี่ยนโฟลเดอร์การติดตั้ง** ได้ในระหว่างการติดตั้ง เลือกตำแหน่งสำหรับการติดตั้ง ESET Endpoint Security ตามค่าเริ่มต้นแล้ว โปรแกรมที่ติดตั้งไปยังไดเรกทอรีต่อไปนี้:

C:\Program Files\ESET\ESET Security

คุณสามารถระบุตำแหน่งสำหรับโมดูลและข้อมูลของโปรแกรมได้ ตามค่าเริ่มต้น โมดูลและข้อมูลเหล่านั้นจะถูกติดตั้งลงในไดเรกทอรีต่อไปนี้ตามลำดับ:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

คลิก **เรียกดู** เพื่อเปลี่ยนแปลงตำแหน่งหล่านี้ (ไม่แนะนำ)

คลิก **ย้อนกลับ** และดำเนินการติดตั้งต่อไป

การติดตั้ง (.msi)

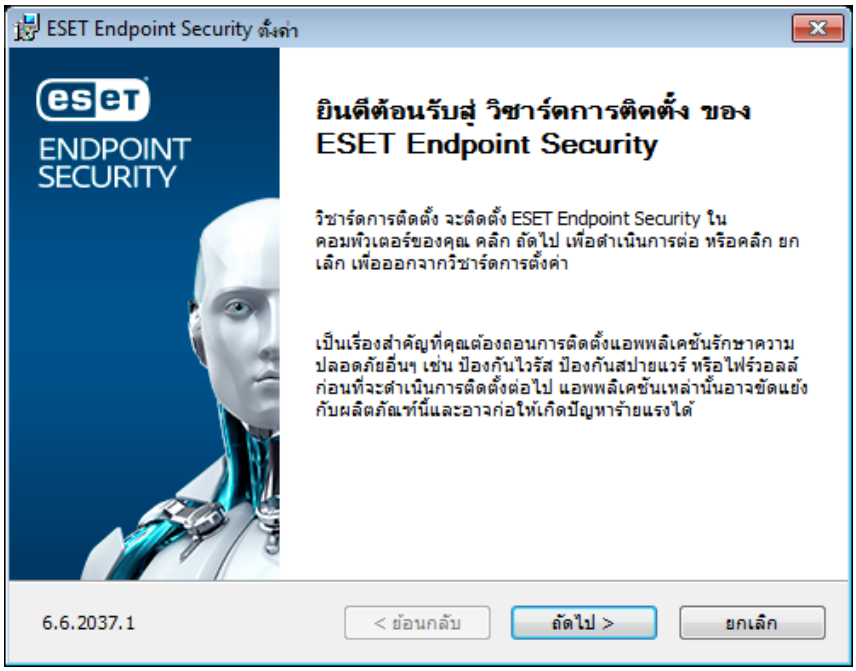
เมื่อคุณเริ่มต้นโปรแกรมติดตั้ง .msi วิซาร์ดการติดตั้งจะนำคุณเข้าสู่กระบวนการติดตั้ง

ในสภาพแวดล้อมทางธุรกิจ โปรแกรมติดตั้ง .msi ต้องการแพ็คเกจติดตั้ง เป็นสิ่งหลักเนื่องจากการปรับใช้แบบออฟไลน์และแบบระยะไกลที่ใช้เครื่องมือที่หลากหลาย เช่น ESET PROTECT

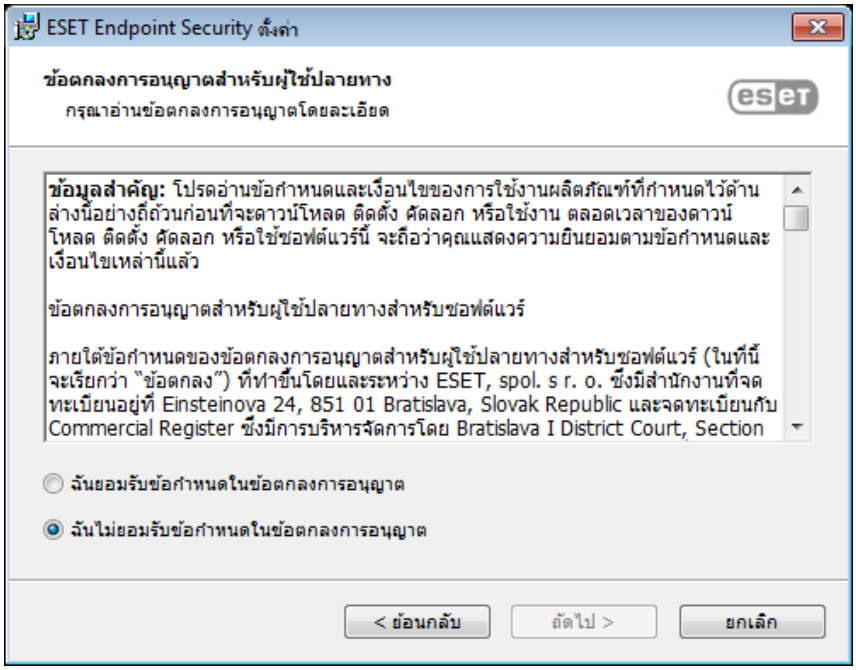
ตรวจสอบว่าไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอื่นในคอมพิวเตอร์ของคุณ ถ้ามีการติดตั้งโซลูชันการป้องกันไวรัสสองชนิดขึ้นไปบนคอมพิวเตอร์เครื่องเดียว อาจมีการทำงานที่ขัดแย้งกัน ขอแนะนำให้คุณลบการติดตั้งโปรแกรมป้องกันไวรัสอื่นในระบบของคุณ ดูบทความฐานความรู้ของคุณเพื่อดูรายการเครื่องมือถอนติดตั้งสำหรับซอฟต์แวร์ป้องกันไวรัสที่ใช้กันทั่วไป (ให้บริการเป็นภาษาอังกฤษและภาษาอื่นๆ อีกมากมาย)

ตัวติดตั้ง ESET Endpoint Security ที่สร้างขึ้นใน ESET PROTECT จะรองรับ Windows 10 Enterprise for Virtual Desktops และ Windows 10 โหมดหลายเซสชัน

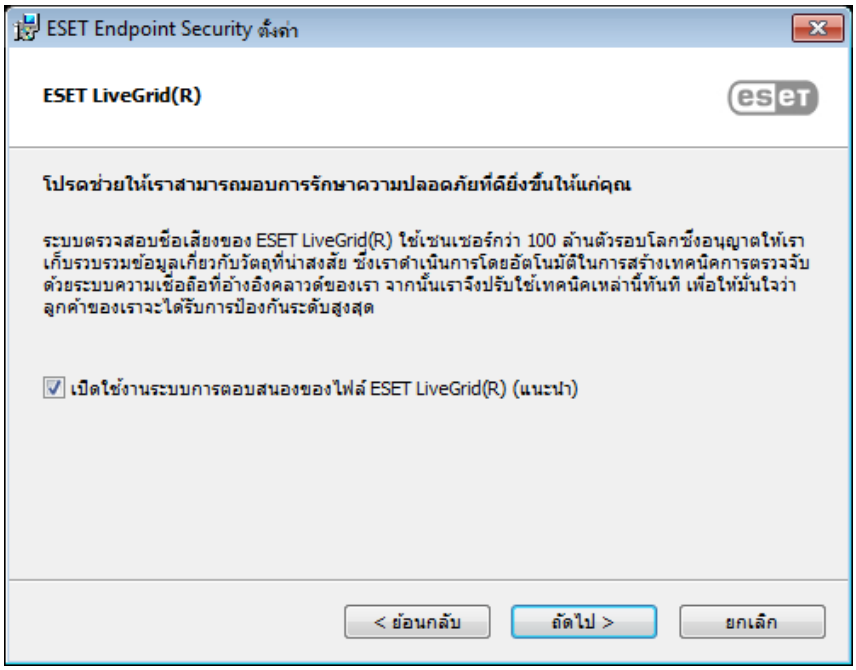
1. เลือกภาษาที่ต้องการแล้วคลิก **ถัดไป**



2. อ่านข้อตกลงใบอนุญาตผู้ใช้ปลายทาง แล้วคลิก**ฉันยอมรับเงื่อนไขในข้อตกลงใบอนุญาต** เพื่อยอมรับข้อตกลงของข้อตกลงใบอนุญาตผู้ใช้ปลายทาง คลิก**ถัดไป** หลังจากคุณยอมรับข้อกำหนดเพื่อดำเนินการติดตั้งต่อ



3. เลือกการตั้งค่าสำหรับ ระบบคำติชมสำหรับ ESET LiveGrid® โดย ESET LiveGrid® จะช่วยให้แน่ใจได้ว่า ESET จะได้รับรายงานเกี่ยวกับการแฝงตัวใหม่โดยทันทีอย่างต่อเนื่อง ซึ่งจะทำให้เราสามารถปกป้องลูกค้าของเราได้ดียิ่งขึ้น และระบบนี้ยังช่วยให้คุณสามารถส่งภัยคุกคามใหม่ไปยังห้องปฏิบัติการไวรัสของ ESET ซึ่งเราจะวิเคราะห์ ดำเนินการ และเพิ่มรายการภัยคุกคามดังกล่าวไปยังกลไกการตรวจจับ คลิก **การตั้งค่าขั้นสูง** เพื่อ กำหนดค่าพารามิเตอร์การติดตั้งเพิ่มเติม



4. ขั้นตอนสุดท้ายคือการยืนยันการติดตั้งโดยการคลิก **ติดตั้ง** หลังจากที่ติดตั้งเสร็จสมบูรณ์แล้ว คุณจะได้รับข้อความให้ เปิดใช้งาน ESET Endpoint Security

การติดตั้งขั้นสูง (.msi)

การติดตั้งขั้นสูงช่วยให้คุณสามารถปรับแต่งพารามิเตอร์การติดตั้งที่ไม่มีให้ใช้ได้ด้วยตัวเองเมื่อดำเนินการติดตั้งแบบปกติ

1. คุณสามารถ **เปลี่ยนโฟลเดอร์การติดตั้ง** ได้ในระหว่างการติดตั้ง เลือกตำแหน่งสำหรับการติดตั้ง ESET Endpoint Security ตามค่าเริ่มต้นแล้ว โปรแกรมที่ติดตั้งไปยังไดเรกทอรีต่อไปนี้:

C:\Program Files\ESET\ESET Security

คุณสามารถระบุตำแหน่งสำหรับโมดูลและข้อมูลของโปรแกรมได้ ตามค่าเริ่มต้น โมดูลและข้อมูลเหล่านั้นจะถูกติดตั้งลงในไดเรกทอรีต่อไปนี้ตามลำดับ:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

คลิก **เรียกดู** เพื่อเปลี่ยนแปลงตำแหน่งหล่านี้ (ไม่แนะนำ)

2. เลือกองค์ประกอบผลิตภัณฑ์ที่ติดตั้งได้ คุณสามารถเลือกการตั้งค่าสำหรับ การสแกนคอมพิวเตอร์ และ การป้องกัน ทั้งหมดที่มีอยู่ องค์ประกอบ มิเรอร์การอัพเดท สามารถใช้เพื่ออัพเดทคอมพิวเตอร์เครื่องอื่นบนเครือข่ายของคุณได้ การตรวจสอบและการจัดการระยะไกล (RMM) เป็นกระบวนการตรวจสอบและควบคุมระบบซอฟต์แวร์ที่ใช้เอเจนต์ที่ติดตั้งในเครื่อง ที่สามารถเข้าถึงได้โดยการจัดการของผู้ให้บริการ
3. คลิก **ติดตั้ง** เพื่อเริ่มขั้นตอนการติดตั้ง

การติดตั้งโมดูลขั้นต่ำ

เพื่อเป็นการลดปริมาณรับส่งข้อมูลบนเครือข่ายจากการมีตัวติดตั้งขนาดใหญ่ และช่วยคุณประหยัดทรัพยากรของระบบ ESET จึงมาพร้อมกับตัวติดตั้งโมดูลขั้นต่ำ ซึ่งจะมีเพียงโมดูลพื้นฐานที่จำเป็นเท่านั้น และจะดาวน์โหลดโมดูลที่เหลือในระหว่างการอัพเดทโมดูลขั้นต้นหลังจากเปิดใช้งานผลิตภัณฑ์แล้ว จุดแข็งหลักของแนวทางนี้ก็คือการทำให้ตัวติดตั้งมีขนาดเล็กลง และทำให้ ESET Endpoint Security ดาวน์โหลดเฉพาะโมดูลแอพพลิเคชันล่าสุดเท่านั้นเมื่อคุณเปิดใช้งานผลิตภัณฑ์

ตัวติดตั้งโมดูลขั้นต่ำจะยังคงมีโมดูลต่อไปนี้อยู่

- ตัวโหลด

- การสื่อสาร Direct Cloud
- การรองรับการแปล
- การกำหนดค่า
- SSL

เมื่อเปิดใช้งานผลิตภัณฑ์แล้ว คุณจะเห็นสถานะ **กำลังเริ่มต้นการป้องกัน** ซึ่งจะแจ้งข้อมูลเกี่ยวกับการเริ่มต้นคุณลักษณะให้คุณทราบ

หากพบปัญหาเกี่ยวกับการดาวน์โหลดโมดูล (เช่น การตั้งค่าพร็อกซี่ ไม่มีเครือข่าย และอื่นๆ) ระบบจะแสดงสถานะการแจ้งเตือนแอพพลิเคชัน **ต้องการการตรวจสอบจากคุณ** ให้คลิก **อัพเดท** > **ตรวจหาการอัพเดท** ในหน้าต่างโปรแกรมหลักเพื่อเริ่มกระบวนการอัพเดทอีกครั้ง

เมื่อพยายามไม่สำเร็จหลายครั้ง ระบบจะแสดงสถานะแอพพลิเคชัน **การตั้งค่าการป้องกันล้มเหลว** สีแดงขึ้น คลิก ลองอีกครั้ง เพื่อเริ่มการตั้งค่าการป้องกันอีกครั้ง หากกระบวนการเริ่มต้นล้มเหลวและคุณยังไม่สามารถดาวน์โหลดโมดูลได้ โปรด ดาวน์โหลดตัวติดตั้ง MSI

หากคอมพิวเตอร์ไคลเอ็นต์ไม่มีการเชื่อมต่ออินเทอร์เน็ตหรือทำงานแบบออฟไลน์อยู่ คุณสามารถใช้วิธีการต่อไปนี้ดาวน์โหลดไฟล์อัพเดทจากเซิร์ฟเวอร์การอัพเดทของ ESET ได้
- การอัพเดทจากมิเรอร์
- การใช้เครื่องมือมิเรอร์

การติดตั้งบรรทัดคำสั่ง

คุณสามารถติดตั้ง ESET Endpoint Security ในระบบโดยใช้บรรทัดคำสั่งหรือคุณสามารถติดตั้งจากระยะไกลโดยใช้งานไคลเอ็นต์จาก ESET PROTECT

พารามิเตอร์ที่รองรับ

APPDIR=<path>

- พาธ - พาธไดเรกทอรีที่ถูกต้อง
- ไดเรกทอรีการติดตั้งแอพพลิเคชัน

APPDATADIR=<path>

- พาธ - พาธไดเรกทอรีที่ถูกต้อง
- ไดเรกทอรีการติดตั้งข้อมูลแอพพลิเคชัน

MODULEDIR=<path>

- พาธ - พาธไดเรกทอรีที่ถูกต้อง

- โมดูลการติดตั้งแอพพลิเคชัน

ADDLOCAL=<list>

- การติดตั้งองค์ประกอบ - รายการของคุณลักษณะแบบไม่ใช่คำสั่งเพื่อติดตั้งภายใน
- การใช้งานกับแพ็คเกจ .msi ของ ESET: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- สำหรับข้อมูลเกี่ยวกับคุณสมบัติ **ADDLOCAL** โปรดดูที่ http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

ADDEXCLUDE=<list>

- รายการ ADDEXCLUDE คือรายการที่คั่นด้วยเครื่องหมายจุลภาคของชื่อคุณลักษณะทั้งหมดที่ไม่ได้ติดตั้ง โดยเป็นการแทนที่สำหรับ REMOVEที่เลิกใช้แล้ว
- เมื่อมีการเลือกคุณลักษณะที่จะไม่ติดตั้ง เช่นนั้นพาธทั้งหมด (เช่น คุณลักษณะย่อยทั้งหมด) และคุณลักษณะแบบมองไม่เห็นที่เกี่ยวข้องจะต้องอยู่ในรายการอย่างชัดเจน
- การใช้งานกับแพ็คเกจ .msi ของ ESET: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

ADDEXCLUDE ไม่สามารถใช้ร่วมกับ **ADDLOCAL**

ดูเอกสารประกอบสำหรับเวอร์ชัน **msiexec** ที่ใช้สำหรับเปลี่ยนบรรทัดคำสั่งอย่างเหมาะสม

กฎ

- รายการ **ADDLOCAL** เป็นรายการของชื่อคุณลักษณะทั้งหมดที่คั่นออกจากกันด้วยเครื่องหมายจุลภาคที่จะติดตั้ง
- เมื่อเลือกคุณลักษณะที่คุณจะติดตั้ง พาธทั้งหมด (คุณลักษณะหลักทั้งหมด) ต้องรวมอยู่ในรายการอย่างชัดเจน
- ดูกฎเพิ่มเติมเพื่อให้ใช้งานได้อย่างถูกต้อง

องค์ประกอบและคุณลักษณะ

การติดตั้งองค์ประกอบโดยใช้พารามิเตอร์ ADDLOCAL/ADDEXCLUDE จะไม่สามารถทำงานร่วมกับ ESET Endpoint Antivirus ได้

คุณลักษณะจะถูกแบ่งออกเป็น 4 ประเภท:

- **จำเป็น** – คุณลักษณะจะถูกติดตั้งอยู่เสมอ
- **ไม่บังคับ** – สามารถยกเลิกการเลือกคุณลักษณะเพื่อไม่ต้องติดตั้งคุณลักษณะได้

- **แบบที่มองไม่เห็น** - คุณลักษณะที่จำเป็นต้องใช้เพื่อทำให้คุณลักษณะอื่นทำงานได้อย่างถูกต้อง
- **ตัวยึด** - คุณลักษณะที่ไม่มีผลกระทบกับผลิตภัณฑ์ แต่จะต้องอยู่ในรายการกับคุณลักษณะย่อย

ชุดคุณลักษณะของ ESET Endpoint Security มีดังต่อไปนี้:

คำอธิบาย	ชื่อคุณสมบัติ	คุณลักษณะผู้ปกครอง	การแสดงผล
องค์ประกอบของโปรแกรมพื้นฐาน	Computer		ตัวยึด
กลไกการตรวจจับ	Antivirus	Computer	จำเป็น
กลไกการตรวจจับ / การสแกนมัลแวร์	Scan	Computer	จำเป็น
กลไกการตรวจจับ / การป้องกันระบบไฟล์แบบเรียลไทม์	RealtimeProtection	Computer	จำเป็น
กลไกการตรวจจับ / มัลแวร์สแกน / การป้องกันไฟล์เอกสาร	DocumentProtection	Antivirus	ไม่บังคับ
การควบคุมอุปกรณ์	DeviceControl	Computer	ไม่บังคับ
การป้องกันเครือข่าย	Network		ตัวยึด
การป้องกันเครือข่าย / ไฟร์วอลล์	Firewall	Network	ไม่บังคับ
การป้องกันเครือข่าย / การป้องกันการโจมตีเครือข่าย / ...	IdsAndBotnetProtection	Network	ไม่บังคับ
เบราว์เซอร์ที่ปลอดภัย	OnlinePaymentProtection	WebAndEmail	ไม่บังคับ
เว็บและอีเมล	WebAndEmail		ตัวยึด
เว็บและอีเมล์/การกรองโปรโตคอล	ProtocolFiltering	WebAndEmail	แบบมองไม่เห็น
เว็บและอีเมล / การป้องกันการเข้าถึงเว็บไซต์	WebAccessProtection	WebAndEmail	ไม่บังคับ
เว็บและอีเมล / การป้องกันอีเมลไคลเอ็นต์	EmailClientProtection	WebAndEmail	ไม่บังคับ
เว็บและอีเมล / การป้องกันอีเมลไคลเอ็นต์ / อีเมลไคลเอ็นต์	MailPlugins	EmailClientProtection	แบบมองไม่เห็น
เว็บและอีเมล / การป้องกันอีเมลไคลเอ็นต์ / การป้องกันสแปมอีเมลไคลเอ็นต์	Antispam	EmailClientProtection	ไม่บังคับ
เว็บและอีเมล / การควบคุมการเข้าถึงเว็บไซต์	WebControl	WebAndEmail	ไม่บังคับ
เครื่องมือ / ESET RMM	Rmm		ไม่บังคับ
อัพเดท / โปรไฟล์ / มิเรอร์การอัพเดท	UpdateMirror		ไม่บังคับ
ปลั๊กอิน ESET Inspect	EnterpriseInspector		แบบมองไม่เห็น

ชุดคุณลักษณะแบบกลุ่ม:

คำอธิบาย	ชื่อคุณสมบัติ	คุณลักษณะ
คุณลักษณะที่จำเป็นทั้งหมด	_Base	แบบมองไม่เห็น
คุณลักษณะที่สามารถใช้งานได้ทั้งหมด	ALL	แบบมองไม่เห็น

กฎเพิ่มเติม

- หากคุณลักษณะ **WebAndEmail** ใดๆ ก็ตามถูกเลือกเพื่อติดตั้ง คุณลักษณะ **ProtocolFiltering** แบบมองไม่เห็นจะต้องรวมอยู่ในรายการด้วย
- ชื่อของคุณลักษณะทั้งหมดนั้นตรงตามตัวพิมพ์ ตัวอย่างเช่นUpdateMirror ไม่เท่ากับ UPDATEMIRROR

รายการคุณสมบัติของการกำหนดค่า

คุณสมบัติ	ค่า	คุณลักษณะ
CFG_POTENTIALLYUNWANTED_ENABLED=	0 - ปิดใช้งานแล้ว 1 - เปิดใช้งานแล้ว	การตรวจหา PUA
CFG_LIVEGRID_ENABLED=	ดูด้านล่าง	ดูคุณสมบัติของ LiveGrid ด้านล่าง
FIRSTSCAN_ENABLE=	0 - ปิดใช้งานแล้ว 1 - เปิดใช้งานแล้ว	วางกำหนดการและเรียกใช้การสแกนคอมพิวเตอร์หลังการติดตั้ง
CFG_PROXY_ENABLED=	0 - ปิดใช้งานแล้ว 1 - เปิดใช้งานแล้ว	การตั้งค่าพร็อกซีเซิร์ฟเวอร์
CFG_PROXY_ADDRESS=	<ip>	ที่อยู่ IP พร็อกซีเซิร์ฟเวอร์
CFG_PROXY_PORT=	<port>	หมายเลขพอร์ตพร็อกซีเซิร์ฟเวอร์
CFG_PROXY_USERNAME=	<username>	ชื่อผู้ใช้สำหรับการตรวจสอบสิทธิ์
CFG_PROXY_PASSWORD=	<password>	รหัสผ่านสำหรับการตรวจสอบสิทธิ์
ACTIVATION_DATA=	ดูด้านล่าง	การเปิดใช้งานผลิตภัณฑ์, รหัสใบอนุญาตหรือไฟล์ใบอนุญาตแบบออฟไลน์
ACTIVATION_DLG_SUPPRESS=	0 - ปิดใช้งานแล้ว 1 - เปิดใช้งานแล้ว	เมื่อตั้งให้เป็น "1" โปรดอย่าแสดงหน้าต่างโต้ตอบการเปิดใช้งานผลิตภัณฑ์หลังการเริ่มใช้งานครั้งแรก
ADMINCFG=	<path>	พาธสู่การกำหนดค่า XML แบบส่งออก (ค่าเริ่มต้น *cfg.xml*)

คุณสมบัติการกำหนดค่าเฉพาะใน ESET Endpoint Security

CFG_EPFW_MODE=	0 - อัตโนมัติ (ค่าเริ่มต้น) 1 - แบบมีการโต้ตอบ 2 - ตามนโยบาย 3 - การเรียนรู้	โหมดการกรองไฟร์วอลล์
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	วันสิ้นสุดของโหมดการเรียนรู้เป็นบันทึกการลงเวลา Unix

คุณสมบัติของ LiveGrid®

เมื่อทำการติดตั้ง ESET Endpoint Security ด้วย `CFG_LIVEGRID_ENABLED` แล้ว พฤติกรรมของผลิตภัณฑ์หลังการติดตั้งจะเป็น:

คุณลักษณะ	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
ระบบความเชื่อถือ ESET LiveGrid®	เปิด	เปิด
ระบบตรวจสอบความน่าเชื่อถือไฟล์ ESET LiveGrid®	ปิด	เปิด
ส่งสถิติที่ไม่ระบุชื่อ	ปิด	เปิด

คุณสมบัติ ACTIVATION_DATA

รูปแบบ	วิธี
`ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE`	การเปิดใช้งานโดยใช้รหัสใบอนุญาตของ ESET (ต้องเปิดใช้การเชื่อมต่ออินเทอร์เน็ต)
`ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf`	การเปิดใช้งานโดยใช้ไฟล์ใบอนุญาตแบบออฟไลน์

คุณสมบัติทางภาษา

ภาษาของ ESET Endpoint Security (คุณต้องระบุทั้งสองคุณสมบัติ)

คุณสมบัติ	ค่า
`PRODUCT_LANG=`	ทศนิยม LCID (ID ตำแหน่งที่ตั้ง) ตัวอย่างเช่น 1033 สำหรับภาษาอังกฤษ (สหรัฐอเมริกา) โปรดดู รายการรหัสภาษา
`PRODUCT_LANG_CODE=`	สตริง LCID (ชื่อทางวัฒนธรรมของภาษา) ในแบบตัวพิมพ์เล็ก ตัวอย่างเช่น en-us สำหรับภาษาอังกฤษ (สหรัฐอเมริกา) โปรดดู รายการรหัสภาษา

เริ่มต้นคุณสมบัติใหม่

ระบุพารามิเตอร์ต่อไปนี้เพื่อรีสตาร์ทคอมพิวเตอร์หลังจากการติดตั้ง:

คุณสมบัติ	ค่า	คุณลักษณะ
`REBOOT_WHEN_NEEDED=`	0 - ปิดใช้งานแล้ว 1 - เปิดใช้งานแล้ว	หากเปิดใช้งาน คอมพิวเตอร์จะรีสตาร์ทหลังจากติดตั้ง
`REBOOT_CANCELABLE=`	0 - ปิดใช้งานแล้ว 1 - เปิดใช้งานแล้ว	หากเปิดใช้งาน ผู้ใช้จะยกเลิกการรีสตาร์ทคอมพิวเตอร์ได้
`REBOOT_POSTPONE=`	ค่าเป็นวินาที	จำนวนสูงสุดของเวลาเป็นวินาทีที่ผู้ใช้สามารถเลื่อนการรีสตาร์ทของคอมพิวเตอร์

i REBOOT_CANCELABLE และ REBOOT_POSTPONE จะพร้อมใช้งานเฉพาะเมื่อ REBOOT_WHEN_NEEDED เปิดใช้งาน

ตัวอย่างบรรทัดคำสั่งการติดตั้ง

ตรวจสอบให้แน่ใจว่าได้อ่าน ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง และมีสิทธิ์ของผู้ดูแลระบบก่อนเรียกใช้การติดตั้ง

ยกเว้นส่วน **NetworkProtection** จากการติดตั้ง (คุณต้องระบุคุณลักษณะลูกทั้งหมดอีกด้วย):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

หากคุณต้องการให้ ESET Endpoint Security ของคุณกำหนดค่าหลังการติดตั้งโดยอัตโนมัติ คุณสามารถระบุพารามิเตอร์การกำหนดค่าพื้นฐานภายในคำสั่งการติดตั้งได้
เปิดใช้งานการติดตั้ง ESET Endpoint Security ด้วย ESET LiveGrid®:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

ติดตั้งไปยังไดเรกทอรีการติดตั้งแอพพลิเคชันอื่นนอกเหนือจากค่าเริ่มต้น
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

ติดตั้งและเปิดใช้งาน ESET Endpoint Security โดยใช้รหัสใบอนุญาตของ ESET ของคุณ
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

การติดตั้งแบบเงียบพร้อมด้วยการบันทึกอย่างละเอียด (มีประโยชน์สำหรับการแก้ไขปัญหา) และ RMM เฉพาะกับองค์ประกอบที่จำเป็น:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

การบังคับการติดตั้งแบบเงียบเต็มรูปแบบด้วยภาษาที่ระบุ
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

ตัวเลือกบรรทัดคำสั่งหลังการติดตั้ง

- ESET CMD –นำเข้าไฟล์การกำหนดค่าของ .xml หรือเปิด/ปิดคุณลักษณะด้านความปลอดภัย
- เครื่องมือสแกนของบรรทัดคำสั่ง – เรียกใช้การสแกนคอมพิวเตอร์จากบรรทัดคำสั่ง

การปรับใช้โดยใช้ GPO หรือ SCCM

นอกจากการติดตั้ง ESET Endpoint Security โดยตรงในเวิร์กสเตชันไคลเอนต์แล้ว คุณยังสามารถติดตั้งโดยใช้เครื่องมือการจัดการ เช่น Group Policy Object (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris หรือ Puppet ได้ด้วยเช่นกัน

ได้รับการจัดการ (แนะนำ)

สำหรับคอมพิวเตอร์ที่ได้รับการจัดการ เราจะติดตั้งเอเจนท์ ESET Management เป็นอย่างแรก จากนั้นจึงปรับใช้ ESET Endpoint Security ผ่าน ESET PROTECT จำเป็นต้องติดตั้ง ESET PROTECT ในเครือข่ายของคุณ

1. ดาวน์โหลดตัวติดตั้งแบบแสตนด์อโลนสำหรับเอเจนท์ ESET Management
2. จัดเตรียมสคริปต์การปรับใช้ GPO/SCCM ระยะไกล
3. ปรับใช้เอเจนท์ ESET Management โดยใช้ GPO หรือ SCCM
4. ตรวจสอบให้แน่ใจว่าได้เพิ่มคอมพิวเตอร์ไคลเอ็นต์ไปยัง ESET PROTECT แล้ว
5. ปรับใช้และเปิดใช้งาน ESET Endpoint Security ไปยังคอมพิวเตอร์ไคลเอ็นต์ของคุณ

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
- ปรับใช้ ESET Management Agent ผ่าน SCCM หรือ GPO
- ปรับใช้ ESET Management Agent ด้วย Group Policy Object (GPO)

ไม่ได้รับการจัดการ

สำหรับคอมพิวเตอร์ที่ไม่ได้รับการจัดการ คุณสามารถปรับใช้ ESET Endpoint Security ไปยังเวิร์กสเตชันไคลเอ็นต์ ซึ่งวิธีนี้เป็นวิธีที่ไม่แนะนำเนื่องจากคุณไม่สามารถตรวจสอบและบังคับใช้นโยบายสำหรับผลิตภัณฑ์ ESET endpoint ทุกอุปกรณ์ของคุณบนเวิร์กสเตชันได้

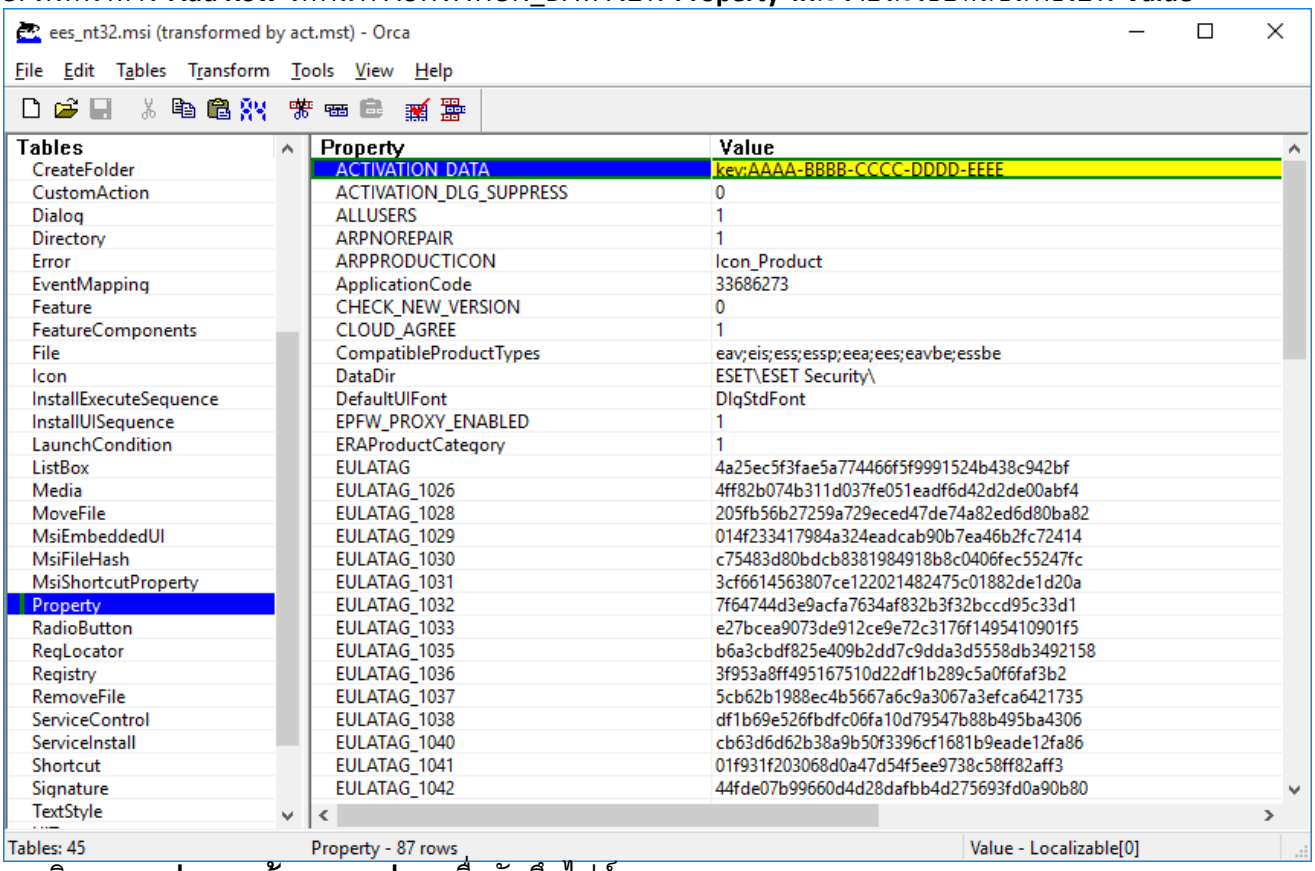
ตามค่าเริ่มต้น ESET Endpoint Security จะไม่เปิดใช้งานหลังการติดตั้ง ดังนั้นจึงไม่สามารถทำงานได้

ตัวเลือกที่ 1 (การติดตั้งซอฟต์แวร์)

1. ดาวน์โหลดโปรแกรมติดตั้ง .msi สำหรับ ESET Endpoint Security
2. สร้างแพ็คเกจการแปลง.mst จากไฟล์ .msi (ตัวอย่างเช่น การใช้ตัวแก้ไข Orca .msi) เพื่อรวมคุณสมบัติการเปิดใช้งานผลิตภัณฑ์ (ดูที่ `ACTIVATION_DATA` ใน การติดตั้งบรรทัดคำสั่ง)

   แสดงขั้นตอนสำหรับการสร้าง .mst ใน Orca

1. เปิด Orca
2. โหลดโปรแกรมติดตั้ง .msi โดยคลิก **File** > **Open**
3. คลิก **Transform** > **New Transform**
4. คลิก **Property** ในส่วน **Tables** จากนั้นในเมนู **Tables** > **Add row**
5. ในหน้าต่าง **Add Row** ให้พิมพ์ ACTIVATION_DATA เป็น **Property** และรายละเอียดลิขสิทธิ์เป็น **Value**



6. คลิก **การแปลง** > **สร้างการแปลง** เพื่อบันทึกไฟล์.mst

1. ไม่บังคับ: หากต้องการนำเข้าไฟล์การกำหนดค่า ESET Endpoint Security .xml ที่ปรับแต่งเองของคุณ (ตัวอย่าง เช่น เพื่อเปิดใช้ RMM หรือกำหนดค่าการตั้งค่าพร็อกซีเซิร์ฟเวอร์) ให้วางไฟล์ cfg.xml ในตำแหน่งเดียวกับโปรแกรมติดตั้ง .msi
2. ปรับใช้โปรแกรมติดตั้ง .msi กับไฟล์ .mst จากระยะไกลโดยใช้ GPO (ผ่านการติดตั้งซอฟต์แวร์) หรือ SCCM

ตัวเลือกที่ 2 (การใช้งานตามกำหนดการ)

1. ดาวน์โหลดโปรแกรมติดตั้ง .msi สำหรับ ESET Endpoint Security
2. จัดเตรียมสคริปต์การติดตั้งบรรทัดคำสั่งเพื่อรวมคุณสมบัติการเปิดใช้งานผลิตภัณฑ์ (ดูที่ `ACTIVATION_DATA`)
3. กำหนดให้โปรแกรมติดตั้ง .msi และสคริปต์ .cmd สามารถเข้าถึงในเครือข่ายสำหรับเวิร์กสเตชันทั้งหมด
4. ไม่บังคับ: หากต้องการนำเข้าไฟล์การกำหนดค่า ESET Endpoint Security .xml ที่ปรับแต่งเองของคุณ (ตัวอย่าง เช่น เพื่อเปิดใช้ RMM หรือกำหนดค่าการตั้งค่าพร็อกซีเซิร์ฟเวอร์) ให้วางไฟล์ cfg.xml ในตำแหน่งเดียวกับโปรแกรมติดตั้ง .msi
5. ใช้การติดตั้งบรรทัดคำสั่งที่จัดเตรียมไว้โดยใช้ GPO หรือ SCCM

- สำหรับ GPO ให้ใช้ การตั้งค่านโยบายกลุ่ม > งานตามกำหนดการของนโยบายแบบกลุ่ม > งานที่ดำเนินการทันที

> หากคุณไม่ต้องการใช้ ESET PROTECT เพื่อจัดการผลิตภัณฑ์ ESET Endpoint จากระยะไกล ESET Endpoint Security จะประกอบด้วยปลั๊กอิน ESET สำหรับ RMM ซึ่งจะช่วยคุณดูแลและควบคุมระบบซอฟต์แวร์โดยใช้เอเจนท์ที่ติดตั้งภายในระบบซึ่งสามารถเข้าถึงได้โดยการจัดการผู้ให้บริการ ค้นหาข้อมูลเพิ่มเติม

การอัพเกรดเป็นเวอร์ชันล่าสุด

ESET Endpoint Security เวอร์ชันใหม่ได้ออกมาเพื่อปรับปรุงประสิทธิภาพหรือแก้ไขปัญหาที่ไม่สามารถแก้ไขได้โดยการอัพเดทอัตโนมัติของโมดูลโปรแกรม

การอัพเกรดเป็นเวอร์ชันใหม่กว่าสามารถทำได้หลายวิธี:

1. ใช้ ESET PROTECT, หรือ ESET PROTECT Cloud โดยอัตโนมัติ
2. ใช้ GPO หรือ SCCM โดยอัตโนมัติ
3. ใช้การอัพเดทโปรแกรม โดยอัตโนมัติ
   เนื่องจากมีการแจกจ่ายการอัพเกรดโปรแกรมให้แก่ผู้ใช้ทั้งหมดและอาจส่งผลกระทบต่อการกำหนดค่าบางอย่างในระบบ การอัพเกรดนี้จึงออกมาหลังจากผ่านการทดสอบมาเป็นระยะเวลานาน เพื่อให้มั่นใจว่าทำงานกับการกำหนดค่าในระบบทั้งหมดได้ หากคุณต้องการอัพเกรดเป็นเวอร์ชันใหม่ทันทีเมื่อมีการออก ให้ใช้วิธีหนึ่งจากด้านล่างนี้
   ตรวจสอบให้แน่ใจว่าคุณได้เปิดใช้งาน **โหมดอัพเดท** ใน การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์** > **การอัพเดทผลิตภัณฑ์**
4. ด้วยตนเอง โดยการดาวน์โหลดและ เวอร์ชันใหม่กว่าทับเวอร์ชันที่มีอยู่ก่อนหน้า

คำแนะนำสถานการณ์การอัพเดท

ฉันจะจัดการหรือต้องการจัดการผลิตภัณฑ์ ESET ของฉันจากระยะไกล

หากคุณจัดการผลิตภัณฑ์ ESET Endpoint มากกว่า 10 ผลิตภัณฑ์ ให้พิจารณาจัดการการอัพเกรดโดยใช้ ESET PROTECT หรือ ESET PROTECT Cloud โปรดดูเอกสารต่อไปนี้:

- ESET PROTECT | อัพเกรดซอฟต์แวร์ ESETผ่านงานไคลเอ็นต์
- ESET PROTECT | คำแนะนำสำหรับธุรกิจขนาดเล็กถึงขนาดกลางที่จัดการผลิตภัณฑ์ ESET Endpoint สำหรับ Windows ไม่เกิน 250 รายการ

- บทแนะนำเกี่ยวกับ ESET PROTECT Cloud

การอัพเกรดบนไคลเอ็นต์เวิร์กสเตชันด้วยตนเอง

หากต้องการอัพเกรด ESET Endpoint Security บนเวิร์กสเตชันของไคลเอ็นต์แต่ละเครื่องด้วยตนเอง:

1. ให้ตรวจสอบว่าเวอร์ชันที่คุณติดตั้งอยู่ในปัจจุบันได้รับการรองรับ
2. ยืนยันว่าระบบปฏิบัติการของคุณนั้นรองรับ
2. ดาวน์โหลดและ ติดตั้งเวอร์ชันล่าสุด ทับเวอร์ชันที่มีอยู่ก่อนหน้านี้

> ไม่มีการรับประกันว่าการติดตั้งเวอร์ชันล่าสุดแทนที่เวอร์ชันก่อนหน้าจะประสบความสำเร็จสำหรับเวอร์ชันที่มีการรองรับอยู่ในระดับ “สิ้นสุดอายุการใช้งาน” ดูนโยบายการสิ้นสุดอายุการใช้งานเพื่อตรวจสอบระดับการรองรับ ESET Endpoint Security ของคุณ
> หากต้องการอัพเกรดจากเวอร์ชันที่ไม่รองรับ ให้ถอนการติดตั้ง ESET Endpoint Security ของคุณก่อน อ่านฐานความรู้ ESET ต่อไปนี้เพื่อศึกษาข้อมูลเพิ่มเติมเกี่ยวกับการอัพเกรด ESET Endpoint Security บนเวิร์กสเตชันของไคลเอ็นต์

การอัพเกรดอัตโนมัติสำหรับผลิตภัณฑ์ดั้งเดิม

เวอร์ชันผลิตภัณฑ์ ESET ของคุณไม่รองรับอีกต่อไป และผลิตภัณฑ์ของคุณได้รับการอัพเกรดให้เป็นเวอร์ชันล่าสุด

⚠ ปัญหาการติดตั้งทั่วไป

> ผลิตภัณฑ์ ESET เวอร์ชันใหม่ในแต่ละเวอร์ชันจะมีการแก้ไขบั๊กและปรับปรุงหลายประการ ลูกค้าเดิมที่มีใบอนุญาตที่ถูกต้องของผลิตภัณฑ์ ESET จะสามารถอัพเกรดผลิตภัณฑ์เดิมให้เป็นเวอร์ชันล่าสุดได้ฟรี

หากต้องการทำการติดตั้งให้เสร็จสิ้น:

1. ให้คลิก **ยอมรับและดำเนินการต่อ** เพื่อยอมรับ ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง และยอมรับนโยบายความเป็นส่วนตัว หากคุณไม่ยอมรับข้อตกลงผู้ใช้ปลายทาง ให้คลิก **ถอนการติดตั้ง** คุณจะไม่สามารถคืนค่าเป็นเวอร์ชันก่อนหน้าได้
2. คลิก **อนุญาตทั้งหมดและดำเนินการต่อ** เพื่ออนุญาต ระบบสะท้อนกลับ ESET LiveGrid® หรือคลิก **ดำเนินการต่อ** หากคุณไม่ต้องการมีส่วนร่วม
3. หลังเปิดใช้งานผลิตภัณฑ์ ESET ใหม่ด้วยรหัสใบอนุญาตของคุณ หน้าแรกจะปรากฏขึ้น หากไม่พบข้อมูลใบอนุญาต ให้ดำเนินการต่อไปด้วยใบอนุญาตทดลองใหม่ หากใบอนุญาตของคุณที่ใช้กับผลิตภัณฑ์ก่อนหน้านี้ไม่ถูกต้อง ให้ เปิดใช้งานผลิตภัณฑ์ ESET ของคุณ
4. ต้องรีสตาร์ทอุปกรณ์เพื่อดำเนินการติดตั้งให้เสร็จสมบูรณ์

การอัพเดทการรักษาความปลอดภัยและความเสถียร

การอัพเดท ESET Endpoint Security เป็นส่วนสำคัญในการทำให้เราสามารถปกป้องคุณจากรหัสที่เป็นอันตรายอย่างสมบูรณ์ได้ต่อไป ESET Endpoint Security เวอร์ชันใหม่แต่ละเวอร์ชันมีการปรับปรุงและการแก้ไขบั๊กมากมาย เราขอแนะนำให้คุณอัพเดท ESET Endpoint Security เป็นระยะๆ เพื่อป้องกันจุดอ่อนด้านความปลอดภัยและภัยคุกคาม ESET Endpoint Security จะใช้ได้จนถึงขั้นที่กำหนดของวงจรชีวิตผลิตภัณฑ์เช่นเดียวกับผลิตภัณฑ์อื่นๆ ของ ESET

อ่านเพิ่มเติมเกี่ยวกับ:
นโยบายสิ้นสุดอายุการใช้งาน (ผลิตภัณฑ์ธุรกิจ)
การอัพเดทผลิตภัณฑ์
ฮอตฟิกซ์เกี่ยวกับความปลอดภัยและความเสถียร
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเปลี่ยนแปลงใน ESET Endpoint Security โปรดอ่านบทความฐานความรู้ของ ESET ดังต่อไปนี้

การอัพเดทอัตโนมัติช่วยให้มั่นใจได้ถึงความปลอดภัยและเสถียรภาพสูงสุดของผลิตภัณฑ์ของคุณ คุณไม่สามารถปิดใช้งานการอัพเดทการรักษาความปลอดภัยและเสถียรภาพได้

การเปิดใช้งานผลิตภัณฑ์

หลังจากที่ติดตั้งเสร็จสมบูรณ์แล้ว คุณจะได้รับข้อความให้เปิดใช้ผลิตภัณฑ์ของคุณ

การเปิดใช้งานผลิตภัณฑ์สามารถทำได้หลายวิธี ตัวเลือกในการเปิดใช้งานในหน้าต่างการเปิดใช้งานอาจแตกต่างกันไปตามแต่ละประเทศ รวมถึงวิธีการแจกจ่าย (หน้าเว็บ ESET ซีดี/ดีวีดี ประเภทการติดตั้ง .msi หรือ .exe เป็นต้น)

คุณสามารถเปิดใช้งาน ESET Endpoint Security ได้ใน หน้าต่างโปรแกรมหลัก > **วิธีใช้และการสนับสนุน** > **เปิดใช้งานผลิตภัณฑ์** หรือไปยัง **สถานะการป้องกัน** > **เปิดใช้งานผลิตภัณฑ์**

คุณสามารถใช้วิธีการใด ๆ ต่อไปนี้เพื่อเปิดใช้งาน ESET Endpoint Security:

- **ใช้รหัสใบอนุญาตที่ซื้อมา**- สตริงที่ไม่ซ้ำกันในรูปแบบ XXXX-XXXX-XXXX-XXXX-XXXX ซึ่งใช้ในการระบุรหัสประจำตัวของเจ้าของใบอนุญาตและเปิดใช้งานใบอนุญาต
- **ESET HUB** – บัญชี ESET HUB ที่คุณจำเป็นต้องสร้าง ESET HUB เป็นเกตเวย์กลางไปยัง ESET PROTECT ซึ่งเป็นแพลตฟอร์มการรักษาความปลอดภัยแบบครบวงจร ซึ่งจะมีข้อมูลประจำตัว การสมัครใช้งาน และการจัดการผู้ใช้แบบรวมศูนย์สำหรับโมดูลแพลตฟอร์ม ESET ทั้งหมด คุณยังสามารถใช้ตัวเลือกนี้เพื่อเปิดใช้งาน ESET Endpoint Security ด้วยเครื่องมือการจัดการใบอนุญาตเวอร์ชันที่เก่ากว่า (ESET Business Account หรือ ESET MSP Administrator)
- **ใบอนุญาตแบบออฟไลน์** – ไฟล์ที่สร้างขึ้นมาโดยอัตโนมัติซึ่งจะโอนไปยังผลิตภัณฑ์ ESET เพื่อให้ข้อมูลใบ

อนุญาต หากใบอนุญาตยอมให้คุณดาวน์โหลดไฟล์ใบอนุญาตแบบออฟไลน์ (.lf) เราสามารถใช้ไฟล์นั้นทำการเปิดใช้งานแบบออฟไลน์ จำนวนใบอนุญาตแบบออฟไลน์จะถูกลบออกจากจำนวนใบอนุญาตที่ใช้ได้ทั้งหมด สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการสร้างไฟล์ออฟไลน์ ดูที่คู่มือผู้ใช้ออนไลน์ของ ESET Business Account

คลิก **เปิดใช้งานในภายหลัง** ถ้าคอมพิวเตอร์ของคุณเป็นสมาชิกของเครือข่ายที่จัดการ และผู้ดูแลของคุณจะดำเนินการเปิดใช้งานระยะไกลผ่าน ESET PROTECT นอกจากนี้ คุณยังสามารถใช้ตัวเลือกนี้ได้ หากต้องการเปิดใช้งานไคลเอ็นต์นี้ในภายหลัง

หากคุณมีชื่อผู้ใช้และรหัสผ่านที่ใช้เปิดใช้งานผลิตภัณฑ์ ESET เวอร์ชันเก่า ให้ แปลงข้อมูลประจำตัวการเข้าสู่ระบบเดิมของคุณเป็นรหัสใบอนุญาต

คุณสามารถเปลี่ยนใบอนุญาตผลิตภัณฑ์ของคุณเมื่อใดก็ได้โดยไปที่ หน้าต่างโปรแกรมหลัก > **วิธีใช้และสนับสนุน** > **เปลี่ยนใบอนุญาต** คุณจะเห็น ID ใบอนุญาตสาธารณะที่ใช้เพื่อระบุใบอนุญาตของคุณกับฝ่ายสนับสนุน ESET

ESET PROTECT สามารถเปิดใช้งานคอมพิวเตอร์ไคลเอ็นต์โดยไม่ต้องแจ้งให้ทราบได้โดยใช้ใบอนุญาตที่ผู้ดูแลทำให้สามารถใช้งานได้ โปรดดูคำแนะนำที่ วิธีใช้แบบออนไลน์ของ ESET PROTECT

⚠ ไม่สามารถเปิดใช้งานผลิตภัณฑ์ได้ใช่หรือไม่

การป้อนรหัสใบอนุญาตของคุณระหว่างการเปิดใช้งาน

การอัพเดทอัตโนมัติมีความสำคัญต่อความปลอดภัยของคุณ ESET Endpoint Security จะรับรายการอัพเดทต่างๆ หลังจากที่ได้รับการเปิดใช้งานแล้วโดยใช้ **รหัสใบอนุญาต** ของคุณ

หากคุณไม่ป้อนรหัสใบอนุญาตหลังการติดตั้ง ผลิตภัณฑ์ของคุณจะไม่ถูกเปิดใช้งาน คุณสามารถเปลี่ยนใบอนุญาตของคุณได้ใน หน้าต่างหลักของโปรแกรม เพื่อเปลี่ยนใบอนุญาต ให้คลิก **วิธีใช้และการสนับสนุน** > **เปิดใช้งานใบอนุญาต** และป้อนข้อมูลใบอนุญาตที่คุณได้รับพร้อมกับผลิตภัณฑ์ความปลอดภัยของ ESET ของคุณลงในหน้าต่างการเปิดใช้งานผลิตภัณฑ์

เมื่อเข้าสู่ **รหัสใบอนุญาต** เป็นสิ่งสำคัญมากที่จะต้องป้อนให้ตรงตามที่ได้เขียนไว้:

- รหัสใบอนุญาตของคุณคือสตริงที่ไม่ซ้ำกันในรูปแบบ XXXX-XXXX-XXXX-XXXX-XXXX ซึ่งใช้ในการระบุรหัสประจำตัวของเจ้าของใบอนุญาตและเปิดใช้งานใบอนุญาต

เราขอแนะนำให้คุณคัดลอกและวางรหัสใบอนุญาตของคุณจากอีเมลลงทะเบียนของคุณเพื่อให้มั่นใจว่าถูกต้อง

บัญชี ESET HUB

ESET HUB เป็นเกตเวย์กลางไปยัง ESET PROTECT ซึ่งเป็นแพลตฟอร์มการรักษาความปลอดภัยแบบครบวงจร ซึ่งจะมีข้อมูลประจำตัว การสมัครใช้งาน และการจัดการผู้ใช้แบบรวมศูนย์สำหรับโมดูลแพลตฟอร์ม ESET ทั้งหมด เมื่อใช้ ESET HUB คุณสามารถทำสิ่งต่อไปนี้ได้:

- ดูภาพรวมการสมัครใช้งานความปลอดภัย
- ตรวจสอบการใช้และสถานะการบริการที่สมัครสมาชิก
- จัดสรรและควบคุมการเข้าถึงแบบละเอียดไปยังแพลตฟอร์ม ESET แต่ละแพลตฟอร์ม
- ใช้การลงชื่อเข้าใช้แบบครั้งเดียวกับแพลตฟอร์ม ESET ที่เข้าถึงได้และเชื่อมโยงไว้ทั้งหมด

คุณยังสามารถใช้ตัวเลือกการเปิดใช้งานนี้เพื่อเปิดใช้งาน ESET Endpoint Security ด้วยเครื่องมือการจัดการใบอนุญาตเวอร์ชันที่เก่ากว่า (ESET Business Account หรือ ESET MSP Administrator)

คุณสามารถ สร้างบัญชี ESET HUB และเข้าสู่ระบบด้วย **ที่อยู่อีเมล** และ **รหัสผ่าน** ของคุณ

หากคุณลืมรหัสผ่านของคุณ ให้คลิก **ฉันลืมรหัสผ่าน** แล้วคุณจะถูกเปลี่ยนเส้นทางไปที่ ESET HUB ป้อนที่อยู่อีเมลของคุณ แล้วคลิก **ลงชื่อเข้าใช้** เพื่อยืนยัน จากนั้นคุณจะได้รับข้อความพร้อมคำแนะนำวิธีรีเซ็ตรหัสผ่าน

วิธีใช้สิทธิการใช้งานใบอนุญาตแบบเดิมเพื่อเปิดใช้งานผลิตภัณฑ์เอ็นพอยต์ ESET

หากคุณมีชื่อผู้ใช้และรหัสผ่าน และต้องการรับรหัสใบอนุญาต โปรดไปที่ ESET Business Account พอร์ทัล ซึ่งคุณสามารถแปลงข้อมูลการเข้าสู่ระบบของคุณเป็นรหัสใบอนุญาตใหม่ได้

การเปิดใช้งานล้มเหลว

หากการเปิดใช้งาน ESET Endpoint Security ไม่ประสบความสำเร็จ สถานการณ์ที่พบมากที่สุดคือ:

- รหัสใบอนุญาตมีการใช้งานอยู่แล้ว

- คุณได้ป้อนรหัสใบอนุญาตที่ไม่ถูกต้อง
- ข้อมูลในแบบฟอร์มการเปิดใช้งานหายไปหรือไม่ถูกต้อง
- การสื่อสารกับเซิร์ฟเวอร์การเปิดใช้งานล้มเหลว
- ไม่มีหรือปิดใช้งานการเชื่อมต่อไปยังเซิร์ฟเวอร์การเปิดใช้งาน ESET

ตรวจสอบว่าคุณได้ป้อนรหัสใบอนุญาตที่เหมาะสมหรือแนบใบอนุญาตแบบออฟไลน์ แล้วลองเปิดใช้งานอีกครั้ง

หากคุณไม่สามารถเปิดใช้งานได้ แพ็คเกจต้อนรับของเราจะนำคุณไปรู้จักกับคำถามทั่วไป ข้อผิดพลาด ปัญหาที่เกี่ยวกับการเปิดใช้งานและการอนุญาต (พร้อมให้ใช้งานในรูปแบบภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษา)

- เริ่มต้นการแก้ไขปัญหาการเปิดใช้งานผลิตภัณฑ์ของ ESET

การลงทะเบียน

โปรดลงทะเบียนใบอนุญาตของคุณโดยกรอกช่องในแบบฟอร์มการลงทะเบียนให้เสร็จสมบูรณ์แล้วคลิก **ทำต่อ** โดยต้องกรอกช่องที่ทำเครื่องหมายว่าจำเป็นในวงเล็บ ข้อมูลนี้จะใช้สำหรับกรณีที่เกี่ยวข้องกับใบอนุญาต ESET ของคุณเท่านั้น

ความคืบหน้าของการเปิดใช้งาน

ESET Endpoint Security กำลังเปิดใช้งานอยู่ตอนนี้ ขั้นตอนนี้อาจใช้เวลาสักครู่

เปิดใช้งานสำเร็จแล้ว

เปิดใช้งานสำเร็จแล้วและเปิดใช้งาน ESET Endpoint Security แล้วตอนนี้ นับแต่นี้ไป ESET Endpoint Security จะได้รับการอัพเดทเป็นประจำเพื่อระบุชี้มัลแวร์ตัวล่าสุดและทำให้คอมพิวเตอร์ของคุณปลอดภัยอยู่เสมอ คลิก **เสร็จ** เพื่อดำเนินการเปิดใช้งานผลิตภัณฑ์ให้เสร็จสิ้น

ปัญหาการติดตั้งทั่วไป

หากพบปัญหาในระหว่างการติดตั้ง วิซาร์ดการติดตั้งจะให้ตัวแก้ไขปัญหาที่จะช่วยแก้ปัญหาหากเป็นไปได้

คลิก **เรียกใช้ตัวแก้ไขปัญหา** เพื่อให้ตัวแก้ไขปัญหาเริ่มทำงาน เมื่อดำเนินการเสร็จสิ้น โปรดดำเนินการตามโซลูชันที่แนะนำ

หากปัญหายังคงอยู่ โปรดดูรายการ ข้อผิดพลาดทั่งไปของการติดตั้งและวิธีแก้ไข

คู่มือสำหรับผู้เริ่มต้น

บทนี้จะให้ภาพรวมเริ่มต้นของ ESET Endpoint Security และการตั้งค่าพื้นฐานของโปรแกรม

ไอคอนในถาดข้อมูลระบบ

มีตัวเลือกและคุณลักษณะของการตั้งค่าที่สำคัญที่สุดบางรายการสามารถใช้ได้ด้วยการคลิกขวาที่ไอคอนในถาดข้อมูลระบบ 

> หากต้องการเข้าถึงเมนูไอคอนถาดระบบ (พื้นที่แจ้งเตือนของ Windows) โปรดตรวจสอบให้แน่ใจว่าโหมดเริ่มต้นของ องค์ประกอบส่วนติดต่อผู้ใช้ ถูกตั้งค่าเป็นเต็ม

หยุดการป้องกันชั่วคราว – แสดงกล่องข้อความยืนยันที่ปิดใช้งาน กลไกการตรวจจับ ที่ป้องกันการโจมตีโดยการควบคุมไฟล์ การสื่อสารทางเว็บและอีเมล เมนู **ช่วงเวลา** แบบเลื่อนลงช่วยให้คุณสามารถระบุระยะเวลาที่การป้องกันจะถูกปิดใช้งานได้

ปิดไฟร์วอลล์ชั่วขณะ (อนุญาตการรับส่งทั้งหมด) – สลับไฟร์วอลล์เป็นสถานะไม่ใช้งาน โปรดดู เครือข่าย สำหรับข้อมูลเพิ่มเติม

ปิดกั้นการรับส่งของเครือข่ายทั้งหมด – ปิดกั้นการรับส่งของเครือข่ายทั้งหมด คุณสามารถเปิดใช้งานอีกครั้งได้โดยการคลิกที่**หยุดปิดกั้นการรับส่งข้อมูลเครือข่ายทั้งหมด**

การตั้งค่าขั้นสูง – เปิดการตั้งค่าขั้นสูงของ ESET Endpoint Security หากต้องการเปิดการตั้งค่าขั้นสูงจาก หน้าต่างโปรแกรมหลัก ให้กด F5 บนแป้นพิมพ์หรือคลิก **การตั้งค่า** > **การตั้งค่าขั้นสูง**

ไฟล์บันทึก – ไฟล์บันทึก ประกอบไปด้วยข้อมูลเกี่ยวกับเหตุการณ์ของโปรแกรมสำคัญที่เกิดขึ้น และให้ภาพรวมของการตรวจพบ

เปิด ESET Endpoint Security – เปิด หน้าต่างโปรแกรมหลัก ของ ESET Endpoint Security จากไอคอนถาด (พื้นที่แจ้งเตือนของ Windows)

รีเซ็ตเค้าโครงหน้าต่าง - รีเซ็ตหน้าต่างของ ESET Endpoint Security เป็นขนาดและตำแหน่งเริ่มต้นบนหน้าจอ

โหมดสี – เปิด การตั้งค่าส่วนต่อประสานผู้ใช้ ซึ่งคุณสามารถเปลี่ยนสีของ GUI ได้

ตรวจหาการอัปเดต เริ่มการอัพเดทโมดูลหรือการอัพเดทผลิตภัณฑ์เพื่อให้แน่ใจว่าคุณได้รับการป้องกัน ESET Endpoint Security จะตรวจสอบการอัพเดทอัตโนมัติหลายครั้งต่อวัน

เกี่ยวกับ – ให้ข้อมูลระบบ, รายละเอียดเกี่ยวกับเวอร์ชันของ ESET Endpoint Security ที่ติดตั้ง, โมดูลโปรแกรมที่ติดตั้ง และข้อมูลเกี่ยวกับระบบปฏิบัติการและทรัพยากรระบบ

แป้นพิมพ์ลัด

เพื่อให้การนำทางใน ESET Endpoint Security ดียิ่งขึ้น คุณสามารถใช้แป้นพิมพ์ลัดต่อไปนี้ได้:

แป้นพิมพ์ลัด	การทำงาน
F1	เปิดหน้าวิธีใช้
F5	เปิด การตั้งค่าขั้นสูง
ลูกศรขึ้น / ลูกศรลง	การนำทางในรายการเมนูแบบเลื่อนลง
TAB	ย้ายไปยังองค์ประกอบ GUI ถัดไปในหน้าต่าง
Shift+TAB	ย้ายไปยังองค์ประกอบ GUI ก่อนหน้าในหน้าต่าง
ESC	ปิดหน้าต่างข้อความที่ใช้งาน
Ctrl+U	แสดงข้อมูลเกี่ยวกับใบอนุญาต ESET และคอมพิวเตอร์ของคุณ (รายละเอียดสำหรับการสนับสนุนด้านเทคนิค)
Ctrl+R	รีเซ็ตหน้าต่างผลิตภัณฑ์กลับเป็นขนาดและตำแหน่งตามค่าเริ่มต้นบนหน้าจอ
ALT + ลูกศรซ้าย	ย้อนกลับ
ALT + ลูกศรขวา	ไปข้างหน้า
ALT+Home	นำทางในหน้าแรก

คุณยังสามารถใช้ปุ่มเมาส์ย้อนกลับหรือไปข้างหน้าสำหรับการนำทางได้ด้วยเช่นกัน

โปรไฟล์

ตัวจัดการโปรไฟล์ถูกใช้อยู่สองส่วนภายใน ESET Endpoint Security ในส่วน **การสแกนตามต้องการ** และในส่วน **อัพเดท**

การสแกนคอมพิวเตอร์

โปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าใน ESET Endpoint Security จะมีอยู่ด้วยกันทั้งหมด 4 รายการ:

- **การสแกนแบบสมาร์ท** - เป็นการสแกนขั้นสูงตามค่าเริ่มต้น โดยโปรไฟล์การสแกนแบบสมาร์ทใช้เทคโนโลยี Smart Optimization ซึ่งไม่รวมไฟล์ที่พบว่าปลอดภัยในการสแกนก่อนหน้านี้และไม่ได้ถูกแก้ไขตั้งแต่การสแกนครั้งก่อนหน้า วิธีนี้ช่วยให้เวลาในการสแกนลดลงโดยมีผลกระทบต่อความปลอดภัยของระบบน้อยที่สุด
- **การสแกนเมนูบริบท** - คุณสามารถเริ่มสแกนไฟล์ใดก็ได้จากเมนูบริบทได้ตามต้องการ โปรไฟล์การสแกนเมนูบริบทจะช่วยให้คุณกำหนดการกำหนดค่าการสแกนซึ่งจะใช้เมื่อคุณเปิดการสแกนวิธีนี้
- **สแกนเชิงลึก** - โปรไฟล์การสแกนเชิงลึกไม่ได้ใช้ Smart Optimization โดยค่าเริ่มต้น ดังนั้นจะไม่มีไฟล์ใดที่ไม่รวมอยู่ในการสแกนเมื่อใช้โปรไฟล์นี้
- **การสแกนคอมพิวเตอร์** - เป็นโปรไฟล์ตามค่าเริ่มต้นที่ใช้ในการสแกนคอมพิวเตอร์มาตรฐาน

คุณสามารถบันทึกพารามิเตอร์การสแกนที่ต้องการได้เพื่อการสแกนในอนาคต ขอแนะนำให้คุณสร้างโปรไฟล์อีกโปรไฟล์หนึ่ง (ที่มีเป้าหมายการสแกน วิธีการสแกน และพารามิเตอร์อื่นๆ) สำหรับแต่ละการสแกนที่ใช้เป็นประจำ

หากต้องการสร้างโปรไฟล์ใหม่ ให้เปิด การตั้งค่าขั้นสูง **กลไกการตรวจจับ** > **การสแกนมัลแวร์** > **การสแกนตามต้องการ** > **รายการโปรไฟล์** > **แก้ไข** หน้าต่าง **ตัวจัดการโปรไฟล์** มีเมนูแบบเลื่อนลง **โปรไฟล์ที่เลือก** ซึ่งแสดงโปรไฟล์การสแกนที่มีอยู่และตัวเลือกสำหรับสร้างโปรไฟล์ใหม่ เพื่อช่วยให้คุณสร้างโปรไฟล์การสแกนให้เหมาะสมกับความต้องการ โปรดไปที่ ThreatSense เพื่อดูคำอธิบายของพารามิเตอร์แต่ละรายการของการตั้งค่าการสแกน

> สมมติว่าคุณต้องการสร้างโปรไฟล์การสแกนของคุณเอง และการกำหนดค่า **การสแกนคอมพิวเตอร์ของคุณ**การกำหนดค่าบางส่วนเป็นสิ่งที่เหมาะสม แต่คุณไม่ต้องการสแกน รันไทม์แพ็คเกอร์ หรือ แอพพลิเคชันที่อาจไม่ปลอดภัย และคุณยังต้องการใช้ **ตรวจหาวิธีการแก้ไขเสมอ** ให้ป้อนชื่อของโปรไฟล์ใหม่ของคุณในหน้าต่าง **ตัวจัดการโปรไฟล์** แล้วคลิก **เพิ่ม** เลือกโปรไฟล์ใหม่ของคุณจากเมนูแบบเลื่อนลง **โปรไฟล์ที่เลือก** แล้วปรับพารามิเตอร์ที่เหลือเพื่อให้ตรงกับความต้องการ จากนั้นคลิก**ตกลง** เพื่อบันทึกโปรไฟล์ของคุณ

อัพเดท

เครื่องมือแก้ไขโปรไฟล์ใน การตั้งค่าการอัพเดท จะช่วยให้ผู้ใช้สร้างโปรไฟล์การอัพเดทใหม่ สร้างและใช้โปรไฟล์แบบกำหนดเองของคุณ (นอกเหนือจาก **โปรไฟล์ของฉัน** ที่เป็นค่าเริ่มต้น) ต่อเมื่อคอมพิวเตอร์ของคุณใช้วิธีการเชื่อมต่อหลายวิธีในการอัพเดทเซิร์ฟเวอร์

ตัวอย่างเช่น แล็ปท็อปที่โดยปกติแล้วจะเชื่อมต่อกับเซิร์ฟเวอร์ในระบบ (มิเรอร์) ในเครือข่ายในระบบ แต่จะดาวน์โหลดการอัพเดทโดยตรงจากเซิร์ฟเวอร์การอัพเดทของ ESET เมื่อตัดการเชื่อมต่อจากเครือข่ายในระบบ (การเดินทางเพื่อธุรกิจ) อาจใช้โปรไฟล์สองโปรไฟล์: โปรไฟล์แรกใช้เพื่อเชื่อมต่อกับเซิร์ฟเวอร์ในระบบ และอีกโปรไฟล์

หนึ่งใช้เพื่อเชื่อมต่อกับเซิร์ฟเวอร์ของ ESET หลังจากโปรไฟล์เหล่านี้ได้รับการกำหนดค่าแล้ว ให้นำทางไปยัง **เครื่องมือ** > **เครื่องมือวางกำหนดการ** และแก้ไขพารามิเตอร์งานการอัพเดท กำหนดโปรไฟล์หนึ่งเป็นโปรไฟล์หลักและอีกแบบหนึ่งเป็นโปรไฟล์สำรอง

โปรไฟล์การอัพเดท – โปรไฟล์การอัพเดทที่ใช้อยู่ในขณะนี้ เมื่อต้องการเปลี่ยนแปลง ให้เลือกโปรไฟล์จากเมนูแบบเลื่อนลง

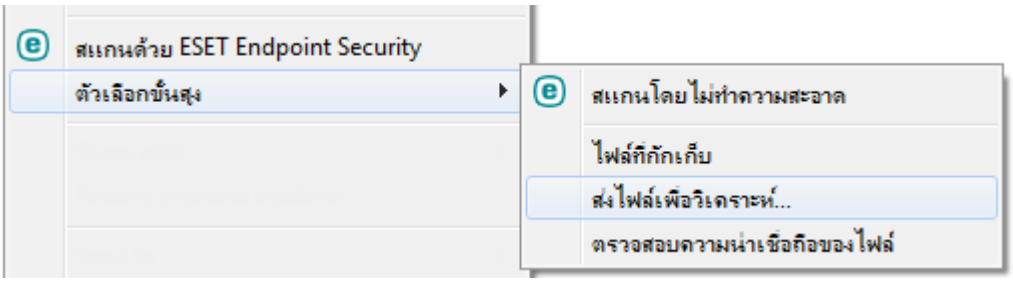
รายการของโปรไฟล์ – สร้างโปรไฟล์อัพเดทใหม่หรือลบโปรไฟล์อัพเดทที่มีอยู่

เมนูบริบท

เมนูบริบทจะปรากฏเมื่อคลิกขวาที่วัตถุ (ไฟล์) เมนูนี้จะแสดงการทำงานทั้งหมดที่สามารถดำเนินการกับวัตถุนั้น

คุณสามารถรวมองค์ประกอบการควบคุม ESET Endpoint Security ไว้ในเมนูบริบทได้ ตัวเลือกการตั้งค่าสำหรับฟังก์ชันนี้จะมีอยู่ใน การตั้งค่าขั้นสูง > **อินเทอร์เฟซผู้ใช้** > **องค์ประกอบของอินเทอร์เฟซผู้ใช้**

รวมเข้ากับเมนูบริบท – รวมองค์ประกอบการควบคุม ESET Endpoint Security ไว้ในเมนูบริบท

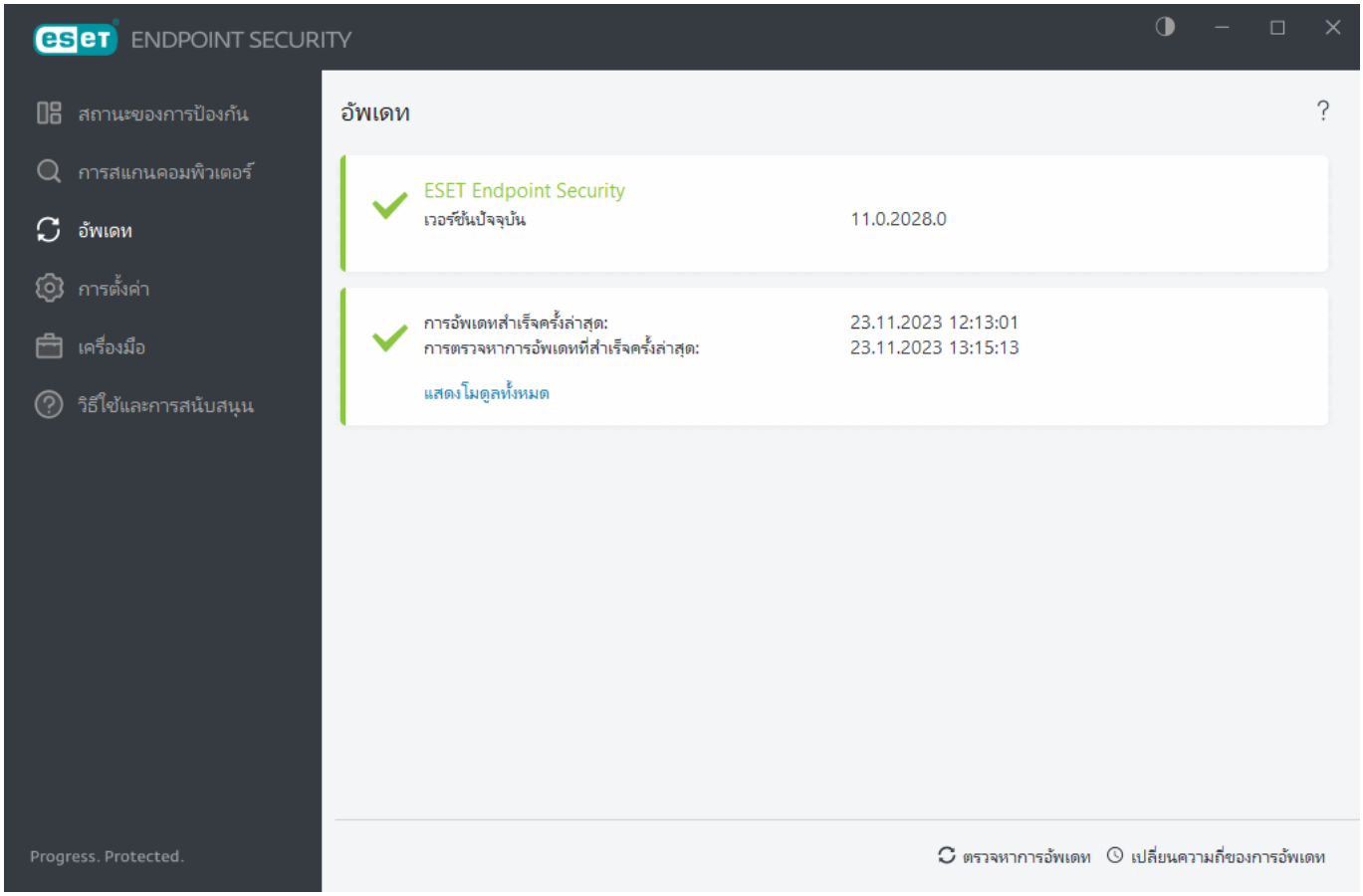


การตั้งค่าการอัพเดท

การอัพเดท ESET Endpoint Security เป็นประจำเป็นวิธีการที่ดีที่สุดในการให้การรักษาความปลอดภัยสูงสุดแก่คอมพิวเตอร์ โมดูลการอัพเดทจะช่วยให้มั่นใจได้ว่าทั้งโมดูลโปรแกรมและส่วนประกอบของระบบจะอัพเดทอยู่เสมอ

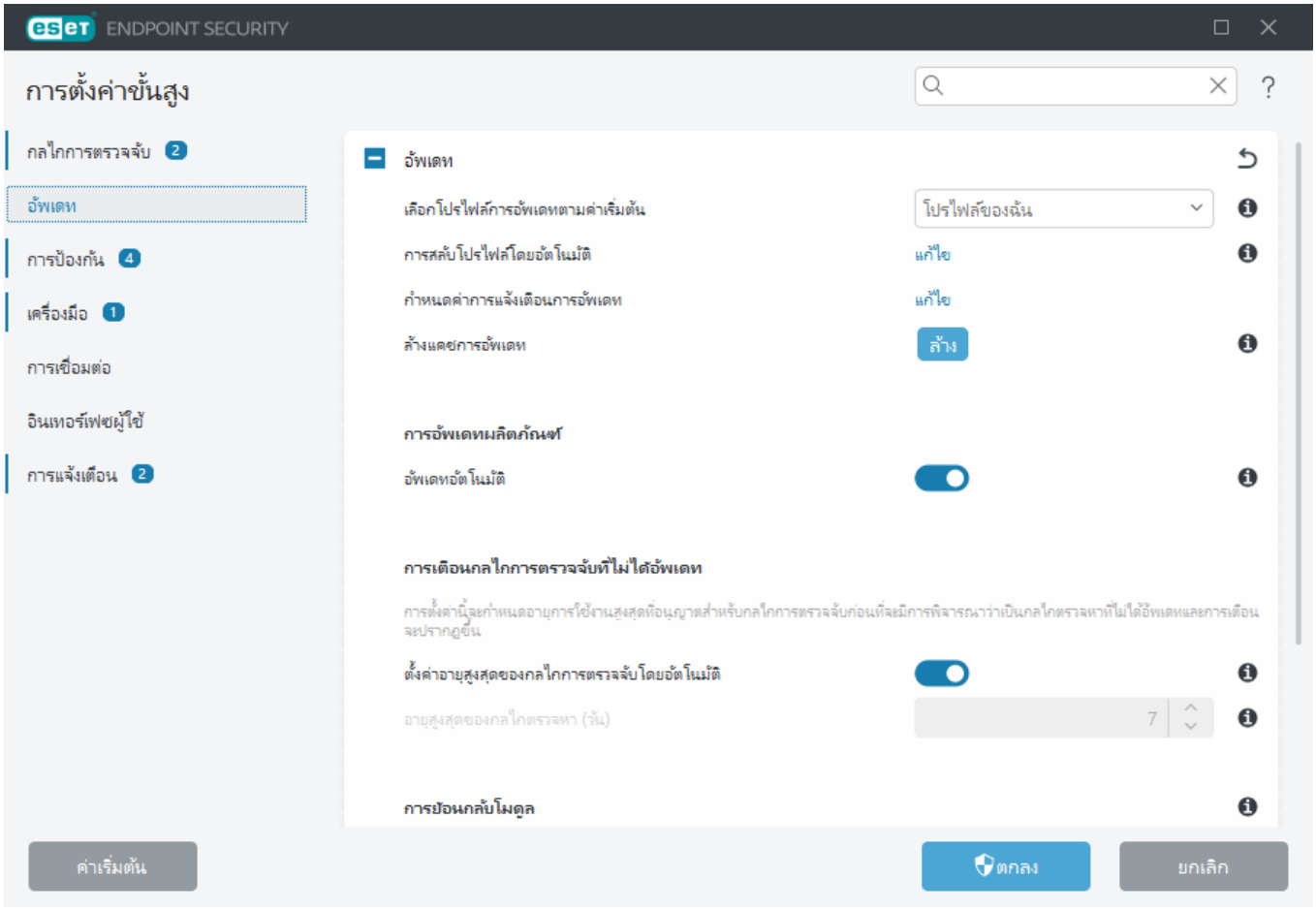
เมื่อคลิก **อัพเดท** ในหน้าต่างโปรแกรมหลัก คุณสามารถดูสถานะการอัพเดทในปัจจุบัน รวมถึงวันที่และเวลาของการอัพเดทที่สำเร็จครั้งล่าสุด และดูว่าจะต้องมีการอัพเดทหรือไม่ได้

นอกเหนือจากการอัพเดทอัตโนมัติแล้ว คุณยังสามารถคลิก **ตรวจหาการอัพเดท** เพื่อเรียกใช้การอัพเดทด้วยตนเองได้



การตั้งค่าขั้นสูง > **อัพเดท** จะมีตัวเลือกการอัพเดทเพิ่มเติม เช่น โหมดอัพเดท การเข้าถึงพร็อกซีเซิร์ฟเวอร์ และการเชื่อมต่อ LAN

หากคุณประสบปัญหากับการอัพเดท ให้คลิกที่ **ล้าง** เพื่อล้างไฟล์แคชการอัพเดท หากยังคงไม่สามารถอัพเดทโมดูลโปรแกรมได้ โปรดดูที่ส่วน ข้อความการแก้ไขปัญหาสำหรับ "การอัพเดทโมดูลล้มเหลว"

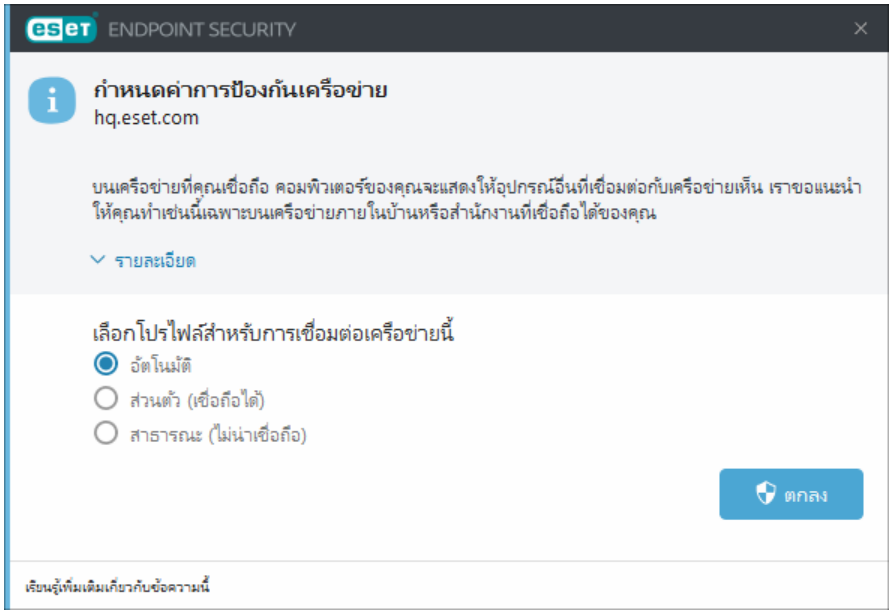


ตัวเลือก **เลือกโดยอัตโนมัติ** ใน การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์**> **อัพเดท** > **อัพเดทโมดูล** จะเปิดใช้งานโดยค่าเริ่มต้น เมื่อใช้งานเซิร์ฟเวอร์การอัพเดท ESET สำหรับรับการอัพเดท เราแนะนำให้ปล่อยตัวเลือกนั้นไว้ตามเดิม

โปรแกรมต้องได้รับการอัพเดทโดยอัตโนมัติเพื่อให้การทำงานมีประสิทธิภาพสูงสุด การอัพเดทอัตโนมัติจะเกิดขึ้นต่อเมื่อมีการป้อนรหัสใบอนุญาตที่ถูกต้องใน **วิธีใช้และการสนับสนุน** > **เปิดใช้งานผลิตภัณฑ์** หากคุณไม่ได้ป้อนชื่อรหัสใบอนุญาต หลังการติดตั้ง คุณสามารถทำเมื่อใดก็ได้ สำหรับข้อมูลโดยละเอียดเพิ่มเติมเกี่ยวกับการเปิดใช้งาน โปรดดูวิธีเปิดใช้งาน ESET Endpoint Security

กำหนดค่าการป้องกันเครือข่าย

โดยค่าเริ่มต้น ESET Endpoint Security จะใช้การตั้งค่า Windows เมื่อมีการตรวจพบการเชื่อมต่อเครือข่ายรายการใหม่ หากต้องการแสดงหน้าต่างโต้ตอบเมื่อตรวจพบเครือข่ายใหม่ ให้เปลี่ยน การกำหนดโปรไฟล์การป้องกันเครือข่าย เป็น **ถาม** การกำหนดค่าการป้องกันเครือข่ายจะเกิดขึ้นเมื่อใดก็ตามที่คอมพิวเตอร์ของคุณเชื่อมต่อกับเครือข่ายใหม่



คุณสามารถเลือกจาก โปรไฟล์การเชื่อมต่อเครือข่าย ต่อไปนี้:

อัตโนมัติ — ESET Endpoint Security จะเลือกโปรไฟล์โดยอัตโนมัติ ตาม ตัวเปิดใช้งาน ที่กำหนดค่าไว้สำหรับแต่ละโปรไฟล์

ส่วนตัว – สำหรับเครือข่ายที่เชื่อถือได้ (เครือข่ายในบ้านหรือที่ทำงาน) ผู้ใช้เครือข่ายรายอื่นสามารถมองเห็นคอมพิวเตอร์และไฟล์ที่ใช้ร่วมกันที่เก็บไว้ในคอมพิวเตอร์ของคุณได้ และผู้ใช้รายอื่นบนเครือข่ายสามารถเข้าถึงทรัพยากรระบบได้ (เปิดใช้งานการเข้าถึงไฟล์ที่แชร์และเครื่องพิมพ์ การติดต่อสื่อสาร RPC ขาเข้า และการแชร์ผ่านเดสก์ท็อปจากระยะไกล) เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าถึงเครือข่ายภายในที่ปลอดภัย ระบบจะกำหนดโปรไฟล์นี้ไปยังการเชื่อมต่อเครือข่ายโดยอัตโนมัติหากมีการกำหนดค่าเป็น "โดเมน" หรือเครือข่าย "ส่วนตัว" ใน Windows

สาธารณะ – สำหรับเครือข่ายที่ไม่เชื่อถือ (เครือข่ายสาธารณะ) ไฟล์และโฟลเดอร์ในระบบของคุณจะไม่ถูกใช้ร่วมกันหรือมองเห็นได้สำหรับผู้ใช้รายอื่นบนเครือข่าย และการแบ่งปันทรัพยากรระบบจะถูกปิดใช้งาน เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าสู่เครือข่ายไร้สาย ระบบจะกำหนดโปรไฟล์นี้ไปยังการเชื่อมต่อเครือข่ายโดยอัตโนมัติหากมีการกำหนดค่าเป็น "โดเมน" หรือเครือข่าย "ส่วนตัว" ใน Windows

โปรไฟล์ที่ผู้ใช้กำหนด – คุณสามารถเลือก โปรไฟล์ที่คุณสร้าง จากเมนูแบบเลื่อนลง ตัวเลือกนี้จะใช้ได้ก็ต่อเมื่อคุณได้สร้างโปรไฟล์แบบกำหนดเองอย่างน้อยหนึ่งโปรไฟล์

การกำหนดค่าเครือข่ายที่ไม่ถูกต้องอาจทำให้เกิดความเสี่ยงด้านการรักษาความปลอดภัยของคอมพิวเตอร์ของคุณ

เครื่องมือควบคุมการเข้าถึงเว็บไซต์

ถ้าคุณเปิดใช้งานการควบคุมการเข้าถึงเว็บไซต์แล้วใน ESET Endpoint Security คุณต้องกำหนดค่าการควบคุมการเข้าถึงเว็บไซต์สำหรับบัญชีผู้ใช้ที่คุณต้องการเพื่อให้การควบคุมการเข้าถึงเว็บไซต์ทำงานอย่างถูกต้อง โปรดอ่านบท การควบคุมการเข้าถึงเว็บไซต์ สำหรับคำแนะนำเกี่ยวกับวิธีสร้างคำแนะนำเฉพาะสำหรับเวิร์กสเตชันของลูกค้าเพื่อป้องกันจากเนื้อหาที่อาจไม่เหมาะสม

แฮชที่ถูกบล็อก

การใช้ ESET Inspect ในสภาพแวดล้อมการทำงาน จะช่วยให้ผู้ดูแลระบบสามารถบล็อกการเข้าถึงไฟล์สั่งทำการที่ระบุโดยอิงตามแฮชได้ หากคุณพยายามเข้าถึงไฟล์สั่งทำการซึ่งผู้ดูแลระบบบล็อกการเข้าถึงไว้ ESET Endpoint Security จะแสดงการแจ้งเตือนนี้:

การเข้าถึงไฟล์ถูกบล็อก – แอพพลิเคชัน (ชื่อของแอพพลิเคชันจะปรากฏขึ้น) พยายามเข้าถึงไฟล์ที่ไม่ได้รับอนุญาตจากผู้ดูแลระบบของคุณ

หากคุณเป็นผู้ดูแลระบบและต้องการอนุญาตให้เข้าถึงแอพพลิเคชันที่ระบุในการแจ้งเตือน โปรดดูที่ แฮชที่ถูกบล็อก ในวิธีใช้แบบออนไลน์สำหรับ ESET Inspect หากคุณเป็นผู้ใช้และต้องการเปลี่ยนลักษณะการทำงานของแอพลิเคชัน ให้ติดต่อผู้ดูแลระบบของคุณ

การทำงานกับ ESET Endpoint Security

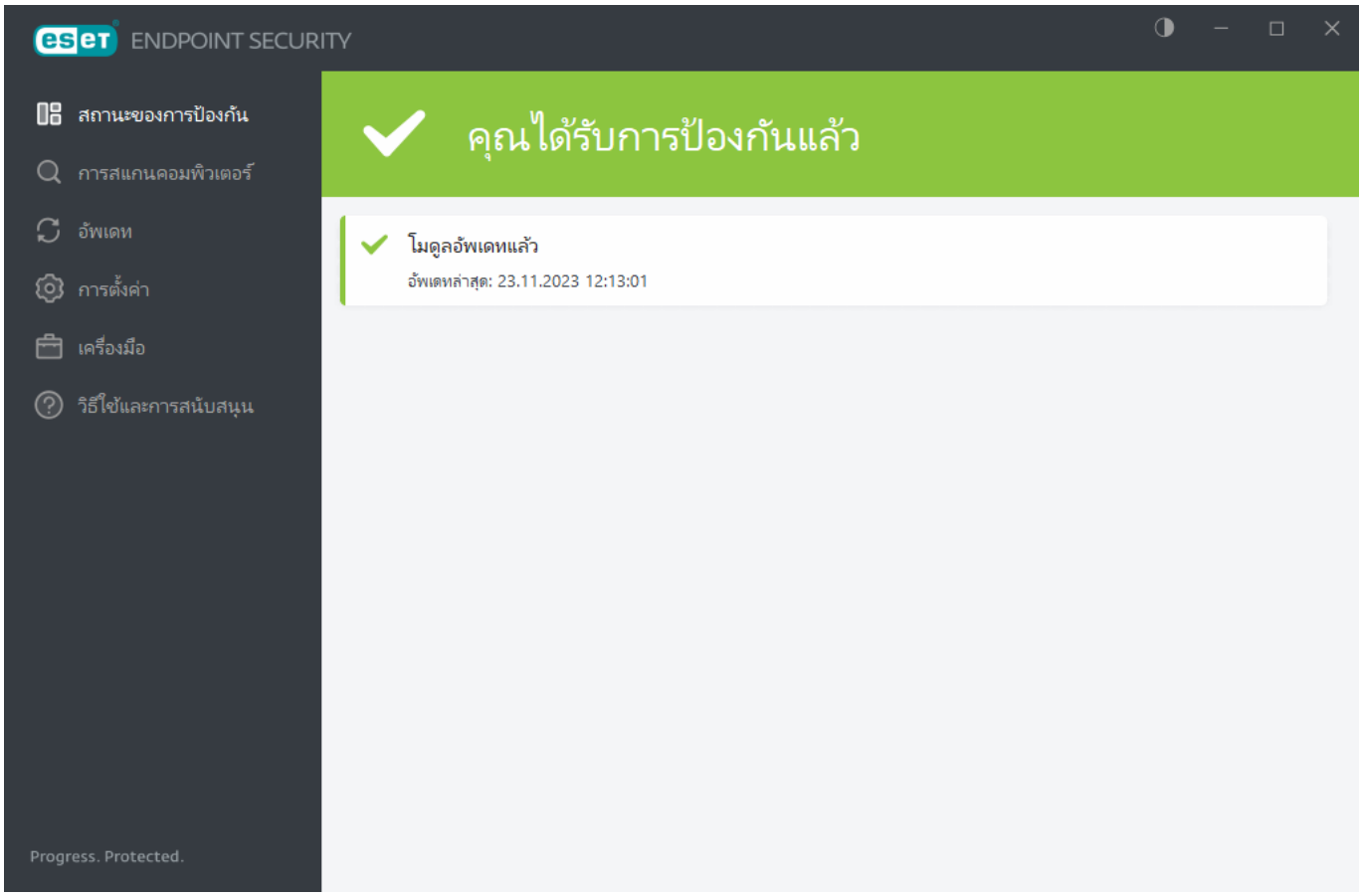
หน้าต่างโปรแกรมหลักของ ESET Endpoint Security จะแบ่งออกเป็นสองส่วน หน้าต่างหลักที่ด้านขวาจะแสดงข้อมูลที่เกี่ยวข้องกับตัวเลือกที่เลือกจากเมนูหลักทางด้านซ้าย

> **คำแนะนำพร้อมภาพประกอบ**
> โปรดดู เปิดหน้าต่างโปรแกรมหลังของผลิตภัณฑ์ ESET สำหรับ Windows เพื่อดูคำแนะนำพร้อมภาพประกอบของเราซึ่งมีให้แบบภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษา

คุณสามารถเลือกโทนสีของ ESET Endpoint Security GUI ได้ที่มุมบนขวาของหน้าต่างโปรแกรมหลัก คลิกไอคอน**โทนสี** (ไอคอนจะเปลี่ยนไปตามโทนสีที่เลือกในปัจจุบัน) ถัดจากไอคอน**ย่อขนาด** และเลือกโทนสีจากเมนูแบบเลื่อนลง:

- **เหมือนกับสีของระบบ** ตั้งค่าโทนสี ESET Endpoint Security ตามการตั้งค่าระบบปฏิบัติการของคุณ
- **มืด** ESET Endpoint Security จะมีโทนสีเข้ม (โหมดมืด)

- **สว่าง** ESET Endpoint Security จะมีโทนสีสว่าง ซึ่งเป็นโทนสีมาตรฐาน



ตัวเลือกเมนูหลัก:

สถานะของการป้องกัน – แจ้งข้อมูลเกี่ยวกับสถานะของการป้องกันของ ESET Endpoint Security

การสแกนคอมพิวเตอร์ - กำหนดค่าและเริ่มต้นสแกนคอมพิวเตอร์ของคุณหรือสร้างการสแกนแบบกำหนดเอง

อัพเดท – แสดงข้อมูลเกี่ยวกับโมดูลและการอัพเดทกลไกตรวจหา

เครื่องมือ - คุณลักษณะที่ช่วยให้การดูแลโปรแกรมง่ายขึ้นและเสนอตัวเลือกเพิ่มเติมสำหรับผู้ใช้ขั้นสูง

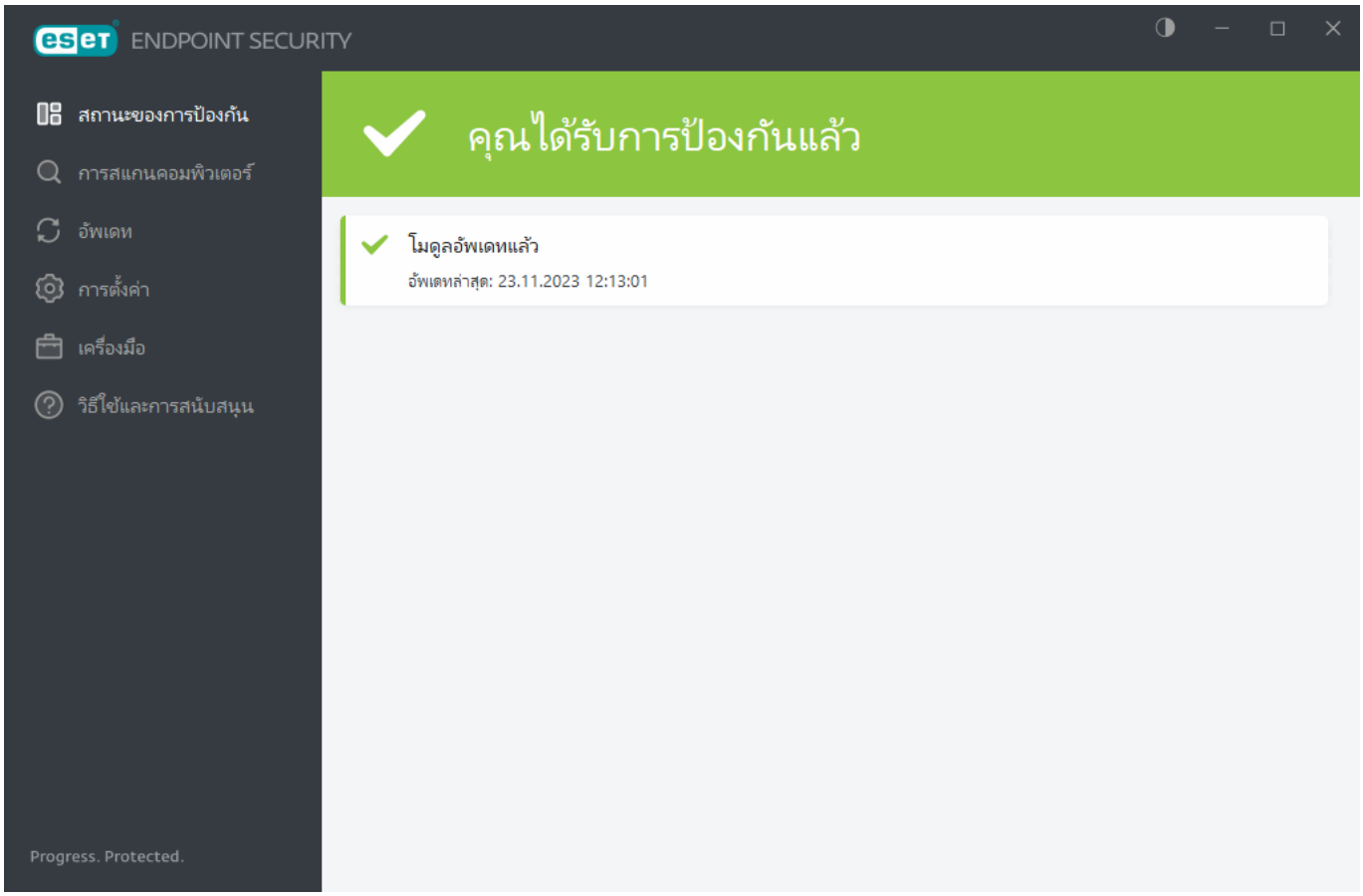
การตั้งค่า – มีตัวเลือกการกำหนดค่าสำหรับฟีเจอร์การป้องกันของ ESET Endpoint Security และการเข้าถึง การตั้งค่าขั้นสูง

ความช่วยเหลือและการสนับสนุน – แสดงข้อมูลเกี่ยวกับใบอนุญาตของคุณ, ผลิตภัณฑ์ ESET ที่ติดตั้ง, ลิงก์ไปยังความช่วยเหลือออนไลน์, ฐานความรู้ของ ESET และ การสนับสนุนทางเทคนิค

สถานะการป้องกัน

หน้าต่าง **สถานะการป้องกัน** จะแสดงข้อมูลเกี่ยวกับการป้องกันปัจจุบันของคอมพิวเตอร์ของคุณและการอัพเดทครั้งล่าสุด สถานะ **การป้องกันสูงสุด** สีเขียวจะแสดงว่ามีการป้องกันสูงสุด

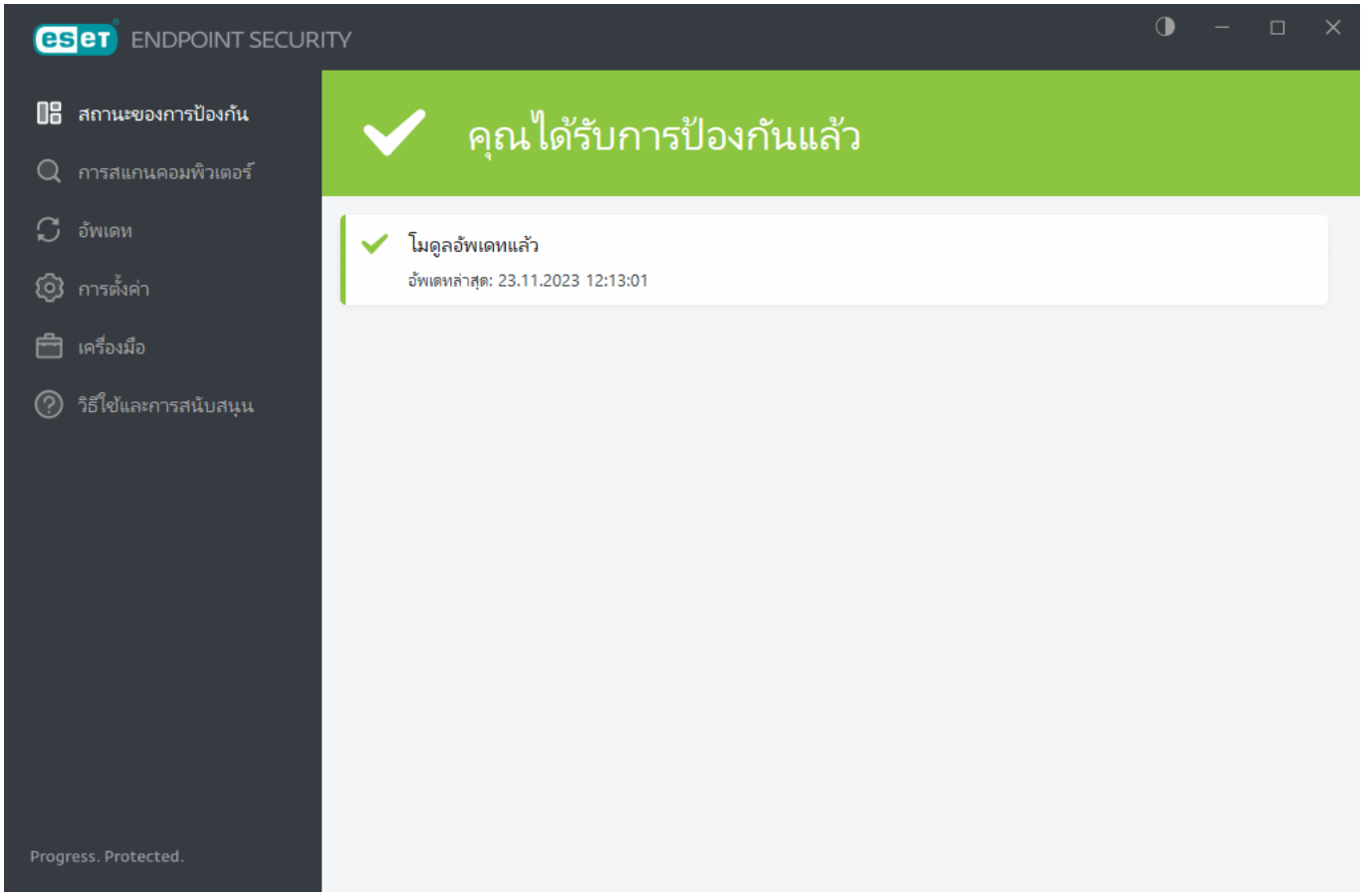
หน้าต่าง **สถานะการป้องกัน** จะแสดง การแจ้งเตือน พร้อมข้อมูลโดยละเอียดและวิธีแก้ไขปัญหาที่แนะนำเพื่อปรับปรุงความปลอดภัยของ ESET Endpoint Security แล้วเปิดคุณลักษณะเพิ่มเติม หรือให้การปกป้องสูงสุด



ไอคอนสีเขียวและสถานะ **คุณได้รับการป้องกันแล้ว** สีเขียวแสดงว่ามีการป้องกันขั้นสูงสุด

ควรทำอย่างไรเมื่อโปรแกรมทำงานไม่ถูกต้อง

ไอคอนเครื่องหมายถูกสีเขียวจะปรากฏขึ้นถัดจากโมดูลโปรแกรมทั้งหมดที่สามารถทำงานได้เต็มที่ เครื่องหมายอัศเจรีย์สีแดงหรือไอคอนการแจ้งเตือนสีส้มจะปรากฏขึ้นหากโมดูลต้องการความสนใจ ข้อมูลเพิ่มเติมเกี่ยวกับโมดูลซึ่งรวมถึงคำแนะนำของเราเกี่ยวกับวิธีการเรียกคืนการทำงานแบบเต็มรูปแบบ จะแสดงอยู่ที่ส่วนบนของหน้าต่าง หากต้องการเปลี่ยนสถานะของโมดูล ให้คลิก **ตั้งค่า** ในเมนูหลัก จากนั้นคลิกโมดูลที่ต้องการ



ไอคอนเครื่องหมายอัศเจรีย์สีแดง (!) เป็นตัวระบุว่าไม่มีการใช้การป้องกันสูงสุดของคอมพิวเตอร์ของคุณ คุณอาจได้รับการแจ้งเตือนประเภทนี้ในสถานการณ์ดังต่อไปนี้:

- **การป้องกันไวรัสและสปายแวร์ถูกหยุดชั่วคราว** – คลิก **เริ่มต้นโมดูลการป้องกันไวรัสและสปายแวร์ทั้งหมด** เพื่อเปิดใช้งานการป้องกันไวรัสและสปายแวร์ในช่อง **สถานะการป้องกัน** อีกครั้ง หรือ **เปิดใช้งานการป้องกันไวรัสและสปายแวร์** ในช่อง **การตั้งค่า** ในหน้าต่างหลักของโปรแกรม
- การป้องกันไวรัสไม่ทำงาน – การเริ่มต้นเครื่องมือสแกนไวรัสล้มเหลว โมดูล ESET Endpoint Security ส่วนใหญ่จะทำงานไม่ถูกต้อง
- **การป้องกันการฟิชชิ่งไม่ทำงาน** – คุณลักษณะนี้ไม่ทำงานเนื่องจากโมดูลโปรแกรมอื่นๆ ที่จำเป็นไม่ได้เปิดใช้งานอยู่
- **ไฟร์วอลล์ของถูกปิดใช้งาน** – ปัญหานี้จะแสดงเป็นการไอคอนสีแดงและการแจ้งเตือนความปลอดภัยที่อยู่ถัดจากรายการ **เครือข่าย** คลิก **เปิดใช้งานโหมดการกรอง** เพื่อเปิดใช้งานการป้องกันเครือข่ายอีกครั้ง
- **การเริ่มต้นไฟร์วอลล์ล้มเหลว** – ไฟร์วอลล์ถูกปิดใช้งานเนื่องจากปัญหาการรวมระบบ เริ่มต้นระบบคอมพิวเตอร์ของคุณใหม่ให้เร็วที่สุดเท่าที่ทำได้
- **กลไกตรวจหาไม่อัพเดท** – ข้อผิดพลาดนี้จะปรากฏขึ้นหลังจากความพยายามในการอัพเดทกลไกการตรวจจับ (ก่อนหน้านี้คือฐานข้อมูลไวรัส) ล้มเหลวหลายครั้ง ขอแนะนำให้คุณตรวจสอบการตั้งค่าการอัพเดท สาเหตุทั่วไปสำหรับข้อผิดพลาดนี้คือข้อมูลการตรวจสอบสิทธิ์ที่ป้อนไม่ถูกต้องหรือ การตั้งค่าการเชื่อมต่อ ที่กำหนด

ค่าไม่ถูกต้อง

- **ผลิตภัณฑ์ไม่ได้เปิดใช้งาน**หรือ**ใบอนุญาตของคุณหมดอายุแล้ว**– สิ่งนี้จะระบุโดยไอคอนสถานะการป้องกันเป็นสีแดง โปรแกรมจะไม่สามารถอัพเดทได้หลังจากใบอนุญาตของคุณหมดอายุ ปฏิบัติตามคำแนะนำต่อไปนี้ในหน้าต่างการเตือนเพื่อต่ออายุใบอนุญาต
- **ระบบป้องกันการบุกรุกโฮสต์ (HIPS) ถูกปิดใช้งาน** – ปัญหานี้จะแสดงเมื่อ HIPS ถูกปิดใช้งาน คอมพิวเตอร์ของคุณไม่ได้รับการป้องกันจากภัยคุกคามบางชนิดและควรเปิดใช้งานการป้องกันอีกครั้งในทันทีโดยคลิก **เปิดใช้งาน HIPS**
- **ไม่มีการอัพเดทประจำที่กำหนดไว้** – ESET Endpoint Security จะไม่ตรวจหาหรือรับรายการอัพเดทที่สำคัญ เว้นแต่ว่าคุณจะได้วางกำหนดการงานอัพเดทเอาไว้
- **การเข้าถึงเครือข่ายถูกปิดกั้น** – แสดงขึ้นเมื่องาน **แยกคอมพิวเตอร์ออกจากเครือข่าย** ของไคลเอนต์ในเวิร์กสเตชันจาก ESET PROTECT ถูกเรียกใช้ โปรดติดต่อผู้ดูแลระบบของคุณสำหรับข้อมูลเพิ่มเติม
- **การป้องกันระบบไฟล์แบบเรียลไทม์ถูกหยุดชั่วคราว** – การป้องกันระบบไฟล์แบบเรียลไทม์ถูกปิดใช้งานโดยผู้ใช้ คอมพิวเตอร์ของคุณไม่ได้รับการป้องกันจากภัยคุกคาม คลิก เปิดใช้งานการป้องกันแบบเรียลไทม์เพื่อเปิดใช้งานการทำงานนี้อีกครั้ง

ตัวอักษร "i" สีส้มแสดงว่าผลิตภัณฑ์ ESET ของคุณต้องการการดำเนินการสำหรับปัญหาที่ไม่ร้ายแรง สาเหตุที่เป็นไปได้คือ:

- **การป้องกันการเข้าถึงเว็บถูกปิดใช้งาน** – คลิกที่การแจ้งเตือนความปลอดภัยเพื่อเปิดใช้งานการป้องกันการเข้าถึงเว็บอีกครั้ง จากนั้นคลิก **เปิดใช้งานการป้องกันการเข้าถึงเว็บ**
- **ใบอนุญาตของคุณใกล้หมดอายุแล้ว/ใบอนุญาตของคุณจะหมดอายุในวันนี้** – คุณจะทราบปัญหานี้ได้จากไอคอนสถานะการป้องกันซึ่งจะแสดงเครื่องหมายอัศเจรีย์ หลังจากใบอนุญาตหมดอายุ โปรแกรมจะไม่สามารถอัพเดทและไอคอนสถานะการป้องกันจะเปลี่ยนเป็นสีแดง
- **การป้องกันบอตเน็ตถูกหยุดชั่วคราว** – คลิก **เปิดใช้งานการป้องกันบอตเน็ต** เพื่อเปิดใช้งานคุณลักษณะนี้อีกครั้ง
- **การป้องกันการโจมตีเครือข่าย (IDS) ถูกหยุดชั่วคราว** – คลิก **เปิดใช้งานการป้องกันการโจมตีเครือข่าย (IDS)** เพื่อเปิดใช้งานคุณลักษณะนี้อีกครั้ง
- **การป้องกันสแปมอีเมลไคลเอ็นต์ถูกหยุดไว้ชั่วคราว** คลิก **เปิดใช้งานการป้องกันสแปมอีเมลไคลเอ็นต์** เพื่อเปิดใช้งานฟีเจอร์นี้อีกครั้ง
- **การควบคุมการเข้าถึงเว็บไซต์ถูกหยุดชั่วคราว** – คลิก **เปิดใช้งานการควบคุมการเข้าถึงเว็บไซต์ เพื่อเปิดใช้งานคุณลักษณะนี้อีกครั้ง**
- **การเขียนทับนโยบายใช้งานได้** – การกำหนดค่าที่ตั้งค่าโดยนโยบายจะถูกเขียนทับชั่วคราวจนกว่าการ

แก้ไขปัญหาจะเสร็จสมบูรณ์ เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเขียนทับการตั้งค่าของนโยบายได้ สำหรับข้อมูลเพิ่มเติม โปรดดู วิธีการใช้โหมดเขียนทับ

- **การควบคุมอุปกรณ์ถูกหยุดชั่วคราว** – คลิก **เปิดใช้งานการควบคุมอุปกรณ์** เพื่อเปิดใช้งานคุณลักษณะนี้อีกครั้ง

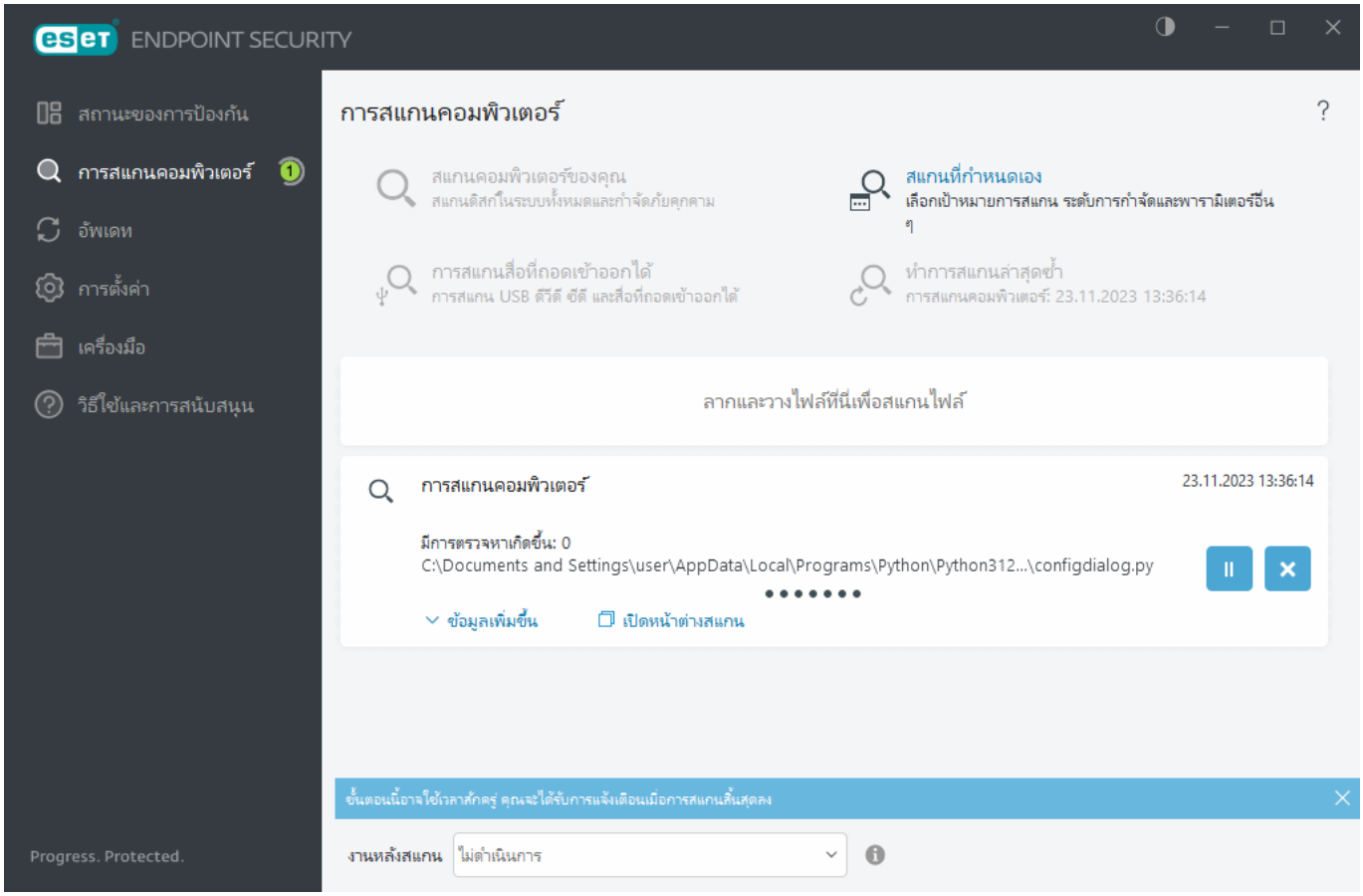
หากต้องการปรับสถานะการมองเห็นภายในผลิตภัณฑ์ในบานหน้าต่างแรกของ ESET Endpoint Security โปรดดู สถานะแอพพลิเคชัน

หากคุณไม่สามารถแก้ไขปัญหาโดยใช้วิธีแก้ไขที่แนะนำได้ ให้คลิก **วิธีใช้และการสนับสนุน** เพื่อเข้าถึงไฟล์วิธีใช้ หรือค้นหา ฐานความรู้ ESET หากคุณยังคงต้องการความช่วยเหลือ คุณสามารถส่งคำร้องถึงฝ่ายสนับสนุนทางเทคนิคของ ESET ได้ ฝ่ายสนับสนุนทางเทคนิคของ ESET จะตอบคำถามของคุณอย่างรวดเร็วและค้นหาการแก้ไขปัญหา

หากสถานะเป็นของคุณลักษณะที่ถูกปิดกั้นโดยนโยบาย ESET PROTECT ลิงก์จะไม่สามารถคลิกได้

การสแกนคอมพิวเตอร์

เครื่องมือสแกนตามต้องการเป็นส่วนสำคัญของ ESET Endpoint Security ซึ่งใช้เพื่อสแกนไฟล์และโฟลเดอร์ในคอมพิวเตอร์ของคุณ เมื่อพิจารณาถึงความปลอดภัย การสแกนคอมพิวเตอร์ไม่ใช่สิ่งที่จะดำเนินการต่อเมื่อสงสัยว่ามีการติดไวรัส แต่ต้องสแกนสม่ำเสมอเป็นส่วนหนึ่งของมาตรการรักษาความปลอดภัย เราขอแนะนำให้คุณสแกนข้อมูลของระบบโดยละเอียดเป็นประจำ (ตัวอย่างเช่น เดือนละครั้ง) เพื่อตรวจหาไวรัส ซึ่งไม่พบโดย การป้องกันระบบไฟล์แบบเรียลไทม์ กรณีนี้สามารถเกิดขึ้นได้ถ้าการป้องกันระบบไฟล์แบบเรียลไทม์ถูกปิดใช้งานในขณะนี้ ถ้ากลไกตรวจหาเก่าเกินไป หรือไฟล์ไม่ถูกตรวจพบว่าเป็นไวรัสเมื่อบันทึกลงในดิสก์



มี **การสแกนคอมพิวเตอร์** สองประเภท **สแกนคอมพิวเตอร์ของคุณ** จะสแกนระบบอย่างรวดเร็ว โดยไม่ต้องมีการกำหนดค่าพารามิเตอร์การสแกนเพิ่มเติม **การสแกนที่กำหนดเอง** ช่วยให้คุณสามารถเลือกโปรไฟล์ใดๆ ที่สแกนไว้ก่อนหน้าและระบุการสแกนได้อย่างเจาะจง

โปรดดู ความคืบหน้าของการสแกน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับกระบวนการสแกน

สแกนคอมพิวเตอร์

การสแกนคอมพิวเตอร์ของคุณ จะช่วยให้คุณเริ่มต้นการสแกนคอมพิวเตอร์และทำความสะอาดไฟล์ที่ติดไวรัสได้อย่างรวดเร็วโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ข้อดีของ **การสแกนคอมพิวเตอร์** คือสามารถใช้งานได้ง่ายและไม่ต้องมีการกำหนดค่าการสแกนอย่างละเอียด การสแกนคอมพิวเตอร์ของคุณจะตรวจสอบทุกไฟล์ในไดรฟ์ในระบบ รวมทั้งทำความสะอาดหรือลบการแฝงตัวที่ตรวจพบโดยอัตโนมัติ โปรแกรมจะตั้งค่าระดับการทำความสะอาดเป็นค่าเริ่มต้นโดยอัตโนมัติ สำหรับข้อมูลโดยละเอียดเพิ่มเติมเกี่ยวกับประเภทการทำความสะอาด โปรดดูที่ ทำความสะอาด

คุณยังสามารถใช้คุณลักษณะ **การสแกนแบบลากและวาง** เพื่อสแกนไฟล์หรือโฟลเดอร์ด้วยตัวเองได้อีกด้วย โดยให้คลิกที่ไฟล์หรือโฟลเดอร์ แล้วเลื่อนตัวชี้เม้าส์ไปยังบริเวณที่ทำเครื่องหมายขณะที่กดปุ่มเม้าส์ค้างไว้ จากนั้นจึงปล่อยนิ้ว หลังจากนั้น แอพพลิเคชันจะเลื่อนมาที่เบื้องหน้า

ตัวเลือกในการสแกนต่อไปนี้มีให้ใช้ที่ใต้ **การสแกนขั้นสูง**:

การสแกนที่กำหนดเอง

การสแกนแบบกำหนดเอง ช่วยให้คุณสามารถระบุพารามิเตอร์การสแกน เช่น เป้าหมายและวิธีของการสแกน ข้อดีของ**การสแกนที่กำหนดเอง**คือคุณสามารถกำหนดค่าพารามิเตอร์โดยละเอียดได้ คุณสามารถบันทึกการกำหนดค่าไว้ไปยังโปรไฟล์การสแกนที่ผู้ใช้กำหนด ซึ่งจะเป็นประโยชน์ถ้ามีการสแกนซ้ำกับพารามิเตอร์เดียวกัน

การสแกนสื่อที่ถอดเข้าออกได้

คล้ายกับ **การสแกนคอมพิวเตอร์ของคุณ** – เริ่มต้นการสแกนสื่อที่ถอดเข้าออกได้ (เช่น CD/DVD/USB) ที่เชื่อมต่ออยู่กับคอมพิวเตอร์ในขณะนี้อย่างรวดเร็ว การทำงานนี้อาจมีประโยชน์เมื่อคุณเชื่อมต่ออุปกรณ์ USB กับคอมพิวเตอร์และต้องการสแกนเนื้อหาเพื่อหามัลแวร์และสิ่งที่อาจเป็นภัยคุกคามอื่นๆ

การสแกนประเภทนี้สามารถเริ่มต้นทำงานด้วยการคลิก **การสแกนแบบกำหนดเอง** เลือก **การควบคุมอุปกรณ์** จากเมนูแบบเลื่อนลง **เป้าหมายการสแกน** แล้วคลิก **สแกน**

ทำซ้ำการสแกนครั้งล่าสุด

อนุญาตให้คุณเริ่มต้นการสแกนที่ทำล่าสุดโดยใช้การตั้งค่าเดียวกับที่สแกนครั้งที่แล้ว

เมนูแบบเลื่อนลง **การทำงานหลังสแกน** ทำให้คุณสามารถตั้งค่าการทำงานที่จะดำเนินการโดยอัตโนมัติหลังจากการสแกนเสร็จสิ้นได้:

- **ไม่มีการทำงาน** – หลังจากสแกนเสร็จสิ้น จะไม่มีการดำเนินการใดๆ
- **ปิดระบบ** – คอมพิวเตอร์จะปิดหลังจากสแกนเสร็จสิ้น
- **รีสตาร์ทหากจำเป็น** – คอมพิวเตอร์จะรีสตาร์ทก็ต่อเมื่อจำเป็นเพื่อกำจัดภัยคุกคามที่ตรวจพบเท่านั้น
- **เริ่มต้นระบบใหม่** – ปิดโปรแกรมที่เปิดอยู่ทั้งหมด แล้วเริ่มต้นคอมพิวเตอร์ใหม่หลังจากสแกนเสร็จสิ้น
- **บังคับให้รีสตาร์ทเครื่องหากจำเป็น** – ระบบจะบังคับให้คอมพิวเตอร์รีสตาร์ทก็ต่อเมื่อจำเป็นเพื่อกำจัดภัยคุกคามที่ตรวจพบเท่านั้น
- **บังคับให้รีบูต** – บังคับให้ปิดโปรแกรมที่เปิดอยู่ทั้งหมดโดยไม่ต้องรอการโต้ตอบของผู้ใช้และรีสตาร์ทคอมพิวเตอร์หลังจากการสแกนเสร็จสิ้น
- **พักเครื่อง** – บันทึกเซสชันของคุณและปรับคอมพิวเตอร์เข้าสู่สถานะการใช้พลังงานต่ำเพื่อให้คุณสามารถกลับมาทำงานต่อได้อย่างรวดเร็ว

- **ไฮเบอร์เนต** – รวบรวมทุกสิ่งที่คุณได้เรียกใช้บน RAM แล้วย้ายมาไว้ในไฟล์พิเศษบนฮาร์ดไดรฟ์ของคุณ คอมพิวเตอร์ของคุณจะปิด แต่จะกลับมายังสถานะก่อนหน้านี้ในครั้งต่อไปที่คุณเริ่มคอมพิวเตอร์อีกครั้ง

> การดำเนินการ **พักการทำงาน** หรือ **ไฮเบอร์เนต** จะใช้งานได้ตามการตั้งค่าระบบปฏิบัติการสำหรับการเปิดเครื่องและพักการทำงานของคอมพิวเตอร์หรือความสามารถของคอมพิวเตอร์/แล็ปท็อปของคุณ โปรดทราบว่าคอมพิวเตอร์ขณะพักการทำงานยังคงเป็นคอมพิวเตอร์ที่ทำงานอยู่ คอมพิวเตอร์ยังทำงานพื้นฐานและใช้ไฟฟ้าเมื่อคอมพิวเตอร์ทำงานด้วยแบตเตอรี่ หากต้องการยืดอายุการใช้งานแบตเตอรี่ ตัวอย่างเช่น เมื่ออยู่นอกสำนักงาน เราขอแนะนำให้คุณใช้ตัวเลือกไฮเบอร์เนต

การดำเนินการที่เลือกจะเริ่มต้นหลังจากการสแกนที่ทำงานอยู่ทั้งหมดสิ้นสุดแล้ว เมื่อคุณเลือก **ปิดเครื่อง** หรือ **เริ่มต้นระบบใหม่** หน้าต่างข้อความยืนยันจะแสดงการนับถอยหลัง 30 วินาที (คลิก **ยกเลิก** เพื่อปิดใช้งานการทำงานที่ร้องขอ)

> เราขอแนะนำให้คุณเรียกใช้การสแกนคอมพิวเตอร์อย่างน้อยเดือนละหนึ่งครั้ง การสแกนสามารถกำหนดค่าเป็นงานตามกำหนดการได้จาก **เครื่องมือ** > **เครื่องมือวางกำหนดการ** ฉันสามารถกำหนดเวลาการสแกนคอมพิวเตอร์รายสัปดาห์ได่อย่างไร

เครื่องมือเริ่มต้นการสแกนที่กำหนดเอง

คุณสามารถใช้ Custom Scan เพื่อสแกนหน่วยความจำที่ใช้งาน เครือข่าย หรือส่วนใดส่วนหนึ่งของดิสก์แทนการสแกนทั้งดิสก์ เมื่อต้องการเลือกจุดที่จะสแกน ให้คลิก **การสแกนขั้นสูง** > **การสแกนแบบกำหนดเอง** และเลือกเป้าหมายที่ต้องการจากโครงสร้างโฟลเดอร์

คุณสามารถเลือกโปรไฟล์จากเมนูแบบเลื่อนลง **โปรไฟล์** ที่จะใช้งานเมื่อสแกนเป้าหมายใดเป้าหมายหนึ่งเป็นการเฉพาะ โปรไฟล์ตามค่าเริ่มต้นคือ **การสแกนแบบสมาร์ท** และยังมีโปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าอีกสามรายการ ได้แก่ **การสแกนเชิงลึก** **การสแกนเมนูบริบท** และ **การสแกนคอมพิวเตอร์** โปรไฟล์ของการสแกนเหล่านี้ใช้ พารามิเตอร์ ThreatSense ที่แตกต่างกัน ตัวเลือกที่มีอยู่นี้จะอธิบายใน การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การสแกนมัลแวร์** > **การสแกนตามต้องการ** > ThreatSense

โครงสร้างโฟลเดอร์ (แบบต้นไม้) ยังมีเป้าหมายการสแกนที่เฉพาะเจาะจงอีกด้วย

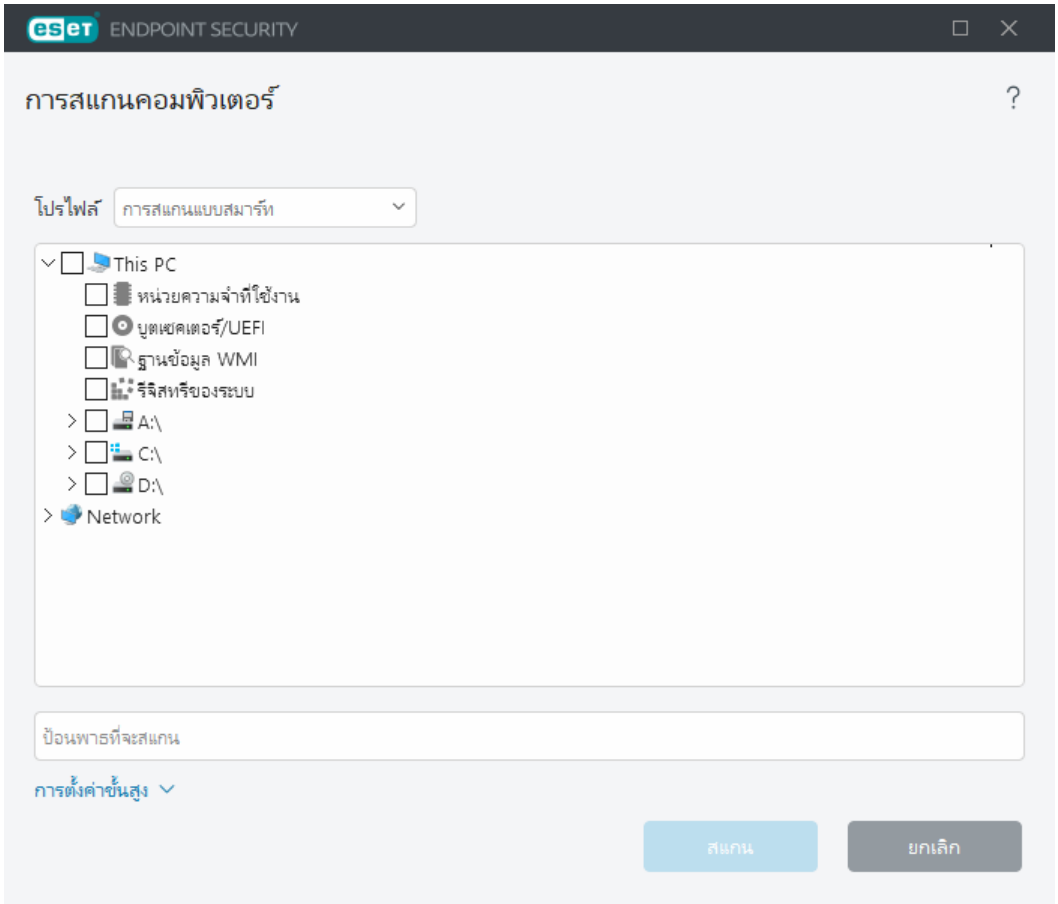
- **หน่วยความจำที่ใช้งาน** – สแกนกระบวนการและข้อมูลทั้งหมดที่ใช้อยู่ในปัจจุบันโดยหน่วยความจำที่ใช้งาน
- **ส่วนการบูต/UEFI** – สแกนส่วนการบูตและ UEFI สำหรับมัลแวร์ที่มี อ่านเพิ่มเติมเกี่ยวกับเครื่องมือสแกน UEFI ได้ใน ประมวลศัพท์
- **ฐานข้อมูล WMI** – สแกนทั้งฐานข้อมูล Windows Management Instrumentation (WMI), เนมสเปซทั้งหมด, ตัวอย่างทุกระดับ และรวมถึงคุณสมบัติทั้งหมด การค้นหาสำหรับการอ้างอิงสำหรับไฟล์ที่ติดไวรัสหรือ

มัลแวร์ที่ฝังเป็นข้อมูล

- **รีจิสทรีของระบบ** – สแกนทั้งรีจิสทรีของระบบ, คีย์และคีย์ย่อยทั้งหมด การค้นหาสำหรับการอ้างอิงสำหรับไฟล์ที่ติดไวรัสหรือมัลแวร์ที่ฝังเป็นข้อมูล เมื่อทำความสะอาดการตรวจหา การอ้างอิงจะยังคงอยู่ในรีจิสทรีเพื่อให้แน่ใจว่าจะไม่มีข้อมูลที่สำคัญสูญหาย

หากต้องการไปยังเป้าหมายการสแกน (ไฟล์หรือโฟลเดอร์) อย่างรวดเร็ว ให้พิมพ์พาธของเป้าหมายดังกล่าวลงในช่องข้อความใต้ลำดับโครงสร้าง พาธต้องตรงตามตัวพิมพ์เล็กและใหญ่ โปรดเลือกกล่องกาเครื่องหมายในลำดับโครงสร้างหากต้องการให้ระบบสแกนเป้าหมายด้วย

> **วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์**
> หากต้องการกำหนดตารางงานทั่วไป ให้อ่าน วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์



คุณสามารถกำหนดค่าพารามิเตอร์การกำจัดไวรัสสำหรับการสแกนใน การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การสแกนมัลแวร์** > **การสแกนตามต้องการ** > **ThreatSense** > **การกำจัด** เมื่อต้องการเรียกใช้การสแกนโดยไม่ทำความสะอาด ให้คลิก **การตั้งค่าขั้นสูง** แล้วเลือก **สแกนโดยไม่ต้องทำความสะอาด** ประวัติการสแกนจะถูกบันทึกลงในบันทึกการสแกน

เมื่อเลือก **ละเว้นการยกเว้น** ไฟล์ที่มีนามสกุลไฟล์ที่ไม่ได้รับการสแกนก่อนหน้านี้จะถูกสแกนโดยไม่มีข้อยกเว้น

คลิก **สแกน** เพื่อเรียกใช้การสแกนโดยใช้พารามิเตอร์ที่กำหนดเองที่คุณตั้งค่าไว้

สแกนในฐานะผู้ดูแลระบบ อนุญาตให้คุณเรียกใช้การสแกนภายใต้บัญชีของผู้ดูแลระบบ ใช้ตัวเลือกนี้หากผู้ใช้ปัจจุบันไม่มีสิทธิ์ในการเข้าถึงไฟล์ที่คุณต้องการสแกน ปุ่มนี้จะไม่มีให้ใช้ได้หากผู้ใช้ปัจจุบันไม่สามารถเรียกการทำงาน UAC ในฐานะผู้ดูแลระบบได้

คุณสามารถดูบันทึกการสแกนคอมพิวเตอร์เมื่อสแกนเสร็จแล้วได้ด้วยการคลิกที่ แสดงบันทึก

ความคืบหน้าของการสแกน

หน้าต่างความคืบหน้าของการสแกนจะแสดงสถานะปัจจุบันของการสแกนและข้อมูลเกี่ยวกับจำนวนไฟล์ที่พบว่ามีรหัสที่เป็นอันตราย

เป็นเรื่องปกติที่โปรแกรมไม่สามารถสแกนบางไฟล์ได้ เช่น ไฟล์ที่ป้องกันด้วยรหัสผ่านหรือไฟล์ที่ระบบใช้งานโดยเฉพาะ (โดยทั่วไปคือ *pagefile.sys* และไฟล์บันทึก) ดูรายละเอียดเพิ่มเติมได้จาก บทความฐานความรู้ของเรา

วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์
หากต้องการกำหนดตารางงานทั่วไป ให้อ่าน วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์

ความคืบหน้าของการสแกน – แถบความคืบหน้าจะแสดงสถานะของการสแกนที่กำลังทำงานอยู่

เป้าหมาย – ชื่อของวัตถุที่สแกนและตำแหน่งของวัตถุในปัจจุบัน

การตรวจหาเกิดขึ้น - แสดงจำนวนทั้งหมดของไฟล์ที่สแกน ภัยคุกคามที่พบ และภัยคุกคามที่กำจัดระหว่างการสแกน

คลิก "ข้อมูลเพิ่มเติม" เพื่อแสดงข้อมูลต่อไปนี้:

- **ผู้ใช้** – ชื่อของบัญชีผู้ใช้ที่เริ่มการสแกน
- **วัตถุที่สแกน** – จำนวนของวัตถุที่สแกนแล้ว
- **ระยะเวลา** – เวลาที่ผ่านไป

ไอคอนหยุดชั่วคราว – หยุดการสแกนชั่วคราว

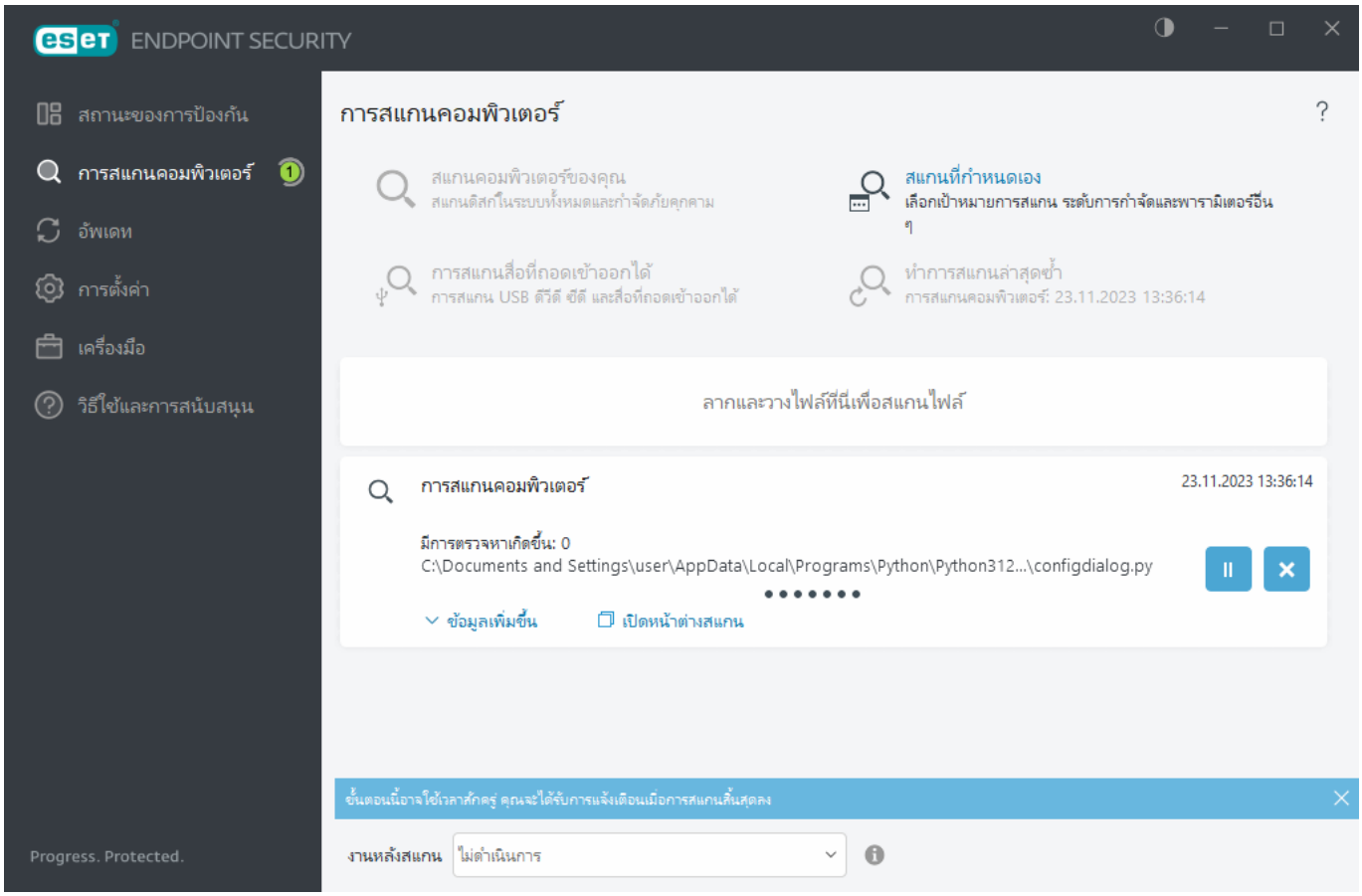
ไอคอนทำงานต่อ – ตัวเลือกนี้จะปรากฏเมื่อหยุดการสแกนไว้ชั่วคราว คลิกที่ไอคอนเพื่อทำการสแกนต่อไป

ไอคอนหยุด – สิ้นสุดการสแกน

คลิก **เปิดหน้าต่างการสแกน** เพื่อเปิด บันทึกการสแกนคอมพิวเตอร์ พร้อมรายละเอียดเพิ่มเติมเกี่ยวกับการสแกน

เลื่อนบันทึกการสแกน – ถ้าเปิดใช้งานตัวเลือกนี้ บันทึกการสแกนจะเลื่อนลงโดยอัตโนมัติเมื่อมีการเพิ่มรายการใหม่เพื่อให้รายการล่าสุดปรากฏขึ้น

> คลิกแว่นขยายหรือลูกศรเพื่อแสดงรายละเอียดเกี่ยวกับการสแกนที่กำลังทำงานอยู่ คุณสามารถเรียกใช้การสแกนอื่นที่คล้ายกันได้โดยคลิก **สแกนคอมพิวเตอร์ของคุณ** หรือ **สแกนขั้นสูง** > **สแกนแบบกำหนดเอง**



เมนูแบบเลื่อนลง **การทำงานหลังสแกน** ทำให้คุณสามารถตั้งค่าการทำงานที่จะดำเนินการโดยอัตโนมัติหลังจากการสแกนเสร็จสิ้นได้:

- **ไม่มีการทำงาน** – หลังจากสแกนเสร็จสิ้น จะไม่มีการดำเนินการใดๆ
- **ปิดระบบ** – คอมพิวเตอร์จะปิดหลังจากสแกนเสร็จสิ้น
- **รีสตาร์ทหากจำเป็น** – คอมพิวเตอร์จะรีสตาร์ทก็ต่อเมื่อจำเป็นเพื่อกำจัดภัยคุกคามที่ตรวจพบเท่านั้น
- **เริ่มต้นระบบใหม่** – ปิดโปรแกรมที่เปิดอยู่ทั้งหมด แล้วเริ่มต้นคอมพิวเตอร์ใหม่หลังจากสแกนเสร็จสิ้น
- **บังคับให้รีสตาร์ทเครื่องหากจำเป็น** – ระบบจะบังคับให้คอมพิวเตอร์รีสตาร์ทก็ต่อเมื่อจำเป็นเพื่อกำจัดภัยคุกคามที่ตรวจพบเท่านั้น
- **บังคับให้รีบูต** – บังคับให้ปิดโปรแกรมที่เปิดอยู่ทั้งหมดโดยไม่ต้องรอการโต้ตอบของผู้ใช้และรีสตาร์ทคอมพิวเตอร์หลังจากการสแกนเสร็จสิ้น

- **พักเครื่อง** – บันทึกเซสชันของคุณและปรับคอมพิวเตอร์เข้าสู่สถานะการใช้พลังงานต่ำเพื่อให้คุณสามารถกลับมาทำงานต่อได้อย่างรวดเร็ว
- **ไฮเบอร์เนต** – รวบรวมทุกสิ่งที่คุณได้เรียกใช้บน RAM แล้วย้ายมาไว้ในไฟล์พิเศษบนฮาร์ดไดรฟ์ของคุณ คอมพิวเตอร์ของคุณจะปิด แต่จะกลับมายังสถานะก่อนหน้านี้ในครั้งต่อไปที่คุณเริ่มคอมพิวเตอร์อีกครั้ง

> การดำเนินการ **พักการทำงาน** หรือ **ไฮเบอร์เนต** จะใช้งานได้ตามการตั้งค่าระบบปฏิบัติการสำหรับการเปิดเครื่องและพักการทำงานของคอมพิวเตอร์หรือความสามารถของคอมพิวเตอร์/แล็ปท็อปของคุณ โปรดทราบว่าคอมพิวเตอร์ขณะพักการทำงานยังคงเป็นคอมพิวเตอร์ที่ทำงานอยู่ คอมพิวเตอร์ยังทำงานพื้นฐานและใช้ไฟฟ้าเมื่อคอมพิวเตอร์ทำงานด้วยแบตเตอรี่ หากต้องการยืดอายุการใช้งานแบตเตอรี่ ตัวอย่างเช่น เมื่ออยู่นอกสำนักงาน เราขอแนะนำให้คุณใช้ตัวเลือกไฮเบอร์เนต

การดำเนินการที่เลือกจะเริ่มต้นหลังจากการสแกนที่ทำงานอยู่ทั้งหมดสิ้นสุดแล้ว เมื่อคุณเลือก **ปิดเครื่อง** หรือ **เริ่มต้นระบบใหม่** หน้าต่างข้อความยืนยันจะแสดงการนับถอยหลัง 30 วินาที (คลิก **ยกเลิก** เพื่อปิดใช้งานการทำงานที่ร้องขอ)

บันทึกการสแกนคอมพิวเตอร์

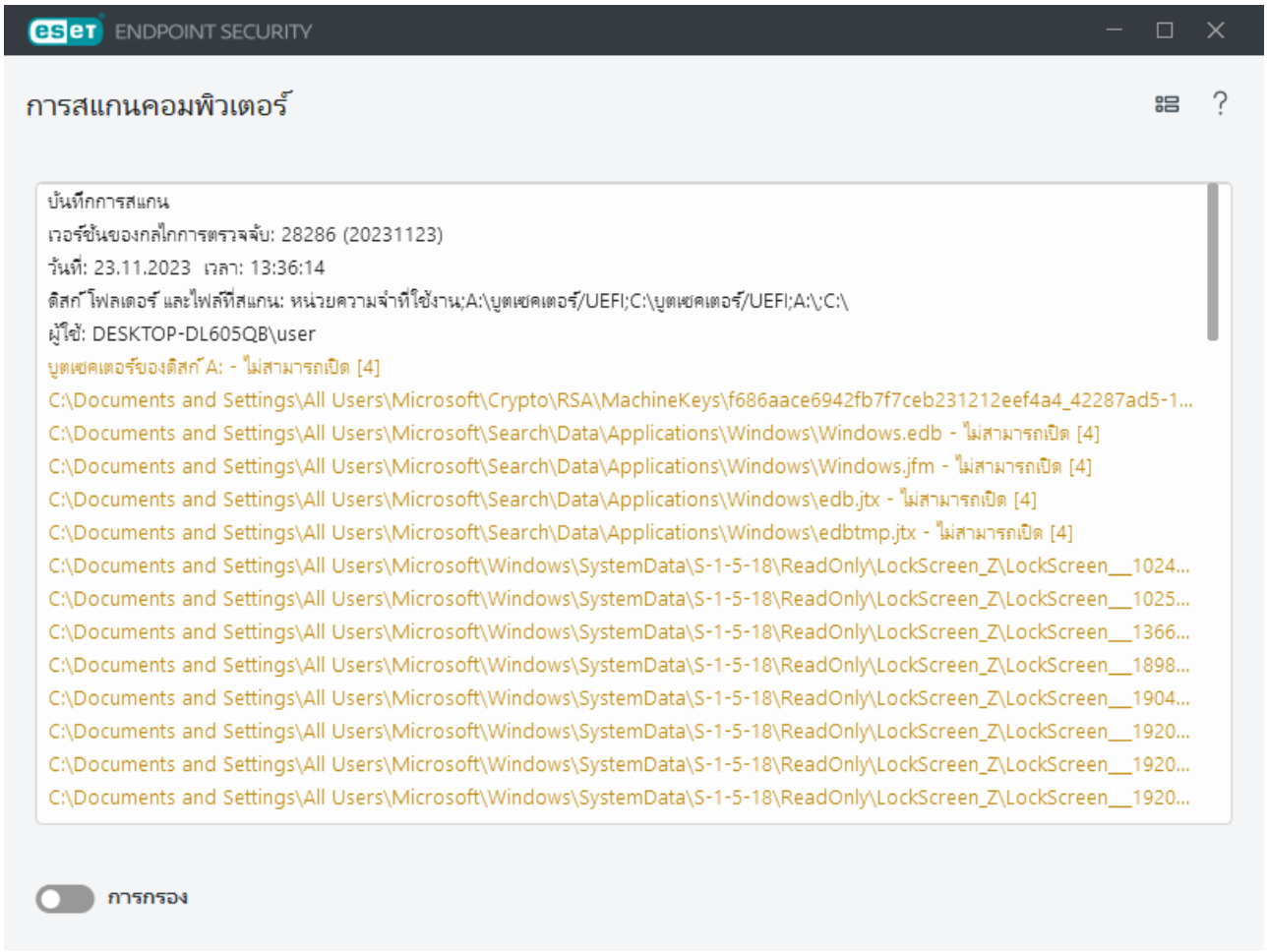
คุณสามารถดูข้อมูลโดยละเอียดที่เกี่ยวข้องกับการสแกนที่ต้องการได้ใน ไฟล์บันทึก บันทึกการสแกนประกอบด้วยข้อมูลต่อไปนี้:

- เวอร์ชันของกลไกตรวจหา:
- วันที่และเวลาที่เริ่ม
- รายการของดิสก์ โฟลเดอร์ และไฟล์ที่สแกน
- ชื่อการสแกนตามกำหนดการ (การสแกนตามกำหนดการเท่านั้น)
- ผู้ใช้ที่เริ่มการสแกน
- สถานะการสแกน
- จำนวนวัตถุที่สแกน
- จำนวนการตรวจหาที่พบ
- เวลาที่ดำเนินการเสร็จ
- เวลาสแกนทั้งหมด

> หากงานตามกำหนดการเดียวกันที่ถูกดำเนินการก่อนยังคงทำงานอยู่ การเริ่มต้นงานสแกนคอมพิวเตอร์ตามกำหนดการใหม่จะถูกข้าม งานสแกนตามกำหนดการที่ถูกข้ามไปจะสร้างบันทึกการสแกนคอมพิวเตอร์ที่มีวัตถุที่ถูกสแกน 0 รายการ พร้อมสถานะ **การสแกนไม่เริ่มต้นเนื่องจากการสแกนก่อนหน้านี้ยังคงทำงานอยู่**

ในการค้นหาบันทึกการสแกนก่อนหน้า ในหน้าต่างโปรแกรมหลัก ให้เลือก **เครื่องมือ** > **ไฟล์บันทึก** ในเมนูแบบ

เลื่อนลง ให้เลือก **การสแกนคอมพิวเตอร์** แล้วคลิกสองครั้งที่การบันทึกที่ต้องการ



หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับบันทึก "ไม่สามารถเปิดได้" "พบข้อผิดพลาดเมื่อเปิด" และ/หรือ "อาร์ไคฟ์เสียหาย" โปรดดู บทความฐานความรู้ ESET ของเรา

คลิกที่ไอคอนแถบเลื่อน **การกรอง** เพื่อเปิดหน้าต่าง การกรองบันทึก ซึ่งคุณสามารถกำหนดการค้นหาที่แคบลงโดยใช้เกณฑ์ที่กำหนดเองได้ หากต้องการดูเมนูบริบท ให้คลิกขวาที่รายการบันทึกนั้นๆ:

การทำงาน	การใช้งาน
กรองบันทึกเดียวกัน	เปิดใช้งานการกรองบันทึก บันทึกจะแสดงเฉพาะการบันทึกประเภทเดียวกันกับที่เลือกไว้
กรอง	ตัวเลือกนี้จะเปิดหน้าต่างการกรองบันทึกและช่วยให้คุณระบุเกณฑ์การกรองสำหรับรายการบันทึกที่ระบุ คำสั่งลัด: `Ctrl+Shift+F`
เปิดใช้งานตัวกรอง	เปิดใช้งานการตั้งค่าการกรอง หากคุณเปิดใช้งานการกรองเป็นครั้งแรก คุณต้องกำหนดการตั้งค่า และหน้าต่างการกรองบันทึกจะเปิดขึ้น
ปิดใช้งานตัวกรอง	ปิดการกรอง (เหมือนกับการคลิกสวิตช์ที่ด้านล่าง)
คัดลอก	คัดลอกการบันทึกที่ไฮไลท์ไว้ลงในคลิปบอร์ด คำสั่งลัด: `Ctrl+C`
คัดลอกทั้งหมด	คัดลอกการบันทึกทั้งหมดไปยังหน้าต่าง
ส่งออก	ส่งการบันทึกที่ไฮไลท์ไว้ลงในคลิปบอร์ดออกไปยังไฟล์ XML
ส่งออกทั้งหมด	ตัวเลือกนี้จะส่งการบันทึกทั้งหมดออกไปยังไฟล์ XML
คำอธิบายการตรวจหา	เปิดสารานุกรมภัยคุกคามของ ESET ซึ่งมีข้อมูลโดยละเอียดเกี่ยวกับอันตรายและอาการของการแฝงตัวที่ทำไฮไลต์ไว้

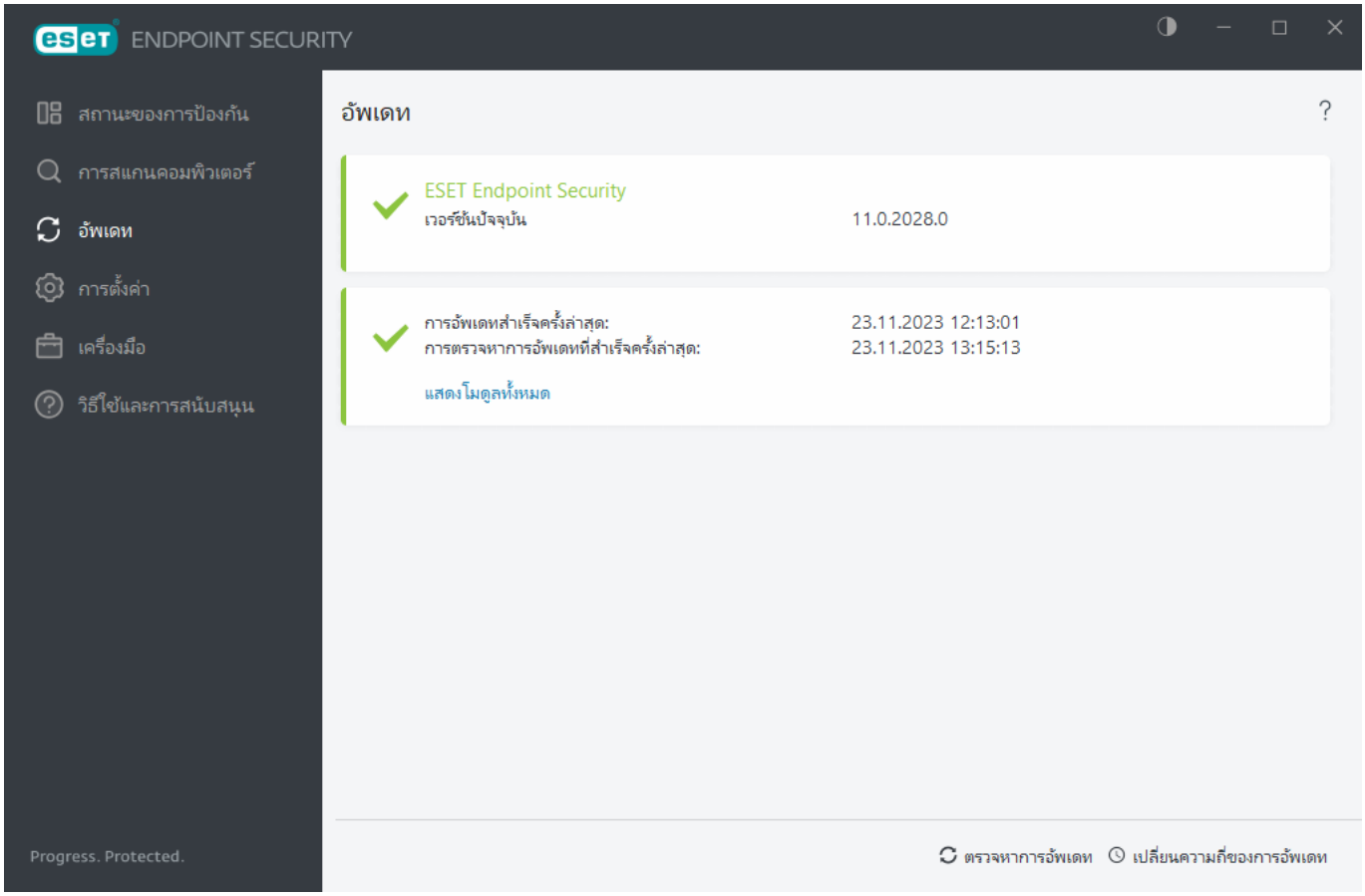
อัพเดท

การอัพเดท ESET Endpoint Security เป็นประจำเป็นวิธีการที่ดีที่สุดเพื่อให้มั่นใจว่าคอมพิวเตอร์มีระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัพเดทจะช่วยให้มั่นใจได้ว่าทั้งโมดูลโปรแกรมและส่วนประกอบของระบบจะอัพเดทอยู่เสมอ

เมื่อคลิก **อัพเดท** ในหน้าต่างโปรแกรมหลัก คุณสามารถดูสถานะการอัพเดทในปัจจุบัน รวมถึงวันที่และเวลาของการอัพเดทที่สำเร็จครั้งล่าสุด และดูว่าจะต้องมีการอัพเดทหรือไม่ได้

นอกเหนือจากการอัพเดทอัตโนมัติแล้ว คุณยังสามารถคลิก **ตรวจหาการอัพเดท** เพื่อเรียกใช้การอัพเดทด้วยตนเองได้ การอัพเดทโมดูลและส่วนประกอบของโปรแกรมอย่างสม่ำเสมอเป็นสิ่งที่สำคัญในการรักษาการปกป้องอย่างแบบเต็มรูปแบบจากรหัสที่เป็นอันตราย โปรดให้ความสนใจในการกำหนดค่าและการทำงานของโปรแกรม คุณต้องเปิดใช้งานผลิตภัณฑ์ของคุณโดยใช้รหัสใบอนุญาตเพื่อรับการอัพเดท หากคุณไม่ได้อัพเดทในระหว่างการติดตั้ง คุณจะต้อง เปิดใช้งาน ESET Endpoint Security เพื่อเข้าถึงเซิร์ฟเวอร์อัพเดทของ ESET รหัสใบอนุญาตจะถูกส่งเป็นอีเมลจาก ESET ไปหาคุณหลังทำการซื้อ ESET Endpoint Security

หากคุณเปิดใช้งาน ESET Endpoint Security ด้วยไฟล์ใบอนุญาตแบบออฟไลน์ โดยไม่มีชื่อผู้ใช้และรหัสผ่าน แล้วลองอัพเดท ข้อมูลที่เป็นสีแดง **การอัพเดทโมดูลล้มเหลว**จะบ่งบอกว่าคุณสามารถดาวน์โหลดมิเรอร์การอัพเดทเท่านั้น



เวอร์ชันปัจจุบัน – หมายเลขติดตั้งรุ่น ESET Endpoint Security

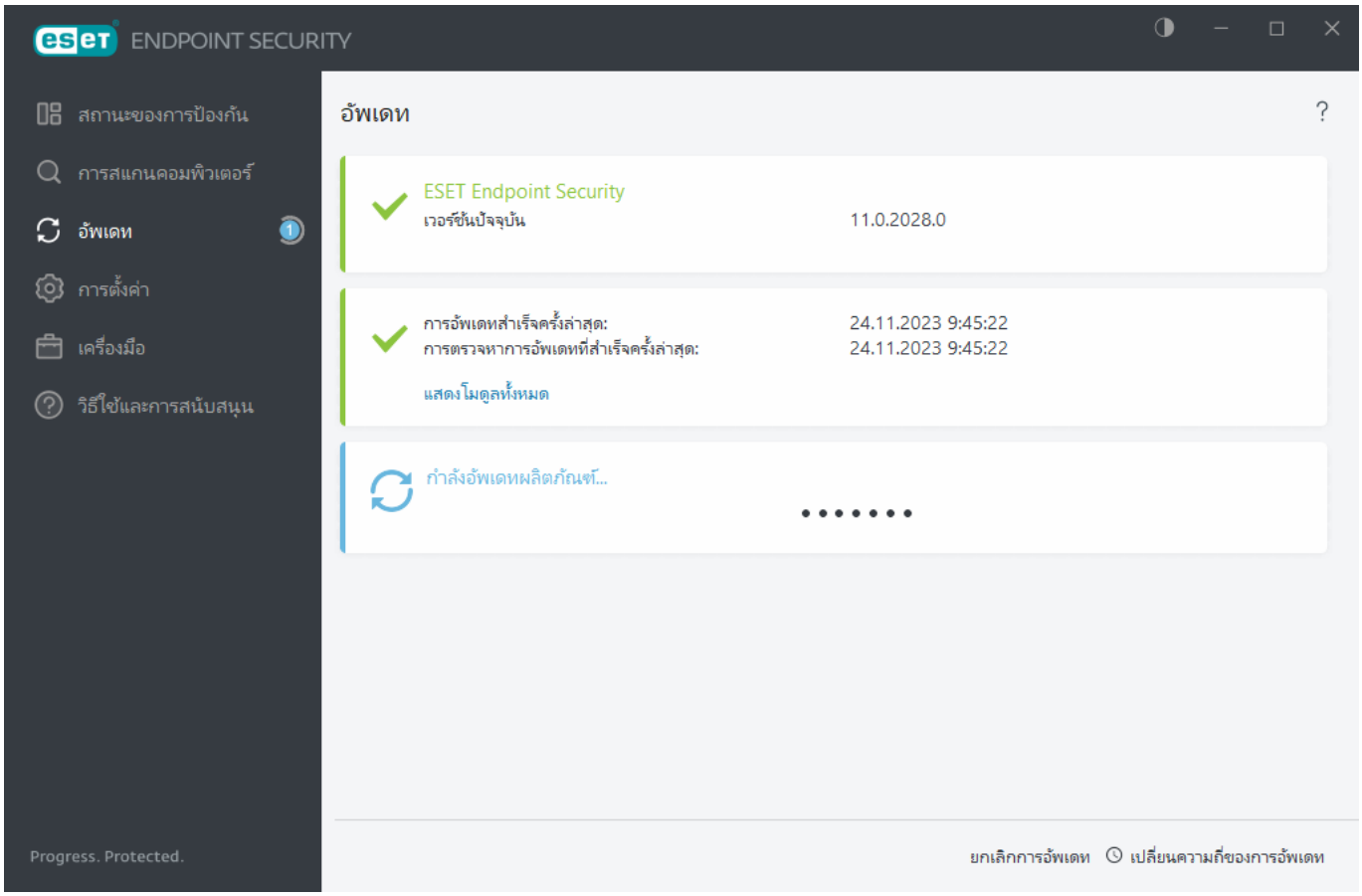
การอัพเดทสำเร็จครั้งล่าสุด – วันที่และเวลาที่อัพเดทที่สำเร็จล่าสุด ให้อ้างถึงวันที่ล่าสุด ซึ่งหมายถึงกลไกตรวจหาเป็นข้อมูลปัจจุบัน

ตรวจหาการอัพเดทสำเร็จครั้งล่าสุด – วันที่และเวลาที่พยายามอัพเดทโมดูลครั้งล่าสุด

แสดงโมดูลทั้งหมด – คลิกที่ลิงก์เพื่อเปิดรายการโมดูลที่ติดตั้งแล้วและตรวจสอบเวอร์ชันและการอัพเดทล่าสุดของโมดูล

กระบวนการอัพเดท

หลังจากคลิก **ตรวจสอบการอัพเดท** กระบวนการการดาวน์โหลดจะเริ่มต้นทำงาน แถบแสดงความคืบหน้าการดาวน์โหลดและเวลาที่เหลือสำหรับการดาวน์โหลดจะปรากฏขึ้น เมื่อต้องการขัดจังหวะการอัพเดท ให้คลิก **ยกเลิกการอัพเดท**



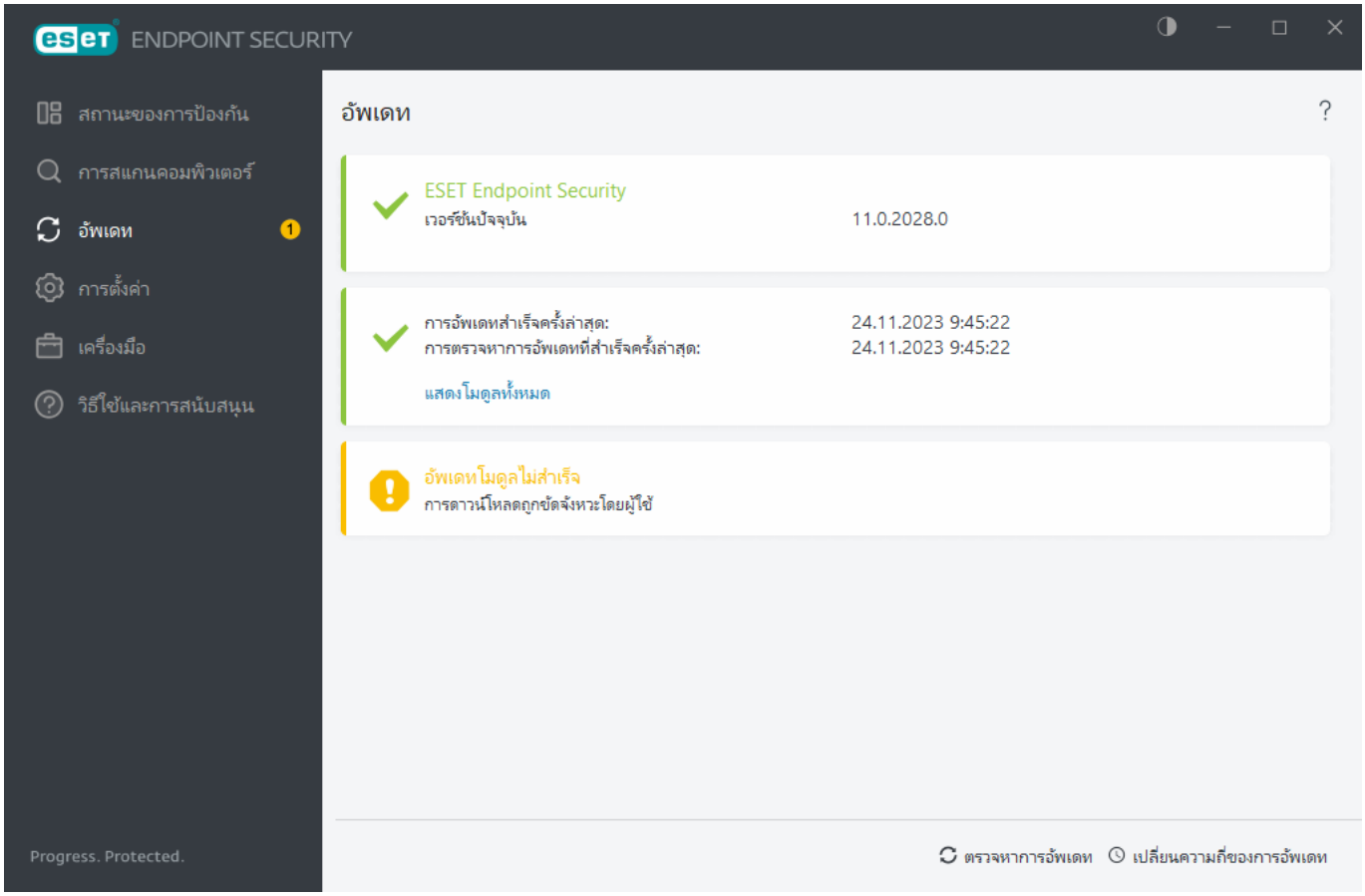
ในสถานการณ์ปกติ คุณจะเห็นเครื่องหมายถูกสีเขียวในหน้าต่าง **อัพเดท** ที่ระบุว่าโปรแกรมนั้นอัพเดทแล้ว หากไม่มีเครื่องหมายถูกสีเขียว แสดงว่าโปรแกรมไม่ได้อัพเดท และมีความเสี่ยงมากขึ้นในการติดไวรัส โปรดอัพเดทโมดูลเร็วที่สุดเท่าที่ทำได้

การอัพเดทที่ไม่สำเร็จ

กลไกตรวจหาไม่อัพเดท – ข้อผิดพลาดจะปรากฏขึ้นหลังจากการพยายามอัพเดทโมดูลที่ล้มเหลวหลายครั้ง ขอแนะนำให้คุณตรวจสอบการตั้งค่าการอัพเดท สาเหตุทั่วไปสำหรับข้อผิดพลาดนี้คือข้อมูลการตรวจสอบสิทธิ์ที่ป้อนไม่ถูกต้องหรือ การตั้งค่าการเชื่อมต่อ ที่กำหนดค่าไม่ถูกต้อง

การแจ้งเตือนก่อนหน้านี้จะเกี่ยวข้องกับข้อความ **การอัพเดทโมดูลล้มเหลว** เกี่ยวกับการอัพเดทล้มเหลวสองข้อความต่อไปนี้:

1. **ใบอนุญาตไม่ถูกต้อง** – ใบอนุญาตของคุณไม่ได้เปิดใช้งาน เราขอแนะนำให้คุณตรวจสอบข้อมูลการตรวจสอบสิทธิ์ คลิก **วิธีใช้และการสนับสนุน** > **เปลี่ยนใบอนุญาต** จากเมนูหลักเพื่อป้อนรหัสใบอนุญาตใหม่
2. **เกิดข้อผิดพลาดระหว่างดาวน์โหลดไฟล์การอัพเดท** – สาเหตุที่เป็นไปได้ของข้อผิดพลาดคือการตั้งค่าการเชื่อมต่ออินเทอร์เน็ตไม่ถูกต้อง เราขอแนะนำให้คุณตรวจสอบการเชื่อมต่ออินเทอร์เน็ตของคุณ (ด้วยการเปิดเว็บไซต์ในเว็บเบราว์เซอร์ของคุณ) ถ้าเว็บไซต์ไม่เปิด เป็นไปได้มากว่าไม่มีการเริ่มต้นการเชื่อมต่ออินเทอร์เน็ตหรือมีปัญหาในการเชื่อมต่อกับคอมพิวเตอร์ของคุณ ตรวจสอบให้แน่ใจว่าคุณมีการเชื่อมต่ออินเทอร์เน็ตที่ใช้ได้จากผู้ให้บริการอินเทอร์เน็ต (ISP) ของคุณ



สำหรับข้อมูลเพิ่มเติม โปรดดู บทความฐานความรู้ของ ESET

วิธีสร้างงานการอัพเดท

คุณสามารถเรียกการอัพเดทได้ด้วยตนเองโดยคลิก **ตรวจสอบการอัพเดท** ในหน้าต่างหลักที่ปรากฏหลังจากคลิก **อัพเดท** จากเมนูหลัก

การอัพเดทยังสามารถเรียกใช้งานเป็นงานตามกำหนดการ หากต้องการการกำหนดค่างานตามกำหนดการ ให้คลิก **เครื่องมือ** > **เครื่องมือวางกำหนดการณ์** ตามค่าเริ่มต้น งานการอัพเดทต่อไปนี้จะมีการเปิดใช้งานใน ESET Endpoint Security:

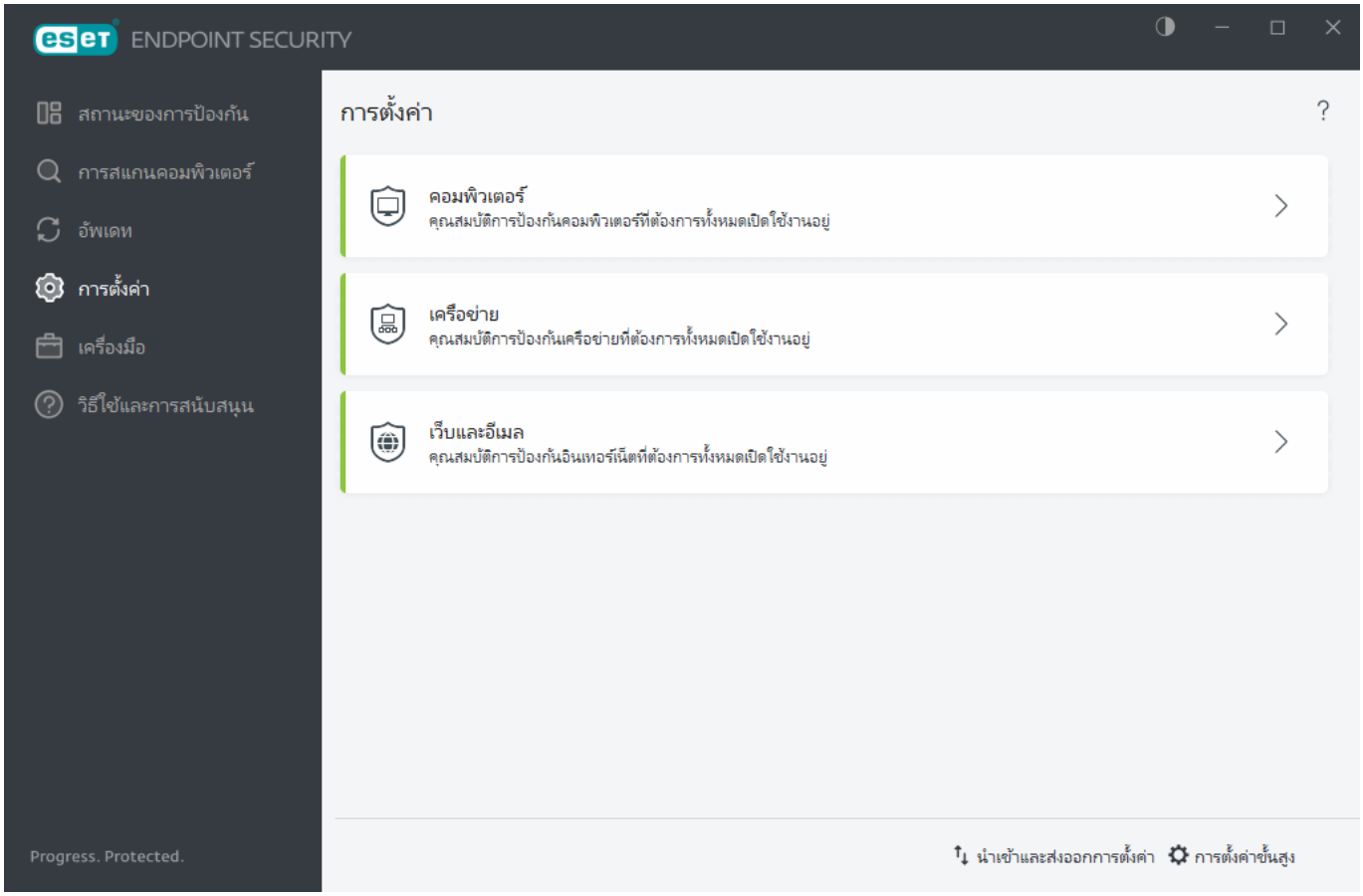
- **การอัพเดทอัตโนมัติเป็นประจำ**
- **การอัพเดทอัตโนมัติหลังจากผู้ใช้เข้าสู่ระบบ**

งานการอัพเดทแต่ละงานจะสามารถแก้ไขได้เพื่อให้เหมาะกับความต้องการของคุณ นอกเหนือจากงานการอัพเดทเริ่มต้นแล้ว คุณสามารถสร้างงานการอัพเดทใหม่ด้วยการกำหนดค่าที่ผู้ใช้กำหนดได้ สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการสร้างและการกำหนดค่างานการอัพเดท โปรดดูที่ เครื่องมือวางกำหนดการ

การตั้งค่า

คุณสามารถค้นหากลุ่มของฟีเจอร์การป้องกันที่พร้อมใช้งาน ใน หน้าต่างโปรแกรมหลัก > **การตั้งค่า**

เมื่อสร้างนโยบายจากเว็บคอนโซล ESET PROTECT คุณจะสามารถเลือกธงของการตั้งค่าแต่ละรายการได้ การตั้งค่าที่มีธงบังคับจะมีลำดับความสำคัญและไม่สามารถเขียนทับโดยนโยบายที่ใหม่กว่าได้ (แม้ว่านโยบายที่ใหม่กว่าจะมีธงบังคับ) สิ่งนี้ช่วยให้มั่นใจได้ว่าการตั้งค่านี้จะไม่ถูกเปลี่ยนแปลง (โดยผู้ใช้หรือโดยนโยบายที่ใหม่กว่าในระหว่างที่รวมข้อมูล เป็นต้น) สำหรับข้อมูลเพิ่มเติม โปรดดู ธง ในวิธีใช้ออนไลน์ของ ESET PROTECT



เมนู **ตั้งค่า** ประกอบด้วยส่วนต่อไปนี้:

คอมพิวเตอร์

เครือข่าย

เว็บและอีเมล

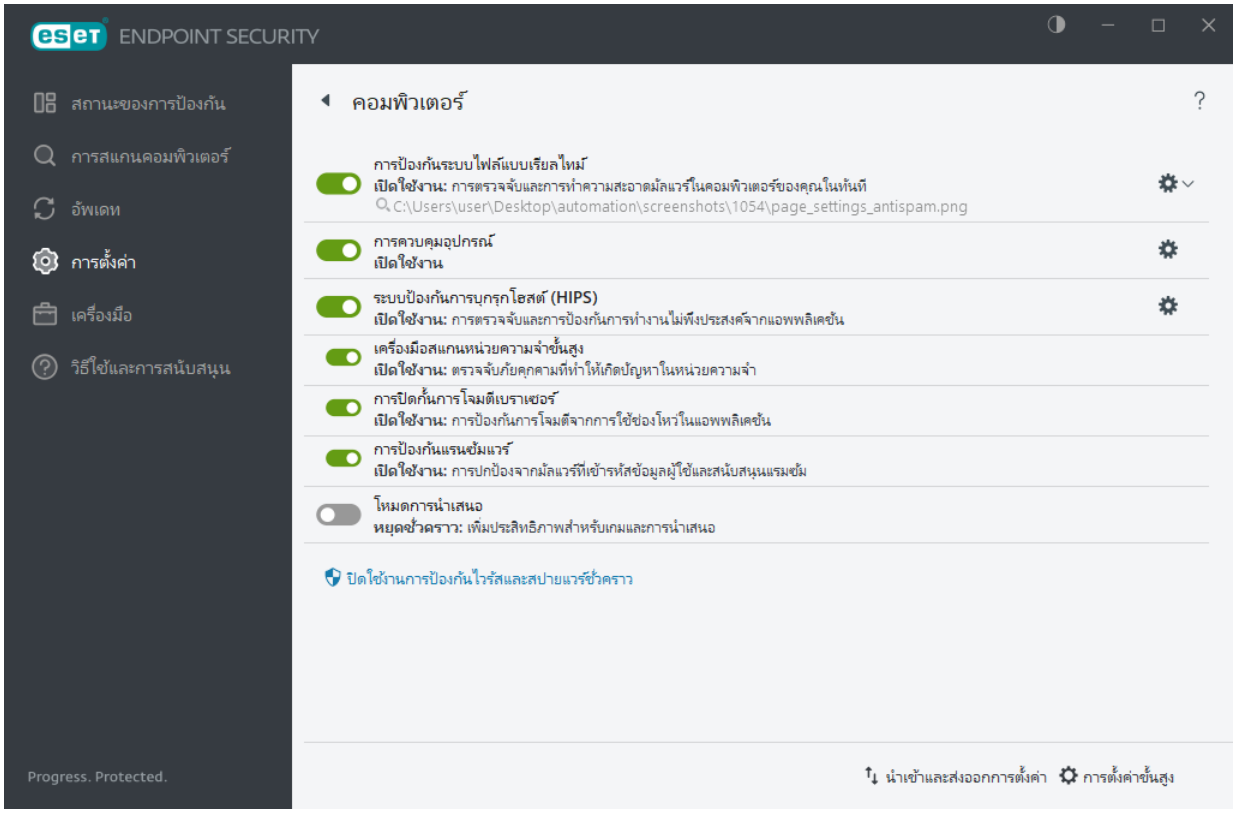
เมื่อมีการใช้นโยบาย ESET PROTECT คุณจะเห็นไอคอนแม่กุญแจ อยู่ถัดจากส่วนประกอบเฉพาะ นโยบายที่ใช้โดย ESET PROTECT สามารถเขียนทับได้ในระบบหลังจากตรวจสอบสิทธิ์ผู้ใช้ที่เข้าสู่ระบบ (เช่น ผู้ดูแล เป็นต้น) สำหรับข้อมูลเพิ่มเติม โปรดดู วิธีใช้ออนไลน์ของ ESET PROTECT

มาตรการการปกป้องที่ปิดใช้งานด้วยวิธีนี้ทั้งหมดจะกลับมาเปิดใช้งานอีกครั้งหลังเริ่มต้นระบบคอมพิวเตอร์ใหม่

ตัวเลือกเพิ่มเติมมีให้ใช้ได้ที่ด้านล่างของหน้าต่างการตั้งค่า ใช้ลิงก์ การตั้งค่าขั้นสูง เพื่อตั้งค่าพารามิเตอร์ที่มีรายละเอียดมากขึ้นสำหรับแต่ละโมดูล ใช้ การตั้งค่านำเข้า/ส่งออก เพื่อโหลดพารามิเตอร์การตั้งค่าโดยใช้ไฟล์การกำหนดค่า .xml หรือเพื่อบันทึกพารามิเตอร์การตั้งค่าปัจจุบันของคุณลงในไฟล์การกำหนดค่า

คอมพิวเตอร์

คลิก **คอมพิวเตอร์** ใน หน้าต่างหลักของโปรแกรม > **การตั้งค่า** เพื่อดูภาพรวมของโมดูลการป้องกันทั้งหมด:



ในส่วน **คอมพิวเตอร์** คุณสามารถเปิดหรือปิดใช้งานองค์ประกอบต่อไปนี้ได้:

- การป้องกันระบบไฟล์แบบเรียลไทม์ – โปรแกรมจะสแกนไฟล์ทั้งหมดเพื่อหารหัสที่เป็นอันตรายเมื่อเปิด สร้าง หรือเรียกใช้ไฟล์ในคอมพิวเตอร์ของคุณ คลิกที่ไอคอนฟันเฟือง ⚙ ถัดจากการป้องกันระบบไฟล์แบบเรียลไทม์ และคลิกแก้ไขการยกเว้น เพื่อเปิด หน้าต่างการตั้งค่าการยกเว้น ซึ่งช่วยให้คุณสามารถยกเว้นการสแกนไฟล์และโฟลเดอร์ได้ หากต้องการเปิดการตั้งค่าขั้นสูงสำหรับ การป้องกันระบบไฟล์แบบเรียลไทม์ ให้คลิก กำหนดค่า
- การควบคุมอุปกรณ์ – ให้การควบคุมอุปกรณ์ (ซีดี/ดีวีดี/USB/...) อัตโนมัติ โมดูลนี้จะช่วยให้คุณสามารถปิดกั้นหรือปรับตัวกรอง/สิทธิ์ที่ขยาย และกำหนดความสามารถของผู้ใช้ในการเข้าถึงและทำงานกับอุปกรณ์เหล่านี้ได้
- Host Intrusion Prevention System (HIPS) – ระบบ HIPS จะตรวจสอบเหตุการณ์ที่เกิดขึ้นภายในระบบปฏิบัติการและตอบสนองเหตุการณ์ตามชุดของกฎที่กำหนดเอง
- **เครื่องสแกนหน่วยความจำขั้นสูง** ทำงานผสมผสานกับการปิดกั้นการโจมตีเบราเซอร์เพื่อเสริมสร้างการป้องกันมัลแวร์ที่ถูกออกแบบมาเพื่อหลบเลี่ยงการตรวจหาของผลิตภัณฑ์การป้องกันมัลแวร์ด้วยวิธี

obfuscation หรือ วิธีเข้ารหัส เครื่องมือสแกนหน่วยความจำขั้นสูงจะเปิดใช้งานตามค่าเริ่มต้น อ่านข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้ใน ประมวลศัพท์

- **การป้องกันการโจมตีแบบ Exploit** – ได้รับการออกแบบมาเพื่อปกป้องประเภทของแอพพลิเคชันที่มักถูกโจมตี เช่น เว็บเบราว์เซอร์ PDF ผู้อ่าน อีเมลไคลเอ็นต์และองค์ประกอบของ MS Office การป้องกันการโจมตีแบบ Exploit จะเปิดใช้งานเป็นค่าเริ่มต้น อ่านข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้ใน ประมวลศัพท์
- **การป้องกันแรนซั่มแวร์** เป็นระดับการปกป้องอีกชั้นหนึ่งที่ทำงานเป็นส่วนหนึ่งของคุณลักษณะ HIPS คุณจะต้องเปิดใช้งานระบบความเชื่อถือ ESET LiveGrid® เอาไว้จึงจะสามารถใช้งานโล่ห์ป้องกันโปรแกรมเรียกค่าไถ่ได้ อ่านเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้
- โหมดการนำเสนอ – คุณลักษณะสำหรับผู้ใช้ที่ต้องการใช้ซอฟต์แวร์อย่างต่อเนื่อง ไม่ต้องการให้การแจ้งเตือนมารบกวน และต้องการลดการใช้งาน CPU คุณจะได้รับข้อความการเตือน (อาจทำให้เกิดความเสี่ยงด้านความปลอดภัย) และหน้าต่างหลักจะเปลี่ยนเป็นสีส้มหลังจากเปิดใช้งาน โหมดการนำเสนอ

หยุดการป้องกันไวรัสและสปายแวร์ชั่วคราว – เมื่อใดก็ตามที่คุณปิดใช้งานการป้องกันไวรัสและสปายแวร์ชั่วคราว คุณสามารถเลือกช่วงเวลาที่คุณต้องการปิดใช้งานองค์ประกอบที่เลือกได้โดยใช้เมนูแบบเลื่อนลง จากนั้นคลิก **นำไปใช้** เพื่อปิดใช้งานองค์ประกอบความปลอดภัย เมื่อต้องการเปิดใช้งานการป้องกันอีกครั้ง ให้คลิก **เปิดใช้งานการป้องกันไวรัสและสปายแวร์**

หากต้องการหยุดชั่วคราวหรือปิดใช้งานโมดูลการป้องกันแต่ละโมดูล ให้คลิกไอคอนปุ่มสลับ

⚠ การปิดโมดูลการป้องกันอาจลดระดับการป้องกันของคอมพิวเตอร์ของคุณ

ตรวจพบภัยคุกคาม

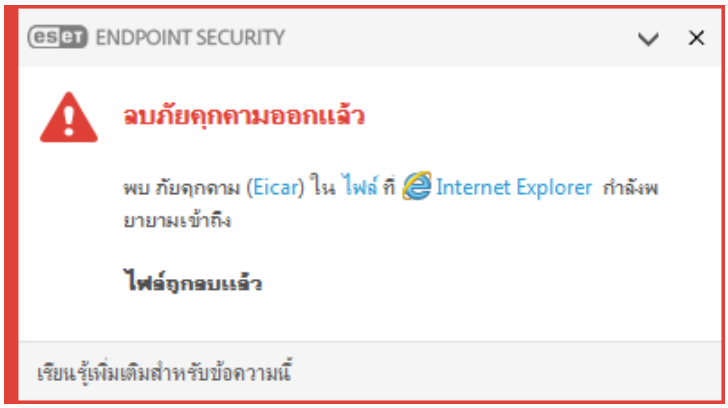
การบุกรุกสามารถเข้าสู่ระบบได้จากจุดเข้าใช้ต่างๆ เช่น หน้าเว็บ โฟลเดอร์ที่ใช้ร่วมกัน ผ่านอีเมล หรือจากอุปกรณ์ที่ถอดเข้าออกได้ (USB, ดิสก์ภายนอก, ซีดี, ดีวีดี เป็นต้น)

พฤติกรรมมาตรฐาน

สำหรับตัวอย่างทั่วไปของวิธีจัดการกับการบุกรุกโดย ESET Endpoint Security ระบบจะตรวจพบการบุกรุกโดยใช้:

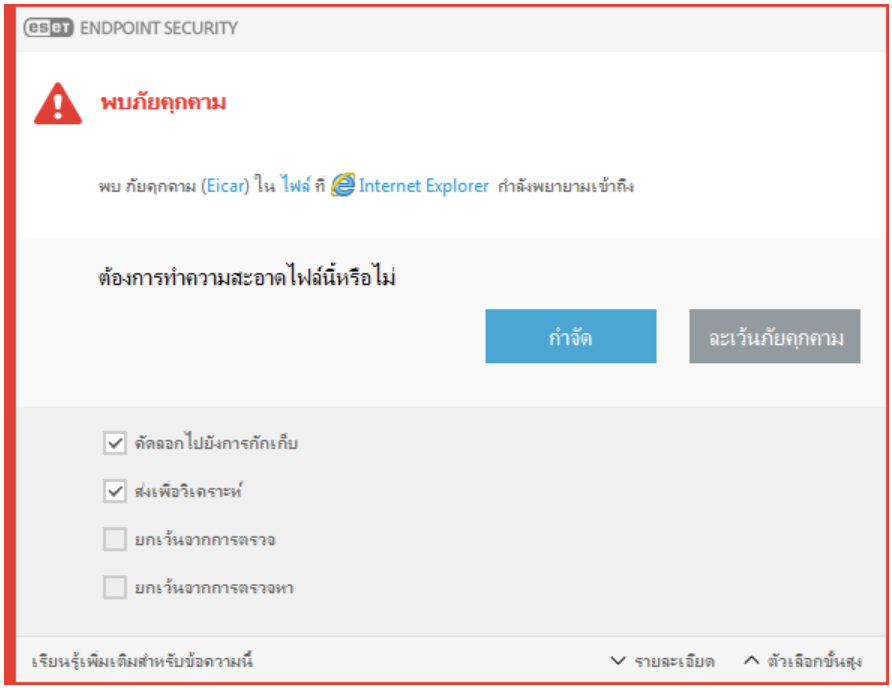
- การป้องกันระบบไฟล์แบบเรียลไทม์
- การป้องกันการเข้าถึงเว็บ
- การป้องกันอีเมลไคลเอ็นต์
- การสแกนคอมพิวเตอร์ตามต้องการ

ในแต่ละรายการจะใช้ระดับการกำจัดมาตรฐาน และจะพยายามกำจัดไฟล์และย้ายไปยัง การกักเก็บ หรือสิ้นสุดการเชื่อมต่อ หน้าต่างการแจ้งเตือนจะปรากฏขึ้นในพื้นที่การแจ้งเตือนในมุมขวาล่างของหน้าจอ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวัตถุที่ถูกตรวจจับ/กำจัด โปรดดูที่ ไฟล์บันทึก สำหรับข้อมูลเพิ่มเติมเกี่ยวกับระดับการกำจัดและพฤติกรรม โปรดดูที่ การกำจัด



การกำจัดและการลบ

หากไม่มีการดำเนินการที่กำหนดไว้ล่วงหน้าสำหรับการป้องกันระบบไฟล์แบบเรียลไทม์ คุณจะได้รับข้อความให้เลือกตัวเลือกในหน้าต่างการเตือน โดยทั่วไปแล้วจะมีตัวเลือก **กำจัด**, **ลบ** และ **ไม่มีการทำงาน** ไม่ขอแนะนำให้เลือก **ไม่มีการทำงาน** เนื่องจากจะเป็นการทิ้งไฟล์ที่ติดไวรัสไว้โดยไม่กำจัด ข้อยกเว้นคือ เมื่อคุณแน่ใจว่าไฟล์ดังกล่าวไม่มีอันตราย และตรวจพบผิดพลาดว่ามีไวรัส



ใช้การกำจัดถ้าไฟล์ถูกโจมตีโดยไวรัส ซึ่งทำให้มีการแนบรหัสที่เป็นอันตรายกับไฟล์นั้น ในกรณีนี้ ขั้นแรกให้พยายามกำจัดไฟล์ที่ติดไวรัส เพื่อคืนกลับสู่สภาวะเดิม ถ้าไฟล์มีเฉพาะรหัสที่เป็นอันตราย ไฟล์ดังกล่าวจะถูกลบ

ถ้าไฟล์ที่ติดไวรัสถูก "ล็อค" หรือมีการใช้งานโดยกระบวนการของระบบ โดยปกติโปรแกรมจะลบไฟล์นี้หลังจากที่ใช้งานแล้ว (โดยทั่วไปมักจะลบหลังจากเริ่มต้นระบบใหม่)

การเรียกคืนจากการกักเก็บ

การกักเก็บนั้นสามารถเข้าถึงได้จาก หน้าต่างโปรแกรมหลัก ของ ESET Endpoint Security โดยการคลิก **เครื่องมือ** > **การกักเก็บ**

นอกจากนี้ไฟล์ที่ถูกกักเก็บยังสามารถเรียกคืนไปยังตำแหน่งดั้งเดิมได้อีกด้วย:

- ใช้คุณสมบัติ **เรียกคืน** สำหรับการดำเนินการดังกล่าว ซึ่งสามารถใช้งานได้จากเมนูบริบทโดยคลิกไฟล์ที่ต้องการในการกักเก็บ
- หากไฟล์ถูกทำเครื่องหมายเป็น แอพพลิเคชันที่อาจไม่พึงประสงค์ ตัวเลือก **เรียกคืนและยกเว้นจากการสแกน** จะเปิดใช้งาน ทั้งนี้โปรดดู การยกเว้น
- นอกจากนี้เมนูบริบทยังมีตัวเลือก **เรียกคืนไปที่** ซึ่งช่วยให้คุณสามารถเรียกคืนไฟล์ไปยังตำแหน่งอื่นนอกเหนือจากตำแหน่งที่ถูกลบได้
- ในบางกรณีจะไม่สามารถใช้งานฟังก์ชันการเรียกคืนได้ ตัวอย่างเช่น ไฟล์ที่ตั้งอยู่ในการแชร์เครือข่ายที่อ่านได้อย่างเดียวเท่านั้น

มีภัยคุกคามหลายรายการ

ถ้าไฟล์ที่ติดไวรัสไม่ได้รับการกำจัดในระหว่างการสแกนคอมพิวเตอร์ (หรือ ระดับการกำจัด ถูกกำหนดเป็น **ไม่มีการกำจัด**) ระบบจะแสดงหน้าต่างการเตือนให้คุณเลือกการทำงานสำหรับไฟล์เหล่านั้น

การลบไฟล์ในอาร์ไคฟ์

ในโหมดการกำจัดเริ่มต้น ระบบจะลบทั้งอาร์ไคฟ์ต่อเมื่อมีไฟล์ที่ติดไวรัส และไม่มีไฟล์ที่ปลอดไวรัสเลย กล่าวอีกนัยหนึ่งก็คือ โปรแกรมจะไม่ลบอาร์ไคฟ์ ถ้ายังมีไฟล์ที่ไม่เป็นอันตรายรวมอยู่ด้วย โปรดใช้ความระมัดระวังเมื่อสแกนการกำจัดอย่างเข้มงวด เมื่อเปิดใช้งานการกำจัดอย่างเข้มงวด โปรแกรมจะลบอาร์ไคฟ์แม้ว่าจะมีไฟล์ที่ติดไวรัสเพียงไฟล์เดียวก็ตาม โดยไม่คำนึงถึงสถานะของไฟล์อื่น ๆ ในอาร์ไคฟ์

ถ้าคอมพิวเตอร์ของคุณแสดงสัญญาณการติดไวรัสจากมัลแวร์ ตัวอย่างเช่น ทำงานช้า ค้างบ่อยๆ เป็นต้น เราขอแนะนำให้คุณดำเนินการดังนี้:

- เปิด ESET Endpoint Security แล้วคลิกสแกนคอมพิวเตอร์

- คลิก **การสแกนแบบสมาร์ท** (สำหรับข้อมูลเพิ่มเติม ดูที่ การสแกนคอมพิวเตอร์)
- หลังจากสแกนเสร็จสิ้นแล้ว ให้ตรวจดูบันทึกสำหรับจำนวนไฟล์ที่สแกน ไฟล์ที่ติดไวรัส และไฟล์ที่ล้าง

หากคุณต้องการสแกนเฉพาะบางส่วนของดิสก์ ให้คลิก **การสแกนที่กำหนดเอง** และเลือกเป้าหมายที่จะสแกนหาไวรัส

เครือข่าย

เปิด หน้าต่างโปรแกรมหลัก > **การตั้งค่า** > **เครือข่าย** เพื่อกำหนดการตั้งค่าการป้องกันเครือข่ายพื้นฐาน หรือแก้ไขปัญหาการสื่อสารในเครือข่าย

หากต้องการหยุดชั่วคราวหรือปิดใช้งานโมดูลการป้องกันแต่ละโมดูล ให้คลิกไอคอนปุ่มสลับ

⚠ การปิดโมดูลการป้องกันอาจลดระดับการป้องกันของคอมพิวเตอร์ของคุณ

คลิกไอคอนฟันเฟือง ⚙ ที่อยู่ถัดจากโมดูลการป้องกันเพื่อเข้าถึงการตั้งค่าขั้นสูง

ไฟร์วอลล์ – กรองการสื่อสารในเครือข่ายทั้งหมดตามการกำหนดค่าของ ESET Endpoint Security

กำหนดค่า – เปิดหน้าต่างไฟร์วอลล์ในการตั้งค่าขั้นสูงซึ่งคุณจะสามารถระบุวิธีที่ไฟร์วอลล์จะจัดการการสื่อสารในเครือข่ายได้

ปิดไฟร์วอลล์ชั่วคราว (อนุญาตการรับส่งทั้งหมด) – ตัวเลือกที่ตรงกันข้ามกับการปิดกั้นการรับส่งของเครือข่ายทั้งหมด หากเลือกตัวเลือกนี้ ตัวเลือกการกรองของไฟร์วอลล์ทั้งหมดจะถูกปิด และระบบจะอนุญาตการเชื่อมต่อขาเข้าและขาออกทั้งหมด คลิก **เปิดใช้งานไฟร์วอลล์** เพื่อ เปิดใช้งานไฟร์วอลล์ใหม่อีกครั้งในขณะที่การกรองการรับส่งข้อมูลผ่านเครือข่ายอยู่ในโหมดนี้

บล็อกการรับส่งข้อมูลทั้งหมด – ไฟร์วอลล์จะบล็อกการสื่อสารขาเข้าและขาออกทั้งหมด ใช้ตัวเลือกนี้เฉพาะเมื่อคุณสงสัยเกี่ยวกับความเสี่ยงด้านความปลอดภัยที่สำคัญ ซึ่งต้องการตัดการเชื่อมต่อระบบจากเครือข่าย ขณะที่การกรองการรับส่งข้อมูลของเครือข่ายอยู่ในโหมด **ปิดกั้นการรับส่งข้อมูลทั้งหมด** ให้คลิก **หยุดปิดกั้นการรับส่งข้อมูลทั้งหมด** เพื่อเรียกคืนการดำเนินการไฟร์วอลล์ปกติ

โหมดอัตโนมัติ – (เมื่อโหมดการกรองอื่นเปิดใช้งานอยู่) – คลิกเพื่อเปลี่ยน โหมดการกรอง เป็นโหมดการกรองอัตโนมัติ (โดยใช้กฎที่ผู้ใช้กำหนด)

โหมดโต้ตอบ – (เมื่อโหมดการกรองอื่นเปิดใช้งานอยู่) – คลิกเพื่อเปลี่ยนโหมดการกรองเป็นโหมดการกรองเชิงโต้ตอบ

การป้องกันการโจมตีเครือข่าย (IDS) – วิเคราะห์เนื้อหาของการรับส่งข้อมูลเครือข่ายและป้องกันจากการโจมตีเครือข่าย การรับส่งข้อมูลที่ประเมินว่าอาจเป็นอันตรายจะถูกบล็อก ESET Endpoint Security แจ้งให้คุณทราบว่าเมื่อเชื่อมต่อเครือข่ายแบบไร้สายที่ไม่ได้รับการป้องกันหรือมีการป้องกันต่ำ

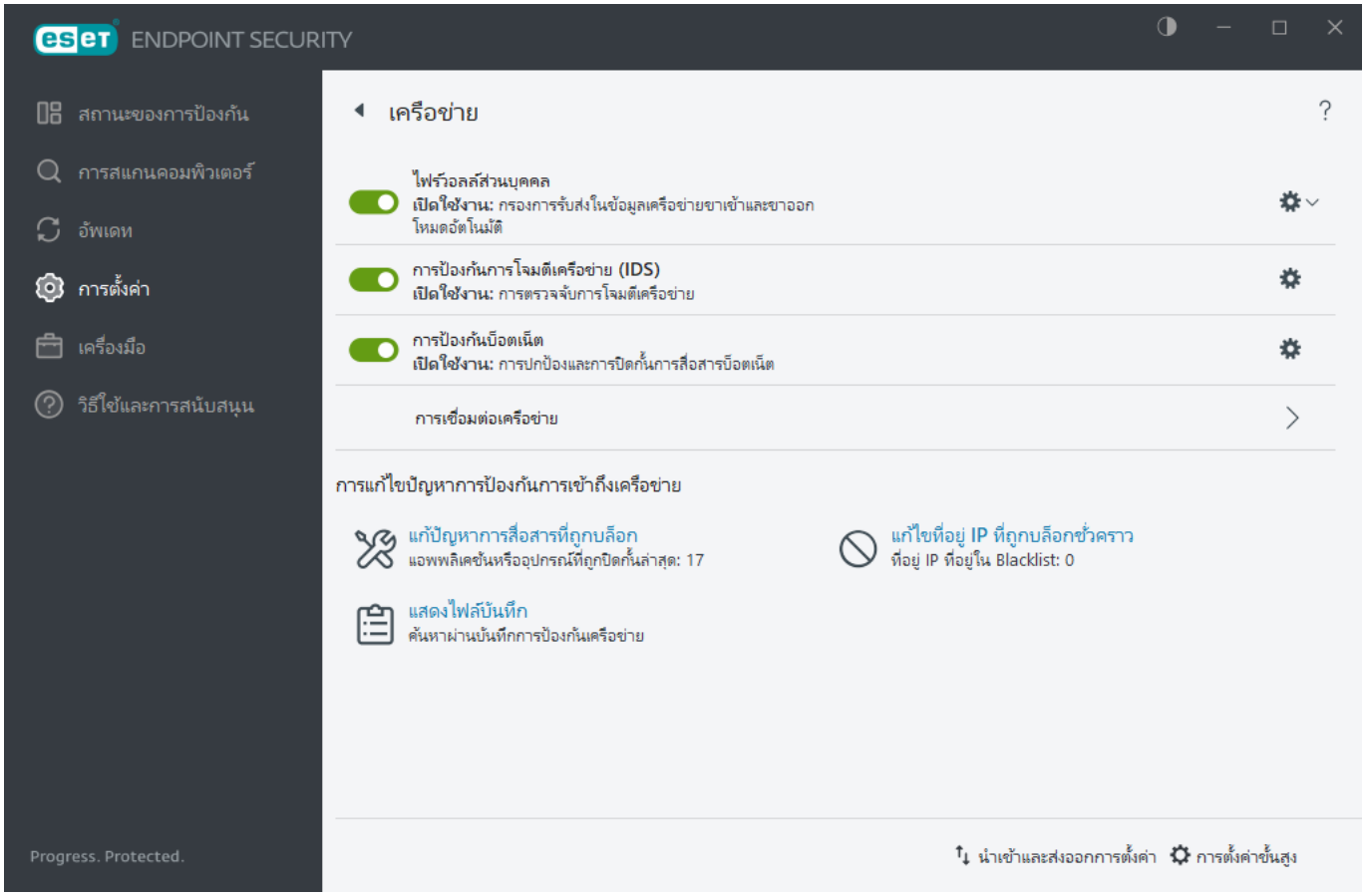
การป้องกันบอทเน็ต – ระบุมัลแวร์ในระบบได้อย่างรวดเร็วและแม่นยำ

การเชื่อมต่อเครือข่าย – แสดงเครือข่ายที่อะแดปเตอร์เครือข่ายเชื่อมต่ออยู่พร้อมข้อมูลโดยละเอียด

แก้ไขการสื่อสารที่ถูกบล็อก – ช่วยให้คุณแก้ไขปัญหาการเชื่อมต่อที่เกิดจากไฟร์วอลล์ของ ESET หากต้องการรายละเอียดเพิ่มเติม โปรดดูที่ วิซาร์ดการแก้ไขปัญหา

แก้ไขที่อยู่ IP ที่ถูกบล็อกชั่วคราว – ดูรายการของ ที่อยู่ IP ที่ถูกตรวจพบว่าเป็นแหล่งที่มาของการโจมตีและเพิ่มลงในบัญชีดำเพื่อปิดกั้นการเชื่อมต่อเป็นระยะเวลาหนึ่ง

แสดงบันทึก – เปิด ไฟล์บันทึก การป้องกันเครือข่าย



การเชื่อมต่อเครือข่าย

แสดงเครือข่ายที่อะแดปเตอร์เครือข่ายเชื่อมต่ออยู่ หากต้องการดูการเชื่อมต่อเครือข่าย ให้เปิด หน้าต่างโปรแกรมหลัก > **การตั้งค่า** > **เครือข่าย** > **การเชื่อมต่อเครือข่าย**

คลิกสองครั้งที่การเชื่อมต่อในรายการเพื่อแสดงรายละเอียดของการเชื่อมต่อและรายละเอียด อะแดปเตอร์เครือข่าย

วางเมาส์เหนือการเชื่อมต่อเครือข่ายที่ต้องการ และคลิกไอคอนเมนู ⋮ ในคอลัมน์ **ที่เชื่อถือได้** เพื่อเลือกตัวเลือกใดตัวเลือกหนึ่งต่อไปนี้

- **แก้ไข** – เปิดหน้าต่าง กำหนดค่าการป้องกันเครือข่าย ซึ่งคุณสามารถกำหนด โปรไฟล์การป้องกันเครือข่าย ให้กับเครือข่านที่ต้องการได้
- **ลืม** – รีเซ็ตการกำหนดค่าการเชื่อมต่อเครือข่ายเป็นค่าเริ่มต้น

รายละเอียดการเชื่อมต่อเครือข่าย

คลิกสองครั้งที่การเชื่อมต่อในรายการ การเชื่อมต่อเครือข่าย เพื่อแสดงรายละเอียดการเชื่อมต่อพร้อมกับรายละเอียดของอะแดปเตอร์เครือข่าย รายละเอียดการเชื่อมต่อเครือข่ายและอะแดปเตอร์ช่วยให้คุณระบุเครือข่ายที่คุณต้องการกำหนดค่าในการ ป้องกันการเข้าถึงเครือข่าย

รายละเอียดการเชื่อมต่อเครือข่าย:

- สถานะของการเชื่อมต่อเครือข่าย
- วันที่และเวลาของการตรวจหาเครือข่ายครั้งแรก
- เวลาที่เครือข่ายใช้งานครั้งล่าสุด
- เวลาทั้งหมดที่ใช้ในการเชื่อมต่อกับเครือข่ายนี้
- โปรไฟล์การเชื่อมต่อเครือข่าย
- โปรไฟล์การเชื่อมต่อเครือข่ายที่กำหนดไว้ใน Windows
- การกำหนดค่าการป้องกันเครือข่าย (กำหนดความน่าเชื่อถือของเครือข่าย)

รายละเอียดของอะแดปเตอร์เครือข่าย:

- ประเภทของการเชื่อมต่อ (แบบมีสาย แบบไร้สาย ฯลฯ)
- ชื่ออะแดปเตอร์เครือข่าย

- คำอธิบายอะแดปเตอร์
- ที่อยู่ IP พร้อมด้วยที่อยู่ MAC
- ที่อยู่ IPv4 และ IPv6 ของเครือข่ายที่มีซับเน็ต
- ส่วนต่อท้าย DNS
- IP เซิร์ฟเวอร์ DNS
- IP เซิร์ฟเวอร์ DHCP
- ที่อยู่ IP และที่อยู่ MAC ของเกตเวย์เริ่มต้น
- ที่อยู่ MAC ของอะแดปเตอร์

การแก้ไขปัญหาการเข้าถึงเครือข่าย

วิซาร์ดการแก้ไขปัญหาจะช่วยคุณแก้ไขปัญหาในการเชื่อมต่อที่เกิดจากไฟร์วอลล์ของ ส่วน **การแก้ไขปัญหาการเข้าถึงเครือข่าย** จะอยู่ใน หน้าต่างโปรแกรมหลัก > **การตั้งค่า** > **เครือข่าย** > **แก้ไขการสื่อสารที่ถูกบล็อก**

เลือกว่าคุณต้องการแสดงการสื่อสารที่ถูกบล็อกสำหรับ **แอพพลิเคชันภายในเครื่อง** หรือบล็อกการสื่อสารจาก **อุปกรณ์ระยะไกล**

จากเมนูแบบเลื่อนลง ให้เลือกระยะเวลาที่ซึ่งการสื่อสารถูกปิดกั้น รายการการสื่อสารที่ถูกปิดกั้นล่าสุดจะให้ภาพรวมเกี่ยวกับชนิดของแอพพลิเคชันหรืออุปกรณ์ ความน่าเชื่อถือและจำนวนของแอพพลิเคชันและอุปกรณ์ที่ถูกปิดกั้นในช่วงเวลาดังกล่าวแก่คุณ สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการสื่อสารที่ปิดกั้น ให้คลิก **รายละเอียด** ขั้นตอนถัดไปคือการยกเลิกการปิดกั้นแอพพลิเคชันหรืออุปกรณ์ที่กำลังประสบปัญหาในการเชื่อมต่อ

เมื่อคุณคลิก **ยกเลิกการปิดกั้น** การสื่อสารที่ถูกปิดกั้นไว้ก่อนหน้าจะได้รับอนุญาต หากคุณยังพบปัญหาเกี่ยวกับแอพพลิเคชัน หรืออุปกรณ์ของคุณไม่ทำงานตามที่คาดไว้ ให้คลิก **สร้างกฎอื่น** และการสื่อสารทั้งหมดที่ถูกบล็อกไว้ก่อนหน้านี้ในอุปกรณ์ดังกล่าวจะได้รับอนุญาต หากปัญหายังคงอยู่ ให้เริ่มต้นระบบคอมพิวเตอร์ของคุณใหม่

คลิก **เปิดกฎของไฟร์วอลล์** เพื่อดูกฎที่สร้างโดยวิซาร์ด นอกจากนี้ คุณสามารถดูกฎที่วิซาร์ดสร้างขึ้นได้ โดยไปที่ การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **ไฟร์วอลล์** > **ขั้นสูง** > **กฎ**

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
- เพิ่มข้อยกเว้นไฟร์วอลล์โดยใช้วิซาร์ดการแก้ไขปัญหา

หากไม่สามารถสร้างกฎได้ คุณจะได้รับข้อความแสดงข้อผิดพลาด คลิก **ลองอีกครั้ง** และทำซ้ำกระบวนการเพื่อยกเลิกการบล็อกการสื่อสาร หรือสร้างกฎอื่นจากรายการการสื่อสารที่ถูกบล็อก

บัญชีดำของที่อยู่ IP แบบชั่วคราว

หากต้องการดูที่อยู่ IP ที่ถูกตรวจพบว่าเป็นแหล่งที่มาของการโจมตีจะถูกเพิ่มเข้าไปยังบัญชีดำเพื่อบล็อกการเชื่อมต่อเป็นระยะเวลาหนึ่ง ให้เปิด หน้าต่างโปรแกรมหลัก > **การตั้งค่า** > **การป้องกันเครือข่าย** > **แก้ไขที่อยู่ IP ที่ถูกบล็อกชั่วคราว** ที่อยู่ IP ที่ถูกปิดกั้นชั่วคราวจะถูกปิดกั้นเป็นเวลา 1 ชั่วโมง

คอลัมน์

ที่อยู่ IP – แสดงที่อยู่ IP ที่ถูกปิดกั้น

เหตุผลในการปิดกั้น - แสดงการโจมตีประเภทต่างๆ ที่ถูกป้องกันจากที่อยู่ (ตัวอย่างเช่น การโจมตีการสแกนพอร์ต TCP)

หมดเวลา – แสดงเวลาและวันที่ที่ที่อยู่จะหมดอายุจากบัญชีดำ

องค์ประกอบการควบคุม

ลบออก – คลิกเพื่อลบที่อยู่ออกจากบัญชีดำก่อนที่ที่อยู่จะหมดอายุจากบัญชีดำ

ลบทั้งหมด – คลิกเพื่อลบที่อยู่ทั้งหมดออกจากบัญชีดำในทันที

เพิ่มข้อยกเว้น – คลิกเพื่อเพิ่มข้อยกเว้นของไฟร์วอลล์ลงในการกรอง IDS

บันทึกการป้องกันเครือข่าย

การป้องกันเครือข่ายของ ESET Endpoint Security จะบันทึกเหตุการณ์สำคัญทั้งหมดในไฟล์บันทึก หากต้องการดูไฟล์บันทึก ให้เปิด หน้าต่างโปรแกรมหลัก > **ตั้งค่า** > **เครือข่าย** > **แสดงบันทึก**

สามารถใช้ไฟล์บันทึกเพื่อตรวจหาข้อผิดพลาดและเปิดเผยการบุกรุกในระบบของคุณ บันทึกการป้องกันเครือข่ายของจะมีข้อมูลต่อไปนี้:

- วันที่และเวลาของเหตุการณ์
- ชื่อของเหตุการณ์
- ที่มา
- ที่อยู่เครือข่ายเป้าหมาย

- โปรโตคอลการสื่อสารของเครือข่าย
- กฎที่ใช้งาน หรือชื่อของเวิร์ม หากสามารถระบุได้
- พาธและชื่อแอพพลิเคชัน
- แฮช
- ผู้ใช้
- ผู้ลงนามของแอพพลิเคชัน (ผู้เผยแพร่)
- ชื่อแพ็คเกจ
- ชื่อบริการ

การวิเคราะห์ข้อมูลนี้โดยละเอียดช่วยให้สามารถตรวจหาความพยายามในการบุกรุกการรักษาความปลอดภัยของระบบ ปัจจัยอื่นๆ อีกมากมายสามารถระบุความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นนี้ได้และสามารถป้องกันได้โดยใช้ไฟร์วอลล์ เช่น: การเชื่อมต่อที่บ่อยจากตำแหน่งที่ไม่รู้จัก ความพยายามต่างๆ ที่จะสร้างการเชื่อมต่อ การสื่อสารของแอพพลิเคชันที่ไม่รู้จัก หรือเลขที่พอร์ตที่ผิดปกติที่ใช้งานอยู่

> **การใช้ประโยชน์จากจุดอ่อนของความปลอดภัย**
> ข้อความเกี่ยวกับการใช้ประโยชน์จากจุดอ่อนของความปลอดภัยจะถูกบันทึกไว้แม้จุดอ่อนดังกล่าวจะได้รับการแก้ไขแล้วนับตั้งแต่ตรวจพบและปิดกั้นความพยายามในการใช้ประโยชน์ดังกล่าวบนระดับเครือข่ายก่อนที่การใช้ประโยชน์จะเกิดขึ้นจริง

การแก้ไขปัญหาเกี่ยวกับการป้องกันเครือข่ายของ ESET

หากคุณประสบปัญหาในการเชื่อมต่อกับ ESET Endpoint Security ที่ติดตั้งไว้ มีหลายวิธีที่สามารถบอกได้ว่าการป้องกันเครือข่ายของ ESET เป็นเหตุให้เกิดปัญหานั้นๆ หรือไม่ นอกจากนี้ การป้องกันเครือข่ายของ ESET ยังสามารถช่วยคุณสร้างกฎหรือข้อยกเว้นใหม่เพื่อแก้ไขปัญหาในการเชื่อมต่อได้

ดูหัวข้อต่อไปนี้เพื่อขอความช่วยเหลือในการแก้ไขปัญหาเกี่ยวกับการป้องกันเครือข่ายของ ESET:

- การแก้ไขปัญหาการเข้าถึงเครือข่าย
- การบันทึกและการสร้างกฎหรือข้อยกเว้นการบันทึก
- การสร้างข้อยกเว้นการแจ้งเตือนไฟร์วอลล์
- การบันทึกขั้นสูงสำหรับการป้องกันเครือข่าย
- การแก้ปัญหาเกี่ยวกับเครื่องมือสแกนการรับส่งข้อมูลเครือข่าย

การบันทึกและการสร้างกฎหรือข้อยกเว้นการบันทึก

ตามค่าเริ่มต้น ไฟร์วอลล์ของ ESET ไม่ได้บันทึกการเชื่อมต่อที่ปิดกั้นทั้งหมด หากคุณต้องการดูว่าการป้องกันเครือข่ายได้บล็อกอะไรไปบ้าง ให้เปิด การตั้งค่าขั้นสูง > **เครื่องมือ** > **การวินิจฉัย** > **การบันทึกขั้นสูง** แล้วเปิดใช้งาน **เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันเครือข่าย** หากคุณเห็นบางอย่างในบันทึกที่คุณไม่ต้องการให้ไฟร์วอลล์ปิดกั้น คุณสามารถสร้างกฎหรือกฎ IDS สำหรับบันทึกนั้นโดยการคลิกขวาบนรายการนั้นแล้วเลือก **อย่าปิดกั้นเหตุการณ์คล้ายคลึงกันอีกในอนาคต** โปรดทราบว่าบันทึกของการเชื่อมต่อที่ถูกปิดกั้นทั้งหมดอาจมีรายการนับพันรายการและอาจจะยากต่อการค้นหาการเชื่อมต่อแบบเฉพาะในบันทึกนี้ คุณสามารถปิดการบันทึกได้หลังจากที่คุณแก้ไขปัญหาแล้ว

เมื่อต้องการข้อมูลเพิ่มเติมเกี่ยวกับบันทึก ให้ดูที่ ไฟล์บันทึก

ใช้การบันทึกเพื่อดูอันดับที่การป้องกันเครือข่ายปิดกั้นการเชื่อมต่อเฉพาะ ยิ่งกว่านั้น การสร้างกฎจากบันทึกยังทำให้คุณสามารถสร้างกฎที่ทำในสิ่งที่คุณต้องการเป็นพิเศษได้

สร้างกฎจากบันทึก

ESET Endpoint Security เวอร์ชันใหม่ช่วยให้คุณสามารถสร้างกฎได้จากบันทึก จากเมนูหลัก ให้คลิก**เครื่องมือ** > **ไฟล์บันทึก** เลือก**การป้องกันเครือข่าย** จากเมนูแบบเลื่อนลง คลิกขวาที่รายการบันทึกที่คุณต้องการ แล้วเลือก **อย่าปิดกั้นเหตุการณ์คล้ายกันอีกในอนาคต** จากเมนูเนื้อหา หน้าต่างการแจ้งเตือนจะแสดงกฎใหม่ของคุณ

ถ้าต้องการให้อนุญาตให้สร้างกฎใหม่จากบันทึก ต้องกำหนดค่า ESET Endpoint Security ด้วยการตั้งค่าต่อไปนี้:

1. ตั้งค่าความละเอียดการบันทึกต่ำสุดไปที่ **การวินิจฉัย** ใน การตั้งค่าขั้นสูง > **เครื่องมือ** > **ไฟล์บันทึก**
2. เปิดใช้งาน **แจ้งเกี่ยวกับการโจมตีผ่านช่องโหว่ด้านความปลอดภัย** ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึง** > **การป้องกันการโจมตีเครือข่าย** > **ตัวเลือกขั้นสูง** > **การตรวจหาการบุกรุก**

การสร้างข้อยกเว้นการแจ้งเตือนไฟร์วอลล์

เมื่อไฟร์วอลล์ของ ESET ตรวจพบกิจกรรมเครือข่ายที่เป็นอันตราย หน้าต่างการแจ้งเตือนที่อธิบายกิจกรรมนั้นจะปรากฏขึ้นมา การแจ้งเตือนนี้มีลิงก์ที่จะช่วยให้คุณสามารถเรียนรู้เพิ่มเติมเกี่ยวกับกิจกรรมและตั้งค่าข้อยกเว้นสำหรับกิจกรรมนี้ได้ถ้าต้องการ

ถ้าแอพพลิเคชันของเครือข่ายหรืออุปกรณ์ไม่ได้ใช้มาตรฐานเครือข่ายให้ถูกต้อง ก็อาจทำให้มีการแจ้งเตือน IDS ของไฟร์วอลล์ที่ซ้ำซ้อนได้ คุณสามารถสร้างข้อยกเว้นได้โดยตรงจากการแจ้งเตือนเพื่อป้องกันไม่ให้ไฟร์วอลล์ของ ESET ตรวจพบแอพพลิเคชันหรืออุปกรณ์นี้

การบันทึกขั้นสูงสำหรับการป้องกันเครือข่าย

คุณสมบัตินี้มีจุดมุ่งหมายเพื่อให้ไฟล์บันทึกที่ซับซ้อนมากยิ่งขึ้นสำหรับฝ่ายสนับสนุนด้านเทคนิคของ ESET ให้ใช้คุณลักษณะนี้เฉพาะเมื่อมีการร้องขอจากฝ่ายสนับสนุนด้านเทคนิคของ ESET เท่านั้น เนื่องจากการดำเนินการนี้อาจสร้างไฟล์บันทึกขนาดใหญ่และทำให้เครื่องคอมพิวเตอร์ของคุณช้าลง

1. ไปที่ การตั้งค่าขั้นสูง > **เครื่องมือ** > **การวินิจฉัย** แล้วเปิดใช้งาน **เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันเครือข่าย**
2. พยายามทำซ้ำปัญหาที่คุณกำลังประสบอยู่
3. ปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันเครือข่าย
4. สามารถพบไฟล์บันทึก PCAP ที่สร้างโดยการบันทึกขั้นสูงสำหรับการป้องกันเครือข่ายในไดเรกทอรีเดียวกันกับที่สร้างดัมพ์หน่วยความจำสำหรับวินิจฉัย: *C:\ProgramData\ESET\ESET Security\Diagnostics*

การแก้ปัญหาเกี่ยวกับเครื่องมือสแกนการรับส่งข้อมูลเครือข่าย

ถ้าคุณประสบปัญหาเกี่ยวกับเบราว์เซอร์หรืออีเมลไคลเอ็นต์ของคุณ ขั้นตอนแรกคือการพิจารณาว่าเครื่องมือสแกนการรับส่งข้อมูลเครือข่ายมีการตอบสนองหรือไม่ โดยให้ลองปิดใช้งานเครื่องมือกรองโปรโตคอลแอพพลิเคชันชั่วคราวใน การตั้งค่าขั้นสูง **กลไกการตรวจจับ การรับส่งข้อมูลเครือข่าย** (อย่าลืมเปิดอีกครั้งหลังจากทำเสร็จ ไม่เช่นนั้น เบราว์เซอร์หรืออีเมลไคลเอ็นต์ของคุณจะยังคงอยู่ในสถานะไม่ได้รับการป้องกัน) ถ้าปัญหาของคุณไม่ปรากฏขึ้นมาหลังจากปิดระบบ ต่อไปนี้คือรายการปัญหาที่พบบ่อยและวิธีการแก้ไขปัญหาเหล่านั้น:

อัพเดทหรือรักษาความปลอดภัยของปัญหาในการสื่อสาร

ถ้าแอพพลิเคชันของคุณแจ้งเกี่ยวกับการไม่สามารถอัพเดทหรือช่องทางการสื่อสารไม่ปลอดภัย:

- ถ้าคุณเปิดใช้งาน SSL/TLS ไว้ให้ลองปิดชั่วคราว ถ้าการดำเนินการนั้นช่วยได้ คุณจะสามารถใช้ SSL/TLS ได้ต่อไป และจะดำเนินการอัพเดทได้โดยการยกเว้นการสื่อสารที่มีปัญหา:

ปิดใช้งาน SSL/TLS ดำเนินการอัพเดทใหม่ จะมีข้อความแจ้งคุณเกี่ยวกับการรับส่งข้อมูลทางเครือข่ายที่เข้ารหัส ตรวจสอบให้แน่ใจว่าแอพพลิเคชันนั้นตรงกับแอพพลิเคชันที่คุณกำลังแก้ไขปัญหา และใบรับรองดูเหมือนว่ามาจากเซิร์ฟเวอร์ที่อัพเดทมา จากนั้นเลือกจำการทำงานสำหรับใบรับรองนี้แล้วคลิกละเว้น ถ้าไม่ได้แสดงข้อความที่เกี่ยวข้องอีก คุณสามารถสลับโหมดการกรองกลับไปเป็นอัตโนมัติได้ และจะสามารถแก้ไขปัญหาได้

- ถ้าแอพพลิเคชันดังกล่าวไม่ใช่เบราว์เซอร์หรืออีเมลไคลเอ็นต์ คุณจะสามารถยกเว้นจาก การป้องกันการเข้าถึงเว็บไซต์ (การดำเนินการสิ่งนี้สำหรับเบราว์เซอร์หรืออีเมลไคลเอ็นต์อาจทำให้คุณเกิดความเสี่ยงได้) แอพพลิเคชันใดๆ ที่กรองการสื่อสารไว้ในอดีตจะอยู่ในรายการที่ให้คุณอยู่แล้วเมื่อเพิ่มข้อยกเว้น ดังนั้นจึงไม่จำเป็นต้องเพิ่มแอพพลิเคชันด้วยตัวเอง

ปัญหาในการเข้าถึงอุปกรณ์ในเครือข่ายของคุณ

หากคุณไม่สามารถใช้ฟังก์ชันของอุปกรณ์ใดๆ บนเครือข่ายของคุณ (ซึ่งอาจหมายถึงการเปิดหน้าเว็บของเว็บแคมของคุณหรือการเล่นวิดีโอบนเครื่องเล่นสื่อในบ้าน) ให้ลองเพิ่มที่อยู่ IPv4 และ IPv6 ไปยังรายการที่อยู่ที่ยกเว้น

ปัญหาเกี่ยวกับเว็บไซต์ที่ระบุ

คุณสามารถยกเว้นเว็บไซต์ที่ต้องการได้โดยใช้การจัดการที่อยู่ URL ใน การป้องกันการเข้าถึงเว็บไซต์ ตัวอย่างเช่น ถ้าคุณไม่สามารถเข้าไปที่ https://www.gmail.com/intl/en/mail/help/about.html ให้ลองเพิ่ม *gmail.com* ไปยังรายการที่อยู่ที่ยกเว้น

ข้อผิดพลาดแจ้งว่า "แอพพลิเคชันบางตัวที่สามารถนำเข้าใบรับรองหลักกำลังทำงานอยู่"

เมื่อคุณเปิดใช้งาน SSL/TLS ESET Endpoint Security จะตรวจสอบว่าแอพพลิเคชันที่ติดตั้งเชื่อถือวิธีการกรองโปรโตคอล SSL โดยการนำเข้าใบรับรองไปยังร้านใบรับรองของแอพพลิเคชัน โปรแกรมประยุกต์บางอย่างอาจต้องเริ่มการทำงานเพื่อนำเข้าใบรับรอง ซึ่งรวมถึง Firefox และ Opera ตรวจสอบว่าไม่ได้ใช้งานแอพพลิเคชันเหล่านั้นอยู่ (วิธีการตรวจสอบที่ดีที่สุดคือให้เปิดโปรแกรมจัดการงาน และตรวจสอบว่าไม่มี firefox.exe หรือ opera.exe ด้านใต้แท็บกระบวนการ) จากนั้นให้ลองใหม่

ข้อผิดพลาดเกี่ยวกับผู้ออกใบรับรองที่ไม่น่าเชื่อถือหรือลายเซ็นที่ไม่ถูกต้อง

เป็นไปได้มากว่าข้อผิดพลาดนี้เกิดจากการนำเข้าที่อธิบายไว้ข้างต้นล้มเหลว ขั้นแรก ตรวจสอบว่าไม่มีแอพพลิเคชันที่กล่าวไปทั้งหมดทำงานอยู่ จากนั้นปิดการใช้งาน SSL/TLS และเปิดใช้งานอีกครั้ง ขั้นตอนนี้จะดำเนินการนำเข้าอีกครั้ง

ปิดกั้นภัยคุกคามเครือข่ายแล้ว

สถานการณ์นี้อาจเกิดขึ้นได้เมื่อแอพพลิเคชันบนคอมพิวเตอร์ของคุณพยายามส่งการรับส่งข้อมูลที่เป็นอันตรายไปยังอุปกรณ์อื่นบนเครือข่าย การใช้ประโยชน์จากช่องโหว่ของการรักษาความปลอดภัย หรือตรวจพบความพยายามในการสแกนพอร์ตในระบบของคุณ

คุณสามารถค้นหาประเภทของภัยคุกคามและที่อยู่ IP ของอุปกรณ์ที่เกี่ยวข้องได้ในการแจ้งเตือน คลิก **เปลี่ยนการจัดการภัยคุกคามนี้** เพื่อแสดงตัวเลือกดังต่อไปนี้:

ปิดกั้นต่อไป - ปิดกั้นภัยคุกคามที่ตรวจพบ หากคุณต้องการหยุดรับการแจ้งเตือนเกี่ยวกับภัยคุกคามประเภทนี้จากที่อยู่ระยะไกลที่อยู่ใดที่อยู่หนึ่ง ให้เลือกปุ่มตัวเลือกถัดจาก **ไม่ต้องแจ้งเตือน** ก่อนที่จะคลิก **ดำเนินการบล็อกต่อ** การดำเนินการดังกล่าวนี้จะสร้างกฎของบริการตรวจหาผู้บุกรุก (IDS) ที่มีการกำหนดค่าดังต่อไปนี้: **บล็อก** - เริ่มต้น, **แจ้งเตือน** - ไม่, **บันทึก** - ไม่

อนุญาต - สร้างกฎของบริการตรวจหาผู้บุกรุก (IDS) เพื่ออนุญาตให้มีการตรวจหาภัยคุกคาม เลือกตัวเลือกใดตัวเลือกหนึ่งจากตัวเลือกต่อไปนี้ ก่อนที่จะคลิก**อนุญาต**เพื่อระบุการตั้งค่ากฎ:

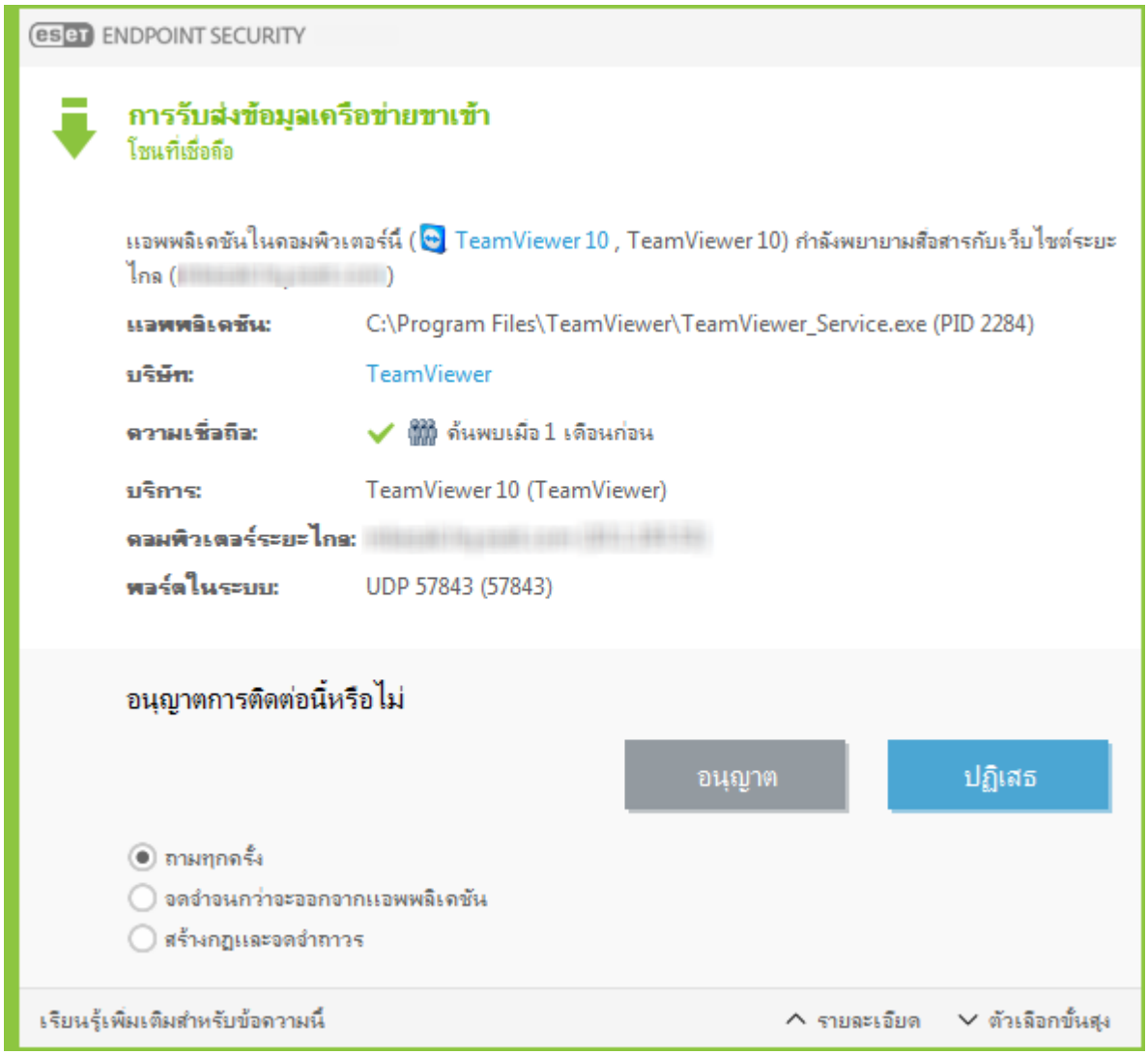
- **แจ้งเตือนก็ต่อเมื่อภัยคุมคามนี้ถูกบล็อก** - การกำหนดค่ากฎ: **บล็อก** - ไม่, **แจ้งเตือน** - ไม่, **บันทึก** - ไม่
- **แจ้งเตือนก็ต่อเมื่อภัยคุมคามนี้เกิดขึ้น** - การกำหนดค่ากฎ: **บล็อก** - ไม่ **แจ้งเตือน** - เริ่มต้น **บันทึก** - เริ่มต้น
- **ไม่ต้องแจ้งเตือน** - การกำหนดค่ากฎ: **บล็อก** - ไม่, **แจ้งเตือน** - ไม่, **บันทึก** - ไม่

ข้อมูลที่แสดงในหน้าต่างการแจ้งเตือนอาจแตกต่างกันไป ขึ้นอยู่กับประเภทของภัยคุกคามที่ตรวจพบ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับภัยคุกคามและข้อกำหนดอื่นๆ ที่เกี่ยวข้อง ดูที่ ประเภทของการโจมตีระยะไกล หรือ ประเภทของการตรวจหา
หากต้องการแก้ไขเหตุการณ์ **ที่อยู่ IP ซ้ำบนเครือข่าย** โปรดดูบทความฐานความรู้ของ ESET

การเริ่มต้นการเชื่อมต่อ – การตรวจหา

ไฟร์วอลล์จะตรวจหาการเชื่อมต่อเครือข่ายที่สร้างขึ้นใหม่ในแต่ละครั้ง โหมดไฟร์วอลล์แบบแอคทีฟจะกำหนดว่าการดำเนินการใดจะทำงานในกฎใหม่ หากเปิดใช้งาน **โหมดอัตโนมัติ** หรือ **โหมดนโยบาย** ไฟร์วอลล์จะดำเนินการตามการทำงานที่กำหนดไว้ล่วงหน้าโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ

โหมดตอบสนองจะแสดงหน้าต่างข้อมูลที่รายงานการตรวจหาการเชื่อมต่อเครือข่ายใหม่ พร้อมข้อมูลอย่างละเอียดเกี่ยวกับการเชื่อมต่อนั้น คุณสามารถเลือกที่จะ **อนุญาต** หรือ **ปฏิเสธ** (บล็อก) การเชื่อมต่อได้ ถ้าคุณอนุญาตการเชื่อมต่อเดียวกันหลายครั้งในหน้าต่างข้อความ เราขอแนะนำให้คุณสร้างกฎใหม่สำหรับการเชื่อมต่อ ในการดำเนินการดังกล่าว ให้เลือก **สร้างกฎและจดจำอย่างถาวร** แล้วบันทึกการทำงานเป็นกฎใหม่สำหรับไฟร์วอลล์ หากไฟร์วอลล์รู้จักการเชื่อมต่อเดียวกันนี้ในอนาคต ระบบจะใช้กฎที่มีอยู่โดยที่ผู้ใช้ไม่ต้องดำเนินการใด



เมื่อสร้างกฎใหม่ ให้อนุญาตเฉพาะการเชื่อมต่อที่คุณรู้ว่าปลอดภัยเท่านั้น ถ้าอนุญาตการเชื่อมต่อทั้งหมด ไฟร์วอลล์จะไม่สามารถดำเนินการให้สำเร็จได้ตามวัตถุประสงค์ พารามิเตอร์ที่สำคัญสำหรับการเชื่อมต่อมีดังต่อไปนี้:

แอพพลิเคชัน – ตำแหน่งของไฟล์ที่เรียกใช้ได้และ ID กระบวนการ อย่าอนุญาตการเชื่อมต่อสำหรับแอพพลิเคชันและกระบวนการที่ไม่รู้จัก

ผู้ลงนาม ชื่อผู้เผยแพร่แอปพลิเคชันของแอพพลิเคชัน คลิกข้อความเพื่อแสดงใบรับรองความปลอดภัยของบริษัท

ความเชื่อถือ – ระดับความเสี่ยงของการเชื่อมต่อ การเชื่อมต่อต่างๆ จะได้รับการกำหนดระดับความเสี่ยง: ดี (สีเขียว), ไม่ทราบ (สีส้ม) หรือ มีความเสี่ยง (สีแดง) โดยใช้ชุดกฎการวิเคราะห์พฤติกรรมที่จะตรวจสอบลักษณะของแต่ละการเชื่อมต่อ จำนวนผู้ใช้ และเวลาที่ค้นพบ ข้อมูลนี้ได้รับการรวบรวมโดยเทคโนโลยี ESET LiveGrid®

บริการ – ชื่อของบริการ หากแอพพลิเคชันเป็นบริการของ Windows

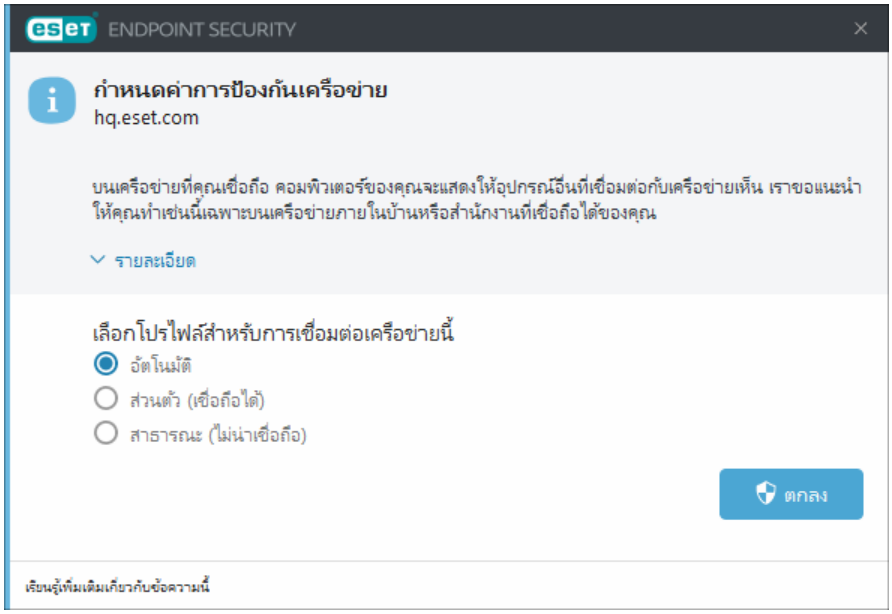
คอมพิวเตอร์ระยะไกล – ที่อยู่ของอุปกรณ์ระยะไกล อนุญาตเฉพาะการเชื่อมต่อไปยังที่อยู่ที่เชื่อถือและรู้จัก

พอร์ตระยะไกล – พอร์ตการสื่อสาร การสื่อสารบนพอร์ตทั่วไป (ตัวอย่างเช่น การรับส่งข้อมูลทางเว็บ - เลขที่พอร์ต 80,443) สามารถอนุญาตได้ในสถานการณ์ปกติ

การแฝงตัวในคอมพิวเตอร์มักจะใช้การเชื่อมต่ออินเทอร์เน็ตและการเชื่อมต่อที่ซ่อนไว้เพื่อให้ระบบระยะไกลติดไวรัส หากกำหนดค่ากฎไว้อย่างถูกต้อง ไฟร์วอลล์จะเป็นเครื่องมือที่มีประโยชน์สำหรับการป้องกันการโจมตีของรหัสที่เป็นอันตรายจำนวนมาก

พบเครือข่ายใหม่

โดยค่าเริ่มต้น ESET Endpoint Security จะใช้การตั้งค่า Windows เมื่อมีการตรวจพบการเชื่อมต่อเครือข่ายรายการใหม่ หากต้องการแสดงหน้าต่างโต้ตอบเมื่อตรวจพบเครือข่ายใหม่ ให้เปลี่ยน การกำหนดโปรไฟล์การป้องกันเครือข่าย เป็น **ถาม** การกำหนดค่าการป้องกันเครือข่ายจะเกิดขึ้นเมื่อใดก็ตามที่คอมพิวเตอร์ของคุณเชื่อมต่อกับเครือข่ายใหม่



คุณสามารถเลือกจาก โปรไฟล์การเชื่อมต่อเครือข่าย ต่อไปนี้:

อัตโนมัติ — ESET Endpoint Security จะเลือกโปรไฟล์โดยอัตโนมัติ ตาม ตัวเปิดใช้งาน ที่กำหนดค่าไว้สำหรับแต่ละโปรไฟล์

ส่วนตัว – สำหรับเครือข่ายที่เชื่อถือได้ (เครือข่ายในบ้านหรือที่ทำงาน) ผู้ใช้เครือข่ายรายอื่นสามารถมองเห็นคอมพิวเตอร์และไฟล์ที่ใช้ร่วมกันที่เก็บไว้ในคอมพิวเตอร์ของคุณได้ และผู้ใช้รายอื่นบนเครือข่ายสามารถเข้าถึงทรัพยากรระบบได้ (เปิดใช้งานการเข้าถึงไฟล์ที่แชร์และเครื่องพิมพ์ การติดต่อสื่อสาร RPC ขาเข้า และการแชร์ผ่านเดสก์ท็อปจากระยะไกล) เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าถึงเครือข่ายภายในที่ปลอดภัย ระบบจะกำหนดโปรไฟล์นี้ไปยังการเชื่อมต่อเครือข่ายโดยอัตโนมัติหากมีการกำหนดค่าเป็น "โดเมน" หรือเครือข่าย "ส่วนตัว" ใน Windows

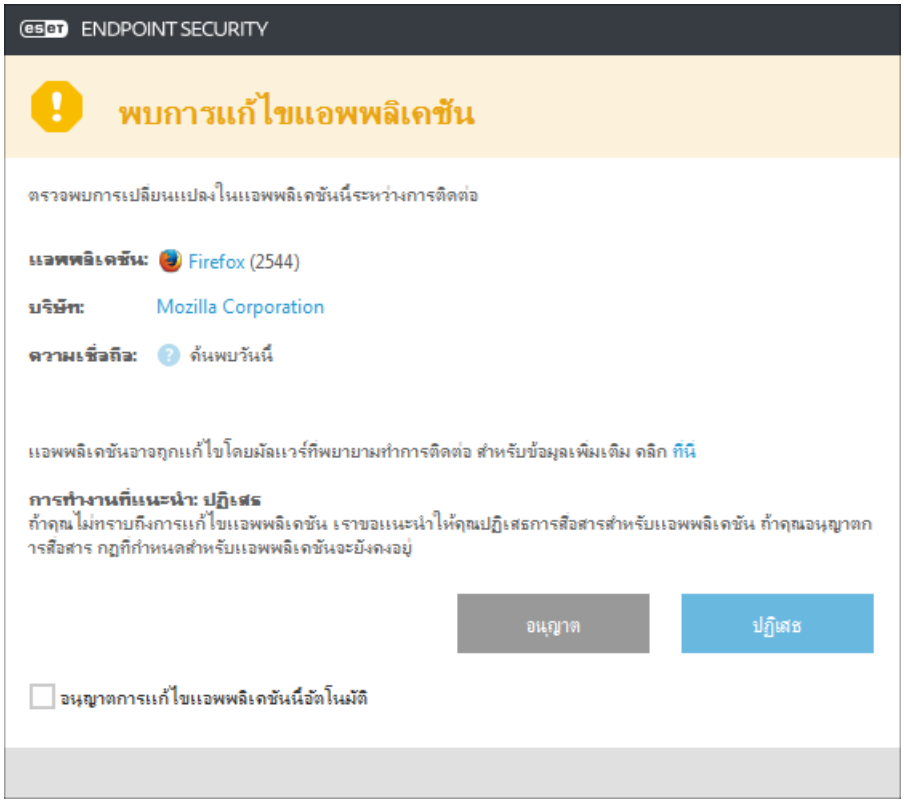
สาธารณะ – สำหรับเครือข่ายที่ไม่เชื่อถือ (เครือข่ายสาธารณะ) ไฟล์และโฟลเดอร์ในระบบของคุณจะไม่ถูกใช้ร่วมกันหรือมองเห็นได้สำหรับผู้ใช้รายอื่นบนเครือข่าย และการแบ่งปันทรัพยากรระบบจะถูกปิดใช้งาน เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าสู่เครือข่ายไร้สาย ระบบจะกำหนดโปรไฟล์นี้ไปยังการเชื่อมต่อเครือข่ายโดยอัตโนมัติหากมีการกำหนดค่าเป็น "โดเมน" หรือเครือข่าย "ส่วนตัว" ใน Windows

โปรไฟล์ที่ผู้ใช้กำหนด – คุณสามารถเลือกโปรไฟล์จากหนึ่งใน โปรไฟล์หนึ่งที่คุณสร้าง ได้จากเมนูแบบเลื่อนลง ตัวเลือกนี้จะใช้ได้ก็ต่อเมื่อคุณได้สร้างโปรไฟล์แบบกำหนดเองอย่างน้อยหนึ่งโปรไฟล์เท่านั้น

การกำหนดค่าเครือข่ายที่ไม่ถูกต้องอาจทำให้เกิดความเสี่ยงด้านการรักษาความปลอดภัยของคอมพิวเตอร์ของคุณ

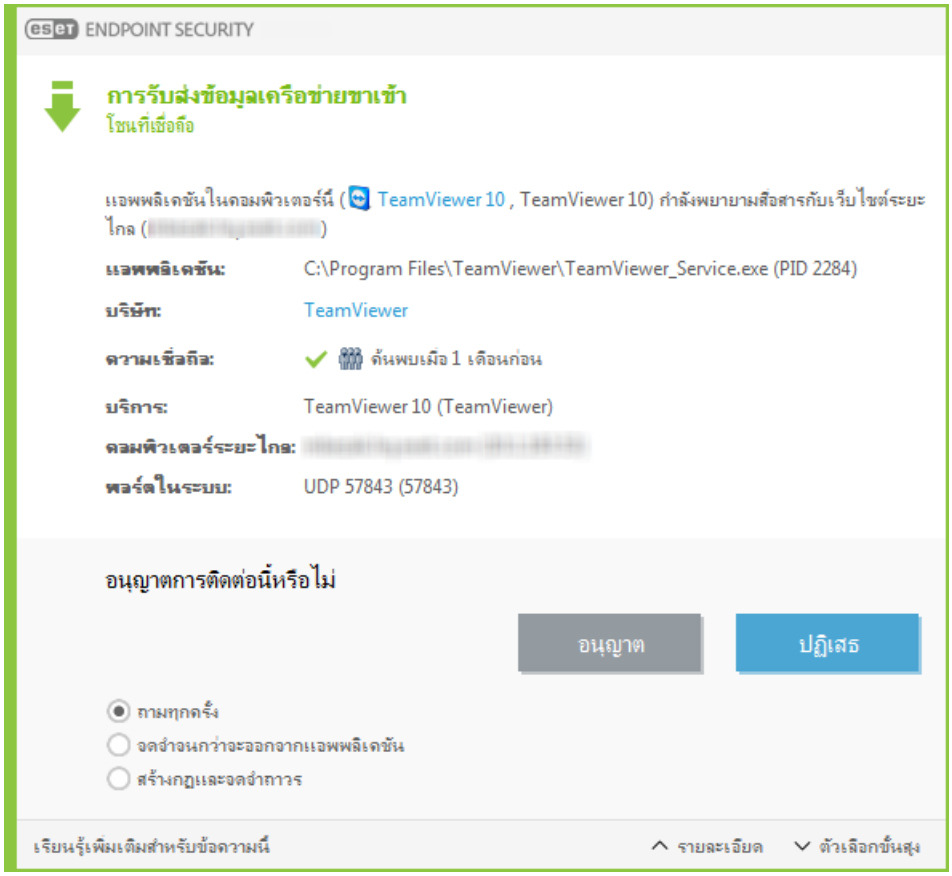
การเปลี่ยนแปลงแอพพลิเคชัน

ไฟล์วอลล์ตรวจพบการแก้ไขในแอพพลิเคชัน ซึ่งใช้เพื่อสร้างการเชื่อมต่อขาออกจากคอมพิวเตอร์ของคุณ เป็นไปได้ว่า มีการอัพเดทแอพพลิเคชันเป็นเวอร์ชันใหม่ ในทางตรงกันข้าม การแก้ไขอาจเกิดจากแอพพลิเคชันที่เป็นอันตราย ถ้าคุณไม่ทราบว่ามีการแก้ไขที่ถูกต้อง เราขอแนะนำให้คุณปฏิเสธการเชื่อมต่อ และ สแกนคอมพิวเตอร์ของคุณ โดยใช้ กลไกตรวจหาเวอร์ชันล่าสุด หากคุณแน่ใจถึงการดัดแปลงใดๆ และอนุญาตให้มีการสื่อสารด้วยช่องกาเครื่องหมาย **อนุญาตการแก้ไขแอพพลิเคชันนี้อัตโนมัติ** กฎที่กำหนดสำหรับแอพพลิเคชันนี้จะยังคงอยู่



การสื่อสารขาเข้าที่เชื่อถือ

ตัวอย่างของการเชื่อมต่อขาเข้าภายในโซนที่เชื่อถือ:
คอมพิวเตอร์ระยะไกลจากโซนที่เชื่อถือ ซึ่งพยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันในระบบที่ทำงานบนคอมพิวเตอร์ของคุณ



แอพพลิเคชัน – แอพพลิเคชันที่เรียกใช้โดยอุปกรณ์ระยะไกล

เส้นทางแอพลิเคชัน – ตำแหน่งที่ตั้งของแอพลิเคชัน

แอพพลิเคชัน Microsoft Store – ชื่อของแอพพลิเคชันใน Microsoft Store

ผู้ลงนาม ชื่อผู้เผยแพร่แอปพลิเคชันของแอพพลิเคชัน คลิกข้อความเพื่อแสดงใบรับรองความปลอดภัยของบริษัท

ความเชื่อถือ – ความเชื่อถือของแอพพลิเคชันที่ได้รับโดยเทคโนโลยี ESET LiveGrid®

บริการ - ชื่อของบริการที่ทำงานอยู่บนคอมพิวเตอร์ของคุณในขณะนี้

คอมพิวเตอร์ระยะไกล – คอมพิวเตอร์ระยะไกลที่พยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันบนคอมพิวเตอร์ของคุณ

พอร์ตระยะไกล – พอร์ตที่ใช้สำหรับการสื่อสาร

ถามทุกครั้ง - หากการกระทำตามค่าเริ่มต้นสำหรับกฎถูกตั้งให้เป็น **ถาม** หน้าต่างข้อความจะปรากฏขึ้นในแต่ละครั้งที่กฎทำงาน

จดจำจนกว่าจะออกจากแอพพลิเคชัน - ESET Endpoint Security จะจดจำการกระทำที่เลือกจนกว่าจะเริ่มต้นระบบ

คอมพิวเตอร์ใหม่

สร้างกฎและจดจำอย่างถาวร - หากคุณเลือกตัวเลือกนี้ก่อนที่จะอนุญาตหรือปฏิเสธการติดต่อ ESET Endpoint Security จะจดจำการกระทำและใช้การกระทำดังกล่าวหากแอพพลิเคชันเชื่อมต่อกับคอมพิวเตอร์ระยะไกลอีกครั้ง

อนุญาต – อนุญาตการสื่อสารขาเข้า

ปฏิเสธ – ปฏิเสธการสื่อสารขาเข้า

แก้ไขกฎ – ช่วยให้คุณกำหนดคุณสมบัติกฎเองโดยใช้ เครื่องมือแก้ไขกฎของไฟร์วอลล์

การสื่อสารขาออกที่เชื่อถือ

ตัวอย่างของการเชื่อมต่อขาออกภายในโซนที่เชื่อถือ:
แอพพลิเคชันในระบบที่พยายามเริ่มต้นการเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่นภายในเครือข่ายของระบบ หรือภายในเครือข่ายในโซนที่เชื่อถือ

แอพพลิเคชัน – แอพพลิเคชันที่เรียกใช้โดยอุปกรณ์ระยะไกล

เส้นทางแอพลิเคชัน – ตำแหน่งที่ตั้งของแอพลิเคชัน

แอพพลิเคชัน Microsoft Store – ชื่อของแอพพลิเคชันใน Microsoft Store

ผู้ลงนาม ชื่อผู้เผยแพร่แอปพลิเคชันของแอพพลิเคชัน คลิกข้อความเพื่อแสดงใบรับรองความปลอดภัยของบริษัท

ความเชื่อถือ – ความเชื่อถือของแอพพลิเคชันที่ได้รับโดยเทคโนโลยี ESET LiveGrid®

บริการ - ชื่อของบริการที่ทำงานอยู่บนคอมพิวเตอร์ของคุณในขณะนี้

คอมพิวเตอร์ระยะไกล – คอมพิวเตอร์ระยะไกลที่พยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันบนคอมพิวเตอร์ของคุณ

พอร์ตระยะไกล – พอร์ตที่ใช้สำหรับการสื่อสาร

ถามทุกครั้ง - หากการกระทำตามค่าเริ่มต้นสำหรับกฎถูกตั้งให้เป็น **ถาม** หน้าต่างข้อความจะปรากฏขึ้นในแต่ละครั้งที่กฎทำงาน

จดจำจนกว่าจะออกจากแอพพลิเคชัน - ESET Endpoint Security จะจดจำการกระทำที่เลือกจนกว่าจะเริ่มต้นระบบ

คอมพิวเตอร์ใหม่

สร้างกฎและจดจำอย่างถาวร - หากคุณเลือกตัวเลือกนี้ก่อนที่จะอนุญาตหรือปฏิเสธการติดต่อ ESET Endpoint Security จะจดจำการกระทำและใช้การกระทำดังกล่าวหากแอพพลิเคชันเชื่อมต่อกับคอมพิวเตอร์ระยะไกลอีกครั้ง

อนุญาต – อนุญาตการสื่อสารขาเข้า

ปฏิเสธ – ปฏิเสธการสื่อสารขาเข้า

แก้ไขกฎ – ช่วยให้คุณกำหนดคุณสมบัติกฎเองโดยใช้ เครื่องมือแก้ไขกฎของไฟร์วอลล์

การสื่อสารขาเข้า

ตัวอย่างของการเชื่อมต่ออินเทอร์เน็ตขาเข้า:
คอมพิวเตอร์ระยะไกลที่พยายามสื่อสารกับแอพพลิเคชันที่ทำงานบนคอมพิวเตอร์

แอพพลิเคชัน – แอพพลิเคชันที่เรียกใช้โดยอุปกรณ์ระยะไกล

เส้นทางแอพลิเคชัน – ตำแหน่งที่ตั้งของแอพลิเคชัน

แอพพลิเคชัน Microsoft Store – ชื่อของแอพพลิเคชันใน Microsoft Store

ผู้ลงนาม ชื่อผู้เผยแพร่แอปพลิเคชันของแอพพลิเคชัน คลิกข้อความเพื่อแสดงใบรับรองความปลอดภัยของบริษัท

ความเชื่อถือ – ความเชื่อถือของแอพพลิเคชันที่ได้รับโดยเทคโนโลยี ESET LiveGrid®

บริการ - ชื่อของบริการที่ทำงานอยู่บนคอมพิวเตอร์ของคุณในขณะนี้

คอมพิวเตอร์ระยะไกล – คอมพิวเตอร์ระยะไกลที่พยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันบนคอมพิวเตอร์ของคุณ

พอร์ตระยะไกล – พอร์ตที่ใช้สำหรับการสื่อสาร

ถามทุกครั้ง - หากการกระทำตามค่าเริ่มต้นสำหรับกฎถูกตั้งให้เป็น **ถาม** หน้าต่างข้อความจะปรากฏขึ้นในแต่ละครั้งที่กฎทำงาน

จดจำจนกว่าจะออกจากแอพพลิเคชัน - ESET Endpoint Security จะจดจำการกระทำที่เลือกจนกว่าจะเริ่มต้นระบบคอมพิวเตอร์ใหม่

สร้างกฎและจดจำอย่างถาวร - หากคุณเลือกตัวเลือกนี้ก่อนที่จะอนุญาตหรือปฏิเสธการติดต่อ ESET Endpoint Security จะจดจำการกระทำและใช้การกระทำดังกล่าวหากแอพพลิเคชันเชื่อมต่อกับคอมพิวเตอร์ระยะไกลอีกครั้ง

อนุญาต – อนุญาตการสื่อสารขาเข้า

ปฏิเสธ – ปฏิเสธการสื่อสารขาเข้า

แก้ไขกฎ – ช่วยให้คุณกำหนดคุณสมบัติกฎเองโดยใช้ เครื่องมือแก้ไขกฎของไฟร์วอลล์

การสื่อสารขาออก

ตัวอย่างของการเชื่อมต่ออินเทอร์เน็ตขาออก:
แอพพลิเคชันในระบบที่พยายามเริ่มต้นการเชื่อมต่ออินเทอร์เน็ต

แอพพลิเคชัน – แอพพลิเคชันที่เรียกใช้โดยอุปกรณ์ระยะไกล

เส้นทางแอพลิเคชัน – ตำแหน่งที่ตั้งของแอพลิเคชัน

แอพพลิเคชัน Microsoft Store – ชื่อของแอพพลิเคชันใน Microsoft Store

ผู้ลงนาม ชื่อผู้เผยแพร่แอปพลิเคชันของแอพพลิเคชัน คลิกข้อความเพื่อแสดงใบรับรองความปลอดภัยของบริษัท

ความเชื่อถือ – ความเชื่อถือของแอพพลิเคชันที่ได้รับโดยเทคโนโลยี ESET LiveGrid®

บริการ - ชื่อของบริการที่ทำงานอยู่บนคอมพิวเตอร์ของคุณในขณะนี้

คอมพิวเตอร์ระยะไกล – คอมพิวเตอร์ระยะไกลที่พยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันบนคอมพิวเตอร์ของคุณ

พอร์ตระยะไกล – พอร์ตที่ใช้สำหรับการสื่อสาร

ถามทุกครั้ง - หากการกระทำตามค่าเริ่มต้นสำหรับกฎถูกตั้งให้เป็น **ถาม** หน้าต่างข้อความจะปรากฏขึ้นในแต่ละครั้งที่กฎทำงาน

จดจำจนกว่าจะออกจากแอพพลิเคชัน - ESET Endpoint Security จะจดจำการกระทำที่เลือกจนกว่าจะเริ่มต้นระบบคอมพิวเตอร์ใหม่

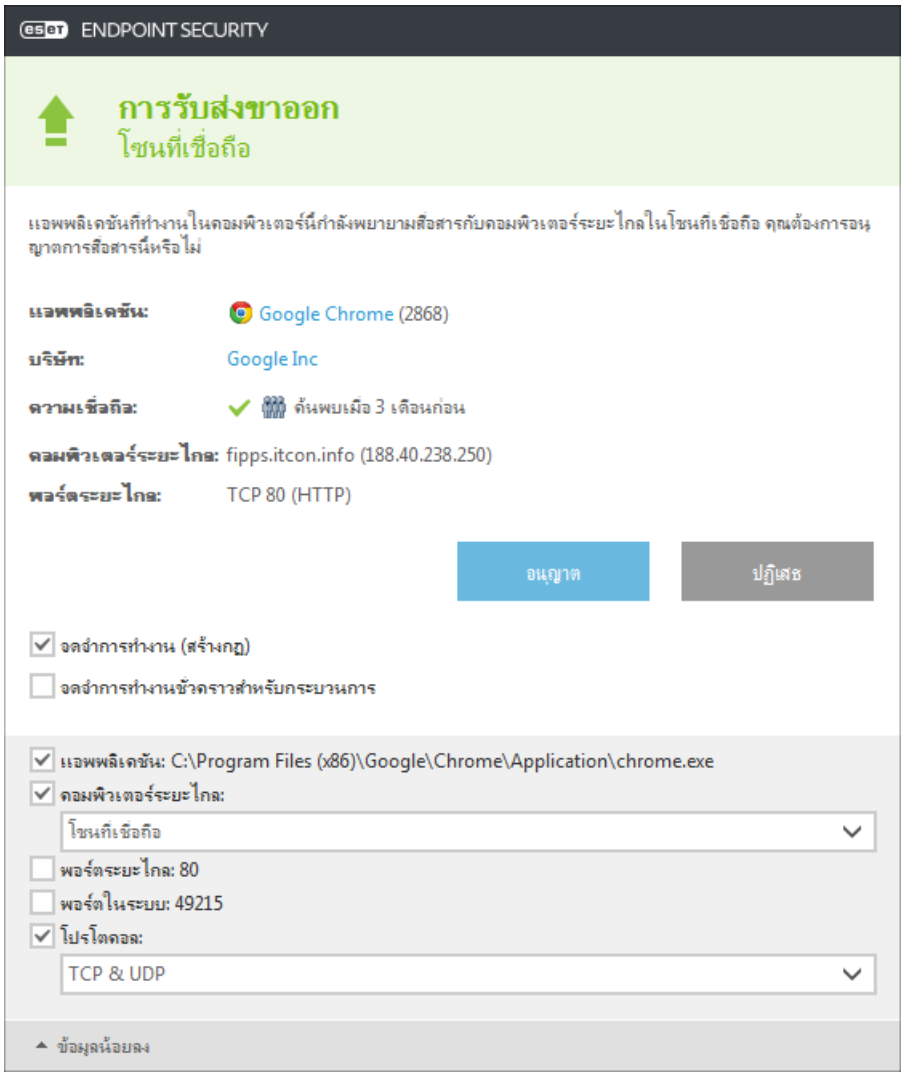
สร้างกฎและจดจำอย่างถาวร - หากคุณเลือกตัวเลือกนี้ก่อนที่จะอนุญาตหรือปฏิเสธการติดต่อ ESET Endpoint

Security จะจดจำการกระทำและใช้การกระทำดังกล่าวหากแอพพลิเคชันเชื่อมต่อกับคอมพิวเตอร์ระยะไกลอีกครั้ง

อนุญาต – อนุญาตการสื่อสารขาเข้า

ปฏิเสธ – ปฏิเสธการสื่อสารขาเข้า

แก้ไขกฎ – ช่วยให้คุณกำหนดคุณสมบัติกฎเองโดยใช้ เครื่องมือแก้ไขกฎของไฟร์วอลล์



ตั้งค่ามุมมองการเชื่อมต่อ

คลิกขวาที่การเชื่อมต่อเพื่อดูตัวเลือกอื่นๆ ที่มีอยู่:

แปลค่าชื่อโฮสต์ – ถ้าเป็นไปได้ ที่อยู่เครือข่ายทั้งหมดจะแสดงในรูปแบบ DNS ไม่ใช่ในรูปแบบที่อยู่ IP ที่เป็นตัวเลข

แสดงเฉพาะการเชื่อมต่อ TCP – รายการจะแสดงเฉพาะการเชื่อมต่อที่อยู่ในชุดโปรโตคอล TCP

แสดงการเชื่อมต่อของรายชื่อ – เลือกตัวเลือกนี้เพื่อแสดงเฉพาะการเชื่อมต่อที่ยังไม่ได้เริ่มต้นการสื่อสาร แต่

ระบบได้เปิดพอร์ตและกำลังรอการเชื่อมต่ออยู่

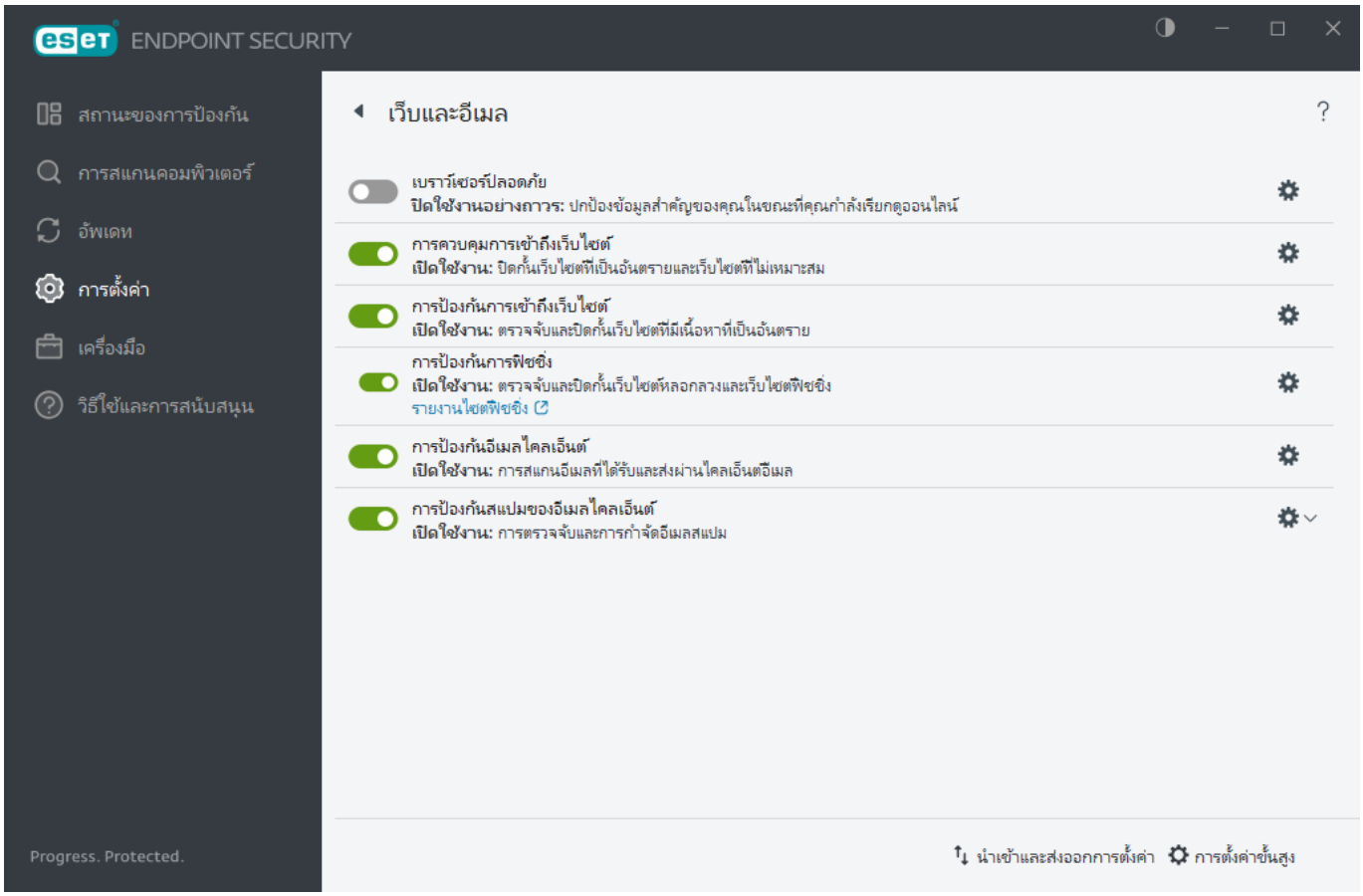
แสดงการเชื่อมต่อภายในคอมพิวเตอร์ – เลือกตัวเลือกนี้เพื่อแสดงเฉพาะการเชื่อมต่อที่คอมพิวเตอร์ระยะไกลเป็นระบบภายใน หรือเรียกว่าการเชื่อมต่อ localhost

เว็บและอีเมล

การเชื่อมต่ออินเทอร์เน็ตเป็นฟีเจอร์มาตรฐานในคอมพิวเตอร์ส่วนบุคคล แต่ยังเป็นสื่อหลักสำหรับการถ่ายโอนโค้ดที่เป็นอันตรายเช่นกัน เปิด หน้าต่างโปรแกรมหลัก > **การตั้งค่า** > **เว็บและอีเมล** เพื่อกำหนดค่าฟีเจอร์ของ ESET Endpoint Security ที่เพิ่มการป้องกันอินเทอร์เน็ต

หากต้องการหยุดชั่วคราวหรือปิดใช้งานโมดูลการป้องกันแต่ละโมดูล ให้คลิกไอคอนปุ่มสลับ

⚠ การปิดโมดูลการป้องกันอาจลดระดับการป้องกันของคอมพิวเตอร์ของคุณ



คลิกไอคอนฟันเฟือง ⚙ ที่อยู่ถัดจากโมดูลการป้องกันเพื่อเข้าถึงการตั้งค่าขั้นสูงสำหรับโมดูลนั้น

เบราว์เซอร์ปลอดภัย – ปกป้องข้อมูลสำคัญของคุณในขณะที่คุณกำลังเรียกดูออนไลน์

โมดูล **การควบคุมการเข้าถึงเว็ปไซต์** จะช่วยให้คุณสามารถกำหนดค่าการตั้งค่าซึ่งจะให้เครื่องมืออัตโนมัติแก่ผู้ดูแลระบบเพื่อช่วยป้องกันเวิร์กสเตชันของพวกเขาและตั้งค่าข้อจำกัดสำหรับการเรียกดูข้อมูลในอินเทอร์เน็ต ฟังก์ชันภายในการควบคุมการเข้าถึงเว็ปไซต์จะป้องกันการเข้าถึงหน้าที่มีเนื้อหาที่ไม่เหมาะสมหรือเป็นอันตราย โปรดดูข้อมูลเพิ่มเติมที่ การควบคุมการเข้าถึงเว็บไซต์

การป้องกันการเข้าถึงเว็บไซต์ จะสแกนหามัลแวร์และฟิชชิ่งในการสื่อสาร HTTP/HTTPS แนะนำให้ปิดการป้องกันการเข้าถึงเว็บไซต์ก็ต่อเมื่อต้องการแก้ไขปัญหาเท่านั้น

การป้องกันฟิชชิ่ง อนุญาตให้คุณปิดกั้นหน้าเว็บที่ทราบว่ามีการแจกจ่ายเนื้อหาการฟิชชิ่ง เราขอแนะนำให้คุณเปิดใช้งานการป้องกันฟิชชิ่งทิ้งไว้

รายงานเว็บไซต์ฟิชชิ่ง – รายงานเว็บไซต์ฟิชชิ่ง/ที่เป็นอันตรายไปยัง ESET เพื่อวิเคราะห์

> ก่อนส่งเว็บไซต์ไปยัง ESET โปรดตรวจสอบว่าเว็บไซต์ตรงตามเกณฑ์อย่างน้อยหนึ่งข้อดังต่อไปนี้:
> • ไม่มีการตรวจพบเว็บไซต์เลย
> • มีการตรวจพบเว็บไซต์ว่าเป็นภัยคุกคามโดยเป็นข้อผิดพลาด ในกรณีนี้ คุณสามารถ รายงานหน้าที่ถูกปอดกั้นอย่างไม่ถูกต้อง

การป้องกันอีเมลไคลเอ็นต์ จะมีการควบคุมการสื่อสารทางอีเมลที่ได้รับผ่านโปรโตคอล POP3(S) และ IMAP(S) เมื่อใช้โปรแกรมปลั๊กอินสำหรับอีเมลไคลเอ็นต์ ESET Endpoint Security มีการควบคุมการสื่อสารทั้งหมดจากอีเมลไคลเอ็นต์

การป้องกันสแปมอีเมลไคลเอ็นต์ จะกรองข้อความอีเมลที่ไม่พึงประสงค์

หากต้องการใช้ **การป้องกันสแปมอีเมลไคลเอ็นต์** ให้คลิกไอคอนฟันเฟือง ⚙ และเลือกจากตัวเลือกต่อไปนี้:

- **กำหนดค่า** – เปิด การตั้งค่าขั้นสูงสำหรับการป้องกันสแปมอีเมลไคลเอ็นต์
- **รายการที่อยู่ของผู้ใช้** (หากเปิดใช้งานอยู่) – เปิด หน้าต่างข้อความ ที่คุณสามารถเพิ่ม แก้ไข หรือลบที่อยู่เพื่อกำหนดกฎการป้องกันสแปมได้ ซึ่งกฎต่างๆ ในรายการนี้จะมีผลใช้กับผู้ใช้ปัจจุบัน
- **รายการที่อยู่ร่วม** (หากเปิดใช้งานอยู่) – เปิด หน้าต่างข้อความ ที่คุณสามารถเพิ่ม แก้ไข หรือลบที่อยู่เพื่อกำหนดกฎการป้องกันสแปมได้ ซึ่งกฎต่างๆ ในรายการนี้จะมีผลใช้กับผู้ใช้ทั้งหมด

การป้องกันฟิชชิ่ง

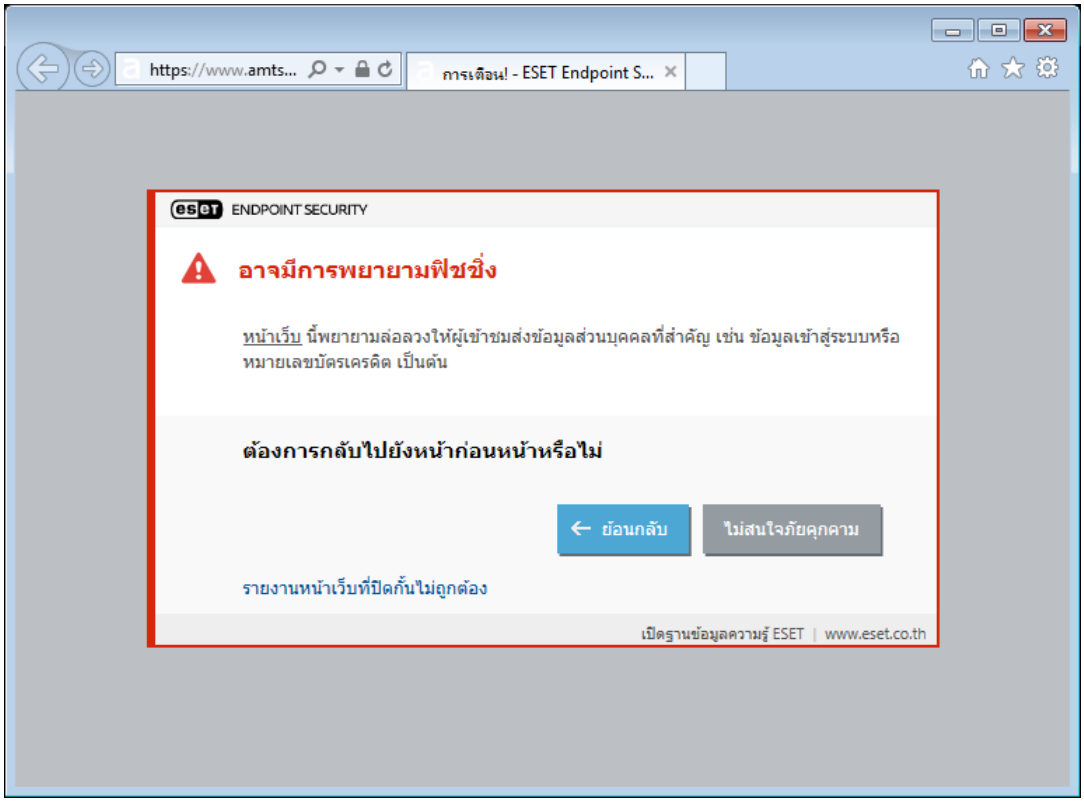
ฟิชชิ่งเป็นกิจกรรมที่ผิดกฎหมายซึ่งใช้กลลวงทางสังคม (การจัดการผู้ใช้เพื่อให้ได้ข้อมูลที่เป็นความลับ) ฟิชชิ่งถูกใช้เพื่อให้ได้รับสิทธิ์การเข้าถึงข้อมูลสำคัญ เช่น หมายเลขบัญชีธนาคาร หมายเลข PIN เป็นต้น ดูข้อมูลเพิ่มเติมได้ใน ประมวลศัพท์ ESET Endpoint Security มีการป้องกันฟิชชิ่ง ซึ่งจะปิดกั้นหน้าเว็บที่เผยแพร่เนื้อหาประเภทดังกล่าว

การป้องกันฟิชชิ่งจะเปิดใช้งานตามค่าเริ่มต้น การตั้งค่านี้สามารถกำหนดค่าได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเว็บไซต์**

โปรดไปที่ บทความฐานความรู้ ของเราหากต้องการข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันฟิชชิ่งใน ESET Endpoint Security

การเข้าถึงเว็บไซต์ฟิชชิ่ง

เมื่อคุณเข้าถึงเว็บไซต์ฟิชชิ่งที่ระบบรู้จัก เว็บเบราว์เซอร์ของคุณจะแสดงข้อความต่อไปนี้ หากคุณยังต้องการเข้าถึงเว็บไซต์ ให้คลิก **ละเว้นภัยคุกคาม** (ไม่แนะนำ)



ตามค่าเริ่มต้น เว็บไซต์ที่อาจเป็นฟิชชิ่งซึ่งมีการกำหนดว่าเป็นบัญชีปลอดภัยจะหมดอายุหลังจากผ่านไปหลายชั่วโมง หากต้องการอนุญาตเว็บไซต์อย่างถาวร โปรดใช้เครื่องมือ การจัดการที่อยู่ URL จาก การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเว็บ** > **การจัดการที่อยู่ URL** > **รายการที่อยู่** คลิก **แก้ไข** และเพิ่มเว็บไซต์ที่คุณต้องการแก้ไขลงในรายการ

รายงานไซต์ฟิชชิ่ง

ลิงก์ **หน้ารายงานที่ถูกบล็อกไม่ถูกต้อง** ช่วยให้คุณรายงานเว็บไซต์ที่ตรวจพบอย่างไม่ถูกต้องว่าเป็นภัยคุกคามได้

อีกวิธีหนึ่งคือ คุณสามารถส่งเว็บไซต์ทางอีเมล ส่งอีเมลไปที่ samples@eset.com โปรดใช้ชื่อเรื่องที่อธิบายชัดเจนและให้ข้อมูลเกี่ยวกับเว็บไซต์มากที่สุดเท่าที่จะเป็นไปได้ (ตัวอย่างเช่น เว็บไซต์ที่คุณใช้อ้างอิง คุณทราบเรื่องเว็บไซต์นี้

ได้อย่างไร เป็นต้น)

นำเข้าและส่งออกการตั้งค่า

คุณสามารถนำเข้าหรือส่งออกไฟล์การกำหนดค่า .xml ของ ESET Endpoint Security ที่กำหนดเองของคุณจากเมนู **การตั้งค่า**

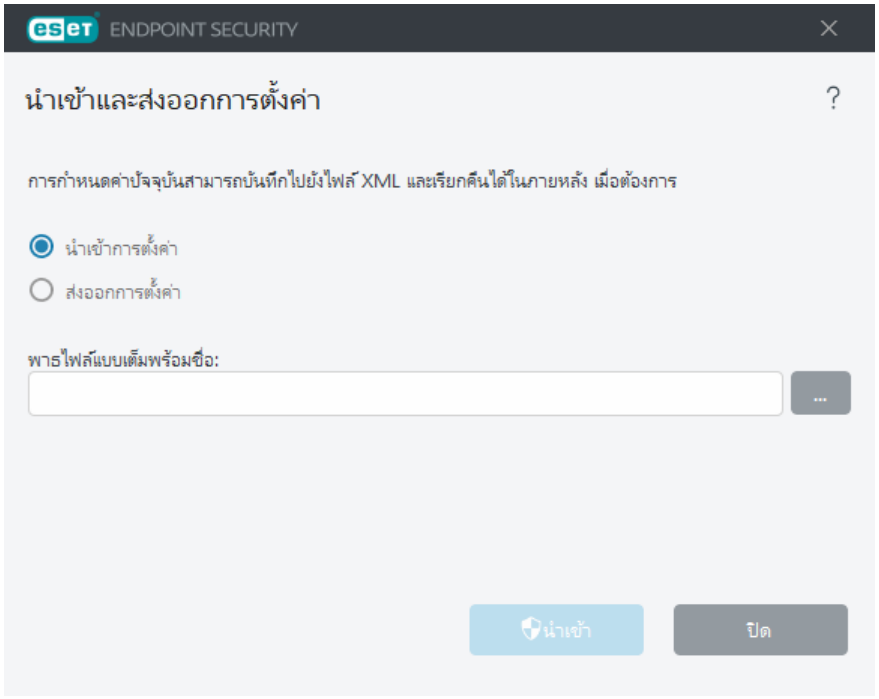
> **คำแนะนำพร้อมภาพประกอบ**
> ดู นำเข้าหรือส่งออกการตั้งค่าการกำหนดค่า ESET โดยใช้ไฟล์ .xml สำหรับคำแนะนำพร้อมภาพประกอบที่แสดงในภาษาอังกฤษและภาษาอื่นๆ

การนำเข้าและการส่งออกไฟล์การกำหนดค่าจะมีประโยชน์ในกรณีที่คุณต้องสำรองการกำหนดค่าปัจจุบันของ ESET Endpoint Security เพื่อใช้งานในภายหลัง ตัวเลือกการตั้งค่าการส่งออกยังใช้งานได้สะดวกเมื่อคุณต้องการใช้การกำหนดค่าที่ต้องการในระบบต่างๆ คุณสามารถนำเข้าไฟล์ .xml ได้อย่างง่ายดายเพื่อส่งการตั้งค่าดังกล่าว

หากต้องการนำเข้าการกำหนดค่า ใน หน้าต่างหลักของโปรแกรม ให้คลิก **ตั้งค่า** > **นำเข้าและส่งออกการตั้งค่า** แล้วเลือก **นำเข้าการตั้งค่า** ป้อนชื่อไฟล์ของไฟล์การกำหนดค่า หรือคลิกปุ่ม **...** เพื่อเรียกดูไฟล์การกำหนดค่าที่คุณต้องการนำเข้า

หากต้องการส่งออกการกำหนดค่า ใน หน้าต่างหลักของโปรแกรม ให้คลิก **ตั้งค่า** > **นำเข้าและส่งออกการตั้งค่า** เลือก **ส่งออกการตั้งค่า** และพิมพ์พาธไฟล์แบบเต็มพร้อมชื่อ คลิก **...** เพื่อไปยังตำแหน่งในคอมพิวเตอร์เพื่อบันทึกไฟล์การกำหนดค่า

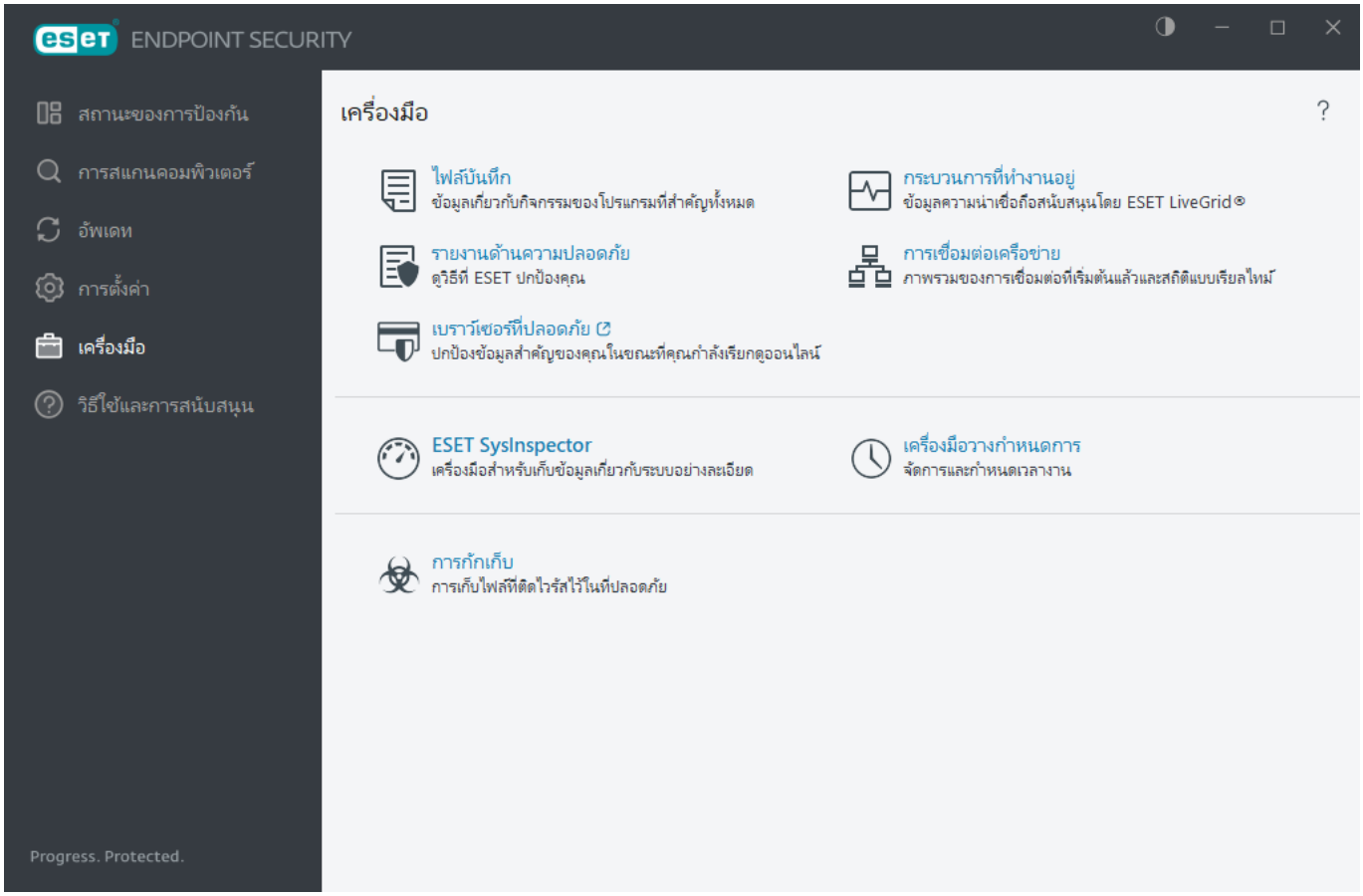
> คุณอาจพบข้อผิดพลาดในขณะส่งออกการตั้งค่า ถ้าคุณไม่มีสิทธิ์เพียงพอในการเขียนไฟล์ที่ส่งออกไปยังไดเรกทอรีที่ระบุ



เครื่องมือ

เมนู **เครื่องมือ** ประกอบด้วยโมดูลที่ช่วยให้การจัดการโปรแกรมง่ายขึ้นและมีตัวเลือกเพิ่มเติมสำหรับผู้ใช้ขั้นสูง

- ไฟล์บันทึก
- กระบวนการที่ทำงานอยู่ (หาก ESET LiveGrid® ได้เปิดใช้อยู่ใน ESET Endpoint Security)
- รายงานด้านความปลอดภัย (สำหรับเอ็นพอยต์ที่ไม่มีการจัดการ)
- การเชื่อมต่อเครือข่าย (หาก ไฟร์วอลล์ เปิดใช้งานอยู่ใน ESET Endpoint Security)
- ESET SysInspector
- เครื่องมือวางกำหนดการ
- ส่งตัวอย่างเพื่อวิเคราะห์ – อนุญาตให้คุณส่งไฟล์ที่น่าสงสัยไปยังห้องปฏิบัติการวิจัยของ ESET เพื่อวิเคราะห์ (อาจไม่สามารถใช้งานได้ขึ้นอยู่กับการกำหนดค่าของ ESET LiveGrid®)
- กักเก็บ



ไฟล์บันทึก

ไฟล์บันทึกประกอบด้วยข้อมูลเกี่ยวกับเหตุการณ์ของโปรแกรมที่สำคัญที่เกิดขึ้นทั้งหมด และให้ภาพรวมของภัยคุกคามที่พบ การบันทึกเป็นเครื่องมือที่จำเป็นในการวิเคราะห์ระบบ การตรวจหาภัยคุกคาม และการแก้ไขปัญหา การบันทึกนั้นดำเนินการในพื้นหลังโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ข้อมูลจะถูกบันทึกตามการตั้งค่าความละเอียดของการบันทึกปัจจุบัน ผู้ใช้สามารถดูข้อความและบันทึกได้โดยตรงจากระบบ ESET Endpoint Security และยังสามารถอาร์ไคฟ์ไฟล์บันทึกได้

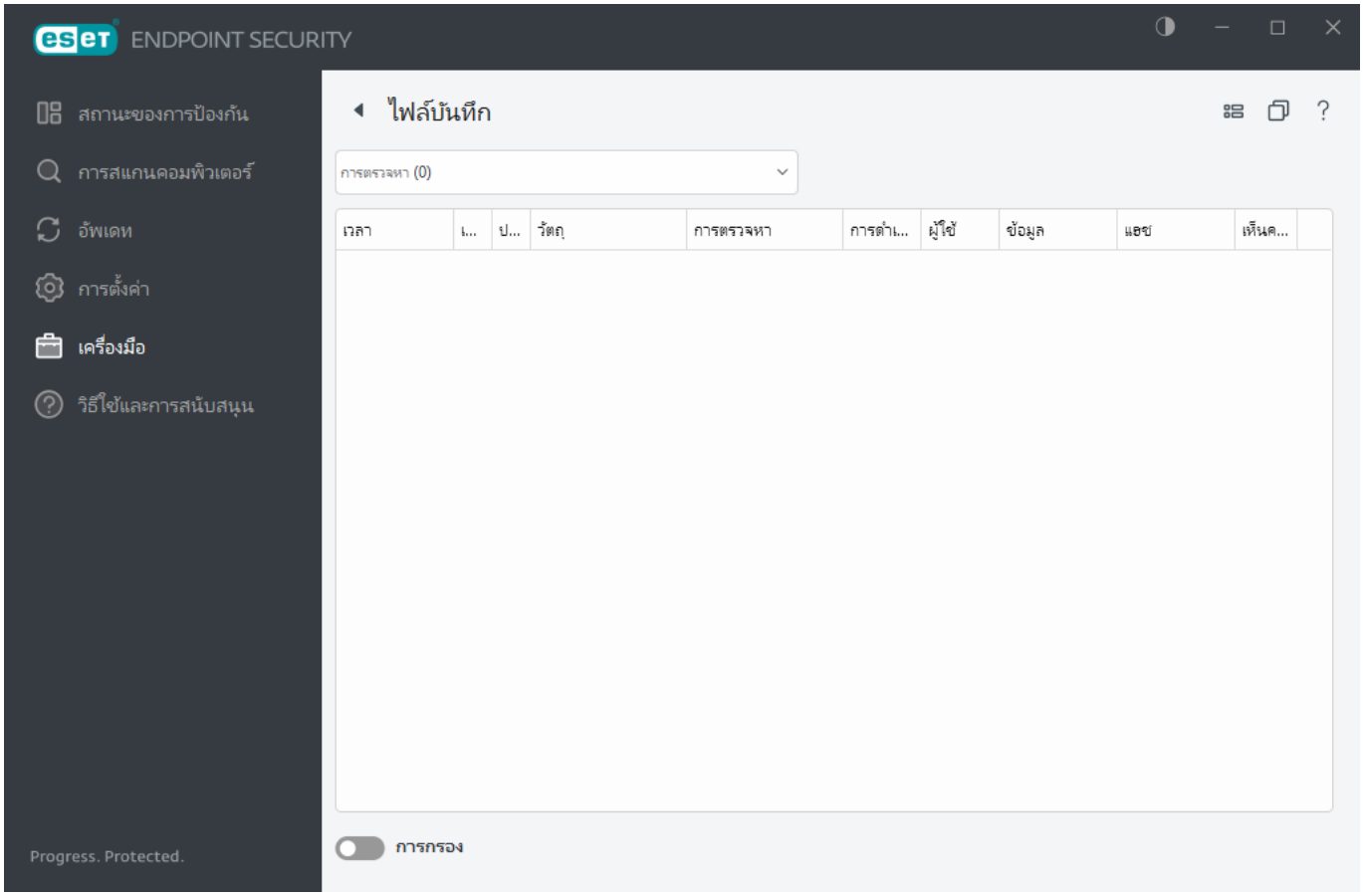
ไฟล์บันทึกนั้นสามารถเข้าถึงได้จากหน้าต่างโปรแกรมหลักโดยคลิก **เครื่องมือ** > **ไฟล์บันทึก** เลือกประเภทการบันทึกที่ต้องการโดยใช้เมนูแบบเลื่อนลง **บันทึก** มีบันทึกที่ใช้ได้ดังต่อไปนี้:

- **การตรวจหา** – บันทึกนี้จะให้ข้อมูลเกี่ยวกับการตรวจหาและการแฝงตัวที่ตรวจพบโดยโมดูล ESET Endpoint Security ข้อมูลจะประกอบด้วยเวลาที่ตรวจพบ ชื่อของการตรวจหา ตำแหน่ง การดำเนินการ และชื่อของผู้ใช้ที่เข้าสู่ระบบในเวลาที่การแฝงตัวถูกตรวจพบ คลิกสองครั้งที่รายการบันทึกเพื่อแสดงรายละเอียดต่างๆ ในหน้าต่างใหม่ การแฝงตัวยังไม่ถูกกำจัดจะทำเครื่องหมายด้วยข้อความสีแดงบนพื้นหลังสีแดงอ่อนเสมอ การแฝงตัวที่ถูกกำจัดแล้วจะทำเครื่องหมายด้วยข้อความสีเหลืองบนพื้นหลังสีขาว PUA ที่ไม่ถูกกำจัดหรือแอปพลิเคชั่นที่อาจไม่ปลอดภัยถูกทำเครื่องหมายด้วยข้อความสีเหลืองบนพื้นหลังสีขาว

- **เหตุการณ์** – การทำงานที่สำคัญทั้งหมดซึ่งดำเนินการโดย ESET Endpoint Security จะบันทึกไว้ในบันทึกเหตุการณ์ บันทึกเหตุการณ์จะมีข้อมูลเกี่ยวกับเหตุการณ์และข้อผิดพลาดที่เกิดขึ้นในโปรแกรม ตัวเลือกนี้ได้รับการออกแบบมาเพื่อช่วยให้ผู้ดูแลระบบและผู้ใช้แก้ไขปัญหาได้ ข้อมูลที่พบในส่วนนี้มักจะช่วยให้คุณพบทางแก้ปัญหาที่เกิดขึ้นในโปรแกรม
- **การสแกนคอมพิวเตอร์** – ผลลัพธ์การสแกนทั้งหมดจะแสดงในหน้าต่างนี้ แต่ละบรรทัดจะแสดงถึงการควบคุมคอมพิวเตอร์หนึ่งรายการ คลิกสองครั้งที่รายการใดก็ได้เพื่อดูรายละเอียดของการสแกนนั้น
- **ไฟล์ที่ถูกปิดกั้น** – มีบันทึกของไฟล์ที่ถูกปิดกั้นและไม่สามารถเข้าถึงได้เมื่อเชื่อมต่อกับ ESET Enterprise Inspector โปรโตคอลจะแสดงถึงเหตุผลและโมดูลที่มาที่ปิดกั้นไฟล์ รวมถึงแอพพลิเคชันและผู้ใช้ที่ใช้งานไฟล์นั้น สำหรับข้อมูลเพิ่มเติม โปรดดู ESET Enterprise Inspector คู่มือผู้ใช้ออนไลน์
- **ไฟล์ที่ส่งแล้ว** – จะมีบันทึกของไฟล์ที่ถูกส่งไปยังESET LiveGrid® หรือ ESET LiveGuard เพื่อการวิเคราะห์
- **บันทึกการตรวจสอบ** – บันทึกแต่ละรายการจะบรรจุข้อมูลเกี่ยวกับวันที่และเวลาเมื่อมีการเปลี่ยนแปลง ประเภทของการเปลี่ยนแปลง คำอธิบาย แหล่งที่มาและผู้ใช้ ดูบันทึกการตรวจสอบสำหรับข้อมูลเพิ่มเติม
- **HIPS** – มีบันทึกของกฎบางกฎที่ทำเครื่องหมายสำหรับการบันทึก โปรโตคอลแสดงแอพพลิเคชันที่เรียกการทำงาน ผลลัพธ์ (ไม่ว่ากฎจะได้รับอนุญาตหรือถูกห้าม) และชื่อของกฎที่สร้างขึ้น
- **เบราว์เซอร์ปลอดภัย**–มีบันทึกของไฟล์ที่ไม่ได้รับการยืนยัน / ไฟล์ที่ไม่น่าเชื่อถือที่โหลดในเบราว์เซอร์
- **การป้องกันเครือข่าย** – บันทึกไฟร์วอลล์จะแสดงการโจมตีระยะไกลทั้งหมดที่ตรวจพบด้วย การป้องกันการโจมตีเครือข่าย หรือ ไฟร์วอลล์ในส่วนนี้คุณจะพบข้อมูลเกี่ยวกับการโจมตีคอมพิวเตอร์ของคุณทั้งหมด คอลัมน์ เหตุการณ์ จะมีรายการของการโจมตีที่ถูกตรวจ คอลัมน์ แหล่งข้อมูล จะแจ้งให้คุณทราบเพิ่มเติมเกี่ยวกับผู้โจมตี คอลัมน์ โปรโตคอล จะเปิดเผยโปรโตคอลการสื่อสารที่ใช้สำหรับการโจมตี การวิเคราะห์ของการบันทึกการป้องกันเครือข่ายอาจช่วยคุณตรวจหาความพยายามในการแฝงตัวในระบบได้ทันเวลา สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการโจมตีทางเครือข่าย โปรดดูที่ IDS และตัวเลือกขั้นสูง

- **เว็บไซต์ที่ถูกกรอง** – ซึ่งรายการนี้มีประโยชน์ถ้าคุณต้องการดูรายการเว็บไซต์ที่ถูกบล็อกโดยฟีเจอร์ การป้องกันการเข้าถึงเว็บไซต์ หรือ การควบคุมการเข้าถึงเว็บไซต์ ในบันทึกเหล่านี้ คุณจะเห็นข้อมูลเวลา, URL, ผู้ใช้ และแอพพลิเคชันที่เปิดการเชื่อมต่อกับเว็บไซต์หนึ่ง

- **การป้องกันสแปมอีเมลไคลเอ็นต์** – มีบันทึกที่เกี่ยวข้องกับข้อความอีเมลที่ทำเครื่องหมายเป็นสแปม
- **การควบคุมการเข้าถึงเว็บไซต์** – แสดงที่อยู่ URL ที่ปิดกั้นและอนุญาต รวมถึงรายละเอียดเกี่ยวกับวิธีการจัดประเภทที่อยู่เหล่านั้น คอลัมน์ การทำงานที่ดำเนินการ จะบอกคุณว่ากฎการกรองนั้นทำงานอย่างไร
- **การควบคุมอุปกรณ์** – มีบันทึกของสื่อหรืออุปกรณ์ที่ถอดเข้าออกได้ที่เชื่อมต่ออยู่กับคอมพิวเตอร์ เฉพาะอุปกรณ์ที่มีกฎการควบคุมอุปกรณ์เท่านั้นที่จะถูกบันทึกลงในไฟล์บันทึก หากกฎไม่ตรงกับอุปกรณ์ที่เชื่อมต่อจะไม่มีการสร้างรายการบันทึกสำหรับอุปกรณ์ที่เชื่อมต่อ นอกจากนี้ คุณยังสามารถดูรายละเอียดต่างๆ เช่น ประเภทอุปกรณ์ หมายเลขซีเรียล ชื่อผู้ขาย และขนาดของสื่อ (หากมี)



เลือกเนื้อหาของบันทึกใดก็ได้ แล้วกด `Ctrl + C` **เพื่อคัดลอกเนื้อหานั้นไปยังคลิปบอร์ด** กด`Ctrl + Shift` ค้างไว้เพื่อเลือกหลายรายการ

คลิก **การกรอง** เพื่อเปิดหน้าต่าง การกรองบันทึก ที่ซึ่งคุณสามารถกำหนดเกณฑ์การกรองได้

คลิกขวาบนบันทึกใดบันทึกหนึ่งเพื่อเปิดเมนูบริบท ตัวเลือกต่อไปนี้จะสามารถใช้ได้ในเมนูบริบท:

- **แสดง** – แสดงข้อมูลโดยละเอียดยิ่งขึ้นเกี่ยวกับบันทึกที่เลือกในหน้าต่างใหม่
- **กรองบันทึกเดียวกัน** – หลังจากเปิดใช้งานตัวกรองนี้ คุณจะเห็นเฉพาะบันทึกประเภทเดียวกันเท่านั้น (การวินิจฉัย การเตือน เป็นต้น)
- **กรอง** – หลังจากคลิกตัวเลือกนี้ คุณจะสามารถกำหนดเกณฑ์การกรองสำหรับรายการบันทึกบางรายการได้ใน หน้าต่างการกรองบันทึก
- **เปิดใช้งานตัวกรอง** – เปิดใช้งานการตั้งค่าตัวกรอง
- **ปิดใช้งานการกรอง** - ล้างการตั้งค่าตัวกรองทั้งหมด (ดังที่อธิบายไว้ที่ด้านบน)
- **คัดลอก/คัดลอกทั้งหมด** – คัดลอกข้อมูลเกี่ยวกับบันทึกทั้งหมดในหน้าต่าง
- **คัดลอกเซลล์** คัดลอกเนื้อหาของเซลล์ที่คลิกขวา
- **ลบ/ลบทั้งหมด** – ลบบันทึกที่เลือกหรือบันทึกทั้งหมดที่ปรากฏ ซึ่งการดำเนินการนี้ต้องใช้สิทธิ์ของผู้ดูแลระบบ

- **ส่งออก** – ส่งออกข้อมูลเกี่ยวกับบันทึกในรูปแบบ XML
- **ส่งออกทั้งหมด** - ส่งออกข้อมูลเกี่ยวกับการบันทึกในรูปแบบ XML ทั้งหมด
- **ค้นหา/ค้นหาถัดไป/ค้นหาก่อนหน้า** – หลังจากคลิกตัวเลือกนี้ คุณสามารถกำหนดเกณฑ์การกรองโดยใช้หน้าต่างการกรองบันทึกเพื่อทำไฮไลต์รายการเฉพาะได้
- **สร้างการยกเว้น** – สร้าง การยกเว้นการตรวจหาโดยใช้วิซาร์ด (ไม่สามารถใช้งานได้กับการตรวจหามัลแวร์)

การกรองบันทึก

คลิก **การกรอง** ใน **เครื่องมือ** > **ไฟล์บันทึก** เพื่อระบุเกณฑ์การกรอง

คุณลักษณะบันทึกการกรองจะช่วยให้คุณค้นหาข้อมูลที่คุณกำลังค้นหาได้ โดยเฉพาะเมื่อมีบันทึกจำนวนมาก คุณลักษณะนี้จะช่วยการบันทึกต่างๆ แคบลง เช่น หากคุณกำลังค้นหาประเภทของเหตุการณ์เฉพาะ สถานะหรือระยะเวลา คุณสามารถกรองบันทึกได้โดยการระบุตัวเลือกการค้นหาบางอย่าง เฉพาะบันทึกที่เกี่ยวข้อง (อิงตามตัวเลือกการค้นหาเหล่านั้น) จะแสดงในหน้าต่างไฟล์บันทึกเท่านั้น

พิมพ์คำหลักที่คุณกำลังค้นหาในช่อง **ค้นหาข้อความ** ใช้เมนู **ค้นหาในคอลัมน์** แบบเลื่อนลงเพื่อค้นหาอย่างละเอียด เลือกหนึ่งในบันทึกจากเมนู **บันทึกประเภทของการบันทึก** แบบเลื่อนลง ระบุ**ช่วงเวลา** จากผลลัพธ์ที่คุณต้องการแสดง คุณยังสามารถใช้ตัวเลือกการค้นหาต่อไป เช่น **ตรงทั้งคำเท่านั้น** หรือ **ตรงตามตัวพิมพ์**

ค้นหาข้อความ

พิมพ์สตริง (คำหรือส่วนหนึ่งของคำ) จะแสดงเฉพาะบันทึกที่มีสตริงนี้ บันทึกอื่นๆ จะถูกยกเว้น

ค้นหาในคอลัมน์

เลือกคอลัมน์ที่จะได้รับการพิจารณาเมื่อทำการค้นหา คุณสามารถตรวจสอบหนึ่งคอลัมน์ที่จะใช้ในการค้นหาได้

ประเภทบันทึก

เลือกการบันทึกหนึ่งประเภทจากเมนูแบบเลื่อนลง:

- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- **มีข้อมูล** – บันทึกข้อความแจ้งข้อมูล รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน

- **ข้อผิดพลาด** – ข้อผิดพลาด เช่น "เกิดข้อผิดพลาดขณะดาวน์โหลดไฟล์" และข้อผิดพลาดร้ายแรงจะถูกบันทึก
- **ร้ายแรง** – บันทึกเฉพาะข้อผิดพลาดร้ายแรง (ข้อผิดพลาดในการเริ่มต้นการป้องกันไวรัส

ช่วงเวลา

ระบุช่วงเวลาที่คุณต้องการให้แสดงผลลัพธ์

- **ไม่ระบุ** (ค่าเริ่มต้น) - ไม่ค้นหาภายในช่วงเวลา ค้นหาการบันทึกทั้งหมด
- **วันสุดท้าย**
- **สัปดาห์ที่แล้ว**
- **เดือนที่แล้ว**
- **ช่วงเวลา** - คุณสามารถระบุเวลาที่แน่นอนได้ (จาก: และ ถึง:) เพื่อกรองเฉพาะบันทึกของช่วงเวลาที่ระบุไว้

ตรงทั้งคำเท่านั้น

ใช้ช่องทำเครื่องหมายนี้ถ้าคุณต้องการค้นหาทั้งคำเพื่อให้ได้ผลลัพธ์ที่แม่นยำยิ่งขึ้น

ตรงตามตัวพิมพ์

เปิดใช้งาน ตัวเลือกนี้ หากคุณจำเป็นต้องใช้ตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ในขณะกรอง เมื่อคุณกำหนดค่าตัวเลือกการกรอง/การค้นหาแล้ว ให้คลิก**ตกลง** เพื่อแสดงบันทึกการกรองหรือค้นหา เพื่อเริ่มการค้นหา ไฟล์บันทึกจะถูกค้นหาจากบนลงล่าง เริ่มจากตำแหน่งปัจจุบันของคุณ (บันทึกที่ถูกไฮไลท์) การค้นหาจะหยุดเมื่อค้นหาบันทึกที่ตรงกันอย่างแรก กด**F3** เพื่อค้นหาบันทึกถัดไปหรือคลิกขวา แล้วเลือก**ค้นหา** เพื่อระบุตัวเลือกการค้นหาของคุณอีกครั้ง

บันทึกการตรวจสอบ

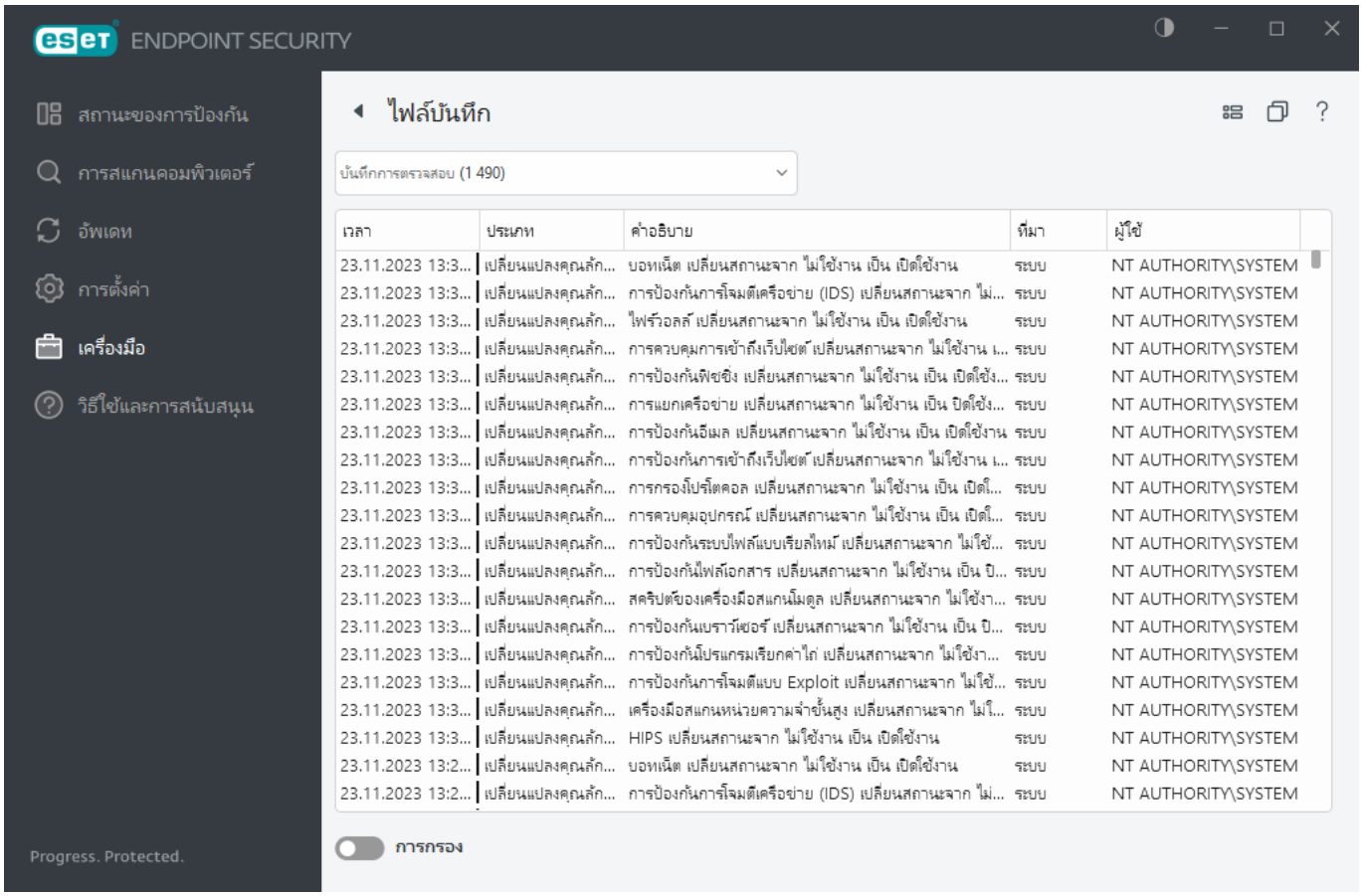
ในสภาพแวดล้อมขององค์กรโดยปกติมักจะมีผู้ใช้หลายรายที่ถูกระบุสิทธิ์การเข้าถึงสำหรับการกำหนดค่าอุปกรณ์ปลายทาง โดยตั้งแต่ที่การแก้ไขของการกำหนดค่าผลิตภัณฑ์อาจส่งผลกระทบอย่างมากต่อวิธีการดำเนินการของผลิตภัณฑ์ดังนั้นจึงเป็นเรื่องสำคัญที่ผู้ดูแลระบบต้องติดตามการเปลี่ยนแปลงที่เกิดขึ้นโดยผู้ใช้เพื่อช่วยผู้ดูแลระบบในการระบุ แก้ไข ทั้งยังป้องกันการเกิดปัญหาที่เหมือนหรือคล้ายคลึงกันในอนาคตได้อย่างรวดเร็ว

บันทึกการตรวจสอบคือการบันทึกประเภทใหม่สำหรับการระบุต้นทางของปัญหา บันทึกการตรวจสอบจะติดตามการเปลี่ยนแปลงในสถานะการกำหนดค่าและการปกป้องแล้วบันทึกสแนปชอตสำหรับอ้างอิงในภายหลัง

บันทึกการตรวจสอบ คลิก **เครื่องมือ** ในเมนูหลักแล้วคลิก **ไฟล์บันทึก** แล้วเลือก **บันทึกการตรวจสอบ** จากเมนูแบบเลื่อนลง

บันทึกการตรวจสอบมีข้อมูลเกี่ยวกับ:

- เวลา - เมื่อมีการเปลี่ยนแปลงเกิดขึ้น
- ประเภท - การตั้งค่าหรือคุณสมบัติประเภทใดที่มีการเปลี่ยนแปลง
- คำอธิบาย - สิ่งใดที่มีการเปลี่ยนแปลงและส่วนใดของการตั้งค่าที่มีการเปลี่ยนแปลงพร้อมกับจำนวนของการตั้งค่าที่มีการเปลี่ยนแปลง
- ที่มา - ที่มาของการเปลี่ยนแปลงคือที่ใด
- ผู้ใช้ - ใครทำการเปลี่ยนแปลง



คลิกขวาที่ประเภทของ **การตั้งค่าที่มีการเปลี่ยนแปลง**ใดๆ พิมพ์ข้อความ audit log ในหน้าต่างไฟล์บันทึกแล้วเลือก **แสดงการเปลี่ยนแปลง** จากเมนูบริบทเพื่อแสดงข้อมูลโดยละเอียดเกี่ยวกับการเปลี่ยนแปลงที่เกิดขึ้น นอกจากนี้ คุณยังสามารถเรียกคืนการเปลี่ยนแปลงการตั้งค่าได้โดยคลิก **เรียกคืน** จากเมนูบริบท (ไม่สามารถใช้งานได้สำหรับผลิตภัณฑ์ที่จัดการโดย ESET PROTECT) หากคุณเลือก **ลบทั้งหมด** จากเมนูบริบท บันทึกที่มีข้อมูล

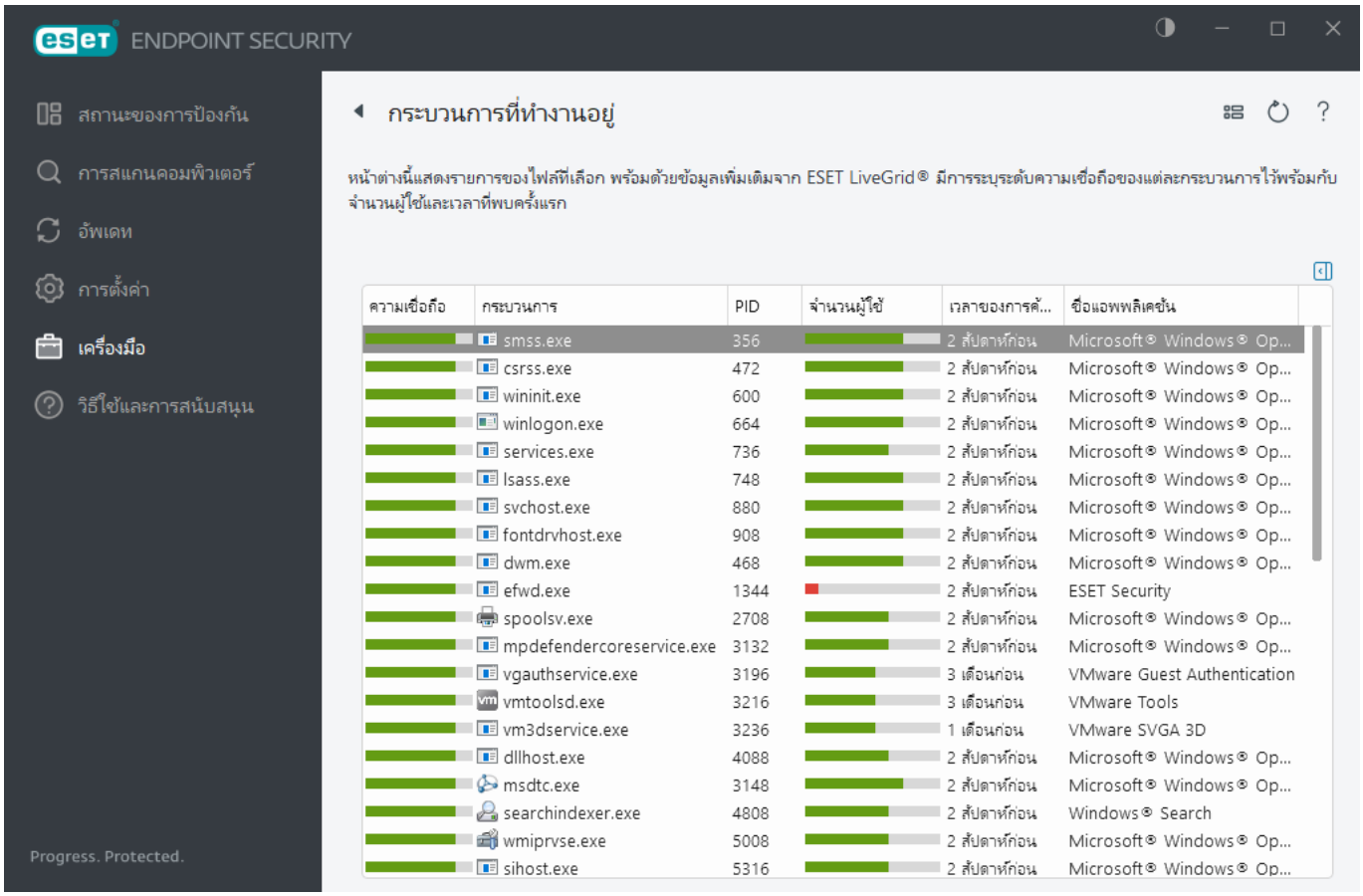
เกี่ยวกับการกระทำนี้จะถูกสร้างขึ้น

หาก **การปรับปรุงประสิทธิภาพไฟล์บันทึกโดยอัตโนมัติ** ถูกเปิดใช้งานใน การตั้งค่าขั้นสูง > **เครื่องมือ** > **ไฟล์บันทึก** บันทึกการตรวจสอบจะถูกจัดเรียงเช่นเดียวกับบันทึกอื่นๆ โดยอัตโนมัติ

หาก **การลบบันทึกที่เก่ากว่า (วัน) โดยอัตโนมัติ** ถูกเปิดใช้งานใน การตั้งค่าขั้นสูง > **เครื่องมือ** > **ไฟล์บันทึก** รายการบันทึกที่เก่ากว่าจำนวนวันที่ระบุจะถูกลบโดยอัตโนมัติ

กระบวนการที่ทำงานอยู่

กระบวนการที่ทำงานอยู่จะแสดง โปรแกรมหรือกระบวนการ ที่ทำงานอยู่ในคอมพิวเตอร์ของคุณ และทำให้ ESET ได้รับรู้ข้อมูลเกี่ยวกับการบุกรุกใหม่ได้ทันทีและต่อเนื่อง ESET Endpoint Security จะแสดงข้อมูลโดยละเอียดเกี่ยวกับกระบวนการที่ทำงานอยู่เพื่อคุ้มครองผู้ใช้ด้วยเทคโนโลยี ESET LiveGrid®



ความเชื่อถือ – ในกรณีส่วนใหญ่ ESET Endpoint Security และเทคโนโลยี ESET LiveGrid® จะกำหนดระดับความเสี่ยงให้กับวัตถุ (ไฟล์ กระบวนการ รหัสรีจิสตรี เป็นต้น) โดยใช้ชุดกฎการวิเคราะห์พฤติกรรมที่ตรวจสอบลักษณะของวัตถุแต่ละรายการ จากนั้นจะชั่งน้ำหนักโอกาสที่จะเป็นกิจกรรมที่เป็นอันตราย จากการวิเคราะห์พฤติกรรมเหล่านี้ วัตถุจะได้รับการกำหนดระดับความเชื่อถือตั้งแต่ 9 – มีความเชื่อถือมากที่สุด (สีเขียว) จนถึง 0 – มีความเชื่อถือ

น้อยที่สุด (สีแดง)

กระบวนการ – ชื่ออิมเมจของโปรแกรมหรือกระบวนการที่เรียกใช้อยู่บนคอมพิวเตอร์ของคุณในขณะนี้ คุณสามารถใช้โปรแกรมจัดการงาน Windows เมื่อต้องการดูกระบวนการทั้งหมดที่ทำงานอยู่บนคอมพิวเตอร์ คุณสามารถเปิดตัวจัดการงานได้โดยการคลิกขวาที่พื้นที่ว่างบนแถบงานแล้วคลิกตัวจัดการงาน หรือโดยการกดปุ่ม **Ctrl+Shift+Esc** บนแป้นพิมพ์ของคุณ

PID – เป็น ID ของกระบวนการที่เรียกใช้อยู่ในระบบปฏิบัติการ Windows

i แอพพลิเคชันที่รู้จักที่ทำเครื่องหมายเป็น สีเขียว หมายถึงไม่ติดไวรัสแน่นอน (รายการที่ปลอดภัย) และจะถูกยกเว้นจากการสแกน เนื่องจากแอพพลิเคชันนี้จะช่วยปรับปรุงความเร็วในการสแกนของการสแกนคอมพิวเตอร์ตามต้องการหรือการป้องกันระบบไฟล์แบบเรียลไทม์ในคอมพิวเตอร์ของคุณ

จำนวนผู้ใช้ – จำนวนผู้ใช้ที่ใช้แอพพลิเคชันที่ระบุ ข้อมูลนี้ได้รับการรวบรวมโดยเทคโนโลยี ESET LiveGrid®

เวลาที่ค้นพบ – ระยะเวลาตั้งแต่เทคโนโลยี ESET LiveGrid® ค้นพบแอพพลิเคชัน

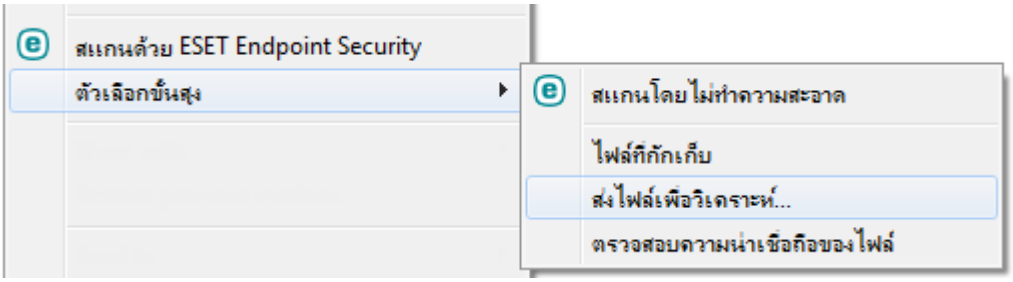
i เมื่อทำเครื่องหมายแอพพลิเคชันเป็นความปลอดภัยระดับ ไม่ทราบ (สีส้ม) ไม่ได้หมายความว่าจะเป็นซอฟต์แวร์ที่เป็นอันตรายเสมอไป โดยปกติแล้วจะเป็นแอพพลิเคชันใหม่ ถ้าคุณไม่แน่ใจเกี่ยวกับไฟล์ดังกล่าว ให้ใช้คุณลักษณะ ส่งไฟล์เพื่อวิเคราะห์ เพื่อส่งไฟล์ดังกล่าวไปยังห้องปฏิบัติการไวรัสของ ESET หากตรวจพบว่าไฟล์เป็นแอพพลิเคชันที่เป็นอันตราย การตรวจหาไฟล์นี้จะถูกเพิ่มในการอัพเดทกลไกตรวจหาที่กำลังจะมีขึ้น

ชื่อแอพพลิเคชัน – ชื่อที่กำหนดของโปรแกรมหรือกระบวนการ

เมื่อคลิกที่แอพพลิเคชันที่ด้านล่าง ข้อมูลต่อไปนี้จะปรากฏที่ด้านล่างของหน้าต่าง:

- **พาธ** – ตำแหน่งของแอพพลิเคชันบนคอมพิวเตอร์ของคุณ
- **คำอธิบาย** – ลักษณะของไฟล์ตามคำอธิบายของระบบปฏิบัติการ
- **เวอร์ชัน** – ข้อมูลจากผู้เผยแพร่แอพพลิเคชัน
- **บริษัท** – ชื่อของผู้ขายหรือกระบวนการแอพพลิเคชัน
- **ผลิตภัณฑ์** – ชื่อแอพพลิเคชันและ/หรือชื่อทางธุรกิจ
- **ขนาด** – ขนาดของไฟล์ในหน่วย kB (กิโลไบต์) หรือ MB (เมกะไบต์)
- **สร้างเมื่อ** – วันที่และเวลาที่สร้างแอพพลิเคชัน
- **แก้ไขล่าสุดเมื่อ** – วันที่และเวลาล่าสุดที่แก้ไขแอพพลิเคชัน

i นอกจากนี้ ยังสามารถตรวจสอบความเชื่อถือในไฟล์ที่ไม่ได้เป็นโปรแกรม/กระบวนการที่ทำงานอยู่ - ทำเครื่องหมายที่ไฟล์ที่คุณต้องการตรวจสอบ แล้วคลิกขวาที่ไฟล์ และจาก เมนูบริบท ให้เลือก **ตัวเลือกขั้นสูง > ตรวจสอบความเชื่อถือของไฟล์โดยใช้ ESET LiveGrid®**



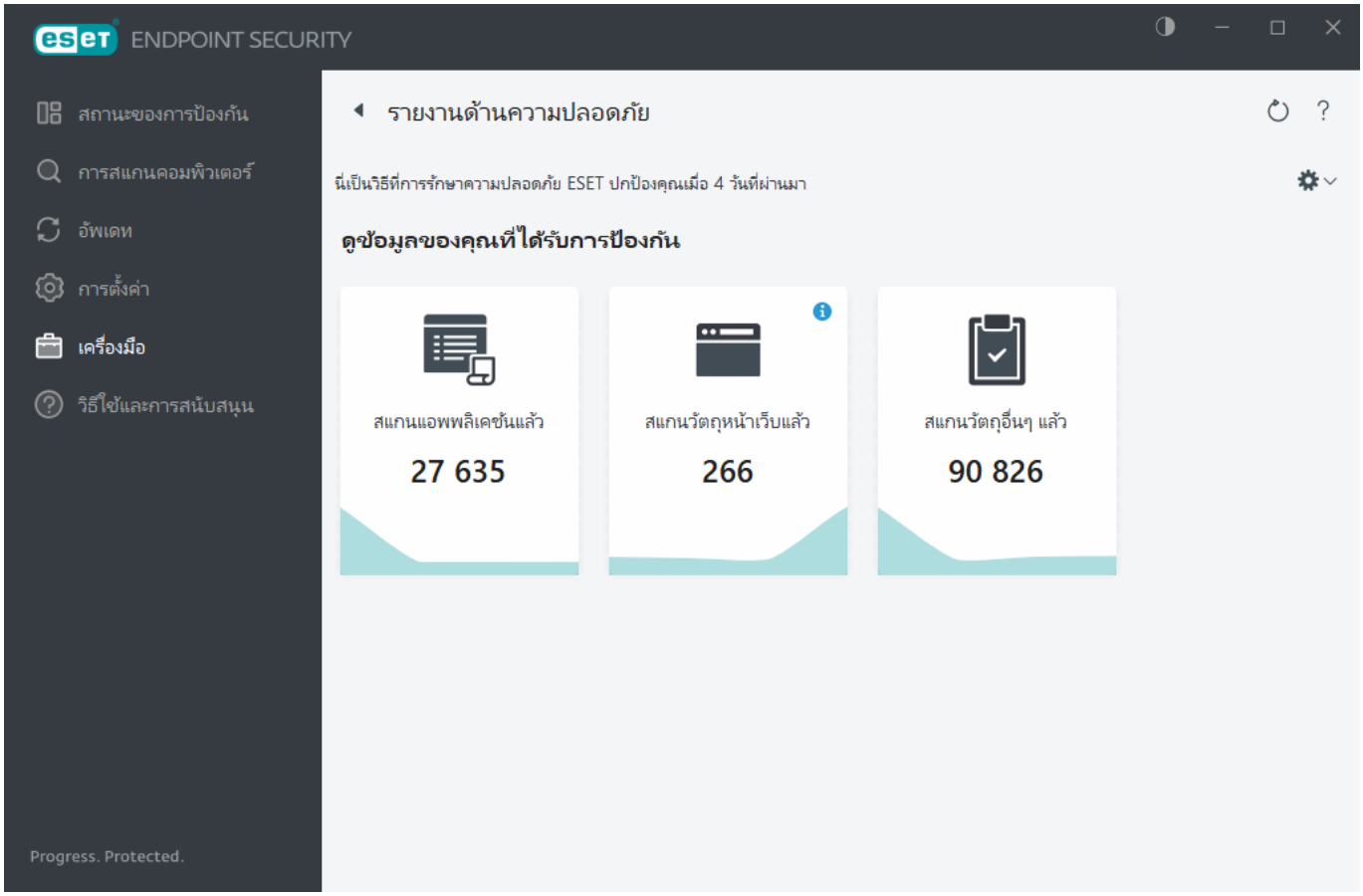
รายงานด้านความปลอดภัย

คุณลักษณะนี้จะให้ภาพรวมสถิติสำหรับประเภทต่อไปนี้:

- **หน้าเว็บที่ถูกปิดกั้น** – แสดงจำนวนหน้าเว็บที่ถูกปิดกั้น (URL ของ PUA ที่อยู่ในบัญชีดำ, ฟิชชิ่ง, เราเตอร์ที่ถูกเจาะระบบ, IP หรือใบรับรอง)
- **ตรวจพบวัตถุอีเมลติดไวรัส** – แสดงจำนวนวัตถุอีเมลติดไวรัสที่ตรวจพบ
- **หน้าเว็บในการควบคุมการเข้าถึงเว็บไซต์ถูกปิดกั้น** – แสดงจำนวนหน้าเว็บที่ถูกปิดกั้นในการควบคุมการเข้าถึงเว็บไซต์
- **ตรวจพบ PUA** – แสดงจำนวนแอพพลิเคชันที่อาจไม่พึงประสงค์ (PUA)
- **ตรวจพบอีเมลสแปม** – แสดงจำนวนอีเมลสแปมที่ตรวจพบ
- **เอกสารที่สแกนแล้ว** – แสดงจำนวนออบเจ็กต์เอกสารที่สแกนแล้ว
- **สแกนแอพพลิเคชันแล้ว** – แสดงจำนวนวัตถุที่สามารถเรียกใช้ที่สแกนแล้วได้
- **สแกนวัตถุอื่นๆ แล้ว** – แสดงจำนวนวัตถุอื่นๆ ที่สแกนแล้ว
- **สแกนวัตถุหน้าเว็บแล้ว** – แสดงจำนวนวัตถุหน้าเว็บที่สแกนแล้ว
- **สแกนวัตถุอีเมลแล้ว** – แสดงจำนวนวัตถุอีเมลที่สแกนแล้ว

ลำดับของประเภทเหล่านี้จะเป็นไปตามค่าตัวเลขจากสูงสุดไปต่ำสุด ประเภทที่มีค่าเป็นศูนย์จะไม่ถูกแสดง คลิก **แสดงเพิ่มขึ้น** เพื่อขยายและแสดงประเภทที่ซ่อนอยู่

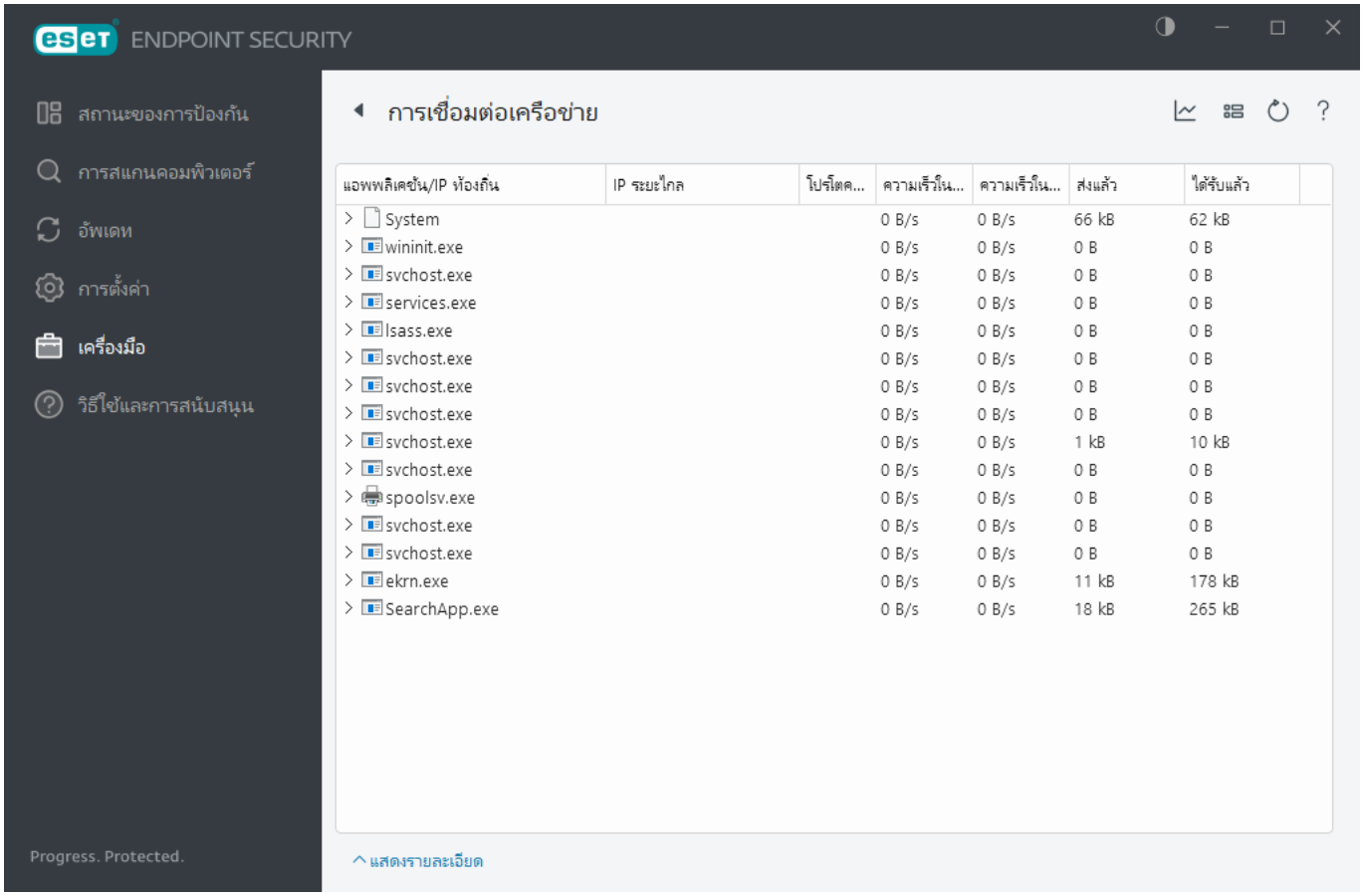
เมื่อคลิกที่ล้อเฟือง ที่มุมขวาบน คุณจะสามารถ **เปิด/ปิดใช้งานการแจ้งเตือนรายงานด้านความปลอดภัย** หรือเลือกว่าจะให้โปรแกรมแสดงข้อมูลจาก 30 วันที่ผ่านมาหรือนับจากที่คุณเริ่มเปิดใช้งานผลิตภัณฑ์ได้ หากคุณติดตั้ง ESET Endpoint Security เป็นเวลาน้อยกว่า 30 วัน คุณจะสามารถเลือกจำนวนวันนับจากที่คุณเริ่มติดตั้งผลิตภัณฑ์ได้เท่านั้น ช่วงเวลา 30 วันจะถูกเลือกตามค่าเริ่มต้น



รีเซ็ตข้อมูล จะล้างสถิติทั้งหมดและลบข้อมูลที่มีอยู่ในรายงานด้านความปลอดภัยออก การทำงานนี้จำเป็นต้องได้รับการยืนยันยกเว้นในกรณีที่คุณยกเลิกการเลือกตัวเลือก **ถามก่อนรีเซ็ตสถิติ** ใน การตั้งค่าขั้นสูง > **การแจ้งเตือน > การแจ้งเตือนแบบโต้ตอบ > ข้อความการยืนยัน**

การเชื่อมต่อเครือข่าย

ในส่วนการเชื่อมต่อเครือข่าย คุณจะพบรายการการเชื่อมต่อที่ใช้งานอยู่และรอดำเนินการ ส่วนนี้ช่วยให้คุณสามารถควบคุมแอพพลิเคชันทั้งหมดที่สร้างการเชื่อมต่อขาออก



คลิกไอคอนกราฟ เพื่อเปิด กิจกรรมเครือข่าย

บรรทัดแรกจะแสดงชื่อของแอพพลิเคชันและความเร็วในการรับส่งข้อมูล หากต้องการดูรายการการเชื่อมต่อที่สร้างจากแอพพลิเคชัน (และข้อมูลเพิ่มเติมโดยละเอียด) ให้คลิกที่ **>**

คอลัมน์

แอพพลิเคชัน/IP ในระบบ – ชื่อของแอพพลิเคชัน ที่อยู่ IP ในระบบ และพอร์ตการสื่อสาร

IP ระยะไกล – ที่อยู่ IP และเลขที่พอร์ตของคอมพิวเตอร์ระยะไกล

โปรโตคอล – โปรโตคอลการรับส่งข้อมูลที่ใช้

เพิ่มความเร็ว/ลดความเร็ว – ความเร็วปัจจุบันของข้อมูลขาเข้าและขาออก

ส่ง/ได้รับ – ปริมาณข้อมูลที่แลกเปลี่ยนภายในการเชื่อมต่อ

แสดงรายละเอียด – เลือกตัวเลือกนี้เพื่อแสดงข้อมูลโดยละเอียดเกี่ยวกับการเชื่อมต่อที่เลือก

การเลือกแอพพลิเคชันหรือที่อยู่ IP ในหน้าจอการเชื่อมต่อเครือข่าย แล้วคลิกขวาบนหน้าจอ จะแสดงเมนูบริบทที่มีโครงสร้างดังต่อไปนี้:

แปลค่าชื่อโฮสต์ – ถ้าเป็นไปได้ ที่อยู่เครือข่ายทั้งหมดจะแสดงในรูปแบบ DNS ไม่ใช่ในรูปแบบที่อยู่ IP ที่เป็นตัวเลข

แสดงเฉพาะการเชื่อมต่อ TCP – รายการจะแสดงเฉพาะการเชื่อมต่อที่อยู่ในชุดโปรโตคอล TCP

แสดงการเชื่อมต่อของรายชื่อ – เลือกตัวเลือกนี้เพื่อแสดงเฉพาะการเชื่อมต่อที่ยังไม่ได้เริ่มต้นการสื่อสาร แต่ระบบได้เปิดพอร์ตและกำลังรอการเชื่อมต่ออยู่

แสดงการเชื่อมต่อภายในคอมพิวเตอร์ – เลือกตัวเลือกนี้เพื่อแสดงเฉพาะการเชื่อมต่อที่คอมพิวเตอร์ระยะไกลเป็นระบบภายใน หรือเรียกว่าการเชื่อมต่อ localhost

คลิกขวาที่การเชื่อมต่อเพื่อดูตัวเลือกอื่นๆ ที่มีอยู่:

ปฏิเสธการสื่อสารสำหรับการเชื่อมต่อ – สิ้นสุดการสื่อสารที่เริ่มต้น ตัวเลือกนี้จะสามารถใช้ได้หลังจากคลิกที่การเชื่อมต่อที่ใช้งานเท่านั้น

ความเร็วในการรีเฟรช – เลือกความถี่ในการรีเฟรชการเชื่อมต่อที่ใช้งาน

รีเฟรชทันที – โหลดหน้าต่าง การเชื่อมต่อในเครือข่าย อีกครั้ง

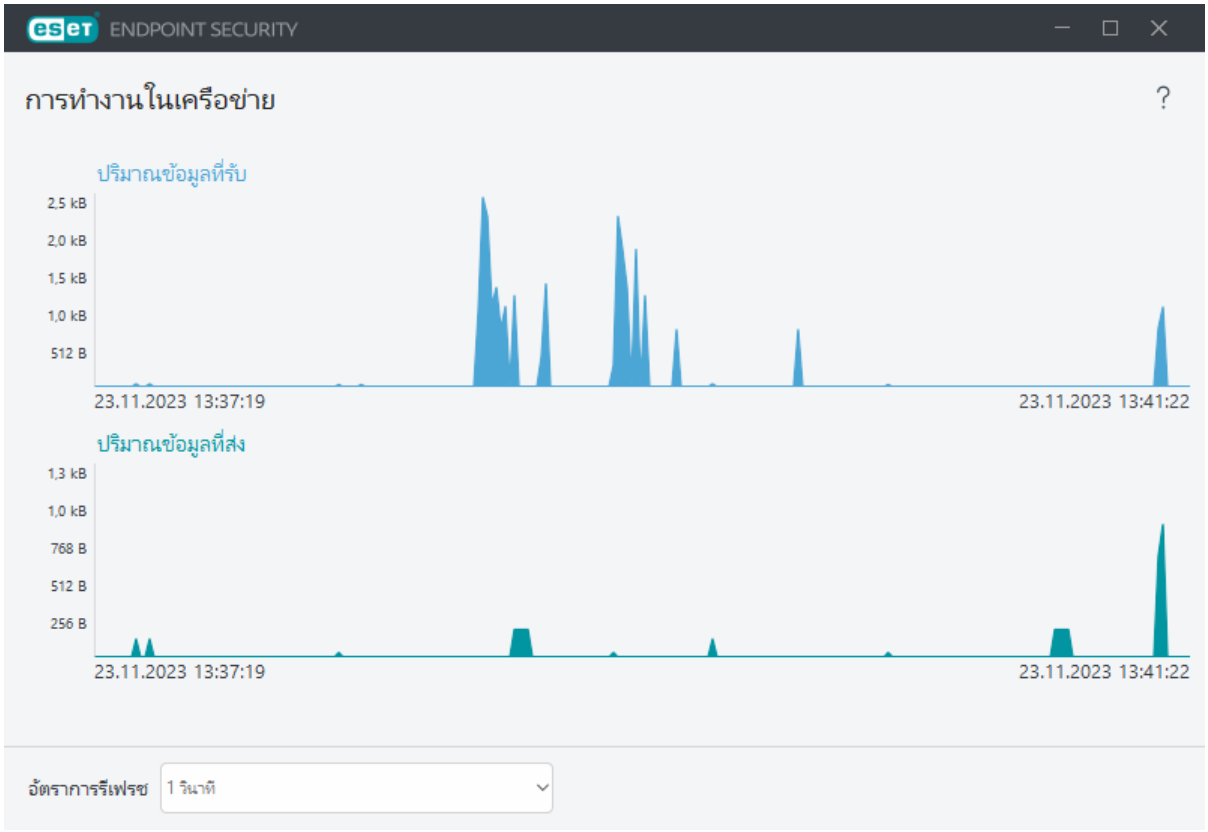
ตัวเลือกต่อไปนี้จะสามารถใช้ได้หลังจากคลิกแอพพลิเคชันหรือกระบวนการเท่านั้น ไม่ใช่คลิกที่การเชื่อมต่อที่ใช้งาน:

ปฏิเสธการสื่อสารสำหรับกระบวนการชั่วคราว – ปฏิเสธการเชื่อมต่อปัจจุบันสำหรับแอพพลิเคชันที่ระบุ ถ้าเริ่มต้นการเชื่อมต่อใหม่แล้ว ไฟร์วอลล์จะใช้กฎที่กำหนดไว้ล่วงหน้า คุณสามารถดูคำอธิบายของการตั้งค่าในส่วน กฎของไฟร์วอลล์ ได้

อนุญาตการสื่อสารสำหรับกระบวนการชั่วคราว – อนุญาตการเชื่อมต่อปัจจุบันสำหรับแอพพลิเคชันที่ระบุ ถ้าเริ่มต้นการเชื่อมต่อใหม่แล้ว ไฟร์วอลล์จะใช้กฎที่กำหนดไว้ล่วงหน้า คุณสามารถดูคำอธิบายของการตั้งค่าในส่วน กฎของไฟร์วอลล์ ได้

การทำงานในเครือข่าย

หากต้องการดู **กิจกรรมเครือข่าย** ปัจจุบันในรูปแบบกราฟ ให้คลิก **เครื่องมือ** > **การเชื่อมต่อเครือข่าย** แล้วคลิกไอคอนกราฟ ด้านล่างของกราฟจะมีเส้นบอกเวลา ซึ่งบันทึกกิจกรรมเครือข่ายแบบเรียลไทม์ตามช่วงเวลาที่เลือกไว้ หากต้องการเปลี่ยนช่วงเวลา ให้เลือกค่าที่เกี่ยวข้องจากเมนูแบบเลื่อนลง **อัตราการรีเฟรช**



ตัวเลือกที่ใช้ได้มีดังนี้:

- **1 วินาที** – กราฟจะรีเฟรชทุกวินาทีและเส้นบอกเวลาจะครอบคลุม 4 นาทีที่ผ่านมา
- **1 นาที (24 ชั่วโมงก่อนหน้า)** – กราฟรีเฟรชทุกนาที และเส้นบอกเวลาจะครอบคลุม 24 ชั่วโมงที่ผ่านมา
- **1 ชั่วโมง (เดือนก่อนหน้า)** – กราฟจะรีเฟรชทุกชั่วโมงและเส้นบอกเวลาจะครอบคลุมหนึ่งเดือนที่ผ่านมา

แกนแนวตั้งของกราฟจะแสดงปริมาณข้อมูลที่ได้รับหรือปริมาณข้อมูลที่ส่ง วางเมาส์เหนือกราฟเพื่อดูจำนวนข้อมูลที่ได้รับ/ข้อมูลที่ส่งในเวลาที่กำหนดโดยละเอียด

ESET SysInspector

ESET SysInspector เป็นแอพพลิเคชันที่จะตรวจสอบคอมพิวเตอร์ของคุณอย่างละเอียด และรวบรวมข้อมูลโดยละเอียดเกี่ยวกับองค์ประกอบของระบบ เช่น ไดรเวอร์และแอพพลิเคชัน การเชื่อมต่อของเครือข่าย หรือรายการรีจิสตรีที่สำคัญ และประเมินระดับความเสี่ยงขององค์ประกอบแต่ละรายการ ข้อมูลนี้จะช่วยระบุสาเหตุของการทำงานของระบบที่น่าสงสัยที่อาจเกิดจากการใช้ซอฟต์แวร์หรือฮาร์ดแวร์ร่วมกันไม่ได้ หรือการติดไวรัสจากมัลแวร์ หากต้องการเรียนรู้วิธีใช้ ESET SysInspector โปรดดูวิธีใช้ออนไลน์ของ ESET SysInspector

หน้าต่าง ESET SysInspector จะแสดงข้อมูลเกี่ยวกับบันทึกดังต่อไปนี้:

- **เวลา** – เวลาของการสร้างบันทึก

- **ความคิดเห็น** – ความคิดเห็นสั้นๆ
- **ผู้ใช้** – ชื่อของผู้ใช้ที่สร้างบันทึก
- **สถานะ** – สถานะของการสร้างบันทึก

การทำงานที่ใช้ได้มีดังนี้:

- **แสดง** – เปิดบันทึกที่เลือกใน ESET SysInspector คุณยังสามารถคลิกขวาที่ไฟล์บันทึกที่ให้และเลือก **แสดง** จากเมนูบริบท
- **สร้าง** – สร้างบันทึกใหม่ รอจนกระทั่ง ESET SysInspector ถูกสร้างขึ้น (สถานะ **สร้างแล้ว**) ก่อนพยายามเข้าถึงบันทึก ระบบจะจัดเก็บบันทึกไว้ใน C:\ProgramData\ESET\ESET Security\SysInspector
- **ลบ** – ลบบันทึกที่เลือกออกจากรายการ

รายการต่อไปนี้จะนำมาใช้ได้จากเมนูบริบทเมื่อเลือกไฟล์บันทึกหนึ่งไฟล์หรือหลายไฟล์:

- **แสดง** – เปิดบันทึกที่เลือกใน ESET SysInspector (ทำงานเช่นเดียวกับการคลิกสองครั้งที่บันทึก)
- **สร้าง** – สร้างบันทึกใหม่ รอจนกระทั่ง ESET SysInspector ถูกสร้างขึ้น (สถานะ **สร้างแล้ว**) ก่อนพยายามเข้าถึงบันทึก
- **ลบ** – ลบบันทึกที่เลือกออกจากรายการ
- **ลบทั้งหมด** – ลบบันทึกทั้งหมด
- **ส่งออก** – ส่งออกบันทึกไปยังไฟล์ .xml หรือ .xml ที่บีบอัด

เครื่องมือวางกำหนดการ

เครื่องมือวางกำหนดการจะจัดการและเรียกใช้งานตามกำหนดการโดยใช้การกำหนดค่าและคุณสมบัติที่กำหนดไว้ล่วงหน้า

เครื่องมือวางกำหนดการณ์นั้นสามารถเข้าถึงได้จาก หน้าต่างโปรแกรมหลัก ของ ESET Endpoint Security โดยคลิก **เครื่องมือ** > **เครื่องมือวางกำหนดการณ์ เครื่องมือวางกำหนดการ** มีรายการงานตามกำหนดการทั้งหมด และคุณสมบัติของการกำหนดค่า เช่น วันที่ที่กำหนดไว้ล่วงหน้า เวลา และโปรไฟล์การสแกนที่ใช้

เครื่องมือวางกำหนดการจะทำหน้าที่ในการวางกำหนดการงานต่อไปนี้: การอัพเดทกลไกตรวจหา การสแกนงาน การตรวจสอบไฟล์การเริ่มต้นของระบบ และการบำรุงรักษาบันทึก คุณสามารถเพิ่มหรือลบงานได้โดยตรงจากหน้าต่างของเครื่องมือวางกำหนดการหลัก (คลิก **เพิ่มงาน** หรือ **ลบ** ที่ส่วนล่างของหน้าต่าง) คลิกขวาที่ใดก็ได้ในหน้าต่างของเครื่องมือวางกำหนดการเพื่อดำเนินการดังต่อไปนี้: แสดงข้อมูลเป็นรายละเอียด ทำงานทันที เพิ่มงานใหม่ และ

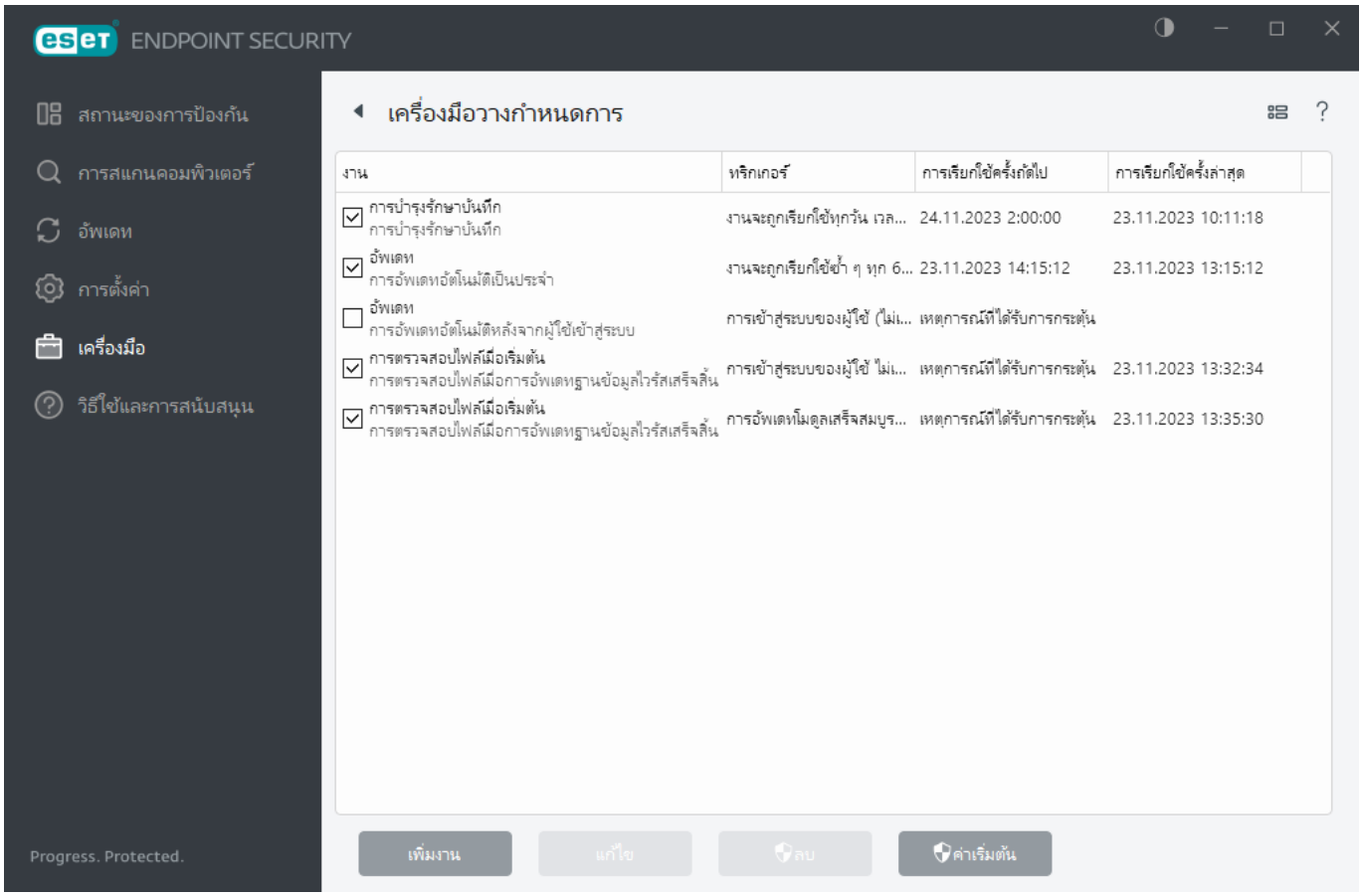
ลบงานที่มีอยู่ ใช้ช่องทำเครื่องหมายที่ด้านหน้าของแต่ละรายการเพื่อเปิด/ปิดการทำงาน

ตามค่าเริ่มต้น งานตามกำหนดการต่อไปนี้จะปรากฏใน **เครื่องมือวางกำหนดการ**:

- **การบำรุงรักษาการบันทึก**
- **การอัพเดทอัตโนมัติเป็นประจำ**
- **การอัพเดทอัตโนมัติหลังจากเชื่อมต่อผ่านหมายเลขโทรศัพท์**
- **การอัพเดทอัตโนมัติหลังจากผู้ใช้เข้าสู่ระบบ**
- **การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้น** (หลังจากการเข้าสู่ระบบของผู้ใช้)
- **การตรวจสอบไฟล์เริ่มต้นอัตโนมัติ** (หลังจากการอัพเดทโมดูลสำเร็จ)

i ใน ESET PROTECT การหน่วงเวลาเรียกใช้งานแบบสุ่มสามารถใช้เพื่อลดภาระงานของเซิร์ฟเวอร์เมื่อเรียกใช้งาน โดยเฉพาะในเครือข่ายขนาดใหญ่ ตัวเลือกนี้ทำให้คุณสามารถกำหนดกรอบเวลาที่จะเรียกใช้งานในทั้งเครือข่าย แทนที่จะเรียกใช้งานบนเวิร์กสเตชันทั้งหมดในทั้งเครือข่ายในเวลาเดียวกัน เมื่อมีการเรียกใช้งาน ค่าเวลาที่ตั้งไว้จะถูกแบ่งออกแบบสุ่ม เพื่อจัดสรรเวลาในการเรียกใช้งานที่ไม่ซ้ำกันสำหรับแต่ละเวิร์กสเตชันในเครือข่าย วิธีนี้จะช่วยป้องกันภาระงานสูงเกินไปในเซิร์ฟเวอร์และปัญหาที่เกี่ยวข้อง (เช่น เซิร์ฟเวอร์บางชนิดอาจรายงานการโจมตีแบบ DoS เมื่อทำงานอัพเดทจำนวนมากในเวลาเดียวกันในเวิร์กสเตชันในทั้งเครือข่าย)

เมื่อต้องการแก้ไขการกำหนดค่าของงานตามกำหนดการที่มีอยู่ (ทั้งค่าเริ่มต้นและที่ผู้ใช้กำหนด) ให้คลิกขวาที่งานและคลิก **แก้ไข** หรือเลือกงานที่คุณต้องการแก้ไขและคลิกปุ่ม **แก้ไข**



เพิ่มงานใหม่

1. คลิกที่ **เพิ่มงาน** ที่ส่วนล่างของหน้าต่าง
2. ป้อนชื่อของงาน
3. เลือกงานที่ต้องการจากเมนูแบบเลื่อนลง:

- **เรียกใช้แอพพลิเคชันภายนอก** – วางกำหนดการเรียกใช้แอพพลิเคชันภายนอก
- **การบำรุงรักษาบันทึก** - ไฟล์บันทึกยังมีข้อมูลที่เหลืออยู่จากบันทึกที่ลบแล้ว งานนี้จะช่วยเพิ่มประสิทธิภาพการบันทึกในไฟล์บันทึกเป็นประจำเพื่อให้มีประสิทธิภาพการทำงานเพิ่มขึ้น
- **การตรวจสอบไฟล์เมื่อเริ่มต้น** – ตรวจสอบไฟล์ที่อนุญาตให้เรียกใช้ได้เมื่อเริ่มต้นระบบหรือเข้าสู่ระบบ
- **สร้างสแนปชอตสถานะของคอมพิวเตอร์** – สร้างสแนปชอตคอมพิวเตอร์ของ ESET SysInspector โดยรวบรวมข้อมูลโดยละเอียดเกี่ยวกับองค์ประกอบของระบบ (ตัวอย่างเช่น ไดรเวอร์ แอพพลิเคชัน) และประเมินระดับความเสี่ยงขององค์ประกอบแต่ละรายการ
- **การสแกนคอมพิวเตอร์ตามต้องการ** – ดำเนินการสแกนคอมพิวเตอร์ของไฟล์และโฟลเดอร์บนคอมพิวเตอร์ของคุณ
- **อัพเดท** – กำหนดเวลาอัพเดทงานโดยการอัพเดทกลไกตรวจหาและโมดูลโปรแกรม

4. เปิดสวิตซ์ **เปิดใช้งาน** ถ้าคุณต้องการเปิดใช้งาน (คุณสามารถดำเนินการในภายหลังได้ด้วยการเลือก/ยกเลิกการเลือกกล่องทำเครื่องหมายในรายการงานตามกำหนดการ) ให้คลิก **ถัดไป** และเลือกหนึ่งในตัวเลือกเวลา:

- **หนึ่งครั้ง** – งานจะดำเนินการตามวันและเวลาที่กำหนดไว้ล่วงหน้า
- **ซ้ำ** – งานจะดำเนินการตามระยะเวลาที่กำหนด
- **รายวัน** – งานจะเรียกใช้ซ้ำทุกวันตามเวลาที่กำหนด
- **รายสัปดาห์** – งานจะเรียกใช้ตามวันที่และเวลาที่เลือก
- **ตามเหตุการณ์** – งานจะดำเนินการตามเหตุการณ์ที่กำหนด

5. **เลือก ข้ามงานเมื่อทำงานด้วยแบตเตอรี่** เพื่อลดการใช้ทรัพยากรของระบบในขณะที่แล็ปท็อปทำงานด้วยพลังงานแบตเตอรี่ งานจะถูกเรียกใช้ตามวันที่และเวลาที่ระบุในช่อง **การเรียกใช้งาน** หากงานไม่สามารถทำงานได้ตามเวลาที่กำหนดไว้ล่วงหน้า คุณสามารถระบุช่วงเวลาที่จะให้มีการดำเนินการอีกครั้ง:

- **เมื่อเวลาที่กำหนดไว้ครั้งต่อไป**
- **เร็วที่สุดเท่าที่ทำได้**
- **ทันที หากเวลาตั้งแต่ครั้งที่แล้วมากกว่าค่าที่ระบุ** (สามารถกำหนดระยะเวลาได้โดยใช้ช่องเลื่อน **เวลาตั้งแต่การใช้งานครั้งล่าสุด**)

หากต้องการตรวจสอบงานที่กำหนดเวลาไว้ ให้คลิกขวาที่งานแล้วคลิก **แสดงรายละเอียดงาน**

ตัวเลือกการสแกนตามกำหนดการ

ในหน้าต่างนี้คุณสามารถระบุตัวเลือกขั้นสูงสำหรับงานสแกนคอมพิวเตอร์ที่กำหนดเวลาได้

เมื่อต้องการเรียกใช้การสแกนโดยไม่ทำความสะอาด ให้คลิก **การตั้งค่าขั้นสูง** แล้วเลือก **สแกนโดยไม่ต้องทำความสะอาด** ประวัติการสแกนจะถูกบันทึกลงในบันทึกการสแกน

เมื่อเลือก **ละเว้นการยกเว้น** ไฟล์ที่มีนามสกุลไฟล์ที่ไม่ได้รับการสแกนก่อนหน้านี้จะถูกสแกนโดยไม่มีข้อยกเว้น

คุณสามารถกำหนดการดำเนินการที่จะเกิดขึ้นโดยอัตโนมัติได้หลังจากสแกนเสร็จโดยใช้เมนูแบบเลื่อนลง:

- **ไม่มีการทำงาน** – หลังจากสแกนเสร็จสิ้น จะไม่มีการดำเนินการใดๆ
- **ปิดระบบ** – คอมพิวเตอร์จะปิดหลังจากสแกนเสร็จสิ้น
- **เริ่มต้นระบบใหม่** – ปิดโปรแกรมที่เปิดอยู่ทั้งหมด แล้วเริ่มต้นคอมพิวเตอร์ใหม่หลังจากสแกนเสร็จสิ้น
- **เริ่มต้นระบบใหม่หากจำเป็น** – คอมพิวเตอร์จะเริ่มต้นใหม่หากจำเป็นเพื่อทำความสะอาดภัยคุกคามที่ตรวจพบเท่านั้น
- **บังคับให้รีบูต** – บังคับให้ปิดโปรแกรมที่เปิดอยู่ทั้งหมดโดยไม่ต้องรอการโต้ตอบของผู้ใช้และรีสตาร์ทคอมพิวเตอร์หลังจากการสแกนเสร็จสิ้น
- **บังคับให้รีบูตเครื่องหากจำเป็น** – คอมพิวเตอร์จะเริ่มต้นใหม่หากจำเป็นเพื่อทำความสะอาดภัยคุกคามที่ตรวจพบเท่านั้น
- **พักเครื่อง** – บันทึกเซสชันของคุณและปรับคอมพิวเตอร์เข้าสู่สถานะการใช้พลังงานต่ำเพื่อให้คุณสามารถกลับมาทำงานต่อได้อย่างรวดเร็ว
- **ไฮเบอร์เนต** – รวบรวมทุกสิ่งที่คุณได้เรียกใช้บน RAM แล้วย้ายมาไว้ในไฟล์พิเศษบนฮาร์ดไดรฟ์ของคุณ คอมพิวเตอร์ของคุณจะปิด แต่จะกลับมายังสถานะก่อนหน้านี้ในครั้งต่อไปที่คุณเริ่มคอมพิวเตอร์อีกครั้ง

> i การดำเนินการ **พักการทำงาน** หรือ **ไฮเบอร์เนต** จะใช้งานได้ตามการตั้งค่าระบบปฏิบัติการสำหรับการเปิดเครื่องและพักการทำงานของคอมพิวเตอร์หรือความสามารถของคอมพิวเตอร์/แล็ปท็อปของคุณ โปรดทราบว่าคอมพิวเตอร์ขณะพักการทำงานยังคงเป็นคอมพิวเตอร์ที่ทำงานอยู่ คอมพิวเตอร์ยังทำงานพื้นฐานและใช้ไฟฟ้าเมื่อคอมพิวเตอร์ทำงานด้วยแบตเตอรี่ หากต้องการยืดอายุการใช้งานแบตเตอรี่ ตัวอย่างเช่น เมื่ออยู่นอกสำนักงาน เราขอแนะนำให้คุณใช้ตัวเลือกไฮเบอร์เนต

เลือก **ไม่สามารถยกเลิกการสแกนได้** เพื่อปฏิเสธผู้ใช้ที่ไม่ได้รับสิทธิ์ให้หยุดการดำเนินการหลังจากการสแกน

เลือกตัวเลือก **ผู้ใช้สามารถหยุดการสแกนเป็นเวลา (นาที)** หากคุณต้องการให้ผู้ใช้ในจำนวนที่จำกัดหยุดสแกนคอมพิวเตอร์ชั่วความตามระยะเวลาที่กำหนดไว้

ดูเพิ่มเติมที่ ความคืบหน้าของการสแกน

ภาพรวมของงานตามกำหนดการ

หน้าต่างข้อความนี้จะแสดงข้อมูลอย่างละเอียดเกี่ยวกับงานตามกำหนดการที่เลือกเมื่อคุณคลิกสองครั้งที่งานที่กำหนดเองหรือคลิกขวาที่งานตามกำหนดการที่กำหนดเองแล้วคลิก **แสดงรายละเอียดงาน**

รายละเอียดงาน

พิมพ์ใน **ชื่องาน** แล้วเลือกหนึ่งในตัวเลือก **ประเภทงาน** จากนั้นคลิก **ถัดไป**:

- **เรียกใช้แอพพลิเคชันภายนอก** – วางกำหนดการเรียกใช้แอพพลิเคชันภายนอก
- **การบำรุงรักษาบันทึก** - ไฟล์บันทึกยังมีข้อมูลที่เหลืออยู่จากบันทึกที่ลบแล้ว งานนี้จะช่วยเพิ่มประสิทธิภาพการบันทึกในไฟล์บันทึกเป็นประจำเพื่อให้มีประสิทธิภาพการทำงานเพิ่มขึ้น
- **การตรวจสอบไฟล์เมื่อเริ่มต้น** – ตรวจสอบไฟล์ที่อนุญาตให้เรียกใช้ได้เมื่อเริ่มต้นระบบหรือเข้าสู่ระบบ
- **สร้างสแนปชอตสถานะของคอมพิวเตอร์** – สร้างสแนปชอตคอมพิวเตอร์ของ ESET SysInspector โดยรวบรวมข้อมูลโดยละเอียดเกี่ยวกับองค์ประกอบของระบบ (ตัวอย่างเช่น ไดรเวอร์ แอพพลิเคชัน) และประเมินระดับความเสี่ยงขององค์ประกอบแต่ละรายการ
- **การสแกนคอมพิวเตอร์ตามต้องการ** – ดำเนินการสแกนคอมพิวเตอร์ของไฟล์และโฟลเดอร์บนคอมพิวเตอร์ของคุณ
- **อัพเดท** – วางกำหนดการงานการอัพเดทโดยการอัพเดทโมดูลเหล่านี้

เวลางาน

งานจะเริ่มดำเนินการซ้ำๆ ตามระยะเวลาที่กำหนดไว้ เลือกหนึ่งในตัวเลือกเวลาต่อไปนี้:

- **หนึ่งครั้ง** – งานจะดำเนินการเพียงครั้งเดียวตามวันที่และเวลาที่กำหนดไว้ล่วงหน้า
- **ซ้ำ** – งานจะเริ่มดำเนินการตามช่วงเวลาที่ระบุ (เป็นชั่วโมง)
- **รายวัน** – งานจะเรียกใช้ทุกวันตามเวลาที่กำหนด
- **รายสัปดาห์** – งานจะเรียกใช้อย่างน้อยหนึ่งครั้งต่อสัปดาห์ตามวันและเวลาที่เลือกไว้
- **ตามเหตุการณ์** – งานจะดำเนินการหลังจากเหตุการณ์ที่กำหนด

ข้ามงานเมื่อทำงานด้วยแบตเตอรี่ – งานจะไม่เริ่มต้นดำเนินการ ถ้าคอมพิวเตอร์ของคุณใช้แบตเตอรี่ในขณะที่งานควรเริ่มต้น นอกจากนี้ยังมีผลกับคอมพิวเตอร์ที่ใช้ UPS ด้วย

เวลางาน – หนึ่งครั้ง

การเรียกใช้งาน – งานที่ระบุจะถูกเรียกใช้งานเพียงครั้งเดียวในวันที่และเวลาที่ระบุ

เวลางาน – รายวัน

งานจะเรียกใช้ทุกวันตามเวลาที่กำหนด

เวลางาน – รายสัปดาห์

งานจะดำเนินการซ้ำทุกสัปดาห์ในวันและเวลาที่เลือกไว้

เวลางาน – ตามเหตุการณ์

งานจะถูกเรียกโดยเหตุการณ์หนึ่งดังต่อไปนี้:

- **ทุกครั้งที่เริ่มต้นคอมพิวเตอร์**
- **ครั้งแรกที่เริ่มต้นคอมพิวเตอร์ในแต่ละวัน**
- **การเชื่อมต่ออินเทอร์เน็ตผ่านหมายเลขโทรศัพท์/VPN**
- **การอัพเดทโมดูลเสร็จสมบูรณ์**
- **การอัพเดทผลิตภัณฑ์เสร็จสมบูรณ์**
- **การเข้าสู่ระบบของผู้ใช้**
- **การตรวจหาภัยคุกคาม**

เมื่อการวางกำหนดการงานถูกเรียกโดยเหตุการณ์ คุณสามารถระบุช่วงเวลาต่ำสุดระหว่างการทำงานเสร็จทั้งสองงาน ตัวอย่างเช่น หากคุณเข้าสู่คอมพิวเตอร์ของคุณหลายครั้งในหนึ่งวัน ให้เลือก 24 ชั่วโมง เพื่อให้ดำเนินการเฉพาะแค่ในครั้งแรกที่เข้าสู่ระบบของวันดังกล่าวและวันถัดไป

งานที่ข้าม

งานสามารถข้ามได้เมื่อคอมพิวเตอร์ทำงานด้วยพลังงานแบตเตอรี่หรือเมื่อปิดเครื่องอยู่ เลือกช่วงเวลาที่จะเรียกใช้งานที่ข้ามไปจากตัวเลือกใดตัวเลือกหนึ่งต่อไปนี้แล้วคลิก **ถัดไป**:

- **เมื่อเวลาที่กำหนดไว้ครั้งต่อไป** – งานจะดำเนินการหากคอมพิวเตอร์เปิดเครื่องอยู่เมื่อถึงเวลาที่กำหนดไว้ครั้งต่อไป
- **เร็วที่สุดเท่าที่ทำได้** – งานจะดำเนินการเมื่อคอมพิวเตอร์เปิดเครื่อง
- **ทันที หากระยะเวลาตั้งแต่เรียกใช้ตามกำหนดการครั้งล่าสุดเกิน (ชั่วโมง)** – หมายถึงเวลาที่ผ่านไปนับตั้งแต่ข้ามการเรียกใช้งานนี้เป็นครั้งแรก หากเกินเวลานี้ งานจะดำเนินการทันที

ทันที หากระยะเวลาตั้งแต่เรียกใช้ตามกำหนดการครั้งล่าสุดเกิน (ชั่วโมง) - ตัวอย่าง

งานตัวอย่างถูกตั้งค่าให้ดำเนินการซ้ำๆ ทุกชั่วโมง ตัวเลือก **ทันที หากระยะเวลาตั้งแต่เรียกใช้ตามกำหนดการครั้งล่าสุดเกิน (ชั่วโมง)** ถูกเลือกอยู่และเวลาที่เกินถูกตั้งเป็นสองชั่วโมง งานจะดำเนินการเวลา 13:00 น. และเมื่อเสร็จสิ้น คอมพิวเตอร์จะเข้าสู่โหมดพักการทำงาน:

• คอมพิวเตอร์จะตื่นขึ้นในเวลา 15:30 น. การข้ามการเรียกใช้ครั้งแรกเกิดขึ้นเมื่อเวลา 14:00 น. เวลาผ่านไปเพียง 1.5 ชั่วโมงนับตั้งแต่ 14:00 น. ดังนั้นงานจะดำเนินการในเวลา 16:00 น.

• คอมพิวเตอร์จะตื่นขึ้นในเวลา 16:30 น. การข้ามการเรียกใช้ครั้งแรกเกิดขึ้นเมื่อเวลา 14:00 น. เวลาผ่านไปสองชั่วโมงครึ่งนับตั้งแต่ 14:00 น. ดังนั้นงานจะดำเนินการทันที

รายละเอียดงาน – อัพเดท

หากคุณต้องการอัพเดทโปรแกรมจากเซิร์ฟเวอร์การอัพเดทสองแห่ง คุณต้องสร้างโปรไฟล์การอัพเดทแยกกันสองโปรไฟล์ หากโปรไฟล์แรกไม่สามารถดาวน์โหลดไฟล์อัพเดท โปรแกรมจะเปลี่ยนไปใช้อีกโปรไฟล์โดยอัตโนมัติ การดำเนินการนี้เหมาะสำหรับ ตัวอย่างเช่น โน้ตบุค ซึ่งโดยปกติจะอัพเดทจากเซิร์ฟเวอร์การอัพเดท LAN ในระบบ แต่เจ้าของมักจะเชื่อมต่อกับอินเทอร์เน็ตในเครือข่ายอื่น ดังนั้น หากโปรแกรมแรกทำงานไม่สำเร็จ โปรแกรมที่สองจะดาวน์โหลดไฟล์อัพเดทจากเซิร์ฟเวอร์การอัพเดทของ ESET โดยอัตโนมัติ

รายละเอียดงาน – เรียกใช้แอพพลิเคชัน

งานนี้จะวางกำหนดการเรียกใช้แอพพลิเคชันภายนอก

ไฟล์ที่เรียกใช้ได้ – เลือกไฟล์ที่เรียกใช้ได้จากโครงสร้างไดเรกทอรี คลิกตัวเลือก **...** หรือป้อนพาธด้วยตนเอง

โฟลเดอร์การทำงาน – กำหนดไดเรกทอรีการทำงานของแอพพลิเคชันภายนอก ไฟล์ชั่วคราวทั้งหมดของ **ไฟล์ที่**

เรียกใช้ได้ ที่เลือกไว้จะสร้างขึ้นภายในไดเรกทอรีนี้

พารามิเตอร์ – พารามิเตอร์ของบรรทัดคำสั่งสำหรับแอพพลิเคชัน (ไม่จำเป็น)

คลิก **สิ้นสุด** เพื่อใช้งาน

การส่งตัวอย่างเพื่อวิเคราะห์

หากคุณพบไฟล์ที่มีพฤติกรรมน่าสงสัยในคอมพิวเตอร์ของคุณหรือเว็บไซต์ที่น่าสงสัยในอินเทอร์เน็ต คุณสามารถส่งไปยังห้องปฏิบัติการวิจัย ESET เพื่อรับการวิเคราะห์ได้ (อาจไม่สามารถใช้งานได้ขึ้นอยู่กับการตั้งค่า ESET LiveGrid® ของคุณ)

อย่าส่งตัวอย่างจนกว่าจะพบว่าตัวอย่างเป็นไปตามเกณฑ์ดังต่อไปนี้:
• ตัวอย่างไม่ได้ถูกตรวจพบโดยผลิตภัณฑ์ ESET ของคุณ
• ตัวอย่างถูกตรวจพบว่าเป็นภัยคุกคามโดยเป็นข้อผิดพลาด
• เราไม่ยอมรับไฟล์ส่วนบุคคลของคุณ (ซึ่งคุณต้องการให้สแกนเพื่อตรวจหามัลแวร์โดย ESET) เป็นตัวอย่าง (ESET Research Lab จะไม่ดำเนินการสแกนตามตามความต้องการของผู้ใช้งาน)
• โปรดใช้ชื่อเรื่องที่อธิบายชัดเจนและให้ข้อมูลเกี่ยวกับไฟล์มากที่สุดเท่าที่จะเป็นไปได้ (ตัวอย่างเช่น ภาพหน้าจอหรือเว็บไซต์ที่คุณดาวน์โหลดไฟล์)

การส่งตัวอย่างทำให้คุณส่งไฟล์หรือไซต์ไปยัง ESET สำหรับการวิเคราะห์โดยใช้หนึ่งในวิธีการต่อไปนี้:

1. การใช้ข้อความตัวอย่างการส่งสามารถดูได้ที่**เครื่องมือ** > **ส่งตัวอย่างเพื่อการวิเคราะห์**
2. อีกวิธีหนึ่งคือ คุณสามารถส่งไฟล์ทางอีเมล ถ้าคุณเลือกตัวเลือกนี้ ให้บรรจุไฟล์เป็นแพ็คโดยใช้ WinRAR/ZIP ป้องกันอาร์ไคฟ์ด้วยรหัสผ่าน "infected" และส่งไปยัง samples@eset.com
3. หากต้องการรายงานสแปม สแปมที่ตรวจพบผิดพลาด หรือเว็บไซต์ที่ถูกจัดหมวดหมู่ไม่ถูกต้องโดยโมดูลการควบคุมการเข้าถึงเว็บไซต์ โปรดดู บทความฐานความรู้ของ ESET

ด้วย **เลือกตัวอย่างเพื่อวิเคราะห์** ที่เปิดอยู่ ให้เลือกคำอธิบายจาก **เหตุผลสำหรับการส่งตัวอย่าง** เมนูแบบเลื่อนลงที่เหมาะกับข้อความของคุณที่สุด:

- ไฟล์ที่น่าสงสัย
- ไซต์ที่น่าสงสัย (เว็บไซต์ที่ติดมัลแวร์)
- การตรวจพบไฟล์ที่ผิดพลาด (ไฟล์ที่ตรวจพบว่าติดไวรัสแต่จริงๆ แล้วไม่ใช่)
- การตรวจไซต์ที่ไม่ผิดพลาด
- อื่นๆ

ไฟล์/ไซต์ – พาธไปยังไฟล์หรือเว็บไซต์ที่คุณต้องการส่ง

อีเมลที่ติดต่อ – โปรแกรมจะส่งอีเมลที่ติดต่อนี้ไปยัง ESET พร้อมกับไฟล์ที่น่าสงสัย และอาจใช้เพื่อติดต่อคุณ ถ้าต้องการข้อมูลเพิ่มเติมสำหรับการวิเคราะห์ คุณจะป้อนอีเมลที่ติดต่อหรือไม่ก็ได้ เลือก **ส่งโดยไม่ระบุชื่อ** เพื่อเว้นช่องว่างไว้

> คุณอาจไม่ได้รับการตอบสนองจาก ESET ยกเว้นในกรณีที่ต้องการข้อมูลเพิ่มเติมจากคุณ เนื่องจากเซิร์ฟเวอร์ของเราได้รับไฟล์หลายหมื่นไฟล์ในแต่ละวัน เราจึงไม่สามารถตอบกลับได้ทั้งหมด
> หากตรวจพบว่าตัวอย่างเป็นแอพพลิเคชันหรือเว็บไซต์ที่เป็นอันตราย การตรวจพบไฟล์นี้จะถูกเพิ่มในการอัพเดทที่กำลังจะมีขึ้นของ ESET

เลือกตัวอย่างเพื่อวิเคราะห์ – ไฟล์ที่น่าสงสัย

สัญญาณและอาการที่พบของการติดไวรัสจากมัลแวร์ – ป้อนคำอธิบายเกี่ยวกับการทำงานของไฟล์ที่น่าสงสัยที่พบในคอมพิวเตอร์ของคุณ

ต้นทางของไฟล์ (ที่อยู่ URL หรือผู้ขาย) – โปรดป้อนต้นทางของไฟล์ (ที่มา) และวิธีที่คุณพบไฟล์นี้

หมายเหตุและข้อมูลเพิ่มเติม – คุณสามารถป้อนข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยในกระบวนการระบุไฟล์ที่น่าสงสัยได้

> ต้องระบุพารามิเตอร์แรก – **สัญญาณและอาการที่พบของการติดไวรัสจากมัลแวร์** แต่การให้ข้อมูลเพิ่มเติมจะช่วยห้องปฏิบัติการของเราในกระบวนการระบุตัวอย่างได้เป็นอย่างมาก

เลือกตัวอย่างเพื่อวิเคราะห์–เว็บไซต์ที่น่าสงสัย

โปรดเลือกตัวเลือกใดตัวเลือกหนึ่งต่อไปนี้จากเมนูแบบเลื่อนลง **เกิดอะไรขึ้นกับไซต์นี้**:

- **ที่ติดไวรัส** – เว็บไซต์ที่มีไวรัสหรือมัลแวร์อื่นๆ ที่แจกจ่ายโดยวิธีต่างๆ
- **การฟิชชิ่ง** – มักใช้เพื่อสามารถเข้าถึงข้อมูลที่มีความละเอียดอ่อน เช่น เลขบัญชีธนาคาร เลข PIN และอื่นๆ อ่านเพิ่มเติมเกี่ยวกับการโจมตีประเภทนี้ได้ใน ประมวลศัพท์
- **หลอกลวง** – เว็บไซต์ที่หลอกลวงหรือเว็บไซต์ฉ้อโกง โดยเฉพาะอย่างยิ่งสำหรับการแสวงหากำไรอย่างรวดเร็ว
- เลือก **อื่นๆ** หากตัวเลือกที่กล่าวถึงก่อนหน้าไม่ใช่ไซต์ที่คุณกำลังจะส่ง

หมายเหตุและข้อมูลเพิ่มเติม – คุณสามารถป้อนข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยในการวิเคราะห์เว็บไซต์ที่น่าสงสัยได้ที่นี่

เลือกตัวอย่างเพื่อวิเคราะห์-การตรวจพบไฟล์ที่ผิดพลาด

เราขอให้คุณส่งไฟล์ที่ตรวจพบว่าติดไวรัส แต่จริงๆ ไม่ได้ติดไวรัส เพื่อปรับปรุงประสิทธิภาพกลไลการป้องกันไวรัสและสปายแวร์ของเราและช่วยให้ผู้อื่นได้รับการป้องกัน การตรวจพบที่ผิดพลาด (FP) อาจเกิดขึ้นเมื่อรูปแบบของไฟล์ตรงกับรูปแบบเดียวกับที่อยู่ในกลไกตรวจหา

ชื่อและเวอร์ชันของแอพพลิเคชัน – ชื่อและเวอร์ชันของโปรแกรม (ตัวอย่างเช่น ตัวเลข ชื่อแทน หรือชื่อรหัส)

ต้นทางของไฟล์ (ที่อยู่ URL หรือผู้ขาย) – โปรดป้อนต้นทางของไฟล์ (ที่มา) และเขียนวิธีที่คุณพบไฟล์นี้

วัตถุประสงค์ของแอพพลิเคชัน – คำอธิบายทั่วไปของแอพพลิเคชัน ประเภทของแอพพลิเคชัน (เช่น เบราว์เซอร์ เครื่องเล่นสื่อ เป็นต้น) และฟังก์ชันการทำงาน

หมายเหตุและข้อมูลเพิ่มเติม – คุณสามารถเพิ่มข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยในการประมวลผลไฟล์ที่น่าสงสัยได้

> ต้องใช้สามพารามิเตอร์แรกเพื่อระบุแอพพลิเคชันที่ถูกต้องและแยกแอพพลิเคชันเหล่านั้นออกจากรหัสที่เป็นอันตราย การให้ข้อมูลเพิ่มเติมจะเป็นการช่วยห้องปฏิบัติการของเราในการระบุและประมวลผลตัวอย่าง

เลือกตัวอย่างเพื่อวิเคราะห์-การตรวจสอบเว็บไซต์ที่ผิดพลาด

เราขอให้คุณส่งไซต์ที่ตรวจพบว่าติดไวรัส การหลอกลวง หรือมีฟิชชิ่ง แต่จริงๆ ไม่ใช่ การตรวจพบที่ผิดพลาด (FP) อาจเกิดขึ้นเมื่อรูปแบบของไฟล์ตรงกับรูปแบบเดียวกับที่อยู่ใน กลไกตรวจหา โปรดให้เว็บไซต์นี้เพื่อปรับปรุงกลไลการป้องกันไวรัสและฟิชชิ่งของพวกเราและช่วยให้ผู้อื่นได้รับการป้องกัน

หมายเหตุและข้อมูลเพิ่มเติม – คุณสามารถเพิ่มข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยในการประมวลผลเว็บไซต์ที่น่าสงสัยได้

เลือกตัวอย่างเพื่อวิเคราะห์-อื่นๆ

ใช้ฟอร์มนี้ถ้าไม่สามารถจัดประเภทไฟล์เป็น **ไฟล์ที่น่าสงสัย** หรือเป็น **การตรวจพบที่ผิดพลาด**

เหตุผลสำหรับการส่งไฟล์ – โปรดป้อนคำอธิบายโดยละเอียดและเหตุผลในการส่งไฟล์

กักเก็บ

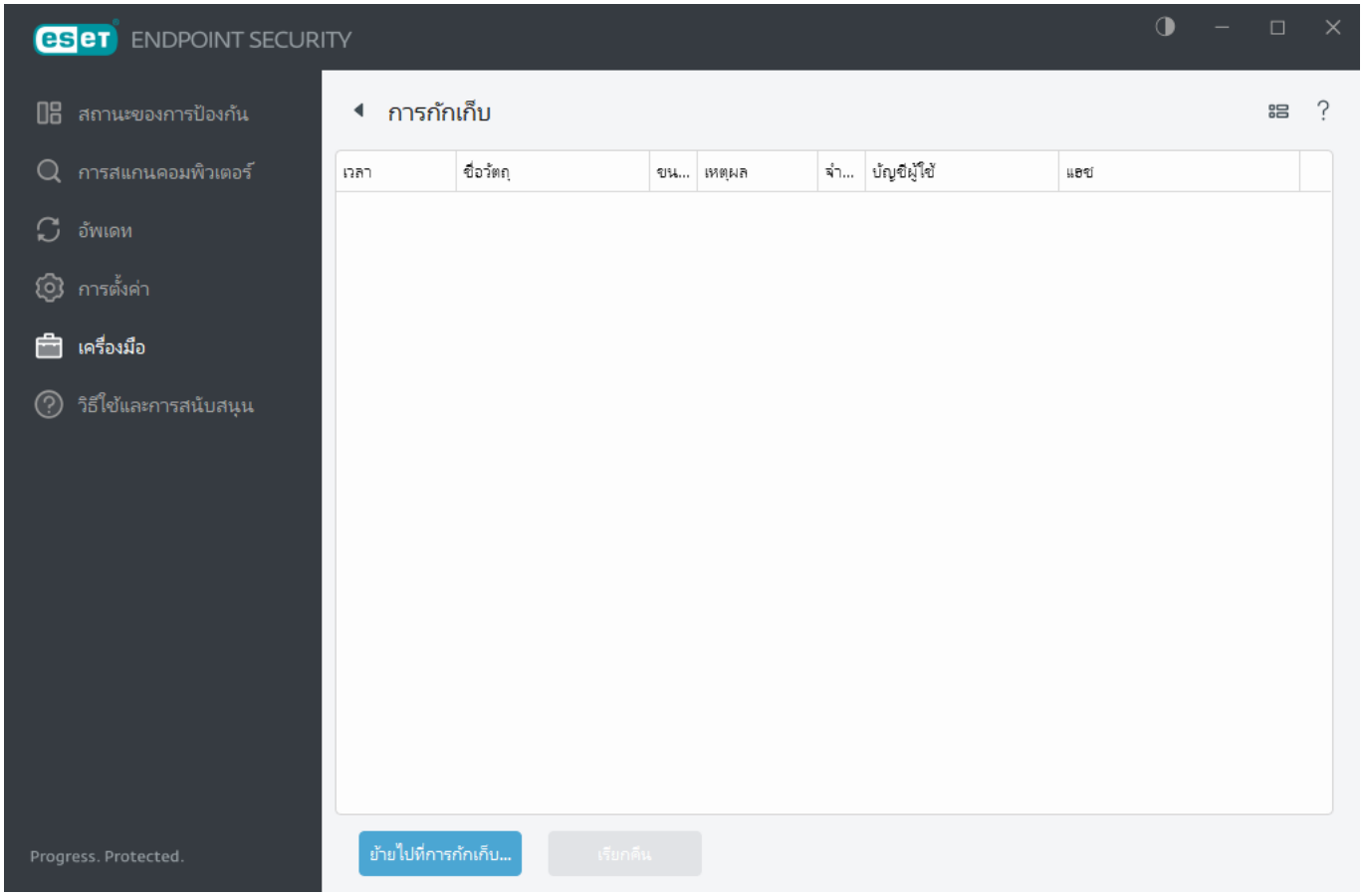
ฟังก์ชันหลักของการกักเก็บคือการจัดเก็บวัตถุที่มีการรายงานไว้อย่างปลอดภัย (เช่น มัลแวร์ ไฟล์ที่ติดไวรัสหรือแอปพลิเคชั่นที่อาจไม่พึงประสงค์)

การกักเก็บนั้นสามารถเข้าถึงได้จาก หน้าต่างโปรแกรมหลัก ของ ESET Endpoint Security โดยการคลิก **เครื่องมือ** > **การกักเก็บ**

ไฟล์ที่เก็บไว้ในโฟลเดอร์กักเก็บนั้นสามารถดูได้ในตารางที่แสดง:

- วันที่และเวลาของการกักเก็บ
- พาธไปยังตำแหน่งดั้งเดิมของไฟล์
- ขนาดของไฟล์เป็นไบต์
- เหตุผลที่กักเก็บ (ตัวอย่างเช่น วัตถุที่เพิ่มมาโดยผู้ใช้)
- และจำนวนครั้งในการตรวจหา (ตัวอย่างเช่น การตรวจหาซ้ำในไฟล์เดียวกันหรือหากเป็นอาร์ไคฟ์ที่มีการบุกรุกหลายครั้ง)

ฉันจัดการการกักเก็บบนไคลเอ็นต์เวิร์กสเตชันจากระยะไกล



การกักเก็บไฟล์

ESET Endpoint Security จะกักเก็บไฟล์ที่ลบโดยอัตโนมัติ (หากคุณไม่ได้ยกเลิกตัวเลือกนี้ใน หน้าต่างเตือนภัย)

ไฟล์เพิ่มเติมที่ควรถูกกักเก็บหาก:

- ไม่สามารถกำจัดได้
- หากเป็นไฟล์ที่ไม่ปลอดภัยหรือระบบแนะนำให้ลบ
- หากมีการตรวจพบด้วยความผิดพลาดโดย ESET Endpoint Security
- หากไฟล์ทำงานน่าสงสัยแต่ไม่มีการตรวจพบโดย เครื่องมือสแกน

คุณมีตัวเลือกหลายประการในการกักเก็บไฟล์:

- คุณสามารถใช้คุณสมบัติลากและวางเพื่อกักเก็บไฟล์ด้วยตัวเองได้ โดยให้คลิกที่ไฟล์หรือโฟลเดอร์ แล้วเลื่อนตัวชี้เมาส์ไปยังบริเวณที่ทำเครื่องหมายขณะที่กดปุ่มเมาส์ค้างไว้ จากนั้นจึงปล่อยนิ้ว หลังจากนั้นแอพพลิเคชันจะเลื่อนมาที่เบื้องหน้า
- คลิก **ย้ายไปที่การกักเก็บ** จากหน้าต่างโปรแกรมหลัก
- นอกจากนี้ยังสามารถใช้เมนูบริบทเพื่อการทำงานนี้ โดยให้คลิกขวาในหน้าต่าง **กักเก็บ** และเลือก **กักเก็บ**

การเรียกคืนจากการกักเก็บ

นอกจากนี้ไฟล์ที่ถูกกักเก็บยังสามารถเรียกคืนไปยังตำแหน่งดั้งเดิมได้อีกด้วย:

- ใช้คุณสมบัติ **เรียกคืน** สำหรับการดำเนินการดังกล่าว ซึ่งสามารถใช้งานได้จากเมนูบริบทโดยคลิกไฟล์ที่ต้องการในการกักเก็บ
- หากไฟล์ถูกทำเครื่องหมายเป็น แอพพลิเคชันที่อาจไม่พึงประสงค์ ตัวเลือก **เรียกคืนและยกเว้นจากการสแกน** จะเปิดใช้งาน ทั้งนี้โปรดดู การยกเว้น
- นอกจากนี้เมนูบริบทยังมีตัวเลือก **เรียกคืนไปที่** ซึ่งช่วยให้คุณสามารถเรียกคืนไฟล์ไปยังตำแหน่งอื่นนอกเหนือจากตำแหน่งที่ถูกลบได้
- ในบางกรณีจะไม่สามารถใช้งานฟังก์ชันการเรียกคืนได้ ตัวอย่างเช่น ไฟล์ที่ตั้งอยู่ในการแชร์เครือข่ายที่อ่านได้อย่างเดียวเท่านั้น

การลบจากการกักเก็บ

คลิกขวารายการที่ระบุ แล้วเลือก **ลบจากการกักเก็บ** หรือเลือกรายการที่คุณต้องการลบแล้วกด **ลบ** บนแป้นพิมพ์ของคุณ คุณยังสามารถเลือกหลายๆ รายการและลบรายการเหล่านั้นพร้อมกัน รายการที่ถูกลบจะถูกนำออกจากอุปกรณ์ของคุณและการกักเก็บอย่างถาวร

การส่งไฟล์จากการกักเก็บ

หากคุณได้กักเก็บไฟล์ที่น่าสงสัยที่ไม่ถูกตรวจพบโดยโปรแกรม หรือหากไฟล์ถูกประเมินว่าติดไวรัสโดยไม่ถูกต้อง (เช่น โดยการวิเคราะห์พฤติกรรมของรหัส) และมีการกักเก็บหลังจากนั้น โปรด ส่งตัวอย่างสำหรับการวิเคราะห์ไปยังห้องปฏิบัติการวิจัยของ ESET หากต้องการส่งไฟล์ ให้คลิกขวาที่ไฟล์และเลือก **ส่งเพื่อวิเคราะห์** จากเมนูบริบท

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
- จัดการการกักเก็บใน ESET PROTECT
- ผลิตภัณฑ์ My ESET แจ้งเตือนการตรวจหาให้ฉันทราบ—ฉันควรทำอย่างไร

วิธีใช้และการสนับสนุน

คลิก **วิธีใช้และการสนับสนุน** ใน หน้าต่างหลักของโปรแกรม เพื่อแสดงข้อมูลสนับสนุนและเครื่องมือแก้ไขปัญหา ซึ่งจะช่วยคุณแก้ปัญหาที่คุณอาจพบ

ผลิตภัณฑ์ที่ติดตั้ง

- เกี่ยวกับESET Endpoint Security – แสดงข้อมูลเกี่ยวกับสำเนา ESET Endpoint Security ของคุณ
- การแก้ไขปัญหาผลิตภัณฑ์ – คลิกลิงก์นี้เพื่อค้นหาวิธีแก้ไขสำหรับปัญหาที่พบบ่อยที่สุด
- การแก้ไขปัญหาใบอนุญาต – คลิกลิงก์นี้เพื่อค้นหาวิธีแก้ไขปัญหาเกี่ยวกับการเปิดใช้งานหรือการเปลี่ยนแปลงใบอนุญาต
- เปลี่ยนใบอนุญาต - คลิกเพื่อเรียกใช้หน้าต่างการเปิดใช้งานและเปิดใช้งานผลิตภัณฑ์ของคุณ

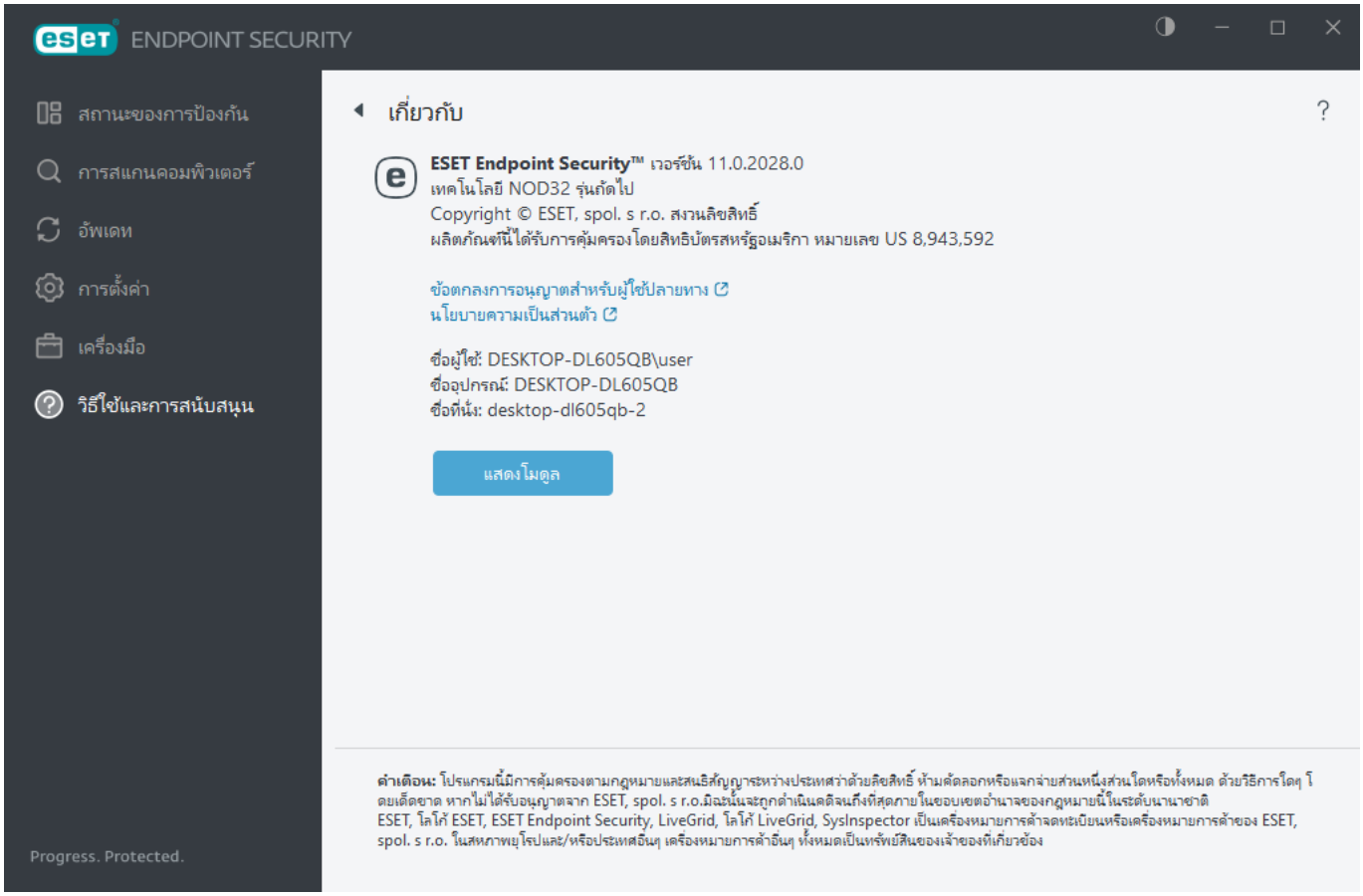
หน้าวิธีใช้ – คลิกลิงค์นี้เพื่อเริ่มต้นหน้าวิธีใช้ ESET Endpoint Security

ฝ่ายสนับสนุนด้านเทคนิค

ฐานความรู้ – ฐานความรู้ของ ESET มีคำตอบสำหรับคำถามที่พบบ่อยที่สุด รวมถึงทางแก้ไขที่แนะนำสำหรับปัญหาต่างๆ ผู้เชี่ยวชาญด้านเทคนิคของ ESET จะอัพเดทข้อมูลนี้เป็นประจำ เพื่อให้ฐานความรู้เป็นเครื่องมือที่มีประสิทธิภาพสูงสุดสำหรับการแก้ไขปัญหาประเภทต่างๆ

เกี่ยวกับ ESET Endpoint Security

หน้าต่างนี้จะแสดงรายละเอียดเกี่ยวกับ ESET Endpoint Security เวอร์ชันที่ติดตั้งและคอมพิวเตอร์ของคุณ



คลิก **แสดงโมดูล** เพื่อดูข้อมูลเกี่ยวกับรายชื่อโมดูลโปรแกรมที่โหลด

- คุณสามารถคัดลอกข้อมูลเกี่ยวกับโมดูลไปไว้ที่คลิปบอร์ดได้ด้วยการคลิก **คัดลอก** การดำเนินการนี้อาจมีประโยชน์เมื่อแก้ไขปัญหา หรือเมื่อติดต่อกับฝ่ายสนับสนุนด้านเทคนิค
- คลิก **กลไกการตรวจจับ** ในหน้าต่างโมดูลเพื่อเปิดเรดาร์ไวรัสของ ESET ซึ่งบรรจุข้อมูลเกี่ยวกับกลไกการตรวจจับของ ESET แต่ละเวอร์ชัน

ส่งข้อมูลการกำหนดค่าระบบ

ESET จำเป็นต้องขอข้อมูลเกี่ยวกับการกำหนดค่า ESET Endpoint Security, ข้อมูลระบบโดยละเอียดและกระบวนการที่ทำงานอยู่ (ไฟล์บันทึก ESET SysInspector) และข้อมูลรีจิสตรีเพื่อการช่วยเหลืออย่างรวดเร็วและถูกต้องที่สุดเท่าที่จะทำได้ ESET จะใช้ข้อมูลนี้เพื่อให้ความช่วยเหลือด้านเทคนิคแก่ลูกค้าเพียงอย่างเดียว

หลังจากที่คุณส่ง แบบฟอร์มเว็บ ข้อมูลการกำหนดค่าระบบของคุณจะถูกส่งให้กับ ESET เลือก **ส่งข้อมูลนี้เสมอ** หากคุณต้องการจำการดำเนินการนี้สำหรับกระบวนการนี้ เมื่อส่ง แบบฟอร์มเว็บ โดยไม่ได้ส่งข้อมูลใดๆ ให้คลิก **ไม่ต้องส่งข้อมูล** และดำเนินการต่อ

คุณสามารถกำหนดค่าการส่งข้อมูลการกำหนดค่าระบบได้ ใน การตั้งค่าขั้นสูง > **เครื่องมือ** > **การวินิจฉัย** ฝ่าย

หากคุณตัดสินใจที่จะส่งข้อมูลการกำหนดค่าระบบ คุณจำเป็นต้องกรอกและส่งแบบฟอร์มเว็บ มิฉะนั้นตั๋วของคุณจะไม่ถูกสร้างและข้อมูลการกำหนดค่าระบบของคุณจะหายไป หากไม่สามารถส่งข้อมูลการกำหนดค่าระบบได้ ให้กรอกแบบฟอร์มเว็บและรอคำแนะนำจากฝ่ายสนับสนุนด้านเทคนิค

ฝ่ายสนับสนุนด้านเทคนิค

ในหน้าต่างโปรแกรมหลัก ให้คลิก **วิธีใช้และการสนับสนุน** > **ฝ่ายสนับสนุนด้านเทคนิค**

ติดต่อฝ่ายสนับสนุนด้านเทคนิค

ขอรับการสนับสนุน – หากคุณไม่พบคำตอบสำหรับปัญหาของคุณ คุณสามารถใช้แบบฟอร์มนี้ซึ่งมีอยู่ในเว็บไซต์ของ ESET เพื่อติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET ได้อย่างรวดเร็ว หน้าต่าง ส่งข้อมูลการกำหนดค่าระบบของคุณ จะปรากฏขึ้นก่อนที่จะกรอกแบบฟอร์มเว็บ ทั้งนี้ขึ้นอยู่กับการตั้งค่าของคุณ

รับข้อมูลสำหรับฝ่ายสนับสนุนด้านเทคนิค

รายละเอียดสำหรับการสนับสนุนด้านเทคนิค – เมื่อได้รับแจ้ง คุณสามารถคัดลอกและส่งข้อมูลไปที่ฝ่ายสนับสนุนด้านเทคนิคของ ESET (เช่น รายละเอียดใบอนุญาต ชื่อผลิตภัณฑ์ เวอร์ชันผลิตภัณฑ์ ระบบปฏิบัติการ และข้อมูลคอมพิวเตอร์) ได้

ESET Log Collector - ลิงก์ไปยังบทความฐานความรู้ของ ESET ที่คุณสามารถดาวน์โหลด ESET Log Collector ซึ่งเป็นแอพพลิเคชันที่รวบรวมข้อมูลโดยอัตโนมัติและบันทึกจากคอมพิวเตอร์เพื่อช่วยให้แก้ไขปัญหาได้รวดเร็วยิ่งขึ้น สำหรับข้อมูลเพิ่มเติมเกี่ยวกับผลิตภัณฑ์ ดูที่ คู่มือผู้ใช้แบบออนไลน์ของ ESET Log Collector

เปิดใช้งาน **การบันทึกขั้นสูง** เพื่อสร้างบันทึกขั้นสูงให้กับคุณลักษณะที่มีทั้งหมดเพื่อช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาได้ ความละเอียดขั้นต่ำในการบันทึกจะถูกตั้งค่าไปที่ระดับ **การวินิจฉัย** การบันทึกขั้นสูงจะปิดใช้งานโดยอัตโนมัติหลังจากสองชั่วโมง นอกจากคุณจะหยุดการบันทึกล่วงหน้าโดยคลิก **หยุดการบันทึกขั้นสูง** เมื่อบันทึกทั้งหมดถูกสร้าง หน้าต่างการแจ้งเตือนจะแสดงขึ้น ซึ่งจะทำให้คุณเข้าถึงโฟลเดอร์การวินิจฉัยที่มีบันทึกที่สร้างได้โดยตรง

การตั้งค่าขั้นสูง

การตั้งค่าขั้นสูงช่วยให้คุณสามารถกำหนด ESET Endpoint Security การตั้งค่าโดยละเอียดเพื่อให้เหมาะกับความต้องการของคุณ

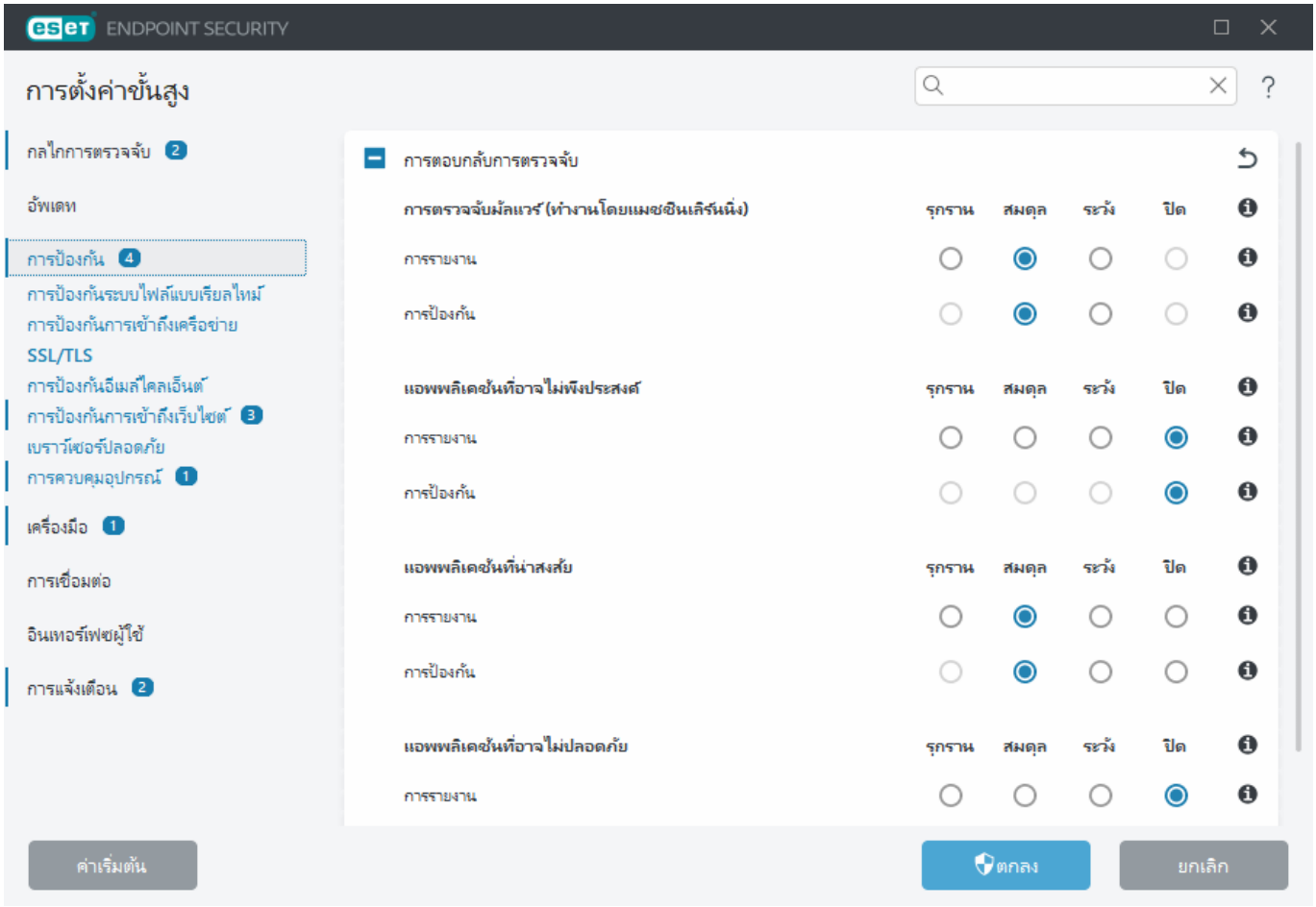
เมื่อต้องการเปิดการตั้งค่าขั้นสูง ให้เปิด หน้าต่างโปรแกรมหลัก แล้วกดปุ่ม **F5** บนแป้นพิมพ์ของคุณ หรือคลิก **ตั้งค่า > การตั้งค่าขั้นสูง**

เมื่อสร้างนโยบายจากเว็บคอนโซล ESET PROTECT คุณจะสามารถเลือกธงของการตั้งค่าแต่ละรายการได้ การตั้งค่าที่มีธงบังคับจะมีลำดับความสำคัญและไม่สามารถเขียนทับโดยนโยบายที่ใหม่กว่าได้ (แม้ว่านโยบายที่ใหม่กว่าจะมีธงบังคับ) สิ่งนี้ช่วยให้มั่นใจได้ว่าการตั้งค่านี้จะไม่ถูกเปลี่ยนแปลง (โดยผู้ใช้หรือโดยนโยบายที่ใหม่กว่าในระหว่างที่รวมข้อมูล เป็นต้น) สำหรับข้อมูลเพิ่มเติม โปรดดู ธง ในวิธีใช้ออนไลน์ของ ESET PROTECT

ระบบอาจให้คุณกรอกรหัสผ่านเพื่อเปิดการตั้งค่าขั้นสูง โดยขึ้นอยู่กับ การตั้งค่าการเข้าถึง ของคุณ

คุณสามารถกำหนดการตั้งค่าต่อไปนี้ในการตั้งค่าขั้นสูงได้

- กลไกการตรวจจับ
- อัพเดท
- การป้องกัน
- เครื่องมือ
- การเชื่อมต่อ
- ส่วนติดต่อกับผู้ใช้
- การแจ้งเตือน



กลไกการตรวจจับ

การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** ช่วยให้คุณสามารถกำหนดค่าตัวเลือกต่อไปนี้:

- การยกเว้น
- ตัวเลือกขั้นสูง
- เครื่องมือสแกนการรับส่งข้อมูลเครือข่าย

การยกเว้น

การยกเว้น จะช่วยให้คุณสามารถยกเว้นวัตถุจากกลไกการตรวจจับได้ ในการทำให้แน่ใจว่าจะมีการสแกนวัตถุทั้งหมด เราขอแนะนำให้สร้างข้อยกเว้นต่อเมื่อจำเป็นจริง ๆ เท่านั้น สถานการณ์ที่คุณอาจต้องยกเว้นวัตถุนั้นอาจรวมถึงการสแกนรายการฐานข้อมูลขนาดใหญ่ที่จะทำให้คอมพิวเตอร์ทำงานช้าในระหว่างการสแกนหรือซอฟต์แวร์ที่ขัดแย้งกับการสแกน

การยกเว้นการทำงาน ซึ่งจะยกเว้นไฟล์และโฟลเดอร์จากการสแกนได้ การยกเว้นการทำงานมีประโยชน์ในการ

ยกเว้นการสแกนระดับไฟล์ของแอพพลิเคชันเกมหรือเมื่อเกิดพฤติกรรมของระบบที่ไม่ปกติหรือมีการทำงานเพิ่มขึ้น

การยกเว้นการตรวจหา – ยกเว้นวัตถุจากการทำความสะอาดโดยใช้ชื่อ พาธ หรือแฮชของการตรวจหา การยกเว้นการตรวจหาไม่ได้ยกเว้นไฟล์และโฟลเดอร์จากการสแกนเช่นเดียวกับการยกเว้นการทำงาน การยกเว้นการตรวจหาจะยกเว้นวัตถุเมื่อถูกตรวจจับโดยกลไกการตรวจจับและมีกฎที่เหมาะสมแสดงอยู่ในรายการการยกเว้นเท่านั้น

โปรดอย่าสับสนกับประเภทการยกเว้นอื่นๆ:

- การยกเว้นกระบวนการ – การดำเนินการของไฟล์ทั้งหมดที่ถือว่าเป็นของการยกเว้นกระบวนการของแอพพลิเคชันถูกยกเว้นจากการสแกน (อาจจำเป็นต้องปรับปรุงความเร็ว backup และความพร้อมให้บริการ)
- ยกเว้นนามสกุลไฟล์
- การยกเว้น HIPS
- ตัวกรองการยกเว้นสำหรับการป้องกันระบบคลาวด์

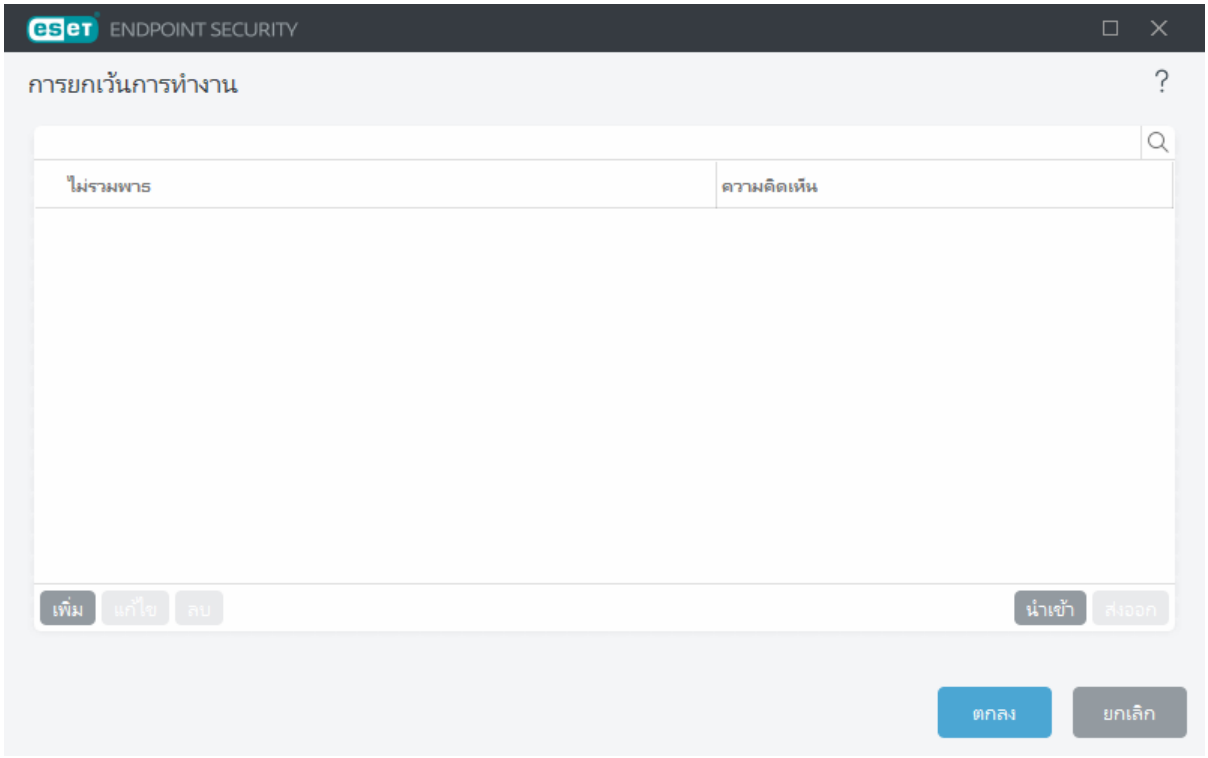
การยกเว้นการทำงาน

การยกเว้นการทำงาน ช่วยให้คุณยกเว้นไฟล์และโฟลเดอร์จากการสแกน

หากต้องการทำให้แน่ใจว่าจะมีการสแกนวัตถุทั้งหมดเพื่อหาภัยคุกคาม เราขอแนะนำให้สร้างการยกเว้นต่อเมื่อจำเป็นจริงๆ เท่านั้น แต่ยังมีบางสถานการณ์ที่คุณอาจจำเป็นต้องยกเว้นวัตถุ ตัวอย่างเช่น รายการฐานข้อมูลขนาดใหญ่ที่จะทำให้คอมพิวเตอร์ทำงานช้าในระหว่างการสแกนหรือซอฟต์แวร์ที่ขัดแย้งกับการสแกน

คุณสามารถเพิ่มไฟล์และโฟลเดอร์ให้ยกเว้นจากการสแกนในรายการการยกเว้นได้ผ่าน การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การยกเว้น** > **การยกเว้นการทำงาน** > **แก้ไข**

ในการ ยกเว้นวัตถุ (พาธ: ไฟล์หรือโฟลเดอร์) จากการสแกน ให้คลิก **เพิ่ม** แล้วป้อนพาธที่ใช้งานได้หรือเลือกพาธในโครงสร้าง



โมดูลการป้องกันระบบไฟล์แบบเรียลไทม์ หรือ**โมดูลการสแกนคอมพิวเตอร์** จะไม่สามารถตรวจพบภัยคุกคามภายในไฟล์ได้ถ้าไฟล์ตรงตามเกณฑ์สำหรับการยกเว้นจากการสแกน

องค์ประกอบการควบคุม

- **เพิ่ม** – เพิ่มรายการใหม่ไปยังการยกเว้นวัตถุจากการสแกน
- **แก้ไข** – ช่วยให้คุณสามารถแก้ไขรายการที่เลือกได้
- **ลบ** – ลบรายการต่างๆ ที่เลือกออก (CTRL + คลิกเพื่อเลือกรายการหลายรายการ)
- **นำเข้า/ส่งออก** – การนำเข้าและการส่งออกการยกเว้นการทำงานจะมีประโยชน์ในกรณีที่คุณต้องสำรองการยกเว้นปัจจุบันเพื่อใช้งานในภายหลัง ตัวเลือกการตั้งค่าการส่งออกยังใช้งานได้สะดวกสำหรับผู้ใช้ในสภาพแวดล้อมที่ไม่ได้รับการจัดการซึ่งต้องการใช้การกำหนดค่าที่ต้องการของพวกเขาในระบบต่างๆ ผู้ใช้เหล่านั้นสามารถนำเข้าไฟล์ .txt ได้อย่างง่ายดายเพื่อส่งการตั้งค่าเหล่านั้น

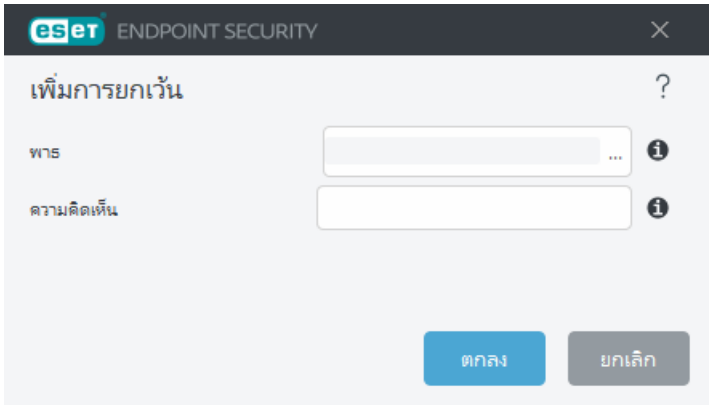
  แสดงตัวอย่างรูปแบบไฟล์นำเข้า/ส่งออก

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

C:\pagefile.sys
```

เพิ่มหรือแก้ไขการยกเว้นการทำงาน

หน้าต่างข้อความนี้จะยกเว้นพาธแบบเฉพาะ (ไฟล์หรือไดเรกทอรี) สำหรับคอมพิวเตอร์เครื่องนี้

ในการเลือกพาธที่เหมาะสม ให้คลิก **...** ในช่อง **พาธ**
เมื่อป้อนด้วยตนเอง ให้ดูเพิ่มเติมที่ ตัวอย่างรูปแบบของการยกเว้น ด้านล่าง



คุณสามารถใช้สัญลักษณ์แทนเพื่อไม่รวมกลุ่มของไฟล์ เครื่องหมายคำถาม (*?*) แสดงถึงอักขระตัวแปรเดียว โดยที่เครื่องหมายดอกจัน (***) แสดงถึงสตริงตัวแปรตั้งแต่ศูนย์อักขระขึ้นไป

- หากคุณต้องการยกเว้นไฟล์และโฟลเดอร์ย่อยทั้งหมดในโฟลเดอร์ ให้พิมพ์พาธไปยังโฟลเดอร์ และใช้มาสก์ ***
- หากคุณต้องการยกเว้นเฉพาะไฟล์ doc ให้ใช้มาสก์ **.doc*
- หากชื่อของไฟล์ที่เรียกใช้ได้มีอักขระจำนวนหนึ่ง (ที่มีอักขระแตกต่างกัน) และคุณทราบเฉพาะอักขระตัวแรก (เช่น "D") ให้ใช้รูปแบบต่อไปนี้:
D????.exe (เครื่องหมายคำถามจะแทนที่อักขระที่ขาดหายไป/ไม่ทราบ

ตัวอย่าง:

- *C:\Tools** – พาธต้องจบด้วยเครื่องหมายคั่นหลัง (\) และดอกจัน (*) เพื่อระบุว่าเป็นโฟลเดอร์ และเนื้อหาของโฟลเดอร์ (ไฟล์และโฟลเดอร์ย่อย) ทั้งหมดนั้นจะถูกยกเว้น
- *C:\Tools*.** — มีพฤติกรรมเช่นเดียวกับ *C:\Tools**
- *C:\Tools* – โฟลเดอร์ *Tools* จะไม่ถูกยกเว้น จากมุมมองของเครื่องมือสแกน *Tools* สามารถเป็นชื่อไฟล์ได้เช่นเดียวกัน
- *C:\Tools*.dat* – สิ่งนี้จะยกเว้นไฟล์.dat ในโฟลเดอร์ *Tools*
- *C:\Tools\sg.dat* – นี่จะยกเว้นไฟล์ที่เฉพาะเจาะจงที่อยู่ในพาธนี้เท่านั้น

คุณสามารถใช้ระบบตัวแปรได้ เช่น *%PROGRAMFILES%* เพื่อระบุข้อยกเว้นการสแกน
• หากไม่ต้องการรวมโฟลเดอร์ Program Files โดยใช้ระบบตัวแปร ให้ใช้พาธ*%PROGRAMFILES%** (จำไว้ว่าให้เพิ่มเครื่องหมายคั่นหลังและดอกจันที่ด้านหลังสุดของพาธ) เมื่อเพิ่มข้อยกเว้น
• หากต้องการยกเว้นไฟล์และโฟลเดอร์ทั้งหมดในไดเรกทอรีย่อยของ*%PROGRAMFILES%* ให้ใช้พาธ *%PROGRAMFILES%\Excluded_Directory**

รายการขยายที่รองรับตัวแปรของระบบ

ตัวแปรต่อไปนี้สามารถใช้ได้ในพาธของรูปแบบการยกเว้น:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

ตัวแปรของระบบที่เฉพาะผู้ใช้ (เช่น *%TEMP%* หรือ *%USERPROFILE%*) หรือตัวแปรแวดล้อม (เช่น *%PATH%*) ไม่รองรับ

การใช้สัญลักษณ์แทนในช่วงกลางของพาธ (ตัวอย่างเช่น *C:\Tools*\Data\file.dat*) อาจใช้การได้ แต่ไม่รองรับอย่างเป็นทางการสำหรับการยกเว้นการทำงาน โปรดดู บทความฐานความรู้ ต่อไปนี้สำหรับข้อมูลเพิ่มเติม
จะไม่มีข้อกำหนดเพื่อใช้สัญลักษณ์แทนในช่วงกลางของพาธเมื่อใช้ การยกเว้นการตรวจหา

คำสั่งของการยกเว้น
• ไม่มีตัวเลือกเพื่อปรับระดับความสำคัญของการยกเว้นโดยใช้ปุ่มบนสุด/ล่าสุด (ต่างจาก กฎของไฟร์วอลล์ ที่จะเรียกใช้กฎตามความสำคัญจากมากไปน้อย)
• เมื่อใช้กฎที่สามารถใช้ได้ครั้งแรกตรงกับเครื่องมือสแกน กฎที่สามารถใช้ได้ครั้งที่สองจะไม่ได้รับการประเมิน
• ยิ่งมีกฎน้อย ประสิทธิภาพการสแกนยิ่งดีขึ้น
• หลีกเลี่ยงการสร้างกฎที่ทำพร้อมกัน

รูปแบบของการยกเว้นพาธ

คุณสามารถใช้สัญลักษณ์แทนเพื่อไม่รวมกลุ่มของไฟล์ เครื่องหมายคำถาม (*?*) แสดงถึงอักขระตัวแปรเดียว โดยที่เครื่องหมายดอกจัน (***) แสดงถึงสตริงตัวแปรตั้งแต่ศูนย์อักขระขึ้นไป

• หากคุณต้องการยกเว้นไฟล์และโฟลเดอร์ย่อยทั้งหมดในโฟลเดอร์ ให้พิมพ์พาธไปยังโฟลเดอร์ และใช้มาสก์ *
• หากคุณต้องการยกเว้นเฉพาะไฟล์ doc ให้ใช้มาสก์ *.doc
• หากชื่อของไฟล์ที่เรียกใช้ได้มีอักขระจำนวนหนึ่ง (ที่มีอักขระแตกต่างกัน) และคุณทราบเฉพาะอักขระตัวแรก (เช่น "D") ให้ใช้รูปแบบต่อไปนี้:
D????.exe (เครื่องหมายคำถามจะแทนที่อักขระที่ขาดหายไป/ไม่ทราบ
ตัวอย่าง:
• *C:\Tools** – พาธต้องจบด้วยเครื่องหมายคั่นหลัง (\) และดอกจัน (*) เพื่อระบุว่าเป็นโฟลเดอร์ และเนื้อหาของโฟลเดอร์ (ไฟล์และโฟลเดอร์ย่อย) ทั้งหมดนั้นจะถูกยกเว้น
• *C:\Tools*.** — มีพฤติกรรมเช่นเดียวกับ *C:\Tools**
• *C:\Tools* – โฟลเดอร์ *Tools* จะไม่ถูกยกเว้น จากมุมมองของเครื่องมือสแกน *Tools* สามารถเป็นชื่อไฟล์ได้เช่นเดียวกัน
• *C:\Tools*.dat* – สิ่งนี้จะยกเว้นไฟล์.dat ในโฟลเดอร์ *Tools*
• *C:\Tools\sg.dat* – นี่จะยกเว้นไฟล์ที่เฉพาะเจาะจงที่อยู่ในพาธนี้เท่านั้น

คุณสามารถใช้ระบบตัวแปรได้ เช่น *%PROGRAMFILES%* เพื่อระบุข้อยกเว้นการสแกน
• หากไม่ต้องการรวมโฟลเดอร์ Program Files โดยใช้ระบบตัวแปร ให้ใช้พาธ*%PROGRAMFILES%** (จำไว้ว่าให้เพิ่มเครื่องหมายคั่นหลังและดอกจันที่ด้านหลังสุดของพาธ) เมื่อเพิ่มข้อยกเว้น
• หากต้องการยกเว้นไฟล์และโฟลเดอร์ทั้งหมดในไดเรกทอรีย่อยของ*%PROGRAMFILES%* ให้ใช้พาธ *%PROGRAMFILES%\Excluded_Directory**

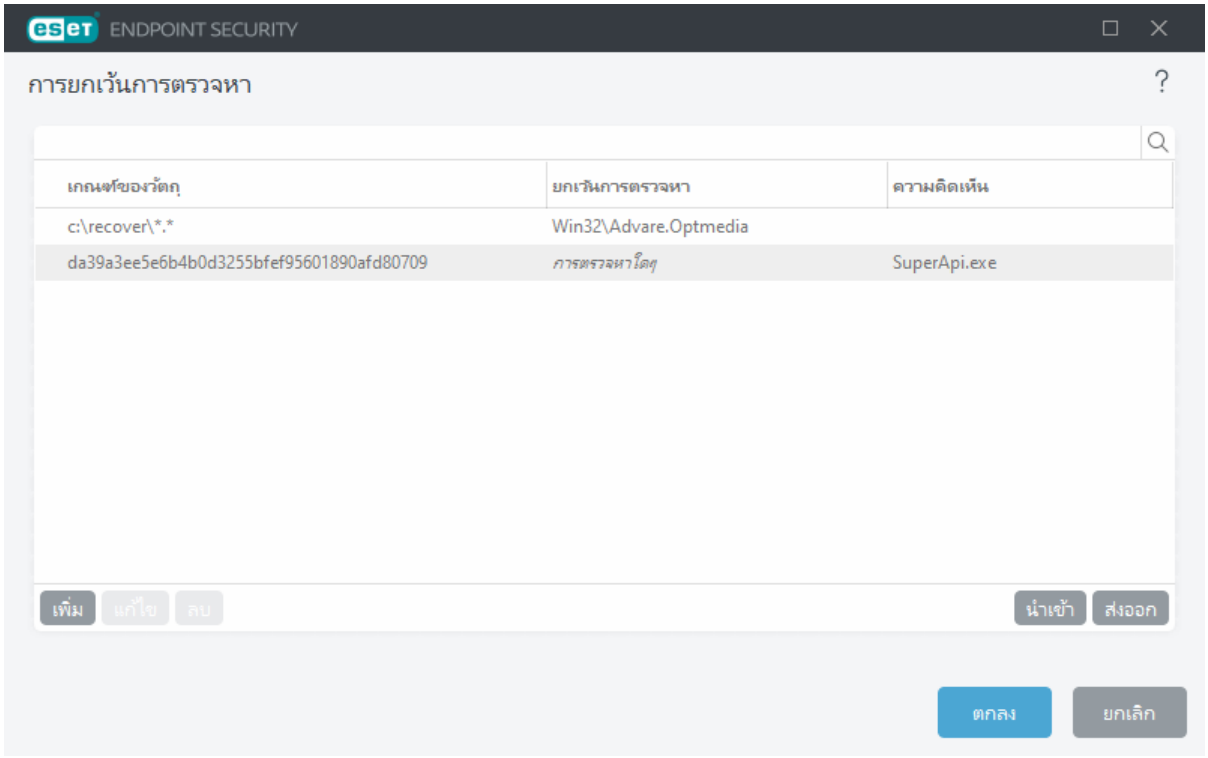
รายการขยายที่รองรับตัวแปรของระบบ

ตัวแปรต่อไปนี้สามารถใช้ได้ในพาธของรูปแบบการยกเว้น:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
ตัวแปรของระบบที่เฉพาะผู้ใช้ (เช่น *%TEMP%* หรือ *%USERPROFILE%*) หรือตัวแปรแวดล้อม (เช่น *%PATH%*) ไม่รองรับ

การยกเว้นการตรวจหา

การยกเว้นการตรวจหาช่วยให้คุณยกเว้นวัตถุจาก การทำความสะอาด โดยการกรองชื่อการตรวจหา พาธของวัตถุ หรือแฮช

การยกเว้นการตรวจหาไม่ได้ยกเว้นไฟล์และโฟลเดอร์จากการสแกนเช่นเดียวกับการยกเว้นการทำงาน การยกเว้นการตรวจหาจะยกเว้นวัตถุเมื่อถูกตรวจจับโดยกลไกการตรวจจับและมีกฎที่เหมาะสมแสดงอยู่ในรายการการยกเว้นเท่านั้น
ตัวอย่างเช่น (โปรดดูแถวแรกของรูปภาพด้านล่าง) เมื่อวัตถุถูกตรวจหาว่าเป็น Win32/Adware.Optmedia และไฟล์ที่ตรวจหาเป็น *C:\Recovery\file.exe* ในแถวที่สอง แต่ละไฟล์ที่มีแฮช SHA-1 ที่เหมาะสม จะถูกยกเว้นเสมอไม่ว่าชื่อของการตรวจหาจะเป็นอย่างไรก็ตาม



เพื่อให้แน่ใจว่าภัยคุกคามทั้งหมดถูกตรวจหา เราแนะนำให้สร้างการยกเว้นการตรวจหาเมื่อจำเป็นจริงๆ เท่านั้น

หากต้องการเพิ่มไฟล์หรือโฟลเดอร์ลงในรายการการยกเว้น ให้ไปที่ การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การยกเว้น** > **การยกเว้นการตรวจหา** > **แก้ไข**

ในการ ยกเว้นวัตถุ (โดยชื่อการตรวจหาหรือแฮช) จากการกำจัด ให้คลิก **เพิ่ม**

สำหรับ แอพพลิเคชันที่อาจไม่พึงประสงค์ และ แอพพลิเคชันที่อาจไม่ปลอดภัย สามารถสร้างการยกเว้นด้วยชื่อการตรวจจับดังนี้:

- ในหน้าต่างการแจ้งเตือนที่รายงานการตรวจจับ (คลิก **แสดงตัวเลือกขั้นสูง** แล้วเลือก **ยกเว้นจากการตรวจ**)
- จากเมนูบริบทไฟล์บันทึกที่ใช้ สร้างวิซาร์ดการยกเว้นการตรวจหา
- ด้วยการคลิก **เครื่องมือ** > **การกักเก็บ** จากนั้นคลิกขวาที่ไฟล์ที่ถูกกักเก็บแล้วเลือก **เรียกคืนและยกเว้นจากการสแกน** จากเมนูบริบท

เกณฑ์การยกเว้นการตรวจหาของวัตถุ

- **พาธ** – จำกัดการยกเว้นการตรวจหาสำหรับพาธเฉพาะ (หรือพาธใดๆ)
- **ชื่อของการตรวจหา** - หากมีชื่อของ การตรวจหา ถัดจากไฟล์ที่ยกเว้น หมายความว่า ไฟล์ดังกล่าวจะถูกยกเว้นสำหรับการตรวจหาที่กำหนดเท่านั้น แต่ไม่ใช่ทั้งหมด หากไฟล์นั้นติดไวรัสมัลแวร์อื่นๆ ในภายหลัง

ไฟล์จะถูกตรวจพบ

- **แฮช** – ยกเว้นไฟล์ที่อิงจากแฮชที่ระบุไว้ SHA-1 ไม่ว่าจะเป็นประเภทของไฟล์ ตำแหน่ง ชื่อ หรือส่วนขยายของไฟล์

องค์ประกอบการควบคุม

- **เพิ่ม** – เพิ่มรายการใหม่ไปยังการยกเว้นวัตถุจากการกำจัด
- **แก้ไข** – ช่วยให้คุณสามารถแก้ไขรายการที่เลือกได้
- **ลบ** – ลบรายการต่างๆ ที่เลือกออก (CTRL + คลิกเพื่อเลือกรายการหลายรายการ)
- **นำเข้า/ส่งออก** – การนำเข้าและการส่งออกการยกเว้นการตรวจหาจะมีประโยชน์ในกรณีที่คุณต้องสำรองการยกเว้นปัจจุบันเพื่อใช้งานในภายหลัง ตัวเลือกการตั้งค่าการส่งออกยังใช้งานได้สะดวกสำหรับผู้ใช้ในสภาพแวดล้อมที่ไม่ได้รับการจัดการซึ่งต้องการใช้การกำหนดค่าที่ต้องการของพวกเขาในระบบต่างๆ ผู้ใช้เหล่านั้นสามารถนำเข้าไฟล์ .txt ได้อย่างง่ายดายเพื่อส่งการตั้งค่าเหล่านั้น

  แสดงตัวอย่างรูปแบบไฟล์นำเข้า/ส่งออก

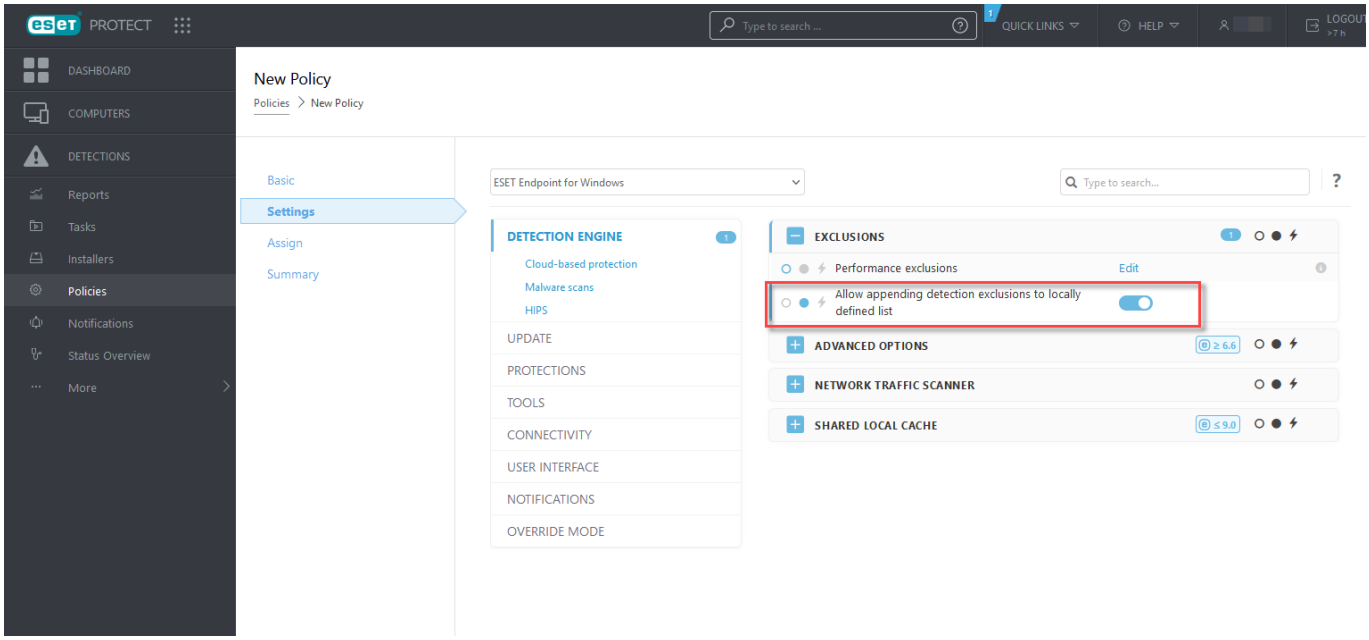
```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","File Hash"]}

4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

การตั้งค่าการยกเว้นการตรวจหาใน ESET PROTECT

วิซาร์ดสำหรับการจัดการการยกเว้นการตรวจหาESET PROTECT – สร้างการยกเว้นการตรวจหาและนำไปใช้กับคอมพิวเตอร์/กลุ่มอื่นๆ

การยกเว้นการตรวจหาที่เป็นไปได้จะแทนที่จาก ESET PROTECT

เมื่อมีการแสดงผลของรายการการยกเว้นการตรวจหาภายในเครื่องอยู่ ผู้ดูแลระบบต้องปรับใช้นโยบายที่ **อนุญาตการผนวกการยกเว้นการตรวจหาไปยังรายการที่กำหนดไว้ในเครื่อง** หลังจากนั้น การยกเว้นการตรวจหาเพิ่มเติมจาก ESET PROTECT จะทำงานตามที่คาดหมาย

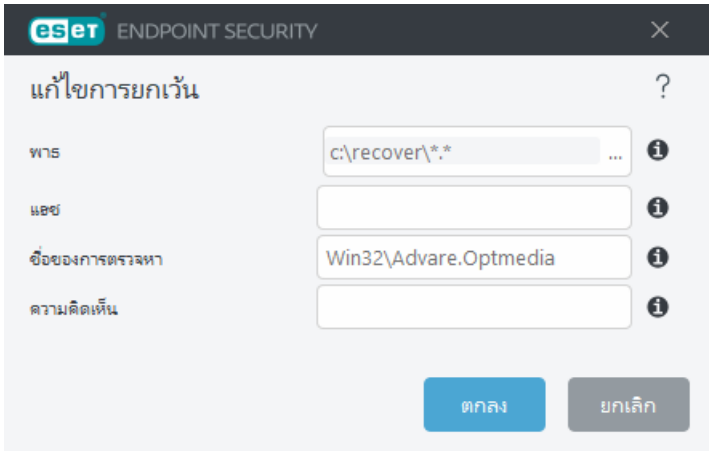


เพิ่มหรือแก้ไขการยกเว้นการตรวจหา

ยกเว้นการตรวจหา

ควรให้ชื่อของการตรวจหาของ ESET ที่ถูกต้อง สำหรับชื่อของการตรวจหาที่ถูกต้อง ให้ดู ไฟล์บันทึก แล้วเลือก **การตรวจหา** จากไฟล์บันทึกเมนูแบบเลื่อนลง จะเป็นประโยชน์เมื่อ ตัวอย่างของการตรวจพบที่ผิดพลาด ถูกตรวจพบใน ESET Endpoint Security การยกเว้นสำหรับการแฝงตัวแบบจริงจะเป็นสิ่งที่อันตรายมาก ให้พิจารณาให้ยกเว้นเฉพาะไฟล์ / ไดเรกทอรีที่ได้รับผลกระทบ โดยคลิก **...** ในช่อง **พาธ** และ/หรือเฉพาะช่วงชั่วคราว การยกเว้นยังใช้กับ แอพพลิเคชันที่อาจไม่พึงประสงค์ แอพพลิเคชันที่อาจไม่ปลอดภัยและแอพพลิเคชันที่น่าสงสัย

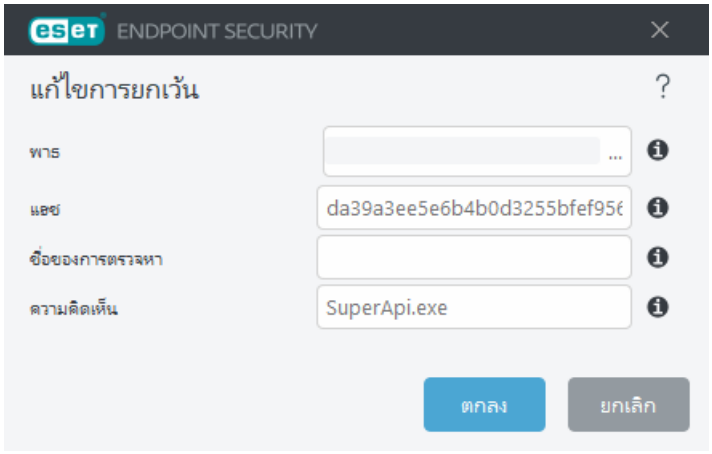
โปรดดู รูปแบบของการยกเว้นพาธ



โปรดดู ตัวอย่างการยกเว้นการตรวจหา ด้านล่าง

ไม่รวมแฮช

ยกเว้นไฟล์ที่อิงจากแฮชที่ระบุไว้ SHA-1 ไม่ว่าจะเป็นประเภทของไฟล์ ตำแหน่ง ชื่อ หรือส่วนขยายของไฟล์



หากต้องการยกเว้นการตรวจหาโดยอิงจากชื่อ ให้ป้อนชื่อของการตรวจหาที่ถูกต้อง:
Win32/Adware.Optmedia
คุณสามารถใช้รูปแบบต่อไปนี้ได้เมื่อคุณไม่รวมการตรวจหาจากหน้าต่างการเตือนESET Endpoint Security:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

องค์ประกอบการควบคุม

- **เพิ่ม** – ยกเว้นวัตถุจากการตรวจหา
- **แก้ไข** – ช่วยให้คุณสามารถแก้ไขรายการที่เลือกได้
- **ลบ** – ลบรายการต่างๆ ที่เลือกออก (CTRL + คลิกเพื่อเลือกรายการหลายรายการ)

สร้างวิซาร์ดการยกเว้นการตรวจหา

การยกเว้นการตรวจหายังสามารถสร้างจากเมนูบริบท ไฟล์บันทึก ได้อีกด้วย (ไม่สามารถใช้งานได้กับการตรวจหามัลแวร์):

1. ในหน้าต่างโปรแกรมหลัก ให้คลิก**เครื่องมือ** > **ไฟล์บันทึก**
2. คลิกขวาที่การตรวจหาใน **บันทึกการตรวจหา**
3. คลิก **สร้างการยกเว้น**

ในการยกเว้นการตรวจหาหนึ่งการตรวจหาหรือมากกว่าโดยอิงตาม **เกณฑ์การยกเว้น** ให้คลิก **เปลี่ยนเกณฑ์**:

- **ไฟล์เฉพาะ**ยกเว้นไฟล์แต่ละรายการโดยอิงแฮชSHA-1
- **การตรวจหา**ยกเว้นไฟล์แต่ละรายการโดยชื่อการตรวจหาของไฟล์
- **พาธ + การตรวจหา** – ยกเว้นไฟล์แต่ละรายการโดยชื่อการตรวจหาและพาธ รวมถึงชื่อไฟล์ (เช่น *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*)

ตัวเลือกที่แนะนำถูกเลือกไว้ล่วงหน้าโดยอิงตามประเภทการตรวจหา

อีกทางเลือกหนึ่ง คุณสามารถเพิ่ม **ความคิดเห็น** ก่อนคลิก **สร้างการยกเว้น** ได้

ตัวเลือกขั้นสูงของกลไกการตรวจจับ

เปิดใช้งานการสแกนขั้นสูงผ่าน AMSI เป็นเครื่องมืออินเทอร์เฟซการสแกนป้องกันมัลแวร์ของ Microsoft ที่ช่วยให้สามารถสแกนสคริปต์ PowerShell, สคริปต์ที่ดำเนินการโดย Windows Script Host และข้อมูลที่สแกนโดยใช้ AMSI SDK ได้

เครื่องมือสแกนการรับส่งข้อมูลเครือข่าย

เครื่องมือสแกนการรับส่งข้อมูลเครือข่ายให้การป้องกันมัลแวร์สำหรับโปรโตคอลแอพพลิเคชัน ซึ่งรวมเทคนิคการสแกนมัลแวร์ขั้นสูงเอาไว้หลายแบบ เครื่องมือสแกนการรับส่งข้อมูลเครือข่ายจะสแกนโปรโตคอล HTTP(S), POP3(S) และ IMAP(S) โดยอัตโนมัติกับทุกอินเทอร์เน็ตเบราว์เซอร์หรืออีเมลไคลเอ็นต์ คุณสามารถเปิด/ปิดเครื่องมือสแกนการรับส่งข้อมูลเครือข่ายได้ใน การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **เครื่องมือสแกนการรับส่งข้อมูลเครือข่าย**

เปิดใช้งานเครื่องมือสแกนการรับส่งข้อมูลเครือข่าย – หากคุณปิดใช้งานตัวเลือกนี้ โปรโตคอล HTTP(S), POP3(S) และ IMAP(S) จะไม่ถูกสแกน โปรดทราบว่าฟีเจอร์ของ ESET Endpoint Security ต่อไปนี้จำเป็นต้องเปิดใช้งานเครื่องมือสแกนการรับส่งข้อมูลบนเครือข่าย:

- การป้องกันการเข้าถึงเว็บ
- การควบคุมการเข้าถึงเว็บไซต์
- เบราว์เซอร์ปลอดภัย
- SSL/TLS
- การป้องกันฟิชชิ่ง
- การป้องกันอีเมลไคลเอ็นต์

การป้องกันแบบคลาวด์

ESET LiveGrid® (สร้างจากระบบการเตือนล่วงหน้าขั้นสูง ESET ThreatSense.Net) จะใช้ข้อมูลที่ผู้ใช้ ESET ส่งมาจากทั่วโลกและส่งข้อมูลไปยัง ESET Research Lab การให้ตัวอย่างที่น่าสงสัยและเมตาดาต้าจากหลากหลายแห่ง ESET LiveGrid® ทำให้เราสามารถตอบสนองความต้องการของลูกค้าได้ทันทีและทำให้ ESET สามารถโต้ตอบภัยคุกคามล่าสุดอยู่เสมอ

ตัวเลือกที่ใช้ได้มีดังนี้:

ตัวเลือกที่ 1: เปิดใช้งานระบบความน่าเชื่อถือของ ESET LiveGrid®

ระบบความเชื่อของ ESET LiveGrid® ให้บัญชีปลอดภัยและบัญชีดำในระบบคลาวด์

ตรวจสอบความเชื่อถือของกระบวนการที่ทำงานอยู่และไฟล์ได้โดยตรงจากส่วนติดต่อของโปรแกรมหรือเมนูบริบทที่มีข้อมูลเพิ่มเติมจาก ESET LiveGrid®

ตัวเลือกที่ 2: เปิดใช้งานระบบตรวจสอบป้อนกลับของ ESET LiveGrid®

ระบบคำติชม ESET LiveGrid® จะเก็บข้อมูลเกี่ยวกับคอมพิวเตอร์ของคุณที่เกี่ยวข้องกับภัยคุกคามที่ตรวจพบใหม่เพิ่มเติมจากระบบความเชื่อถือ ESET LiveGrid® ข้อมูลนี้อาจรวมถึงตัวอย่างหรือสำเนาของไฟล์ที่ภัยคุกคามนั้นปรากฏ พาธไปยังไฟล์นั้น ชื่อไฟล์ วันที่และเวลา กระบวนการที่ภัยคุกคามปรากฏบนคอมพิวเตอร์ของคุณ และข้อมูลเกี่ยวกับระบบปฏิบัติการของคอมพิวเตอร์ของคุณ

ตามค่าเริ่มต้น ESET Endpoint Security จะได้รับการกำหนดค่าส่งไฟล์ที่น่าสงสัยเพื่อรับการวิเคราะห์โดยละเอียดในห้องปฏิบัติการไวรัส ESET ไฟล์ที่มีนามสกุลบางอย่าง เช่น *.doc* หรือ *.xls* จะถูกยกเว้นเสมอ นอกจากนี้คุณยังสามารถเพิ่มนามสกุลอื่นๆ ถ้ามีไฟล์ชนิดใดที่คุณหรือองค์กรของคุณไม่ต้องการส่ง

ตัวเลือกที่ 3: เลือกไม่เปิดใช้งาน ESET LiveGrid®

คุณจะไม่สูญเสียการทำงานในซอฟต์แวร์ แต่ในบางกรณี ESET Endpoint Security อาจตอบสนองต่อภัยคุกคามใหม่ๆ ได้รวดเร็วกว่าการอัพเดทกลไกตรวจหาเมื่อเปิดใช้งาน ESET LiveGrid®

> อ่านเพิ่มเติมเกี่ยวกับ ESET LiveGrid® ใน ประมวลศัพท์
> ดู คำแนะนำพร้อมภาพประกอบ ของเราซึ่งมีให้แบบภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษาเกี่ยวกับวิธีการเปิดหรือปิดใช้งาน ESET LiveGrid® ใน ESET Endpoint Security

การกำหนดค่าการป้องกันแบบระบบคลาวด์ในการตั้งค่าขั้นสูง

หากต้องการเข้าถึงการตั้งค่าขั้นสูงสำหรับ ESET LiveGrid® ให้เปิด การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การป้องกันระบบคลาวด์**

เปิดใช้งานระบบความเชื่อถือของ ESET LiveGrid® (แนะนำ) – ระบบความเชื่อถือของ ESET LiveGrid® ปรับปรุงประสิทธิภาพของโซลูชันการป้องกันมัลแวร์ ESET ด้วยการเปรียบเทียบไฟล์ที่สแกนกับฐานข้อมูลรายการบัญชีปลอดภัยและบัญชีดำในคลาวด์

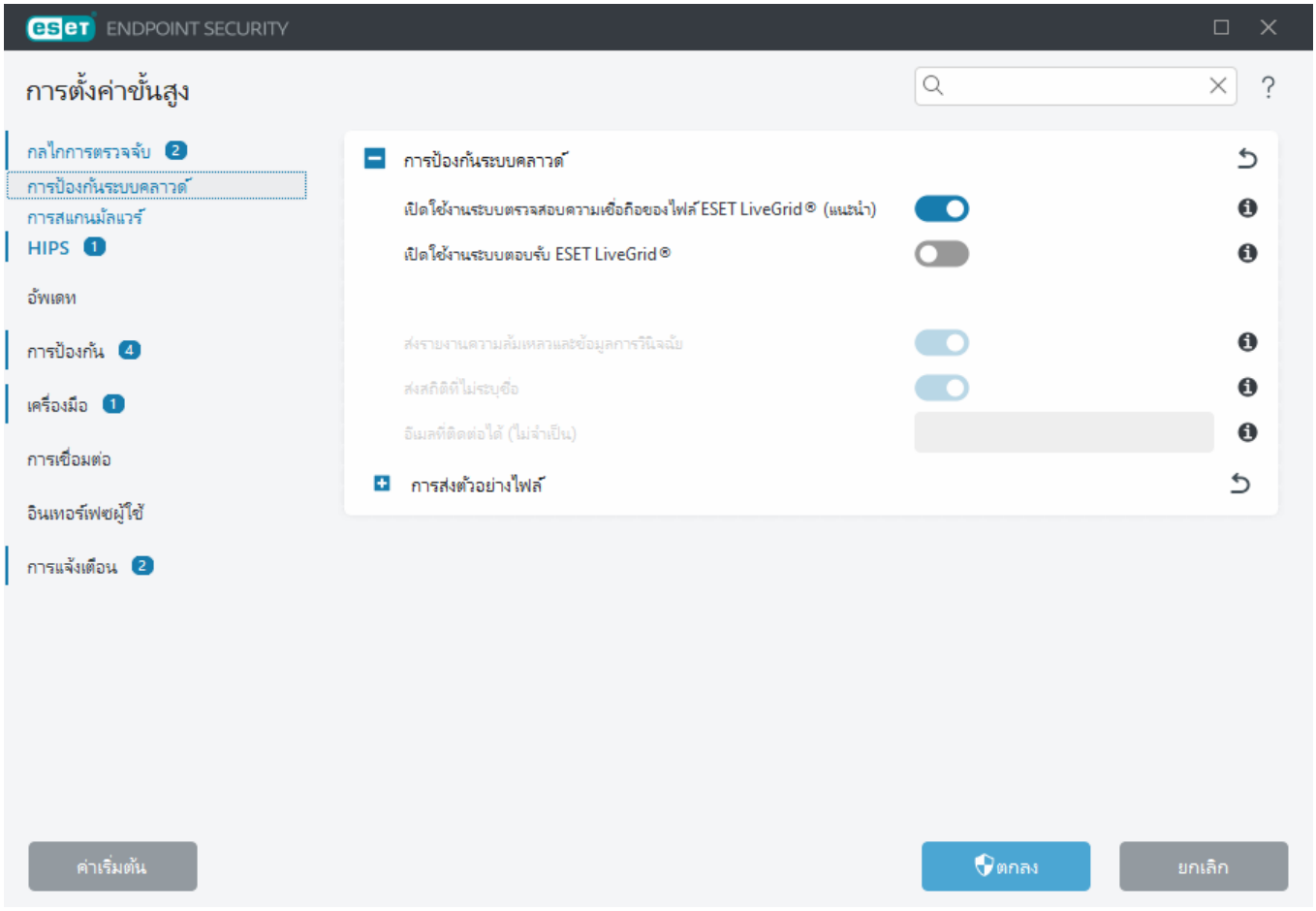
เปิดใช้งานระบบคำติชม ESET LiveGrid® – ส่งข้อมูลการส่งที่เกี่ยวข้อง (อธิบายไว้ใน**ส่วนการส่งตัวอย่าง**ด้านล่าง) พร้อมกับรายงานความผิดพลาดและสถิติไปยังห้องปฏิบัติการวิจัย ESET สำหรับวิเคราะห์เพิ่มเติม

เปิดใช้งาน ESET LiveGuard (ESET LiveGuard เป็นฟังก์ชันเพิ่มเติมที่จำหน่ายโดย ESET และไม่สามารถใช้งานได้ตามค่าเริ่มต้น) – ESET LiveGuard เป็นบริการแบบชำระเงินจาก ESET โดยมีจุดประสงค์เพื่อเพิ่มชั้นการปกป้องที่ออกแบบมาเฉพาะเพื่อลดภัยคุกคามชนิดใหม่ ซึ่งไฟล์ที่น่าสงสัยจะถูกส่งไปยังคลาวด์ของ ESET จากนั้นจะมีการวิเคราะห์ไฟล์เหล่านั้นด้วย กลไกการตรวจจับมัลแวร์ขั้นสูง ของเราภายในคลาวด์ ผู้ใช้ที่ให้ตัวอย่างจะได้รับรายงานพฤติกรรมซึ่งมีเนื้อหาสรุปของพฤติกรรมของตัวอย่างที่สังเกต

ส่งรายงานความล้มเหลวและข้อมูลการวินิจฉัย – ส่งข้อมูลการวินิจฉัยที่เกี่ยวข้องของ ESET LiveGrid® เช่น รายงานความผิดพลาดและโมดูลดัมพ์หน่วยความจำ เราขอแนะนำให้เปิดใช้งานสิ่งนี้ไว้เพื่อช่วยให้ ESET ปรับปรุงผลิตภัณฑ์และปกป้องผู้ใช้ปลายทาง

ส่งสถิติที่ไม่ระบุชื่อ – อนุญาตให้ ESET เก็บข้อมูลเกี่ยวกับภัยคุกคามใหม่ๆ ที่ตรวจพบ เช่น ชื่อภัยคุกคาม วันและเวลาที่ตรวจพบ วิธีที่ตรวจพบ และเมตาดาต้าที่เกี่ยวข้อง เวอร์ชันของผลิตภัณฑ์และการกำหนดค่า รวมถึงข้อมูลเกี่ยวกับระบบของคุณ

อีเมลที่ติดต่อ (ไม่จำเป็น) – อีเมลที่ติดต่อของคุณจะถูกส่งพร้อมกับไฟล์ที่น่าสงสัย และอาจใช้เพื่อติดต่อคุณในกรณีต้องการข้อมูลเพิ่มเติมเพื่อการวิเคราะห์ คุณจะไม่ได้รับการตอบกลับจาก ESET ยกเว้นกรณีที่ต้องการข้อมูลเพิ่มเติม



การส่งตัวอย่าง

การส่งตัวอย่างด้วยตนเอง – เปิดใช้ตัวเลือกในการส่งตัวอย่างไปยัง ESET ด้วยตนเองจากเมนูบริบท การกักเก็บ หรือ เครื่องมือ

ส่งตัวอย่างที่ตรวจพบโดยอัตโนมัติ

เลือกประเภทของตัวอย่างที่จะส่งไปยัง ESET เพื่อการวิเคราะห์และเพื่อปรับปรุงการตรวจหาในอนาคต ตัวเลือกที่ใช้ได้มีดังนี้:

- **ตัวอย่างไฟล์ที่ตรวจพบทั้งหมด** – วัตถุ ทั้งหมดที่ตรวจจับโดย กลไกการตรวจจับ (ซึ่งรวมถึงแอพพลิเคชั่นที่อาจไม่พึงประสงค์เมื่อเปิดใช้งานในการตั้งค่าเครื่องมือสแกน)
- **ตัวอย่างไฟล์ทั้งหมดยกเว้นเอกสาร** – วัตถุต่างๆ ที่ตรวจพบทั้งหมดยกเว้น **เอกสาร** (ดูด้านล่าง)
- **ไม่ส่ง** – วัตถุต่างๆ ที่ตรวจพบจะไม่ส่งไปยัง ESET

ส่งตัวอย่างที่น่าสงสัยโดยอัตโนมัติ

ตัวอย่างเหล่านี้จะถูกส่งไปยัง ESET ในกรณีที่กลไกการตรวจจับตรวจไม่พบ ตัวอย่างเช่น ตัวอย่างที่เกือบจะพลาด

การตรวจหาหรือหนึ่งใน โมดูลการป้องกัน ของ ESET Endpoint Security พิจารณาตัวอย่างเหล่านี้ว่าน่าสงสัยหรือมีพฤติกรรมที่ไม่ชัดเจน

- **ไฟล์ที่เรียกใช้ได้** – รวมถึงไฟล์ เช่น.exe, .dll, .sys
- **อาร์ไคฟ์** – รวมถึงประเภทไฟล์ เช่น .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab
- **สคริปต์** – รวมถึงประเภทไฟล์ เช่น .bat, .cmd, .hta, .js, .vbs, .ps1
- **อื่นๆ** – รวมถึงประเภทไฟล์ เช่น .jar, .reg, .msi, .sfw, .lnk
- **อีเมลสแปมที่เป็นไปได้** – วิธีนี้จะช่วยในการส่งสแปมส่วนต่างๆ ที่เป็นไปได้ หรืออีเมลสแปมที่เป็นไปได้ทั้งหมดพร้อมกับเอกสารแนบไปที่ ESET เพื่อวิเคราะห์ต่อไป การเปิดใช้งานตัวเลือกนี้จะช่วยปรับปรุงการตรวจหาสแปมโดยรวม รวมถึงการปรับปรุงการตรวจหาสแปมสำหรับคุณในอนาคตอีกด้วย
- **เอกสาร** – รวมถึงเอกสาร Microsoft Office หรือ PDF ที่มีหรือไม่มีเนื้อหาที่กำลังใช้งานอยู่

^ ขยายรายการประเภทไฟล์เอกสารที่รวมทั้งหมด

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

การยกเว้น

ตัวกรองการยกเว้นนี้จะช่วยให้คุณสามารถยกเว้นบางไฟล์/โฟลเดอร์จากการส่ง (ตัวอย่างเช่น อาจเป็นประโยชน์ในการไม่รวมไฟล์ที่อาจมีข้อมูลที่เป็นความลับ เช่น เอกสารหรือสเปรดชีต) โปรแกรมจะไม่ส่งไฟล์ที่อยู่ในรายการนี้ไปยังห้องทดลอง ESET เพื่อรับการวิเคราะห์ แม้ว่าจะมีรหัสที่น่าสงสัยก็ตาม ประเภทไฟล์ที่ใช้งานทั่วไปจะถูกยกเว้นตามค่าเริ่มต้น (.doc เป็นต้น) คุณสามารถเพิ่มในรายการของไฟล์ที่ยกเว้น ถ้าต้องการ

หากต้องการแยกไฟล์ที่ดาวน์โหลดจาก download.domain.com ให้ไปที่ การตั้งค่าขั้นสูง > **การป้องกันแบบระบบคลาวด์** > **การส่งตัวอย่าง** > **ข้อยกเว้น** และเพิ่มข้อยกเว้น *download.domain.com*

ขนาดสูงสุดของตัวอย่างไฟล์ (MB) – กำหนดขนาดสูงสุดของตัวอย่างที่ส่งผ่านระบบอัตโนมัติ (1-64 MB)

ESET LiveGuard

หากต้องการเปิดใช้งานบริการ ESET LiveGuard บนเครื่องไคลเอ็นต์โดยใช้เว็บคอนโซล ESET PROTECT ให้ดูที่ การกำหนดค่า ESET LiveGuard สำหรับ ESET Endpoint Security

หากคุณเคยใช้ ESET LiveGrid® ก่อนหน้านี้และปิดใช้งานไปแล้ว อาจยังคงมีแพ็คเกจข้อมูลที่ต้องส่ง แม้ว่าจะปิดใช้งานแล้ว โปรแกรมจะส่งแพ็คเกจดังกล่าวไปยัง ESET เมื่อส่งข้อมูลปัจจุบันทั้งหมดแล้ว โปรแกรมจะไม่สร้างแพ็คเกจเพิ่มเติมอีก

ตัวกรองการยกเว้นสำหรับการป้องกันระบบคลาวด์

ตัวกรองการยกเว้นนี้จะช่วยให้คุณสามารถยกเว้นบางไฟล์หรือโฟลเดอร์จากการส่งตัวอย่าง โปรแกรมจะไม่ส่งไฟล์ที่อยู่ในรายการนี้ไปยังห้องทดลอง ESET เพื่อรับการวิเคราะห์ แม้ว่าจะมีรหัสที่น่าสงสัยก็ตาม ประเภทไฟล์ที่ใช้งานทั่วไป (เช่น .doc เป็นต้น) จะถูกยกเว้นตามค่าเริ่มต้น

คุณลักษณะนี้จะมีประโยชน์ในการยกเว้นไฟล์ที่อาจมีข้อมูลลับเฉพาะ เช่น เอกสารหรือสเปรดชีท

หากต้องการแยกไฟล์ที่ดาวน์โหลดจาก download.domain.com ให้คลิก การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การป้องกันแบบระบบคลาวด์** > **การส่งตัวอย่าง** > **ข้อยกเว้น** และเพิ่มข้อยกเว้น *download.domain.com*

การสแกนมัลแวร์

ส่วน **การสแกนมัลแวร์** สามารถเข้าถึงได้จาก การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การสแกนมัลแวร์** และช่วยให้คุณกำหนดค่าพารามิเตอร์การสแกนสำหรับโปรไฟล์การสแกนได้

การสแกนตามต้องการ

โปรไฟล์ที่เลือก – ชุดที่ระบุของพารามิเตอร์ที่ใช้โดยเครื่องมือสแกนตามต้องการ เมื่อต้องการสร้างการสแกนใหม่ หากต้องการสร้างใหม่ ให้คลิก **แก้ไข** ถัดจาก **รายการของโปรไฟล์** ดูรายละเอียดเพิ่มเติมที่ โปรไฟล์การสแกน

หลังจากที่คุณเลือกโปรไฟล์การสแกนแล้วคุณสามารถกำหนดค่าตัวเลือกต่อไปนี้:

เป้าหมายการสแกน – หากคุณต้องการสแกนเป้าหมายเฉพาะเจาะจงหรือเป้าหมายเป็นกลุ่ม คุณสามารถคลิก **แก้ไข** ถัดจาก **เป้าหมายการสแกน** แล้วเลือกตัวเลือกจากโครงสร้างโฟลเดอร์ (ทรี) ดูรายละเอียดเพิ่มเติมที่ เป้าหมายการสแกน

การตอบกลับการสแกนและการตรวจจับตามต้องการ – คุณสามารถกำหนดค่าระดับการรายงานและการป้องกันสำหรับแต่ละโปรไฟล์การสแกนได้ ตามค่าเริ่มต้น โปรไฟล์การสแกนจะใช้การตั้งค่าเดียวกับที่กำหนดไว้ใน การป้องกันระบบไฟล์แบบเรียลไทม์ ปิดใช้งานปุ่มสลับถัดจาก **ใช้การตั้งค่าการป้องกันแบบเรียลไทม์** เพื่อกำหนดค่าระดับการรายงานที่กำหนดเองและการป้องกัน โปรดอ่าน การป้องกัน เพื่อรับคำอธิบายเกี่ยวกับการรายงานและระดับการป้องกันโดยละเอียด

ThreatSense – ตัวเลือกการตั้งค่าขั้นสูง เช่น นามสกุลไฟล์ที่คุณต้องการควบคุมและวิธีการตรวจหาที่ใช้ ดูรายล

ะเอียดเพิ่มเติมที่ ThreatSense

โปรไฟล์การสแกน

โปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าใน ESET Endpoint Security จะมีอยู่ด้วยกันทั้งหมด 4 รายการ:

- **การสแกนแบบสมาร์ท** - เป็นการสแกนขั้นสูงตามค่าเริ่มต้น โดยโปรไฟล์การสแกนแบบสมาร์ทใช้เทคโนโลยี Smart Optimization ซึ่งไม่รวมไฟล์ที่พบว่าปลอดภัยในการสแกนก่อนหน้านี้และไม่ได้ถูกแก้ไขตั้งแต่การสแกนครั้งก่อนหน้า วิธีนี้ช่วยให้เวลาในการสแกนลดลงโดยมีผลกระทบต่อความปลอดภัยของระบบน้อยที่สุด
- **การสแกนเมนูบริบท** - คุณสามารถเริ่มสแกนไฟล์ใดก็ได้จากเมนูบริบทได้ตามต้องการ โปรไฟล์การสแกนเมนูบริบทจะช่วยให้คุณกำหนดการกำหนดค่าการสแกนซึ่งจะใช้เมื่อคุณเปิดการสแกนวิธีนี้
- **สแกนเชิงลึก** - โปรไฟล์การสแกนเชิงลึกไม่ได้ใช้ Smart Optimization โดยค่าเริ่มต้น ดังนั้นจะไม่มีไฟล์ใดที่ไม่รวมอยู่ในการสแกนเมื่อใช้โปรไฟล์นี้
- **การสแกนคอมพิวเตอร์** - เป็นโปรไฟล์ตามค่าเริ่มต้นที่ใช้ในการสแกนคอมพิวเตอร์มาตรฐาน

คุณสามารถบันทึกพารามิเตอร์การสแกนที่ต้องการได้เพื่อการสแกนในอนาคต ขอแนะนำให้คุณสร้างโปรไฟล์อีกโปรไฟล์หนึ่ง (ที่มีเป้าหมายการสแกน วิธีการสแกน และพารามิเตอร์อื่นๆ) สำหรับแต่ละการสแกนที่ใช้เป็นประจำ

หากต้องการสร้างโปรไฟล์ใหม่ ให้เปิด การตั้งค่าขั้นสูง **กลไกการตรวจจับ** > **การสแกนมัลแวร์** > **การสแกนตามต้องการ** > **รายการโปรไฟล์** > **แก้ไข** หน้าต่าง **ตัวจัดการโปรไฟล์** มีเมนูแบบเลื่อนลง **โปรไฟล์ที่เลือก** ซึ่งแสดงโปรไฟล์การสแกนที่มีอยู่และตัวเลือกสำหรับสร้างโปรไฟล์ใหม่ เพื่อช่วยให้คุณสร้างโปรไฟล์การสแกนให้เหมาะสมกับความต้องการ โปรดไปที่ ThreatSense เพื่อดูคำอธิบายของพารามิเตอร์แต่ละรายการของการตั้งค่าการสแกน

> สมมติว่าคุณต้องการสร้างโปรไฟล์การสแกนของคุณเอง และการกำหนดค่า **การสแกนคอมพิวเตอร์ของคุณ**การกำหนดค่าบางส่วนเป็นสิ่งที่เหมาะสม แต่คุณไม่ต้องการสแกน รันไทม์แพ็คเกอร์ หรือ แอพพลิเคชันที่อาจไม่ปลอดภัย และคุณยังต้องการใช้ **ตรวจหาวิธีการแก้ไขเสมอ** ให้ป้อนชื่อของโปรไฟล์ใหม่ของคุณในหน้าต่าง **ตัวจัดการโปรไฟล์** แล้วคลิก **เพิ่ม** เลือกโปรไฟล์ใหม่ของคุณจากเมนูแบบเลื่อนลง **โปรไฟล์ที่เลือก** แล้วปรับพารามิเตอร์ที่เหลือเพื่อให้ตรงกับความต้องการ จากนั้นคลิก**ตกลง** เพื่อบันทึกโปรไฟล์ของคุณ

เป้าหมายการสแกน

คุณสามารถเลือกเป้าหมายการสแกนที่กำหนดไว้ล่วงหน้าจากเมนูแบบเลื่อนลง **เป้าหมายการสแกน**

- **ตามการตั้งค่าโปรไฟล์** - เลือกเป้าหมายที่ระบุในโปรไฟล์การสแกนที่เลือก
- **สื่อที่ถอดเข้าออกได้** – เลือกดิสเก็ตต์, อุปกรณ์เก็บข้อมูล USB, ซีดี/ดีวีดี

- **ไดรฟ์ในเครื่อง** – เลือกฮาร์ดไดรฟ์ของระบบทั้งหมด
- **ไดรฟ์เครือข่าย** – เลือกไดรฟ์เครือข่ายที่แมปทั้งหมด
- **การเลือกแบบกำหนดเอง** – ยกเลิกการเลือกก่อนหน้านี้ทั้งหมด

โครงสร้างโฟลเดอร์ (แบบต้นไม้) ยังมีเป้าหมายการสแกนที่เฉพาะเจาะจงอีกด้วย

- **หน่วยความจำที่ใช้งาน** – สแกนกระบวนการและข้อมูลทั้งหมดที่ใช้อยู่ในปัจจุบันโดยหน่วยความจำที่ใช้งาน
- **ส่วนการบูต/UEFI** – สแกนส่วนการบูตและ UEFI สำหรับมัลแวร์ที่มี อ่านเพิ่มเติมเกี่ยวกับเครื่องมือสแกน UEFI ได้ใน ประมวลศัพท์
- **ฐานข้อมูล WMI** – สแกนทั้งฐานข้อมูล Windows Management Instrumentation (WMI), เนมสเปซทั้งหมด, ตัวอย่างทุกระดับ และรวมถึงคุณสมบัติทั้งหมด การค้นหาสำหรับการอ้างอิงสำหรับไฟล์ที่ติดไวรัสหรือมัลแวร์ที่ฝังเป็นข้อมูล
- **รีจิสทรีของระบบ** – สแกนทั้งรีจิสทรีของระบบ, คีย์และคีย์ย่อยทั้งหมด การค้นหาสำหรับการอ้างอิงสำหรับไฟล์ที่ติดไวรัสหรือมัลแวร์ที่ฝังเป็นข้อมูล เมื่อทำความสะอาดการตรวจหา การอ้างอิงจะยังคงอยู่ในรีจิสทรีเพื่อให้แน่ใจว่าจะไม่มีข้อมูลที่สำคัญสูญหาย

หากต้องการไปยังเป้าหมายการสแกน (ไฟล์หรือโฟลเดอร์) อย่างรวดเร็ว ให้พิมพ์พาธของเป้าหมายดังกล่าวลงในช่องข้อความใต้ลำดับโครงสร้าง พาธต้องตรงตามตัวพิมพ์เล็กและใหญ่ โปรดเลือกกล่องกาเครื่องหมายในลำดับโครงสร้างหากต้องการให้ระบบสแกนเป้าหมายด้วย

การสแกนในสถานะไม่ใช้งาน

คุณสามารถเปิดใช้งานเครื่องมือสแกนที่อยู่ในสถานะไม่ได้ใช้งานใน การตั้งค่าขั้นสูง > **กลไกการตรวจหา** > **การสแกนมัลแวร์** > **การสแกนในสถานะไม่ได้ใช้งาน**

การสแกนในสถานะไม่ใช้งาน

เปิดใช้งานปุ่มสลับที่อยู่ถัดจาก **เปิดใช้งานการสแกนในสถานะไม่ใช้งาน** เพื่อเปิดใช้งานฟีเจอร์นี้ เมื่อคอมพิวเตอร์อยู่ในสถานะที่ไม่ได้ใช้งาน การสแกนคอมพิวเตอร์แบบเงียบจะดำเนินการบนไดรฟ์ในระบบทั้งหมด

ตามค่าเริ่มต้น การสแกนในสถานะจะไม่ทำงานเมื่อคอมพิวเตอร์ (โน้ตบุ๊ค) กำลังใช้งานแบตเตอรี่ คุณสามารถเขียนทับการตั้งค่านี้ได้โดยเปิดใช้งานแถบเลื่อนที่อยู่ถัดจาก **เรียกใช้แม้ขณะที่คอมพิวเตอร์ใช้พลังงานแบตเตอรี่** ใน

การตั้งค่าขั้นสูง

เปิดใช้งานแถบเลื่อนถัดจากตัวเลือก**เปิดใช้งานการบันทึก**ในการตั้งค่าขั้นสูงเพื่อบันทึกเอาท์พุตการสแกนคอมพิวเตอร์ในส่วนไฟล์บันทึก (จากหน้าต่างหลักของโปรแกรม ให้คลิก**เครื่องมือ** > **ไฟล์บันทึก** แล้วเลือก**การสแกนคอมพิวเตอร์**จากเมนู**บันทึก**แบบเลื่อนลง)

การตรวจหาสภาวะไม่ใช้งาน

ดู การตรวจหาสภาวะไม่ใช้งาน สำหรับรายการแบบเต็มของเงื่อนไขที่จะต้องให้ตรง เพื่อเรียกใช้เครื่องเครื่องสแกนที่มีสถานะไม่ใช้งาน

ThreatSense – ตัวเลือกการตั้งค่าขั้นสูง เช่น นามสกุลไฟล์ที่คุณต้องการควบคุมและวิธีการตรวจหาที่ใช้ ดูรายละเอียดเพิ่มเติมที่ ThreatSense

การตรวจหาสภาวะไม่ใช้งาน

การตั้งค่าการตรวจหาสภาวะไม่ใช้งาน การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การสแกนมัลแวร์** > **การสแกนในสถานะไม่ใช้งาน** > **การตรวจหาสภาวะไม่ใช้งาน** การตั้งค่าเหล่านี้ระบุการเรียกใช้สำหรับ การสแกนในสถานะไม่ใช้งาน:

- **ปิดหน้าจอหรือสกรีนเซฟเวอร์**
- **ล็อคคอมพิวเตอร์**
- **ผู้ใช้ออกจากระบบ**

ใช้ปุ่มสลับสำหรับแต่ละสถานะที่สอดคล้องกันเพื่อเปิดหรือปิดใช้งานการเรียกใช้การตรวจหาสถานะไม่ได้ใช้งาน

การสแกนเมื่อเริ่มต้น

ตามค่าเริ่มต้น การตรวจสอบไฟล์เมื่อเริ่มต้นระบบอัตโนมัติจะดำเนินการเมื่อเริ่มต้นระบบและในระหว่างการอัพเดทกลไกตรวจหา การสแกนนี้จะขึ้นอยู่กับ การกำหนดค่าเครื่องมือวางกำหนดการและงาน

ตัวเลือกการสแกนเมื่อเริ่มต้น เป็นส่วนหนึ่งของงานของเครื่องมือวางกำหนดการ **การตรวจสอบไฟล์เมื่อเริ่มต้นระบบ** ในการแก้ไขการตั้งค่า ให้ไปที่**เครื่องมือ** > **เครื่องมือวางกำหนดการ** แล้วคลิกที่**การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้นอัตโนมัติ** จากนั้นก็**แก้ไข** ในขั้นตอนสุดท้าย หน้าต่าง การตรวจสอบไฟล์เมื่อ

การอัพเดทฐานข้อมูลไวรัสเสร็จสิ้น จะปรากฏขึ้น สำหรับคำแนะนำโดยละเอียดเกี่ยวกับการสร้างและการจัดการงานของเครื่องมือวางกำหนดการ โปรดดูที่ การสร้างงานใหม่

ThreatSense – ตัวเลือกการตั้งค่าขั้นสูง เช่น นามสกุลไฟล์ที่คุณต้องการควบคุมและวิธีการตรวจหาที่ใช้ ดูรายละเอียดเพิ่มเติมที่ ThreatSense

การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้น

เมื่อสร้างงานตามกำหนดการ การตรวจสอบไฟล์เมื่อเริ่มต้นระบบ คุณจะมีตัวเลือกมากมายเพื่อปรับพารามิเตอร์ต่อไปนี้:

เมนูแบบเลื่อนลง **เป้าหมายการสแกน** จะระบุความลึกของการสแกนสำหรับไฟล์ที่เรียกใช้เมื่อเริ่มต้นระบบโดยดูจากอัลกอริทึมที่สลับซับซ้อนและเป็นความลับ ไฟล์จะจัดเรียงในลำดับมากไปหาน้อยตามไฟล์ต่อไปนี้:

- **ไฟล์ที่ลงทะเบียนทั้งหมด** (สแกนไฟล์มากที่สุด)
- **ไฟล์ที่ไม่ได้ใช้บ่อย**
- **ไฟล์ที่ใช้บ่อย**
- **ไฟล์ที่ใช้บ่อยที่สุด**
- **เฉพาะไฟล์ที่ใช้บ่อยที่สุด** (สแกนไฟล์น้อยที่สุด)

กลุ่มเฉพาะสองกลุ่มที่รวมอยู่ด้วยคือ:

- **ไฟล์ที่ใช้งานก่อนผู้ใช้เข้าสู่ระบบ** – ประกอบด้วยไฟล์จากตำแหน่งที่สามารถเข้าถึงได้โดยที่ผู้ใช้ไม่ต้องเข้าสู่ระบบ (รวมถึงตำแหน่งการเริ่มต้นของระบบเกือบทั้งหมด เช่น บริการ, วัตถุตัวช่วยเหลือเบราว์เซอร์, แจ้ง Winlogon, รายการเครื่องมือวางกำหนดการของ Windows, dlls ที่รู้จัก เป็นต้น)
- **ไฟล์ที่ทำงานหลังผู้ใช้เข้าสู่ระบบ** - ประกอบด้วยไฟล์จากตำแหน่งที่สามารถเข้าถึงได้หลังจากที่ผู้ใช้เข้าสู่ระบบแล้วเท่านั้น (ประกอบด้วยไฟล์ที่เรียกใช้โดยผู้ใช้ที่กำหนด โดยทั่วไปจะเป็นไฟล์ใน *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*)

รายการไฟล์ที่จะสแกนจะมีการแก้ไขสำหรับแต่ละกลุ่มข้างต้น หากคุณเลือกสแกนไฟล์ที่เรียกใช้เมื่อเริ่มต้นระบบด้วยการสแกนที่มีความลึกต่ำกว่า ไฟล์ที่ไม่ได้สแกนจะถูกสแกนเมื่อเปิดหรือดำเนินการ

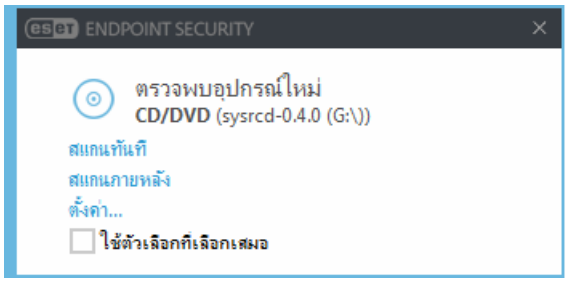
ความสำคัญของการสแกน – ระดับความสำคัญที่ใช้เพื่อกำหนดเวลาที่จะเริ่มต้นสแกน:

- **เมื่อไม่ได้ใช้งาน** – งานจะดำเนินการเฉพาะเมื่อระบบไม่ได้ใช้งาน
- **ต่ำที่สุด** - การโหลดระบบในระดับต่ำที่สุด
- **ต่ำกว่า** – การโหลดระบบในระดับต่ำ
- **ปกติ** – การโหลดระบบในระดับเฉลี่ย

สื่อที่ถอดเข้าออกได้

ESET Endpoint Security จะทำการสแกนสื่อแบบถอดได้ (ซีดี/ดีวีดี/USB/...) โดยอัตโนมัติเมื่อใส่สื่อเข้าไปในคอมพิวเตอร์ ซึ่งอาจเป็นประโยชน์ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์ต้องการป้องกันไม่ให้ผู้ใช้ใช้งานสื่อที่ถอดเข้าออกได้ที่มีเนื้อหาที่ไม่พึงประสงค์

เมื่อใส่สื่อที่ถอดเข้าออกได้ และมีการตั้งค่า **แสดงตัวเลือกการสแกน** ใน การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การสแกนมัลแวร์** > **สื่อที่ถอดเข้าออกได้** ระบบจะแสดงข้อความต่อไปนี้:



ตัวเลือกสำหรับกล่องโต้ตอบนี้:

- **สแกนเดี๋ยวนี้** – ตัวเลือกนี้จะเรียกใช้การสแกนอุปกรณ์สื่อที่ถอดเข้าออกได้
- **ไม่ต้องสแกน** – สื่อที่ถอดเข้าออกได้จะไม่ถูกสแกน
- **ตั้งค่า** – เปิดการตั้งค่าขั้นสูง
- **ใช้ตัวเลือกที่เลือกเสมอ** – เมื่อเลือกตัวเลือกนี้ การดำเนินการแบบเดิมจะเกิดขึ้นเมื่อใส่อุปกรณ์สื่อที่ถอดเข้าออกได้ในเวลาอื่น

นอกจากนี้ ESET Endpoint Security จะมีคุณลักษณะของฟังก์ชันการควบคุมอุปกรณ์ ซึ่งช่วยให้คุณสามารถกำหนดกฎในการใช้งานอุปกรณ์ภายนอกบนเครื่องคอมพิวเตอร์ที่ระบุได้ สามารถดูรายละเอียดเพิ่มเติมเกี่ยวกับการควบคุมอุปกรณ์ได้ในส่วน สื่อที่ถอดเข้าออกได้

ในการเข้าถึงการตั้งค่าสำหรับการสแกนสื่อที่ถอดเข้าออกได้ ให้เปิด การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การ**

สแกนมัลแวร์ > สื่อที่ถอดเข้าออกได้

การกระทำหลังใส่สื่อที่สามารถถอดเข้าออกได้ – เลือกการทำงานเริ่มต้นที่จะดำเนินการเมื่อใส่อุปกรณ์สื่อที่ถอดเข้าออกได้ในคอมพิวเตอร์ (ซีดี/ดีวีดี/USB) เลือกการกระทำที่ต้องการขณะใส่สื่อที่ถอดเข้าออกได้ในคอมพิวเตอร์:

- **ไม่ต้องสแกน** – โปรแกรมจะไม่ดำเนินการ และหน้าต่าง **ตรวจพบอุปกรณ์ใหม่** จะไม่เปิด
- **สแกนอุปกรณ์โดยอัตโนมัติ** – จะทำการสแกนคอมพิวเตอร์สำหรับอุปกรณ์สื่อที่ถอดเข้าออกได้
- **บังคับสแกนอุปกรณ์**–จะทำการสแกนคอมพิวเตอร์สำหรับอุปกรณ์สื่อที่ถอดเข้าออกได้ และไม่สามารถยกเลิกได้
- **แสดงตัวเลือกการสแกน** – เปิดส่วนการตั้งค่า**สื่อที่ถอดเข้าออกได้**

การป้องกันเอกสาร

คุณลักษณะการป้องกันเอกสารจะสแกนเอกสาร Microsoft Office ก่อนที่จะเปิด รวมถึงไฟล์ที่ดาวน์โหลดจาก Internet Explorer โดยอัตโนมัติ เช่น องค์ประกอบ Microsoft ActiveX การป้องกันเอกสารมีระดับการป้องกันอีกชั้นหนึ่งนอกเหนือจากการป้องกันระบบไฟล์แบบเรียลไทม์ และสามารถถูกปิดใช้งานเพื่อเพิ่มประสิทธิภาพการทำงานในระบบที่ไม่ได้รองรับเอกสาร Microsoft Office จำนวนมาก

หากต้องการเปิดใช้งานการป้องกันไฟล์เอกสาร ให้เปิดหน้าต่าง การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การสแกนมัลแวร์** > **การป้องกันไฟล์เอกสาร** แล้วคลิกแถบเลื่อนถัดจาก **เปิดใช้งานการป้องกันไฟล์เอกสาร**

ThreatSense – ตัวเลือกการตั้งค่าขั้นสูง เช่น นามสกุลไฟล์ที่คุณต้องการควบคุมและวิธีการตรวจหาที่ใช้ ดูรายละเอียดเพิ่มเติมที่ ThreatSense

คุณลักษณะนี้เปิดใช้งานโดยแอพพลิเคชันที่ใช้ Microsoft Antivirus API (เช่น Microsoft Office 2000 ขึ้นไป หรือ Microsoft Internet Explorer 5.0 ขึ้นไป)

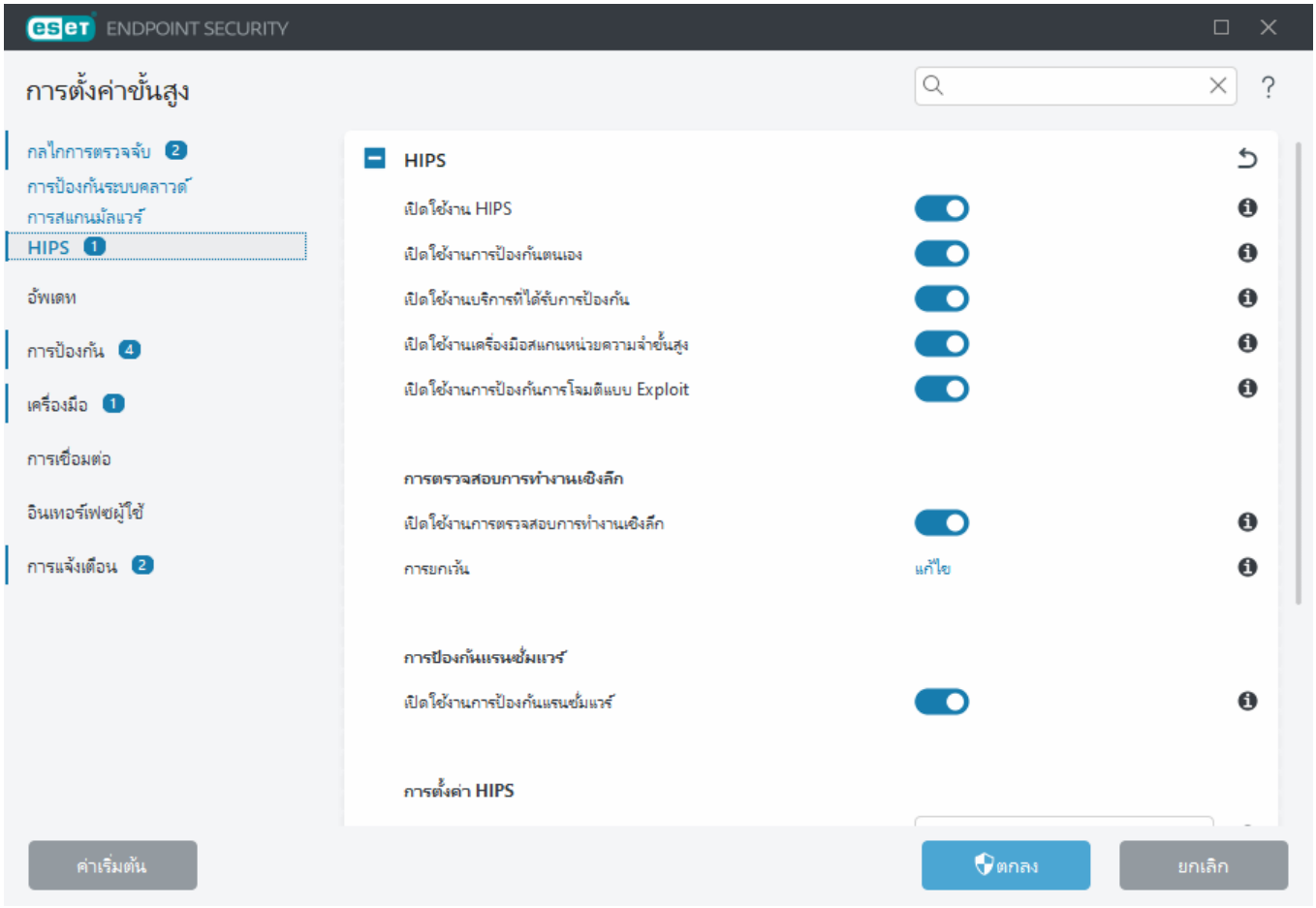
HIPS – ระบบป้องกันการบุกรุกที่ใช้โฮสต์

การเปลี่ยนเป็นการตั้งค่า HIPS ควรดำเนินการโดยผู้ใช้ที่มีประสบการณ์ในการใช้งานเท่านั้น การกำหนดค่าที่ไถูกต้องของการตั้งค่า HIPS จะทำให้ระบบมีปัญหาด้านเสถียรภาพ

ระบบ ป้องกันการบุกรุกที่ใช้โฮสต์ (HIPS) จะป้องกันระบบของคุณจากมัลแวร์และกิจกรรมที่ไม่พึงประสงค์ที่พยายามสร้างผลเสียต่อคอมพิวเตอร์ HIPS ใช้การวิเคราะห์การทำงานขั้นสูงร่วมกับความสามารถในการตรวจหาของการกรองเครือข่าย เพื่อตรวจสอบกระบวนการที่ทำงานอยู่ ไฟล์และรหัสรีจิสตรี HIPS แยกต่างหากจากการป้องกัน

ระบบไฟล์แบบเรียลไทม์และไม่ใช่ไฟร์วอลล์ แต่จะติดตามเฉพาะกระบวนการที่ทำงานอยู่ภายในระบบปฏิบัติการเท่านั้น

คุณสามารถกำหนดการตั้งค่า HIPS ได้ใน การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **HIPS** > **ระบบป้องกันการบุกรุกโฮสต์** สถานะของ HIPS (เปิดใช้งาน/ปิดใช้งาน) จะปรากฏใน หน้าต่างโปรแกรมหลัก ESET Endpoint Security > **การตั้งค่า** > **คอมพิวเตอร์**



HIPS

เปิดใช้งาน HIPS – เปิดใช้งาน HIPS เป็นค่าเริ่มต้นในESET Endpoint Security การปิด HIPS จะปิดการใช้งานคุณลักษณะของ HIPS ที่เหลือ เช่น การป้องกันการโจมตีแบบ Exploit

เปิดใช้งานการป้องกันตนเอง – ESET Endpoint Security ใช้เทคโนโลยี**การป้องกันตนเอง** ในตัว ซึ่งเป็นส่วนหนึ่งของ HIPS เพื่อป้องกันซอฟต์แวร์ที่เป็นอันตรายจากความเสียหายหรือการเปิดใช้งานการป้องกันไวรัสและสปายแวร์ การป้องกันตนเองจะป้องกันระบบที่สำคัญและกระบวนการของ ESET รหัสรีจิสตรีและไฟล์ต่างๆ จากการถูกเปลี่ยนแปลง เอเจนท์ ESET Management จะได้รับการปกป้องเช่นเดียวกันเมื่อติดตั้ง

เปิดใช้งานบริการที่ได้รับการป้องกัน – เปิดใช้การป้องกันสำหรับ บริการ ESET (ekrn.exe) เมื่อเปิดใช้งานแล้ว

บริการจะเริ่มต้นโดยเป็นกระบวนการ Windows ที่ได้รับการป้องกันเพื่อป้องกันการโจมตีจากมัลแวร์ โดยตัวเลือกนี้จะมีให้ใช้งานใน Windows 8.1 และ Windows 10

เครื่องสแกนหน่วยความจำขั้นสูง ทำงานผสมผสานกับการปิดกั้นการโจมตีเบราเซอร์เพื่อเสริมสร้างการป้องกันมัลแวร์ที่ถูกออกแบบมาเพื่อหลบเลี่ยงการตรวจหาของผลิตภัณฑ์การป้องกันมัลแวร์ด้วยวิธี obfuscation หรือการเข้ารหัส เครื่องมือสแกนหน่วยความจำขั้นสูงจะเปิดใช้งานตามค่าเริ่มต้น อ่านข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้ใน ประมวลศัพท์

เปิดใช้งานการป้องกันการโจมตีแบบ Exploit – ได้รับการออกแบบมาเพื่อปกป้องประเภทของแอพพลิเคชันที่มักถูกโจมตี เช่น เว็บเบราว์เซอร์ PDF ผู้อ่าน อีเมลไคลเอ็นต์และองค์ประกอบของ MS Office การป้องกันการโจมตีแบบ Exploit จะเปิดใช้งานเป็นค่าเริ่มต้น อ่านข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้ใน ประมวลศัพท์

การตรวจสอบการทำงานเชิงลึก

การตรวจสอบการทำงานเชิงลึก เป็นระดับการปกป้องอีกชั้นหนึ่งซึ่งทำงานโดยเป็นส่วนหนึ่งของคุณสมบัติ HIPS ส่วนขยายของ HIPS นี้จะวิเคราะห์พฤติกรรมของโปรแกรมทั้งหมดที่เรียกใช้บนคอมพิวเตอร์ และเตือนคุณหากพฤติกรรมของกระบวนการเป็นอันตราย

การยกเว้น HIPS จากการตรวจสอบการทำงานเชิงลึก จะช่วยให้คุณสามารถยกเว้นกระบวนการจากการวิเคราะห์ได้ ในการทำให้แน่ใจว่าจะมีการสแกนกระบวนการทำงานทั้งหมดเพื่อหาภัยคุกคาม เราขอแนะนำให้สร้างข้อยกเว้นต่อเมื่อจำเป็นจริงๆ เท่านั้น

โล่ห์ป้องกันแรนซัมแวร์

เปิดโล่ห์ป้องกันโปรแกรมเรียกค่าไถ่ – เป็นระดับการป้องกันอีกชั้นหนึ่งที่ทำงานเป็นส่วนหนึ่งของคุณลักษณะ HIPS คุณจะต้องเปิดใช้งานระบบความเชื่อถือ ESET LiveGrid® เอาไว้จึงจะสามารถใช้งานโล่ห์ป้องกันโปรแกรมเรียกค่าไถ่ได้ อ่านเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้

เปิดใช้งาน Intel® Threat Detection Technology – ช่วยตรวจจับการโจมตีของแรนซัมแวร์โดยใช้ Telemetry ของ CPU Intel ที่เป็นเอกลักษณ์เพื่อเพิ่มประสิทธิภาพการตรวจจับ ลดผลลัพธ์ที่ผิด และขยายการมองเห็นเพื่อจับเทคนิคการหลบเลี่ยงขั้นสูงได้ ดู ตัวประมวลผลที่รองรับ

เปิดใช้งานโหมดตรวจสอบ – ทุกสิ่งที่การป้องกันแรนซัมแวร์ตรวจพบจะไม่ถูกปิดกั้นโดยอัตโนมัติ แต่จะถูกบันทึกโดยมีการแจ้งเตือนความรุนแรงและถูกส่งไปยังคอนโซลการจัดการพร้อมด้วยธง "โหมดตรวจสอบ" ผู้ดูแลระบบสามารถตัดสินใจได้ว่าจะยกเว้นการตรวจหาดังกล่าวเพื่อป้องกันการตรวจหาเพิ่มเติม หรืออนุญาตการตรวจหา

ต่อไป ซึ่งการกระทำเช่นนี้หมายถึงว่าหลังโหมดตรวจสอบสิ้นสุดลง รายการที่ถูกตรวจพบจะถูกปิดกั้นและลบออก การเปิดใช้งาน/ปิดใช้งานโหมดตรวจสอบจะเป็นการล็อกอินสู่ ESET Endpoint Security อีกด้วย ตัวเลือกนี้จะสามารถใช้งานได้เฉพาะในตัวแก้ไขการกำหนดค่านโยบาย ESET PROTECT เท่านั้น

การตั้งค่า HIPS

โหมดการกรอง สามารถทำงานได้ในหนึ่งในโหมดต่อไปนี้:

โหมดการกรอง	คำอธิบาย
โหมดอัตโนมัติ	มีการเปิดใช้งานการดำเนินการโดยยกเว้นการดำเนินการที่ถูกปิดกั้นตามกฎที่กำหนดไว้ล่วงหน้าเพื่อปกป้องระบบของคุณ
โหมดสมาร์ท	ผู้ใช้จะได้รับแจ้งเฉพาะเหตุการณ์ที่น่าสงสัยมากเท่านั้น
โหมดโต้ตอบ	ผู้ใช้จะได้รับข้อความให้ยืนยันการดำเนินการ
โหมดนโยบาย	ปิดกั้นการดำเนินการทั้งหมดที่ไม่ได้ถูกกำหนดโดยกฎเฉพาะที่อนุญาตให้มีการดำเนินการนั้น
โหมดเรียนรู้	การดำเนินการเปิดใช้งานอยู่และกฎจะถูกสร้างหลังจากการดำเนินการแต่ละครั้ง คุณสามารถดูกฎที่สร้างในโหมดนี้ได้ในตัวแก้ไข **กฎ HIPS** แต่ลำดับความสำคัญจะอยู่ต่ำกว่าลำดับความสำคัญของกฎที่สร้างขึ้นด้วยตนเองหรือกฎที่สร้างในโหมดอัตโนมัติ เมื่อคุณเลือก **โหมดการเรียนรู้** จากเมนูแบบเลื่อนลงของ **โหมดการกรอง** การตั้งค่า **โหมดการเรียนรู้ยุติที่** จะสามารถใช้งานได้ ให้เลือกระยะเวลาที่คุณต้องการใช้งานโหมดการเรียนรู้ ตัวอย่างเช่น ช่วงเวลาสูงสุด 14 วัน เมื่อเกินช่วงเวลาที่ระบุระบบจะขอให้คุณแก้ไขกฎที่ HIPS สร้างเมื่ออยู่ในโหมดการเรียนรู้ อีกทั้งคุณยังสามารถเลือกสร้างโหมดการกรองอื่น หรือขยายเวลาการตัดสินใจและใช้งานโหมดการเรียนรู้ต่อได้

โหมดได้รับการตั้งค่าหลังจากโหมดการเรียนรู้หมดอายุ – เลือกโหมดการกรองที่จะถูกใช้งานหลังจากที่โหมดการเรียนรู้หมดอายุ หลังจากหมดอายุ ตัวเลือก **ถามผู้ใช้** จะต้องใช้สิทธิ์อนุญาตของผู้ดูแลระบบเพื่อทำการเปลี่ยนแปลงโหมดการกรอง HIPS

ระบบ HIPS จะตรวจสอบเหตุการณ์ภายในระบบปฏิบัติการและตอบสนองตามกฎที่คล้ายกับกฎจากไฟร์วอลล์ คลิก **แก้ไข** ถัดจาก **กฎ** เพื่อเปิดหน้าต่างการจัดการ**กฎของ HIPS** ในหน้าต่างการจัดการกฎของ HIPS คุณสามารถเลือก เพิ่ม แก้ไข หรือลบกฎได้ คุณสามารถดูรายละเอียดเพิ่มเติมเกี่ยวกับการสร้างกฎและการดำเนินการ HIPS ได้ใน แก้ไขกฎ HIPS

การยกเว้น HIPS

การยกเว้นทำให้คุณยกเว้นกระบวนการต่างๆ จากการตรวจสอบการทำงานเชิงลึกของ HIPS ได้

หากต้องการแก้ไขข้อยกเว้นของ HIPS ให้เปิด การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **HIPS** > **ระบบป้องกันการบุกรุกโฮสต์** > **การยกเว้น** > **แก้ไข**

อย่าสับสนกับ นามสกุลไฟล์ที่ยกเว้น การตรวจหานามสกุลไฟล์ การยกเว้นการทำงาน หรือ การยกเว้นกระบวนการ

หากต้องการยกเว้นวัตถุ ให้คลิก **เพิ่ม** แล้วป้อนพาธไปยังวัตถุหรือเลือกวัตถุในโครงสร้าง คุณยังสามารถแก้ไขหรือลบรายการที่เลือกไว้ได้ด้วย

การตั้งค่า HIPS ขั้นสูง

ตัวเลือกต่อไปนี้มีประโยชน์สำหรับการแก้ไขข้อบกพร่องและการวิเคราะห์ลักษณะของแอพพลิเคชัน:

อนุญาตให้โหลดไดรเวอร์ได้เสมอ – ไดรเวอร์ที่เลือกจะได้รับอนุญาตให้โหลดเสมอโดยไม่คำนึงถึงโหมดการกรองที่กำหนดค่าไว้ เว้นแต่จะมีการปิดกั้นอย่างชัดเจนโดยกฎของผู้ใช้

บันทึกการดำเนินการที่ปิดกั้นทั้งหมด – การดำเนินการที่ปิดกั้นทั้งหมดจะถูกเขียนไปที่บันทึก HIPS ใช้คุณลักษณะนี้เฉพาะเมื่อแก้ไขปัญหาหรือร้องขอโดยฝ่ายสนับสนุนด้านเทคนิคของ ESET เนื่องจากการดำเนินการนี้อาจสร้างไฟล์บันทึกขนาดใหญ่และทำให้คอมพิวเตอร์ของคุณช้าลง

แจ้งเมื่อมีการเปลี่ยนแปลงในแอพพลิเคชันการเริ่มต้น – แสดงการแจ้งเตือนบนเดสก์ท็อปในแต่ละครั้งที่มีการเพิ่มหรือลบแอพพลิเคชันจากการเริ่มต้นระบบ

อนุญาตให้โหลดไดรเวอร์ได้เสมอ

ไดรเวอร์ที่แสดงในรายการนี้จะได้รับอนุญาตให้โหลดเสมอโดยไม่คำนึงถึงโหมดการกรอง HIPS เว้นแต่จะมีการปิดกั้นอย่างชัดเจนโดยกฎของผู้ใช้

เพิ่ม – เพิ่มไดรเวอร์ใหม่

แก้ไข – แก้ไขไดรเวอร์ที่เลือก

ลบออก – ลบไดรเวอร์ออกจากรายการ

รีเซ็ต – โหลดชุดของไดรเวอร์ระบบอีกครั้ง

คลิก **รีเซ็ต** หากคุณไม่ต้องการให้รวมไดรเวอร์ที่คุณได้เพิ่มเอง ตัวเลือกนี้มีประโยชน์หากคุณเพิ่มไดรเวอร์หลายตัวและคุณไม่สามารถลบไดรเวอร์เหล่านั้นออกจากรายการ

หลังจากติดตั้งแล้ว รายการไดรเวอร์จะว่างเปล่า ESET Endpoint Security จะกรอกรายการดังกล่าวโดยอัตโนมัติเมื่อเวลาผ่านไป

ไดร์เวอร์ที่อนุญาตให้โหลดได้เสมอจะขึ้นอยู่กับแต่ละอุปกรณ์และไม่สามารถแก้ไขได้โดยใช้นโยบาย ESET PROTECT หลังจากติดตั้งแล้ว รายการไดรเวอร์จะว่างเปล่า ESET Endpoint Security จะกรอกรายการดังกล่าวโดยอัตโนมัติเมื่อเวลาผ่านไป

หน้าต่างโต้ตอบ HIPS

หน้าต่างการแจ้งเตือน HIPS จะช่วยให้คุณสร้างกฎตามการทำงานใหม่ที่ HIPS ตรวจพบแล้วระบุเงื่อนไขต่างๆ ว่าจะอนุญาตหรือปฏิเสธการทำงานนั้น

กฎที่สร้างจากหน้าต่างการแจ้งเตือนจะถูกพิจารณาให้เทียบเท่ากับกฎที่สร้างด้วยตนเอง กฎที่สร้างจากหน้าต่างการแจ้งเตือนสามารถมีความเจาะจงได้น้อยกว่ากฎที่เรียกหน้าต่างข้อความนั้นได้ ซึ่งหมายความว่าหลังจากที่สร้างกฎในกล่องข้อความแล้ว การดำเนินการเดียวกันสามารถเรียกใช้หน้าต่างเดียวกันได้ สำหรับข้อมูลเพิ่มเติม ให้ดู ลำดับความสำคัญสำหรับกฎ HIPS

หากการทำงานเริ่มต้นสำหรับกฎถูกตั้งค่าไว้เป็น **ถามทุกครั้ง** หน้าต่างข้อความจะแสดงทุกครั้งที่มีการเรียกใช้กฎ คุณสามารถเลือก **ปฏิเสธ** หรือ **อนุญาต** การดำเนินการ หากคุณไม่เลือกการทำงานภายในเวลาที่กำหนด ระบบจะเลือกการทำงานใหม่ตามกฎ

จดจำจนกว่าแอพพลิเคชันจะออก จะทำให้ใช้การดำเนินการ (**อนุญาต/ปฏิเสธ**) จนกว่าจะมีการเปลี่ยนแปลงกฎหรือโหมดการกรอง การอัพเดทโมดูล HIPS หรือการเริ่มต้นระบบใหม่ หลังจากดำเนินการหนึ่งจากสามรายการเหล่านี้ กฎชั่วคราวจะถูกลบ

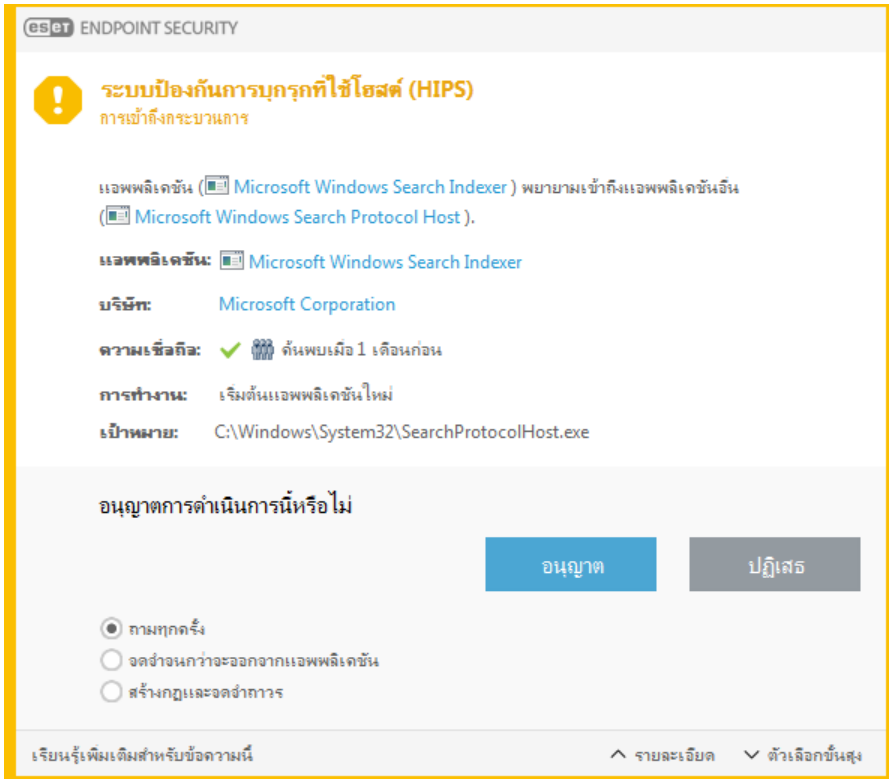
ตัวเลือก **สร้างกฎและจดจำถาวร** จะสร้างกฎ HIPS ใหม่ ซึ่งจะสามารถแก้ไขได้ในภายหลังในส่วน การจัดการกฎ HIPS (จำเป็นต้องมีสิทธิ์ของผู้ดูแลระบบ)

คลิก **รายละเอียด** ที่ด้านล่างสุดเพื่อดูสิ่งที่แอพพลิเคชันเรียกใช้การทำงาน ความเชื่อถือของไฟล์คืออะไร หรือการทำงานใดที่คุณถูกขอให้อนุญาตหรือปฏิเสธ

การตั้งค่าสำหรับพารามิเตอร์กฎอย่างละเอียดเพิ่มเติมสามารถเข้าถึงได้โดยการคลิก **ตัวเลือกขั้นสูง** มีตัวเลือกด้านล่างหากคุณเลือก **สร้างกฎและจดจำถาวร**:

- **สร้างกฎที่ใช้ได้เฉพาะสำหรับแอพพลิเคชันนี้** – หากคุณเลิกเลือกกล่องกาเครื่องหมายกล่องนี้ กฎจะถูกสร้างมาเพื่อแอพพลิเคชันที่มา
- **เฉพาะสำหรับการดำเนินการเท่านั้น** – เลือกไฟล์กฎ/แอพพลิเคชัน/การดำเนินการแบบรีจิสตรี ดูคำอธิบายสำหรับการดำเนินการ HIPS ทั้งหมด
- **เฉพาะสำหรับเป้าหมายเท่านั้น** – เลือกไฟล์กฎ/แอพพลิเคชัน/เป้าหมายแบบรีจิสตรี

หากต้องการหยุดการแจ้งเตือนที่แสดง เปลี่ยนโหมดการกรองเป็น **โหมดอัตโนมัติ** ใน การตั้งค่าขั้นสูง > **กลไกการตรวจหา** > **HIPS** > **พื้นฐาน**



ตรวจพบพฤติกรรมที่สงสัยว่าเป็นการทำงานของแรนซัมแวร์

หน้าต่างโต้ตอบนี้จะปรากฏขึ้นเมื่อตรวจพบพฤติกรรมที่สงสัยว่าเป็นการทำงานของแรนซัมแวร์ คุณสามารถเลือกเพื่อ **ปฏิเสธ** หรือ **อนุญาต** การดำเนินการ

คลิก**รายละเอียด**เพื่อดูพารามิเตอร์การตรวจพบที่เจาะจง หน้าต่างข้อความช่วยให้คุณ **ส่งเพื่อวิเคราะห์** หรือ **แยกออกจากการตรวจหา**

ESET LiveGrid® ต้องเปิดใช้งานเอาไว้เพื่อให้สามารถใช้งานการป้องกันแรนซัมแวร์ได้อย่างถูกต้อง

การจัดการกฎ HIPS

นี่คือรายการของผู้ใช้ที่ได้รับการระบุและกฎที่เพิ่มโดยอัตโนมัติในระบบ HIPS รายละเอียดเพิ่มเติมเกี่ยวกับการสร้างกฎและการทำงานของ HIPS สามารถพบได้ในบท การตั้งค่ากฎ HIPS ดูหลักการทั่วไปของ HIPS

คอลัมน์

กฎ – ชื่อกฎที่ผู้ใช้กำหนดหรือเลือกโดยอัตโนมัติ

เปิดใช้งาน – ปิดใช้งานตัวเลือกนี้ หากคุณต้องการคงกฎไว้ในรายการ แต่ไม่ต้องการใช้กฎ

การทำงาน – กฎที่ระบุการทำงาน – **อนุญาต**, **ปิดกั้น** หรือ **ถาม** – ที่ควรทำงานเมื่อตรงกับเงื่อนไขต่างๆ

ที่มา – ระบบจะใช้กฎนี้ต่อเมื่อแอพพลิเคชันเรียกเหตุการณ์

เป้าหมาย – จะมีการใช้กฎก็ต่อเมื่อการดำเนินการเกี่ยวข้องกับไฟล์ แอพพลิเคชัน หรือรายการรีจิสตรีบางรายการ

ความละเอียดของการบันทึก – ถ้าคุณเปิดใช้งานตัวเลือกนี้ ข้อมูลเกี่ยวกับกฎนี้จะถูกเขียนไปที่ บันทึก HIPS

แจ้ง – การแจ้งเตือนจะปรากฏที่มุมล่างขวาหากมีการเรียกใช้เหตุการณ์

องค์ประกอบการควบคุม

เพิ่ม – สร้างกฎใหม่

แก้ไข – ช่วยให้คุณสามารถแก้ไขรายการที่เลือกได้

ลบออก – ลบรายการที่เลือกออก

จัดอันดับความสำคัญของกฎ HIPS

ไม่มีตัวเลือกเพื่อปรับระดับความสำคัญของกฎ HIPS โดยใช้ปุ่มบนสุด/ล่าสุด (ต่างจาก กฎของไฟร์วอลล์ ที่จะเรียกใช้กฎตามความสำคัญจากมากไปน้อย)

- กฎทั้งหมดที่คุณสร้างจะมีความสำคัญเหมือนกัน
- ยิ่งมีกฎเฉพาะมากขึ้น ยิ่งมีความสำคัญมากขึ้น (เช่น กฎสำหรับแอพพลิเคชันที่เจาะจงมีความสำคัญมากกว่ากฎสำหรับแอพพลิเคชันทั้งหมด)
- ระบบภายในของ HIPS จะประกอบด้วยกฎที่มีความสำคัญมากกว่าที่ไม่สามารถเข้าถึงคุณได้ (เช่น คุณไม่สามารถเขียนทับระบบป้องกันตัวเองที่ระบุถึงกฎต่างๆ ได้)
- กฎที่คุณสร้างอาจทำให้ระบบปฏิบัติการของคุณค้าง และจะไม่ปรับใช้ (จะมีความสำคัญต่ำที่สุด)

การตั้งค่ากฎ HIPS

ดู การจัดการกฎ HIPS ก่อน

ชื่อกฎ – ชื่อกฎที่ผู้ใช้กำหนดหรือเลือกโดยอัตโนมัติ

การทำงาน – ระบุการทำงาน – **อนุญาต ปิดกั้น** หรือ **ถาม** – ที่ควรดำเนินการถ้าเป็นไปตามเงื่อนไข

การดำเนินการที่ได้ผล – คุณต้องเลือกประเภทของการดำเนินการที่กฎจะนำมาปรับใช้ ระบบจะใช้กฎนี้เฉพาะสำหรับการดำเนินการประเภทนี้เท่านั้นและสำหรับเป้าหมายที่เลือก

เปิดใช้งาน – ปิดใช้งานปุ่มสลับนี้หากคุณต้องการคงกฎไว้ในรายการแต่ไม่ปรับใช้

ความละเอียดของการบันทึก – ถ้าคุณเปิดใช้งานตัวเลือกนี้ ข้อมูลเกี่ยวกับกฎนี้จะถูกเขียนไปที่ บันทึก HIPS

แจ้งผู้ใช้ – การแจ้งเตือนจะปรากฏที่มุมล่างขวาหากมีการเรียกใช้เหตุการณ์

กฎประกอบด้วยส่วนต่างๆ ซึ่งจะอธิบายเงื่อนไขที่เรียกใช้งานกฎนี้:

แอพพลิเคชันที่มา– ระบบจะใช้กฎนี้ก็ต่อเมื่อแอพพลิเคชันเรียกใช้เหตุการณ์ เลือก **แอพพลิเคชันที่เจาะจง** จากเมนูแบบเลื่อนลงและคลิก **เพิ่ม** เพื่อเพิ่มไฟล์ หรือคุณสามารถเลือก **ทุกแอพพลิเคชัน** จากเมนูแบบเลื่อนลงเพื่อเพิ่มแอพพลิเคชันทั้งหมด

ไฟล์เป้าหมาย – ระบบจะใช้กฎนี้ก็ต่อเมื่อการดำเนินการเกี่ยวข้องกับเป้าหมายนี้ เลือก **ไฟล์ที่เจาะจง** จากเมนูแบบเลื่อนลงและคลิก **เพิ่ม** เพื่อเพิ่มไฟล์หรือโฟลเดอร์ใหม่ หรือคุณสามารถเลือก **ไฟล์ทั้งหมด** จากเมนูแบบเลื่อนลงเพื่อเพิ่มไฟล์ทั้งหมด

แอพพลิเคชัน – ระบบจะใช้กฎนี้ก็ต่อเมื่อการดำเนินการเกี่ยวข้องกับเป้าหมายนี้ เลือก **แอพพลิเคชันที่เจาะจง** จากเมนูแบบเลื่อนลงและคลิก **เพิ่ม** เพื่อเพิ่มไฟล์หรือโฟลเดอร์ใหม่ หรือคุณสามารถเลือก **ทุกแอพพลิเคชัน** จากเมนูแบบเลื่อนลงเพื่อเพิ่มแอพพลิเคชันทั้งหมด

รายการรีจิสตรี – ระบบจะใช้กฎนี้ต่อเมื่อการดำเนินการเกี่ยวข้องกับเป้าหมายนี้ เลือก **รายการที่เจาะจง** จากเมนูแบบเลื่อนลงและคลิก **เพิ่ม** เพื่อเพิ่มไฟล์หรือโฟลเดอร์ใหม่ หรือคุณสามารถเลือก **รายการทั้งหมด** จากเมนูแบบเลื่อนลงเพื่อเพิ่มแอพพลิเคชันทั้งหมด

> การดำเนินการของกฎบางอย่างที่กำหนดไว้ล่วงหน้าโดย HIPS จะไม่สามารถปิดกั้นหรืออนุญาตได้ตามค่าเริ่มต้น นอกจากนี้ HIPS จะไม่ตรวจสอบการดำเนินการทั้งหมดของระบบ HIPS ตรวจสอบการดำเนินการที่อาจพิจารณาว่าไม่ปลอดภัย

เมื่อระบุพาธ C:\example จะมีผลต่อการทำงานกับโฟลเดอร์เองและ C:\example*.* จะมีผลกับไฟล์ในโฟลเดอร์

การดำเนินการของแอพพลิเคชัน

- **แก้ไขแอพพลิเคชันอื่น** – การใส่เครื่องมือแก้ไขปัญหาในการดำเนินการ ในขณะที่มีการแก้ไขปัญหาของแอพพลิเคชัน ระบบจะตรวจสอบและแก้ไขรายละเอียดต่างๆ ของการทำงาน และจะมีการเข้าถึงข้อมูลการทำงาน
- **ดักฟังเหตุการณ์จากแอพพลิเคชันอื่น** – แอพพลิเคชันที่มาจะพยายามตรวจจับเหตุการณ์ที่มีการกำหนดเป้าหมายไปยังแอพพลิเคชันเฉพาะ (ตัวอย่างเช่น เครื่องมือบันทึกการกดแป้นพิมพ์ที่พยายามตรวจจับเหตุการณ์ของเบราว์เซอร์)
- **สิ้นสุด/พักการทำงานแอพพลิเคชันอื่น** – การพัก การทำงานต่อ หรือการสิ้นสุดกระบวนการ (สามารถเข้าถึงได้โดยตรงจากช่อง Process Explorer หรือ Processes)
- **เริ่มต้นแอพพลิเคชันใหม่** – การเริ่มต้นแอพพลิเคชันหรือกระบวนการใหม่
- **แก้ไขสถานะของแอพพลิเคชันอื่น** – แอพพลิเคชันที่มาจะพยายามเขียนข้อมูลไปยังหน่วยความจำของแอพพลิเคชันเป้าหมายหรือเรียกใช้รหัสในนามของตนเอง ฟังก์ชันการทำงานนี้อาจเป็นประโยชน์เพื่อป้องกันแอพพลิเคชันสำคัญ ด้วยการกำหนดค่าเป็นแอพพลิเคชันเป้าหมายในกฎที่ปิดกั้นการใช้การดำเนินการนี้

การดำเนินการของรีจิสตรี

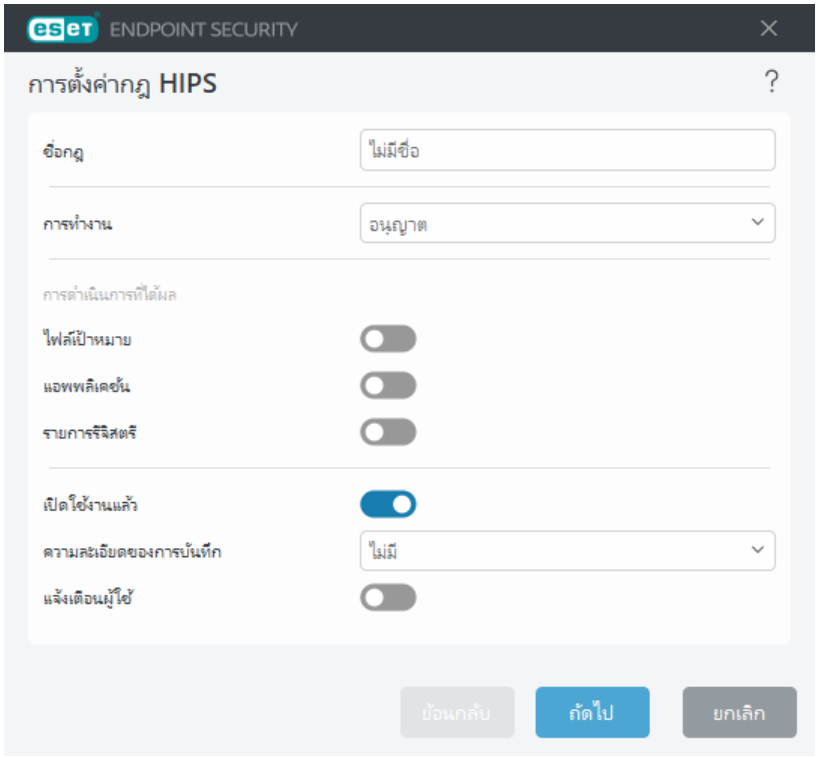
- **แก้ไขการตั้งค่าการเริ่มต้น** – การเปลี่ยนแปลงในการตั้งค่า ซึ่งกำหนดแอพพลิเคชันที่จะถูกเรียกใช้เมื่อเริ่มต้น Windows ซึ่งจะสามารถพบได้ เช่น จากการค้นหารหัส Run ใน Windows Registry
- **ลบจากรีจิสตรี** – การลบรหัสรีจิสตรีหรือค่าของรหัสรีจิสตรี
- **เปลี่ยนชื่อรหัสรีจิสตรี** – การเปลี่ยนชื่อรหัสรีจิสตรี
- **แก้ไขรีจิสตรี** – การสร้างค่าใหม่ของรหัสรีจิสตรี การเปลี่ยนค่าที่มีอยู่ การย้ายข้อมูลในโครงสร้างฐานข้อมูล หรือการตั้งค่าสิทธิ์ของผู้ใช้หรือกลุ่มสำหรับรหัสรีจิสตรี

การใช้สัญลักษณ์แทนในกฎ
ใช้เครื่องหมายดอกจันแทนในกฎสามารถใช้เพื่อแทนรหัสเฉพาะ เช่น “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start” ไม่รองรับวิธีอื่นๆ ในการใช้สัญลักษณ์แทน
การสร้างกฎที่มุ่งเป้าไปยังรหัส HKEY_CURRENT_USER
รหัสนี้เป็นเพียงการเชื่อมโยงไปยังรหัสย่อยที่เหมาะสมของ HKEY_USERS สำหรับผู้ใช้ที่ถูกระบุโดย SID (ตัวระบุที่ปลอดภัย) หากต้องสร้างกฎสำหรับผู้ใช้ปัจจุบันเท่านั้น ให้ใช้พาธที่มุ่งไปยัง HKEY_USERS\%SID% แทนการใช้พาธ HKEY_CURRENT_USER เนื่องจาก SID ทำให้คุณสามารถใช้เครื่องหมายดอกจันเพื่อสร้างกฎที่นำมาใช้กับผู้ใช้ทั้งหมดได้

หากคุณสร้างกฎที่กว้างมาก คำเตือนเกี่ยวกับกฎประเภทนี้จะปรากฏขึ้น

ในตัวอย่างต่อไปนี้ เราจะสาธิตวิธีจำกัดการทำงานที่ไม่พึงประสงค์ของแอพพลิเคชันที่ระบุ:

1. ตั้งชื่อกฎและเลือก**ปิดกั้น** (หรือ **ถาม** หากคุณต้องการหรือเลือกภายหลัง) จากเมนู**การทำงาน** แบบเลื่อนลง
2. เปิดใช้งานสวิตช์ **แจ้งเตือนผู้ใช้** เพื่อแสดงการแจ้งเตือนผู้ใช้เมื่อมีการนำกฎไปใช้
3. เลือกการดำเนินการอย่างน้อยหนึ่งอย่าง ในส่วน**การดำเนินการที่ได้ผล** ว่าจะใช้กฎใด
4. คลิก**ถัดไป**
5. ในหน้าต่าง **แอพพลิเคชันที่มา** เลือก **แอพพลิเคชันที่เจาะจง** จากเมนูแบบเลื่อนลงเพื่อใช้กฎใหม่กับแอพพลิเคชันทั้งหมดที่พยายามจะทำงานกับแอพพลิเคชันที่เลือกไว้บนแอพพลิเคชันที่คุณระบุ
6. คลิก**เพิ่ม** และ **...** เพื่อเลือกพาธไปยังแอพพลิเคชันที่เจาะจง แล้วกด**ตกลง** เพิ่มแอพพลิเคชันหากคุณต้องการ ตัวอย่างเช่น: *C:\Program Files (x86)\Untrusted application\application.exe*
7. เลือก**เขียนข้อมูลในไฟล์** การทำงาน
8. เลือก**ไฟล์ทั้งหมด** จากเมนูแบบเลื่อนลง วิธีนี้จะปิดกั้นความพยายามใดๆ เพื่อเขียนไฟล์โดยแอพพลิเคชันที่เลือกไว้จากขั้นตอนก่อนหน้านี้
9. คลิก **เสร็จสิ้น** เพื่อบันทึกกฎใหม่ของคุณ



เพิ่มแอพพลิเคชัน/พาธของรีจิสตรีสำหรับ HIPS

เลือกพาธแอพพลิเคชันของไฟล์ด้วยการคลิกตัวเลือก ... เมื่อเลือกโฟลเดอร์ แอพพลิเคชันทั้งหมดที่อยู่ในตำแหน่งนี้จะถูกรวมไว้ด้วย

ตัวเลือก **เปิด Registry Editor** จะเริ่มต้นโปรแกรมแก้ไขรีจิสตรีของ Windows (regedit) ในขณะที่เพิ่มพาธของรีจิสตรีให้ป้อนตำแหน่งที่ถูกต้องไปยังฟิลด์ **ค่า**

ตัวอย่างพาธของไฟล์หรือรีจิสตรี:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

อัพเดท

ตัวเลือกการตั้งค่าการอัพเดทจะพร้อมใช้งานใน การตั้งค่าขั้นสูง > **การอัปเดต** ส่วนนี้จะระบุข้อมูลที่มาของการอัพเดทเหมือนกับการใช้เซิร์ฟเวอร์อัพเดทและข้อมูลการตรวจสอบสิทธิ์สำหรับเซิร์ฟเวอร์เหล่านี้

คุณต้องป้อนพารามิเตอร์ที่อัพเดททั้งหมดให้ถูกต้อง เพื่อให้ระบบดาวน์โหลดการอัพเดทอย่างถูกต้อง ถ้าคุณใช้ไฟร์วอลล์ โปรดตรวจสอบให้แน่ใจว่าโปรแกรม ESET ของคุณได้รับอนุญาตให้สื่อสารกับอินเทอร์เน็ต (ตัวอย่างเช่น การเชื่อมต่อ HTTPS)

อัพเดท

โปรไฟล์การอัพเดทที่กำลังใช้งานอยู่แสดงอยู่ในเมนู **เลือกโปรไฟล์การอัพเดทค่าเริ่มต้น** แบบเลื่อนลง

หากต้องการสร้างโปรไฟล์ใหม่ ให้ดูส่วน โปรไฟล์การอัพเดท

การสลับโปรไฟล์อัตโนมัติ – ช่วยให้คุณสามารถตั้งค่าโปรไฟล์การอัพเดทสำหรับ โปรไฟล์การเชื่อมต่อเครือข่าย ที่เฉพาะเจาะจงได้

ตั้งค่าการแจ้งเตือนการอัพเดท – คลิก แก้ไข เพื่อเลือกว่าจะแสดงการแจ้งเตือนแอพพลิเคชันแบบใด คุณสามารถเลือกได้ว่าการแจ้งเตือนจะแสดงบนเดสก์ท็อปและ/หรือส่งโดยใช้อีเมล

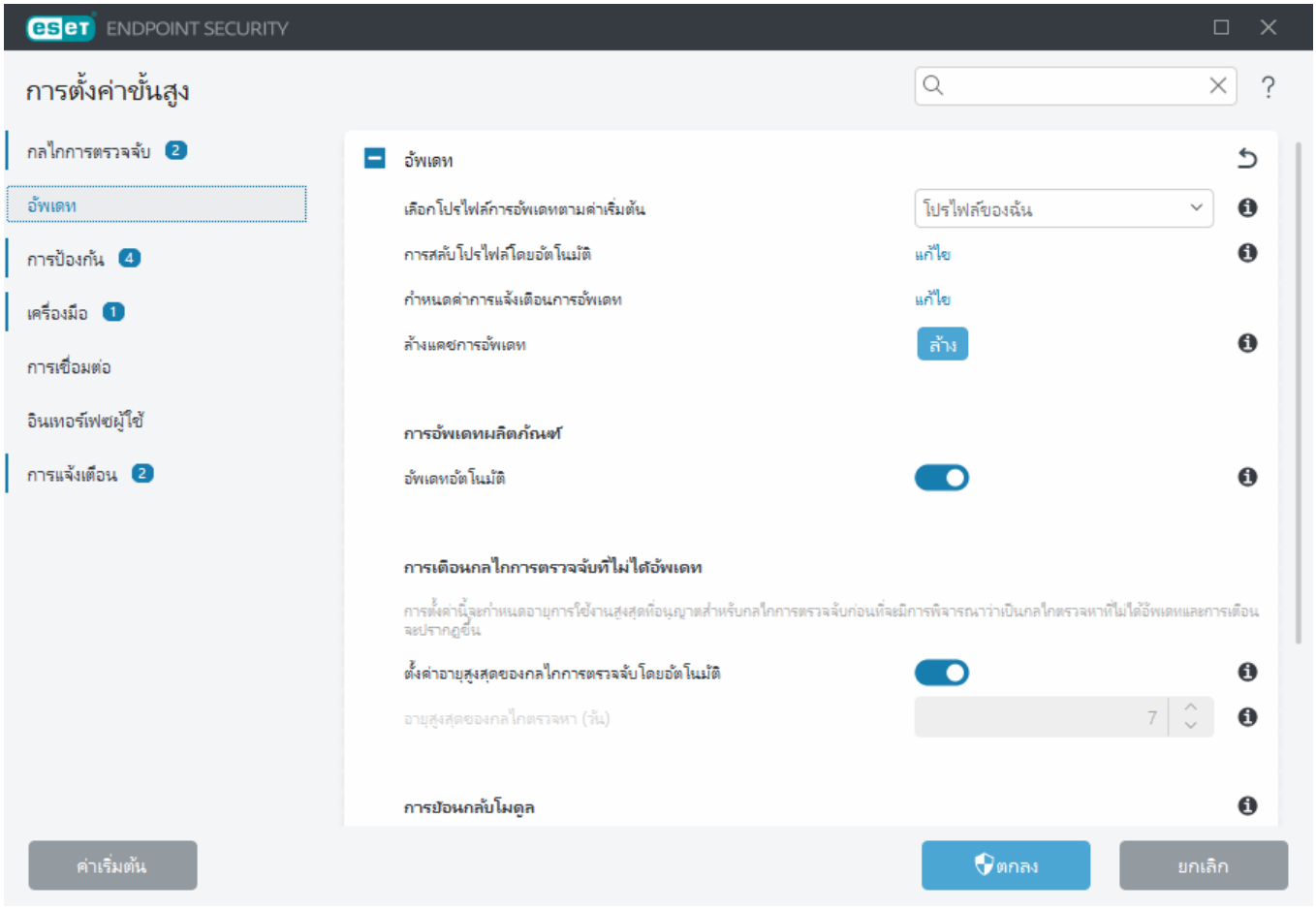
หากคุณกำลังประสบความยากลำบากขณะพยายามดาวน์โหลดการอัพเดทโมดูล ให้คลิก **ล้าง** ถัดจาก **ล้างการอัพเดทแคช** เพื่อล้างไฟล์/แคชชั่วคราว

การเตือนกลไกการตรวจจับที่ไม่ได้อัพเดท

ตั้งค่าอายุสูงสุดของกลไกการตรวจจับโดยอัตโนมัติ – อนุญาตให้ตั้งค่าเวลาสูงสุด (เป็นวัน) หลังจากนั้นกลไกการตรวจหาจะถูกรายงานว่าไม่อัพเดท ค่าเริ่มต้นของ **อายุของกลไกลการตรวจหาสูงสุด (เป็นวัน)** คือ 7

การย้อนกลับโมดูล

หากคุณสงสัยว่าการอัพเดทใหม่ของกลไกตรวจหาและ/หรือโมดูลโปรแกรมอาจไม่เสถียรหรือเสียหาย คุณสามารถ ย้อนกลับไปเป็นเวอร์ชันก่อนหน้า ได้ แล้วปิดการใช้งานการอัพเดทสำหรับช่วงเวลาที่ตั้งค่าไว้



โปรไฟล์

โปรไฟล์การอัพเดทสามารถสร้างขึ้นเพื่อการกำหนดค่าและงานการอัพเดทต่างๆ การสร้างโปรไฟล์การอัพเดทจะเป็นประโยชน์อย่างมากสำหรับผู้ใช้ที่ต้องเดินทางบ่อย ที่ต้องการโปรไฟล์สำรองสำหรับคุณสมบัติการเชื่อมต่ออินเทอร์เน็ตที่มีการเปลี่ยนแปลงเป็นประจำ

เมนู **เลือกโปรไฟล์ที่จะแก้ไข** แบบเลื่อนลงจะแสดงโปรไฟล์ที่เลือกในปัจจุบัน แล้วตั้งค่าเป็น **โปรไฟล์ของฉัน** ตามค่าเริ่มต้น

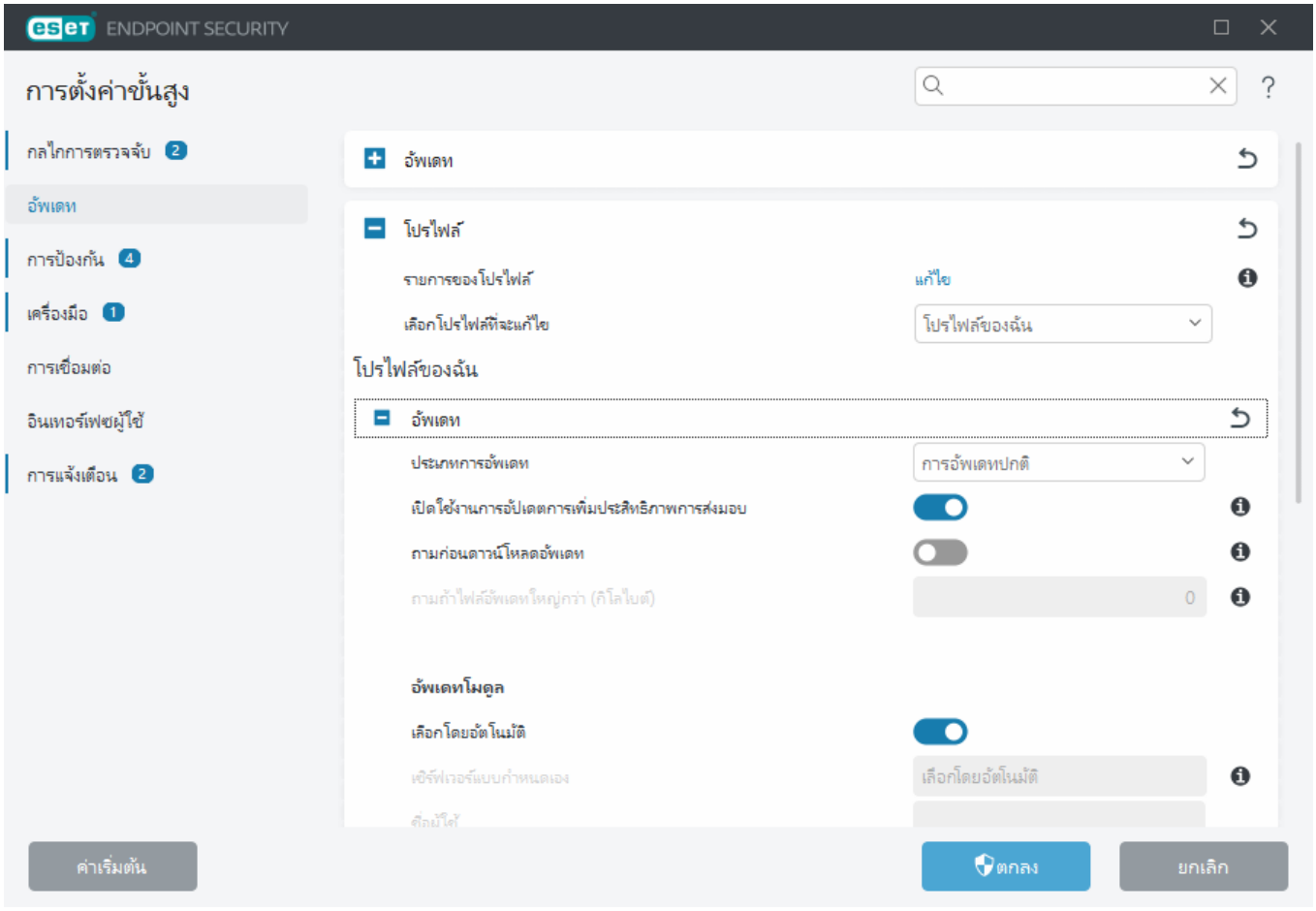
ในการสร้างโปรไฟล์ใหม่ ให้คลิก **แก้ไข** ถัดจาก **รายการของโปรไฟล์** ป้อน **ของคุณเอง** แล้วคลิก **เพิ่ม**

การอัพเดท

ตามค่าเริ่มต้น **ประเภทการอัพเดท** จะถูกตั้งเป็น **การอัพเดทปกติ** เพื่อทำให้แน่ใจว่าไฟล์อัพเดทจะดาวน์โหลดจากเซิร์ฟเวอร์ ESET โดยอัตโนมัติด้วยการรับส่งของเครือข่ายที่น้อยที่สุด การอัพเดทก่อนออก (ตัวเลือก **การอัพเดทก่อนออก**) เป็นการอัพเดทที่ผ่านการทดสอบภายในอย่างละเอียดและจะพร้อมใช้งานทั่วไปในเร็ว ๆ นี้ คุณสามารถใช้ประโยชน์จากการเปิดใช้งานการอัพเดทก่อนออกได้ ด้วยการเข้าถึงวิธีการตรวจหาและการแก้ไขล่าสุด อย่างไรก็ตาม การอัพเดทก่อนออกอาจไม่เสถียรตลอดเวลา และไม่ควรนำไปใช้บนเซิร์ฟเวอร์และเวิร์กสเตชันที่ใช้งานจริง ซึ่งต้องการความพร้อมในการใช้งานและเสถียรภาพสูงสุด การอัพเดทล่าช้าให้สามารถอัพเดทจากเซิร์ฟเวอร์การอัพเดทพิเศษซึ่งให้ฐานข้อมูลไวรัสเวอร์ชันใหม่โดยมีความล่าช้าอย่างน้อย X ชั่วโมง (ได้แก่ ฐานข้อมูลที่ทดสอบในสภาพแวดล้อมจริง และถือว่ามีความเสถียร)

เปิดใช้งานการอัปเดตการเพิ่มประสิทธิภาพการส่งมอบ – เมื่อเปิดใช้งาน ไฟล์อัพเดทสามารถดาวน์โหลดได้จาก CDN (เครือข่ายส่งมอบเนื้อหา) การปิดใช้งานการตั้งค่านี้อาจทำให้การดาวน์โหลดหยุดชะงักและช้าลงเมื่อเซิร์ฟเวอร์การอัพเดทของ ESET โดยเฉพาะมีการใช้งานมากเกินไป การปิดใช้งานจะมีประโยชน์เมื่อไฟร์วอลล์ถูกจำกัดให้เหลือเพียงเข้าถึง ที่อยู่ IP เซิร์ฟเวอร์การอัพเดทของ ESET เท่านั้น หรือเมื่อการเชื่อมต่อไปยังบริการ CDN ไม่ทำงาน

ถามก่อนที่จะดาวน์โหลดอัพเดท – โปรแกรมจะแสดงการแจ้งเตือนที่คุณสามารถเลือกที่จะยืนยันหรือปฏิเสธการดาวน์โหลดไฟล์อัพเดท หากขนาดของไฟล์ที่อัพเดทใหญ่กว่าค่าที่ระบุไว้ในช่อง ถามก่อนที่จะอัพเดทไฟล์ที่ใหญ่กว่า (kB) โปรแกรมจะแสดงข้อความยืนยัน หากขนาดไฟล์อัพเดทถูกตั้งค่าเป็น 0 กิโลไบต์ โปรแกรมจะแสดงข้อความยืนยันเสมอ



การอัพเดทโมดูล

ตัวเลือก **เลือกโดยอัตโนมัติ** เปิดใช้งานตามค่าเริ่มต้น ตัวเลือก **เซิร์ฟเวอร์ที่กำหนดเอง** เป็นตำแหน่งที่ใช้เก็บการอัพเดท หากคุณใช้เซิร์ฟเวอร์การอัพเดท ESET เราขอแนะนำให้คุณคงตัวเลือกที่เลือกเริ่มต้นไว้

เปิดใช้งานการอัพเดทฐานข้อมูลการตรวจหาให้บ่อยขึ้น – ฐานข้อมูลการตรวจหาจะถูกอัพเดทในช่วงเวลาที่สั้นลง การปิดใช้งานการตั้งค่านี้อาจส่งผลกระทบทางลบต่ออัตราการตรวจจับ

อนุญาตให้อัพเดทโมดูลจากสื่อแบบถอดได้ – ให้คุณอัพเดทจากสื่อแบบถอดออกได้ถ้ามีมิเรอร์ที่สร้างไว้ เมื่อเลือก อัตโนมัติ การอัพเดทจะทำงานอยู่เบื้องหลัง ถ้าคุณต้องการแสดงหน้าต่างข้อความการอัพเดท ให้เลือก ถามเสมอ

เมื่อใช้เซิร์ฟเวอร์ HTTP ในระบบ หรือเรียกอีกอย่างว่ามิเรอร์ คุณควรตั้งค่าเซิร์ฟเวอร์การอัพเดทดังนี้:
http://ชื่อคอมพิวเตอร์หรือที่อยู่_IP:2221

เมื่อใช้เซิร์ฟเวอร์ HTTP ด้วย SSL คุณควรตั้งค่าเซิร์ฟเวอร์การอัพเดทดังนี้:
https://ชื่อคอมพิวเตอร์หรือที่อยู่_IP:2221

เมื่อใช้โฟลเดอร์ที่ใช้ร่วมกันในระบบ – คุณควรตั้งค่าเซิร์ฟเวอร์การอัพเดทดังนี้:
\\ชื่อคอมพิวเตอร์หรือที่อยู่_*IP*\โฟลเดอร์ที่ใช้ร่วมกัน

หมายเลขพอร์ตเซิร์ฟเวอร์ของ HTTP จะระบุอยู่ในตัวอย่างด้านบนขึ้นอยู่กับว่าพอร์ตใดที่เซิร์ฟเวอร์ HTTP/HTTPS ของคุณรับข้อมูลอยู่

การอัพเดทผลิตภัณฑ์

ดู การอัพเดทผลิตภัณฑ์

ตัวเลือกการเชื่อมต่อ

โปรดดู ตัวเลือกการเชื่อมต่อ

มิเรอร์การอัพเดท

ดู มิเรอร์การอัพเดท

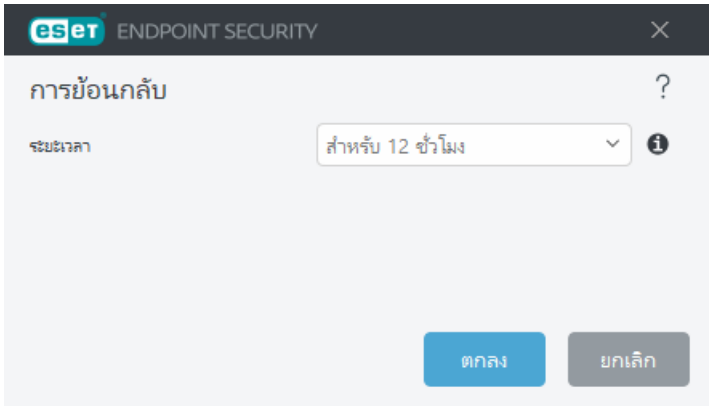
การอัพเดทย้อนหลัง

หากคุณสงสัยว่าการอัพเดทใหม่ของกลไกตรวจหาหรือโมดูลโปรแกรมอาจไม่เสถียรหรือเสียหาย คุณสามารถย้อนกลับเป็นเวอร์ชันก่อนหน้าและปิดใช้งานการอัพเดทชั่วคราว หรือมิฉะนั้น คุณสามารถเปิดใช้งานการอัพเดทที่ปิดใช้งานไว้ก่อนหน้านั้น ถ้าคุณได้เลื่อนการอัพเดทไว้อย่างไม่มีกำหนด

ESET Endpoint Security จะบันทึกสแนปชอตของกลไกการตรวจหาและโมดูลโปรแกรมเพื่อใช้กับคุณลักษณะ การย้อนกลับ หากต้องการสร้างสแนปชอตของฐานข้อมูลไวรัส ให้เปิดใช้งาน **สร้างสแนปชอตของโมดูล** ไว้ เมื่อ **สร้างสแนปชอตของโมดูล** เปิดใช้งาน สแนปชอตแรกจะถูกสร้างขึ้นในการอัพเดทครั้งแรก และสแนปชอตถัดไปจะถูกสร้างขึ้นหลังจากนั้น 48 ชั่วโมง ช่อง **จำนวนสแนปชอตที่เก็บในเครื่อง** จะระบุจำนวนของสแนปชอตกลไกการตรวจหาที่เก็บไว้

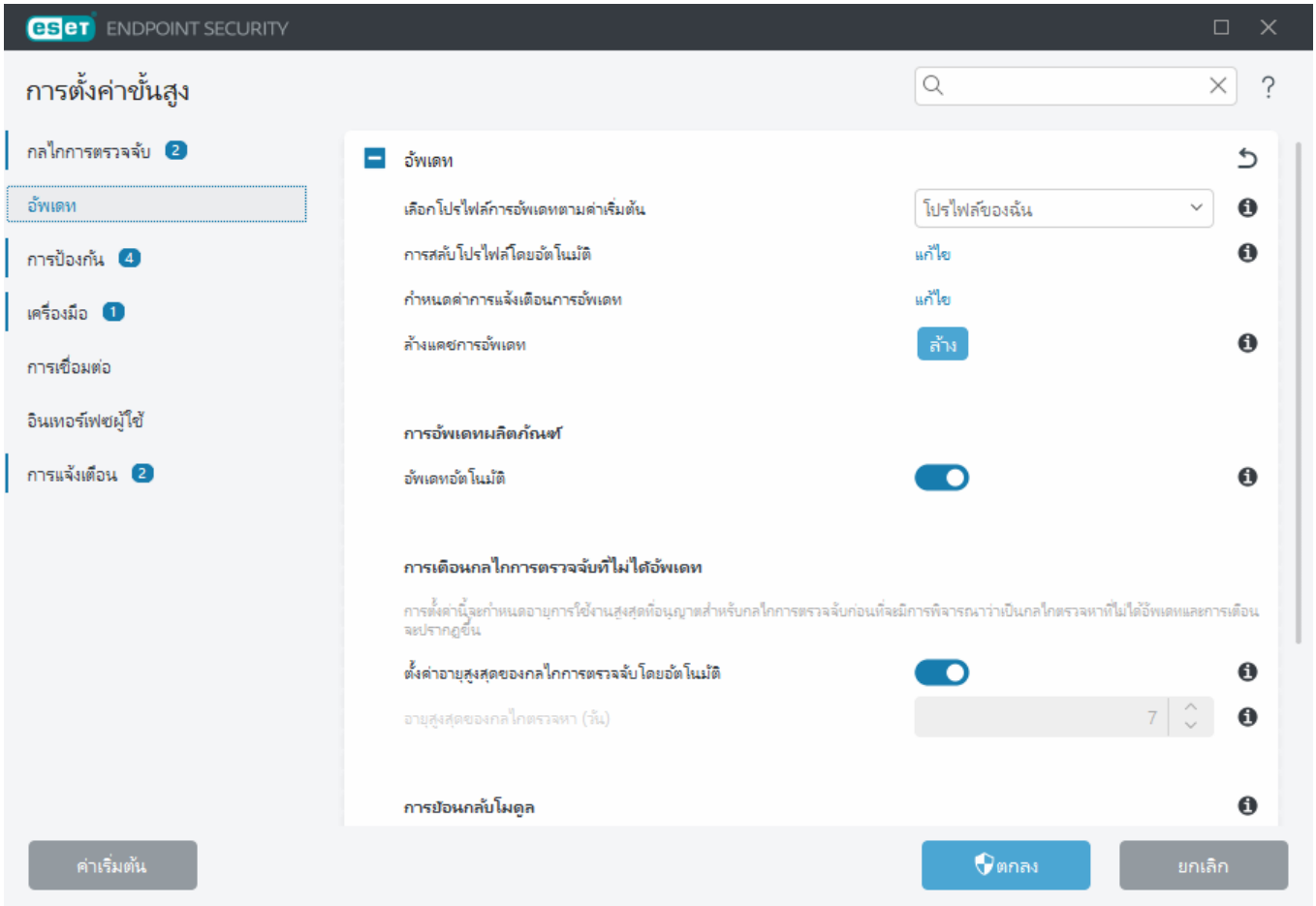
เมื่อถึงจำนวนสูงสุดของสแนปชอต (เช่น สามภาพ) สแนปชอตที่เก่าที่สุดจะถูกแทนที่ด้วยสแนปชอตใหม่ทุก 48 ชั่วโมง ESET Endpoint Security จะย้อนกลับกลไกการตรวจหาและรุ่นการปรับปรุงโมดูลโปรแกรมไปยังสแนปชอตที่เก่าที่สุด

เปิด **การตั้งค่าขั้นสูง** > **อัพเดท** > **อัพเดท** > **โมดูลการย้อนกลับ** > **การย้อนกลับ** เพื่อเลือกช่วงเวลาจากเมนูแบบเลื่อนลง ระยะเวลา



เลือก **จนกว่าจะยกเลิก** เพื่อเลื่อนการอัพเดทเป็นประจำออกไปโดยไม่มีกำหนดจนกว่าคุณจะเรียกการทำงานของการอัพเดทด้วยตนเอง เนื่องจากจะมีความเสี่ยงด้านความปลอดภัย เราจึงไม่แนะนำให้เลือกตัวเลือกนี้

หากทำการย้อนกลับ ปุ่ม **การย้อนกลับ** จะเปลี่ยนเป็น **อนุญาตการอัพเดท** โดยจะไม่สามารถอัพเดทได้ในช่วงเวลาที่เลือกจากเมนู **ระงับการอัพเดท** แบบเลื่อนลง เวอร์ชันของกลไกตรวจหาจะถูกดาวน์เกรดมาเป็นรุ่นเก่าที่สุดที่มีและเก็บไว้เป็นสแนปชอตในระบบไฟล์ของเครื่องคอมพิวเตอร์



สมมติว่า 22700 เป็นหมายเลขรุ่นของเครื่องมือตรวจหาล่าสุด และ 22698 และ 22696 ถูกเก็บไว้เป็นสแนปชอตของกลไกการตรวจหา โปรดทราบว่า 22697 จะไม่พร้อมใช้งาน ในตัวอย่างนี้ คอมพิวเตอร์ถูกปิดในระหว่างการอัพเดท 22697 และมีการอัพเดทล่าสุดพร้อมใช้งานก่อนที่ 22697 จะดาวน์โหลด หากฟิลด์ **จำนวนสแนปชอตที่เก็บในระบบ** เป็น 2 และคุณคลิก **การย้อนกลับ** กลไกการตรวจหา (รวมถึงโมดูลโปรแกรม) จะถูกเรียกคืนเป็นหมายเลขเวอร์ชัน 22696 โดยกระบวนการนี้อาจใช้เวลาสักครู่ ตรวจสอบเวอร์ชันของกลไกการตรวจหาว่าได้ดาวน์เกรดลงหรือไม่ในหน้าจอ อัพเดท

การอัพเดทผลิตภัณฑ์

ส่วน **การอัพเดทผลิตภัณฑ์** ประกอบด้วยตัวเลือกที่เกี่ยวข้องกับการอัพเดทผลิตภัณฑ์ โปรแกรมจะช่วยให้คุณสามารถกำหนดการทำงานได้ล่วงหน้า เมื่อมีการอัพเดทผลิตภัณฑ์ใหม่

การอัพเดทผลิตภัณฑ์จะนำมาซึ่งคุณลักษณะใหม่ หรือเปลี่ยนแปลงคุณลักษณะที่มีในอยู่เวอร์ชันก่อนหน้านี้ การอัพเกรดสามารถทำได้โดยอัตโนมัติโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ หรือคุณสามารถเลือกให้มีการแจ้งเตือนได้ หลังจากการติดตั้งการอัพเดทผลิตภัณฑ์แล้ว อาจจำเป็นต้องรีสตาร์ทคอมพิวเตอร์

การอัพเดทอัตโนมัติ – การหยุดการอัพเดทอัตโนมัติชั่วคราวสำหรับโปรไฟล์การอัพเดทบางโปรไฟล์จะปิดใช้งานการอัพเดทผลิตภัณฑ์อัตโนมัติในขณะที่เชื่อมต่อกับอินเทอร์เน็ตโดยใช้เครือข่ายอื่นหรือการเชื่อมต่อแบบคิดค่าบริการตามปริมาณข้อมูล เปิดใช้งานการตั้งค่านี้ไว้เพื่อให้เข้าถึงคุณลักษณะล่าสุดและการป้องกันสูงสุดที่เป็นไปได้อย่างต่อเนื่อง สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการอัพเดทอัตโนมัติ โปรดดู คำถามที่พบบ่อยเกี่ยวกับการอัพเดทอัตโนมัติ

โดยค่าเริ่มต้น การอัพเดทผลิตภัณฑ์จะถูกดาวน์โหลดจากเซิร์ฟเวอร์ Repository ของ ESET ในสภาพแวดล้อมขนาดใหญ่หรือสภาพแวดล้อมแบบออฟไลน์ การรับส่งข้อมูลจะได้รับการจัดสรรเพื่ออนุญาตการแคชภายในของไฟล์ผลิตภัณฑ์

กำหนดเซิร์ฟเวอร์แบบกำหนดเองสำหรับอัพเดทองค์ประกอบของโปรแกรม

1. กำหนดพาธไปยังการอัพเดทผลิตภัณฑ์ใน ช่อง **เซิร์ฟเวอร์แบบกำหนดเอง** ซึ่งสามารถเป็นลิงค์ HTTP(S), พาธเครือข่ายร่วม SMB, ไดรฟ์ดิสก์ภายใน หรือพาธสื่อที่ถอดเข้าออกได้ สำหรับไดรฟ์เครือข่าย ให้ใช้พาธ UNC แทนที่อักษรไดรฟ์ที่แมป
2. ปล่อย **ชื่อผู้ใช้** และ **รหัสผ่าน** ว่างไว้หากไม่จำเป็น
หากจำเป็น กำหนดข้อมูลการเข้าสู่ระบบที่เหมาะสมได้ที่นี่สำหรับการตรวจสอบสิทธิ์ของ HTTP บนเว็บเซิร์ฟเวอร์แบบกำหนดเอง
3. ยืนยันการเปลี่ยนแปลงและการทดสอบการมีอยู่ของการอัพเดทผลิตภัณฑ์โดยใช้การอัพเดท ESET Endpoint Security มาตรฐาน

การเลือกตัวเลือกที่เหมาะสมที่สุดจะขึ้นอยู่กับเวิร์กสเตชันที่จะนำการตั้งค่าไปใช้ โปรดทราบว่าเวิร์กสเตชันและเซิร์ฟเวอร์นั้นมีความแตกต่างกัน ตัวอย่างเช่น การเริ่มต้นเซิร์ฟเวอร์โดยอัตโนมัติหลังจากการอัพเดทผลิตภัณฑ์อาจทำให้เกิดความเสียหายร้ายแรงต่อบริษัทของคุณได้

ตัวเลือกการเชื่อมต่อ

หากต้องการเข้าถึงตัวเลือกการตั้งค่าพร็อกซีเซิร์ฟเวอร์สำหรับโปรไฟล์การอัพเดทที่เฉพาะเจาะจง ให้เปิด การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์** > **อัพเดท** > **ตัวเลือกการเชื่อมต่อ**

พร็อกซีเซิร์ฟเวอร์

คลิกเมนูแบบเลื่อนลง **โหมดพร็อกซี** แล้วเลือกหนึ่งในสามตัวเลือกต่อไปนี้:

- ไม่ใช้พร็อกซีเซิร์ฟเวอร์
- การเชื่อมต่อผ่านพร็อกซีเซิร์ฟเวอร์
- ใช้การตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วม

เลือก **ใช้การตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วม** เพื่อใช้ การกำหนดค่าพร็อกซีเซิร์ฟเวอร์ ที่มีระบุไว้แล้วในการตั้งค่าขั้นสูง > **การเชื่อมต่อ** > **พร็อกซีเซิร์ฟเวอร์**

เลือก **ไม่ใช้เซิร์ฟเวอร์พร็อกซี** เพื่อระบุว่าจะไม่ใช้พร็อกซีเซิร์ฟเวอร์ในการอัพเดท ESET Endpoint Security

ควรเลือกตัวเลือก **การเชื่อมต่อผ่านพร็อกซีเซิร์ฟเวอร์** ไว้ถ้า:

- พร็อกซีเซิร์ฟเวอร์อื่นนอกเหนือจากที่ระบุไว้ใน **เครื่องมือ** > **พร็อกซีเซิร์ฟเวอร์** ที่ใช้เพื่ออัพเดท ESET Endpoint Security ในการกำหนดค่านี้ ควรระบุข้อมูลสำหรับพร็อกซีใหม่ไว้ในที่อยู่ **พร็อกซีเซิร์ฟเวอร์**, **พอร์ต** การสื่อสาร (3128 ตามค่าเริ่มต้น) และ **ชื่อผู้ใช้** และ **รหัสผ่าน** สำหรับพร็อกซีเซิร์ฟเวอร์ หากต้องใช้
- การตั้งค่าพร็อกซีเซิร์ฟเวอร์ไม่ได้ถูกตั้งค่าให้ใช้ร่วมกัน แต่ ESET Endpoint Security จะเชื่อมต่อกับพร็อกซีเซิร์ฟเวอร์เพื่อการอัพเดท
- คอมพิวเตอร์ของคุณจะเชื่อมต่อกับอินเทอร์เน็ตผ่านพร็อกซีเซิร์ฟเวอร์ การตั้งค่าจะมาจาก เบราว์เซอร์ ระหว่างการติดตั้งโปรแกรม แต่ถ้าการตั้งค่านี้มีการเปลี่ยนแปลง (เช่น หากคุณเปลี่ยน ISP) โปรดตรวจสอบให้แน่ใจว่าการตั้งค่าพร็อกซี ที่อยู่ในหน้าต่างนี้ถูกต้อง มิฉะนั้นโปรแกรมจะไม่สามารถเชื่อมต่อกับเซิร์ฟเวอร์การอัพเดท

การตั้งค่าเริ่มต้นสำหรับพร็อกซีเซิร์ฟเวอร์คือ **ใช้การตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วม**

ใช้การเชื่อมต่อโดยตรงหากพร็อกซีไม่สามารถใช้งานได้ – พร็อกซีจะถูกข้ามระหว่างการอัพเดทถ้าไม่สามารถเข้าถึงได้

Windows Shares

เมื่ออัพเดทจากเซิร์ฟเวอร์ในระบบที่มีระบบปฏิบัติการเวอร์ชันที่ใช้ Windows NT จะต้องมีการตรวจสอบสิทธิ์สำหรับการเชื่อมต่อเครือข่ายแต่ละครั้งเป็นค่าเริ่มต้น

หากต้องการกำหนดค่าบัญชีดังกล่าว ให้เลือกจากเมนูแบบเลื่อนลง **เชื่อมต่อกับ LAN เป็น** ดังนี้:

- **บัญชีระบบ (ค่าเริ่มต้น)**
- **ผู้ใช้ปัจจุบัน**
- **ผู้ใช้ที่ระบุ**

เลือกตัวเลือก **บัญชีระบบ (ค่าเริ่มต้น)** เพื่อใช้บัญชีระบบสำหรับการตรวจสอบสิทธิ์ ตามปกติ กระบวนการตรวจสอบสิทธิ์จะไม่เกิดขึ้น ถ้าไม่มีการป้อนข้อมูลการตรวจสอบสิทธิ์ในส่วนการตั้งค่าการอัพเดทหลัก

เพื่อให้โปรแกรมตรวจสอบสิทธิ์โดยใช้บัญชีผู้ใช้ที่เข้าสู่ระบบในปัจจุบัน ให้เลือก **ผู้ใช้ปัจจุบัน** ข้อเสียของทางเลือกนี้ก็คือโปรแกรมจะไม่สามารถเชื่อมต่อไปยังเซิร์ฟเวอร์การอัพเดทได้ ถ้าไม่มีผู้ใช้เข้าสู่ระบบอยู่ในขณะนั้น

เลือก **ผู้ใช้ที่ระบุ** ถ้าคุณต้องการให้โปรแกรมใช้บัญชีผู้ใช้ที่ระบุสำหรับการตรวจสอบสิทธิ์ ใช้วิธีนี้เมื่อการเชื่อมต่อของบัญชีระบบเริ่มต้นล้มเหลว โปรดทราบว่าบัญชีผู้ใช้ที่ระบุต้องมีสิทธิ์เข้าถึงไดเรกทอรีของไฟล์อัพเดทในเซิร์ฟเวอร์ของระบบ มิฉะนั้น โปรแกรมจะไม่สามารถเริ่มต้นการเชื่อมต่อและดาวน์โหลดการอัพเดท

การตั้งค่า **ชื่อผู้ใช้** และ **รหัสผ่าน** จะเป็นแบบเลือกหรือไม่ก็ได้

⚠ เมื่อเลือก **ผู้ใช้ปัจจุบัน** หรือ **ผู้ใช้ที่ระบุ** อาจเกิดข้อผิดพลาดเมื่อเปลี่ยนข้อมูลประจำตัวของโปรแกรมเป็นผู้ใช้ที่ต้องการ เราแนะนำให้ใส่ข้อมูลการตรวจสอบสิทธิของ LAN ในส่วนการตั้งค่าการอัพเดทหลัก ในส่วนการตั้งค่าการอัพเดทหลัก ควรป้อนข้อมูลการตรวจสอบสิทธิดังนี้: ชื่อโดเมนผู้ใช้ (ถ้าเป็นเวิร์กกรุ๊ป ให้ป้อน ชื่อเวิร์กกรุ๊ป\ชื่อ) และรหัสผ่าน เมื่ออัพเดทจากเวอร์ชัน HTTP ของเซิร์ฟเวอร์ในระบบ จะไม่ต้องมีการตรวจสอบสิทธิ

เลือก **ยกเลิกการเชื่อมต่อ**จากเซิร์ฟเวอร์หลังจากการอัพเดท เพื่อบังคับยกเลิกการเชื่อมต่อ หาก การเชื่อมต่อกับเซิร์ฟเวอร์ยังใช้งานอยู่ แม้จะเป็นช่วงหลังจากดาวน์โหลดการอัพเดทแล้วก็ตาม

มิเรอร์การอัพเดท

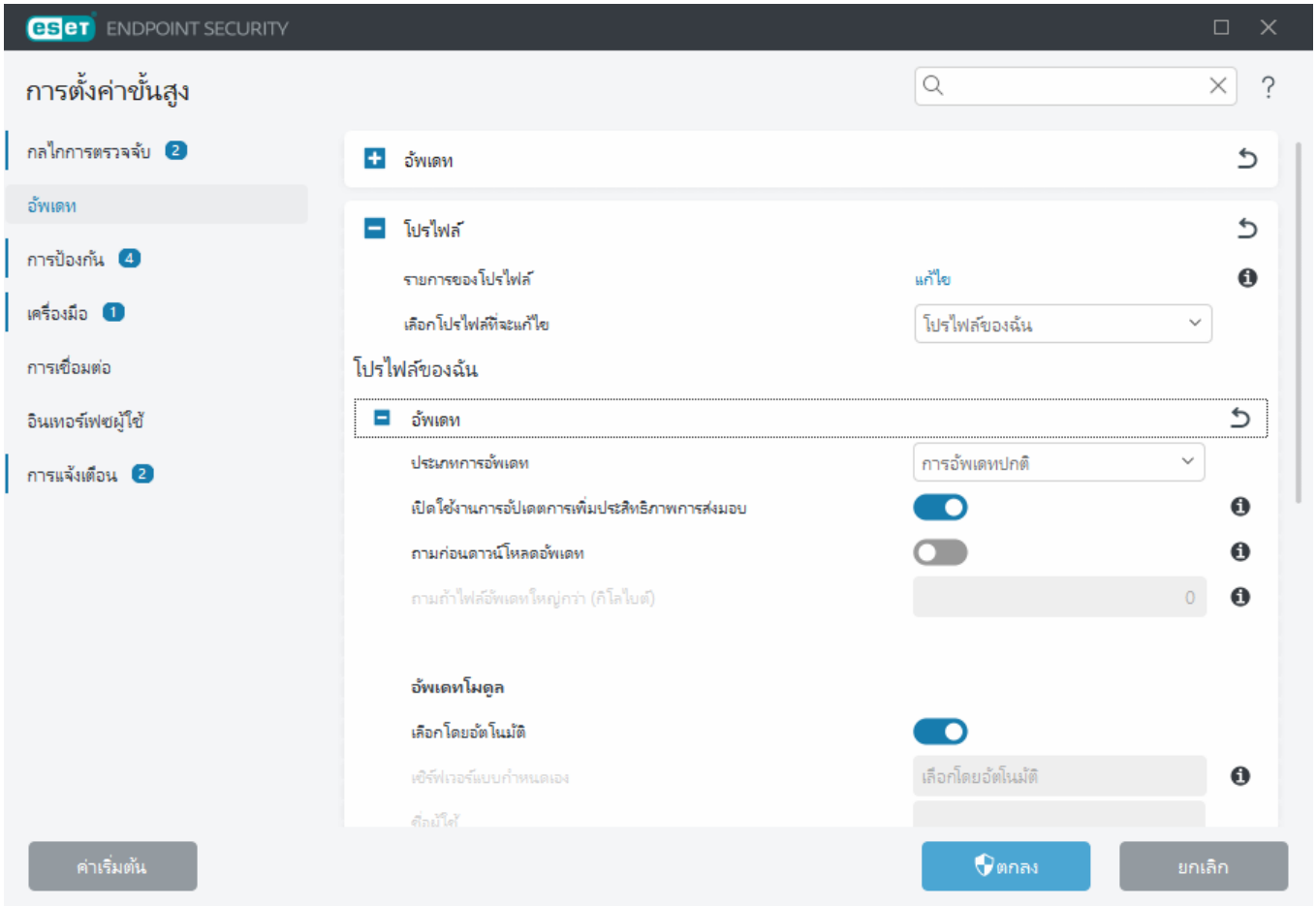
ESET Endpoint Security ช่วยให้ผู้ใช้สามารถสร้างสำเนาของไฟล์การอัพเดท ซึ่งสามารถใช้ในการอัพเดทเวิร์กสเตชันอื่นๆ ในเครือข่าย การใช้ "มิเรอร์" – สำเนาของไฟล์การอัพเดทในสภาพแวดล้อม LAN เป็นวิธีที่สะดวก เนื่องจากไม่จำเป็นต้องดาวน์โหลดไฟล์การอัพเดทจากเซิร์ฟเวอร์การอัพเดทของผู้ขายซ้ำๆ โดยแยกตามแต่ละเวิร์กสเตชัน การ

อัพเดทจะดาวน์โหลดไปยังเซิร์ฟเวอร์มิเรอร์ในระบบ จากนั้นแจกจ่ายไปยังเวิร์กสเตชันทั้งหมดเพื่อหลีกเลี่ยงความเสี่ยงในการเกิดปัญหาโอเวอร์โหลดสำหรับการรับส่งข้อมูลในเครือข่าย การอัพเดทเวิร์กสเตชันที่เป็นไคลเอ็นต์จากมิเรอร์จะช่วยเพิ่มประสิทธิภาพของการจัดสรรภาระงานของเครือข่าย และประหยัดแบนด์วิดธ์ของการเชื่อมต่ออินเทอร์เน็ต

มิเรอร์อัพเดทจะสร้างสำเนาไฟล์อัพเดทที่ใช้ในการอัพเดทเวิร์กสเตชันที่กำลังเรียกใช้ ESET Endpoint Security รุ่นเดียวกันสำหรับ Windows (ตัวอย่างเช่น ESET Endpoint Security สำหรับ Windows เวอร์ชัน 10.x จะสร้างไฟล์อัพเดทเฉพาะสำหรับเวอร์ชัน 10.x ESET Endpoint Antivirus สำหรับ Windows และ ESET Endpoint Security สำหรับ Windows)

เพื่อลดปริมาณการใช้งานอินเทอร์เน็ตบนเครือข่ายที่ใช้ ESET PROTECT ในการจัดการไคลเอนต์จำนวนมาก เราขอแนะนำให้คุณใช้ ESET Bridge แทนที่จะกำหนดค่าไคลเอ็นต์เป็นมิเรอร์ สามารถติดตั้ง ESET Bridge ได้ด้วย ESET PROTECT โดยใช้ตัวติดตั้งแบบออลอินวัน หรือเป็นส่วนประกอบแบบสแตนด์อโลน สำหรับข้อมูลเพิ่มเติมและความแตกต่างระหว่างพร็อกซี Apache HTTP เครื่องมือมิเรอร์และการเชื่อมต่อโดยตรง โปรดดู หน้าวิธีใช้ออนไลน์ของ ESET PROTECT

ตัวเลือกการตั้งค่าสำหรับเซิร์ฟเวอร์มิเรอร์จะอยู่ใน การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์** > **มิเรอร์อัพเดท**



หากต้องการสร้างมิเรอร์บนเวิร์กสเตชันไคลเอ็นต์ ให้เปิดใช้งาน **สร้างมิเรอร์อัพเดท** การเปิดใช้งานตัวเลือกนี้จะเป็นการเปิดใช้ตัวเลือกการกำหนดค่ามิเรอร์อื่นๆ เช่น วิธีที่จะเข้าถึงไฟล์การอัพเดท และพาธการอัพเดทไปยังไฟล์ที่มิเรอร์

เข้าถึงไฟล์อัพเดท

เปิดใช้งานเซิร์ฟเวอร์ HTTP – หากเปิดใช้งาน การอัพเดทไฟล์จะสามารถ เข้าถึงผ่าน HTTP และไม่จำเป็นต้องใช้ข้อมูลการเข้าสู่ระบบ

วิธีการเข้าถึงเซิร์ฟเวอร์มิเรอร์อย่างละเอียดจะอธิบายไว้ใน การอัพเดทจากมิเรอร์ ในการเข้าถึงมิเรอร์ มีวิธีการพื้นฐานสองวิธี โดยสามารถใช้โฟลเดอร์ที่มีไฟล์การอัพเดทในฐานะโฟลเดอร์เครือข่ายที่ใช้ร่วมกัน หรือไคลเอ็นต์สามารถเข้าถึงมิเรอร์ในระบบได้ในเซิร์ฟเวอร์ HTTP ได้

โฟลเดอร์ที่ใช้เฉพาะการเก็บไฟล์การอัพเดทสำหรับมิเรอร์นั้นมีการกำหนดใน **โฟลเดอร์ที่จะเก็บไฟล์ที่ใช้มิเรอร์** หากต้องการเลือกโฟลเดอร์อื่น ให้คลิก **ล้าง** เพื่อลบโฟลเดอร์ที่กำหนดไว้ล่วงหน้า *C:\ProgramData\ESET\ESET Endpoint Security\mirror* แล้วคลิก **แก้ไข** เพื่อเรียกดูโฟลเดอร์ในคอมพิวเตอร์ในระบบหรือโฟลเดอร์เครือข่ายที่ใช้ร่วมกัน ถ้าต้องมีการให้สิทธิ์สำหรับโฟลเดอร์ที่ระบุ จะต้องให้ข้อมูลการตรวจสอบสิทธิ์ในช่อง **ชื่อผู้ใช้** และ **รหัสผ่าน** ถ้าโฟลเดอร์ปลายทางที่เลือกไว้อยู่ที่ดิสก์ของเครือข่ายที่ใช้งานระบบปฏิบัติ Windows NT/2000/XP ชื่อผู้ใช้และรหัสผ่านที่ระบุต้องมีสิทธิ์เขียนสำหรับโฟลเดอร์ที่เลือกไว้ ควรพิมพ์ชื่อผู้ใช้ให้อยู่ในรูปแบบโดเมน/ผู้ใช้หรือเวิร์กกรุ๊ป/ผู้ใช้ โปรดระบุรหัสผ่านที่ตรงกันด้วย

เซิร์ฟเวอร์ HTTP และ SSL สำหรับมิเรอร์

ในส่วน **เซิร์ฟเวอร์ HTTP** ของแท็บ **มิเรอร์** คุณสามารถระบุ **พอร์ตเซิร์ฟเวอร์** ที่เซิร์ฟเวอร์ HTTP จะรับข้อมูลตลอดจนประเภทของ **การตรวจสอบสิทธิ์** ที่ใช้โดยเซิร์ฟเวอร์ HTTP พอร์ตเซิร์ฟเวอร์จะตั้งค่าเป็น **2221** ตามค่าเริ่มต้น

การตรวจสอบสิทธิ์ – ระบุถึงวิธีการตรวจสอบสิทธิ์ที่ใช้สำหรับเข้าถึงไฟล์การอัพเดท ตัวเลือกที่ใช้ได้มีดังนี้: **ไม่มีพื้นฐาน** และ **NTLM** เลือก **พื้นฐาน** เพื่อใช้การเข้ารหัส base64 กับการตรวจสอบสิทธิ์ด้วยชื่อผู้ใช้และรหัสผ่านแบบพื้นฐาน ตัวเลือก **NTLM** จะให้การเข้ารหัสด้วยวิธีการเข้ารหัสที่ปลอดภัย สำหรับการตรวจสอบสิทธิ์ จะใช้ผู้ใช้ที่สร้างบนเวิร์กสเตชันที่ใช้ไฟล์การอัพเดทร่วมกัน การตั้งค่าเริ่มต้นคือ **ไม่มี** ซึ่งจะให้สิทธิ์การเข้าถึงไฟล์การอัพเดทโดยไม่ต้องมีการตรวจสอบสิทธิ์

> ข้อมูลการตรวจสอบสิทธิ์ เช่น **ชื่อผู้ใช้** และ **รหัสผ่าน** มีไว้เพื่อการเข้าถึงเซิร์ฟเวอร์ HTTP มิเรอร์ โปรดกรอกข้อมูลในช่องเหล่านี้เฉพาะเมื่อต้องใช้ชื่อผู้ใช้และรหัสผ่านเท่านั้น

เพิ่ม**ไฟล์ของชุดใบอนุญาต**ของคุณต่อท้าย หรือสร้างใบอนุญาตที่ลงชื่อด้วยตนเองหากคุณต้องการเรียกใช้เซิร์ฟเวอร์ HTTP โดยมีการสนับสนุน HTTPS (SSL) **ประเภทใบอนุญาต**ที่ใช้ได้มีดังนี้: ASN, PEM และ PFX เพื่อความปลอดภัย

เพิ่มเติม คุณสามารถใช้โปรโตคอล HTTPS เพื่อมอบไฟล์การอัพเดทสำหรับดาวน์โหลด เมื่อใช้โปรโตคอลนี้ แทบจะเป็นไปไม่ได้เลยที่จะติดตามการโอนข้อมูลและข้อมูลประจำตัวที่ใช้เข้าสู่ระบบ ตัวเลือก**ประเภทคีย์ส่วนตัว**จะถูกตั้งค่าเป็น**แบบรวม**ตามค่าเริ่มต้น (ดังนั้นตัวเลือก**ไฟล์คีย์ส่วนตัว**จึงปิดใช้งานตามค่าเริ่มต้น) ซึ่งหมายความว่าคีย์ส่วนตัวเป็นส่วนหนึ่งในไฟล์ของชุดใบอนุญาตที่เลือก

ใบรับรองที่ลงนามด้วยตนเองสำหรับมิเรอร์ HTTPS
หากคุณกำลังใช้เซิร์ฟเวอร์มิเรอร์ HTTPS คุณต้องนำเข้าใบรับรองไปยังที่เก็บรูทที่เชื่อถือได้บนเครื่องไคลเอนต์ทั้งหมด โปรดดูที่ การติดตั้งใบรับรองหลักที่เชื่อถือได้ ใน Windows

การอัพเดทจากมิเรอร์

ในการกำหนดค่ามิเรอร์ มีวิธีการพื้นฐานสองวิธี ซึ่งโดยเนื้อหาแล้วคือพื้นที่เก็บที่ไคลเอ็นต์สามารถดาวน์โหลดไฟล์การอัพเดท โฟลเดอร์ที่มีไฟล์การอัพเดทสามารถนำเสนอในฐานะโฟลเดอร์เครือข่ายที่ใช้ร่วมกัน หรือในฐานะเซิร์ฟเวอร์ HTTP

มิเรอร์อัพเดทจะสร้างสำเนาไฟล์อัพเดทที่ใช้ในการอัพเดทเวิร์กสเตชันที่กำลังเรียกใช้ ESET Endpoint Security รุ่นเดียวกันสำหรับ Windows (ตัวอย่างเช่น ESET Endpoint Security สำหรับ Windows เวอร์ชัน 10.x จะสร้างไฟล์อัพเดทเฉพาะสำหรับเวอร์ชัน 10.x ESET Endpoint Antivirus สำหรับ Windows และ ESET Endpoint Security สำหรับ Windows)

การเข้าถึงมิเรอร์โดยใช้เซิร์ฟเวอร์ HTTP ภายใน

นี่คือการกำหนดค่าเริ่มต้นซึ่งระบุในการกำหนดค่าโปรแกรมที่กำหนดไว้ล่วงหน้า หากต้องการเข้าถึงมิเรอร์โดยใช้เซิร์ฟเวอร์ HTTP ให้ไปที่ การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์** > **มิเรอร์อัพเดท** แล้วเลือก **สร้างมิเรอร์อัพเดท**

ในส่วน **เซิร์ฟเวอร์ HTTP** ของแท็บ **มิเรอร์** คุณสามารถระบุ **พอร์ตเซิร์ฟเวอร์** ที่เซิร์ฟเวอร์ HTTP จะรับข้อมูลตลอดจนประเภทของ **การตรวจสอบสิทธิ์** ที่ใช้โดยเซิร์ฟเวอร์ HTTP พอร์ตเซิร์ฟเวอร์จะตั้งค่าเป็น **2221** ตามค่าเริ่มต้น

การตรวจสอบสิทธิ์ – ระบุถึงวิธีการตรวจสอบสิทธิ์ที่ใช้สำหรับเข้าถึงไฟล์การอัพเดท ตัวเลือกที่ใช้ได้มีดังนี้: **ไม่มี** **พื้นฐาน** และ **NTLM** เลือก **พื้นฐาน** เพื่อใช้การเข้ารหัส base64 กับการตรวจสอบสิทธิ์ด้วยชื่อผู้ใช้และรหัสผ่านแบบพื้นฐาน ตัวเลือก **NTLM** จะให้การเข้ารหัสด้วยวิธีการเข้ารหัสที่ปลอดภัย สำหรับการตรวจสอบสิทธิ์ จะใช้ผู้ใช้ที่สร้างบนเวิร์กสเตชันที่ใช้ไฟล์การอัพเดทร่วมกัน การตั้งค่าเริ่มต้นคือ **ไม่มี** ซึ่งจะให้สิทธิ์การเข้าถึงไฟล์การอัพเดทโดยไม่ต้องมีการตรวจสอบสิทธิ์

ถ้าคุณต้องการอนุญาตการเข้าถึงไฟล์การอัพเดทผ่านทางเซิร์ฟเวอร์ HTTP โฟลเดอร์มิเรอร์จะต้องอยู่ในคอมพิวเตอร์เครื่องเดียวกับอินสแตนซ์ของ ESET Endpoint Security ที่ใช้สร้างโฟลเดอร์นั้น

ข้อผิดพลาด **ชื่อผู้ใช้และ/หรือรหัสผ่านไม่ถูกต้อง** จะปรากฏขึ้นในช่องอัพเดทจากเมนูหลักหลังจากพยายามอัพเดทจากมิเรอร์หลายครั้งแต่ไม่สำเร็จ เราขอแนะนำให้คุณนำทางไปที่ การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์** > **อัพเดทมิเรอร์** และตรวจสอบชื่อผู้ใช้และรหัสผ่าน สาเหตุปกติส่วนใหญ่สำหรับข้อผิดพลาดนี้คือข้อมูลการตรวจสอบสิทธิที่ป้อนไม่ถูกต้อง

หลังจากที่เซิร์ฟเวอร์มิเรอร์ของคุณได้รับการกำหนดค่าแล้ว คุณต้องเพิ่มเซิร์ฟเวอร์การอัพเดทใหม่ไปยังเวิร์กสเตชันไคลเอ็นต์ โดยทำตามขั้นตอนต่อไปนี้:

- เปิด การตั้งค่าขั้นสูง แล้วคลิก **อัพเดท** > **โปรไฟล์** > **อัพเดท** > **การอัพเดทโมดูล**
- ยกเลิกการใช้ **เลือกโดยอัตโนมัติ** และเพิ่มเซิร์ฟเวอร์ใหม่ไปที่ช่อง **เซิร์ฟเวอร์การอัพเดท** โดยใช้หนึ่งในรูปแบบต่อไปนี้:
  http://IP_address_of_your_server:2221
  https://IP_address_of_your_server:2221 (ถ้าใช้ SSL)

การเข้าถึงมิเรอร์ผ่านการใช้งานร่วมกันในระบบ

ขั้นแรก ให้สร้างโฟลเดอร์ที่ใช้ร่วมกันบนอุปกรณ์ในระบบหรืออุปกรณ์เครือข่าย เมื่อสร้างโฟลเดอร์สำหรับมิเรอร์ คุณต้องให้สิทธิ์ “เขียน” สำหรับผู้ใช้ที่จะบันทึกไฟล์อัพเดทไปยังโฟลเดอร์ และให้สิทธิ์ “อ่าน” สำหรับผู้ใช้ทั้งหมดที่จะอัพเดท ESET Endpoint Security จากโฟลเดอร์มิเรอร์

ขั้นถัดไป กำหนดค่าการเข้าถึงมิเรอร์ในส่วน การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์** > แท็บ**อัพเดทมิเรอร์** ด้วยการปิดใช้งาน **เปิดใช้งานเซิร์ฟเวอร์ HTTP** ตัวเลือกนี้จะเปิดใช้งานเป็นค่าเริ่มต้นในแพ็คเกจการติดตั้งโปรแกรม

ถ้าโฟลเดอร์ที่ใช้ร่วมกันอยู่ในคอมพิวเตอร์เครื่องอื่นบนเครือข่าย คุณต้องป้อนข้อมูลการตรวจสอบสิทธิ์เพื่อเข้าถึงคอมพิวเตอร์อื่น หากต้องการป้อนข้อมูลการรับรองความถูกต้อง ให้เปิด การตั้งค่าขั้นสูง แล้วคลิก **อัพเดท** > **โปรไฟล์** > **อัพเดท** > **ตัวเลือกการเชื่อมต่อ** > **Windows shares** > **เชื่อมต่อกับ LAN เป็น** นี่เป็นการตั้งค่าเดียวกันกับที่ใช้เพื่อการอัพเดท ดังที่อธิบายไว้ในส่วน เชื่อมต่อกับ LAN เป็น

หากต้องการเข้าถึงโฟลเดอร์มิเรอร์ จะต้องใช้บัญชีเดียวกันกับบัญชีที่เข้าสู่ระบบในคอมพิวเตอร์ที่ใช้สร้างมิเรอร์ ในกรณีที่คอมพิวเตอร์อยู่ในโดเมน ควรใช้ชื่อผู้ใช้ "domain\user" ในกรณีที่คอมพิวเตอร์ไม่ได้อยู่ในโดเมนควรใช้ "IP_address_of_your_server\user" หรือ "hostname\user"

หลังจากที่การกำหนดค่ามิเรอร์เสร็จสมบูรณ์ ที่เวิร์กสเตชันไคลเอ็นต์ ให้ตั้งค่า *\\UNC\PATH* เป็นเซิร์ฟเวอร์การอัพเดทโดยใช้ขั้นตอนด้านล่างนี้:

1. เปิด การตั้งค่าขั้นสูง แล้วคลิก **อัพเดท** > **โปรไฟล์** > **อัพเดท**
2. ยกเลิก**เลือกโดยอัตโนมัติ** ถัดจาก **โมดูลการอัพเดท** และเซิร์ฟเวอร์ใหม่ไปยังช่อง **เซิร์ฟเวอร์การอัพเดท**

โดยใช้รูปแบบ *\\UNC\PATH*

เพื่อให้อัพเดทคุณลักษณะได้อย่างเหมาะสม จะต้องระบุพาธไปยังโฟลเดอร์มิเรอร์เป็นพาธ UNC การอัพเดทจากไดรฟ์ที่แมปในเครือข่ายอาจไม่ทำงาน

การสร้างมิเรอร์โดยใช้เครื่องมือมิเรอร์
เครื่องมือมิเรอร์จะสร้างโครงสร้างของโฟลเดอร์ซึ่งแตกต่างจากที่มิเรอร์ของ Endpoint สร้าง โดยแต่ละโฟลเดอร์จะมีไฟล์อัพเดทสำหรับกลุ่มของผลิตภัณฑ์ คุณจำเป็นต้องระบุพาธแบบเต็มไปยังโฟลเดอร์ที่ถูกต้องในการตั้งค่าอัพเดทของผลิตภัณฑ์ที่ใช้มิเรอร์
ตัวอย่างเช่น หากต้องการอัพเดท ESET PROTECT จากมิเรอร์ ให้ตั้ง อัพเดทเซิร์ฟเวอร์ ไปยัง (ตามตำแหน่งรูทเซิร์ฟเวอร์ HTTP ของคุณ):
`http://your_server_address/mirror/eset_upd/ep10`

ส่วนสุดท้ายจะควบคุมองค์ประกอบของโปรแกรม (PCU) ตามค่าเริ่มต้น องค์ประกอบของโปรแกรมที่ดาวน์โหลดจะถูกเตรียมไว้เพื่อคัดลอกไปยังมิเรอร์ในระบบ ถ้าเปิดใช้งาน **การอัพเดทผลิตภัณฑ์** จะไม่จำเป็นต้องคลิก **อัพเดท** เนื่องจากไฟล์จะถูกคัดลอกไปยังมิเรอร์ในระบบโดยอัตโนมัติเมื่อพร้อมใช้งาน โปรดดูที่ โหมดการอัพเดท สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการอัพเดทผลิตภัณฑ์

การแก้ไขปัญหาการอัพเดทมิเรอร์

ในกรณีส่วนใหญ่ ปัญหาระหว่างการอัพเดทจากเซิร์ฟเวอร์มิเรอร์จะเกิดจากสิ่งใดสิ่งหนึ่งต่อไปนี้: การระบุตัวเลือกโฟลเดอร์มิเรอร์ไม่ถูกต้อง ข้อมูลการตรวจสอบสิทธิ์ไปยังโฟลเดอร์มิเรอร์ไม่ถูกต้อง การกำหนดค่าไม่ถูกต้องในเวิร์กสเตชันที่พยายามเข้าถึงไฟล์การอัพเดทที่ดาวน์โหลดจากมิเรอร์ หรือปัญหาเหล่านี้หลายข้อรวมกัน ด้านล่างนี้เราจะให้ภาพรวมของปัญหาที่พบบ่อยซึ่งอาจเกิดขึ้นระหว่างการอัพเดทจากมิเรอร์:

ESET Endpoint Security จะรายงานข้อผิดพลาดในการเชื่อมต่อไปยังเซิร์ฟเวอร์มิเรอร์ – ซึ่งน่าจะเกิดจากการระบุเซิร์ฟเวอร์การอัพเดทที่ไม่ถูกต้อง (พาธเครือข่ายไปยังโฟลเดอร์มิเรอร์) ที่เวิร์กสเตชันในระบบจะดาวน์โหลดการอัพเดท เมื่อต้องการตรวจสอบโฟลเดอร์ ให้คลิกที่เมนู**เริ่มต้น**ของ Windows คลิก **เรียกใช้** ป้อนชื่อโฟลเดอร์ แล้วคลิก **ตกลง** เนื้อหาของโฟลเดอร์ควรปรากฏ

ESET Endpoint Security ต้องการชื่อผู้ใช้และรหัสผ่าน – ซึ่งน่าจะเกิดจากข้อมูลการตรวจสอบสิทธิ์ (ชื่อผู้ใช้และรหัสผ่าน) ไม่ถูกต้องในส่วนการอัพเดท ชื่อผู้ใช้และรหัสผ่านใช้สำหรับให้สิทธิ์ในการเข้าถึงเซิร์ฟเวอร์การอัพเดท ซึ่งโปรแกรมจะใช้อัพเดท โปรดตรวจสอบว่าข้อมูลการตรวจสอบสิทธิ์ถูกต้อง และป้อนในรูปแบบที่ถูกต้อง ตัวอย่างเช่น โดเมน/ชื่อผู้ใช้ หรือเวิร์กกรุ๊ป/ชื่อผู้ใช้ พร้อมกับรหัสผ่านที่ถูกต้อง ถ้าเซิร์ฟเวอร์มิเรอร์นั้นสามารถเข้าถึงได้โดย “ทุกคน” โปรดทราบว่ากรณีเช่นนี้ไม่ได้หมายความว่าผู้ใช้รายใดก็ได้จะสามารถเข้าถึงได้ “ทุกคน” ไม่ได้หมายถึงผู้ใช้ที่ไม่ได้รับอนุญาต แต่หมายความว่าโฟลเดอร์นั้นเข้าถึงได้โดยผู้ใช้ในโดเมนทั้งหมด ดังนั้น ถ้าโฟลเดอร์นั้นเข้าถึงได้โดย “ทุกคน” ผู้ใช้จะยังคงต้องป้อนชื่อผู้ใช้และรหัสผ่านของโดเมนในส่วนการตั้งค่าการอัพเดท

ESET Endpoint Security รายงานข้อผิดพลาดขณะเชื่อมต่อไปยังเซิร์ฟเวอร์มิเรอร์ – การสื่อสารบนพอร์ตที่กำหนดไว้สำหรับการเข้าถึงเวอร์ชัน HTTP ของมิเรอร์ถูกปิดกั้น

ESET Endpoint Security จะรายงานข้อผิดพลาดในการดาวน์โหลดไฟล์อัพเดท – ซึ่งน่าจะเกิดจากการระบุเซิร์ฟเวอร์การอัพเดทที่ไม่ถูกต้อง (พาธเครือข่ายไปยังโฟลเดอร์มิเรอร์) ที่เวิร์กสเตชันในระบบจะดาวน์โหลดการอัพเดท

การป้องกัน

การป้องกันช่วยปกป้องการโจมตีระบบที่ประสงค์ร้ายโดยการควบคุมไฟล์ อีเมล และการติดต่อสื่อสารทางอินเทอร์เน็ต ตัวอย่างเช่น หากวัตถุที่จัดประเภทเป็นมัลแวร์ถูกตรวจจับ การปรับปรุงแก้ไขจะเริ่มต้นขึ้น การป้องกันสามารถลบวัตถุได้โดยการบล็อกวัตถุก่อน แล้วจึงกำจัด ลบ หรือย้ายไปยังการกักเก็บ

หากต้องการกำหนดค่าการป้องกันโดยละเอียด ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน**

การเปลี่ยนแปลงในส่วนการป้องกันควรดำเนินการโดยผู้ใช้ที่มีประสบการณ์ในการใช้งานเท่านั้น การกำหนดค่าที่ไม่ถูกต้องของการตั้งค่าจะลดระดับความสามารถในการป้องกัน

ในส่วนนี้:

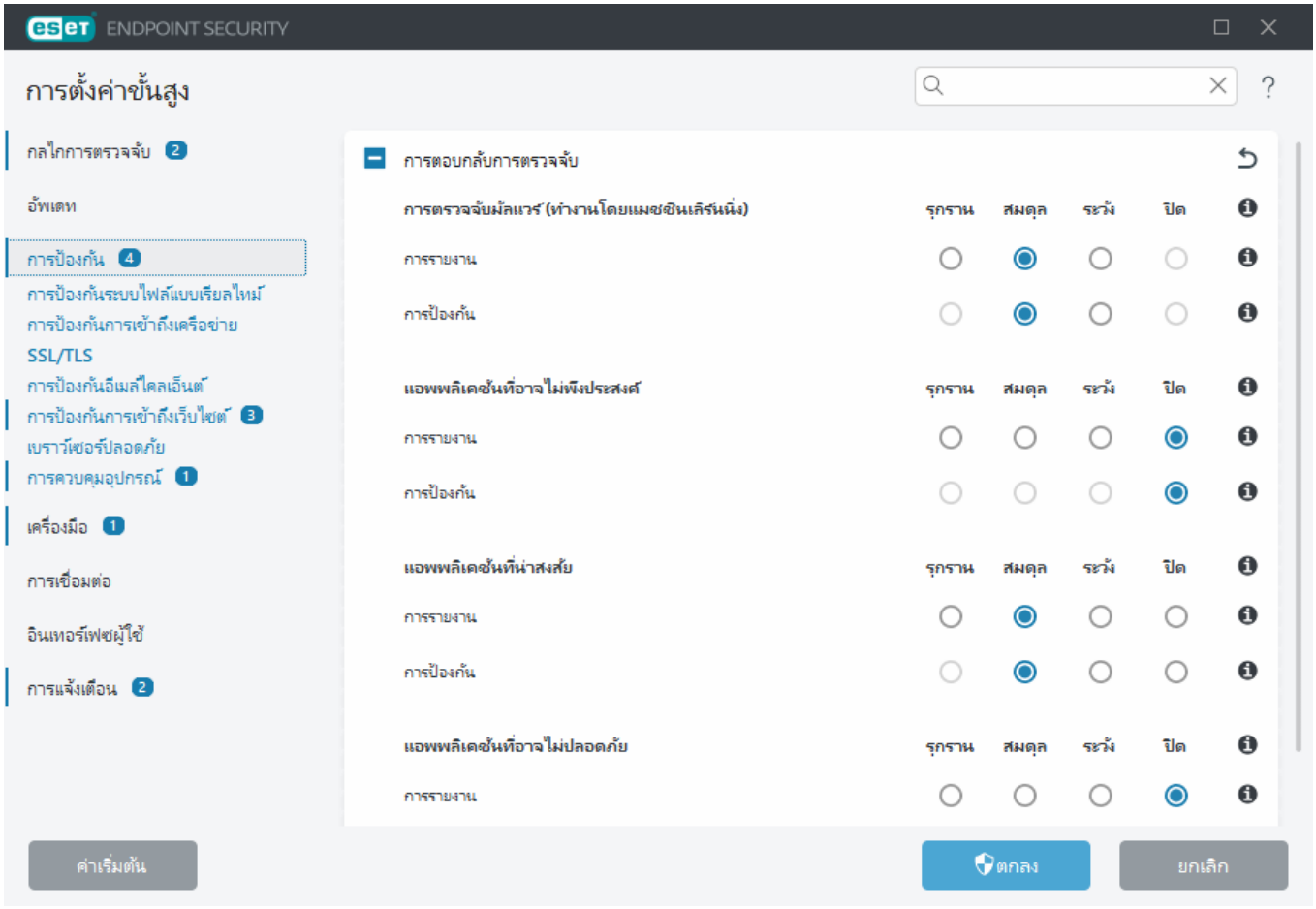
- การตอบกลับการตรวจจับ
- การตั้งค่าการรายงาน
- การตั้งค่าการป้องกัน

การตอบกลับการตรวจจับ

การตอบสนองการตรวจจับช่วยให้คุณสามารถกำหนดค่าระดับการรายงานและการป้องกันของการทำงานประเภทต่อไปนี้:

- **การตรวจหามัลแวร์ (ขับเคลื่อนโดยแมชชีนเลิร์นนิง)** – ไวรัสคอมพิวเตอร์คือโค้ดที่เป็นอันตราย ซึ่งเข้ามาต่อเติมหรือต่อท้ายไฟล์ที่มีอยู่ในคอมพิวเตอร์ของคุณ อย่างไรก็ตาม คำว่า "ไวรัส" เป็นคำที่มักถูกใช้อย่างผิดๆ "มัลแวร์" (ซอฟต์แวร์ที่เป็นอันตราย) คือคำที่ถูกต้องมากกว่า การตรวจจับมัลแวร์ดำเนินการโดยโมดูลกลไกการตรวจจับควบคู่ไปกับส่วนประกอบของ Machine Learning อ่านเพิ่มเติมเกี่ยวกับแอพพลิเคชันประเภทนี้ได้ใน ประมวลศัพท์

- **แอพพลิเคชันที่อาจไม่พึงประสงค์** - เกรย์แวร์หรือแอพพลิเคชันที่อาจไม่พึงประสงค์ (PUA) เป็นซอฟต์แวร์ประเภทกว้างๆ ที่ไม่ได้มีเจตนาที่เป็นอันตรายอย่างชัดแจ้งเมื่อเทียบกับมัลแวร์ประเภทอื่น เช่น ไวรัสหรือม้าโทรจัน อย่างไรก็ตาม ซอฟต์แวร์นี้อาจติดตั้งซอฟต์แวร์อื่นที่ไม่ต้องการเพิ่มเติม เปลี่ยนลักษณะการทำงานของอุปกรณ์ดิจิทัล หรือดำเนินการกิจกรรมที่ผู้ใช้ไม่อนุญาตหรือไม่คาดหมาย อ่านเพิ่มเติมเกี่ยวกับแอพพลิเคชันประเภทนี้ได้ใน ประมวลศัพท์
- **แอพพลิเคชันที่น่าสงสัย** – จะรวมถึงโปรแกรมต่างๆ ที่บีบอัดด้วย แพ็คเกอร์ หรือตัวป้องกันต่างๆ ตัวป้องกันเหล่านี้มักถูกโจมตีโดยผู้เขียนมัลแวร์เพื่อหลบเลี่ยงการตรวจหา
- **แอพพลิเคชันที่อาจไม่ปลอดภัย** – หมายถึงซอฟต์แวร์เชิงพาณิชย์ที่ถูกต้องที่อาจถูกนำไปใช้ในทางที่ผิดเพื่อวัตถุประสงค์ที่เป็นอันตราย ตัวอย่างของแอพพลิเคชันที่อาจไม่ปลอดภัยประกอบด้วยเครื่องมือเข้าถึงระยะไกล แอพพลิเคชันที่พยายามค้นหารหัสผ่าน และเครื่องมือบันทึกการกดแป้นพิมพ์ (โปรแกรมที่บันทึกการใช้แป้นพิมพ์ของผู้ใช้) อ่านเพิ่มเติมเกี่ยวกับแอพพลิเคชันประเภทนี้ได้ใน ประมวลศัพท์



การป้องกันที่ปรับปรุง
ในตอนนี้ แมชชีนเลิร์นนิงขั้นสูงเป็นส่วนหนึ่งของการป้องกันในฐานะชั้นการป้องกันขั้นสูง ซึ่งช่วยปรับปรุงการตรวจหาโดยอิงจากแมชชีนเลิร์นนิง อ่านข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้ใน ประมวลศัพท์

การตั้งค่าการรายงาน

เมื่อมีการตรวจหาเกิดขึ้น (เช่น ภัยคุกคามถูกพบและจัดประเภทเป็นมัลแวร์) ข้อมูลจะถูกบันทึกไปยัง บันทึกการตรวจหา และ การแจ้งเตือนบนเดสก์ท็อป จะเกิดขึ้นเมื่อถูกกำหนดค่าใน ESET Endpoint Security

เกณฑ์การรายงานจะกำหนดค่าสำหรับแต่ละประเภท (เรียกว่า "ประเภท"):

1. การตรวจหามัลแวร์
2. แอพพลิเคชันที่อาจไม่พึงประสงค์
3. อาจไม่ปลอดภัย
4. แอพพลิเคชันที่น่าสงสัย

การรายงานจะทำงานด้วยกลไกการตรวจจับ รวมถึงองค์ประกอบการเรียนรู้ของเครื่อง คุณสามารถกำหนดเกณฑ์การรายงานที่สูงกว่าเกณฑ์ การป้องกัน ในปัจจุบันได้ การตั้งค่าการรายงานเหล่านี้ไม่ส่งผลกระทบต่อการปิดกั้น การกำจัด หรือการลบวัตถุ

โปรดอ่านข้อความต่อไปนี้ก่อนแก้ไขเกณฑ์ (หรือระดับ) สำหรับการรายงานประเภท:

เกณฑ์	คำอธิบาย
รุกราน	การรายงาน ประเภท ถูกกำหนดค่าไว้เป็นความไวสูงสุด ซึ่งจะทำให้มีการรายงานการตรวจจับเพิ่มเติม การตั้งค่า **สูงสุด** อาจระบุวัตถุเป็น ประเภท อย่างไม่ถูกต้องได้
สมดุล	การรายงาน ประเภท จะกำหนดค่าไว้เป็นสมดุล ซึ่งการตั้งค่านี้จะปรับประสิทธิภาพที่มุ่งเน้นความสมดุลระหว่างประสิทธิภาพการทำงานและความถูกต้องของอัตราการตรวจพบ และจำนวนวัตถุที่รายงานไม่ถูกต้อง
ระวัง	การรายงาน ประเภท จะกำหนดค่าให้ลดวัตถุที่รายงานผิดพลาดลงให้น้อยที่สุดในขณะที่ยังคงรักษาระดับการป้องกันที่เพียงพอ โดยจะรายงานวัตถุเมื่อความน่าจะเป็นปรากฏชัดและตรงกับพฤติกรรมของ ประเภท
ปิด	การรายงานสำหรับประเภทไม่ได้เปิดใช้งาน และไม่พบ รายงาน หรือล้างการตรวจหาสำหรับประเภทนี้ เป็นผลให้การตั้งค่านี้ปิดใช้งานการป้องกันจากการตรวจจับประเภทนี้ การปิดนั้นไม่สามารถใช้ได้สำหรับการรายงานมัลแวร์ และเป็นค่าเริ่มต้นสำหรับแอพพลิเคชันที่อาจไม่ปลอดภัย

^ ความพร้อมของโมดูลการป้องกัน ESET Endpoint Security

ความพร้อม (เปิดใช้งาน หรือ ปิดใช้งาน) ของโมดูลการป้องกันสำหรับเกณฑ์ประเภทที่เลือกมีดังต่อไปนี้:

	รุกราน	สมดุล	ระวัง	ปิด*
โมดูลเครื่องมือการเรียนรู้ขั้นสูง	✓ (โหมดรุกราน)	✓ (โหมดระมัดระวัง)	X	X
โมดูลกลไกการตรวจจับ	✔	✔	✔	X
โมดูลการป้องกันอื่นๆ	✔	✔	✔	X

*ไม่แนะนำ

ระบุเวอร์ชันผลิตภัณฑ์ โมดูลโปรแกรม และวันที่สร้าง

1. คลิก **วิธีใช้และการสนับสนุน** > **เกี่ยวกับ ESET Endpoint Security**
2. ในหน้าจอ **เกี่ยวกับ** บรรทัดแรกของข้อความจะแสดงหมายเลขเวอร์ชันของผลิตภัณฑ์ ESET ของคุณ
3. คลิก **องค์ประกอบที่ติดตั้ง** เพื่อเข้าถึงข้อมูลเกี่ยวกับโมดูลเฉพาะ

Keynotes

Keynotes จำนวนหนึ่งเมื่อตั้งค่าเกณฑ์ที่เหมาะสมสำหรับสภาพแวดล้อมของคุณ:

- เกณฑ์**สมดุล**เป็นที่แนะนำสำหรับการตั้งค่าส่วนใหญ่
- แนะนำให้ใช้เกณฑ์ **ระวัง** สำหรับสภาพแวดล้อมที่มุ่งเน้นไปที่การลดวัตถุที่รายงานผิดพลาดโดยซอฟต์แวร์ด้านความปลอดภัยเป็นสำคัญ
- ยิ่งเกณฑ์การรายงานสูงเท่าใด อัตราการตรวจหาก็สูงเท่านั้น แต่ก็มีโอกาสที่จะเป็นวัตถุที่รายงานผิดพลาดได้มากกว่าเช่นเดียวกัน
- จากมุมมองของโลกแห่งความเป็นจริง ไม่มีการรับประกันอัตราการตรวจหา 100% เช่นเดียวกับที่มีโอกาส 0% ที่จะหลีกเลี่ยงไม่ให้มีการจัดประเภทวัตถุที่ไม่ติดไวรัสอย่างผิดๆ ว่าเป็นมัลแวร์
- ทำให้ ESET Endpoint Security และโมดูลอัพเดทอยู่เสมอ เพื่อทำให้เกิดความสมดุลสูงสุด ระหว่างการทำงานและความถูกต้องของอัตราการตรวจหา และจำนวนวัตถุที่รายงานผิดพลาด

การตั้งค่าการป้องกัน

หากวัตถุที่ถูกจัดประเภทเป็นประเภทถูกรายงาน โปรแกรมจะปิดกั้นวัตถุและ กำจัด ลบ หรือย้ายวัตถุไปยัง การกักเก็บ

โปรดอ่านข้อความต่อไปนี้ก่อนแก้ไขเกณฑ์ (หรือระดับ) สำหรับการป้องกันประเภท:

เกณฑ์	คำอธิบาย
รุกราน	การตรวจจับระดับรุกราน (หรือต่ำกว่า) ที่รายงานจะถูกปิดกั้นและการปรับปรุงแก้ไขอัตโนมัติ (เช่น การล้าง) จะเริ่มขึ้น แนะนำให้ใช้การตั้งค่านี้เมื่อ Endpoint ทั้งหมดถูกสแกนด้วยการตั้งค่าแบบรุกราน และมีวัตถุที่รายงานผิดพลาดถูกเพิ่มลงในการยกเว้นการตรวจจับ
สมดุล	การตรวจหาระดับสมดุล (หรือต่ำกว่า) ที่รายงานจะถูกปิดกั้นและการปรับปรุงแก้ไขอัตโนมัติ (เช่น การกำจัด) จะเริ่มขึ้น
ระวัง	การตรวจหาระดับระวังที่รายงานจะถูกปิดกั้นและการปรับปรุงแก้ไขอัตโนมัติ (เช่น การกำจัด) จะเริ่มขึ้น
ปิด	มีประโยชน์ต่อการระบุและยกเว้นวัตถุที่รายงานผิดพลาด การปิดนั้นไม่สามารถใช้ได้สำหรับการรายงานมัลแวร์ และเป็นค่าเริ่มต้นสำหรับแอพพลิเคชันที่อาจไม่ปลอดภัย

แนวทางปฏิบัติ

ไม่ได้รับการจัดการ (เวิร์กสเตชันไคลเอนต์แบบแยก)

เก็บค่าที่แนะนำเป็นค่าเริ่มต้นไว้เช่นนั้น

สภาพแวดล้อมที่ได้รับการจัดการ

การตั้งค่าเหล่านี้มักปรับใช้กับเวิร์กสเตชันผ่านนโยบาย

1. ระยะเริ่มต้น

ระยะนี้อาจใช้เวลาถึงหนึ่งสัปดาห์

- ตั้งค่าเกณฑ์**การรายงาน**ทั้งหมดเป็น**สมดุล**
  หมายเหตุ: หากจำเป็น ให้ตั้งค่าเป็น **รุกราน**
- ตั้งค่าหรือให้ **การป้องกัน** สำหรับมัลแวร์เป็น **สมดุล**
- ตั้งค่า **การป้องกัน** สำหรับประเภทอื่นๆ เป็น **ระวัง**
  หมายเหตุ: ไม่แนะนำให้ตั้งค่าเกณฑ์ **การป้องกัน** เป็นแบบ **รุกราน** ในระยะนี้เนื่องจากการตรวจหาทั้งหมดที่พบจะถูกปรับปรุงแก้ไข รวมถึงรายการที่รายงานผิดพลาดด้วย
- ระบุวัตถุที่รายงานผิดพลาดจาก บันทึกการตรวจหา และเพิ่มวัตถุเหล่านั้นไปยัง การยกเว้นการตรวจหา ก่อน

2. ระยะเปลี่ยนผ่าน

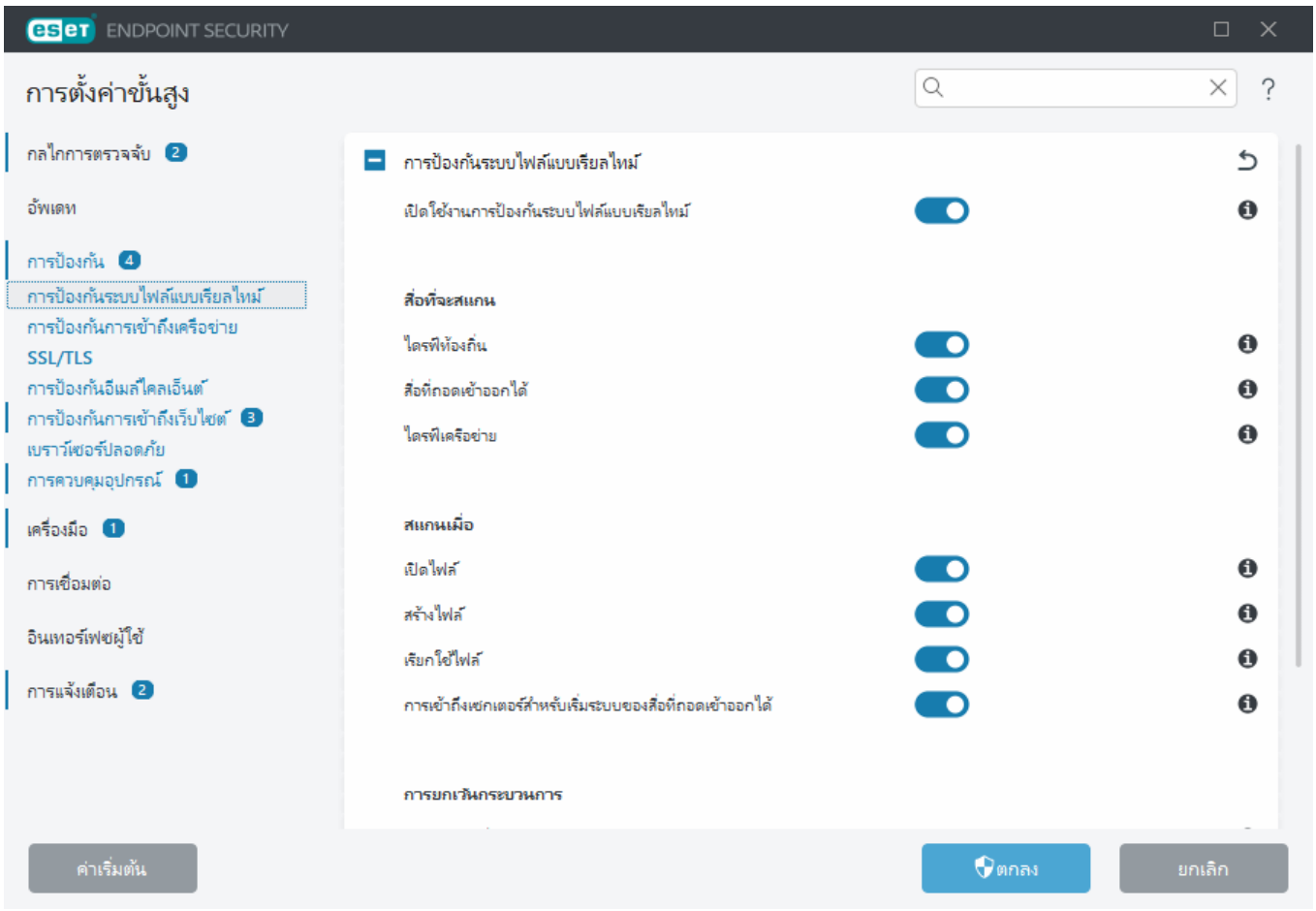
- จัดเตรียม "ระยะการผลิต" ในบางเวิร์กสเตชันเป็นการทดสอบ (ไม่ใช่สำหรับเวิร์กสเตชันทั้งหมดบนเครือข่าย)

3. ระยะการผลิต

- ตั้งค่าเกณฑ์**การป้องกัน**ทั้งหมดเป็น**สมดุล**
- เมื่อจัดการจากระยะไกล ให้ใช้ นโยบายที่กำหนดไว้ล่วงหน้าสำหรับ ESET Endpoint Security
- เกณฑ์การป้องกันแบบ **รุกราน** สามารถตั้งค่าได้หากจำเป็นต้องใช้อัตราการตรวจหาสูงสุดและยอมรับวัตถุที่รายงานผิดพลาดได้
- ตรวจสอบ บันทึกการตรวจหา หรือรายงาน ESET PROTECT สำหรับการตรวจหาที่อาจหายไป

การป้องกันระบบไฟล์แบบเรียลไทม์

การป้องกันระบบไฟล์แบบเรียลไทม์จะควบคุมไฟล์ทั้งหมดในระบบสำหรับรหัสที่เป็นอันตรายเมื่อเปิด สร้าง หรือเรียกใช้



ตามค่าเริ่มต้น การป้องกันแบบเรียลไทม์จะเริ่มต้นทำงานเมื่อเริ่มต้นระบบและให้การสแกนทำงานต่อเนื่อง เราไม่แนะนำให้ปิดใช้งาน **เปิดใช้การป้องกันระบบไฟล์แบบเรียลไทม์** ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันระบบไฟล์แบบเรียลไทม์** > **การป้องกันระบบไฟล์แบบเรียลไทม์**

สื่อที่จะสแกน

ตามค่าเริ่มต้น โปรแกรมจะสแกนสื่อทุกประเภทเพื่อหาสิ่งที่อาจเป็นภัยคุกคาม:

- **ไดรฟ์ท้องถิ่น** – สแกนระบบทั้งหมดและซ่อมแซมฮาร์ดไดรฟ์ (ตัวอย่างเช่น: *C:*\, *D:*\)
- **สื่อที่ถอดเข้าออกได้** – สแกน CD/DVD, อุปกรณ์เก็บข้อมูล USB, การ์ดหน่วยความจำ ฯลฯ
- **ไดรฟ์เครือข่าย** – สแกนไดรฟ์เครือข่ายที่ถูกแมปทั้งหมด (ตัวอย่างเช่น: *H:*\ เป็น *store04*) หรือไดรฟ์เครือข่ายที่เข้าถึงโดยตรง (ตัวอย่างเช่น: *store08*)

เราขอแนะนำให้คุณใช้การตั้งค่าเริ่มต้น และแก้ไขการตั้งค่าเฉพาะบางกรณีเท่านั้น เช่น เมื่อการสแกนสื่อบางชนิดทำให้การรับส่งข้อมูลช้าลงอย่างมาก

สแกนเมื่อ

ตามค่าเริ่มต้น ไฟล์ทั้งหมดจะถูกสแกนเมื่อเปิด สร้าง หรือดำเนินการ ขอแนะนำให้คุณคงการตั้งค่าเริ่มต้นเหล่านี้ไว้ เนื่องจากการตั้งค่าเหล่านี้จะให้การป้องกันแบบเรียลไทม์ในระดับสูงสุดสำหรับคอมพิวเตอร์ของคุณ:

- **เปิดไฟล์** – สแกนเมื่อไฟล์ถูกเปิด
- **สร้างไฟล์** – สแกนไฟล์ที่ถูกสร้างหรือแก้ไข
- **เรียกใช้ไฟล์** – สแกนเมื่อไฟล์ถูกเรียกใช้หรือทำงาน
- **การเข้าถึงบูตเซคเตอร์ของสื่อที่ถอดเข้าออกได้** – เมื่อสื่อที่ถอดเข้าออกได้ที่มีบูตเซคเตอร์เสียบเข้าไปในอุปกรณ์ บูตเซคเตอร์จะสแกนในทันที ตัวเลือกนี้ไม่ได้เปิดใช้งานการสแกนไฟล์สื่อที่ถอดเข้าออกได้ การสแกนไฟล์สื่อที่ถอดเข้าออกได้จะอยู่ใน **สื่อที่จะสแกน** > **สื่อที่ถอดเข้าออกได้** เพื่อให้ **การเข้าถึงบูตเซกเตอร์ของสื่อที่ถอดเข้าออกได้** ทำงานอย่างถูกต้อง ให้เปิดใช้งาน **บูตเซกเตอร์/UEFI** ในพารามิเตอร์ ThreatSense ไว้เสมอ

การยกเว้นกระบวนการ

ดู การยกเว้นกระบวนการ

ThreatSense

การป้องกันระบบไฟล์แบบเรียลไทม์จะตรวจสอบสื่อทุกประเภท และจะถูกเรียกใช้ตามเหตุการณ์ต่าง ๆ ของระบบ เช่น การเข้าถึงไฟล์ เมื่อใช้วิธีการตรวจหาของเทคโนโลยี **ThreatSense** (ดังที่อธิบายไว้ใน ThreatSense) คุณสามารถกำหนดค่าการป้องกันระบบไฟล์แบบเรียลไทม์เพื่อดูแลจัดการกับไฟล์สร้างใหม่ซึ่งแตกต่างจากไฟล์ที่มีอยู่แล้ว ตัวอย่างเช่น คุณสามารถกำหนดค่าการป้องกันระบบไฟล์แบบเรียลไทม์เพื่อตรวจสอบไฟล์ที่สร้างใหม่ได้อย่างใกล้ชิดมากขึ้น

เพื่อให้มีการใช้ทรัพยากรของระบบน้อยที่สุดเมื่อใช้การป้องกันระบบไฟล์แบบเรียลไทม์ ไฟล์ที่ผ่านการสแกนแล้วจะไม่มีการสแกนซ้ำอีก (ยกเว้นกรณีที่มีการแก้ไข) ไฟล์จะถูกสแกนอีกครั้งในทันทีหลังจากอัพเดทกลไกตรวจหาแต่ละครั้ง สามารถควบคุมการทำงานแบบนี้ได้ด้วยการใช้ **การเพิ่มประสิทธิภาพแบบสมาร์ท** หากปิดใช้งาน **การเพิ่มประสิทธิภาพแบบสมาร์ท** ไฟล์ทั้งหมดจะถูกสแกนในแต่ละครั้งที่มีการเข้าถึง หากต้องการแก้ไขการตั้งค่านี้ ให้เปิดการป้องกันขั้นสูง > **การป้องกัน**> **การป้องกันระบบไฟล์แบบเรียลไทม์** คลิก **ThreatSense** > **อื่น ๆ** แล้วเลือก

หรือไม่เลือก **เปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท**

การป้องกันระบบไฟล์แบบเรียลไทม์ยังช่วยให้คุณสามารถกำหนดค่า พารามิเตอร์ ThreatSense เพิ่มเติมได้

การยกเว้นกระบวนการ

กระบวนการคุณลักษณะข้อยกเว้นต่างๆ ช่วยให้คุณยกเว้นกระบวนการแอพพลิเคชันจากการป้องกันระบบไฟล์แบบเรียลไทม์ เพื่อปรับปรุงความเร็วของการสำรองข้อมูล กระบวนการผสมผสานและความพร้อมบริการ เทคนิคบางอย่างที่รู้จักที่ขัดแย้งกับการป้องการมัลแวร์ระดับไฟล์ จะใช้ระหว่างการสำรองข้อมูล วิธีที่มีประสิทธิภาพวิธีเดียวที่จะหลีกเลี่ยงสถานการณ์ทั้งสองแบบคือการปิดใช้งานป้องกันมัลแวร์ โดยการยกเว้นกระบวนการที่ระบุ (ตัวอย่างเช่น โซลูชันการสำรองข้อมูลเหล่านั้น) การทำงานไฟล์ทั้งหมดถือว่ากระบวนการที่ยกเว้นดังกล่าวถูกเพิกเฉยและถูกพิจารณาว่าปลอดภัย ดังนั้นการลดการรบกวนด้วยกระบวนการสำรองข้อมูล เราขอแนะนำให้คุณใช้ความระมัดระวังเมื่อสร้างข้อยกเว้น เครื่องมือการสำรองข้อมูลที่ถูกยกเว้นสามารถเข้าถึงไฟล์ที่ติดไวรัสได้ โดยไม่มีการเรียกใช้คำเตือน ซึ่งเป็นเหตุผลที่การอนุญาตที่ได้รับการขยายจะอนุญาตในโมดูลการป้องกันแบบเรียลไทม์เท่านั้น

อย่าสับสนกับ นามสกุลไฟล์ที่ยกเว้น การยกเว้น HIPS การตรวจหานามสกุลไฟล์ หรือ การตรวจหาการทำงาน

การยกเว้นกระบวนการจะช่วยลดความเสี่ยงของข้อขัดแย้งและที่อาจเกิดขึ้นได้และปรับปรุงประสิทธิภาพของแอพพลิเคชันที่ยกเว้น ซึ่งจะกลายเป็นผลกระทบด้านบวกกับประสิทธิภาพโดยรวมและความมั่นคงของระบบปฏิบัติการ ข้อยกเว้นของกระบวนการ / แอพพลิเคชันเป็นข้อยกเว้นของไฟล์ที่สามารถยกเว้นได้ (*.exe*)

คุณสามารถเพิ่มไฟล์ที่เรียกใช้ได้ลงในรายการประมวลผลที่ที่มีการเว้นได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันระบบไฟล์แบบเรียลไทม์** > **การป้องกันระบบไฟล์แบบเรียลไทม์** > **การยกเว้นการประมวลผล**

คุณลักษณะนี้ได้รับการออกแบบมาเพื่อแยกเครื่องมือการสำรองข้อมูล การยกเว้นกระบวนการของเครื่องมือสำรองข้อมูลจากการสแกนจะไม่ใช่เพียงทำให้มั่นใจเรื่องความมั่นคงของระบบเท่านั้น แต่ยังจะไม่มีผลกระทบต่อประสิทธิภาพของการสำรองข้อมูล ซึ่งการสำรองจะไม่ทำงานช้าลงในขณะที่กำลังใช้งานอยู่

คลิก **แก้ไข** เพื่อเปิดหน้าต่างการจัดการ **ข้อยกเว้นของกระบวนการ** ที่คุณสามารถ เพิ่มข้อยกเว้นต่างๆ และเรียกใช้ไฟล์ที่สามารถยกเว้นได้ (ตัวอย่างเช่น *Backup-tool.exe*) ซึ่งจะแยกออกจากการสแกน เมื่อไฟล์ *.exe* ถูกเพิ่มไปยังข้อยกเว้นแล้ว กิจกรรมของกระบวนการนี้จะไม่ใช่ได้รับการตรวจสอบโดย ESET Endpoint Security และจะไม่มีการสแกนเพื่อทำงานบนการปฏิบัติการของไฟล์ใดที่ดำเนินการโดยกระบวนการนี้

หากคุณไม่ใช้ฟังก์ชันเรียกดูเมื่อเลือกกระบวนการที่สามารถยกเว้นได้ คุณจำเป็นต้องป้อนพาธแบบเต็มให้เป็นแบบยกเว้นได้ด้วยตนเอง มิเช่นนั้น ข้อยกเว้นจะไม่ทำงานอย่างถูกต้องและ HIPS อาจรายงานข้อผิดพลาด

คุณยังสามารถ **แก้ไข** กระบวนการที่มีอยู่หรือ **ลบ** กระบวนการออกจากข้อยกเว้นได้

การป้องกันการเข้าถึงเว็บไซต์จะไม่พิจารณาให้เป็นข้อยกเว้น ดังนั้น หากคุณยกเว้นไฟล์ที่สามารถยกเว้นของเว็บเบราว์เซอร์ของคุณได้ ไฟล์ที่ดาวน์โหลดแล้วจะยังคงสแกนอยู่ วิธีนี้การแฝงตัวจะยังสามารถตรวจพบได้ สถานการณ์นี้เป็นเพียงตัวอย่างเท่านั้น และเราจะไม่แนะนำให้คุณสร้างข้อยกเว้นสำหรับเว็บเบราว์เซอร์

เพิ่มหรือแก้ไขกระบวนการการยกเว้น

หน้าต่างข้อความจะทำให้คุณ **เพิ่ม** กระบวนการต่างๆ ที่ยกเว้นจากการตรวจหาเธรด การยกเว้นกระบวนการจะช่วยลดความเสี่ยงของข้อขัดแย้งและที่อาจเกิดขึ้นได้และปรับปรุงประสิทธิภาพของแอพพลิเคชันที่ยกเว้น ซึ่งจะกลายเป็นผลกระทบด้านบวกกับประสิทธิภาพโดยรวมและความมั่นคงของระบบปฏิบัติการ ข้อยกเว้นของกระบวนการ / แอพพลิเคชันเป็นข้อยกเว้นของไฟล์ที่สามารถยกเว้นได้ (*.exe*)

เลือกพาธไฟล์ของแอพพลิเคชันที่ได้รับการยกเว้นโดยการคลิก... อย่าป้อนชื่อของแอพพลิเคชัน เมื่อไฟล์ *.exe* ถูกเพิ่มไปยังข้อยกเว้นแล้ว กิจกรรมของกระบวนการนี้จะไม่ใช่ได้รับการตรวจสอบโดย ESET Endpoint Security และจะไม่มีการสแกนเพื่อทำงานบนการปฏิบัติการของไฟล์ใดที่ดำเนินการโดยกระบวนการนี้

หากคุณไม่ใช้ฟังก์ชันเรียกดูเมื่อเลือกกระบวนการที่สามารถยกเว้นได้ คุณจำเป็นต้องป้อนพาธแบบเต็มให้เป็นแบบยกเว้นได้ด้วยตนเอง มิเช่นนั้น ข้อยกเว้นจะไม่ทำงานอย่างถูกต้องและ HIPS อาจรายงานข้อผิดพลาด

คุณยังสามารถ **แก้ไข** กระบวนการที่มีอยู่หรือ **ลบ** กระบวนการออกจากข้อยกเว้นได้

เมื่อใดควรแก้ไขการกำหนดค่าการป้องกันแบบเรียลไทม์

การป้องกันแบบเรียลไทม์เป็นองค์ประกอบที่สำคัญที่สุดในการรักษาระบบที่ปลอดภัย โปรดระมัดระวังเมื่อแก้ไขพารามิเตอร์ทุกครั้ง เราขอแนะนำให้คุณแก้ไขพารามิเตอร์ในกรณีพิเศษเท่านั้น

หลังจากการติดตั้ง ESET Endpoint Security การตั้งค่าทั้งหมดจะได้รับการเพิ่มประสิทธิภาพเพื่อให้การรักษาความปลอดภัยให้กับระบบในระดับสูงสุดสำหรับผู้ใช้ หากต้องการคืนค่าการตั้งค่าเริ่มต้น คลิก ↺ ถัดจาก การตั้งค่าขั้นสูง > **การป้องกัน** > **การตอบสนองการตรวจจับ**

การตรวจสอบการป้องกันแบบเรียลไทม์

เมื่อต้องการตรวจสอบว่าการป้องกันแบบเรียลไทม์กำลังทำงานและตรวจหาไวรัส ให้ใช้ไฟล์ทดสอบจาก eicar.com ไฟล์ทดสอบนี้เป็นไฟล์ที่ปลอดภัยซึ่งสามารถตรวจพบโดยโปรแกรมป้องกันไวรัสทุกประเภท ไฟล์นี้สร้างขึ้นโดยบริ

ษัท EICAR (European Institute for Computer Antivirus Research) เพื่อทดสอบการทำงานของโปรแกรมป้องกันไวรัส

ไฟล์มีให้ดาวน์โหลดได้แล้วที่นี่ http://www.eicar.org/download/eicar.com
หลังจากที่คุณป้อน URL นี้ลงในเบราว์เซอร์ของคุณ คุณควรเห็นข้อความว่าภัยคุกคามถูกลบออกแล้ว

ควรทำอย่างไรเมื่อการป้องกันแบบเรียลไทม์ไม่ทำงาน

ในบทนี้ เราจะอธิบายปัญหาที่อาจเกิดขึ้นเมื่อใช้การป้องกันแบบเรียลไทม์ และวิธีการแก้ปัญหาดังกล่าวด้วย

การป้องกันแบบเรียลไทม์ถูกปิดใช้งาน

หากผู้ใช้ปิดใช้งานการป้องกันแบบเรียลไทม์โดยไม่ได้ตั้งใจ คุณควรเปิดใช้งานคุณลักษณะนี้อีกครั้ง หากต้องการเปิดใช้งานการป้องกันแบบเรียลไทม์อีกครั้ง ให้ไปที่ **การตั้งค่า** ในหน้าต่างโปรแกรมหลัก แล้วคลิก **คอมพิวเตอร์** > **การป้องกันระบบไฟล์แบบเรียลไทม์**

ากการป้องกันแบบเรียลไทม์ไม่สามารถเริ่มต้นเมื่อระบบเริ่มต้น เป็นไปได้ว่าอาจเกิดจากการปิดใช้งานตัวเลือก **เปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์** หากต้องการตรวจสอบว่าตัวเลือกนี้เปิดใช้งานอยู่หรือไม่ ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันระบบไฟล์แบบเรียลไทม์**

ถ้าการป้องกันแบบเรียลไทม์ไม่พบหรือไม่กำจัดการแฝงตัว

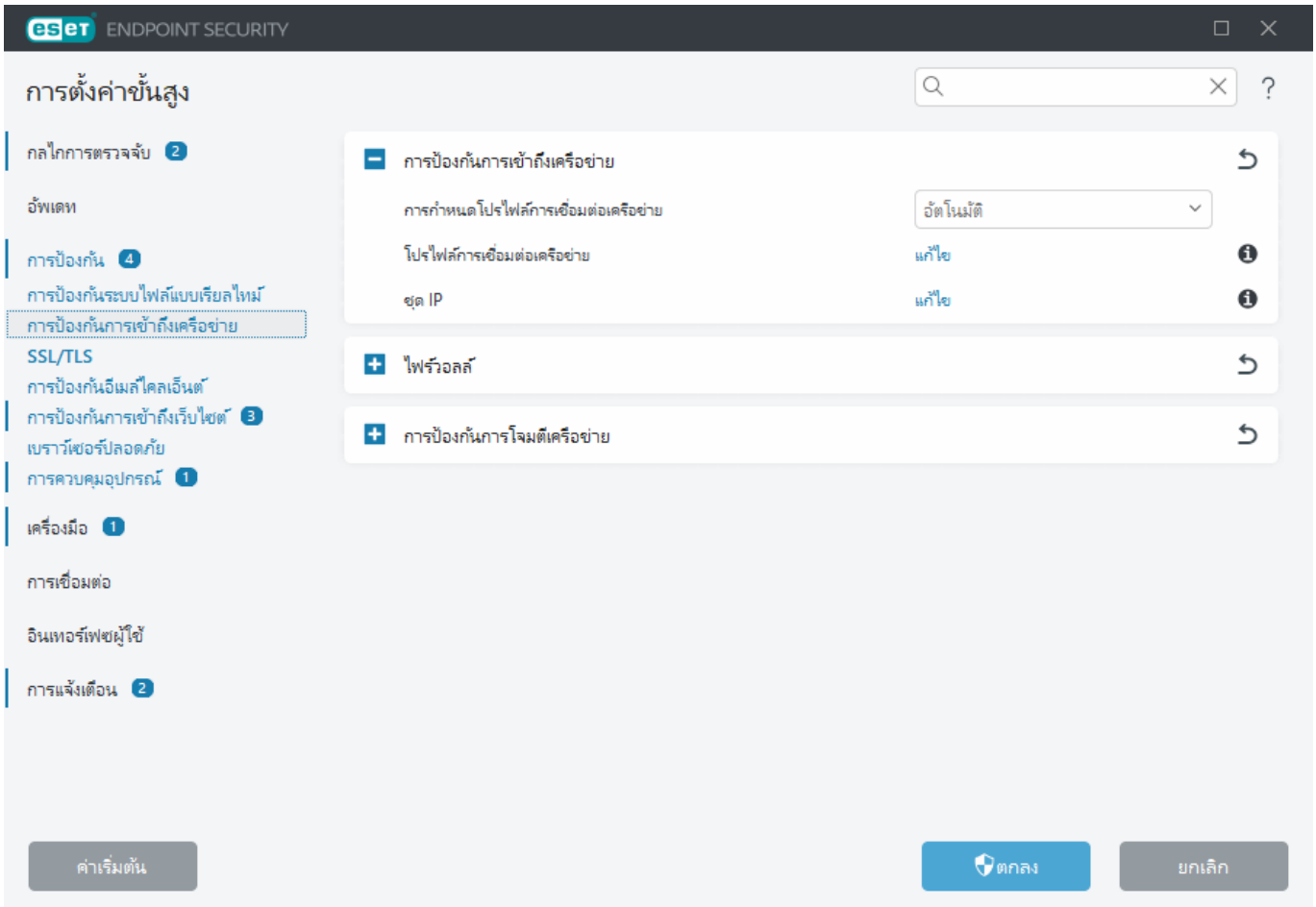
ตรวจสอบว่าไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอื่นในคอมพิวเตอร์ของคุณ หากโปรแกรมป้องกันไวรัสสองโปรแกรมถูกติดตั้งในเวลาเดียวกัน อาจเกิดความขัดแย้งขึ้นได้ ขอแนะนำให้คุณลบการติดตั้งโปรแกรมป้องกันไวรัสอื่นในระบบของคุณก่อนติดตั้ง ESET

การป้องกันแบบเรียลไทม์ไม่เริ่มต้นทำงาน

หากการป้องกันแบบเรียลไทม์ไม่เริ่มต้นเมื่อระบบเริ่มต้น (และ **เปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์** เปิดใช้งานอยู่) ปัญหานี้อาจเกิดจากข้อขัดแย้งกับโปรแกรมอื่นๆ หากต้องการแก้ไขปัญหานี้ ให้ สร้างบันทึก ESET SysInspector แล้วส่งไปยังฝ่ายสนับสนุนด้านเทคนิคของ ESET เพื่อการวิเคราะห์

การป้องกันการเข้าถึงเครือข่าย

การป้องกันการเข้าถึงเครือข่ายช่วยให้คุณกำหนดค่าการเชื่อมต่อเครือข่ายทั้งหมดของคุณได้อย่างละเอียด คุณสามารถอนุญาต/ปฏิเสธการเข้าถึงคอมพิวเตอร์ของคุณบนเครือข่ายแบบเฉพาะเจาะจง อนุญาต/ปฏิเสธการเข้าถึงอุปกรณ์เครือข่ายจากคอมพิวเตอร์ของคุณ และทำสิ่งอื่นๆ ได้ตามการกำหนดค่า ตามค่าเริ่มต้น ESET Endpoint Security จะมีกฎของไฟร์วอลล์ที่กำหนดค่าไว้ล่วงหน้าและการป้องกันการเข้าถึงเครือข่ายเพื่อความปลอดภัยสูงสุด อย่างไรก็ตาม ในบางสภาพแวดล้อมการทำงานอาจต้องใช้การกำหนดค่าแบบกำหนดเอง การเปลี่ยนการตั้งค่าเริ่มต้นควรดำเนินการโดยผู้ใช้ที่มีประสบการณ์เท่านั้น



คุณสามารถกำหนดการตั้งค่าต่อไปนี้ได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** (คลิกลิงก์ด้านล่างเพื่อดูคำอธิบายโดยละเอียดของแต่ละตัวเลือกการป้องกันการเข้าถึงเครือข่าย):

การป้องกันการเข้าถึงเครือข่าย

โปรไฟล์การเชื่อมต่อเครือข่าย – สามารถใช้ส่วนกำหนดค่าเพื่อควบคุมการป้องกันการเข้าถึงเครือข่าย และไฟร์วอลล์สำหรับการเชื่อมต่อเครือข่ายที่เฉพาะเจาะจงได้

ชุด IP – คุณสามารถกำหนดคอลเลกชันที่อยู่ IP ที่สร้างกลุ่มที่อยู่ IP เชิงตรรกะหนึ่งกลุ่ม ซึ่งสามารถใช้สำหรับกฎของไฟร์วอลล์ และกฎ การป้องกันการโจมตีแบบ Brute-Force ได้

ไฟร์วอลล์

การป้องกันการโจมตีเครือข่าย

โปรไฟล์การเชื่อมต่อเครือข่าย

คุณสามารถใช้โปรไฟล์เพื่อควบคุมการป้องกันเครือข่ายของ ESET Endpoint Security สำหรับ การเชื่อมต่อเครือข่าย ที่ต้องการได้ เมื่อสร้างหรือแก้ไข กฎของไฟร์วอลล์, กฎ IDS หรือ กฎการป้องกันการโจมตีแบบ Brute-Force คุณสามารถกำหนดกฎเหล่านี้ให้มีผลใช้กับโปรไฟล์ที่ต้องการหรือกับโปรไฟล์ทั้งหมดได้ เมื่อมีโปรไฟล์ทำงานในการเชื่อมต่อเครือข่าย โปรไฟล์จะใช้เฉพาะกฎร่วม (กฎที่ไม่ระบุโปรไฟล์) และกฎที่กำหนดไปที่โปรไฟล์นั้นเท่านั้น คุณสามารถสร้างโปรไฟล์หลายรายการซึ่งกำหนดกฎแตกต่างกันไปยังการเชื่อมต่อเครือข่าย เพื่อแก้ไขการทำงานของไฟร์วอลล์ได้อย่างง่ายดาย

คุณสามารถกำหนดค่าโปรไฟล์การเชื่อมต่อเครือข่ายและการกำหนดได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **การป้องกันการเข้าถึงเครือข่าย**

การกำหนดโปรไฟล์การเชื่อมต่อเครือข่าย – ช่วยให้คุณสามารถเลือกได้ว่าจะให้ระบบกำหนดโปรไฟล์ที่กำหนดไว้ล่วงหน้าหรือโปรไฟล์แบบกำหนดเองให้กับการเชื่อมต่อเครือข่ายที่เพิ่งค้นพบโดยอัตโนมัติ (เลือก **อัตโนมัติ** จากเมนูแบบเลื่อนลง) ตาม ตัวเปิดใช้งาน ที่กำหนดค่าไว้ในโปรไฟล์การเชื่อมต่อเครือข่าย หรือให้ระบบถาม (เลือก **ถาม** จากเมนูแบบเลื่อนลง) เมื่อคุณต้องการ กำหนดค่าการป้องกันเครือข่าย และกำหนดโปรไฟล์ด้วยตนเองทุกครั้งที่ตรวจพบการเชื่อมต่อเครือข่ายใหม่

คุณยังสามารถกำหนดโปรไฟล์การเชื่อมต่อเครือข่ายแบบเฉพาะเจาะจงได้ด้วยตนเองใน หน้าต่างโปรแกรมหลัก > **การตั้งค่า** > **เครือข่าย** > **การเชื่อมต่อเครือข่าย** วางเมาส์เหนือการเชื่อมต่อเครือข่ายที่ต้องการและคลิกไอคอนเมนู ⋮ > **แก้ไข** เพื่อเปิดหน้าต่าง กำหนดค่าการป้องกันเครือข่าย และเลือกโปรไฟล์

โปรไฟล์การเชื่อมต่อเครือข่าย – คลิก **แก้ไข** เพื่อ เพิ่มหรือแก้ไขโปรไฟล์การเชื่อมต่อเครือข่าย

โปรไฟล์ต่อไปนี้จะถูกกำหนดไว้ล่วงหน้า และไม่สามารถแก้ไข/ลบได้:

ส่วนตัว – สำหรับเครือข่ายที่เชื่อถือได้ (เครือข่ายในบ้านหรือที่ทำงาน) ผู้ใช้เครือข่ายรายอื่นสามารถมองเห็นคอมพิวเตอร์และไฟล์ที่ใช้ร่วมกันที่เก็บไว้ในคอมพิวเตอร์ของคุณได้ และผู้ใช้รายอื่นบนเครือข่ายสามารถเข้าถึง

ทรัพยากรระบบได้ (เปิดใช้งานการเข้าถึงไฟล์ที่แชร์และเครื่องพิมพ์ การติดต่อสื่อสาร RPC ขาเข้า และการแชร์ผ่านเดสก์ท็อปจากระยะไกล) เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าถึงเครือข่ายภายในที่ปลอดภัย ระบบจะกำหนดโปรไฟล์นี้ไปยังการเชื่อมต่อเครือข่ายโดยอัตโนมัติหากมีการกำหนดค่าเป็น "โดเมน" หรือเครือข่าย "ส่วนตัว" ใน Windows

สาธารณะ – สำหรับเครือข่ายที่ไม่เชื่อถือ (เครือข่ายสาธารณะ) ไฟล์และโฟลเดอร์ในระบบของคุณจะไม่ถูกใช้ร่วมกันหรือมองเห็นได้สำหรับผู้ใช้รายอื่นบนเครือข่าย และการแบ่งปันทรัพยากรระบบจะถูกปิดใช้งาน เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าสู่เครือข่ายไร้สาย ระบบจะกำหนดโปรไฟล์นี้ไปยังการเชื่อมต่อเครือข่ายโดยอัตโนมัติหากมีการกำหนดค่าเป็น "โดเมน" หรือเครือข่าย "ส่วนตัว" ใน Windows

เมื่อการเชื่อมต่อเครือข่ายเปลี่ยนไปใช้โปรไฟล์อื่น การแจ้งเตือนจะปรากฏขึ้นที่มุมขวาล่างของหน้าจอ

เพิ่มหรือแก้ไขโปรไฟล์การเชื่อมต่อเครือข่าย

คุณสามารถเพิ่มหรือแก้ไข โปรไฟล์การเชื่อมต่อเครือข่าย ได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **การป้องกันการเข้าถึงเครือข่าย** > **โปรไฟล์การเชื่อมต่อเครือข่าย** > **แก้ไข** หากต้องการแก้ไขโปรไฟล์ ให้คุณเลือกโปรไฟล์จากรายการหน้าต่าง **โปรไฟล์การเชื่อมต่อเครือข่าย**

โปรไฟล์ต่อไปนี้จะถูกกำหนดไว้ล่วงหน้า และไม่สามารถแก้ไข/ลบได้:

ส่วนตัว – สำหรับเครือข่ายที่เชื่อถือได้ (เครือข่ายในบ้านหรือที่ทำงาน) ผู้ใช้เครือข่ายรายอื่นสามารถมองเห็นคอมพิวเตอร์และไฟล์ที่ใช้ร่วมกันที่เก็บไว้ในคอมพิวเตอร์ของคุณได้ และผู้ใช้รายอื่นบนเครือข่ายสามารถเข้าถึงทรัพยากรระบบได้ (เปิดใช้งานการเข้าถึงไฟล์ที่แชร์และเครื่องพิมพ์ การติดต่อสื่อสาร RPC ขาเข้า และการแชร์ผ่านเดสก์ท็อปจากระยะไกล) เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าถึงเครือข่ายภายในที่ปลอดภัย ระบบจะกำหนดโปรไฟล์นี้ไปยังการเชื่อมต่อเครือข่ายโดยอัตโนมัติหากมีการกำหนดค่าเป็น "โดเมน" หรือเครือข่าย "ส่วนตัว" ใน Windows

สาธารณะ – สำหรับเครือข่ายที่ไม่เชื่อถือ (เครือข่ายสาธารณะ) ไฟล์และโฟลเดอร์ในระบบของคุณจะไม่ถูกใช้ร่วมกันหรือมองเห็นได้สำหรับผู้ใช้รายอื่นบนเครือข่าย และการแบ่งปันทรัพยากรระบบจะถูกปิดใช้งาน เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าสู่เครือข่ายไร้สาย ระบบจะกำหนดโปรไฟล์นี้ไปยังการเชื่อมต่อเครือข่ายโดยอัตโนมัติหากมีการกำหนดค่าเป็น "โดเมน" หรือเครือข่าย "ส่วนตัว" ใน Windows

บนสุด/ขึ้น/ลง/ล่างสุด  – ช่วยให้คุณปรับระดับความสำคัญของโปรไฟล์การเชื่อมต่อเครือข่ายได้ (โปรไฟล์การเชื่อมต่อเครือข่ายจะได้รับการประเมินและนำไปใช้โดยลำดับความสำคัญ โดยจะนำโปรไฟล์ที่ตรงกันครั้งแรกมาใช้เสมอ)

เพิ่มหรือแก้ไขโปรไฟล์

โปรไฟล์การเชื่อมต่อเครือข่ายแบบกำหนดเองช่วยให้คุณนำกฎของไฟร์วอลล์ และกฎการป้องกันการโจมตีแบบ Brute-Force ไปใช้ รวมถึงกำหนดการตั้งค่าเพิ่มเติมสำหรับการเชื่อมต่อเครือข่ายที่เฉพาะเจาะจงได้ คุณระบุว่าจะกำหนดโปรไฟล์ที่กำหนดเองไปยังการเชื่อมต่อเครือข่ายใดได้ในส่วน ตัวเปิดใช้งาน

หากต้องการต้องการเปิดเครื่องมือแก้ไขโปรไฟล์ ในหน้าต่าง **โปรไฟล์การเชื่อมต่อเครือข่าย** ให้ทำดังนี้:

- คลิก **เพิ่ม**
- เลือกโปรไฟล์ที่มีอยู่ และคลิก **แก้ไข**
- เลือกโปรไฟล์ที่มีอยู่ และคลิก **คัดลอก**

ชื่อ – ชื่อที่กำหนดเองสำหรับโปรไฟล์ของคุณ

คำอธิบาย – คำอธิบายของโปรไฟล์เพื่อช่วยระบุโปรไฟล์

ที่อยู่ที่เชื่อถือได้เพิ่มเติม – ที่อยู่ที่กำหนดในส่วนนี้จะเพิ่มลงในโซนที่เชื่อถือได้ของการเชื่อมต่อเครือข่ายที่ใช้โปรไฟล์นี้ (โดยไม่คำนึงถึงประเภทการป้องกันของเครือข่าย)

การเชื่อมต่อที่เชื่อถือได้ – ผู้ใช้เครือข่ายรายอื่นสามารถมองเห็นคอมพิวเตอร์และไฟล์ที่ใช้ร่วมกันที่เก็บไว้ในคอมพิวเตอร์ของคุณได้ และผู้ใช้รายอื่นบนเครือข่ายสามารถเข้าถึงทรัพยากรระบบได้ (เปิดใช้งานการเข้าถึงไฟล์ที่แชร์และเครื่องพิมพ์ การติดต่อสื่อสาร RPC ขาเข้า และการแชร์ผ่านเดสก์ท็อปจากระยะไกล) เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อสร้างโปรไฟล์สำหรับการเชื่อมต่อเครือข่ายท้องถิ่นที่ปลอดภัย ระบบจะถือว่าซับเน็ตเครือข่ายที่เชื่อมต่อโดยตรงทั้งหมดเชื่อถือได้ ตัวอย่างเช่น หากอะแดปเตอร์เครือข่ายเชื่อมต่อกับเครือข่ายนี้ด้วยที่อยู่ IP 192.168.1.5 และซับเน็ตมาสก์ 255.255.255.0 ซับเน็ต 192.168.1.0/24 จะเพิ่มไปยังโซนที่เชื่อถือได้ของการเชื่อมเครือข่ายนั้น หากอแดปเตอร์มีที่อยู่/ซับเน็ตที่เพิ่มเข้ามา ที่อยู่/ซับเน็ตทั้งหมดจะเชื่อถือได้

รายงานการเข้ารหัส WiFi ที่มีการป้องกันต่ำ – ESET Endpoint Security จะส่ง การแจ้งเตือนผ่านเดสก์ท็อป ให้คุณเมื่อเชื่อมต่อเครือข่ายแบบไร้สายที่ไม่ได้รับการป้องกันหรือมีการป้องกันต่ำ

ตัวเปิดใช้งาน เงื่อนไขที่กำหนดเองซึ่งต้องปฏิบัติตามเพื่อกำหนดโปรไฟล์การเชื่อมต่อเครือข่ายนี้ให้กับการเชื่อมต่อเครือข่าย ดูคำอธิบายโดยละเอียดได้ที่ ตัวเปิดใช้งาน

ตัวเปิดใช้งาน

ตัวเปิดใช้งานคือเงื่อนไขที่กำหนดเองซึ่งต้องปฏิบัติตามเพื่อกำหนด โปรไฟล์การเชื่อมต่อเครือข่าย ไปยัง การเชื่อมต่อเครือข่าย หากเครือข่ายที่เชื่อมต่อมีแอตทริบิวต์เดียวกับที่กำหนดไว้ในตัวเปิดใช้งานสำหรับโปรไฟล์เครือข่ายที่เชื่อมต่อ ระบบจะใช้โปรไฟล์นั้นกับเครือข่าย โปรไฟล์การเชื่อมต่อเครือข่ายสามารถมีตัวเปิดใช้งานได้มากกว่าหนึ่งโปรไฟล์ หากมีตัวเปิดใช้งานหลายตัว ตรรกะ OR จะมีผลใช้ (จะต้องเป็นไปตามอย่างน้อยหนึ่งเงื่อนไข) คุณสามารถกำหนดตัวเปิดใช้งานได้ใน เครื่องมือแก้ไขโปรไฟล์การเชื่อมต่อเครือข่าย การสร้างโปรไฟล์การเชื่อมต่อเครือข่ายแบบกำหนดเองควรดำเนินการโดยผู้ใช้ที่มีประสบการณ์

ตัวเปิดใช้งานจะมีดังต่อไปนี้ (หากคุณต้องการทราบรายละเอียดเครือข่ายที่คุณเชื่อมต่ออยู่ โปรดดูที่ การเชื่อมต่อเครือข่าย):

อะแดปเตอร์:

ชนิดอะแดปเตอร์ – ใช้โปรไฟล์หากมีการสร้างการเชื่อมต่อเครือข่ายบนอแดปเตอร์ที่เลือก
ชื่ออะแดปเตอร์ – ใช้โปรไฟล์หากชื่ออะแดปเตอร์เครือข่ายตรงกัน
IP ของอะแดปเตอร์ – ใช้โปรไฟล์หากที่อยู่ IP ของอะแดปเตอร์เครือข่ายตรงกัน

DNS

ส่วนต่อท้าย DNS – ใช้โปรไฟล์หากชื่อโดเมนตรงกัน
DNS IP — ใช้โปรไฟล์หากที่อยู่ IP ของเซิร์ฟเวอร์ DNS ตรงกัน

WINS

ใช้โปรไฟล์ถ้าที่อยู่ IP Windows Internet Name Service (WINS) ที่แมปไว้ตรงกัน

DHCP

DHCP IP – จับคู่ที่อยู่ IP ของเซิร์ฟเวอร์ DHCP

เกตเวย์เริ่มต้น

IP – ใช้โปรไฟล์หากที่อยู่ IP ของเกตเวย์เริ่มต้นตรงกัน
ที่อยู่ MAC – ใช้โปรไฟล์หากที่อยู่ MAC ของเกตเวย์เริ่มต้นตรงกัน

Wi-Fi

SSID – ใช้โปรไฟล์หาก SSID (ชื่อ Wi-Fi) ตรงกัน
ชื่อโปรไฟล์ – ใช้โปรไฟล์หากชื่อโปรไฟล์ Wi-Fi ตรงกัน
ประเภทความปลอดภัย – ใช้โปรไฟล์หากประเภทความปลอดภัยตรงกับประเภทที่เลือกจากเมนูแบบเลื่อนลง (ถ้าคุณต้องการจับคู่ตัวเปิดใช้งานมากกว่าหนึ่งตัวให้สร้าง ตัวเปิดใช้งานอื่น)
ประเภทการเข้ารหัส – ใช้โปรไฟล์หากประเภทการเข้ารหัสตรงกับประเภทที่เลือกจากเมนูแบบเลื่อนลง (ถ้าคุณต้องการจับคู่ตัวเปิดใช้งานมากกว่าหนึ่งตัวให้สร้าง ตัวเปิดใช้งานอื่น)
ความปลอดภัยของเครือข่าย – ใช้โปรไฟล์หากเครือข่ายเป็น **เปิด/แบบปลอดภัย**

โปรไฟล์ Windows

ใช้โปรไฟล์ถ้ามีการกำหนดค่าเครือข่ายใน Windows เป็น **โดเมน/ส่วนตัว/สาธารณะ**

ตรวจสอบสิทธิ์

การตรวจสอบสิทธิ์ของเครือข่ายจะค้นหาเซิร์ฟเวอร์ที่ต้องการในเครือข่าย และใช้การเข้ารหัสแบบไม่สมมาตร (RSA) เพื่อตรวจสอบสิทธิ์เซิร์ฟเวอร์นั้น ชื่อเครือข่ายที่ได้รับการตรวจสอบสิทธิ์ต้องตรงกับชื่อที่ตั้งไว้ในการตั้งค่าเซิร์ฟเวอร์การตรวจสอบสิทธิ์ ชื่อต้องตรงตามตัวพิมพ์เล็กและใหญ่ ชื่อเซิร์ฟเวอร์สามารถพิมพ์เป็นที่อยู่ IP, DNS หรือชื่อ NetBIOS ก็ได้
ดาวน์โหลดเซิร์ฟเวอร์การตรวจสอบสิทธิ์ของ ESET.
สามารถนำเข้าคีย์สาธารณะโดยใช้ไฟล์ประเภทใดก็ได้ดังต่อไปนี้:
• คีย์สาธารณะที่เข้ารหัส PEM (.pem) ซึ่งคุณสามารถสร้างคีย์นี้โดยใช้เซิร์ฟเวอร์การตรวจสอบสิทธิ์ของ ESET
• รหัสสาธารณะที่เข้ารหัส
• ใบรับรองรหัสสาธารณะ (.crt)
คลิก **ทดสอบ** เพื่อทดสอบการตั้งค่าของคุณ หากการตรวจสอบสิทธิ์เสร็จสมบูรณ์ ข้อความ การตรวจสอบสิทธิ์ของเซิร์ฟเวอร์เสร็จสมบูรณ์ จะปรากฏขึ้น ถ้าไม่กำหนดค่าการตรวจสอบสิทธิ์อย่างถูกต้อง ข้อความแสดงข้อผิดพลาดต่อไปนี้จะปรากฏ:
การตรวจสอบสิทธิ์ของเซิร์ฟเวอร์ล้มเหลว ลายเซ็นไม่ถูกต้องหรือไม่ตรงกัน
ลายเซ็นเซิร์ฟเวอร์ไม่ตรงกับคีย์สาธารณะที่ป้อน
การตรวจสอบสิทธิ์ของเซิร์ฟเวอร์ล้มเหลว ชื่อเครือข่ายไม่ตรงกัน
ชื่อเครือข่ายที่กำหนดค่าไว้ไม่ตรงกับชื่อเครือข่ายของเซิร์ฟเวอร์การตรวจสอบสิทธิ์ โปรดตรวจสอบชื่อทั้งสองเพื่อให้แน่ใจว่าเหมือนกัน
การตรวจสอบสิทธิ์ของเซิร์ฟเวอร์ล้มเหลว การตอบรับจากเซิร์ฟเวอร์ไม่ถูกต้องหรือไม่มีการตอบรับ
ไม่ได้รับการตอบกลับถ้าเซิร์ฟเวอร์ไม่ทำงานหรือไม่สามารถเข้าถึงได้ อาจได้รับการตอบกลับที่ไม่ถูกต้องถ้าชื่อเซิร์ฟเวอร์ HTTP อื่นทำงานในที่อยู่ที่ระบุ
ป้อนคีย์สาธารณะไม่ถูกต้อง
ยืนยันว่าไฟล์ของรหัสสาธารณะที่คุณป้อนไม่เสียหาย

ชุด IP

ชุด IP คือชุดของที่อยู่ IP ที่สร้างกลุ่มเชิงตรรกะของที่อยู่ IP หนึ่งกลุ่ม ซึ่งมีประโยชน์เมื่อนำชุดที่อยู่เดียวกันมาใช้ซ้ำใน กฎของไฟร์วอลล์ หลายกฎหรือ กฎการป้องกันการโจมตีแบบ Brute-Force นอกจากนี้ ESET Endpoint Security ยังมีชุด IP ที่กำหนดไว้ล่วงหน้าซึ่งมีการใช้กฎภายในด้วย ตัวอย่างหนึ่งของกลุ่มดังกล่าวคือ **โซนที่เชื่อถือ** โซนที่เชื่อถือได้หมายถึงกลุ่มที่อยู่เครือข่ายซึ่งผู้ใช้เครือข่ายรายอื่นสามารถมองเห็นคอมพิวเตอร์และไฟล์ที่ใช้ร่วมกันที่เก็บไว้ในคอมพิวเตอร์ของคุณได้ และผู้ใช้รายอื่นบนเครือข่ายสามารถเข้าถึงทรัพยากรระบบได้

หากต้องการเพิ่มชุด IP ให้ทำดังนี้:

1. เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **ชุด IP** > **แก้ไข**
2. คลิก **เพิ่ม** พิมพ์ **ชื่อ** และ **คำอธิบาย** สำหรับโซน และพิมพ์ที่อยู่ IP ระยะไกลใน **ที่อยู่คอมพิวเตอร์ระยะไกล (IPv4/IPv6, ช่วง, มาสก์)**
3. คลิก**ตกลง**

ดูข้อมูลเพิ่มเติมได้ที่ แก้ไขชุด IP

แก้ไขชุด IP

ดูข้อมูลเพิ่มเติมเกี่ยวกับชุด IP ได้ที่ ชุด IP

คอลัมน์

ชื่อ – ชื่อกลุ่มของคอมพิวเตอร์ระยะไกล

คำอธิบาย - คำอธิบายทั่วไปของกลุ่ม

ที่อยู่ IP – ที่อยู่ IP ระยะไกลที่อยู่ในชุด IP

องค์ประกอบการควบคุม

เมื่อคุณ **เพิ่ม** หรือ **แก้ไข** โซน ช่องต่อไปนี้จะสามารถใช้งานได้:

ชื่อ – ชื่อกลุ่มของคอมพิวเตอร์ระยะไกล

คำอธิบาย - คำอธิบายทั่วไปของกลุ่ม

ที่อยู่คอมพิวเตอร์ระยะไกล (IPv4, IPv6, ระยะ, มาส์ก) – อนุญาตให้คุณเพิ่มที่อยู่ระยะไกล ช่วงที่อยู่ หรือซับเน็ต

ลบ - ลบโซนออกจากรายการ

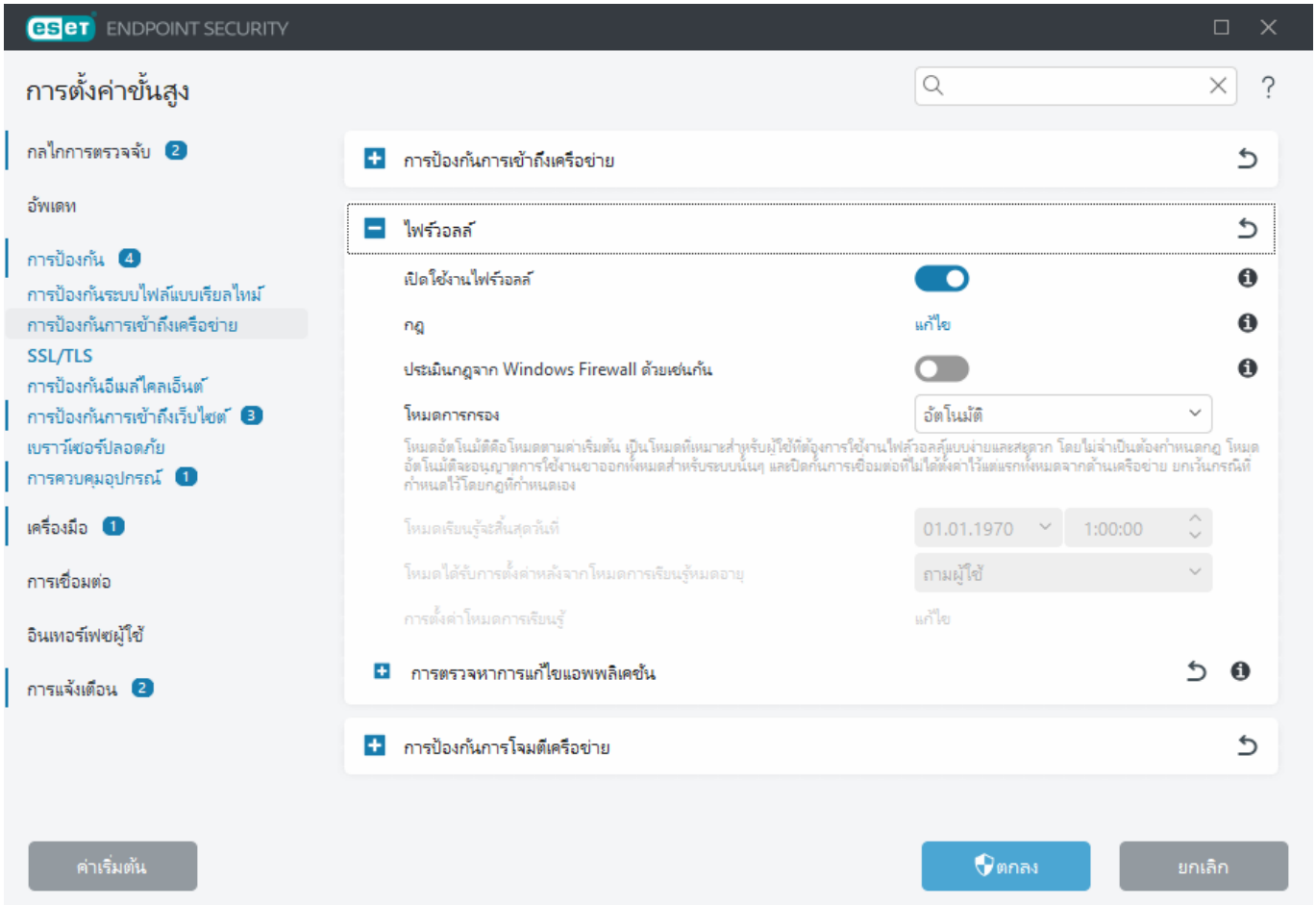
ไม่สามารถลบชุด IP ที่กำหนดไว้ล่วงหน้าได้

ตัวอย่างที่อยู่ IP
เพิ่มที่อยู่ IPv4:
ที่อยู่เดี่ยว – เพิ่มที่อยู่ IP ของคอมพิวเตอร์แต่ละเครื่อง (ตัวอย่างเช่น *192.168.0.10*)
ช่วงที่อยู่ – ป้อนที่อยู่ IP แรกและสุดท้ายเพื่อระบุช่วง IP ของคอมพิวเตอร์หลายเครื่อง (ตัวอย่างเช่น *192.168.0.1-192.168.0.99*)
ซับเน็ต - ซับเน็ต (กลุ่มของคอมพิวเตอร์) กำหนดโดยที่อยู่ IP และมาสก์ ตัวอย่างเช่น 255.255.255.0 เป็นมาสก์เครือข่ายสำหรับซับเน็ต 192.168.1.0 เพื่อแยกประเภทซับเน็ตทั้งหมดใน *192.168.1.0/24*
เพิ่มที่อยู่ IPv6:
ที่อยู่เดี่ยว – เพิ่มที่อยู่ IP ของคอมพิวเตอร์แต่ละเครื่อง (ตัวอย่างเช่น *2001:718:1c01:16:214:22ff:fec9:ca5*):
ซับเน็ต - ซับเน็ต (กลุ่มของคอมพิวเตอร์) กำหนดโดยที่อยู่ IP และมาสก์ (ตัวอย่างเช่น: *2002:c0a8:6301:1::1/64*)

ไฟร์วอลล์

ไฟร์วอลล์จะควบคุมการรับส่งข้อมูลเครือข่ายขาเข้าและขาออกทั้งหมดบนคอมพิวเตอร์ของคุณ โดยยึดตามกฎภายในและกฎที่คุณกำหนด ซึ่งจะทำงานด้วยการอนุญาตหรือปฏิเสธการเชื่อมต่อเครือข่ายแต่ละแห่ง ไฟร์วอลล์จะให้การป้องกันการโจมตีจากอุปกรณ์ระยะไกลและสามารถบล็อกบริการบางอย่างที่เป็นภัยคุกคามได้

หากต้องการกำหนดค่าไฟร์วอลล์ ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **ไฟร์วอลล์**



ไฟร์วอลล์

เปิดใช้งานไฟร์วอลล์

เราขอแนะนำให้คุณเปิดคุณลักษณะนี้ไว้เพื่อให้แน่ใจว่าระบบของคุณจะปลอดภัยอยู่เสมอ เมื่อเปิดใช้งานไฟร์วอลล์ การรับส่งข้อมูลเครือข่ายจะถูกสแกนทั้งสองฝั่ง

กฎ

การตั้งค่ากฎจะอนุญาตให้คุณ ดูและแก้ไขกฎของไฟร์วอลล์ทั้งหมด ที่มีผลใช้กับการรับส่งข้อมูลที่สร้างโดยแอพพลิเคชันแต่ละรายการภายในโซนที่เชื่อถือได้และอินเทอร์เน็ต

กฎจากไฟร์วอลล์ Windows ที่กำหนดค่าโดยใช้ Group Policy (GPO) จะไม่ได้รับการประเมิน

คุณสามารถสร้างกฎ IDS เมื่อ บอทเน็ต โจมตีคอมพิวเตอร์ของคุณได้ โดยคุณสามารถแก้ไขกฎได้โดยไปที่ การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันเครือข่าย** > **การป้องกันการโจมตีเครือข่าย** > **กฎ IDS** และคลิกที่ **แก้ไข**

ประเมินกฎจาก Windows Firewall ด้วยเช่นกัน

ในโหมดการกรองอัตโนมัติ การรับส่งข้อมูลขาเข้าที่ได้รับอนุญาตตามกฎไฟร์วอลล์ของ Windows จะได้รับการประเมินและประมวลผล เว้นแต่จะถูกบล็อกโดยกฎของ ESET อย่างชัดเจน

โหมดการกรอง

การทำงานของไฟร์วอลล์เปลี่ยนแปลงโดยขึ้นอยู่กับโหมดการกรอง โหมดการกรองจะมีผลกับระดับการโต้ตอบของผู้ใช้ที่ต้องการด้วย

การทำงานของไฟร์วอลล์เปลี่ยนแปลงโดยขึ้นอยู่กับโหมดการกรอง โหมดการกรองจะมีผลกับระดับการโต้ตอบของผู้ใช้ที่ต้องการด้วย โหมดการกรองต่อไปนี้มีให้ใช้งานได้สำหรับไฟร์วอลล์ของ ESET Endpoint Security:

โหมดการกรอง	คำอธิบาย
โหมดอัตโนมัติ	โหมดเริ่มต้น โหมดนี้เหมาะสำหรับผู้ใช้ที่ต้องการการใช้งานไฟร์วอลล์ที่สะดวกและง่ายดาย โดยไม่จำเป็นต้องกำหนดกฎ กฎที่กำหนดเองและกำหนดโดยผู้ใช้นั้นสามารถสร้างได้ แต่ไม่จำเป็นต้องใช้ใน **โหมดอัตโนมัติ** โหมดอัตโนมัติจะอนุญาตการรับส่งข้อมูลขาออกทั้งหมดสำหรับระบบและปิดกั้นการรับส่งข้อมูลขาเข้าส่วนใหญ่ไว้โดยจะยกเว้นการรับส่งข้อมูลบางอย่างจากโซนที่เชื่อถือ (ดังที่ระบุไว้ใน IDS และตัวเลือกขั้นสูง/บริการที่อนุญาต) และตอบสนองต่อการสื่อสารขาออกล่าสุด
โหมดโต้ตอบ	อนุญาตให้คุณสร้างการกำหนดค่าที่กำหนดเองสำหรับไฟร์วอลล์ เมื่อตรวจพบการสื่อสารและไม่มีกฎที่ใช้กับการสื่อสารนั้น หน้าต่างข้อความที่รายงานการเชื่อมต่อที่ไม่รู้จักจะปรากฏ หน้าต่างข้อความจะมีตัวเลือกให้อนุญาตหรือปฏิเสธการเชื่อมต่อ และสามารถบันทึกสิ่งที่คุณเลือกเพื่อใช้เป็นกฎใหม่สำหรับไฟร์วอลล์ได้ ถ้าคุณเลือกที่จะสร้างกฎใหม่ การเชื่อมต่อประเภทนี้หลังจากนั้นทั้งหมดจะได้รับการอนุญาตหรือถูกปิดกั้นตามกฎนั้น
โหมดนโยบาย	ปิดกั้นการเชื่อมต่อทั้งหมดที่ไม่ได้ระบุตามกฎเฉพาะที่อนุญาตไว้ โหมดนี้อนุญาตให้ผู้ใช้ขั้นสูงกำหนดกฎที่ใช้ได้เฉพาะการเชื่อมต่อที่ต้องการและมีการรักษาความปลอดภัย การเชื่อมต่ออื่นๆ ที่ไม่ได้ระบุไว้ทั้งหมดจะถูกปิดกั้นโดยไฟร์วอลล์
โหมดเรียนรู้	สร้างและบันทึกกฎโดยอัตโนมัติ โหมดนี้เหมาะสำหรับการกำหนดค่าเริ่มต้นของไฟร์วอลล์ แต่ไม่ควรเปิดไว้เป็นเวลานาน ผู้ใช้ไม่จำเป็นต้องดำเนินการใดๆ เนื่องจาก ESET Endpoint Security จะบันทึกกฎตามพารามิเตอร์ที่กำหนดไว้ล่วงหน้า ควรใช้โหมดการเรียนรู้จนกว่ากฎทั้งหมดสำหรับการสื่อสารที่จำเป็นจะถูกสร้างขึ้นเพื่อป้องกันความเสี่ยงด้านความปลอดภัย

โหมดการเรียนรู้จะสิ้นสุดที่ – ตั้งค่าวันที่และเวลาเมื่อโหมดการเรียนรู้สิ้นสุดลงโดยอัตโนมัติ คุณยังสามารถปิดโหมดการเรียนรู้ด้วยตนเองเมื่อใดก็ได้

โหมดที่ได้รับการตั้งค่าหลังจากโหมดการเรียนรู้หมดอายุ – ระบุโหมดการกรองที่ไฟร์วอลล์ของ จะแปลงไปยังช่วงเวลาหลังจากโหมดการเรียนรู้สิ้นสุด อ่านเพิ่มเติมเกี่ยวกับโหมดการกรองได้ที่ตารางด้านบน หลังจากเสร็จสิ้นตัวเลือก **ถามผู้ใช้** จะต้องใช้สิทธิ์อนุญาตของผู้ดูแลระบบเพื่อทำการเปลี่ยนแปลงโหมดการกรองไฟร์วอลล์

การตั้งค่าโหมดการเรียนรู้ – คลิก **แก้ไข** เพื่อกำหนดค่าพารามิเตอร์สำหรับการบันทึกกฎที่สร้างในโหมดการเรียนรู้

การตรวจหาการแก้ไขแอพพลิเคชัน

คุณสมบัติการตรวจหาการแก้ไขแอพพลิเคชัน จะแสดงการแจ้งเตือนหากมีแอพพลิเคชันที่ถูกแก้ไขซึ่งมีกฎไฟร์วอลล์พยายามเริ่มต้นการเชื่อมต่อ

การตั้งค่าโหมดการเรียนรู้

โหมดเรียนรู้จะสร้างและบันทึกกฎของการสื่อสารแต่ละรายการที่สร้างขึ้นในระบบโดยอัตโนมัติ ผู้ใช้ไม่จำเป็นต้องดำเนินการใดๆ เนื่องจาก ESET Endpoint Security จะบันทึกกฎตามพารามิเตอร์ที่กำหนดไว้ล่วงหน้า

โหมดนี้สามารถก่อให้เกิดความเสี่ยงต่อระบบของคุณได้ และโหมดนี้แนะนำให้ใช้เพื่อการกำหนดค่าเริ่มต้นของไฟร์วอลล์เท่านั้น

เลือก **การเรียนรู้** จากเมนูแบบเลื่อนลงใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **ไฟร์วอลล์** > **ไฟร์วอลล์** > **โหมดการกรอง** เพื่อเปิดใช้งานตัวเลือกโหมดการเรียนรู้ คลิก **แก้ไข** ถัดจาก **การตั้งค่าโหมดการเรียนรู้** เพื่อกำหนดค่าตัวเลือกต่อไปนี้:

> ขณะที่อยู่ในโหมดการเรียนรู้ ไฟร์วอลล์จะไม่กรองการสื่อสาร โดยจะอนุญาตการสื่อสารขาเข้าและขาออกทั้งหมด ในโหมดนี้ คอมพิวเตอร์ของคุณจะไม่ได้รับการป้องกันโดยไฟร์วอลล์อย่างเต็มที่

การรับส่งขาเข้าจากโซนที่เชื่อถือ ตัวอย่างของการเชื่อมต่อขาเข้าภายในโซนที่เชื่อถือจะเป็นอุปกรณ์ระยะไกลจากภายในโซนที่เชื่อถือ ซึ่งพยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันในระบบที่ทำงานบนคอมพิวเตอร์ของคุณ

การรับส่งขาออกไปยังโซนที่เชื่อถือ แอพพลิเคชันในระบบที่พยายามสร้างการเชื่อมต่อกับอุปกรณ์เครื่องอื่นภายในเครือข่ายในระบบ หรือภายในเครือข่ายในโซนที่เชื่อถือ

การรับส่งทางอินเทอร์เน็ตขาเข้า อุปกรณ์ระยะไกลที่พยายามสื่อสารกับแอพพลิเคชันที่ทำงานบนคอมพิวเตอร์

การรับส่งทางอินเทอร์เน็ตขาออก แอพพลิเคชันในระบบที่พยายามสร้างการเชื่อมต่อกับอุปกรณ์เครื่องอื่น

แต่ละส่วนอนุญาตให้คุณระบุพารามิเตอร์ที่จะเพิ่มไปยังกฎสร้างใหม่:

เพิ่มพอร์ตในระบบ – รวมเลขที่พอร์ตในระบบของการสื่อสารในเครือข่าย สำหรับการสื่อสารขาออก โดยทั่วไป ระบบจะสร้างเลขที่แบบสุ่ม ด้วยเหตุผลนี้ เราขอแนะนำให้เปิดใช้ตัวเลือกนี้เฉพาะสำหรับการสื่อสารขาเข้าเท่านั้น

เพิ่มแอพพลิเคชัน – รวมชื่อของแอพพลิเคชันในระบบ ตัวเลือกนี้เหมาะสำหรับกฎในระดับแอพพลิเคชันในอนาคต (กฎที่กำหนดการสื่อสารสำหรับแอพพลิเคชันทั้งหมด) ตัวอย่างเช่น คุณสามารถเปิดใช้การสื่อสารเฉพาะสำหรับเว็บเบราว์เซอร์หรืออีเมลไคลเอ็นต์

เพิ่มพอร์ตระยะไกล – รวมเลขที่พอร์ตระยะไกลของการสื่อสารในเครือข่าย ตัวอย่างเช่น คุณสามารถอนุญาตหรือปฏิเสธบริการเฉพาะที่เชื่อมโยงกับเลขที่พอร์ตมาตรฐาน (HTTP – 80, POP3 – 110 เป็นต้น)

เพิ่มที่อยู่ IP / โซนที่เชื่อถือระยะไกล – ที่อยู่ IP หรือโซนระยะไกลสามารถใช้เป็นพารามิเตอร์สำหรับกฎใหม่ ซึ่งกำหนดการเชื่อมต่อในเครือข่ายทั้งหมดระหว่างระบบภายในและที่อยู่/โซนระยะไกล ตัวเลือกนี้เหมาะสำหรับกรณีที่คุณต้องการกำหนดการทำงานการสำหรับอุปกรณ์บางเครื่องหรือกลุ่มของอุปกรณ์ในเครือข่าย

จำนวนกฎสูงสุดสำหรับแอพพลิเคชัน – ถ้าแอพพลิเคชันสื่อสารผ่านหลายพอร์ตไปยังที่อยู่ IP ต่างๆ เป็นต้น ไฟร์วอลล์ในโหมดเรียนรู้จะสร้างจำนวนกฎที่เหมาะสมสำหรับแอพพลิเคชันนี้ ตัวเลือกนี้อนุญาตให้คุณจำกัดจำนวนกฎที่สามารถสร้างได้สำหรับแอพพลิเคชันหนึ่ง

หน้าต่างข้อความ - สิ้นสุดโหมดเรียนรู้

เมื่อถึงระยะเวลาการใช้งานของโหมดการเรียนรู้ คุณจะได้รับข้อความให้สลับไปยังโหมดการกรองแบบ **โต้ตอบ** หรือ **ตามนโยบาย** เมื่อไฟร์วอลล์อยู่ในโหมดเรียนรู้ จะมีการสร้างกฎใหม่โดยไม่มีการโต้ตอบของผู้ใช้

โปรดดู โหมดกรอง เพื่อดูข้อมูลเพิ่มเติมเกี่ยวกับโหมดกรองแต่ละโหมด

เราขอแนะนำให้คุณตรวจสอบกฎที่สร้างในโหมดการเรียนรู้ด้วยการคลิก **เปิดเครื่องมือแก้ไขกฎ**

กฎของไฟร์วอลล์

กฎของไฟร์วอลล์จะมีเงื่อนไขจำนวนหนึ่งที่ใช้เพื่อทดสอบการเชื่อมต่อเครือข่ายทั้งหมดอย่างสมเหตุสมผล และการทำงานทั้งหมดที่กำหนดไปยังเงื่อนไขเหล่านี้ เมื่อใช้ กฎไฟร์วอลล์ คุณสามารถกำหนดการกระทำที่จะดำเนินการเมื่อเริ่มต้นการเชื่อมต่อเครือข่ายประเภทต่างๆ ได้

กฎจะได้รับการประเมินจากตามความสำคัญจากมากไปน้อย และคุณสามารถเห็นลำดับความสำคัญของกฎได้ใน

คอลัมน์แรก การทำงานของกฎการจับคู่แรกจะใช้กับแต่ละการเชื่อมต่อเครือข่ายที่ถูกประเมิน

การเชื่อมต่อจะแบ่งออกเป็นการเชื่อมต่อขาเข้าและขาออก การเชื่อมต่อขาเข้าจะสร้างขึ้นโดยอุปกรณ์ระยะไกลที่พยายามสร้างการเชื่อมต่อกับระบบภายใน การเชื่อมต่อขาออกจะทำงานในทางกลับกัน โดยระบบภายในจะติดต่อกับอุปกรณ์ระยะไกล

ถ้าระบบตรวจพบการสื่อสารที่ไม่รู้จัก คุณต้องพิจารณาอย่างรอบคอบว่าจะอนุญาตหรือปฏิเสธการสื่อสารนี้ การเชื่อมต่อที่ไม่พึงประสงค์ ไม่ปลอดภัย หรือไม่รู้จักอาจทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบ หากมีการสร้างการเชื่อมต่อดังกล่าว เราขอแนะนำให้คุณให้ความสนใจเป็นพิเศษต่ออุปกรณ์ระยะไกลและแอพพลิเคชันที่พยายามจะเชื่อมต่อกับคอมพิวเตอร์ของคุณ การแฝงตัวจำนวนมากพยายามที่จะหาและส่งข้อมูลส่วนบุคคล หรือดาวน์โหลดแอพพลิเคชันที่เป็นอันตรายต่อเวิร์กสเตชันของโฮสต์ ไฟร์วอลล์จะช่วยให้คุณสามารถตรวจหาและสิ้นสุดการเชื่อมต่อดังกล่าว

คุณสามารถดูและแก้ไขกฎของไฟร์วอลล์ได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **ไฟร์วอลล์** > **กฎ** > **แก้ไข**

ถ้าคุณมีกฎของไฟร์วอลล์หลายกฎ คุณสามารถใช้ตัวกรองเพื่อแสดงเฉพาะกฎที่ต้องการได้ หากต้องการกรองกฎของไฟร์วอลล์ ให้คลิก **ตัวกรองเพิ่มเติม** เหนือรายการกฎของไฟร์วอลล์ คุณสามารถกรองกฎตามเกณฑ์ต่อไปนี้:

- ที่มา
- ทิศทาง
- การทำงาน
- สถานะการใช้งาน

โดยค่าเริ่มต้น ระบบจะซ่อนกฎของไฟร์วอลล์ที่กำหนดไว้ล่วงหน้าไว้ หากต้องการแสดงกฎที่กำหนดไว้ล่วงหน้าทั้งหมด ให้ปิดใช้งานปุ่มสลับถัดจาก **ซ่อนกฎที่มีมาให้ (กำหนดไว้ล่วงหน้า)** คุณสามารถปิดใช้งานกฎเหล่านี้ แต่คุณไม่สามารถลบกฎที่กำหนดไว้ล่วงหน้า

คลิกไอคอนการค้นหา 🔍 ตรงมุมบนขวาเพื่อค้นหากฎ

คอลัมน์

ลำดับความสำคัญ – กฎจะได้รับการประเมินจากตามความสำคัญมากไปน้อย และคุณสามารถเห็นลำดับความสำคัญของกฎได้ในคอลัมน์แรก

เปิดใช้งาน – แสดงว่ากฎกำลังเปิดใช้งานหรือปิดใช้งานอยู่ โดยต้องเลือกช่องทำเครื่องหมายที่ตรงกันเพื่อเปิดใช้กฎ

แอพพลิเคชัน – แอพพลิเคชันที่จะใช้กฎนี้

ทิศทาง – ทิศทางของการสื่อสาร (ขาเข้า/ขาออก/สองทาง)

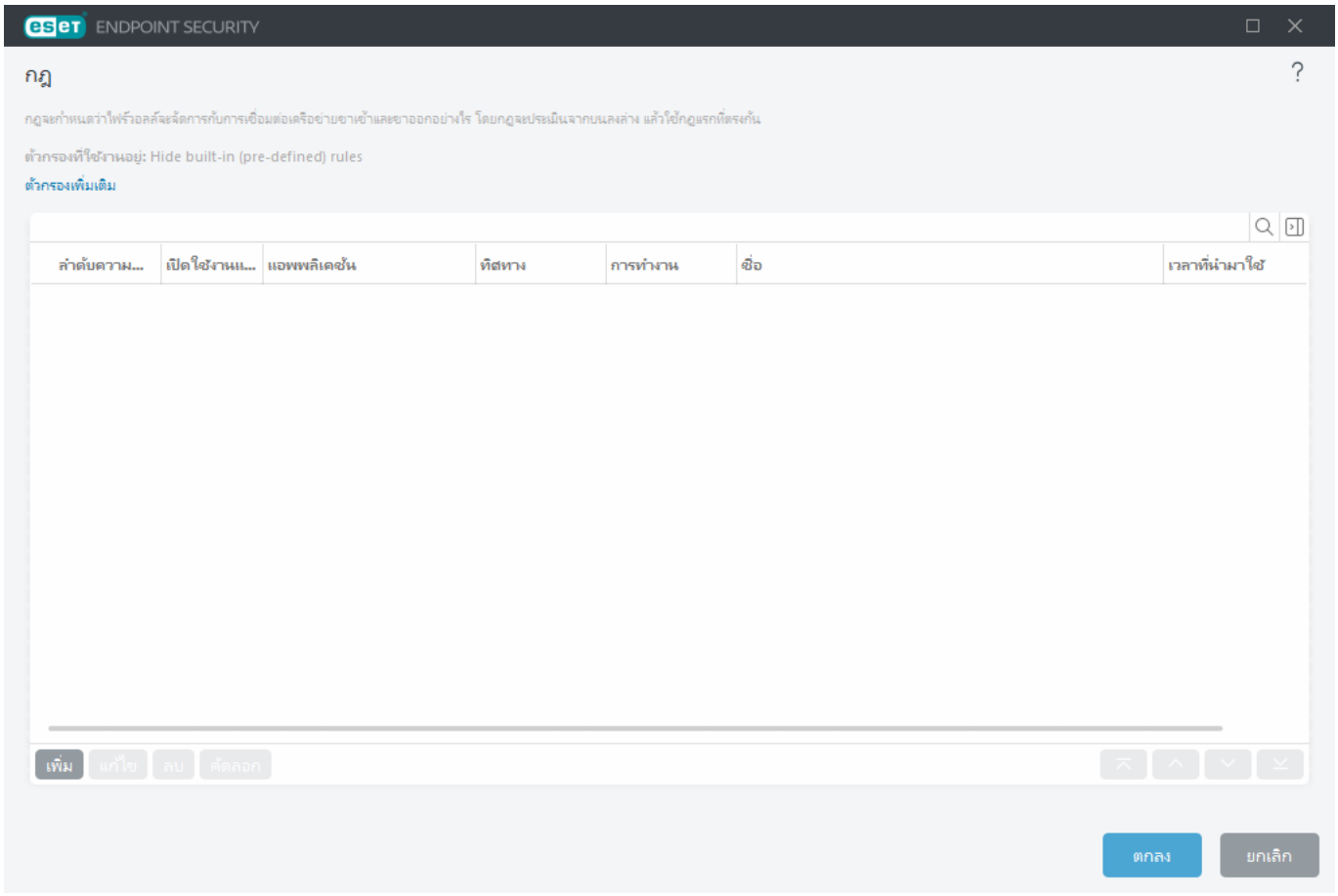
การทำงาน – แสดงสถานะของการสื่อสาร (ปิดกั้น/อนุญาต/ถาม)

ชื่อ – ชื่อของกฎ ไอคอน ESET หมายถึงกฎมีการกำหนดไว้ล่วงหน้า

จำนวนครั้งที่ใช้ – จำนวนครั้งทั้งหมดที่ใช้กฎ

คลิกไอคอนขยาย เพื่อแสดงรายละเอียดกฎ

คุณสามารถเลือกคอลัมน์ที่จะแสดงได้โดยคลิกขวาที่ส่วนหัวตาราง



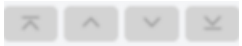
องค์ประกอบการควบคุม

เพิ่ม – สร้างกฎใหม่

แก้ไข – แก้ไขกฎที่มีอยู่

ลบออก – ลบกฎที่มีอยู่

คัดลอก - สร้างสำเนาของกฎที่เลือก

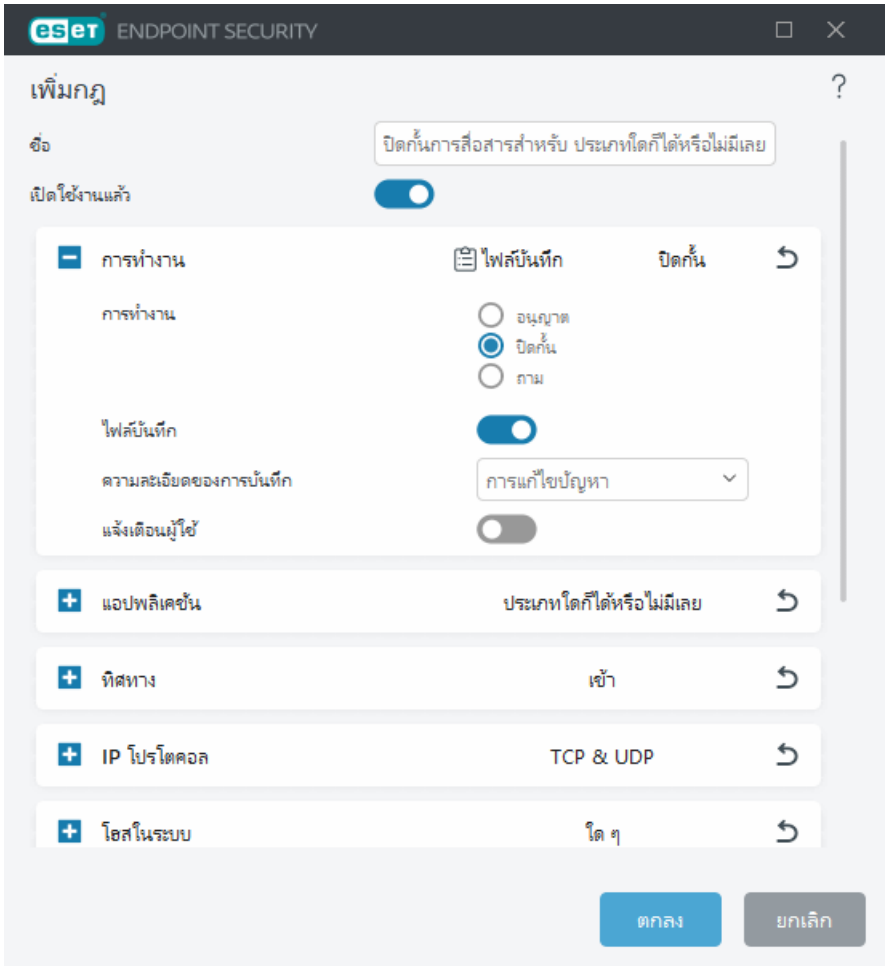
 **บนสุด/ขึ้น/ลง/ล่างสุด** – อนุญาตให้คุณปรับระดับความสำคัญของกฎ (กฎจะถูกเรียกใช้จากบนลงล่าง)

การเพิ่มหรือแก้ไขกฎของไฟร์วอลล์

กฎของไฟร์วอลล์จะแสดงเงื่อนไขจำนวนหนึ่งที่ใช้เพื่อทดสอบการเชื่อมต่อเครือข่ายและการทำงานทั้งหมดที่กำหนดไปยังเงื่อนไขเหล่านี้อย่างสมเหตุสมผล อาจจำเป็นต้องแก้ไขหรือเพิ่มกฎของไฟร์วอลล์เมื่อมีการเปลี่ยนแปลงการตั้งค่าเครือข่าย (ตัวอย่างเช่น เมื่อมีการเปลี่ยนแปลงที่อยู่เครือข่ายหรือหมายเลขพอร์ตสำหรับฝั่งระยะไกล) เพื่อให้แน่ใจว่าแอพพลิเคชันที่ได้รับผลจากกฎจะดำเนินการได้อย่างถูกต้อง ผู้ใช้ที่มีประสบการณ์ควรเป็นผู้สร้างกฎของไฟร์วอลล์ที่กำหนดเอง

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
- สร้างหรือแก้ไขกฎของไฟร์วอลล์ใน ESET Endpoint Security
- สร้างหรือแก้ไขกฎของไฟร์วอลล์สำหรับไคลเอ็นต์เวิร์กสเตชันใน ESET PROTECT

หากต้องการเพิ่มหรือแก้ไขกฎของไฟร์วอลล์ ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **ไฟร์วอลล์** > **กฎ** > **แก้ไข** ในหน้าต่าง กฎของไฟร์วอลล์ ให้คลิก **เพิ่ม** หรือ **แก้ไข**



ชื่อ – พิมพ์ชื่อสำหรับกฎ

เปิดใช้งานแล้ว – เปิดใช้งานปุ่มสลับเพื่อใช้กฎ

เพิ่มการดำเนินการและเงื่อนไขสำหรับกฎของไฟร์วอลล์:

การทำงาน

การดำเนินการ – เลือกตัวเลือกนี้หากคุณต้องการ **อนุญาต/บล็อก** การสื่อสารที่ตรงกับเงื่อนไขที่กำหนดไว้ในกฎนี้ หรือหากคุณต้องการให้ ESET Endpoint Security **ถาม** ทุกครั้งที่มีการสื่อสารเกิดขึ้น
กฎการบันทึก – หากมีการใช้กฎ กฎดังกล่าวจะบันทึกไว้ใน ไฟล์บันทึก
ความละเอียดของการบันทึก เลือก ความละเอียดของการบันทึก สำหรับกฎนี้
แจ้งผู้ใช้ จะแสดงการแจ้งเตือนเมื่อมีการปรับใช้กฎ

แอพพลิเคชัน

ระบุแอพพลิเคชันที่ต้องการให้กฎนี้มีผลใช้
พาธแอพพลิเคชัน – คลิก **...** และนำทางไปยังแอพพลิเคชันหรือป้อนพาธแบบเต็มไปยังแอพพลิเคชัน (ตัวอย่างเช่น C:\Program Files\Firefox\Firefox.exe) อย่าป้อนเพียงชื่อของแอพพลิเคชัน
ลายเซ็นแอพพลิเคชัน – คุณสามารถนำกฎไปใช้กับแอพพลิเคชันตามลายเซ็นของแอพพลิเคชัน (ชื่อผู้เผยแพร่) เลือกตัวเลือกจากเมนูแบบเลื่อนลงหากคุณต้องการนำกฎไปใช้กับแอพพลิเคชันที่มี **ลายเซ็นที่ถูกต้อง** หรือแอพพลิเคชันที่ **ลงนามโดยผู้ลงนามที่กำหนดไว้** หากคุณเลือกแอพพลิเคชันที่ **ลงนามโดยผู้ลงนามที่กำหนดไว้** คุณต้องกำหนดผู้ลงนามในช่อง **ชื่อของผู้ลงนาม**
แอพพลิเคชัน Microsoft Store – เลือกแอพพลิเคชันที่ติดตั้งจาก Microsoft Store ในเมนูแบบเลื่อนลง
บริการ – คุณสามารถเลือกบริการของระบบแทนโปรแกรมได้ เปิดเมนูแบบเลื่อนลงเพื่อเลือกบริการ
นำไปใช้กับการประมวลผลย่อย – แอปพลิเคชันบางแอพอาจเรียกใช้การประมวลผลหลายอย่าง ขณะที่คุณเห็นหน้าต่างโปรแกรมประยุกต์เพียงหน้าต่างเดียว เปิดใช้งานปุ่มสลับนี้เพื่อให้แน่ใจว่ากฎจะมีผลใช้กับทุกขั้นตอนสำหรับโปรแกรมที่ระบุ

ทิศทาง

เลือก **ทิศทาง** ของการสื่อสารที่กฎนี้จะมีผลใช้:
• **ทั้งคู่** – การสื่อสารขาเข้าและขาออก
• **เข้า** – การสื่อสารขาเข้าเท่านั้น
• **ออก** – การสื่อสารขาออกเท่านั้น

IP โปรโตคอล

เลือก **โปรโตคอล** จากเมนูแบบเลื่อนลง หากคุณต้องการใช้กฎนี้กับโพรโตคอลที่ต้องการเท่านั้น

โฮสในระบบ

ที่อยู่ในระบบ ช่วงที่อยู่หรือซับเน็ตที่กฎนี้จะมีผลใช้ หากไม่มีการระบุที่อยู่ กฎจะมีผลใช้กับการสื่อสารทั้งหมดกับโฮสต์ในระบบ คุณสามารถเพิ่มที่อยู่ IP, ช่วงที่อยู่ หรือซับเน็ตลงในช่องข้อความ **IP** โดยตรง หรือเลือกจาก ชุด IP ที่มีอยู่โดยคลิก **แก้ไข** ถัดจาก **ชุด IP**

พอร์ตในระบบ

หมายเลข **พอร์ต** ในระบบ หากไม่มีการระบุเลขที่ไว้ กฎจะมีผลใช้งานกับพอร์ตทุกพอร์ต เพิ่มพอร์ตการสื่อสารรายการเดียวหรือเพิ่มช่วงของพอร์ตการสื่อสาร

โฮสระยะไกล

ที่อยู่ระยะไกล ช่วงที่อยู่ หรือซับเน็ตที่กฎนี้จะมีผลใช้ หากไม่มีการระบุที่อยู่ กฎจะมีผลใช้กับการสื่อสารทั้งหมดกับโฮสต์ระยะไกล คุณสามารถเพิ่มที่อยู่ IP, ช่วงที่อยู่ หรือซับเน็ตลงในช่องข้อความ **IP** โดยตรง หรือเลือกจาก ชุด IP ที่มีอยู่โดยคลิก **แก้ไข** ถัดจาก **ชุด IP**

พอร์ตระยะไกล

หมายเลข **พอร์ต** ระยะไกล หากไม่มีการระบุเลขที่ไว้ กฎจะมีผลใช้งานกับพอร์ตทุกพอร์ต เพิ่มพอร์ตการสื่อสารรายการเดียวหรือเพิ่มช่วงของพอร์ตการสื่อสาร

โปรไฟล์

กฎของไฟร์วอลล์สามารถนำไปใช้กับ โปรไฟล์การเชื่อมต่อเครือข่าย ที่เฉพาะเจาะจงได้
รายการใดก็ได้ – กฎจะมีผลใช้กับการเชื่อมต่อเครือข่ายใดๆ แม้จะมีการใช้โปรไฟล์แล้วก็ตาม
ที่เลือกไว้ – กฎจะมีผลใช้กับการเชื่อมต่อเครือข่ายตามโปรไฟล์ที่เลือกไว้ เลือกกล่องทำเครื่องหมายถัดจากโปรไฟล์ที่คุณเลือก

ในตัวอย่างนี้ เราสร้างกฎใหม่เพื่ออนุญาตให้แอพพลิเคชันเว็บเบราว์เซอร์ Firefox เข้าถึงเว็บไซต์บนอินเทอร์เน็ต / เครือข่ายภายในระบบได้:
1. ในส่วน **การดำเนินการ** เลือก **อนุญาต** > **การดำเนินการ**
2. ในส่วน **แอพพลิเคชัน** ให้ระบุ **พาธแอพพลิเคชัน** ของเว็บเบราว์เซอร์ (ตัวอย่างเช่น C:\Program Files\Firefox\Firefox.exe) อย่าป้อนเพียงชื่อของแอพพลิเคชัน
3. ในส่วน **ทิศทาง** ให้เลือก **ทิศทาง** > **ออก**
4. ในส่วน **โปรโตคอล IP** ให้เลือก **TCP & UDP** จากเมนูแบบเลื่อนลงสำหรับ **โปรโตคอล**
5. ในส่วน **พอร์ตระยะไกล** ให้ระบุหมายเลข **พอร์ต** เป็น *80,443* เพื่ออนุญาตการเรียกดูแบบมาตรฐาน

กฎที่กำหนดไว้ล่วงหน้าสามารถแก้ไขได้จำกัด

การตรวจหาการแก้ไขแอพพลิเคชัน

คุณสมบัติการตรวจหาการแก้ไขแอพพลิเคชัน จะแสดงการแจ้งเตือนหากมีแอพพลิเคชันที่ถูกแก้ไขซึ่งมีกฎไฟร์วอลล์พยายามเริ่มต้นการเชื่อมต่อ การแก้ไขแอพพลิเคชันคือกลไกของการแทนที่แอพพลิเคชันดั้งเดิมด้วยแอพพลิเคชันอื่นเป็นการชั่วคราวหรือโดยถาวรโดยไฟล์ที่เรียกใช้ได้ที่แตกต่างกัน (ป้องกันกฎไฟร์วอลล์ที่ไม่เหมาะสม)

โปรดทราบว่าคุณลักษณะนี้ไม่ได้สร้างขึ้นเพื่อตรวจหาการแก้ไขของแอพพลิเคชันใดๆ โดยทั่วไป เป้าหมายคือเพื่อหลีกเลี่ยงกฎของไฟร์วอลล์ที่ไม่เหมาะสม และจะตรวจสอบเฉพาะแอพพลิเคชันที่มีกฎของไฟร์วอลล์ที่ระบุเท่านั้น

หากต้องการแก้ไข **การตรวจหาการแก้ไขแอพพลิเคชัน** ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **ไฟร์วอลล์** > **การตรวจหาการแก้ไขแอพพลิเคชัน**

เปิดใช้งานการตรวจหาการแก้ไขแอพพลิเคชัน – ถ้าเลือกตัวเลือกนี้ โปรแกรมจะตรวจสอบแอพพลิเคชันเพื่อหาการเปลี่ยนแปลง (การอัพเดท การติดไวรัส การแก้ไขอื่นๆ) เมื่อแอพพลิเคชันที่แก้ไขพยายามเริ่มต้นการเชื่อมต่อไฟร์วอลล์จะแจ้งให้คุณทราบ

อนุญาตให้มีการแก้ไขแอพพลิเคชันที่ลงชื่อ (เชื่อถือ) – ไม่ต้องแจ้งเตือนถ้าแอพพลิเคชันก่อนและหลังการแก้ไขมีลายเซ็นดิจิทัลที่ถูกต้องและเป็นลายเดียวกัน

รายชื่อแอพพลิเคชันที่ยกเว้นจากการตรวจหา – หน้าต่างนี้จะให้คุณเพิ่มหรือลบแอพพลิเคชันแต่ละรายการออกจากรายการที่อนุญาตให้แก้ไขโดยไม่ต้องแจ้งเตือน

รายการแอพพลิเคชันที่ยกเว้นจากการตรวจหา

ไฟร์วอลล์ใน ESET Endpoint Security จะตรวจหาการเปลี่ยนแปลงของแอพพลิเคชันที่มีกฎ (โปรดดู การตรวจหาการแก้ไขแอพพลิเคชัน)

ในบางกรณี คุณอาจไม่ต้องการใช้ฟังก์ชันนี้สำหรับบางแอพพลิเคชัน ถ้าคุณต้องการยกเว้นจากการตรวจสอบโดยไฟร์วอลล์

เพิ่ม – เปิดหน้าต่างซึ่งคุณสามารถเลือกแอพพลิเคชันเพื่อเพิ่มไปยังรายการแอพพลิเคชันที่ยกเว้นจากการตรวจหาการแก้ไขได้ คุณสามารถเลือกจากรายการแอพพลิเคชันที่กำลังทำงานอยู่ได้ด้วยการสื่อสารบนเครือข่ายแบบเปิดซึ่งมีกฎไฟร์วอลล์อยู่ หรือเพิ่มแอพพลิเคชันเฉพาะ

แก้ไข – เปิดหน้าต่างซึ่งคุณสามารถเปลี่ยนตำแหน่งของแอพพลิเคชันที่อยู่ในรายการแอพพลิเคชันที่ยกเว้นจากการตรวจหาการแก้ไขได้ คุณสามารถเลือกจากรายการแอพพลิเคชันที่กำลังทำงานอยู่ได้ด้วยการสื่อสารบนเครือข่ายแบบเปิดซึ่งมีกฎไฟร์วอลล์อยู่ หรือเปลี่ยนตำแหน่งที่ตั้งด้วยตนเอง

ลบออก – ลบรายการออกจากรายการแอพพลิเคชันที่ยกเว้นจากการตรวจหาการแก้ไข

เปิดใช้งานการป้องกันการโจมตีเครือข่าย (IDS)

การป้องกันการโจมตีเครือข่าย (IDS) จะปรับปรุงการตรวจหาช่องโหว่ของจุดอ่อนที่รู้จัก อ่านเพิ่มเติมเกี่ยวกับการป้องกันการโจมตีเครือข่ายใน ประมวลศัพท์ หากต้องการกำหนดค่าการป้องกันการโจมตีเครือข่าย ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **การป้องกันการโจมตีเครือข่าย**

การป้องกันการโจมตีเครือข่าย (IDS) – วิเคราะห์เนื้อหาของการรับส่งของเครือข่ายและป้องกันการโจมตีเครือข่าย การรับส่งใด ๆ ที่ได้รับพิจารณาว่าเป็นอันตรายจะถูกปิดกั้น

เปิดใช้งานการป้องกันบอตเน็ต – ตรวจหาและปิดกั้นการสื่อสารกับคำสั่งที่เป็นอันตราย และควบคุมเซิร์ฟเวอร์ที่เกิดขึ้นตามรูปแบบปกติเมื่อคอมพิวเตอร์ติดไวรัสและบ็อตพยายามสื่อสาร อ่านเพิ่มเติมเกี่ยวกับการป้องกันบอตเน็ตในประมวลศัพท์

กฎ IDS – ตัวเลือกนี้อนุญาตให้คุณกำหนดค่าตัวเลือกการกรองขั้นสูงเพื่อตรวจหาการโจมตีและการใช้ช่องโหว่ประเภทต่างๆ ที่สามารถใช้เพื่อทำอันตรายคอมพิวเตอร์ของคุณได้

เหตุการณ์สำคัญทั้งหมดที่ตรวจพบโดยการป้องกันเครือข่ายจะถูกบันทึกไว้ในไฟล์บันทึก ดูข้อมูลเพิ่มเติมได้จาก บันทึกการป้องกันเครือข่าย

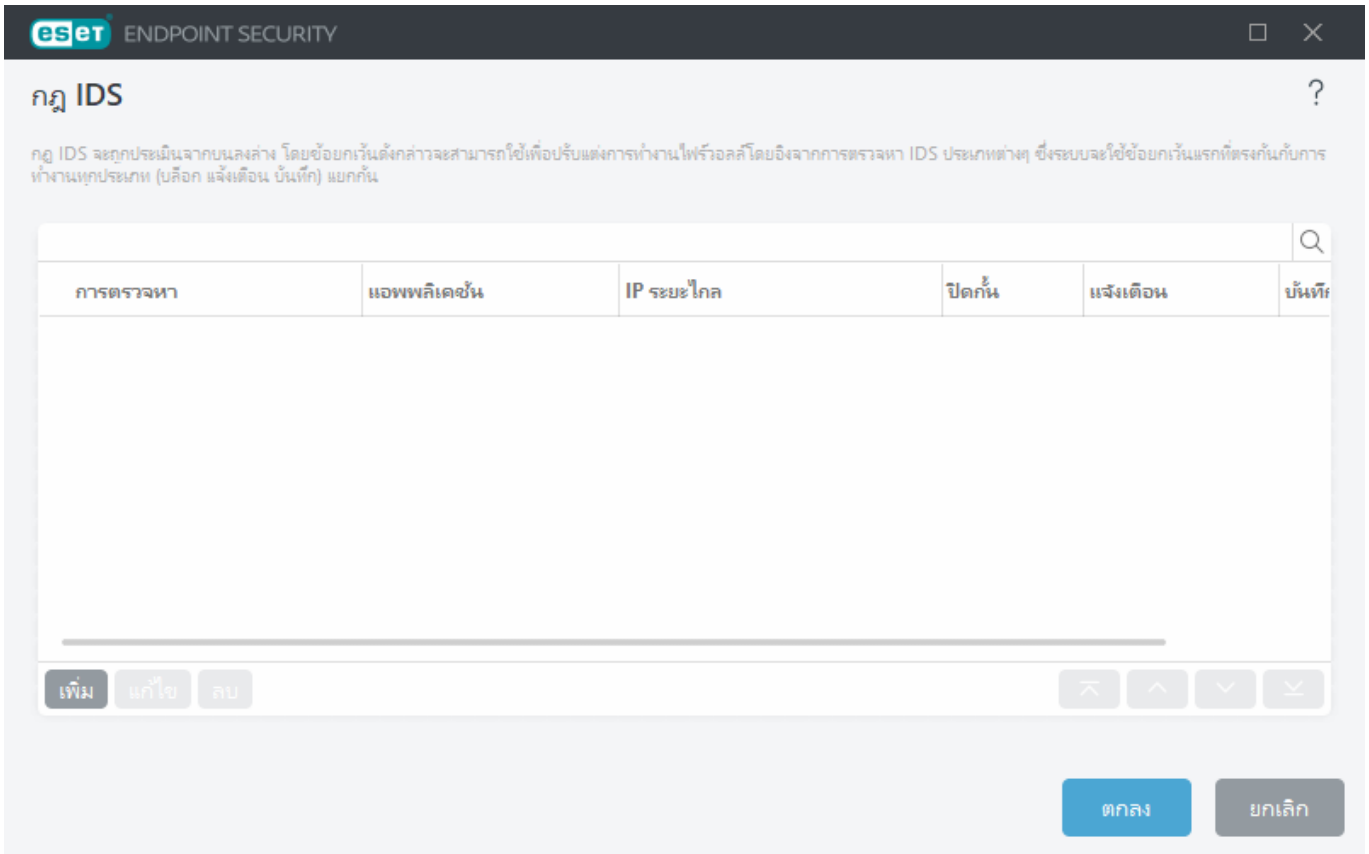
กฎ IDS

ในบางสถานการณ์ บริการการตรวจหาผู้บุรุก (IDS) อาจตรวจพบว่าการสื่อสารระหว่างเราเตอร์หรืออุปกรณ์เครือข่ายภายในอื่นๆ อาจเป็นการโจมตีได้ ตัวอย่างเช่น คุณสามารถเพิ่มที่อยู่ที่แน่ใจว่าปลอดภัยไปยังที่อยู่ที่ยกเว้นของโซน IDS เพื่อข้าม IDS ได้

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
- สร้างกฎ IDS บนเวิร์กสเตชันไคลแอนต์ใน ESET Endpoint Security
- สร้างกฎ IDS สำหรับเวิร์กสเตชันไคลแอนต์ใน ESET PROTECT

การจัดการกฎ IDS

- **เพิ่ม** – คลิกเพื่อสร้างกฎ IDS ใหม่
- **แก้ไข** – คลิกเพื่อแก้ไขกฎ IDS ที่มีอยู่
- **ลบออก** – เลือกและคลิกตัวเลือกนี้หากคุณต้องการลบกฎที่มีอยู่ออกจากรายการกฎ IDS
- **บนสุด/ขึ้น/ลง/ล่างสุด** – อนุญาตให้คุณปรับระดับความสำคัญของกฎ (ข้อยกเว้นจะถูกประเมินจากบนลงล่าง)



แท็บ **การยกเว้น** จะปรากฏขึ้นหากผู้ดูแลระบบ สร้างการยกเว้น IDS ในเว็บคอนโซล ESET PROTECT การยกเว้น IDS

สามารถมีกฎการอนุญาตเท่านั้นและจะได้รับการประเมินก่อนกฎ IDS

ตัวแก้ไขกฎ

การตรวจหา – ประเภทการยกเว้นการตรวจหา

ชื่อภัยคุกคาม – คุณสามารถระบุชื่อภัยคุกคามสำหรับการตรวจหาบางรายการที่มีอยู่ได้

แอพพลิเคชัน – เลือกพาธไฟล์ของแอพพลิเคชันที่ได้รับการยกเว้นโดยการคลิก ... (ตัวอย่างเช่น *C:\Program Files\Firefox\Firefox.exe*) อย่าป้อนชื่อของแอพพลิเคชัน

ที่อยู่ IP ระยะไกล – รายการที่อยู่ / ระยะ / ซับเน็ต IPv4 หรือ IPv6 โดยที่อยู่ที่มากกว่าหนึ่งแห่งจะต้องคั่นด้วยเครื่องหมายจุลภาค

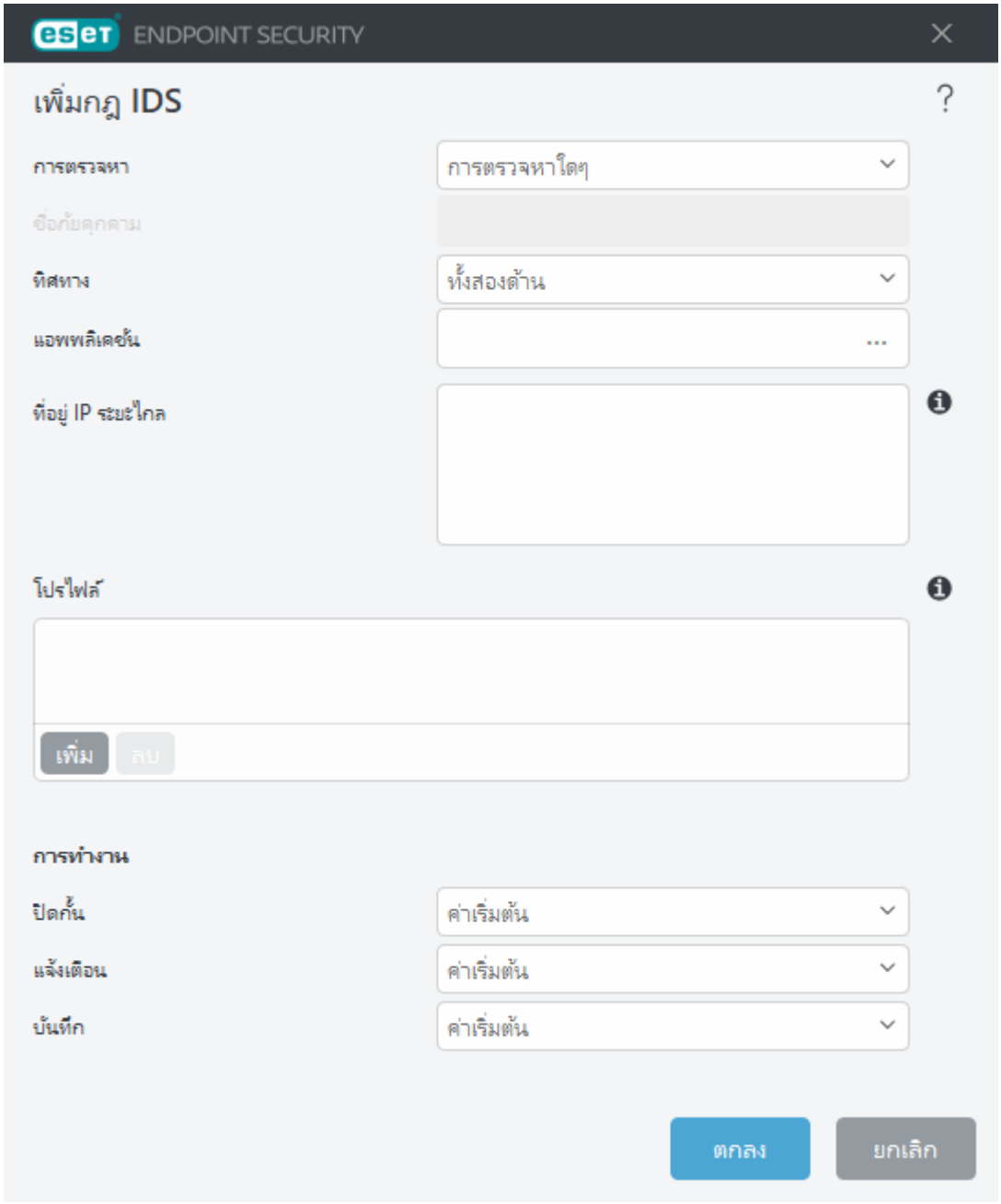
โปรไฟล์ – คุณสามารถเลือก โปรไฟล์การเชื่อมต่อเครือข่าย ที่จะใช้กฎนี้

การทำงาน

ปิดกั้น – แต่ละกระบวนการของระบบมีค่าเริ่มต้นของการทำงานและการทำงานที่กำหนดเป็นของตนเอง (ปิดกั้นหรืออนุญาต) เมื่อต้องการเขียนทับค่าเริ่มต้นของการทำงานสำหรับ ESET Endpoint Security คุณสามารถเลือกปิดกั้นหรืออนุญาตค่าเริ่มต้นนั้นโดยใช้เมนูแบบเลื่อนลง

แจ้งเตือน – เลือก ใช่ เพื่อแสดง แอพพลิเคชันบนเดสก์ท็อป ในคอมพิวเตอร์ของคุณ เลือก ไม่ หากคุณไม่ต้องการการแจ้งเตือนบนเดสก์ท็อป ค่าที่จะมีให้ใช้งานคือค่าเริ่มต้น/ใช่/ไม่

บันทึก – เลือก**ใช่** เพื่อบันทึกกิจกรรมลงใน ไฟล์บันทึกของ ESET Endpoint Security เลือก **ไม่** หากคุณไม่ต้องการบันทึกกิจกรรม ค่าที่มีให้ใช้งานคือ **ค่าเริ่มต้น/ใช่/ไม่**



คุณต้องการแสดงการแจ้งเตือนและรวบรวมบันทึกในแต่ละครั้งที่กิจกรรมเกิดขึ้น:
1. คลิก **เพิ่ม** เพื่อเพิ่มกฎ IDS ใหม่
2. เลือกการเตือนเฉพาะจากเมนู **การตรวจหา** แบบเลื่อนลง
3. คลิก **...** แล้วเลือกพาธไฟล์ ของแอพพลิเคชันที่ คุณต้องการใช้การแจ้งเตือน
4. ปล่อยให้เป็น **ค่าเริ่มต้น** ในเมนู **ปิดกั้น** แบบเลื่อนลง วิธีนี้จะสืบทอดการกระทำที่ใช้โดย ESET Endpoint Security
5. ตั้งค่าทั้ง **การแจ้งเตือน** และเมนู **บันทึก** แบบเลื่อนลงเพื่อ **ใช่**
6. คลิก **ตกลง** เพื่อบันทึกการแจ้งเตือน

คุณต้องการลบการแจ้งเตือนที่เกิดขึ้นอีกครั้งออกสำหรับประเภทของการตรวจหาที่คุณไม่คิดว่าเป็นภัยคุกคาม :

1. คลิก **เพิ่ม** เพื่อเพิ่มข้อยกเว้น IDS
2. เลือกการเตือนแบบเฉพาะเจาะจงจากเมนูแบบเลื่อนลงสำหรับ **การตรวจหา** เช่น **เซสชัน SMB ที่ไม่มีส่วนขยายด้านการรักษาความปลอดภัย** หรือ **การโจมตีแบบสแกนพอร์ต TCP**
3. เลือก **ใน** จากเส้นทางเมนูแบบเลื่อนลงในกรณีที่มาจากการสื่อสารขาเข้า
4. ตั้งค่าเมนู **การแจ้งเตือน** แบบเลื่อนลงไปยัง **ไม่**
5. ตั้งค่าเมนู **บันทึก** แบบเลื่อนลง **ใช่**
6. ปล่อย**แอพพลิเคชัน** ว่างเปล่า
7. หากการสื่อสารไม่ได้มาจากที่อยู่ IP เฉพาะ ให้ปล่อย **ที่อยู่ IP ระยะไกล** ว่างไว้
8. คลิก **ตกลง** เพื่อบันทึกการแจ้งเตือน

การป้องกันการโจมตีแบบ Brute-Force

การป้องกันการโจมตีแบบ Brute-force จะบล็อกการโจมตีด้วยการคาดเดารหัสผ่านสำหรับบริการ RDP และ SMB การโจมตีแบบ Brute-force เป็นวิธีการค้นหารหัสผ่านเป้าหมายโดยลองใช้ชุดตัวอักษร ตัวเลข และสัญลักษณ์ทั้งหมดรวมกันอย่างเป็นระบบ หากต้องการกำหนดค่าการป้องกันการโจมตีแบบ Brute-Force ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **การป้องกันการโจมตีเครือข่าย** > **การป้องกันการโจมตีแบบ Brute-Force**

เปิดใช้งานการป้องกันการโจมตีแบบ Brute-force – ESET Endpoint Security ตรวจสอบเนื้อหาการรับส่งข้อมูลเครือข่ายและบล็อกความพยายามในการโจมตีด้วยการคาดเดารหัสผ่าน

กฎ – ช่วยให้คุณสร้าง แก้ไข และดูกฎสำหรับการเชื่อมต่อเครือข่ายขาเข้าและขาออกได้ หากต้องการข้อมูลเพิ่มเติม โปรดดู กฎ

การยกเว้น – รายการส่วนขยายที่กำหนดโดยที่อยู่ IP หรือพาธของแอพพลิเคชัน คุณสามารถสร้างและแก้ไขการยกเว้นได้ใน ESET PROTECT หากต้องการข้อมูลเพิ่มเติม โปรดดู การยกเว้น

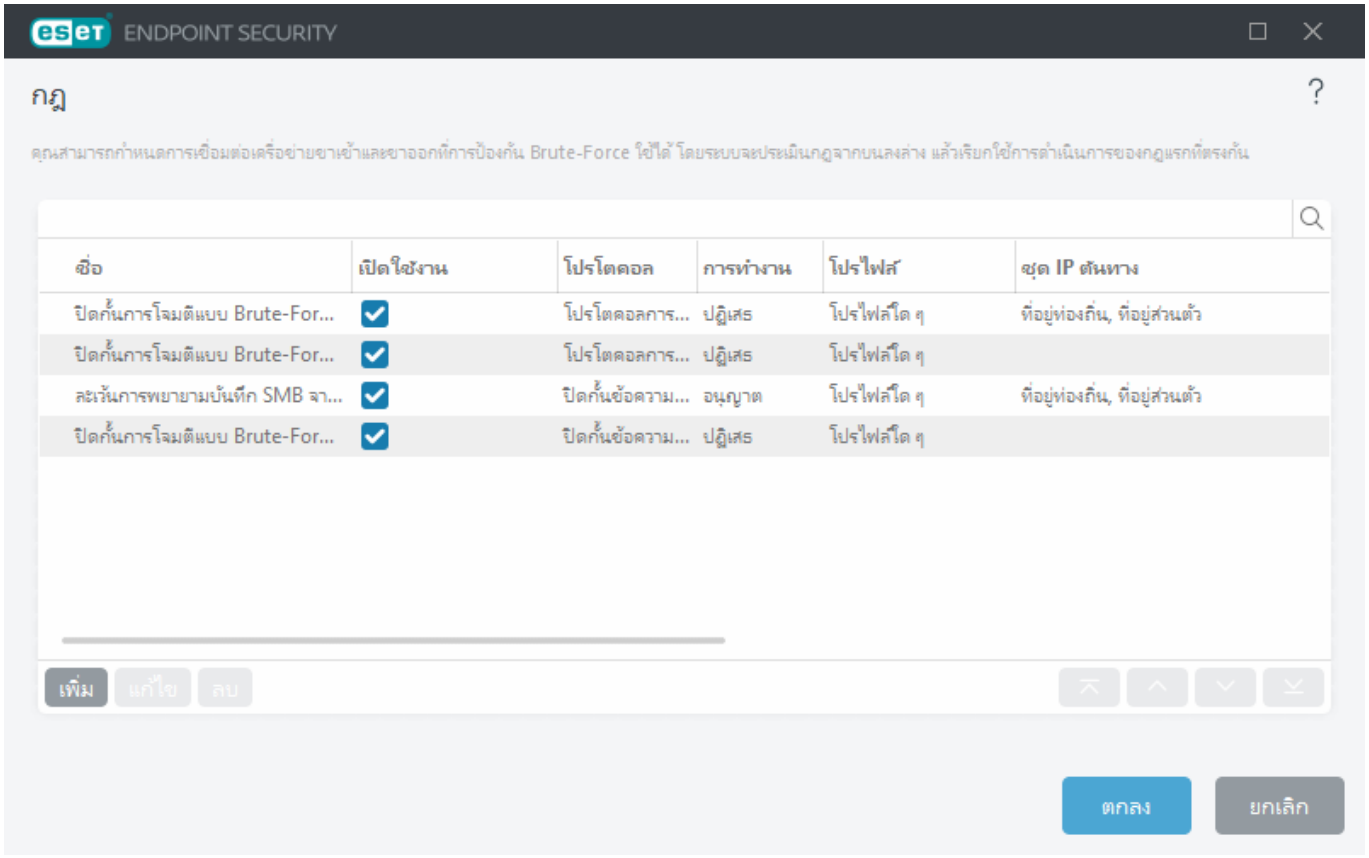
หากต้องการข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันการโจมตีแบบ Brute-Force โปรดดู บทความในคู่มือการรักษาความปลอดภัยดิจิทัลของ ESET

กฎ

กฎการป้องกันการโจมตีแบบ Brute-force จะช่วยให้คุณสร้าง แก้ไข และดูกฎสำหรับการเชื่อมต่อเครือข่ายขาเข้าและขาออกได้ กฎที่กำหนดไว้ล่วงหน้าไม่สามารถแก้ไขหรือลบได้

การจัดการกฎการป้องกันการโจมตีแบบ Brute-Force

- **เพิ่ม** – คลิกเพื่อสร้างกฎการป้องกันการโจมตีแบบ Brute-Force ใหม่
- **แก้ไข** – คลิกเพื่อแก้ไขกฎการป้องกันการโจมตีแบบ Brute-Force ที่มีอยู่
- **ลบออก** – เลือกและคลิกตัวเลือกนี้หากคุณต้องการลบข้อยกเว้นที่มีอยู่ออกจากรายการกฎ IDS
- **บนสุด/ขึ้น/ลง/ล่างสุด** – ปรับระดับความสำคัญของกฎ



เพื่อให้แน่ใจว่ามีการป้องกันสูงสุดที่เป็นไปได้ จะมีการใช้กฎการบล็อกที่มีค่า **ความพยายามสูงสุด** ต่ำสุดเมื่อกฎการบล็อกหลายกฎตรงกับเงื่อนไขการตรวจหา แม้ว่ากฎจะอยู่ในตำแหน่งรายการกฎที่ต่ำกว่าก็ตาม

ตัวแก้ไขกฎ

ชื่อ – ชื่อของกฎ

เปิดใช้งาน – ปิดใช้งานปุ่มสลับนี้หากคุณต้องการคงกฎไว้ในรายการแต่ไม่ปรับใช้

การดำเนินการ – เลือกว่าจะ **ปฏิเสธ** หรือ **อนุญาต** การเชื่อมต่อหากมีการปฏิบัติตามการตั้งค่ากฎ

โปรโตคอล – โปรโตคอลการสื่อสารที่กฎนี้จะตรวจสอบ

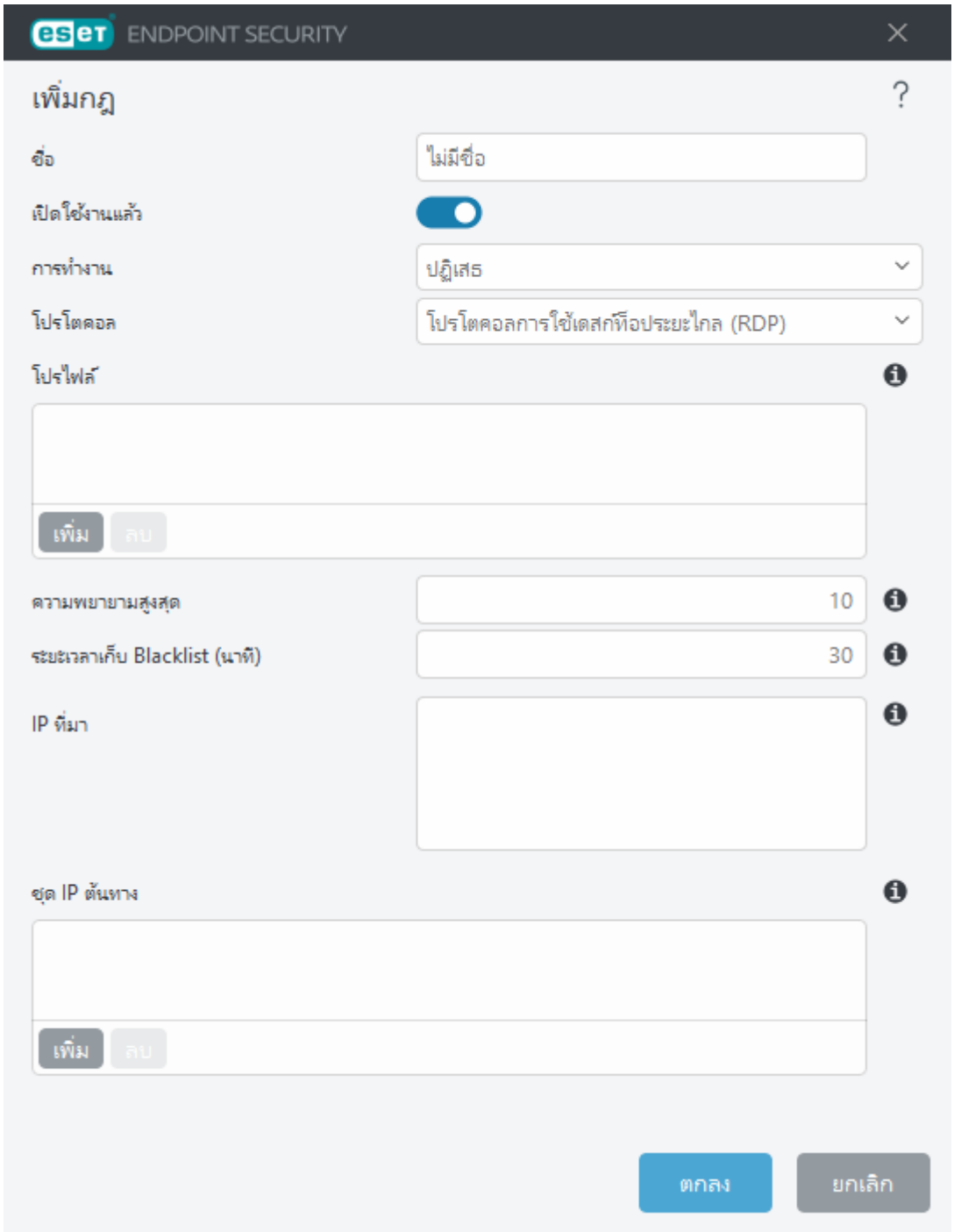
โปรไฟล์ – คุณสามารถเลือก โปรไฟล์การเชื่อมต่อเครือข่าย ที่จะใช้กฎนี้

ความพยายามสูงสุด: จำนวนสูงสุดของความพยายามโจมตีซ้ำที่อนุญาตจนกว่าที่อยู่ IP จะถูกปิดกั้นและเพิ่มลงใน Blacklist

ระยะเวลาการเก็บรักษา Blacklist (นาที) – ตั้งเวลาสำหรับให้ที่อยู่หมดอายุจาก Blacklist

IP ที่มา – รายการ / ช่วง / เครือข่ายย่อยของที่อยู่ IP โดยที่อยู่ที่มากกว่าหนึ่งแห่งจะต้องคั่นด้วยเครื่องหมายจุลภาค

ชุด IP ต้นทาง – ชุดที่อยู่ IP ที่คุณได้กำหนดไว้แล้วใน ชุด IP



การยกเว้น

การยกเว้น Brute-Force สามารถใช้เพื่อระงับการตรวจหา Brute-Force สำหรับเกณฑ์แบบเฉพาะได้ โดยการยกเว้นเหล่านี้จะสร้างขึ้นจาก ESET PROTECT โดยอิงการตรวจหา Brute-Force

คอลัมน์

- **การตรวจหา** – ประเภทการยกเว้นการตรวจหา
- **แอพพลิเคชัน** – เลือกพาธไฟล์ของแอพพลิเคชันที่ได้รับการยกเว้นโดยการคลิก ... (ตัวอย่างเช่น *C:\Program Files\Firefox\Firefox.exe*) อย่าป้อนชื่อของแอพพลิเคชัน
- **IP ระยะไกล** – รายการที่อยู่ / ระยะ / ซับเน็ต IPv4 หรือ IPv6 โดยที่อยู่ที่มากกว่าหนึ่งแห่งจะต้องคั่นด้วยเครื่องหมายจุลภาค

การจัดการการยกเว้น

การยกเว้นจะปรากฏขึ้นหากผู้ดูแลระบบ สร้างการยกเว้น Brute-Force ในเว็บคอนโซล ESET PROTECT การยกเว้นสามารถมีกฎการอนุญาตเท่านั้นและจะได้รับการประเมินก่อนกฎ IDS

ตัวเลือกขั้นสูง

คุณสามารถเปิดใช้หรือปิดใช้งานการตรวจหาการโจมตีและการโจมตีช่องโหว่หลายชนิดที่อาจเป็นอันตรายต่อคอมพิวเตอร์ของคุณได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเครือข่าย** > **การป้องกันการโจมตีเครือข่าย** > **ตัวเลือกขั้นสูง**

ในบางกรณี คุณจะไม่ได้รับการแจ้งเตือนภัยคุกคามเกี่ยวกับการสื่อสารที่ปิดกั้น โปรดศึกษาส่วน การบันทึกและการสร้างกฎหรือข้อยกเว้นการบันทึก สำหรับคำแนะนำในการดูการสื่อสารที่ปิดกั้นที่อยู่ในบันทึกไฟร์วอลล์

ความพร้อมในการใช้งานสำหรับตัวเลือกในหน้าต่างนี้อาจแตกต่างกันไป ทั้งนี้จะขึ้นอยู่กับประเภทหรือเวอร์ชันของผลิตภัณฑ์ของ ESET และโมดูลไฟร์วอลล์ รวมทั้งเวอร์ชันของระบบปฏิบัติการของคุณ

การตรวจหาการบุกรุก

- **โปรโตคอล SMB** – ตรวจหาและปิดกั้นปัญหาด้านความปลอดภัยต่างๆ ในโปรโตคอล SMB กล่าวคือ:

- **การตรวจหาการตรวจสอบสิทธิ์การโจมตีด้วยการใช้เซิร์ฟเวอร์ลวง** – ป้องกันการโจมตีที่ใช้การหลอกลวงระหว่างการตรวจสอบสิทธิ์เพื่อให้ได้ข้อมูลการเข้าสู่ระบบของผู้ใช้
- **การตรวจหาการหลีกเลี่ยง IDS ระหว่างการเปิดไปป์ที่กำหนดชื่อ** – การตรวจหาเทคนิคการหลีกเลี่ยงที่รู้จักที่ใช้ในการเปิดไปป์ที่กำหนดชื่อ MSRPCS ในโปรโตคอล SMB
- **การตรวจหา CVE** (Common Vulnerabilities and Exposures) – วิธีการตรวจหาการโจมตี รูปแบบ จุดอ่อน และการโจมตีด้านการรักษาความปลอดภัยจำนวนมากที่นำมาปรับใช้งานในโปรโตคอล SMB โปรดดู เว็บไซต์ CVE ที่ cve.mitre.org เพื่อค้นหาและดูข้อมูลโดยละเอียดเพิ่มเติมเกี่ยวกับตัวระบุ CVE (CVEs)
- **โปรโตคอล RPC** – ตรวจหาและปิดกั้น CVE ต่างๆ ในระบบการเรียกขั้นตอนระยะไกลที่พัฒนาสำหรับ Distributed Computing Environment (DCE)
- **โปรโตคอล RDP** – ตรวจหาและปิดกั้น CVE ต่างๆ ในโปรโตคอล RDP (ดูที่ด้านบน)
- **การตรวจหาการโจมตี ARP Poisoning** – การตรวจหาการโจมตี ARP Poisoning ที่เรียกใช้การโจมตีแบบคนกลางในการสื่อสารหรือการตรวจหาการดักจับที่สวิตช์เครือข่าย ARP (Address Resolution Protocol) ถูกใช้โดยแอพพลิเคชันหรืออุปกรณ์ของเครือข่ายเพื่อระบุที่อยู่อีเธอร์เน็ต
- **การตรวจหาการโจมตี TCP/UDP Port Scanning** – ตรวจหาการโจมตีซอฟต์แวร์การสแกนพอร์ตแอพพลิเคชันที่ออกแบบมาเพื่อโพรบโฮสต์สำหรับพอร์ตที่เปิดอยู่โดยการส่งคำขอของไคลเอ็นต์ไปยังช่วงของที่อยู่พอร์ต โดยมีเป้าหมายในการค้นหาพอร์ตที่เปิดใช้งานและการใช้ประโยชน์จากจุดอ่อนของบริการ อ่านเพิ่มเติมเกี่ยวกับการโจมตีประเภทนี้ได้ใน ประมวลศัพท์
- **บล็อกที่อยู่ที่ไม่ปลอดภัยหลังการตรวจหาการโจมตี** – ที่อยู่ IP ที่ถูกตรวจพบว่าเป็นแหล่งที่มาของการโจมตีจะถูกเพิ่มไปยังบัญชีดำเพื่อป้องกันการเชื่อมต่อในช่วงเวลาหนึ่ง คุณสามารถกำหนด **ระยะเวลาการเก็บรักษาบัญชีดำ** ซึ่งก็คือระยะเวลาในการบล็อกที่อยู่ หลังจากถูกตรวจพบว่าเป็นการโจมตี
- **การแจ้งเตือนเกี่ยวกับการตรวจจับการโจมตี** – เปิดการแจ้งเตือนที่พื้นที่แจ้งเตือนของ Windows ที่มุมขวาล่างสุดของหน้าจอ
- **แสดงการแจ้งเตือนยังใช้เพื่อแจ้งเมื่อมีการโจมตีจุดอ่อนด้านการรักษาความปลอดภัย** – แจ้งให้คุณทราบถ้าตรวจพบการโจมตีจุดอ่อนด้านการรักษาความปลอดภัย หรือถ้าภัยคุกคามพยายามเข้าสู่ระบบด้วยวิธีนี้

การตรวจสอบแพ็คเก็ต

- **อนุญาตการเชื่อมต่อขาเข้าไปยังการใช้การดูแลระบบร่วมกันในโปรโตคอล SMB** - การใช้การดูแลระบบร่วมกัน (admin shares) คือเครือข่ายเริ่มต้นที่ให้ใช้พาร์ติชันฮาร์ดไดรฟ์ร่วมกัน (*C$*, *D$*, ...) ในระบบพร้อมกับโฟลเดอร์ระบบ (*ADMIN$*) การปิดใช้งานการเชื่อมต่อกับการใช้การดูแลระบบร่วมกันจะช่วยลดความ

เสี่ยงทางด้านความปลอดภัยหลาย ๆ อย่างได้ ตัวอย่างเช่น เวิร์ม Conficker จะโจมตีพจนานุกรมเพื่อเชื่อมต่อกับการใช้การดูแลระบบร่วมกัน

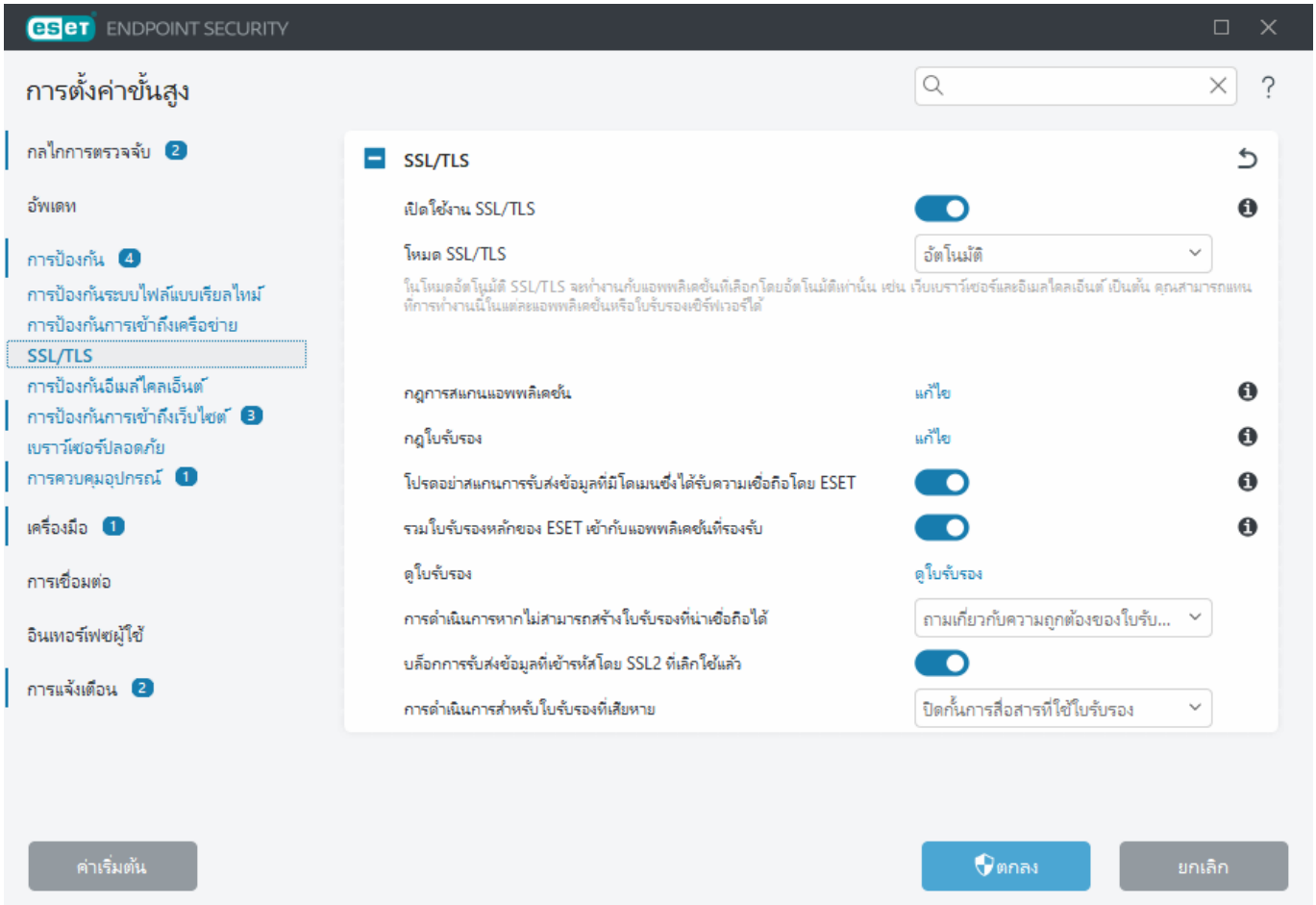
- **ปฏิเสธ SMB dialect แบบเก่า (ที่ไม่มีการสนับสนุน)** – ปฏิเสธเซสชัน SMB ที่ใช้ SMB dialect แบบเก่าที่ IDS ที่ไม่มีการสนับสนุน ระบบปฏิบัติการของ Windows ที่ทันสมัยรองรับ SMB dialect แบบเก่าเนื่องจากมีความเข้ากันได้แบบย้อนหลังกับระบบปฏิบัติการเก่า เช่น Windows 95 ผู้โจมตีสามารถใช้ dialect แบบเก่าในเซสชัน SMB เพื่อหลีกเลี่ยงการตรวจสอบข้อมูลการรับส่งได้ ปฏิเสธ SMB dialect แบบเก่าหากคอมพิวเตอร์ของคุณไม่จำเป็นต้องใช้ไฟล์ (หรือใช้การสื่อสาร SMB ทั่วไป) ร่วมกับคอมพิวเตอร์ที่มี Windows เวอร์ชันเก่า
- **ปฏิเสธเซสชัน SMB ที่ไม่มีความปลอดภัยแบบขยาย** – สามารถใช้ความปลอดภัยแบบขยายได้ในระหว่างการเจรจาของเซสชัน SMB เพื่อให้กลไกการตรวจสอบสิทธิ์มีความปลอดภัยมากกว่าการตรวจสอบสิทธิ์แบบ LAN Manager Challenge/Response (LM) โครงร่างแบบ LM ถูกพิจารณาว่าอ่อนแอและไม่แนะนำให้ใช้
- **ปฏิเสธการเปิดไฟล์ที่เรียกใช้ได้ในเซิร์ฟเวอร์ที่อยู่นอกโซนที่เชื่อถือในโปรโตคอล SMB** – ยกเลิกการเชื่อมต่อเมื่อคุณพยายามเปิดไฟล์ที่เรียกใช้ได้ (.exe, .dll เป็นต้น) จากโฟลเดอร์ที่ใช้งานร่วมกันในเซิร์ฟเวอร์ที่ไม่ได้เป็นของโซนที่เชื่อถือในไฟร์วอลล์ โปรดทราบว่าการคัดลอกไฟล์ที่เรียกใช้ได้จากแหล่งที่เชื่อถือได้นั้นถูกต้องตามกฎหมาย อย่างไรก็ตาม การตรวจหานี้จะช่วยลดความเสี่ยงจากการเปิดไฟล์ที่ไม่ต้องการในเซิร์ฟเวอร์ที่เป็นอันตราย (ตัวอย่างเช่น ไฟล์ที่เปิดด้วยการคลิกไฮเปอร์ลิงค์ไปยังไฟล์ที่เรียกใช้ได้ที่เป็นอันตรายร่วมกัน)
- **ปฏิเสธการตรวจสอบสิทธิ์ NTLM ในโปรโตคอล SMB สำหรับการเชื่อมต่อเซิร์ฟเวอร์ใน/นอกโซนที่เชื่อถือ** – โปรโตคอลที่ใช้แบบแผนการตรวจสอบสิทธิ์ NTLM (ทั้งสองเวอร์ชัน) นั้นอยู่ภายใต้การโจมตีแบบส่งต่อข้อมูลการเข้าสู่ระบบ (ที่รู้จักในชื่อการโจมตี SMB Relay ในกรณีของโปรโตคอล SMB) การปฏิเสธการตรวจสอบสิทธิ์ NTLM ที่มีเซิร์ฟเวอร์อยู่ภายนอกโซนที่เชื่อถือจะช่วยลดความเสี่ยงจากการส่งต่อข้อมูลการเข้าสู่ระบบโดยเซิร์ฟเวอร์ที่เป็นอันตรายที่อยู่ภายนอกโซนที่เชื่อถือ ในทำนองเดียวกัน คุณสามารถปฏิเสธการตรวจสอบสิทธิ์ NTLM ที่มีเซิร์ฟเวอร์ในโซนที่เชื่อถือได้

- **อนุญาตการสื่อสารกับบริการ Security Account Manager** – สำหรับข้อมูลเพิ่มเติมเกี่ยวกับบริการนี้ โปรดดู [MS-SAMR]
- **อนุญาตการสื่อสารกับบริการ Local Security Authority** – สำหรับข้อมูลเพิ่มเติมเกี่ยวกับบริการนี้ โปรดดู [MS-LSAD] และ [MS-LSAT]
- **อนุญาตการสื่อสารกับบริการรีจิสตรีระยะไกล** – สำหรับข้อมูลเพิ่มเติมเกี่ยวกับบริการนี้ โปรดดู [MS-RRP]
- **อนุญาตการสื่อสารกับบริการ Services Control Manager** – สำหรับข้อมูลเพิ่มเติมเกี่ยวกับบริการนี้ โปรดดู [MS-SCMR]

- **อนุญาตการสื่อสารกับบริการเซิร์ฟเวอร์** – สำหรับข้อมูลเพิ่มเติมเกี่ยวกับบริการนี้ โปรดดู [MS-SRVS]
- **อนุญาตการสื่อสารกับบริการอื่นๆ** – บริการ MSRPC อื่นๆ MSRPC เป็นการใช้งาน Microsoft ของกลไก DCE RPC นอกจากนี้ MSRPC สามารถใช้ไปป์ที่กำหนดชื่อที่ดำเนินการในโปรโตคอล SMB (การใช้ไฟล์ในเครือข่ายร่วมกัน) เพื่อส่ง (การส่ง ncacn_np) บริการ MSRPC ให้ส่วนติดต่อสำหรับการเข้าถึงและการจัดการระบบ Windows จากระยะไกล เราได้ค้นพบว่ามีจุดอ่อนของการรักษาความปลอดภัยหลายจุดซึ่งถูกนำไปใช้งานอย่างแพร่หลายในระบบ MSRPC ของ Windows (เวิร์ม Conficker, เวิร์ม Sasser,...) ปิดใช้งานการสื่อสารกับบริการ MSRPC ที่คุณไม่จำเป็นต้องใช้เพื่อลดความเสี่ยงด้านความปลอดภัยหลายอย่าง (เช่น การเรียกใช้รหัสทางไกลหรือการโจมตีความล้มเหลวของบริการ)

SSL/TLS

ESET Endpoint Security สามารถตรวจสอบภัยคุกคามการสื่อสารที่ใช้โปรโตคอล SSL คุณสามารถใช้โหมดการกรองต่างๆ เพื่อตรวจสอบการสื่อสารที่ป้องกันด้วย SSL ด้วยใบรับรองที่เชื่อถือ ใบรับรองที่ไม่รู้จัก หรือใบรับรองที่ถูกยกเว้นจากการตรวจสอบของการสื่อสารที่ป้องกันด้วย SSL หากต้องการแก้ไขการตั้งค่า SSL/TLS ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **SSL/TLS**



เปิดใช้งานSSL/TLS – หากปิดใช้งาน ESET Endpoint Security จะไม่สแกนการสื่อสารผ่าน SSL/TLS

โหมด SSL/TLS สามารถใช้งานได้ในตัวเลือกดังต่อไปนี้:

โหมดการกรอง	คำอธิบาย
อัตโนมัติ	โหมดเริ่มต้นจะสแกนเฉพาะแอพพลิเคชันที่เหมาะสมเท่านั้น เช่น เว็บเบราว์เซอร์และอีเมลไคลเอ็นต์ คุณสามารถแทนที่ได้โดยการเลือกแอพพลิเคชันที่มีการสแกนการสื่อสาร
แบบมีการโต้ตอบ	หากคุณเข้าสู่ไซต์ที่ป้องกันด้วย SSL ใหม่ (ที่มีใบรับรองที่ไม่รู้จัก) ระบบจะแสดงข้อความการเลือกการทำงาน โหมดนี้อนุญาตให้คุณสร้างรายการของใบรับรอง SSL / แอพพลิเคชันที่จะถูกยกเว้นจากการสแกน
อ้างอิงตามนโยบาย	โหมดนโยบาย - เลือกตัวเลือกนี้เพื่อสแกนการสื่อสารที่ป้องกันด้วย SSL ทั้งหมด ยกเว้นการสื่อสารที่ป้องกันโดยใบรับรองที่ยกเว้นจากการตรวจสอบ ถ้ามีการสร้างการสื่อสารใหม่ที่ใช้ใบรับรองที่ไม่รู้จักและลงชื่อแล้ว คุณจะไม่ได้รับแจ้ง และการสื่อสารดังกล่าวจะถูกกรองโดยอัตโนมัติ เมื่อคุณเข้าถึงเซิร์ฟเวอร์ที่มีใบรับรองที่ไม่เชื่อถือ ซึ่งได้ทำเครื่องหมายไว้ว่าน่าเชื่อถือ (ใบรับรองดังกล่าวอยู่ในรายการใบรับรองที่เชื่อถือ) ระบบจะอนุญาตให้มีการสื่อสารกับเซิร์ฟเวอร์ และเนื้อหาของช่องทางการสื่อสารจะถูกกรอง

กฎการสแกนแอพพลิเคชัน – ช่วยให้คุณสามารถปรับแต่งการทำงานของ ESET Endpoint Security สำหรับแอพพลิเคชันที่ต้องการได้

กฎการใบรับรอง – ช่วยให้คุณสามารถปรับแต่งการทำงานของ ESET Endpoint Security สำหรับใบรับรอง SSL ที่ต้องการได้

อย่าสแกนการรับส่งข้อมูลผ่านโดเมนที่ ESET เชื่อถือได้ – เมื่อเปิดใช้งาน ระบบจะแยกการสื่อสารกับโดเมนที่เชื่อถือได้ออกจากการสแกน รายการที่อนุญาตในตัวที่จัดการโดย ESET จะใช้บ่งบอกถึงความน่าเชื่อถือของโดเมน

รวมใบรับรองหลักของ ESET เข้ากับแอพพลิเคชันที่รองรับ – เพื่อให้การสื่อสาร SSL ทำงานอย่างถูกต้องในเบราว์เซอร์/อีเมลไคลเอ็นต์ของคุณ จะต้องมีการเพิ่มใบรับรองหลักสำหรับ ESET ในรายการใบรับรองหลักที่รู้จัก (ผู้เผยแพร่) เมื่อเปิดใช้งาน ESET Endpoint Security จะเพิ่มใบรับรอง ESET SSL Filter CA ลงในเบราว์เซอร์ที่รู้จักโดยอัตโนมัติ (ตัวอย่างเช่น Opera) สำหรับเบราว์เซอร์ที่ต้องใช้ที่เก็บใบรับรองของระบบ โปรแกรมจะเพิ่มใบรับรองโดยอัตโนมัติ ตัวอย่างเช่น Firefox จะกำหนดค่าการอนุญาต Trust Root ในที่เก็บใบรับรองของระบบโดยอัตโนมัติ

เมื่อต้องการใช้ใบรับรองกับเบราว์เซอร์ที่ไม่สนับสนุน ให้คลิกที่ **ดูใบรับรอง** > **รายละเอียด** > **คัดลอกไปยังไฟล์** จากนั้นนำเข้าสู่เบราว์เซอร์ด้วยตนเอง

การดำเนินการหากไม่สามารถสร้างความน่าเชื่อถือให้ใบรับรอง – ในบางกรณี ใบรับรองเว็บไซต์ไม่สามารถตรวจสอบได้โดยผู้ออกใบรับรองหลักที่เชื่อถือได้ (TRCA) (ตัวอย่างเช่น ใบรับรองหมดอายุ, ใบรับรองที่ไม่น่าเชื่อถือ, ใบรับรองไม่ถูกต้องสำหรับโดเมน หรือลายเซ็นที่สามารถแยกวิเคราะห์ได้ แต่ไม่ได้เซ็นชื่อใบรับรองอย่างถูกต้อง) เว็บไซต์ที่ถูกต้องจะใช้ใบรับรองที่เชื่อถือได้เสมอ หากเว็บไซต์ไม่ได้ให้ใบรับรอง อาจหมายความว่าผู้โจมตีกำลังถอดรหัสการสื่อสารของคุณหรือเว็บไซต์กำลังประสบปัญหาทางเทคนิค

หากเลือก **ถามเกี่ยวกับความถูกต้องของใบรับรอง** (ที่เลือกไว้ตามค่าเริ่มต้น) คุณจะได้รับข้อความให้เลือกการทำงานที่จะดำเนินการเมื่อมีการสร้างการสื่อสารที่เข้ารหัส ข้อความให้เลือกการทำงานจะปรากฏขึ้น ซึ่งคุณจะสามารถตัดสินใจได้ว่าจะทำเครื่องหมายใบรับรองเป็นเชื่อถือได้หรือยกเว้น ถ้าใบรับรองไม่ปรากฏในรายการของ TRCA หน้าต่างจะเป็น สีแดง ถ้าใบรับรองปรากฏในรายการของ TRCA หน้าต่างจะเป็น สีเขียว

คุณสามารถเลือก **ปิดกั้นการสื่อสารที่ใช้ใบรับรอง** เพื่อสิ้นสุดการเชื่อมต่อที่เข้ารหัสไปยังไซต์ที่ใช้ใบรับรองที่ไม่ได้ยืนยันเสมอ

บล็อกการรับส่งข้อมูลที่เข้ารหัสโดย SSL2 ที่ล้าสมัย การสื่อสารโดยใช้ – โปรโตคอล SSL เวอร์ชันก่อนหน้าจะถูกบล็อกโดยอัตโนมัติ

การดำเนินการสำหรับใบรับรองที่เสียหาย – ใบรับรองที่เสียหายหมายถึงใบรับรองเป็นรูปแบบที่ ESET Endpoint Security ไม่รู้จัก หรือได้รับความเสียหาย (ตัวอย่างเช่น ถูกเขียนทับโดยข้อมูลแบบสุ่ม) ในกรณีนี้ เราขอแนะนำให้ให้เลือก **ปิดกั้นการสื่อสารที่ใช้ใบรับรอง** ไว้ หากเลือก **สอบถามเกี่ยวกับความถูกต้องของใบรับรอง** ผู้ใช้จะได้รับข้อความเตือนให้เลือกการดำเนินการที่จะเกิดขึ้นเมื่อมีการสร้างการสื่อสารที่เข้ารหัส

i บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
- การแจ้งเตือนใบรับรองในผลิตภัณฑ์ ESET
- "การรับส่งข้อมูลทางเครือข่ายที่เข้ารหัส: ใบรับรองที่ไม่เชื่อถือ" จะปรากฏขึ้นเมื่อเยี่ยมชมหน้าเว็บ

กฎการสแกนแอพพลิเคชัน

กฎการสแกนแอพพลิเคชัน สามารถใช้เพื่อปรับแต่งพฤติกรรมของ ESET Endpoint Security สำหรับแอพพลิเคชันบางแอพพลิเคชัน และจดจำการดำเนินการที่เลือกเมื่อ **โหมด SSL/TLS** อยู่ใน **โหมดโต้ตอบ** คุณสามารถดูและแก้ไขรายการได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **SSL/TLS** > **กฎการสแกนแอพพลิเคชัน** > **แก้ไข**

หน้าต่าง **กฎการสแกนแอพพลิเคชัน** ประกอบด้วยส่วนต่างๆ ต่อไปนี้:

คอลัมน์

แอพพลิเคชัน – เลือกไฟล์ที่เรียกใช้ได้จากโครงสร้างไดเรกทอรี คลิกตัวเลือก **...** หรือป้อนพาธด้วยตนเอง

การดำเนินการสแกน – เลือก **สแกน** หรือ **ละเว้น** เพื่อสแกนหรือละเว้นการสื่อสาร เลือก **อัตโนมัติ** เพื่อสแกนในโหมดอัตโนมัติ และถามในโหมดที่มีการโต้ตอบ เลือก **ถาม** เพื่อถามผู้ใช้ว่าจะทำอย่างไรเสมอ

องค์ประกอบการควบคุม

เพิ่ม – เพิ่มแอพพลิเคชันที่กรอง

แก้ไข – เลือกแอพพลิเคชันที่คุณต้องการกำหนดค่าแล้วคลิก **แก้ไข**

ลบออก – เลือกแอพพลิเคชันที่คุณต้องการลบแล้วคลิก **ลบออก**

นำเข้า/ส่งออก – นำเข้าแอพพลิเคชันจากไฟล์ หรือบันทึกรายการแอพพลิเคชันปัจจุบันของคุณลงในไฟล์

OK/ยกเลิก – คลิก **OK** ถ้าคุณต้องการบันทึกการเปลี่ยนแปลง หรือคลิก**ยกเลิก** ถ้าคุณต้องการออกโดยไม่บันทึก

กฎใบรับรอง

กฎใบรับรอง สามารถใช้เพื่อปรับแต่งการทำงานของ ESET Endpoint Security สำหรับใบรับรอง SSL บางรายการ และจดจำการดำเนินการที่เลือกเมื่อ **โหมด SSL/TLS** อยู่ใน **โหมดโต้ตอบ** คุณสามารถดูและแก้ไขรายการได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **SSL/TLS** > **กฎใบรับรอง** > **แก้ไข**

หน้าต่าง **กฎใบรับรอง** ประกอบด้วยส่วนต่างๆ ดังนี้:

คอลัมน์

ชื่อ – ชื่อของใบรับรอง

ผู้ออกใบรับรอง – ชื่อของผู้สร้างใบรับรอง

หัวเรื่องของใบรับรอง – ช่องหัวเรื่องระบุถึงเอนทิตีที่เกี่ยวข้องกับคีย์สาธารณะที่เก็บไว้ในช่องหัวเรื่องคีย์สาธารณะ

การเข้าถึง – เลือก **อนุญาต** หรือ **ปิดกั้น** เป็น **ตั้งค่าการเข้าถึง** เพื่อ อนุญาต/ปิดกั้นการสื่อสารที่รักษาความปลอดภัยโดยใบรับรองนี้โดยไม่คำนึงถึงความน่าเชื่อถือของการสื่อสารนั้น เลือก **อัตโนมัติ** เพื่ออนุญาตใบรับรองที่เชื่อถือ และถามสำหรับใบรับรองที่ไม่เชื่อถือ เลือก **ถาม** เพื่อถามผู้ใช้ว่าจะทำอย่างไรเสมอ

สแกน – เลือก **สแกน** หรือ **ละเว้น** เป็น **การทำงานของการสแกน** เพื่อสแกนหรือละเว้นการสื่อสารที่รักษาความปลอดภัยโดยใบรับรองนี้ เลือก **อัตโนมัติ** เพื่อสแกนในโหมดอัตโนมัติ และถามในโหมดที่มีการโต้ตอบ เลือก **ถาม** เพื่อถามผู้ใช้ว่าจะทำอย่างไรเสมอ

องค์ประกอบการควบคุม

เพิ่ม - เพิ่มใบรับรองใหม่แล้วปรับการตั้งค่าของใบรับรองเกี่ยวกับตัวเลือกในการเข้าถึงและการสแกน

แก้ไข – เลือกใบรับรองที่คุณต้องการกำหนดค่าแล้วคลิก **แก้ไข**

ลบ – เลือกใบรับรองที่คุณต้องการลบแล้วคลิก **ลบออก**

OK/ยกเลิก – คลิก **OK** ถ้าคุณต้องการบันทึกการเปลี่ยนแปลง หรือคลิก**ยกเลิก** ถ้าคุณต้องการออกโดยไม่บันทึก

การรับส่งข้อมูลทางเครือข่ายที่เข้ารหัส

หากระบบของคุณได้รับการกำหนดค่าให้ใช้การสแกน SSL/TLS ระบบจะแสดงหน้าต่างข้อความให้คุณเลือกการดำเนินการปรากฏขึ้นมาในสองสถานการณ์ ได้แก่:

สถานการณ์แรก ถ้าเว็บไซต์ใช้ใบรับรองที่ไม่สามารถตรวจสอบได้หรือไม่ถูกต้อง และ ESET Endpoint Security ได้รับการกำหนดค่าให้ถามผู้ใช้ในกรณีดังกล่าว (ตามค่าเริ่มต้น ใช่สำหรับใบรับรองที่ไม่สามารถตรวจสอบได้ ไม่สำหรับใบรับรองที่ไม่ถูกต้อง) กล่องข้อความจะถามคุณว่าคุณต้องการ **อนุญาต** หรือ **ปิดกั้น** การเชื่อมต่อนั้น หากใบรับรองไม่ได้อยู่ใน Trusted Root Certification Authorities store (TRCA) จึงสามารถพิจารณาได้ว่าไม่เชื่อถือ

สถานการณ์ที่สอง หาก**โหมด SSL/TLS** ถูกตั้งค่าเป็น **โหมดโต้ตอบ** กล่องข้อความของแต่ละเว็บไซต์จะถามว่าจะ **สแกน** หรือ **ละเว้น** การรับส่งข้อมูล บางแอพพลิเคชันตรวจสอบว่าการรับส่งข้อมูล SSL ของตนไม่ได้รับการแก้ไขหรือตรวจสอบจากผู้ใดเลย ในกรณีนี้ ESET Endpoint Security ต้อง **ละเว้น** การรับส่งข้อมูลดังกล่าวและปล่อยให้แอพพลิเคชันทำงาน

> **ตัวอย่างพร้อมภาพประกอบ**
> บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
> - การแจ้งเตือนใบรับรองในผลิตภัณฑ์ ESET บน Windows
> - "การรับส่งข้อมูลทางเครือข่ายที่เข้ารหัส: ใบรับรองที่ไม่เชื่อถือ" จะปรากฏขึ้นเมื่อเยี่ยมชมหน้าเว็บ

ในทั้งสองกรณี ผู้ใช้สามารถเลือกที่จะจดจำการทำงานที่เลือกได้ การดำเนินการที่บันทึกไว้จะถูกเก็บไว้ใน กฎของใบรับรอง

การป้องกันอีเมลไคลเอ็นต์

หากต้องการกำหนดค่าการป้องกันอีเมลไคลเอ็นต์ ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันอีเมลไคลเอ็นต์** และเลือกตัวเลือกการกำหนดค่าต่อไปนี้:

- การป้องกันการส่งข้อมูลอีเมล
- การป้องกันกล่องจดหมาย
- การจัดการรายการที่อยู่
- ThreatSense

การป้องกันการส่งข้อมูลอีเมล

โปรโตคอล IMAP(S) และ POP3(S) เป็นโปรโตคอลที่ใช้งานกันอย่างแพร่หลาย เพื่อรับการสื่อสารทางอีเมลในแอพพลิเคชันอีเมลไคลเอ็นต์ Internet Message Access Protocol (IMAP) เป็นโปรโตคอลอินเทอร์เน็ตหนึ่งสำหรับการเรียกคืนอีเมล IMAP มีข้อได้เปรียบบางอย่างที่เหนือกว่า POP3 ตัวอย่างเช่น หลายไคลเอ็นต์สามารถเชื่อมต่อพร้อมกันได้ในกล่องจดหมายเดียวกัน และรักษาข้อมูลสถานะของข้อความ เช่น อ่านข้อความหรือยัง ตอบกลับแล้วหรือยัง หรือลบข้อความแล้วหรือยัง โมดูลการป้องกันที่มอบการควบคุมนี้จะเริ่มต้นโดยอัตโนมัติเมื่อมีการเริ่มต้นระบบ จากนั้นจะทำงานในหน่วยความจำ

ESET Endpoint Security มีการป้องกันโปรโตคอลเหล่านี้ โดยไม่พิจารณาถึงอีเมลไคลเอ็นต์ที่ใช้ และไม่ได้กำหนดให้ต้องกำหนดค่าอีเมลไคลเอ็นต์อีกครั้ง ตามค่าเริ่มต้น การติดต่อสื่อสารผ่านโปรโตคอล POP3 และ IMAP ทั้งหมดจะถูกสแกน โดยไม่คำนึงถึงค่าเริ่มต้นหมายเลขพอร์ต POP3/IMAP
โปรโตคอล MAPI ไม่ถูกสแกน อย่างไรก็ตาม การสื่อสารกับเซิร์ฟเวอร์ Microsoft Exchange สามารถสแกนได้โดยใช้โมดูลการรวม ในอีเมลไคลเอ็นต์ เช่น Microsoft Outlook

> ESET Endpoint Security ยังสนับสนุนการสแกนโปรโตคอล IMAPS (585, 993) และ POP3S (995) ที่จะใช้ช่องทางที่เข้ารหัสเพื่อโอนข้อมูลระหว่างเซิร์ฟเวอร์กับไคลเอ็นต์ ESET Endpoint Security จะตรวจสอบการสื่อสารโดยใช้โปรโตคอล SSL (Secure Socket Layer) และ TLS (Transport Layer Security)
> การสื่อสารที่เข้ารหัสจะถูกสแกนตามค่าเริ่มต้น หากต้องการดูการตั้งค่าเครื่องมือสแกน ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > SSL/TLS

หากต้องการกำหนดค่าการป้องกันการส่งข้อมูลอีเมล ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันอีเมลไคลเอ็นต์** > **การป้องกันการส่งข้อมูลอีเมล**

เปิดใช้งานการป้องกันการส่งข้อมูลอีเมล – เมื่อเปิดใช้งาน ESET Endpoint Security จะสแกนการส่งข้อมูลอีเมล

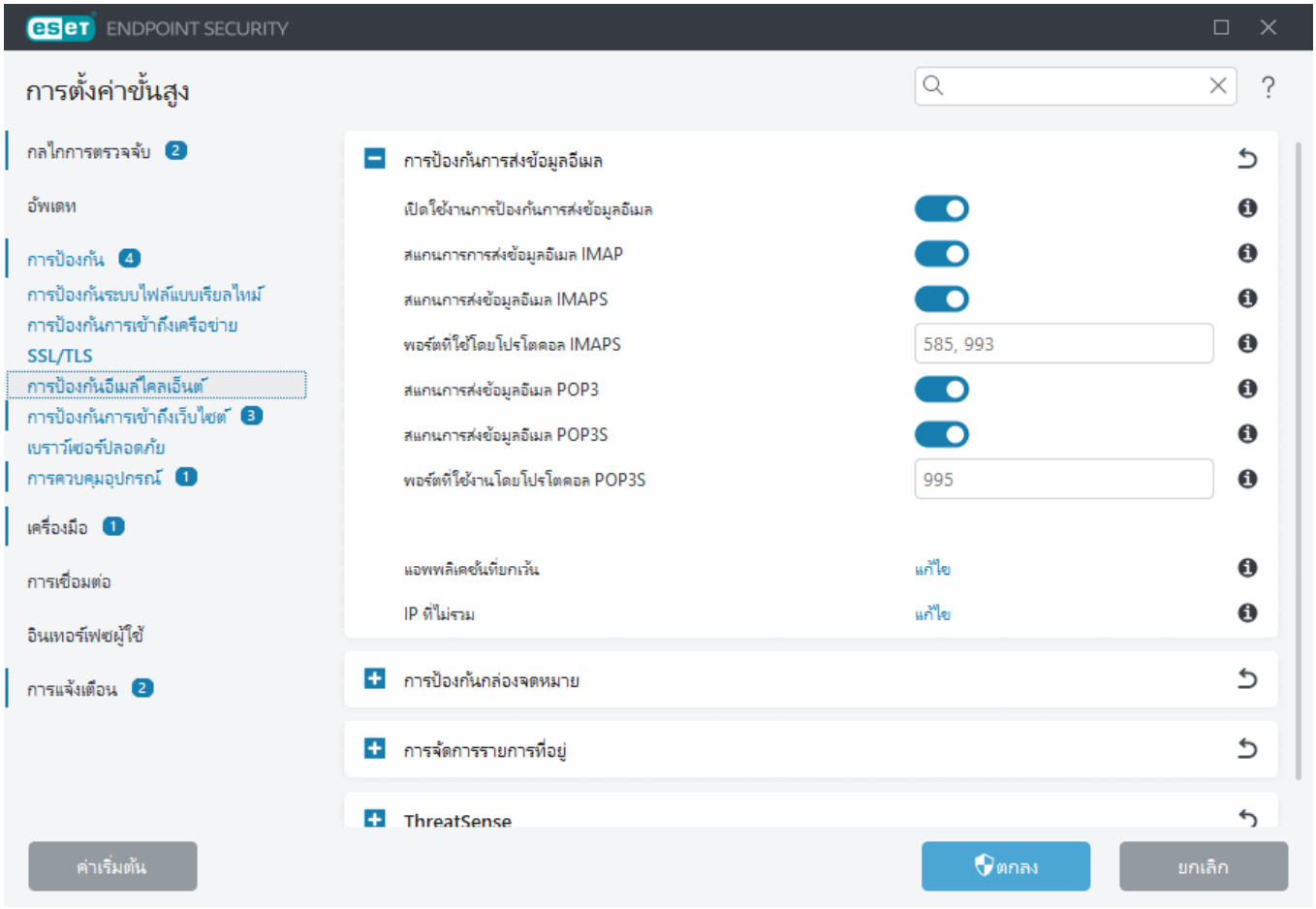
คุณสามารถเลือกโปรโตคอลการส่งจดหมายที่ต้องการสแกนได้โดยคลิกปุ่มสลับถัดจากตัวเลือกต่อไปนี้ (ระบบจะสแกนโปรโตคอลทั้งหมดตามค่าเริ่มต้น):

- **สแกนการการส่งข้อมูลอีเมล IMAP**
- **สแกนการส่งข้อมูลอีเมล IMAPS**
- **สแกนการส่งข้อมูลอีเมล POP3**
- **สแกนการส่งข้อมูลอีเมล POP3S**

โดยค่าเริ่มต้น, ESET Endpoint Security จะสแกนการส่งข้อมูลแบบ IMAPS และ POP3S บนพอร์ตมาตรฐาน หากต้องการเพิ่มพอร์ตที่กำหนดเองสำหรับโปรโตคอล IMAPS และ POP3S ให้เพิ่มพอร์ตเหล่านั้นลงในช่องถัดจาก **พอร์ตที่ใช้โดยโปรโตคอล IMAPS** หรือ **พอร์ตที่ใช้โดยโปรโตคอล POP3S** เลขที่พอร์ตหลายเลขที่ต้องคั่นด้วยเครื่องหมายคอมมา

แอพพลิเคชันที่ยกเว้น – ช่วยให้คุณสามารถแยกแอพพลิเคชันบางแอพออกจากการสแกนโดยฟีเจอร์การป้องกันการส่งข้อมูลอีเมลได้ ซึ่งจะมีประโยชน์เมื่อการป้องกันการเข้าถึงเว็บไซต์ทำให้เกิดปัญหาด้านความเข้ากันได้

IP ที่ยกเว้น – ช่วยให้คุณสามารถแยกที่อยู่ระยะไกลที่ต้องการออกจากการสแกนโดยการป้องกันการส่งข้อมูลอีเมล ซึ่งจะมีประโยชน์เมื่อการป้องกันการเข้าถึงเว็บไซต์ทำให้เกิดปัญหาความเข้ากันได้



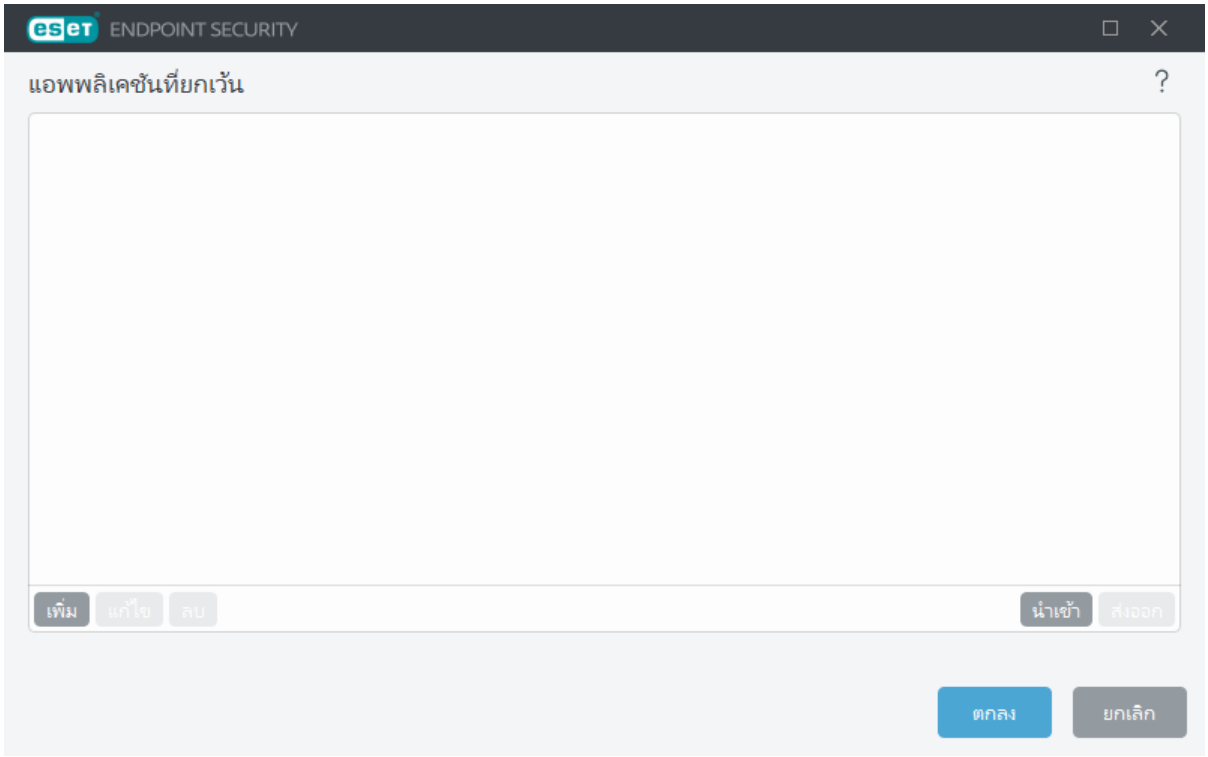
แอพพลิเคชันที่ยกเว้น

หากต้องการยกเว้นการสแกนการรับส่งข้อมูลสำหรับบางแอพพลิเคชันโดยเฉพาะ ให้เพิ่มแอพนั้นลงในรายการ การสื่อสารของ HTTP(S)/POP3(S)/IMAP(S) ของแอพพลิเคชันที่เลือกจะไม่ได้รับการตรวจสอบเพื่อหาภัยคุกคาม เราขอแนะนำให้ใช้ตัวเลือกนี้เฉพาะสำหรับแอพพลิเคชันที่ทำงานได้อย่างไม่ถูกต้องและการสื่อสารของแอพพลิเคชันเหล่านั้นกำลังถูกสแกนอยู่

แอพพลิเคชันและบริการที่ทำงานอยู่จะสามารถใช้งานได้ที่นี่โดยอัตโนมัติเมื่อคุณคลิก **เพิ่ม** คลิก **...** และไปยังแอพพลิเคชันเพื่อเพิ่มการยกเว้นด้วยตนเอง

แก้ไข – แก้ไขรายการที่เลือกจากรายการ

ลบออก – ลบรายการที่เลือกออกจากรายการ



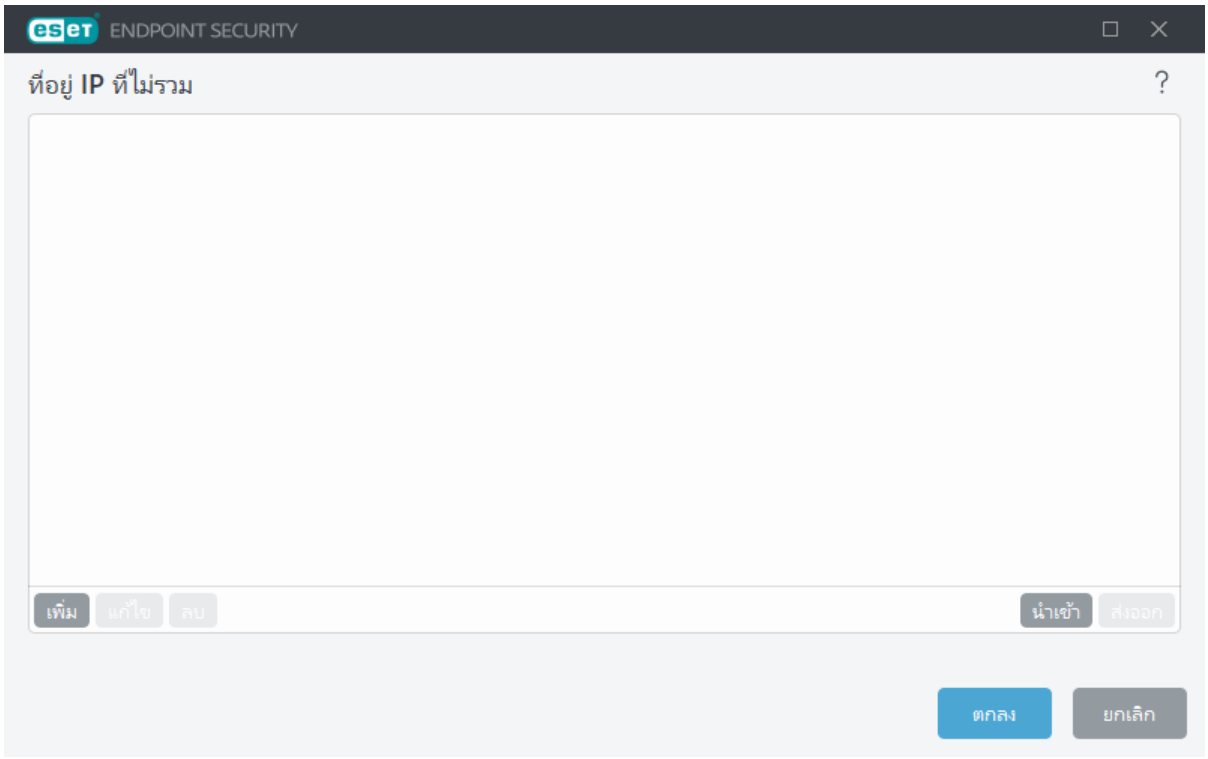
IP ที่ไม่รวม

รายการที่อยู่ในรายการจะถูกยกเว้นจากการสแกน การสื่อสารของ HTTP(S)/POP3(S)/IMAP(S) จาก/ไปยังที่อยู่ที่เลือกจะไม่ได้รับการตรวจสอบเพื่อหาภัยคุกคาม เราขอแนะนำให้คุณใช้ตัวเลือกนี้เฉพาะสำหรับที่อยู่ที่ทราบว่าเชื่อถือได้เท่านั้น

เพิ่ม - คลิกเพื่อเพิ่มที่อยู่ IP/ช่วงที่อยู่/ซับเน็ต ให้กับจุดระยะไกลซึ่งมีการใช้กฎ

แก้ไข – แก้ไขรายการที่เลือกจากรายการ

ลบออก – ลบรายการที่เลือกออกจากรายการ



ตัวอย่างที่อยู่ IP

เพิ่มที่อยู่ IPv4:

ที่อยู่เดี่ยว – เพิ่มที่อยู่ IP ของคอมพิวเตอร์แต่ละเครื่อง (ตัวอย่างเช่น *192.168.0.10*)

ช่วงที่อยู่ – ป้อนที่อยู่ IP แรกและสุดท้ายเพื่อระบุช่วง IP ของคอมพิวเตอร์หลายเครื่อง (ตัวอย่างเช่น *192.168.0.1-192.168.0.99*)

✓ **ซับเน็ต** - ซับเน็ต (กลุ่มของคอมพิวเตอร์) กำหนดโดยที่อยู่ IP และมาสก์ ตัวอย่างเช่น 255.255.255.0 เป็นมาสก์เครือข่ายสำหรับซับเน็ต 192.168.1.0 เพื่อแยกประเภทซับเน็ตทั้งหมดใน *192.168.1.0/24*

เพิ่มที่อยู่ IPv6:

ที่อยู่เดี่ยว – เพิ่มที่อยู่ IP ของคอมพิวเตอร์แต่ละเครื่อง (ตัวอย่างเช่น *2001:718:1c01:16:214:22ff:fec9:ca5*):

ซับเน็ต - ซับเน็ต (กลุ่มของคอมพิวเตอร์) กำหนดโดยที่อยู่ IP และมาสก์ (ตัวอย่างเช่น: *2002:c0a8:6301:1::1/64*)

การป้องกันกล่องจดหมาย

การผสานการทำงาน ESET Endpoint Security กับกล่องจดหมายจะเพิ่มระดับการป้องกันโค้ดที่เป็นอันตรายในข้อความอีเมล

หากต้องการกำหนดค่าการป้องกันกล่องจดหมาย ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันอีเมลไคลเอ็นต์** > **การป้องกันกล่องจดหมาย**

เปิดใช้งานการปกป้องอีเมลโดยปลั๊กอินไคลเอ็นต์ – เมื่อปิดใช้งาน การป้องกันโดยอีเมลปลั๊กอินไคลเอ็นต์จะปิด

เลือกอีเมลที่จะสแกน:

- **อีเมลที่ได้รับ**
- **อีเมลที่ส่ง**
- **อีเมลที่อ่าน**
- **อีเมลที่มีการแก้ไข**

> เราขอแนะนำให้คุณเปิดใช้งาน **เปิดใช้งานการปกป้องอีเมลโดยปลั๊กอินไคลเอ็นต์** ไว้ แม้ว่าการผสานการทำงานจะไม่ได้เปิดใช้หรือทำงานอยู่ การสื่อสารทางอีเมลจะยังคงได้รับการป้องกันจาก การป้องกันการส่งข้อมูลอีเมล (IMAP/IMAPS และ POP3/POP3S)

สแกนหาสแปม

อีเมลที่ไม่พึงประสงค์ หรือสแปม จัดเป็นปัญหาการสื่อสารทางอิเล็กทรอนิกส์ลำดับต้นๆ โดยมีสัดส่วนร้อยละ 30 ของการสื่อสารทางอีเมลทั้งหมด ฟีเจอร์การป้องกันสแปมอีเมลไคลเอ็นต์จะทำหน้าที่ป้องกันปัญหานี้ การป้องกันสแปมอีเมลไคลเอ็นต์เป็นการกรองข้อมูลที่มีประสิทธิภาพ เพื่อทำให้กล่องขาเข้ามีความปลอดภัย เนื่องจากรวมหลักการรักษาความปลอดภัยอีเมลแบบต่างๆ ไว้ด้วยกัน สำหรับการตรวจหาสแปม หลักการสำคัญอย่างหนึ่งคือการจดจำอีเมลที่ไม่พึงประสงค์จากที่อยู่ที่เชื่อถือ (อนุญาตแล้ว) และที่อยู่สแปม (บล็อกแล้ว) ที่กำหนดไว้ล่วงหน้า

วิธีหลักที่ใช้เพื่อตรวจหาสแปมคือ การสแกนคุณสมบัติของข้อความอีเมล ระบบจะสแกนข้อความที่ได้รับตามเกณฑ์การป้องกันสแปมขั้นพื้นฐาน (การกำหนดข้อความ, การวิเคราะห์พฤติกรรมแบบสถิติ อัลกอริทึมในการรับรู้ และวิธีเฉพาะอื่นๆ) และค่าดัชนีผลลัพธ์จะเป็นตัวกำหนดว่าข้อความเป็นสแปมหรือไม่

เปิดใช้งานการป้องกันสแปมอีเมลไคลเอ็นต์ – เมื่อเปิดใช้งาน ระบบจะสแกนหาสแปมจากข้อความที่ได้รับ

ใช้เครื่องมือสแกนสแปมขั้นสูง – จะมีการดาวน์โหลดข้อมูลป้องกันสแปมเพิ่มเติมเป็นระยะๆ เพื่อเพิ่มความสามารถในการป้องกันสแปมและให้ผลลัพธ์ที่ดีขึ้น

การบันทึกคะแนนสแปม – กลไกการป้องกันสแปมของ ESET Endpoint Security จะระบุคะแนนสแปมไปที่ข้อความที่สแกนแล้วทุกข้อความ โดยข้อความจะถูกบันทึกไว้ใน บันทึกการป้องกันสแปม (หน้าต่างโปรแกรมหลัก > **เครื่องมือ** > **ไฟล์บันทึก** > **การป้องกันสแปมอีเมลไคลเอ็นต์**)

- **ไม่มี** – คะแนนจากการสแกนเพื่อป้องกันสแปมจะไม่ถูกบันทึก
- **จัดประเภทใหม่และทำเครื่องหมายว่าเป็นสแปม** – เลือกตัวเลือกนี้ถ้าคุณต้องการบันทึกคะแนนสแปม

สำหรับข้อความที่ทำเครื่องหมายว่าเป็น SPAM.

- **ทั้งหมด** - ข้อความทั้งหมดจะได้รับการบันทึกไปที่บันทึกพร้อมด้วยคะแนนสแปม

> เมื่อคุณคลิกข้อความในโฟลเดอร์อีเมลขยะ คุณสามารถเลือก **จัดประเภทข้อความที่เลือกใหม่ว่าไม่เป็นสแปม** และข้อความจะถูกย้ายไปที่กล่องข้อความเข้า เมื่อคุณคลิกข้อความที่คุณคิดว่าเป็นสแปมในกล่องข้อความเข้า ให้เลือก **จัดประเภทข้อความใหม่เป็นสแปม** และข้อความจะถูกย้ายไปที่โฟลเดอร์อีเมลขยะ คุณสามารถเลือกหลายๆ ข้อความและดำเนินการกับทุกข้อความพร้อมกันได้

การผสานการทำงาน – ช่วยให้คุณสามารถผสานการป้องกันกล่องจดหมายเข้ากับอีเมลไคลเอ็นต์ของคุณได้ ดูข้อมูลเพิ่มเติมได้ที่ การผสานการทำงาน

การตอบสนอง – ช่วยให้คุณปรับแต่งการจัดการข้อความสแปมได้ ดูรายละเอียดเพิ่มเติมได้ที่ การตอบสนอง

การรวม

การรวม ESET Endpoint Security กับอีเมลไคลเอ็นต์ของคุณจะเพิ่มระดับการป้องกันรหัสที่เป็นอันตรายในข้อความอีเมล หากอีเมลไคลเอ็นต์ของคุณได้รับการรองรับ คุณสามารถเปิดใช้งานการรวมใน ESET Endpoint Security ได้ เมื่อรวมเข้าอีเมลไคลเอ็นต์ของคุณ แถบเครื่องมือของ ESET Endpoint Security จะถูกแทรกลงในอีเมลไคลเอ็นต์ โดยตรง ซึ่งจะทำให้การป้องกันอีเมลมีประสิทธิภาพมากยิ่งขึ้น เมื่อต้องการแก้ไขการตั้งค่าการผสานการทำงาน ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันอีเมลไคลเอ็นต์** > **การป้องกันกล่องจดหมาย** > **การผสานการทำงาน**

รวมเข้ากับ Microsoft Outlook – ขณะนี้ Microsoft Outlook เป็นอีเมลไคลเอ็นต์เดียวที่ได้รับการรองรับเท่านั้น การป้องกันอีเมลทำงานเป็นปลั๊กอิน ประโยชน์สำคัญของปลั๊กอินคือ การทำงานที่ไม่ขึ้นอยู่กับโปรโตคอลที่ใช้ เมื่ออีเมลไคลเอ็นต์ได้รับข้อความที่เข้ารหัส ระบบจะดำเนินการถอดรหัสและส่งไปยังเครื่องมือสแกนไวรัส โปรดดู บทความฐานความรู้ของ ESET สำหรับรายการเวอร์ชัน Microsoft Outlook ที่รองรับทั้งหมด

การประมวลผลอีเมลไคลเอ็นต์ขั้นสูง – ประมวลผล เหตุการณ์พิเศษของ Outlook Messaging API (MAPI) ได้แก่: วัตถุที่มีการแก้ไข (`fnevObjectModified`) และวัตถุที่สร้างขึ้น (`fnevObjectCreated`) หากคุณพบว่าระบบหน่วงช้าลงเมื่อทำงานกับอีเมลไคลเอ็นต์ของคุณที่ปิดใช้งานตัวเลือกนี้แล้ว

แถบเครื่องมือ Microsoft Outlook

การป้องกัน Microsoft Outlook ทำงานเป็นโมดูลปลั๊กอิน หลังจากติดตั้ง ESET Endpoint Security แล้ว แถบเครื่องมือนี้จะได้รับการป้องกันไวรัส และจะมีการเพิ่มตัวเลือกการป้องกันสแปมอีเมลไคลเอ็นต์ ลงใน Microsoft Outlook:

สแปม – ทำเครื่องหมายข้อความที่เลือกว่าเป็นสแปม หลังจากที่ทำเครื่องหมาย "ลักษณะเฉพาะ" ของข้อความจะถูกส่งไปยังเซิร์ฟเวอร์ส่วนกลางที่เก็บฐานข้อมูลของสแปม ถ้าเซิร์ฟเวอร์ได้รับ "ลักษณะเฉพาะ" ที่คล้ายกันเพิ่มเติมจากผู้ใช้หลายราย ข้อความนั้นจะถูกจัดเป็นสแปมในอนาคต

ไม่ใช่สแปม – ทำเครื่องหมายข้อความที่เลือกว่าไม่ใช่สแปม

ที่อยู่สแปม (ถูกบล็อก ซึ่งเป็นรายการของที่อยู่สแปม) – เพิ่มที่อยู่ผู้ส่งใหม่ใน รายการที่อยู่ เป็นที่อยู่ที่ถูกบล็อก ข้อความทั้งหมดที่ได้รับจากรายการนี้จะถูกจัดเป็นสแปมโดยอัตโนมัติ

โปรดระมัดระวัง การแอบอ้าง – การปลอมแปลงที่อยู่ของผู้ส่งในข้อความอีเมลเพื่อทำให้ผู้รับอีเมลเข้าใจผิดไปอ่านและตอบกลับข้อความนั้น

ที่อยู่ที่เชื่อถือ (อนุญาต ซึ่งเป็นรายการของที่อยู่ที่เชื่อถือ) – เพิ่มที่อยู่ผู้ส่งใหม่ใน รายการที่อยู่ เป็นที่อยู่ที่อนุญาต ข้อความทั้งหมดที่ได้รับจากที่อยู่ที่อนุญาตจะไม่ถูกจัดเป็นสแปมโดยอัตโนมัติ

ESET Endpoint Security – ดับเบิลคลิกที่ไอคอนเพื่อเปิดหน้าต่างหลักของ ESET Endpoint Security

สแกนข้อความซ้ำ – ช่วยให้คุณสามารถเริ่มต้นการตรวจสอบอีเมลด้วยตนเองได้ คุณสามารถระบุข้อความที่จะตรวจสอบ และคุณสามารถเปิดใช้การสแกนซ้ำอีเมลที่ได้รับ ดูข้อมูลเพิ่มเติมได้ที่ การป้องกันกล่องจดหมาย

การตั้งค่าเครื่องมือสแกน – แสดงตัวเลือกการตั้งค่า การป้องกันกล่องจดหมาย

การตั้งค่าป้องกันสแปม – แสดงตัวเลือกการตั้งค่า การป้องกันกล่องจดหมาย

รายการที่อยู่การป้องกันสแปม – เปิดหน้าต่าง การจัดการรายการที่อยู่ ซึ่งคุณจะสามารถเข้าถึงรายการของที่อยู่ที่ยกเว้น เชื่อถือ และที่เป็นสแปมได้

ข้อความยืนยัน

การแจ้งเตือนนี้จะทำหน้าที่ตรวจสอบว่าผู้ใช้ต้องการดำเนินการที่เลือกจริงหรือไม่ ซึ่งจะช่วยป้องกันการดำเนินการผิดพลาดได้

แต่ในหน้าต่างข้อความนี้จะมีตัวเลือกเพื่อปิดใช้การยืนยันอยู่ด้วย

สแกนข้อความซ้ำ

แถบเครื่องมือของ ESET Endpoint Security ที่รวมอยู่ในอีเมลไคลเอ็นต์จะช่วยให้ผู้ใช้สามารถระบุตัวเลือกต่างๆ สำหรับการตรวจสอบอีเมลได้ ตัวเลือก **สแกนข้อความซ้ำ** มีโหมดการสแกนอยู่สองโหมด:

ข้อความทั้งหมดในโฟลเดอร์ปัจจุบัน – สแกนข้อความในโฟลเดอร์ที่แสดงอยู่ในปัจจุบัน

เฉพาะข้อความที่เลือก – สแกนเฉพาะข้อความที่ผู้ใช้ทำเครื่องหมายเท่านั้น

ช่องทำเครื่องหมาย **สแกนข้อความที่สแกนแล้วซ้ำ** จะมีตัวเลือกให้ผู้ใช้สามารถเรียกใช้การสแกนข้อความที่ได้สแกนแล้วก่อนหน้านี้

การตอบกลับ

ESET Endpoint Security สามารถย้ายข้อความที่สแกนหรือเพิ่มข้อความที่กำหนดเองไปยังหัวเรื่องได้ โดยขึ้นอยู่กับผลการสแกนข้อความ คุณสามารถกำหนดการตั้งค่าเหล่านี้ได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันอีเมลไคลเอ็นต์** > **การป้องกันกล่องจดหมาย** > **การตอบกลับ**

การป้องกันสแปมอีเมลไคลเอ็นต์ใน ESET Endpoint Security ช่วยให้คุณสามารถกำหนดค่าพารามิเตอร์สำหรับข้อความต่อไปนี้ได้:

เพิ่มข้อความในหัวเรื่องอีเมล – ช่วยให้คุณสามารถเพิ่มสตริงคำนำหน้าที่กำหนดเองในบรรทัดหัวเรื่องของข้อความซึ่งจัดประเภทว่าเป็นสแปม **ข้อความ** เริ่มต้นคือ "[SPAM]"

ย้ายไปยังโฟลเดอร์สแปม – เมื่อเปิดใช้งาน ข้อความสแปมจะถูกย้ายไปยังโฟลเดอร์อีเมลขยะเริ่มต้น และข้อความที่จัดประเภทใหม่ว่าไม่ใช่สแปมจะถูกย้ายไปที่กล่องข้อความเข้า เมื่อคุณคลิกขวาที่ข้อความอีเมลและเลือก ESET Endpoint Security จากเมนูบริบท คุณจะสามารถเลือกจากตัวเลือกที่มีผลบังคับใช้

ย้ายไปยังโฟลเดอร์ที่กำหนดเอง – เมื่อเปิดใช้งานข้อความสแปมจะถูกย้ายไปยังโฟลเดอร์ที่ระบุไว้ด้านล่าง

โฟลเดอร์ – ระบุโฟลเดอร์แบบกำหนดเองที่คุณต้องการย้ายอีเมลที่ติดไวรัสเมื่อตรวจพบ

หากมีข้อความที่มีการพบไวรัส โดยค่าเริ่มต้น ESET Endpoint Security จะพยายามกำจัดไวรัสในข้อความดังกล่าว หากไม่สามารถกำจัดไวรัสในข้อความได้ คุณสามารถเลือก **การดำเนินการหากไม่สามารถกำจัดไวรัสได้** จากตัวเลือกต่อไปนี้:

- **ไม่มีการทำงาน** – ถ้าเลือกตัวเลือกนี้ โปรแกรมจะระบุสิ่งที่แนบมาที่ติดไวรัส แต่จะคงอีเมลไว้โดยไม่ดำเนินการใดๆ
- **ลบอีเมล** – โปรแกรมจะแจ้งให้ผู้ใช้ทราบเกี่ยวกับการแฝงตัว และลบข้อความ
- **ย้ายอีเมลไปยังโฟลเดอร์รายการที่ถูกลบ** – โปรแกรมจะย้ายอีเมลที่ติดไวรัสไปยังโฟลเดอร์รายการที่ถูกลบโดยอัตโนมัติ
- **ย้ายอีเมลไปยังโฟลเดอร์** (การกระทำที่เป็นค่าเริ่มต้น) – อีเมลที่ติดไวรัสจะถูกย้ายไปยังโฟลเดอร์ที่ระบุโดยอัตโนมัติ

โฟลเดอร์ – ระบุโฟลเดอร์แบบกำหนดเองที่คุณต้องการย้ายอีเมลที่ติดไวรัสเมื่อตรวจพบ

ทำเครื่องหมายข้อความสแปมว่าอ่านแล้ว – เปิดใช้งานตัวเลือกนี้เพื่อทำเครื่องหมายสแปมว่าอ่านแล้วโดยอัตโนมัติ การทำเช่นนี้จะช่วยให้คุณให้ความสนใจกับข้อความที่ "ไม่ติดไวรัส" เท่านั้น

ทำเครื่องหมายข้อความที่จัดประเภทใหม่ว่ายังไม่ได้อ่าน – ข้อความเดิมที่จัดประเภทเป็นสแปม แต่ทำเครื่องหมายว่า "ไม่ติดไวรัส" ในภายหลัง จะแสดงเป็นข้อความที่ยังไม่ได้อ่าน

หลังจากตรวจสอบอีเมลแล้ว ระบบสามารถแสดงการแจ้งเตือนที่มีผลลัพธ์การสแกนต่อท้ายข้อความ คุณสามารถเลือกเพื่อ **เพิ่มข้อความแท็กต่อท้ายอีเมลที่ได้รับหรืออ่านแล้ว** หรือ **เพิ่มข้อความแท็กต่อท้ายอีเมลที่ส่ง** โปรดทราบว่า ในบางสถานการณ์ ข้อความแท็กอาจไม่ปรากฏในข้อความ HTML ที่เป็นปัญหา หรือถ้าข้อความถูกปลอมแปลงโดยมัลแวร์ คุณสามารถเพิ่มข้อความแท็กไว้ในอีเมลที่ได้รับและอีเมลที่อ่านแล้ว หรือในอีเมลที่ส่ง หรือทั้งสองอย่าง ตัวเลือกที่ใช้ได้มีดังนี้:

- **ไม่** - ไม่มีการเพิ่มข้อความแท็ก
- **เมื่อการตรวจหาเกิดขึ้น** – โปรแกรมจะทำเครื่องหมายเฉพาะข้อความที่มีซอฟต์แวร์ที่เป็นอันตรายว่าตรวจสอบแล้ว (ค่าเริ่มต้น)
- **ไปยังอีเมลทุกฉบับเมื่อสแกน** – โปรแกรมจะเพิ่มข้อความต่อท้ายอีเมลที่สแกนทั้งหมด

อัพเดทหัวเรื่องอีเมลที่ได้รับและอ่านแล้ว/ อัพเดทหัวเรื่องของอีเมลที่ส่งแล้ว – เปิดใช้งานตัวเลือกนี้เพื่อเพิ่มข้อความที่กำหนดเองที่ระบุไว้ด้านล่างลงในข้อความ

ข้อความที่จะเพิ่มลงในหัวเรื่องของอีเมลที่ตรวจพบ – แก้ไขแม่แบบนี้หากคุณต้องการแก้ไขรูปแบบคำนำหน้าของหัวเรื่องของอีเมลที่ติดไวรัส ฟังก์ชันนี้จะแทนที่หัวเรื่องของความ "สวัสดี" ด้วยรูปแบบต่อไปนี้: "สวัสดี [ชื่อการตรวจพบไวรัส]" ตัวแปร %DETECTIONNAME% จะแสดงแทนการตรวจหา

การจัดการรายการที่อยู่

ฟีเจอร์การป้องกันสแปมอีเมลไคลเอ็นต์ใน ESET Endpoint Security ช่วยให้คุณสามารถกำหนดค่าพารามิเตอร์ต่างๆ สำหรับรายการที่อยู่ หากต้องการกำหนดค่ารายการที่อยู่ ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันอีเมลไคลเอ็นต์** > **การจัดการรายการที่อยู่**

เปิดใช้งานรายการที่อยู่ของผู้ใช้ – เปิดใช้งานตัวเลือกนี้เพื่อเปิดใช้งานรายการที่อยู่ของผู้ใช้

รายการที่อยู่ของผู้ใช้ – รายการที่อยู่อีเมลที่คุณสามารถเพิ่ม แก้ไข หรือลบที่อยู่เพื่อกำหนดกฎการป้องกันสแปมได้ กฎในรายการนี้จะถูกนำไปใช้กับผู้ใช้ปัจจุบัน

เปิดใช้งานรายการที่อยู่ร่วม – เปิดใช้งานตัวเลือกนี้เพื่อเปิดใช้งานรายการที่อยู่ร่วมซึ่งใช้ร่วมกันโดยผู้ใช้ทั้งหมดในอุปกรณ์เครื่องนี้

รายการที่อยู่ร่วม – รายการที่อยู่อีเมลที่คุณสามารถเพิ่ม แก้ไข หรือลบที่อยู่เพื่อกำหนดกฎการป้องกันสแปมได้ กฎในรายการนี้จะถูกนำไปใช้กับผู้ใช้ทั้งหมด

อนุญาตและเพิ่มไปยังรายการที่อยู่ของผู้ใช้โดยอัตโนมัติ

ถือว่าที่อยู่ต่างๆ จากสมุดที่อยู่เป็นแบบเชื่อถือได้ - ที่อยู่จากรายการติดต่อของคุณจะถือว่าเชื่อถือได้โดยไม่มีการเพิ่มลงในรายการที่ผู้ใช้อนุญาต

เพิ่มที่อยู่ของผู้รับจากข้อความขาออก – เพิ่มที่อยู่ของผู้รับจากข้อความที่ส่งไปยังรายการที่อยู่ของผู้ใช้เป็นอนุญาตแล้ว

เพิ่มที่อยู่จากข้อความที่จัดประเภทใหม่ว่าไม่ใช่สแปม – เพิ่มที่อยู่ของผู้ส่งจากข้อความที่จัดประเภทใหม่ว่าไม่ใช่สแปมไปยังรายการที่อยู่ของผู้ใช้เป็น อนุญาตแล้ว

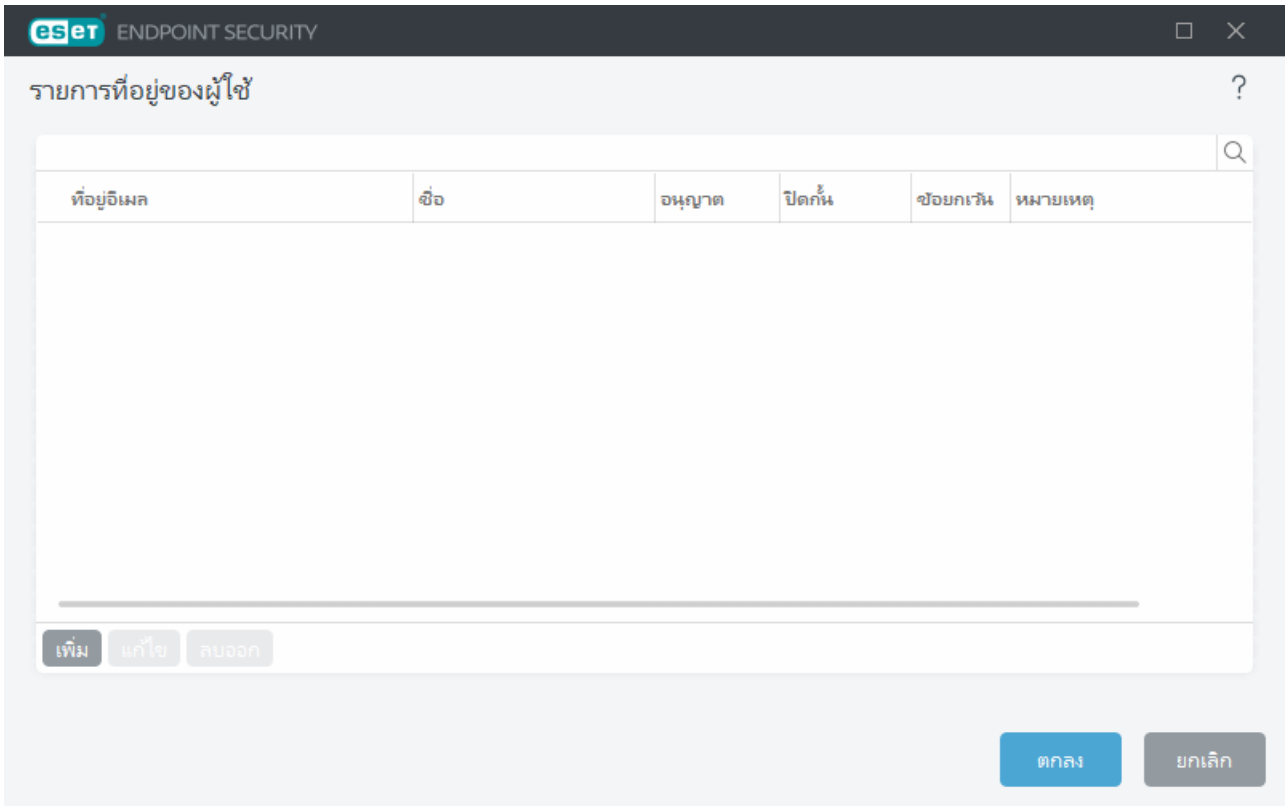
เพิ่มรายการที่อยู่ของผู้ใช้เป็นข้อยกเว้นโดยอัตโนมัติ

เพิ่มที่อยู่จากบัญชีของตนเอง – เพิ่มที่อยู่ของคุณจากบัญชีอีเมลไคลเอ็นต์ที่มีอยู่ไปยังรายการที่อยู่ของผู้ใช้เป็นข้อยกเว้น

รายการที่อยู่

เพื่อป้องกันอีเมลที่ไม่พึงประสงค์ ESET Endpoint Security ทำให้คุณสามารถจำแนกที่อยู่อีเมลในรายการที่อยู่ได้

เมื่อต้องการแก้ไขรายการที่อยู่ ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันอีเมลไคลเอ็นต์** > **การจัดการรายการที่อยู่** แล้วคลิก **แก้ไข** ถัดจาก **รายการที่อยู่ของผู้ใช้** หรือ **รายการที่อยู่ร่วม**



คอลัมน์

ที่อยู่อีเมล – ที่อยู่ที่จะนำกฎไปใช้

ชื่อ – ชื่อกฎที่กำหนดเอง

อนุญาต/บล็อก/ข้อยกเว้น – ปุ่มตัวเลือกที่ใช้ในการกำหนดการทำงานที่จะใช้สำหรับที่อยู่อีเมล (คลิกปุ่มตัวเลือกในคอลัมน์ที่ต้องการเพื่อเปลี่ยนการทำงานอย่างรวดเร็ว):

- **อนุญาต** - ที่อยู่ที่ถือว่าปลอดภัยและมาจากบุคคลที่คุณต้องการรับข้อความ
- **บล็อก** - ที่อยู่ที่ถือว่าไม่ปลอดภัย/สแปม และมาจากบุคคลที่คุณไม่ต้องการรับข้อความ
- **ข้อยกเว้น** - ที่อยู่ที่มีการตรวจสแปมเสมอ และเป็นที่อยู่ที่อาจถูกแอบอ้างและใช้สำหรับส่งสแปม

หมายเหตุ – ข้อมูลเกี่ยวกับวิธีสร้างกฎและตัวเลือกว่าจะนำไปใช้กับทั้งโดเมน / โดเมนระดับล่างหรือไม่

การจัดการที่อยู่

- **เพิ่ม** – คลิกเพื่อเพิ่มกฎสำหรับที่อยู่ใหม่
- **แก้ไข** – เลือกและคลิกเพื่อแก้ไขกฎที่มีอยู่
- **ลบออก** – เลือกและคลิกหากคุณต้องการลบกฎออกจากรายการที่อยู่

เพิ่ม/แก้ไขที่อยู่

หน้าต่างนี้ช่วยให้คุณเพิ่มหรือแก้ไขที่อยู่ในส่วน การจัดการรายการที่อยู่ และกำหนดค่าการดำเนินการที่จะใช้ได้:

ที่อยู่อีเมล – ที่อยู่ที่จะนำกฎไปใช้ ไม่รองรับอักขระตัวแทน

ชื่อ – ชื่อกฎที่กำหนดเอง

การทำงาน – การทำงานที่จะใช้หากที่อยู่อีเมลของผู้ติดต่อตรงกับที่อยู่ที่ระบุในช่อง **ที่อยู่อีเมล**:

- **อนุญาต** - ที่อยู่ที่ถือว่าปลอดภัยและมาจากบุคคลที่คุณต้องการรับข้อความ
- **บล็อก** - ที่อยู่ที่ถือว่าไม่ปลอดภัย/สแปม และมาจากบุคคลที่คุณไม่ต้องการรับข้อความ
- **ข้อยกเว้น** - ที่อยู่ที่มีการตรวจสแปมเสมอ และเป็นที่อยู่ที่อาจถูกแอบอ้างและใช้สำหรับส่งสแปม

ทั้งโดเมน – เลือกตัวเลือกนี้เพื่อให้ใช้กฎกับทั้งโดเมนของผู้ติดต่อ (ไม่ใช่เฉพาะที่อยู่ที่ระบุในช่อง **ที่อยู่อีเมล** แต่รวมถึงที่อยู่อีเมลทั้งหมดในโดเมน *address.info*)

โดเมนระดับล่าง – เลือกตัวเลือกนี้เพื่อให้ใช้กฎกับโดเมนระดับล่างของผู้ติดต่อ (*address.info* คือโดเมน และ *my.address.info* คือโดเมนย่อย)

ผลการประมวลผลที่อยู่

เมื่อเพิ่มที่อยู่ใหม่หรือเปลี่ยนการทำงานที่ใช้สำหรับที่อยู่อีเมล ESET Endpoint Security จะแสดงข้อความแจ้งเตือน เนื้อหาของข้อความการแจ้งเตือนจะแตกต่างกันไปตามการดำเนินการของคุณ

เลือกกล่องกาเครื่องหมาย **ไม่ต้องถามอีก** เพื่อดำเนินการอัตโนมัติโดยไม่ต้องแสดงข้อความในครั้งถัดไป

ThreatSense

ThreatSense ประกอบด้วยวิธีการตรวจหาภัยคุกคามที่ซับซ้อนหลายรูปแบบ เทคโนโลยีนี้เป็นการป้องกันในเชิงรุก ซึ่งหมายความว่าจะมีการป้องกันตั้งแต่ช่วงต้นที่มีการแพร่กระจายของภัยคุกคามใหม่ เทคโนโลยีนี้จะใช้การผสมผสานของการวิเคราะห์รหัส การจำลองรหัส ฐานข้อมูลทั่วไป และฐานข้อมูลไวรัส ซึ่งทำงานร่วมกันอย่างสอดคล้องเพื่อเพิ่มประสิทธิภาพของการรักษาความปลอดภัยให้กับระบบได้อย่างมาก กลไกการสแกนสามารถควบคุมสตรีมข้อมูลต่างๆ ได้พร้อมกัน ซึ่งเพิ่มประสิทธิภาพและอัตราการตรวจพบสูงสุด นอกจากนี้ เทคโนโลยี ThreatSense ยังช่วยกำจัดรูทคิทด้วย

ตัวเลือกการตั้งค่าของเทคโนโลยี ThreatSense ช่วยให้ผู้ใช้สามารถระบุพารามิเตอร์การสแกนต่างๆ ได้:

- ประเภทไฟล์และนามสกุลที่จะสแกน
- การใช้วิธีการตรวจหาต่างๆ ร่วมกัน
- ระดับการกำจัด เป็นต้น

หากต้องการเข้าสู่หน้าต่างการตั้งค่า ให้คลิก **ThreatSense** ใน การตั้งค่าขั้นสูง สำหรับโมดูลที่ใช้เทคโนโลยี ThreatSense (โปรดดูด้านล่าง) สถานการณ์ของการรักษาความปลอดภัยที่ต่างกันอาจต้องใช้การกำหนดค่าที่ต่างกัน โปรดทราบว่า ThreatSense สามารถกำหนดค่าแยกกันได้สำหรับโมดูลการป้องกันต่อไปนี้:

- การป้องกันระบบไฟล์แบบเรียลไทม์
- การสแกนขณะอยู่ในสถานะไม่ใช้งาน
- การสแกนเมื่อเริ่มต้น
- การป้องกันเอกสาร
- การป้องกันอีเมลไคลเอ็นต์
- การป้องกันการเข้าถึงเว็บ
- การสแกนคอมพิวเตอร์

พารามิเตอร์ ThreatSense มีการปรับให้เหมาะสำหรับแต่ละโมดูลมากที่สุด อีกทั้งการแก้ไขเหล่านี้จะมีผลกับการทำงานของระบบมากด้วยเช่นกัน ตัวอย่างเช่น การเปลี่ยนพารามิเตอร์เพื่อให้สแกนรันไทม์แพ็คเกอร์เสมอ หรือเปิดใช้การวิเคราะห์พฤติกรรมขั้นสูงในโมดูลการป้องกันระบบไฟล์แบบเรียลไทม์อาจทำให้ระบบทำงานช้าลง (โดยปกติโปรแกรมจะสแกนเฉพาะไฟล์ที่สร้างขึ้นใหม่โดยใช้วิธีการเหล่านี้) เราขอแนะนำให้คุณคงพารามิเตอร์ ThreatSense เริ่มต้นไว้สำหรับโมดูลทั้งหมด ยกเว้นการสแกนคอมพิวเตอร์

วัตถุที่จะสแกน

ส่วนนี้จะช่วยให้คุณสามารถกำหนดว่าจะสแกนหาการแฝงตัวจากองค์ประกอบและไฟล์คอมพิวเตอร์ใด

หน่วยความจำที่ใช้งาน – สแกนหาภัยคุกคามที่โจมตีหน่วยความจำที่ใช้งานของระบบ

ส่วนการบูต/UEFI – การสแกนบูตเซคเตอร์สำหรับมัลแวร์ที่มีอยู่ในบันทึกการบูตหลัก อ่านเพิ่มเติมเกี่ยวกับ UEFI ในประมวลศัพท์

ไฟล์อีเมล – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: DBX (Outlook Express) และ EML

อาร์ไคฟ์ – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE และอื่นๆ อีกมากมาย

อาร์ไคฟ์แบบคลายตัวเอง - อาร์ไคฟ์แบบคลายตัวเอง หรือ Self-extracting archives (SFX) คืออาร์ไคฟ์ที่สามารถคลายตัวเองได้

รันไทม์แพ็คเกอร์ – หลังจากเรียกใช้แล้ว รันไทม์แพ็คเกอร์ (ไม่เหมือนกับประเภทที่เก็บเอกสารมาตรฐาน) จะคลายออกในหน่วยความจำ นอกเหนือจากแพ็คเกอร์คงที่แบบมาตรฐาน (UPX, yoda, ASPack, FSG เป็นต้น) เครื่องมือสแกนจะสามารถจดจำประเภทหรือแพ็คเกอร์อื่นๆ เพิ่มเติมผ่านการใช้การจำลองรหัส

ตัวเลือกการสแกน

เลือกวิธีที่ใช้เมื่อสแกนหาการแฝงตัวบนระบบ ตัวเลือกที่ใช้ได้มีดังนี้:

การวิเคราะห์พฤติกรรม – การวิเคราะห์พฤติกรรมเป็นอัลกอริทึมที่วิเคราะห์การทำงาน (ที่เป็นอันตราย) ของโปรแกรม ข้อได้เปรียบสำคัญของเทคโนโลยีนี้คือความสามารถในการระบุซอฟต์แวร์ที่เป็นอันตรายซึ่งไม่มีอยู่ก่อนหน้านั้น หรือไม่เป็นที่รู้จักของกลไกตรวจหาก่อนหน้า ข้อเสียคือมีโอกาสที่จะเกิดการเตือนผิดพลาด (แม้จะน้อยมากก็ตาม)

วิเคราะห์พฤติกรรมขั้นสูง/ลายเซ็น DNA - การวิเคราะห์พฤติกรรมขั้นสูงเป็นอัลกอริทึมการวิเคราะห์พฤติกรรมขั้นสูงที่พัฒนาโดย ESET ปรับให้เหมาะสมกับการตรวจหาเวิร์มของคอมพิวเตอร์และม้าโทรจัน และเขียนในภาษาที่ใช้เขียนโปรแกรมระดับสูง การใช้การวิเคราะห์พฤติกรรมขั้นสูงจะช่วยเพิ่มความสามารถในการตรวจหาภัยคุกคามของผลิตภัณฑ์ ESET ได้เป็นอย่างมาก ฐานข้อมูลไวรัสสามารถตรวจหาและระบุไวรัสได้อย่างเชื่อถือได้ การใช้ระบบอัพเดทอัตโนมัติ ทำให้ฐานข้อมูลใหม่ใช้ได้หลังจากค้นพบภัยคุกคามเพียงไม่กี่ชั่วโมง ข้อเสียของฐานข้อมูลไวรัสคือระบบจะตรวจหาไวรัสเฉพาะที่รู้จักเท่านั้น (หรือเวอร์ชันที่มีการแก้ไขเล็กน้อยของไวรัสเหล่านี้)

การกำจัด

การตั้งค่าการกำจัด จะเป็นตัวกำหนดการทำงานของ ESET Endpoint Security ขณะกำจัดวัตถุ

การยกเว้น

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่า ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะสแกน

อื่นๆ

เมื่อกำหนดค่ากลไก ThreatSense สำหรับการสแกนคอมพิวเตอร์ จะสามารถใช้ตัวเลือกในส่วน **อื่นๆ** ได้ดังต่อไปนี้:

สแกนสตรีมข้อมูลสำรอง (ADS) – สตรีมข้อมูลสำรองที่ใช้งานโดยระบบไฟล์ NTFS เป็นการเชื่อมโยงไฟล์และโฟลเดอร์ซึ่งจะไม่ปรากฏสำหรับเทคนิคการสแกนทั่วไป การแฝงตัวจำนวนมากพยายามหลีกเลี่ยงการตรวจหานี้ โดยปลอมแปลงตัวเองเป็นสตรีมข้อมูลสำรอง

เรียกใช้การสแกนเบื้องหลังโดยมีลำดับความสำคัญต่ำ – ลำดับการสแกนแต่ละลำดับจะใช้ทรัพยากรของระบบจำนวนหนึ่ง หากคุณทำงานกับโปรแกรมที่ใช้ทรัพยากรระบบจำนวนมาก คุณสามารถเปิดใช้การสแกนเบื้องหลังที่มีลำดับความสำคัญต่ำ และประหยัดทรัพยากรไว้สำหรับแอพพลิเคชันของคุณ

บันทึกวัตถุทั้งหมด – บันทึกการสแกน จะแสดงไฟล์ที่สแกนแล้วทั้งหมดในอาร์ไคฟ์ที่ขยายในตัว รวมถึงไฟล์ที่ไม่ติดไวรัส (อาจสร้างข้อมูลบันทึกการสแกนจำนวนมากและเพิ่มขนาดไฟล์บันทึกการสแกน)

เปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท – เมื่อเปิดใช้การเพิ่มประสิทธิภาพแบบสมาร์ท ระบบจะใช้การตั้งค่าที่มีประสิทธิภาพที่สุดเพื่อให้แน่ใจว่าการสแกนจะมีประสิทธิภาพและความเร็วสูงสุดไปพร้อมกัน ซึ่งโมดูลการป้องกันต่างๆ จะสแกนข้อมูลอย่างชาญฉลาด โดยใช้ประโยชน์จากวิธีการสแกนต่างๆ และนำมาใช้งานกับประเภทไฟล์ที่ระบุ หากคุณปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท เราจะใช้เฉพาะการตั้งค่าที่ผู้ใช้กำหนดไว้ในแกน ThreatSense ของโมดูลเฉพาะเมื่อทำการสแกนเท่านั้น

เก็บบันทึกการลงเวลาเข้าถึงล่าสุด – เลือกตัวเลือกนี้เพื่อเก็บเวลาแรกเริ่มที่เข้าถึงไฟล์ที่สแกนแทนการอัพเดทเวลาเหล่านั้น (ตัวอย่างเช่น สำหรับใช้กับระบบสำรองข้อมูล)

ขีดจำกัด

ส่วนขีดจำกัดช่วยให้คุณสามารถระบุขนาดสูงสุดของวัตถุ และระดับของอาร์ไคฟ์ที่ซ้อนที่จะสแกน:

การตั้งค่าวัตถุ

ขนาดวัตถุสูงสุด – กำหนดขนาดสูงสุดของวัตถุที่จะสแกน โมดูลป้องกันไวรัสที่กำหนดจะสแกนเฉพาะวัตถุที่เล็กกว่าขนาดที่ระบุเท่านั้น ผู้ที่สามารถแก้ไขตัวเลือกนี้ควรเป็นผู้ใช้ขั้นสูง ซึ่งอาจมีเหตุผลบางอย่างสำหรับการยกเว้นวัตถุขนาดใหญ่จากการสแกน ค่าเริ่มต้น: ไม่จำกัด

เวลาสแกนสูงสุดสำหรับวัตถุ (วินาที) – กำหนดค่าสูงสุดสำหรับสแกนไฟล์ในวัตถุที่มีการบรรจุ (เช่น อาร์ไคฟ์ RAR/ZIP หรืออีเมลที่มีไฟล์แนบหลายรายการ) การตั้งค่านี้จะไม่ถูกปรับใช้สำหรับไฟล์สแตนด์อโลน การสแกนจะหยุดทันทีหากมีการป้อนค่าที่ผู้ใช้กำหนดและพ้นระยะเวลาดังกล่าว โดยไม่คำนึงว่าการสแกนแต่ละไฟล์ในวัตถุที่มีการบรรจุจะเสร็จสิ้นแล้วหรือไม่ ในกรณีที่อาร์ไคฟ์บรรจุไฟล์ขนาดใหญ่ การสแกนจะหยุดช้ากว่าไฟล์ที่ถูกดึงข้อมูลจากอาร์ไคฟ์ (ตัวอย่างเช่น เมื่อตัวแปรที่ผู้ใช้กำหนดคือ 3 วินาที แต่การดึงข้อมูลของไฟล์คือ 5 วินาที) ไฟล์ที่เหลือในอาร์ไคฟ์จะไม่ถูกสแกนเมื่อพ้นระยะเวลาดังกล่าว หากต้องการจำกัดเวลาในการสแกน ซึ่งรวมถึงอาร์ไคฟ์ขนาดใหญ่ ให้ใช้ **ขนาดวัตถุสูงสุด** และ **ขนาดไฟล์สูงสุดในอาร์ไคฟ์** (ไม่แนะนำให้ใช้เนื่องจากความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นได้) ค่าเริ่มต้น: ไม่จำกัด

ตั้งค่าการสแกนอาร์ไคฟ์

ระดับการซ้อนของอาร์ไคฟ์ – ระบุความลึกสูงสุดของการสแกนอาร์ไคฟ์ ค่าเริ่มต้น: 10

ขนาดไฟล์สูงสุดในอาร์ไคฟ์ – ตัวเลือกนี้ช่วยให้คุณสามารถระบุขนาดไฟล์สูงสุดสำหรับไฟล์ที่อยู่ในอาร์ไคฟ์ (เมื่อดึงข้อมูล) ที่จะสแกนได้ ค่าเริ่มต้น: ไม่จำกัด ค่าสูงสุดคือ 3 GB

เราไม่แนะนำให้แก้ไขค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดที่จะต้องแก้ไขค่านี้ในสถานการณ์ปกติ

การป้องกันการเข้าถึงเว็บ

การป้องกันการเข้าถึงเว็บไซต์ช่วยให้คุณสามารถกำหนดการตั้งค่าโมดูล การป้องกันอินเทอร์เน็ต ขั้นสูง ตัวเลือกต่อไปนี้จะพร้อมใช้งานใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเว็บไซต์** > **การป้องกันการเข้าถึงเว็บไซต์**:

เปิดใช้งานการป้องกันการเข้าถึงเว็บ – เมื่อปิดใช้งาน จะไม่มีการเรียกใช้การป้องกันการเข้าถึงเว็บไซต์และการป้องกันฟิชชิ่ง

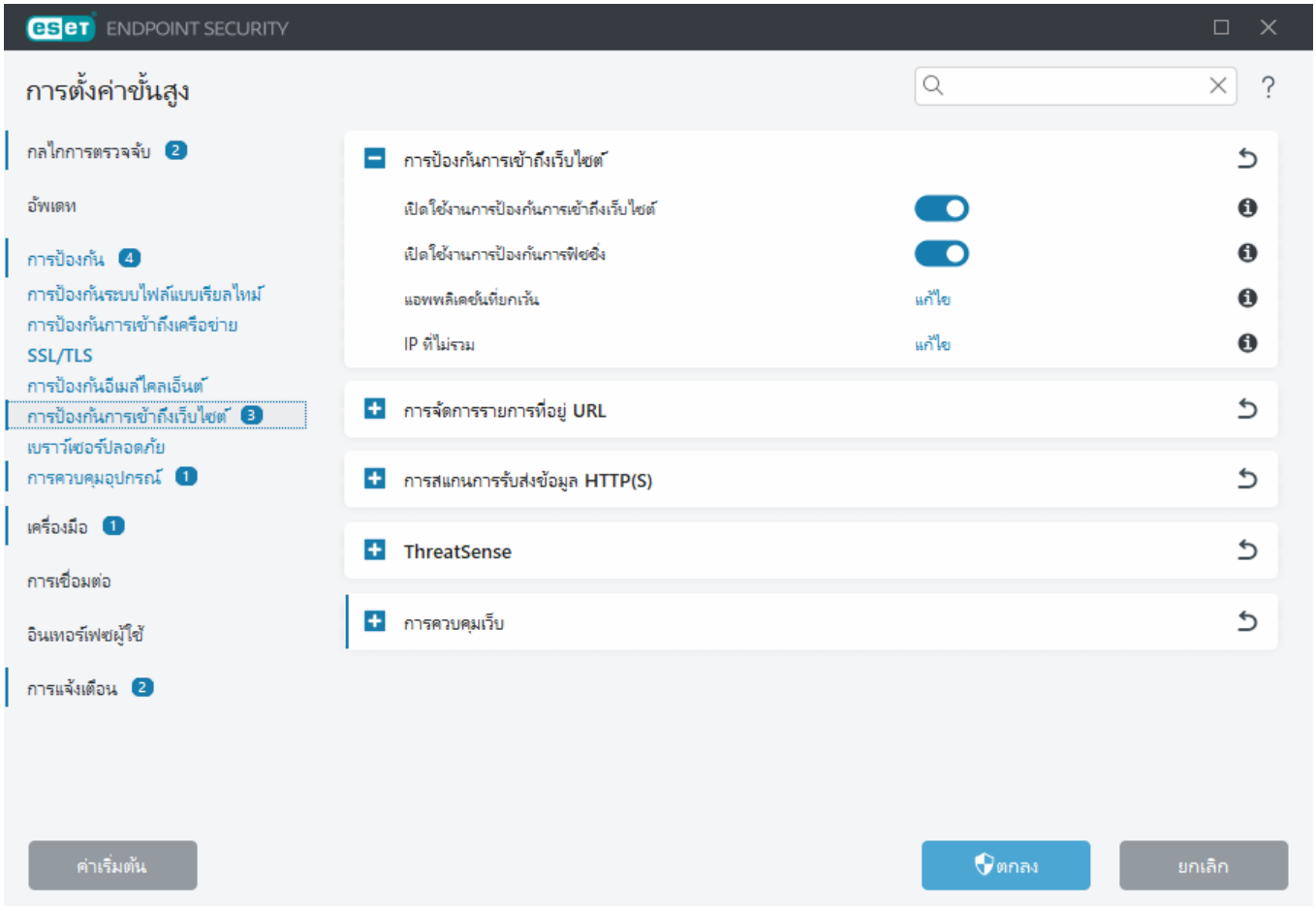
> เราขอแนะนำให้คุณเปิดใช้งานการป้องกันการเข้าถึงเว็บไซต์และไม่ยกเว้นแอพพลิเคชันหรือที่อยู่ IP ตามค่าเริ่มต้นใดๆ

สแกนสคริปต์เบราว์เซอร์ – เมื่อเปิดใช้งาน กลไกการตรวจจับจะตรวจสอบโปรแกรม JavaScript ทั้งหมดที่เรียกใช้โดยเว็บเบราว์เซอร์

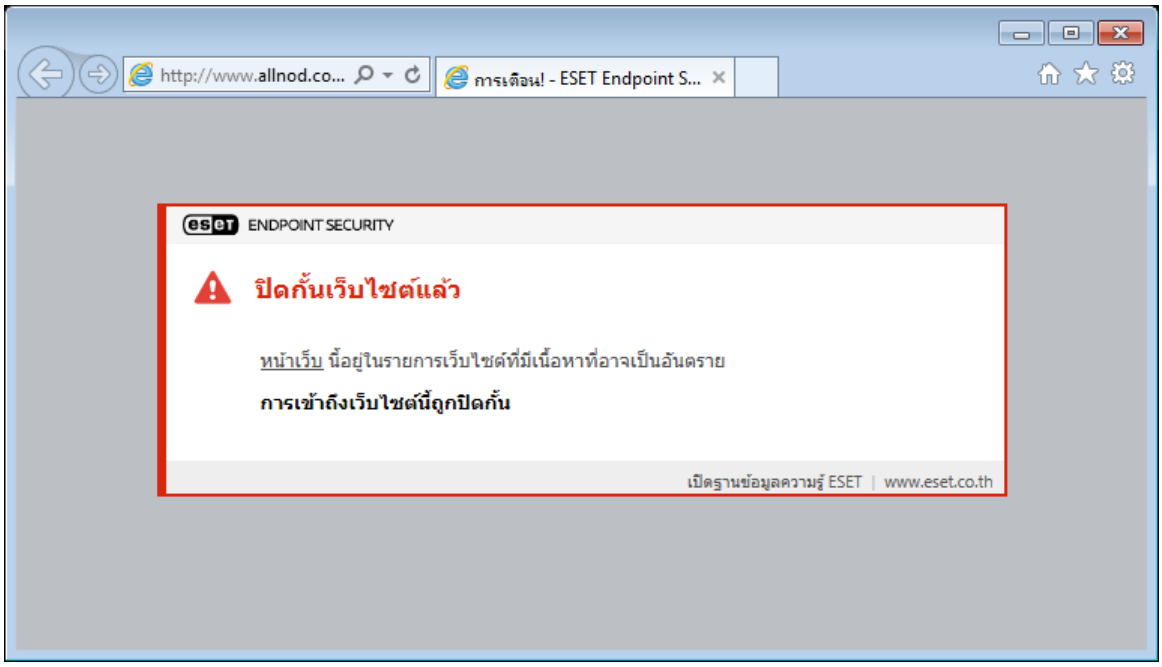
เปิดใช้งานการป้องกันฟิชชิ่ง – เมื่อเปิดใช้งาน หน้าเว็บฟิชชิ่งจะถูกบล็อก โปรดดู การป้องกันการฟิชชิ่ง สำหรับข้อมูลเพิ่มเติม

แอพพลิเคชันที่ยกเว้น – ช่วยให้คุณสามารถแยกแอพพลิเคชันบางแอพออกจากการสแกนโดยฟีเจอร์การป้องกันการเข้าถึงเว็บไซต์ได้ ซึ่งจะมีประโยชน์เมื่อการป้องกันการเข้าถึงเว็บไซต์ทำให้เกิดปัญหาความเข้ากันได้

IP ที่ยกเว้น – ช่วยให้คุณสามารถแยกที่อยู่ระยะไกลที่ต้องการออกจากการสแกนโดยการป้องกันการเข้าถึงเว็บไซต์ ซึ่งจะมีประโยชน์เมื่อการป้องกันการเข้าถึงเว็บไซต์ทำให้เกิดปัญหาความเข้ากันได้



การป้องกันการเข้าถึงเว็บไซต์จะแสดงข้อความต่อไปนี้ในเบราว์เซอร์ของคุณเมื่อเว็บไซต์ถูกปิดกั้น:



บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
- ยกเลิกการปิดกั้นเว็บไซต์ที่ปลอดภัยในแต่ละเวิร์กสเตชันใน ESET Endpoint Security

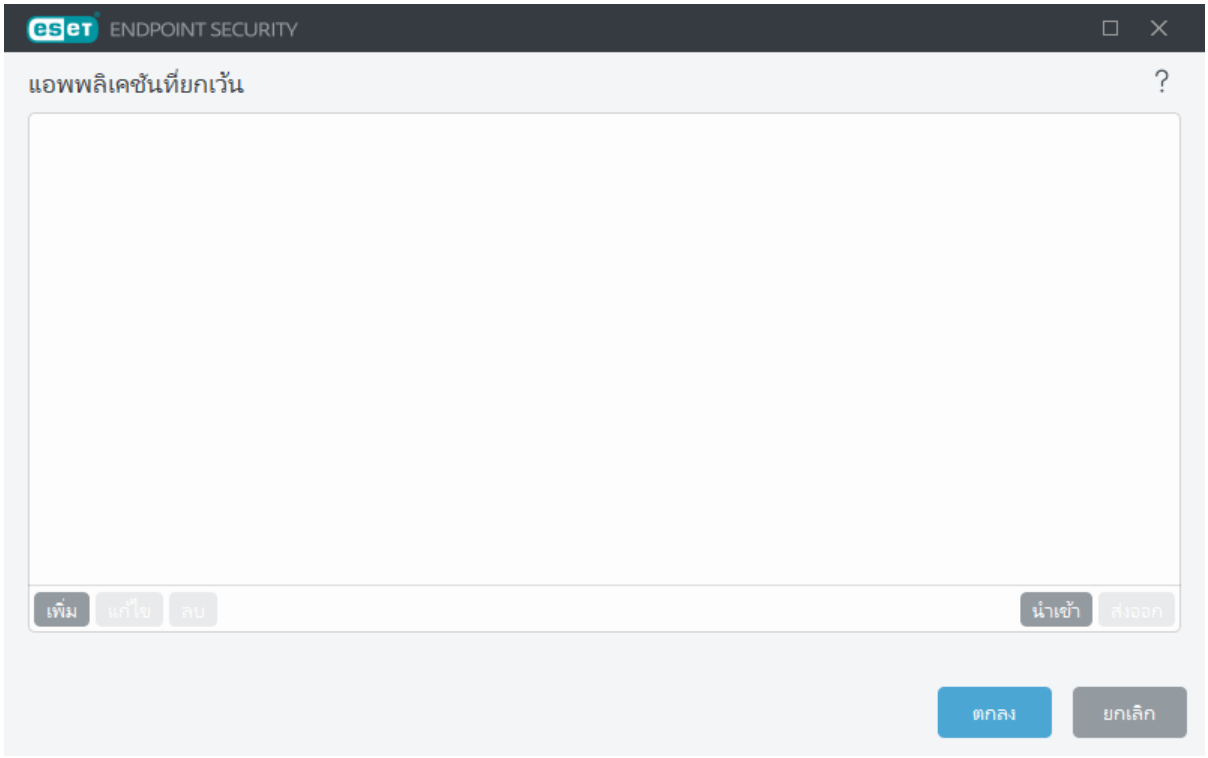
แอพพลิเคชันที่ยกเว้น

หากต้องการยกเว้นการสแกนการรับส่งข้อมูลสำหรับบางแอพพลิเคชันโดยเฉพาะ ให้เพิ่มแอพนั้นลงในรายการ การสื่อสารของ HTTP(S)/POP3(S)/IMAP(S) ของแอพพลิเคชันที่เลือกจะไม่ได้รับการตรวจสอบเพื่อหาภัยคุกคาม เราขอแนะนำให้ใช้ตัวเลือกนี้เฉพาะสำหรับแอพพลิเคชันที่ทำงานได้อย่างไม่ถูกต้องและการสื่อสารของแอพพลิเคชันเหล่านั้นกำลังถูกสแกนอยู่

แอพพลิเคชันและบริการที่ทำงานอยู่จะสามารถใช้งานได้ที่นี่โดยอัตโนมัติเมื่อคุณคลิก **เพิ่ม** คลิก **...** และไปยังแอพพลิเคชันเพื่อเพิ่มการยกเว้นด้วยตนเอง

แก้ไข – แก้ไขรายการที่เลือกจากรายการ

ลบออก – ลบรายการที่เลือกออกจากรายการ



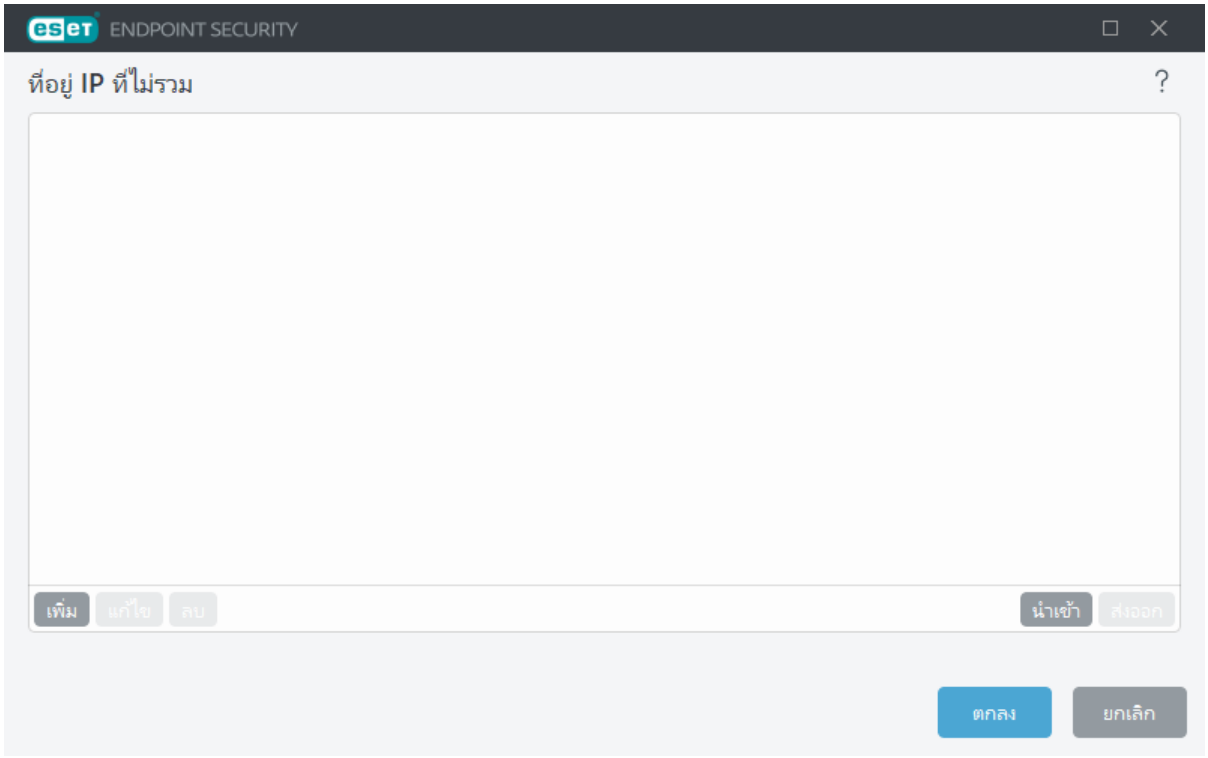
IP ที่ไม่รวม

รายการที่อยู่ในรายการจะถูกยกเว้นจากการสแกน การสื่อสารของ HTTP(S)/POP3(S)/IMAP(S) จาก/ไปยังที่อยู่ที่เลือกจะไม่ได้รับการตรวจสอบเพื่อหาภัยคุกคาม เราขอแนะนำให้คุณใช้ตัวเลือกนี้เฉพาะสำหรับที่อยู่ที่ทราบว่าเชื่อถือได้เท่านั้น

เพิ่ม - คลิกเพื่อเพิ่มที่อยู่ IP/ช่วงที่อยู่/ซับเน็ต ให้กับจุดระยะไกลซึ่งมีการใช้กฎ

แก้ไข – แก้ไขรายการที่เลือกจากรายการ

ลบออก – ลบรายการที่เลือกออกจากรายการ



ตัวอย่างที่อยู่ IP
เพิ่มที่อยู่ IPv4:
ที่อยู่เดียว – เพิ่มที่อยู่ IP ของคอมพิวเตอร์แต่ละเครื่อง (ตัวอย่างเช่น *192.168.0.10*)
ช่วงที่อยู่ – ป้อนที่อยู่ IP แรกและสุดท้ายเพื่อระบุช่วง IP ของคอมพิวเตอร์หลายเครื่อง (ตัวอย่างเช่น *192.168.0.1-192.168.0.99*)
ซับเน็ต - ซับเน็ต (กลุ่มของคอมพิวเตอร์) กำหนดโดยที่อยู่ IP และมาสก์ ตัวอย่างเช่น 255.255.255.0 เป็นมาสก์เครือข่ายสำหรับซับเน็ต 192.168.1.0 เพื่อแยกประเภทซับเน็ตทั้งหมดใน *192.168.1.0/24*
เพิ่มที่อยู่ IPv6:
ที่อยู่เดียว – เพิ่มที่อยู่ IP ของคอมพิวเตอร์แต่ละเครื่อง (ตัวอย่างเช่น *2001:718:1c01:16:214:22ff:fec9:ca5*):
ซับเน็ต - ซับเน็ต (กลุ่มของคอมพิวเตอร์) กำหนดโดยที่อยู่ IP และมาสก์ (ตัวอย่างเช่น: *2002:c0a8:6301:1::1/64*)

การจัดการรายการที่อยู่ URL

ส่วน **การจัดการรายการ URL** ใน การตั้งค่าขั้นสูง **การป้องกัน** > **การป้องกันการเข้าถึงเว็บไซต์** ช่วยให้คุณสามารถระบุที่อยู่ HTTP ที่ต้องการบล็อก อนุญาต หรือแยกออกจากการสแกนเนื้อหา

SSL/TLS ต้องเปิดใช้งานหากคุณต้องการกรอง HTTPS นอกเหนือจาก HTTP มิฉะนั้นจะเพิ่มเฉพาะโดเมนของไซต์ HTTPS ที่คุณเข้าชมเท่านั้น จะไม่เพิ่ม URL เต็ม

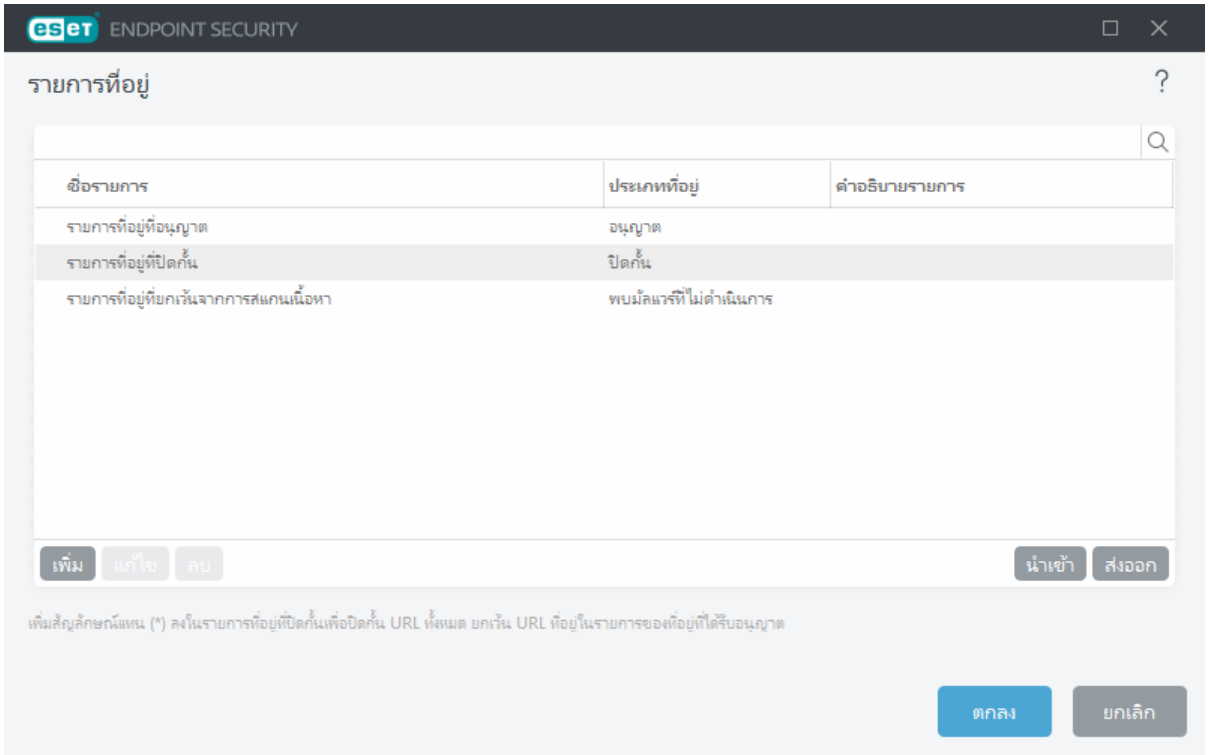
เว็บไซต์ใน **รายการที่อยู่ที่ปิดกั้น** จะไม่สามารถเข้าถึงได้เว้นแต่จะอยู่ใน **รายการที่อยู่ที่อนุญาต** ด้วยเช่นกัน เว็บไซต์ใน **รายการที่อยู่ที่ยกเว้นจากการสแกนเนื้อหา** จะไม่ถูกสแกนหารหัสที่เป็นอันตรายเมื่อเข้าถึง

ถ้าคุณต้องการปิดกั้นที่อยู่ HTTP ทั้งหมดยกเว้นที่อยู่ใน **รายการที่อยู่ที่อนุญาต** ที่ใช้งาน ให้เพิ่ม * ไปยัง **รายการที่**

อยู่ที่ปิดกั้น ที่ใช้งาน

คุณสามารถใช้สัญลักษณ์พิเศษ * (ดอกจัน) และ ? (เครื่องหมายคำถาม) ในรายการได้ (เครื่องหมายคำถาม) ได้ขณะสร้างรายการที่อยู่ โดยเครื่องหมายดอกจันจะแทนสตริงอักขระ และเครื่องหมายคำถามจะแทนสัญลักษณ์ ครระมัดระวังเมื่อระบุที่อยู่ที่ยกเว้น เนื่องจากรายการดังกล่าวควรมีเฉพาะที่อยู่ที่เชื่อถือและปลอดภัยเท่านั้น ในทำนองเดียวกัน คุณควรตรวจสอบให้แน่ใจว่ามีการใช้สัญลักษณ์ * และ ? ในรายการนี้อย่างถูกต้อง โปรดดู เพิ่มที่อยู่ HTTP / มาสก์ของโดเมน เพื่อดูวิธีทำให้ทั้งโดเมนรวมถึงโดเมนย่อยทั้งหมดตรงกันได้อย่างปลอดภัย ในการเปิดใช้งานรายการ ให้เลือก **รายการที่ใช้งาน** หากคุณต้องการให้ระบบแจ้งเมื่อป้อนที่อยู่จากรายการปัจจุบัน ให้เลือก **แจ้งเมื่อนำไปใช้**

> **ที่อยู่ที่ ESET เชื่อถือ**
> หากเปิดใช้งาน **ห้ามสแกนการรับส่งข้อมูลผ่านโดเมนที่ ESET เชื่อถือ** กับ SSL/TLS โดเมนในรายการที่อนุญาตที่ ESET จัดการจะไม่ได้รับผลกระทบจากการกำหนดค่าการจัดการรายการ URL



องค์ประกอบการควบคุม

เพิ่ม – สร้างรายการใหม่เพิ่มเติมจากรายการที่กำหนดไว้ล่วงหน้า ส่วนนี้จะมีประโยชน์เมื่อคุณต้องการแยกที่อยู่ออกเป็นกลุ่มๆ ตัวอย่างเช่น รายการของที่อยู่ที่ปิดกั้นรายการหนึ่งอาจประกอบด้วยที่อยู่จากบัญชีดำสาธารณะภายนอก และรายการถัดไปอาจประกอบด้วยบัญชีดำของคุณเอง ซึ่งทำให้ง่ายขึ้นต่อการอัพเดทรายการภายนอกในขณะที่เก็บส่วนของคุณไว้เหมือนเดิม

แก้ไข – แก้ไขรายการที่มีอยู่ ใช้สิ่งนี้ในการเพิ่มหรือลบที่อยู่ออก

ลบ – ลบรายการที่มีอยู่ สามารถใช้งานได้กับรายการที่สร้างด้วย **เพิ่ม** เท่านั้น ไม่สามารถใช้กับรายการตามค่าเริ่มต้นได้

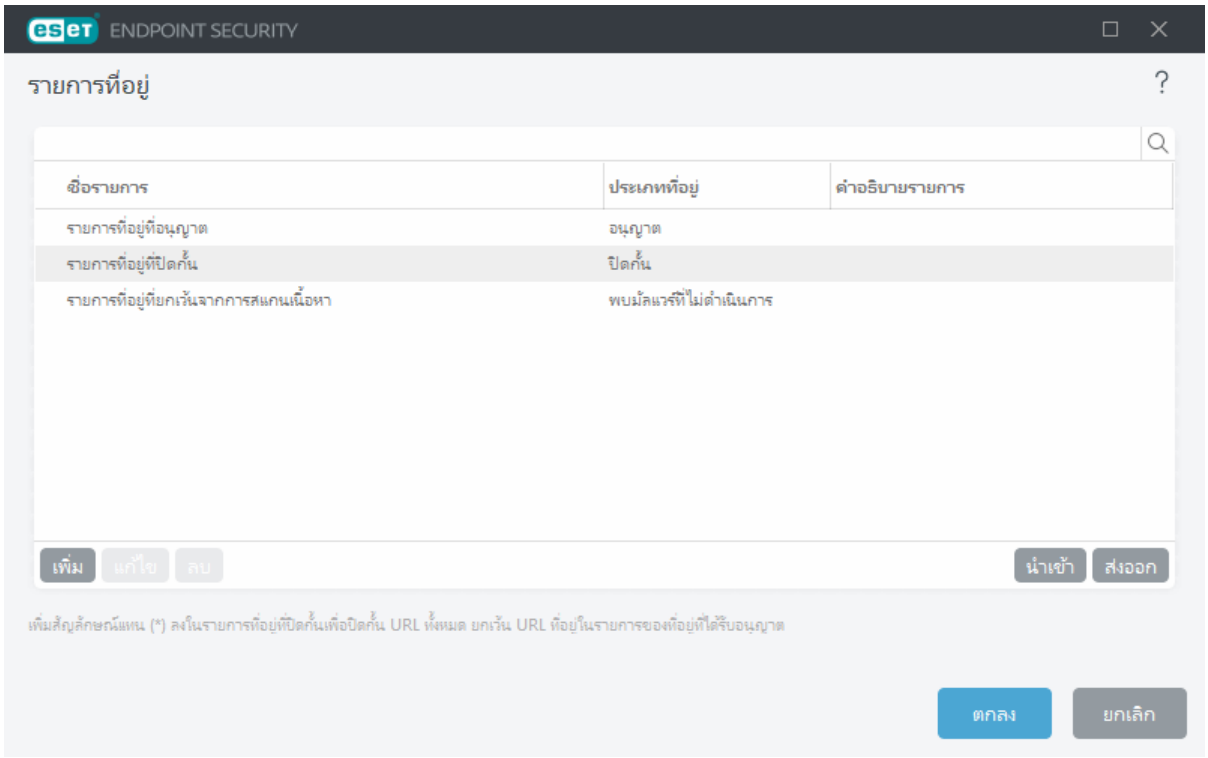
รายการที่อยู่

ในส่วนนี้ คุณสามารถระบุรายการของที่อยู่ HTTP(S) ที่จะถูกปิดกั้น อนุญาต หรือยกเว้นจากการตรวจสอบ

ตามค่าเริ่มต้นแล้ว จะมีสามรายการดังต่อไปนี้:

- **รายการที่อยู่ที่ยกเว้นจากการสแกนเนื้อหา** – ไม่มีการตรวจสอบรหัสที่เป็นอันตรายสำหรับที่อยู่ที่เพิ่มไว้ในรายการนี้
- **รายการที่อยู่ที่อนุญาต** – ถ้าเปิดใช้งานตัวเลือก อนุญาตการเข้าถึงเฉพาะที่อยู่ HTTP ในรายการของที่อยู่ที่อนุญาต และรายการของที่อยู่ที่ปิดกั้นประกอบด้วย * (จับคู่ทุกอย่าง) ผู้ใช้จะสามารถเข้าถึงที่อยู่ที่ระบุในรายการนี้ได้เท่านั้น ที่อยู่ในรายการนี้จะได้รับอนุญาตแม้ว่ารวมอยู่ในรายการที่อยู่ที่ปิดกั้น
- **รายการที่อยู่ที่ปิดกั้น** - ผู้ใช้จะไม่สามารถเข้าถึงที่อยู่ที่ระบุในรายการนี้เว้นแต่ที่อยู่นั้นอยู่ในรายการที่อยู่ที่อนุญาต

คลิกที่ **เพิ่ม** เพื่อสร้างรายการใหม่ หากต้องการลบรายการที่เลือกไว้ ให้คลิกที่ **ลบออก**



บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
- ยกเลิกการปิดกั้นเว็บไซต์ที่ปลอดภัยในแต่ละเวิร์กสเตชันใน ESET Endpoint Security

สำหรับข้อมูลเพิ่มเติม โปรดดูที่การจัดการที่อยู่ URL

สร้างรายการที่อยู่ใหม่

หน้าต่างข้อความนี้ทำให้คุณสามารถกำหนดค่า รายการของที่อยู่/มาสก์ URL ที่จะถูกปิดกั้น อนุญาต หรือยกเว้นจากการตรวจสอบ

คุณสามารถกำหนดค่าตัวเลือกต่อไปนี้ได้:

ประเภทรายการที่อยู่ - มีประเภทรายการสามประเภท:

- **ละเว้นมัลแวร์ที่พบ** – จะไม่มีการตรวจสอบโค้ดที่เป็นอันตรายสำหรับที่อยู่ที่เพิ่มในรายการนี้
- **ถูกปิดกั้น** - การเข้าถึงที่อยู่ที่ระบุในรายการนี้จะถูกปิดกั้น
- **อนุญาต** –การเข้าถึงที่อยู่ที่ระบุในรายการนี้จะได้รับอนุญาต ที่อยู่ในรายการนี้จะได้รับอนุญาตแม้จะตรงกับรายการที่อยู่ที่ถูกปิดกั้น

ชื่อรายการ – ระบุชื่อของรายการ ช่องนี้จะไม่มีให้ใช้งานขณะแก้ไขหนึ่งในรายการที่กำหนดไว้ล่วงหน้า

คำอธิบายรายการ - พิมพ์คำอธิบายโดยย่อสำหรับรายการ (ไม่จำเป็น) ไม่มีให้ใช้งานขณะแก้ไขหนึ่งในรายการที่กำหนดไว้ล่วงหน้า

เมื่อต้องการเปิดใช้งานรายการ ให้เลือก **รายการที่ใช้งาน** ถัดจากรายการนั้น หากคุณต้องการให้มีการแจ้งเตือนเมื่อมีการใช้รายการใดรายการหนึ่งขณะเข้าถึงเว็บไซต์ต่างๆ ให้เลือก **แจ้งเตือนเมื่อปรับใช้** ตัวอย่างเช่น คุณจะได้รับการแจ้งเตือนเมื่อเว็บไซต์ถูกปิดกั้นหรือได้รับอนุญาตเนื่องจากเว็บไซต์นั้นอยู่ในรายการที่อยู่ที่ปิดกั้นหรืออนุญาต การแจ้งเตือนจะแจ้งชื่อของรายการนั้น

ความรุนแรงของการบันทึก – เลือกความรุนแรงของการบันทึกจากเมนูแบบเลื่อนลง ESET PROTECT สามารถรวบรวมบันทึกที่มีรายละเอียดการเตือนได้

ความละเอียดการบันทึก ข้อมูล และ คำเตือน จะมีให้ใช้งานสำหรับกฎที่มีองค์ประกอบที่ไม่มีอักขระตัวแทนอย่างน้อยสององค์ประกอบภายในโดเมนเท่านั้น ตัวอย่างเช่น:
- *.domain.com/*
- *www.domain.com/*

องค์ประกอบการควบคุม

เพิ่ม – เพิ่มที่อยู่ URL ใหม่ไปยังรายการ (ป้อนค่าได้หลายค่าโดยใส่ตัวคั่น)

แก้ไข – แก้ไขที่อยู่ที่มีอยู่ในรายการ มีให้ใช้งานสำหรับที่อยู่ที่สร้างด้วย **เพิ่ม** เท่านั้น

ลบออก – ลบที่อยู่ที่มีอยู่ในรายการ มีให้ใช้งานสำหรับที่อยู่ที่สร้างด้วย **เพิ่ม** เท่านั้น

นำเข้า – นำเข้าไฟล์ที่มีที่อยู่ URL (แยกค่าด้วยตัวแบ่งบรรทัด ตัวอย่างเช่น *.txt โดยใช้การเข้ารหัส UTF-8)

สำหรับข้อมูล โปรดดูบท วิธีการเพิ่มมาสก์ URL

วิธีการเพิ่มมาสก์ URL

ดูคำแนะนำในหน้าต่างข้อความนี้ก่อนพิมพ์ที่อยู่ที่ต้องการ/มาสก์ของโดเมน

ESET Endpoint Security ให้ผู้ใช้สามารถปิดกั้นการเข้าถึงเว็บไซต์ที่ระบุ และป้องกันไม่ให้เบราว์เซอร์อินเทอร์เน็ตแสดงเนื้อหา นอกจากนี้ คุณยังสามารถระบุที่อยู่ซึ่งต้องการยกเว้นจากการตรวจสอบได้ด้วย หากไม่ทราบชื่อเต็มของเซิร์ฟเวอร์ระยะไกล หรือผู้ใช้ต้องการระบุทั้งกลุ่มของเซิร์ฟเวอร์ระยะไกล คุณสามารถใช้มาสก์เพื่อระบุกลุ่มดังกล่าวได้ มาสก์นี้ได้แก่สัญลักษณ์ "?" และ "*":

- ใช้ ? เพื่อแทนสัญลักษณ์
- ใช้ * เพื่อแทนสตริงข้อความ

ตัวอย่างเช่น *.c?m จะมีผลกับที่อยู่ทั้งหมด ซึ่งส่วนหลังจะเริ่มต้นด้วยตัวอักษร c สิ้นสุดด้วยตัวอักษร m และมีสัญลักษณ์ที่ไม่ทราบอยู่ตรงกลาง (.com, .cam เป็นต้น)

ตัวอย่างเช่น มาสก์ *x? หมายถึงที่อยู่ที่มี x เป็นอักขระตัวก่อนสุดท้าย หากต้องการทำให้ตรงกันทั้งโดเมน ให้พิมพ์ลงในฟอร์ม **.domain.com/** สามารถระบุคำนำหน้าโปรโตคอล *http://*, *https://* ในมาสก์ได้แต่ไม่บังคับ ถ้าไม่มีคำนำหน้า มาสก์จะจับคู่กับโปรโตคอลใดก็ได้ สัญลักษณ์ '*.' ที่อยู่ด้านหน้าของลำดับจะแสดงผลเป็นพิเศษหากใช้ขึ้นต้นชื่อโดเมน แรกสุด สัญลักษณ์แทน * ต้องไม่ตรงกับเครื่องหมายทับ ('/') ในกรณีนี้ ทั้งนี้เพื่อกันไม่ให้เกิดการหลีกเลี่ยงมาสก์ ตัวอย่างเช่น มาสก์ **.domain.com* จะไม่ตรงกับ *http://anydomain.com/anypath#.domain.com* (คำต่อท้ายเหล่านี้สามารถต่อท้าย URL ใดๆ โดยไม่ส่งผลต่อการดาวน์โหลด) ถัดมา สัญลักษณ์ "*." ยังต้องตรงกับสตริงเปล่าในกรณีพิเศษนี้ ทั้งนี้เพื่อทำให้ทั้งโดเมนรวมถึงโดเมนย่อยทั้งหมดตรงกันโดยใช้มาสก์เดียวร่วมกัน ตัวอย่างเช่น มาสก์ **.domain.com* ยังตรงกับ *http://domain.com* อีกด้วย การใช้ **domain.com* นั้นไม่ถูกต้อง เนื่องจาก

มาสก์ดังกล่าวจะไปตรงกับ *http://anotherdomain.com* เช่นกัน

ความละเอียดการบันทึก ข้อมูล และ คำเตือน จะมีให้ใช้งานสำหรับกฎที่มีองค์ประกอบที่ไม่มีอักขระตัวแทนอย่างน้อยสององค์ประกอบภายในโดเมนเท่านั้น ตัวอย่างเช่น:
- *.domain.com/*
- *www.domain.com/*

การสแกนการรับส่งข้อมูล HTTP(S)

โดยค่าเริ่มต้น ESET Endpoint Security มีการกำหนดค่าให้สแกน HTTP และ HTTPS การจราจรซึ่งใช้โดยเบราว์เซอร์อินเทอร์เน็ตและแอพพลิเคชันอื่นๆ คุณควรปิดใช้งานการสแกนการรับส่งข้อมูลเฉพาะในกรณีที่คุณกำลังประสบปัญหากับซอฟต์แวร์ของบริษัทอื่นและต้องการทราบว่าปัญหาดังกล่าวเกิดจาก ESET Endpoint Security หรือไม่

เปิดใช้งานการสแกนการรับส่งข้อมูล HTTP – การรับส่งข้อมูล HTTP จะถูกตรวจสอบบนพอร์ตทั้งหมดสำหรับแอพพลิเคชั่นทั้งหมดเสมอ

เปิดใช้งานการสแกนการรับส่งข้อมูล HTTPS – การรับส่งข้อมูล HTTPS จะใช้ช่องทางที่เข้ารหัสเพื่อโอนข้อมูลระหว่างเซิร์ฟเวอร์กับไคลเอ็นต์ โดย ESET Endpoint Security จะตรวจสอบการสื่อสารด้วยโปรโตคอล SSL (Secure Socket Layer) และ TLS (Transport Layer Security) โปรแกรมจะสแกนเฉพาะการรับส่งข้อมูลในพอร์ตที่กำหนดใน **พอร์ตที่ใช้งานโดยโปรโตคอล HTTPS** โดยไม่คำนึงถึงเวอร์ชันของระบบปฏิบัติการ (คุณสามารถเพิ่มพอร์ตไปยัง 443 และ 0-65535 ที่กำหนดไว้ล่วงหน้าได้)

ThreatSense

ThreatSense ประกอบด้วยวิธีการตรวจหาภัยคุกคามที่ซับซ้อนหลายรูปแบบ เทคโนโลยีนี้เป็นการป้องกันในเชิงรุก ซึ่งหมายความว่าจะมีการป้องกันตั้งแต่ช่วงต้นที่มีการแพร่กระจายของภัยคุกคามใหม่ เทคโนโลยีนี้จะใช้การผสมผสานของการวิเคราะห์รหัส การจำลองรหัส ฐานข้อมูลทั่วไป และฐานข้อมูลไวรัส ซึ่งทำงานร่วมกันอย่างสอดคล้องเพื่อเพิ่มประสิทธิภาพของการรักษาความปลอดภัยให้กับระบบได้อย่างมาก กลไกการสแกนสามารถควบคุมสตรีมข้อมูลต่างๆ ได้พร้อมกัน ซึ่งเพิ่มประสิทธิภาพและอัตราการตรวจพบสูงสุด นอกจากนี้ เทคโนโลยี ThreatSense ยังช่วยกำจัดรูทคิทด้วย

ตัวเลือกการตั้งค่าของเทคโนโลยี ThreatSense ช่วยให้ผู้ใช้สามารถระบุพารามิเตอร์การสแกนต่างๆ ได้:

- ประเภทไฟล์และนามสกุลที่จะสแกน
- การใช้วิธีการตรวจหาต่างๆ ร่วมกัน
- ระดับการกำจัด เป็นต้น

หากต้องการเข้าสู่หน้าต่างการตั้งค่า ให้คลิก **ThreatSense** ใน การตั้งค่าขั้นสูง สำหรับโมดูลที่ใช้เทคโนโลยี ThreatSense (โปรดดูด้านล่าง) สถานการณ์ของการรักษาความปลอดภัยที่ต่างกันอาจต้องใช้การกำหนดค่าที่ต่างกัน โปรดทราบว่า ThreatSense สามารถกำหนดค่าแยกกันได้สำหรับโมดูลการป้องกันต่อไปนี้:

- การป้องกันระบบไฟล์แบบเรียลไทม์
- การสแกนขณะอยู่ในสถานะไม่ใช้งาน
- การสแกนเมื่อเริ่มต้น
- การป้องกันเอกสาร
- การป้องกันอีเมลไคลเอ็นต์
- การป้องกันการเข้าถึงเว็บ
- การสแกนคอมพิวเตอร์

พารามิเตอร์ ThreatSense มีการปรับให้เหมาะสำหรับแต่ละโมดูลมากที่สุด อีกทั้งการแก้ไขเหล่านี้จะมีผลกับการทำงานของระบบมากด้วยเช่นกัน ตัวอย่างเช่น การเปลี่ยนพารามิเตอร์เพื่อให้สแกนรันไทม์แพ็คเกอร์เสมอ หรือเปิดใช้การวิเคราะห์พฤติกรรมขั้นสูงในโมดูลการป้องกันระบบไฟล์แบบเรียลไทม์อาจทำให้ระบบทำงานช้าลง (โดยปกติโปรแกรมจะสแกนเฉพาะไฟล์ที่สร้างขึ้นใหม่โดยใช้วิธีการเหล่านี้) เราขอแนะนำให้คุณคงพารามิเตอร์ ThreatSense เริ่มต้นไว้สำหรับโมดูลทั้งหมด ยกเว้นการสแกนคอมพิวเตอร์

วัตถุที่จะสแกน

ส่วนนี้จะช่วยให้คุณสามารถกำหนดว่าจะสแกนหาการแฝงตัวจากองค์ประกอบและไฟล์คอมพิวเตอร์ใด

หน่วยความจำที่ใช้งาน – สแกนหาภัยคุกคามที่โจมตีหน่วยความจำที่ใช้งานของระบบ

ส่วนการบูต/UEFI – การสแกนบูตเซคเตอร์สำหรับมัลแวร์ที่มีอยู่ในบันทึกการบูตหลัก อ่านเพิ่มเติมเกี่ยวกับ UEFI ในประมวลศัพท์

ไฟล์อีเมล – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: DBX (Outlook Express) และ EML

อาร์ไคฟ์ – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE และอื่นๆ อีกมากมาย

อาร์ไคฟ์แบบคลายตัวเอง - อาร์ไคฟ์แบบคลายตัวเอง หรือ Self-extracting archives (SFX) คืออาร์ไคฟ์ที่สามารถคลายตัวเองได้

รันไทม์แพ็คเกอร์ – หลังจากเรียกใช้แล้ว รันไทม์แพ็คเกอร์ (ไม่เหมือนกับประเภทที่เก็บเอกสารมาตรฐาน) จะ

คลายออกในหน่วยความจำ นอกเหนือจากแพ็คเกอร์คงที่แบบมาตรฐาน (UPX, yoda, ASPack, FSG เป็นต้น) เครื่องมือสแกนจะสามารถจดจำประเภทหรือแพ็คเกอร์อื่นๆ เพิ่มเติมผ่านการใช้การจำลองรหัส

ตัวเลือกการสแกน

เลือกวิธีที่ใช้เมื่อสแกนหาการแฝงตัวบนระบบ ตัวเลือกที่ใช้ได้มีดังนี้:

การวิเคราะห์พฤติกรรม – การวิเคราะห์พฤติกรรมเป็นอัลกอริทึมที่วิเคราะห์การทำงาน (ที่เป็นอันตราย) ของโปรแกรม ข้อได้เปรียบสำคัญของเทคโนโลยีนี้คือความสามารถในการระบุซอฟต์แวร์ที่เป็นอันตรายซึ่งไม่มีอยู่ก่อนหน้านั้น หรือไม่เป็นที่รู้จักของกลไกตรวจหาก่อนหน้า ข้อเสียคือมีโอกาสที่จะเกิดการเตือนผิดพลาด (แม้จะน้อยมากก็ตาม)

วิเคราะห์พฤติกรรมขั้นสูง/ลายเซ็น DNA - การวิเคราะห์พฤติกรรมขั้นสูงเป็นอัลกอริทึมการวิเคราะห์พฤติกรรมขั้นสูงที่พัฒนาโดย ESET ปรับให้เหมาะสมกับการตรวจหาเวิร์มของคอมพิวเตอร์และม้าโทรจัน และเขียนในภาษาที่ใช้เขียนโปรแกรมระดับสูง การใช้การวิเคราะห์พฤติกรรมขั้นสูงจะช่วยเพิ่มความสามารถในการตรวจหาภัยคุกคามของผลิตภัณฑ์ ESET ได้เป็นอย่างมาก ฐานข้อมูลไวรัสสามารถตรวจหาและระบุไวรัสได้อย่างเชื่อถือได้ การใช้ระบบอัพเดทอัตโนมัติ ทำให้ฐานข้อมูลใหม่ใช้ได้หลังจากค้นพบภัยคุกคามเพียงไม่กี่ชั่วโมง ข้อเสียของฐานข้อมูลไวรัสคือระบบจะตรวจหาไวรัสเฉพาะที่รู้จักเท่านั้น (หรือเวอร์ชันที่มีการแก้ไขเล็กน้อยของไวรัสเหล่านี้)

การกำจัด

การตั้งค่าการกำจัด จะเป็นตัวกำหนดการทำงานของ ESET Endpoint Security ขณะกำจัดวัตถุ

การยกเว้น

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่า ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะสแกน

อื่นๆ

เมื่อกำหนดค่ากลไก ThreatSense สำหรับการสแกนคอมพิวเตอร์ จะสามารถใช้ตัวเลือกในส่วน **อื่นๆ** ได้ดังต่อไปนี้:

สแกนสตรีมข้อมูลสำรอง (ADS) – สตรีมข้อมูลสำรองที่ใช้งานโดยระบบไฟล์ NTFS เป็นการเชื่อมโยงไฟล์และโฟลเดอร์ซึ่งจะไม่ปรากฏสำหรับเทคนิคการสแกนทั่วไป การแฝงตัวจำนวนมากพยายามหลีกเลี่ยงการตรวจหานี้ โดยปลอมแปลงตัวเองเป็นสตรีมข้อมูลสำรอง

เรียกใช้การสแกนเบื้องหลังโดยมีลำดับความสำคัญต่ำ – ลำดับการสแกนแต่ละลำดับจะใช้ทรัพยากรของระบบจำนวนหนึ่ง หากคุณทำงานกับโปรแกรมที่ใช้ทรัพยากรระบบจำนวนมาก คุณสามารถเปิดใช้การสแกนเบื้องหลังที่มีลำดับความสำคัญต่ำ และประหยัดทรัพยากรไว้สำหรับแอพพลิเคชันของคุณ

บันทึกวัตถุทั้งหมด – บันทึกการสแกน จะแสดงไฟล์ที่สแกนแล้วทั้งหมดในอาร์ไคฟ์ที่ขยายในตัว รวมถึงไฟล์ที่ไม่ติดไวรัส (อาจสร้างข้อมูลบันทึกการสแกนจำนวนมากและเพิ่มขนาดไฟล์บันทึกการสแกน)

เปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท – เมื่อเปิดใช้การเพิ่มประสิทธิภาพแบบสมาร์ท ระบบจะใช้การตั้งค่าที่มีประสิทธิภาพที่สุดเพื่อให้แน่ใจว่าการสแกนจะมีประสิทธิภาพและความเร็วสูงสุดไปพร้อมกัน ซึ่งโมดูลการป้องกันต่างๆ จะสแกนข้อมูลอย่างชาญฉลาด โดยใช้ประโยชน์จากวิธีการสแกนต่างๆ และนำมาใช้งานกับประเภทไฟล์ที่ระบุ หากคุณปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท เราจะใช้เฉพาะการตั้งค่าที่ผู้ใช้กำหนดไว้ในแกน ThreatSense ของโมดูลเฉพาะเมื่อทำการสแกนเท่านั้น

เก็บบันทึกการลงเวลาเข้าถึงล่าสุด – เลือกตัวเลือกนี้เพื่อเก็บเวลาแรกเริ่มที่เข้าถึงไฟล์ที่สแกนแทนการอัพเดทเวลาเหล่านั้น (ตัวอย่างเช่น สำหรับใช้กับระบบสำรองข้อมูล)

ขีดจำกัด

ส่วนขีดจำกัดช่วยให้คุณสามารถระบุขนาดสูงสุดของวัตถุ และระดับของอาร์ไคฟ์ที่ซ้อนที่จะสแกน:

การตั้งค่าวัตถุ

ขนาดวัตถุสูงสุด – กำหนดขนาดสูงสุดของวัตถุที่จะสแกน โมดูลป้องกันไวรัสที่กำหนดจะสแกนเฉพาะวัตถุที่เล็กกว่าขนาดที่ระบุเท่านั้น ผู้ที่สามารถแก้ไขตัวเลือกนี้ควรเป็นผู้ใช้ขั้นสูง ซึ่งอาจมีเหตุผลบางอย่างสำหรับการยกเว้นวัตถุขนาดใหญ่จากการสแกน ค่าเริ่มต้น: ไม่จำกัด

เวลาสแกนสูงสุดสำหรับวัตถุ (วินาที) – กำหนดค่าสูงสุดสำหรับสแกนไฟล์ในวัตถุที่มีการบรรจุ (เช่น อาร์ไคฟ์ RAR/ZIP หรืออีเมลที่มีไฟล์แนบหลายรายการ) การตั้งค่านี้จะไม่ถูกปรับใช้สำหรับไฟล์สแตนด์อโลน การสแกนจะหยุดทันทีหากมีการป้อนค่าที่ผู้ใช้กำหนดและพ้นระยะเวลาดังกล่าว โดยไม่คำนึงว่าการสแกนแต่ละไฟล์ในวัตถุที่มีการบรรจุจะเสร็จสิ้นแล้วหรือไม่ ในกรณีที่อาร์ไคฟ์บรรจุไฟล์ขนาดใหญ่ การสแกนจะหยุดช้ากว่าไฟล์ที่ถูกดึงข้อมูลจากอาร์ไคฟ์ (ตัวอย่างเช่น เมื่อตัวแปรที่ผู้ใช้กำหนดคือ 3 วินาที แต่การดึงข้อมูลของไฟล์คือ 5 วินาที) ไฟล์ที่เหลือในอาร์ไคฟ์จะไม่ถูกสแกนเมื่อพ้นระยะเวลาดังกล่าว หากต้องการจำกัดเวลาในการสแกน ซึ่งรวมถึงอาร์ไคฟ์ขนาดใหญ่ ให้ใช้ **ขนาดวัตถุสูงสุด** และ **ขนาดไฟล์สูงสุดในอาร์ไคฟ์** (ไม่แนะนำให้ใช้เนื่องจากความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นได้) ค่าเริ่มต้น: ไม่จำกัด

ตั้งค่าการสแกนอาร์ไคฟ์

ระดับการซ้อนของอาร์ไคฟ์ – ระบุความลึกสูงสุดของการสแกนอาร์ไคฟ์ ค่าเริ่มต้น: 10

ขนาดไฟล์สูงสุดในอาร์ไคฟ์ – ตัวเลือกนี้ช่วยให้คุณสามารถระบุขนาดไฟล์สูงสุดสำหรับไฟล์ที่อยู่ในอาร์ไคฟ์ (เมื่อดึงข้อมูล) ที่จะสแกนได้ ค่าเริ่มต้น: ไม่จำกัด ค่าสูงสุดคือ 3 GB

เราไม่แนะนำให้แก้ไขค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดที่จะต้องแก้ไขค่านี้ในสถานการณ์ปกติ

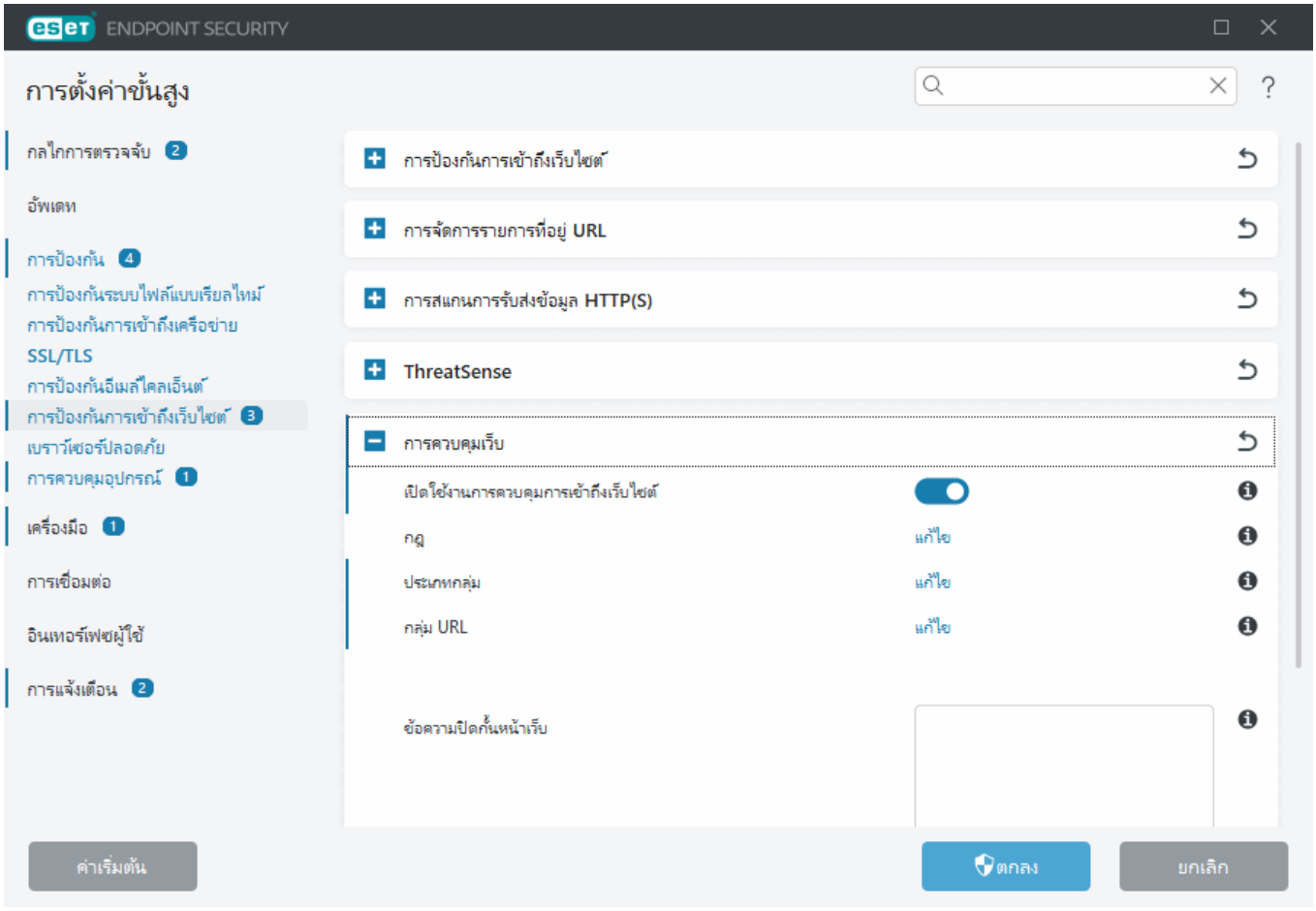
การควบคุมเว็บ

ส่วนการควบคุมการเข้าถึงเว็บไซต์จะช่วยให้คุณสามารถกำหนดการตั้งค่าเพื่อปกป้องบริษัทของคุณจากความเสี่ยงในการรับผิดทางกฎหมาย การควบคุมการเข้าถึงเว็บไซต์สามารถควบคุมดูแลการเข้าถึงเว็บไซต์ที่ฝ่าฝืนสิทธิในทรัพย์สินทางปัญญา เป้าหมายคือเพื่อป้องกันพนักงานจากการเข้าถึงหน้าต่างๆ ที่มีเนื้อหาไม่เหมาะสมหรือเป็นอันตราย หรือหน้าที่อาจส่งผลกระทบด้านลบต่อประสิทธิภาพ

การควบคุมการเข้าถึงเว็บไซต์ช่วยให้คุณบล็อกหน้าเว็บที่อาจมีเนื้อหาที่ไม่เหมาะสม นอกจากนี้ นายจ้างหรือผู้ดูแลระบบสามารถห้ามการเข้าถึงเว็บไซต์ที่กำหนดไว้ล่วงหน้าได้มากกว่า 27 ประเภทและกว่า 140 ประเภทย่อย

การควบคุมการเข้าถึงเว็บไซต์จะปิดใช้งานตามค่าเริ่มต้น หากต้องการเปิดการใช้งานการควบคุมเว็บ:

1. เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันการเข้าถึงเว็บไซต์** > **การป้องกันการเข้าถึงเว็บไซต์**
2. เปิดใช้งานปุ่มสลับ **เปิดใช้งานการควบคุมการเข้าถึงเว็บไซต์** เพื่อเปิดใช้งานการควบคุมการเข้าถึงเว็บไซต์ใน ESET Endpoint Security
3. กำหนดค่าการเข้าถึงหน้าเว็บที่เฉพาะเจาะจง คลิก **แก้ไข** ถัดจาก **กฎ** เพื่อเข้าถึง หน้าต่าง ตัวแก้ไขกฎการควบคุมเว็บไซต์

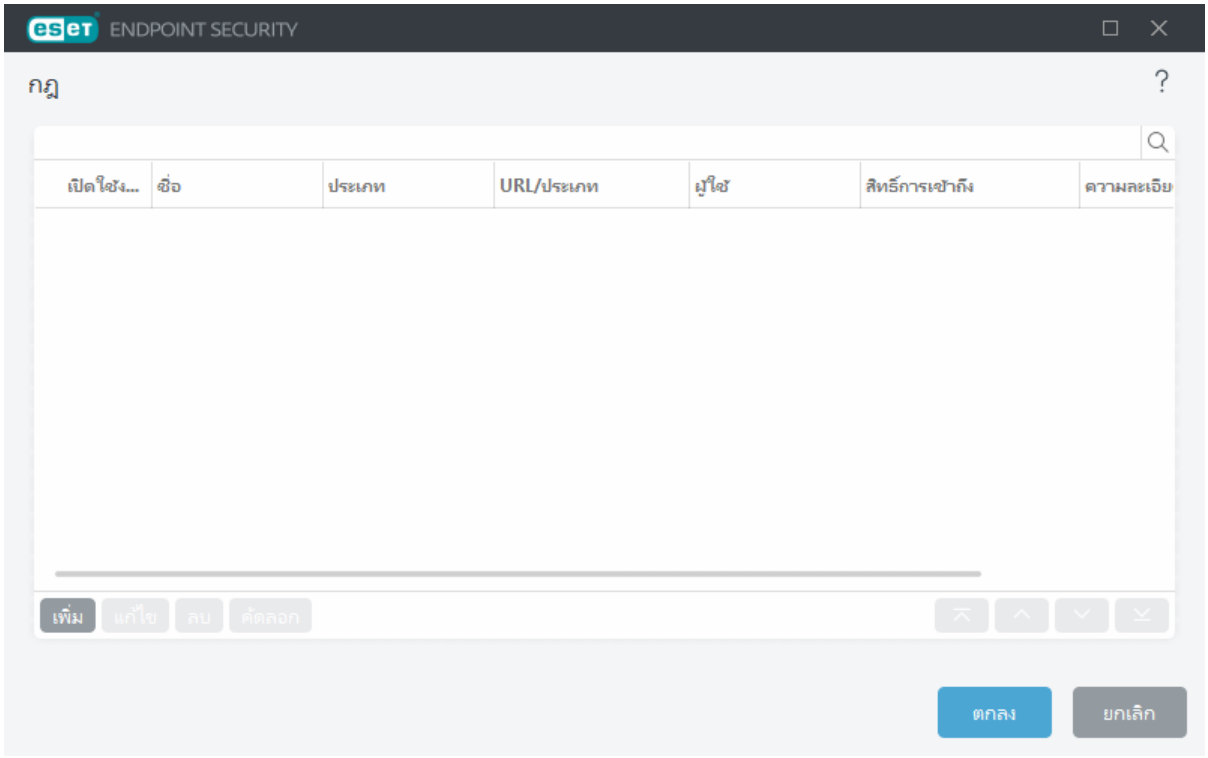


ช่อง **ข้อความหน้าเว็บที่ถูกบล็อก** และ **กราฟิกหน้าเว็บที่ถูกบล็อก** จะอนุญาตให้คุณ ปรับแต่งข้อความที่ปรากฏเมื่อเว็บไซต์ถูกบล็อก

หากคุณต้องการปิดกั้นหน้าเว็บทั้งหมด และเหลือไว้ให้ใช้งานเพียงบางหน้าเท่านั้น ให้ใช้ การจัดการที่อยู่ URL

กฎการควบคุมการเข้าถึงเว็บไซต์

หน้าต่าง **ตัวแก้ไขกฎ** จะแสดงกฎที่มีอยู่ตาม URL หรือตามประเภท



รายการกฎประกอบด้วยคำอธิบายกฎจำนวนมาก เช่น ชื่อ ประเภทการปิดกั้น การทำงานหลังจากจับคู่กฎการควบคุมการเข้าถึงเว็บไซต์และความรุนแรงของการบันทึก

คลิกที่ **เพิ่ม** หรือ **แก้ไข** เพื่อจัดการกฎ คลิก **คัดลอก** เพื่อสร้างกฎใหม่โดยมีตัวเลือกที่กำหนดไว้ล่วงหน้า ซึ่งใช้สำหรับกฎอื่นที่เลือกไว้ โดยการกด **Ctrl** และคลิก คุณสามารถเลือกหลายกฎและลบกฎที่เลือกทั้งหมดได้ กล่องทำเครื่องหมาย**เปิดใช้งาน** จะปิดใช้งานหรือเปิดใช้งานกฎ ซึ่งจะมีประโยชน์ถ้าคุณไม่ต้องการลบกฎอย่างถาวรในกรณีที่คุณต้องการใช้อีกในอนาคต

กฎจะจัดเรียงไว้ตามลำดับความสำคัญ โดยกฎที่มีลำดับความสำคัญสูงจะอยู่ด้านบนสุด หากต้องการเปลี่ยนความสำคัญของกฎ ให้เลือกกฎและคลิกปุ่มลูกศรเพื่อเพิ่มหรือลดความสำคัญของกฎ คลิกลูกศรคู่เพื่อย้ายกฎไปยังบนสุดหรือล่างสุดของรายการ

ดูเพิ่มเติมเกี่ยวกับ การสร้างกฎ

การเพิ่มกฎการควบคุมเว็บ

หน้าต่างกฎการควบคุมเว็บจะช่วยให้คุณสามารถสร้างหรือแก้ไขกฎการกรองสำหรับควบคุมเว็บที่มีอยู่ได้

ชื่อ

ป้อนคำอธิบายของกฎในช่อง **ชื่อ** เพื่อคำอธิบายที่ดีขึ้น

เปิดใช้งาน

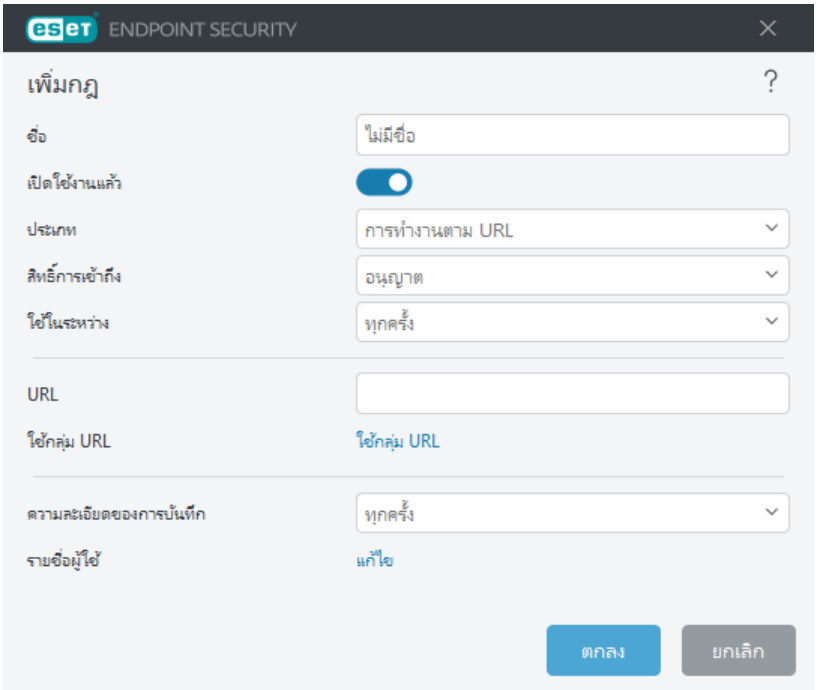
คลิกสวิตช์ **เปิดใช้งาน** เพื่อปิดหรือเปิดใช้งานกฎ ซึ่งจะมีประโยชน์หากคุณไม่ต้องการลบกฎอย่างถาวร

การทำงาน

เลือกระหว่าง **การกระทำตาม URL** หรือ **การกระทำแบบหมวดหมู่**:

การทำงานตาม URL

สำหรับกฎที่ควบคุมการเข้าถึงเว็บไซต์ที่ระบุ ให้ป้อน URL ลงในช่อง **URL**
สัญลักษณ์พิเศษ * (ดอกจัน) และ ? (เครื่องหมายคำถาม) จะไม่สามารถใช้ในรายการที่อยู่ URL ได้ เมื่อสร้างกลุ่ม URL ที่มีเว็บไซต์ที่มาพร้อมกับโดเมนระดับบนหลายๆ โดเมน (TLDs) ต้องเพิ่มแต่ละ TLD แยกกัน หากคุณเพิ่มโดเมนลงในกลุ่ม เนื้อหาทั้งหมดที่อยู่บนโดเมนนี้และโดเมนย่อยทั้งหมด (ตัวอย่างเช่น *sub.examplepage.com*) จะถูกปิดกั้นหรืออนุญาตตามการเลือกการทำงานตาม URL ของคุณ
URL หรือ **ใช้กลุ่ม URL** – กำหนดว่าจะใช้ลิงก์ URL หรือ กลุ่ม URL ของลิงก์ที่จะอนุญาต บล็อก หรือเตือนผู้ใช้เมื่อเข้าถึงหนึ่งใน URL เหล่านี้



การทำงานตามประเภท

กฎจะมีผลใช้ตามหมวดหมู่เว็บไซต์
หมวดหมู่ URL หรือ **ใช้กลุ่ม** – เลือกหมวดหมู่เว็บไซต์หรือ กลุ่มหมวดหมู่ ที่จะอนุญาต บล็อก หรือเตือนผู้ใช้เมื่อตรวจพบหนึ่งในหมวดหมู่เหล่านี้

สิทธิ์การเข้าถึง

- **อนุญาต** – อนุญาตการเข้าถึงที่อยู่/หมวดหมู่ URL
- **เตือน** – บล็อกการเข้าถึงที่อยู่/หมวดหมู่ URL คุณสามารถคลิก **ย้อนกลับ** เพื่อกลับไปยังเว็บไซต์ก่อนหน้า หรือคลิก **ดำเนินการต่อ** เพื่อเข้าถึงเว็บไซต์ หากคุณคลิก **ดำเนินการต่อ** หน้าการบล็อกจะไม่ปรากฏในครั้งต่อไปที่คุณเยี่ยมชมเว็บไซต์
- **เตือนทุกครั้ง** – บล็อกการเข้าถึงที่อยู่/หมวดหมู่ URL คุณสามารถคลิก **ย้อนกลับ** เพื่อกลับไปยังเว็บไซต์ก่อนหน้า หรือคลิก **ดำเนินการต่อ** เพื่อเข้าถึงเว็บไซต์ หน้าการบล็อกจะปรากฏขึ้นทุกครั้งที่คุณเข้าสู่เว็บไซต์
- **บล็อก** – บล็อกการเข้าถึงที่อยู่/หมวดหมู่ URL คุณสามารถคลิก **ย้อนกลับ** เพื่อกลับไปยังเว็บไซต์ก่อนหน้า

ใช้ในระหว่าง

ให้คุณใช้กฎที่สร้างขึ้นได้ในช่วงเวลาหนึ่ง เลือกช่วงเวลาที่สร้างจากเมนูแบบเลื่อนลงสำหรับ **นำไปใช้ระหว่าง** ข้อมูลเพิ่มเติมเกี่ยวกับสล็อตเวลา

ความละเอียดของการบันทึก

- **เสมอ** – บันทึกการสื่อสารออนไลน์ทั้งหมด
- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม
- **ข้อมูล** – บันทึกข้อความแจ้งข้อมูล รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน
- **ไม่มี** – จะไม่สร้างบันทึกใดๆ

ความละเอียดของการบันทึกสามารถกำหนดค่าต่างหากสำหรับแต่ละรายการได้ บันทึกที่มีสถานะ **คำเตือน** สามารถรวบรวมได้โดย ESET PROTECT

รายชื่อผู้ใช้

- **เพิ่ม** – เปิดหน้าต่างข้อความ **เลือกผู้ใช้หรือกลุ่ม** ซึ่งจะทำให้คุณสามารถเลือกผู้ใช้ที่ต้องการได้ เมื่อไม่มีการป้อนผู้ใช้ กฎจะถูกใช้กับผู้ใช้ทุกคน
- **ลบออก** – ลบผู้ใช้ที่เลือกออกจากตัวกรอง

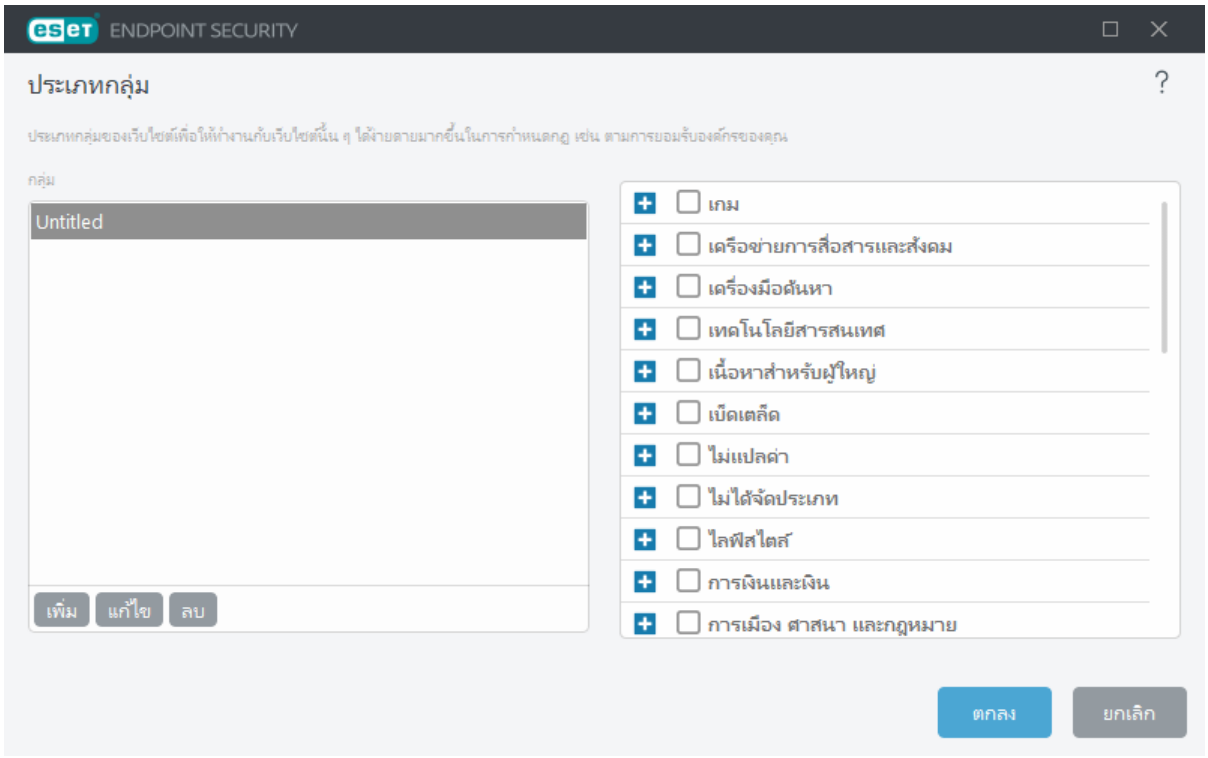
ประเภทกลุ่ม

หน้าต่างกลุ่มประเภทแบ่งออกเป็นสองส่วน ส่วนซ้ายของหน้าต่างจะประกอบด้วยรายการของกลุ่มประเภท

- **เพิ่ม** – คลิกเพื่อสร้างกลุ่มประเภทใหม่
- **แก้ไข** – คลิกเพื่อแก้ไขกลุ่มประเภทที่มีอยู่
- **ลบออก** – เลือกและคลิกตัวเลือกนี้หากคุณต้องการลบกลุ่มประเภทที่มีอยู่ออกจากรายการกลุ่มประเภท

ส่วนขวาของหน้าต่างประกอบด้วยรายการประเภทและประเภทย่อย ให้เลือกประเภทในรายการประเภทเพื่อแสดงประเภทย่อย โดยแต่ละกลุ่มจะประกอบด้วยประเภทย่อยสำหรับผู้ใหญ่และ/หรือไม่เหมาะสมโดยทั่วไป รวมถึงประเภทที่สามารถยอมรับได้โดยทั่วไป เมื่อคุณเปิดหน้าต่างตัวกลุ่มประเภทและคลิกกลุ่มแรก คุณสามารถเพิ่มหรือลบประเภท/ประเภทย่อยจากรายการกลุ่มที่เหมาะสม (ตัวอย่างเช่น ความรุนแรง หรือ อาวุธ) นอกจากนี้ยังสามารถบล็อกหน้าเว็บที่มีเนื้อหาที่ไม่เหมาะสม โดยระบบจะแจ้งผู้ใช้เมื่อเข้าถึงหน้าเว็บที่ถูกบล็อก

เลือกกล่องทำเครื่องหมายเพื่อเพิ่มหรือลบประเภทย่อยไปยังกลุ่มเฉพาะ



ตัวอย่างของประเภทที่ผู้ใช้อาจไม่คุ้นเคยได้แก่:

- **เบ็ดเตล็ด** – มักเป็นที่อยู่ IP ส่วนบุคคล (ในระบบ) เช่น อินทราเน็ต, 192.168.0.0/16 เป็นต้น เมื่อคุณได้รับรหัสข้อผิดพลาด 403 หรือ 404 เว็บไซต์จะจับคู่ประเภทนี้ด้วย
- **ไม่แปลค่า** – ประเภทนี้ประกอบด้วยหน้าเว็บที่ไม่มีการแปลค่า เนื่องจากเกิดข้อผิดพลาดในขณะเชื่อมต่อกับ

กลไกฐานข้อมูลการควบคุมการเข้าถึงเว็บไซต์

- **ไม่ได้จัดประเภท** – หน้าเว็บที่ไม่รู้จักซึ่งยังไม่มีอยู่ในฐานข้อมูลการควบคุมการเข้าถึงเว็บไซต์
- **พร็อกซี** – ระบบอาจใช้หน้าเว็บ เช่น นิรนาม เครื่องมือเปลี่ยนเส้นทาง หรือเซิร์ฟเวอร์พร็อกซีสาธารณะเพื่อให้สามารถเข้าถึงหน้าเว็บ (โดยไม่ระบุชื่อ) ซึ่งมักถูกห้ามโดยตัวกรองการควบคุมการเข้าถึงเว็บไซต์
- **การใช้ไฟล์ร่วมกัน** – หน้าเว็บเหล่านี้มีข้อมูลจำนวนมาก เช่น รูปภาพ วิดีโอ หรือหนังสืออิเล็กทรอนิกส์ ซึ่งอาจมีความเสี่ยง ว่าไซต์เหล่านี้จะมีเนื้อหาที่อาจไม่เหมาะสมหรือเนื้อหาสำหรับผู้ใหญ่

> คุณสามารถรายงาน การจัดหมวดหมู่ที่ไม่ถูกต้องของ URL ได้

> ประเภทย่อยสามารถอยู่ในกลุ่มใดๆ ก็ได้ มีประเภทย่อยบางประเภทที่ไม่รวมอยู่ในกลุ่มที่กำหนดไว้ (ตัวอย่าง เช่น เกม) ในการจับคู่ประเภทย่อยที่ต้องการโดยใช้ตัวกรองการควบคุมการเข้าถึงเว็บไซต์ ให้เพิ่มในกลุ่มที่คุณต้องการ

กลุ่ม URL

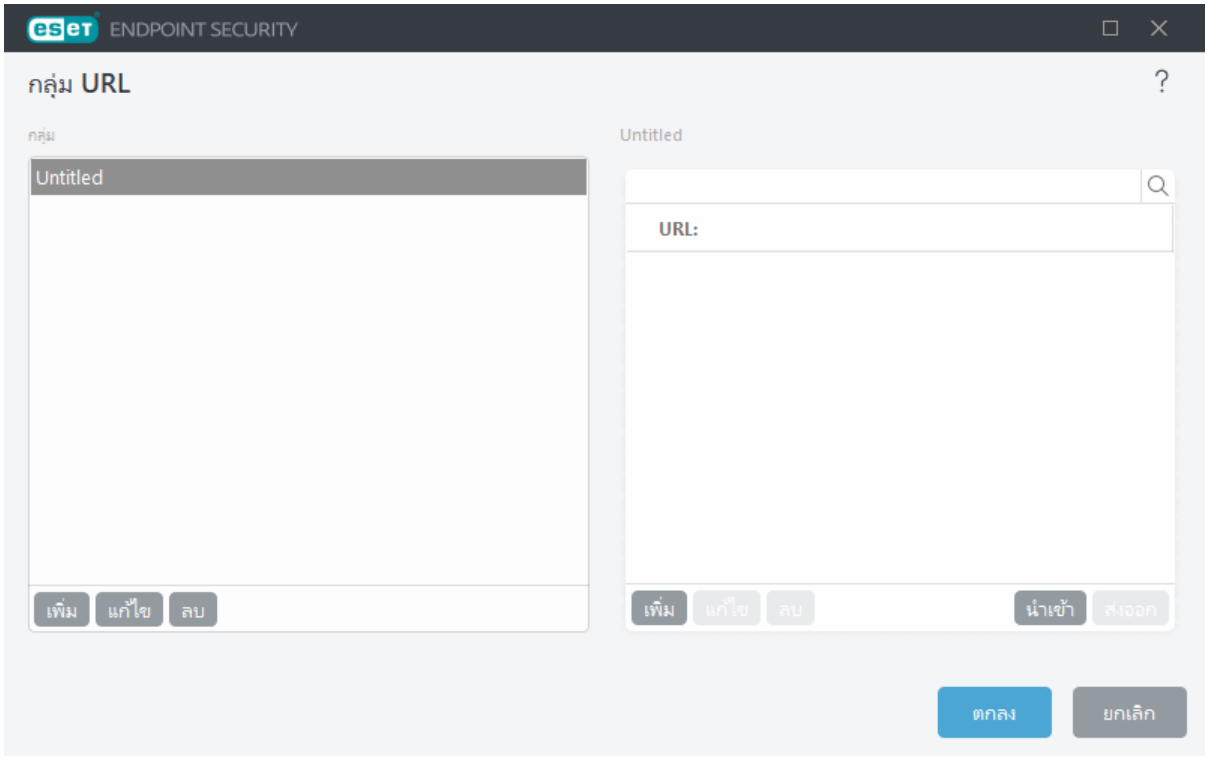
กลุ่ม URL จะอนุญาตให้คุณสร้างกลุ่มที่มีลิงก์ URL หลายลิงก์ที่คุณต้องการสร้างกฎ (อนุญาต/บล็อกเว็บไซต์บางเว็บไซต์)

สร้างกลุ่ม URL ใหม่

หากต้องการสร้างกลุ่ม URL ใหม่ให้คลิก **เพิ่ม** และป้อนชื่อของกลุ่ม URL ใหม่

การใช้กลุ่ม URL จะมีประโยชน์เมื่อผู้ดูแลระบบต้องการสร้างกฎสำหรับหน้าเว็บเพิ่มเติม (ปิดกั้นหรืออนุญาต โดยขึ้นอยู่กับการเลือกของคุณ)

เพิ่มที่อยู่ URL ไปยังรายการกลุ่ม URL - ด้วยตนเอง



หากต้องการเพิ่มที่อยู่ URL ไปยังรายการให้เลือกกลุ่ม URL แล้วคลิก **เพิ่ม** ตรงมุมล่างขวาของหน้าต่าง

สัญลักษณ์พิเศษ * (ดอกจัน) และ ? (เครื่องหมายคำถาม) จะไม่สามารถใช้ในรายการที่อยู่ URL ได้

ไม่จำเป็นต้องป้อนชื่อเต็มของโดเมนด้วย http:// หรือ https://

หากคุณเพิ่มโดเมนไปยังกลุ่ม เนื้อหาทั้งหมดที่อยู่ในโดเมนนี้และโดเมนย่อยทั้งหมด (ตัวอย่างเช่น *sub.examplepage.com*) จะถูกปิดกั้นหรือได้รับอนุญาตขึ้นอยู่กับการเลือกการทำงานตาม URL ของคุณ

หากมีความขัดแย้งระหว่างกฎสองข้อในโดเมนเดียวกันโดยกฎข้อแรกนั้นดำเนินการปิดกั้นโดเมน และกฎข้อที่สองนั้นอนุญาตโดเมน โดเมนหรือที่อยู่ IP ดังกล่าวจะถูกปิดกั้นอยู่ดี สำหรับข้อมูลเพิ่มเติมในการสร้างกฎ ดูการทำงานตาม URL

เพิ่มที่อยู่ URL ไปยังรายการกลุ่ม URL - นำเข้าโดยใช้ไฟล์ .txt

คลิก **นำเข้า** เพื่อนำเข้าไฟล์ที่มีรายการของที่อยู่ URL (แยกค่าด้วยตัวแบ่งบรรทัด ตัวอย่างเช่นไฟล์ .txt โดยใช้การเข้ารหัส UTF-8) สัญลักษณ์พิเศษ * (ดอกจัน) และ ? สัญลักษณ์พิเศษ * (ดอกจัน) และ ? (เครื่องหมายคำถาม) จะไม่สามารถใช้ในรายการที่อยู่ URL ได้

การใช้กลุ่ม URL ในการควบคุมการเข้าถึงเว็บไซต์

หากคุณต้องการตั้งค่าการกระทำให้ดำเนินการกับเฉพาะกลุ่ม URL บางกลุ่ม ให้เปิด ตัวแก้ไขกฎการควบคุมการเข้าถึงเว็บไซต์ เลือกกลุ่ม URL ของคุณโดยใช้ เมนูแบบเลื่อนลง ปรับพารามิเตอร์อื่นๆ แล้วจากนั้นคลิก **ตกลง**

> การปิดกั้นหรือการอนุญาตหน้าเว็บหนึ่งจะมีความถูกต้องมากกว่าการปิดกั้นหรือการอนุญาตหน้าเว็บทั้งประเภท โปรดระมัดระวังเมื่อเปลี่ยนการตั้งค่าเหล่านี้ และเพิ่มประเภท/หน้าเว็บในรายการ

ปิดกั้นการปรับแต่งข้อความหน้าเว็บแล้ว

ช่อง **ข้อความปิดกั้นหน้าเว็บ** และ **ปิดกั้นกราฟิกหน้าเว็บ** จะอนุญาตให้คุณปรับแต่งข้อความที่ปรากฏได้ง่ายๆ เมื่อเว็บไซต์ถูกปิดกั้น

การใช้งาน

มาปิดกั้นประเภทเว็บไซต์ที่เป็น "อาวุธ" กันเถอะ

ตัวอย่างของข้อความหน้าเว็บที่ถูกปิดกั้นจะเป็น:

```
หน้าเว็บ %URL_OR_CATEGORY% ถูกปิดกั้นเนื่องจากพิจารณาว่าไม่เหมาะสมหรือมีเนื้อหาที่เป็นอันตราย
โปรดติดต่อผู้ดูแลระบบของคุณสำหรับรายละเอียด
```

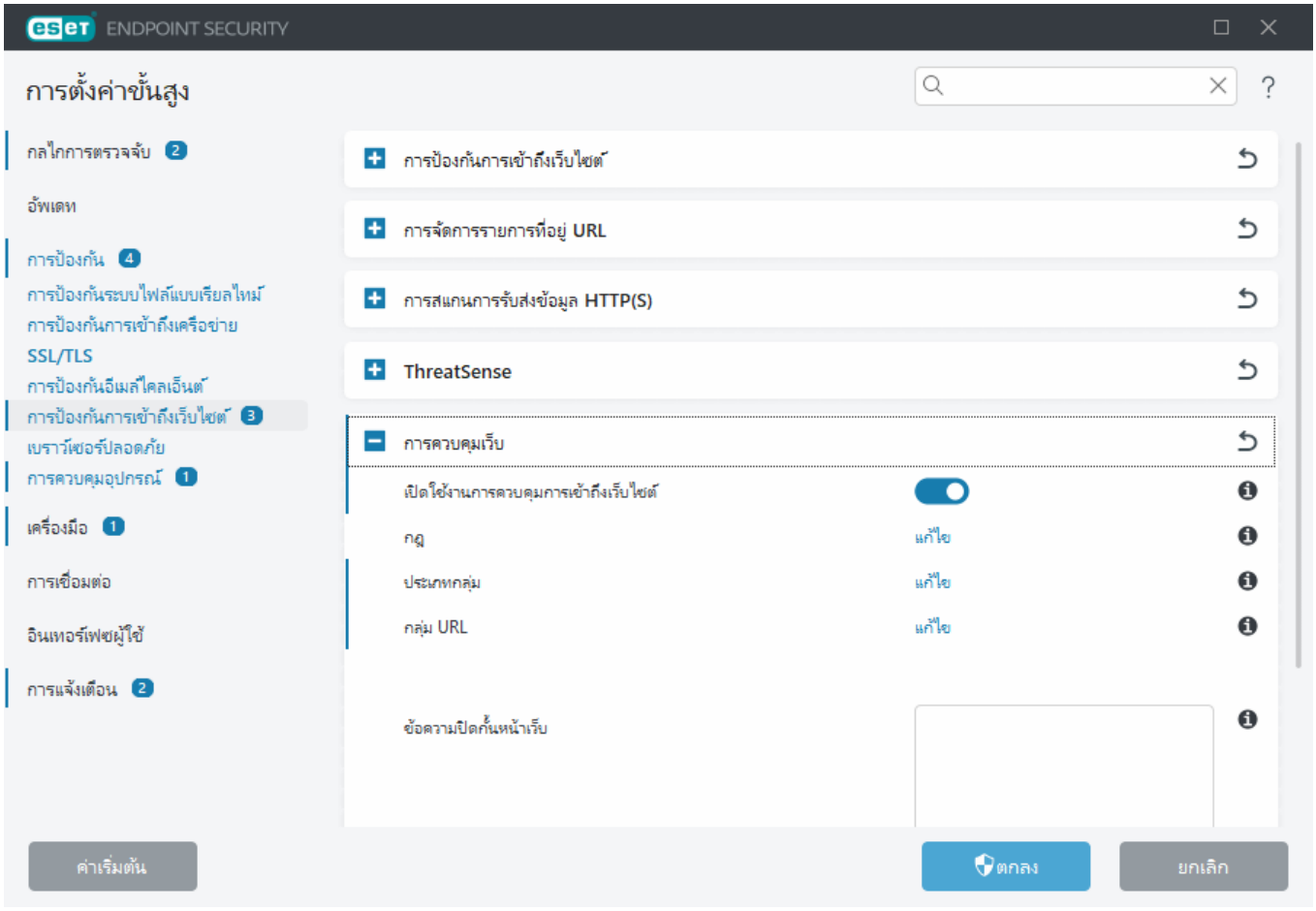
ตัวแปร	คำอธิบาย
%CATEGORY%	ปิดกั้นประเภทการควบคุมการเข้าถึงเว็บไซต์
%URL_OR_CATEGORY%	ปิดกั้นเว็บไซต์หรือประเภทการควบคุมการเข้าถึงเว็บไซต์ (ขึ้นอยู่กับกฎการปิดกั้นการควบคุมการเข้าถึงเว็บไซต์).
%STR_GOBACK%	ค่าปุ่ม "ย้อนกลับ"
%product_name%	ชื่อของผลิตภัณฑ์ ESET (ESET Endpoint Security)
%product_version%	เวอร์ชันของผลิตภัณฑ์ ESET

ตัวอย่างของกราฟิกหน้าเว็บที่ถูกปิดกั้นจะเป็น:

```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

ขนาดรูปภาพ (ความกว้าง/ความสูง) จะถูกปรับขนาดโดยอัตโนมัติหากมีขนาดใหญ่เกินไป

การกำหนดค่าใน ESET Endpoint Security จะมีลักษณะดังนี้:



หน้าต่างข้อความ - การควบคุมการเข้าถึงเว็บไซต์

หน้าที่หลักของการควบคุมการเข้าถึงเว็บไซต์คือการควบคุมเว็บไซต์ที่เข้าถึงของผู้ใช้แต่ละคนในเครือข่ายบริษัท ผู้ดูแลระบบเครือข่ายต้องสามารถกำหนดประเภทของเว็บไซต์ที่ผู้ใช้สามารถเข้าถึงได้ ไม่ว่าจะเป็นการเข้าถึงโดยผู้ใช้หรือกลุ่มผู้ใช้ การรวมเข้ากับบริการไดเรกทอรีจะทำให้สามารถใช้กลุ่มไดเรกทอรีที่ใช้งานสำหรับการกำหนดค่าการควบคุมการเข้าถึงเว็บไซต์ การทำงานนี้จะปิดใช้งานตามค่าเริ่มต้น ถ้าคุณต้องการเปิดใช้งานคุณลักษณะนี้ ให้ตั้ง **เปิดใช้งานการควบคุมการเข้าถึงเว็บไซต์** เป็นเปิด คลิก **แก้ไข** เพื่อเข้าถึง ตัวแก้ไขกฎ คลิก **แก้ไข** ถัดจาก กลุ่มประเภท เพื่อแก้ไขกลุ่มที่กำหนดไว้ หรือคลิก **แก้ไข** ที่อยู่ถัดจาก ตัวแก้ไขกลุ่ม URL เพื่อเพิ่มกลุ่ม URL ใหม่

เบราว์เซอร์ที่ปลอดภัย

เบราว์เซอร์ปลอดภัยเป็นระดับการป้องกันเพิ่มเติมซึ่งออกแบบมาเพื่อปกป้องข้อมูลการเงินของคุณในระหว่างที่ทำธุรกรรมออนไลน์

ระบบชื่อเสียงของ ESET LiveGrid® จะต้องถูกเปิดใช้งาน (เปิดใช้งานโดยค่าเริ่มต้น) เพื่อให้แน่ใจว่าการป้องกันเบราว์เซอร์ปลอดภัยทำงานอย่างถูกต้อง

หากต้องการกำหนดค่าลักษณะการทำงานของเบราว์เซอร์ปลอดภัย ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **เบราว์เซอร์ปลอดภัย**

คุณสามารถตัวเลือกการกำหนดค่าเบราว์เซอร์ปลอดภัยต่อไปนี้ได้:

- **รักษาความปลอดภัยเบราว์เซอร์ทั้งหมด** เว็บเบราว์เซอร์ที่รองรับทั้งหมดจะเริ่มต้นในโหมดปลอดภัย ซึ่งช่วยให้คุณสามารถเรียกใช้อินเทอร์เน็ต เข้าถึงธนาคารบนอินเทอร์เน็ต และซื้อของออนไลน์ รวมถึงการทำธุรกรรมในหน้าต่างเบราว์เซอร์ที่มีการป้องกันโดยไม่ต้องเปลี่ยนเส้นทาง

พื้นฐาน

การป้องกันเบราว์เซอร์

เปิดใช้งาน **ป้องกันเบราว์เซอร์ทั้งหมด** เพื่อเริ่มใช้งาน เว็บเบราว์เซอร์ที่รองรับ ในโหมดปลอดภัย ซึ่งช่วยให้คุณสามารถเรียกใช้อินเทอร์เน็ต เข้าถึงธนาคารบนอินเทอร์เน็ต และซื้อของออนไลน์ รวมถึงการทำธุรกรรมในหน้าต่างเบราว์เซอร์ที่มีการป้องกันโดยไม่ต้องเปลี่ยนเส้นทาง

โหมดการติดตั้งส่วนขยาย – จากเมนูแบบเลื่อนลง คุณสามารถเลือกว่าจะอนุญาตส่วนขยายใดให้สามารถติดตั้งโดยเบราว์เซอร์ที่ ESET ป้องกันได้: การเปลี่ยนโหมดการติดตั้งส่วนขยายจะไม่มีผลกับส่วนขยายเบราว์เซอร์ที่ติดตั้งไว้ก่อนหน้านี้:

- **ส่วนขยายที่จำเป็น** – ในโหมดนี้ จะอนุญาตเฉพาะส่วนขยายที่จำเป็นที่สุดที่พัฒนาโดยผู้ผลิตเบราว์เซอร์เฉพาะรายเท่านั้น
- **ส่วนขยายทั้งหมด** – ในโหมดนี้ จะอนุญาตส่วนขยายทั้งหมดที่ได้รับการสนับสนุนโดยเบราว์เซอร์เฉพาะ

เบราว์เซอร์ที่มีการป้องกัน

การป้องกันหน่วยความจำที่ได้รับการปรับปรุง – หากเปิดใช้งาน หน่วยความจำของเบราว์เซอร์ที่ปลอดภัยจะได้รับการป้องกันไม่ให้ถูกสอดส่องโดยกระบวนการอื่นๆ

การป้องกันแป้นพิมพ์ – หากเปิดใช้งานแล้ว ข้อมูลที่ป้อนผ่านแป้นพิมพ์ไปในเบราว์เซอร์ที่ปลอดภัยจะถูกซ่อนจากแอพพลิเคชันอื่น การเปิดใช้งานจะเพิ่มการป้องกัน เครื่องมือบันทึกการกดแป้นพิมพ์

กรอบสีเขียวของเบราว์เซอร์ – หากปิดใช้งาน การแจ้งเตือนข้อมูลในเบราว์เซอร์ และกรอบสีเขียวรอบๆ เบราว์เซอร์จะถูกซ่อนไว้

ตั้งค่าการแจ้งเตือนแบบโต้ตอบของเบราว์เซอร์ปลอดภัย – ช่วยให้คุณเปิดหน้าต่างการแจ้งเตือนแบบโต้ตอบได้

ในบางสถานการณ์ การแจ้งเตือนแบบโต้ตอบเฉพาะจะแสดงเมื่อมีข้อผิดพลาดในการเริ่มต้นเบราว์เซอร์ปลอดภัยอย่างถูกต้องเท่านั้น หากต้องการข้อมูลเพิ่มเติม โปรดดู การเตือนแบบโต้ตอบ

การแจ้งเตือนในเบราว์เซอร์

เบราว์เซอร์ที่มีการป้องกันจะแจ้งให้คุณทราบเกี่ยวกับสถานะปัจจุบันผ่านการแจ้งเตือนในเบราว์เซอร์และสีของกรอบเบราว์เซอร์

การแจ้งเตือนในเบราว์เซอร์จะแสดงในแท็บทางด้านขวา

หากต้องการขยายการแจ้งเตือนในเบราว์เซอร์ ให้คลิกไอคอน ESET หากต้องการย่อขนาดการแจ้งเตือน ให้คลิกข้อความการแจ้งเตือน หากต้องการปิดการแจ้งเตือนข้อมูลและกรอบเบราว์เซอร์สีเขียว ให้คลิกไอคอนปิด

สามารถปิดได้เฉพาะการแจ้งเตือนข้อมูลและกรอบเบราว์เซอร์สีเขียวเท่านั้น

การแจ้งเตือนในเบราว์เซอร์

ประเภทการแจ้งเตือน	สถานะ
การแจ้งเตือนแบบมีข้อมูลและ กรอบเบราว์เซอร์สีเขียว	การป้องกันสูงสุดจะมั่นใจได้และการแจ้งเตือนในเบราว์เซอร์จะย่อขนาดลงตามค่าเริ่มต้น
คำเตือนและกรอบเบราว์เซอร์สีส้ม	เบราว์เซอร์ที่มีการป้องกันต้องการความสนใจจากคุณหากมีปัญหาที่ไม่ร้ายแรง สำหรับข้อมูลเพิ่มเติมเกี่ยวกับปัญหาหรือวิธีแก้ไขปัญหา ให้ทำตามคำแนะนำของการแจ้งเตือนในเบราว์เซอร์
การเตือนความปลอดภัยและกรอบเบราว์เซอร์สีแดง	เบราว์เซอร์ไม่ได้รับการป้องกัน ให้รีสตาร์ทเบราว์เซอร์เพื่อให้แน่ใจว่าการป้องกันทำงานอยู่ หากต้องการแก้ไขข้อขัดแย้งกับไฟล์ที่โหลดในเบราว์เซอร์ ให้เปิด ไฟล์บันทึก > **เบราว์เซอร์ปลอดภัย** และตรวจสอบให้แน่ใจว่าไฟล์ที่บันทึกไว้จะไม่โหลดในครั้งต่อไปที่คุณเริ่มเบราว์เซอร์ หากปัญหายังคงอยู่ โปรดติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET โดยทำตามคำแนะนำใน บทความฐานความรู้ ของเรา

การควบคุมอุปกรณ์

ESET Endpoint Security มอบฟังก์ชันการควบคุมแบบอัตโนมัติกับอุปกรณ์ (CD/DVD/USB/ฯลฯ) โมดูลนี้จะช่วยให้คุณสามารถปิดกั้นหรือปรับตัวกรอง/สิทธิ์ที่ขยาย และกำหนดความสามารถของผู้ใช้ในการเข้าถึงและทำงานกับอุปกรณ์

เหล่านี้ได้ คุณลักษณะนี้เป็นประโยชน์ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์ต้องการป้องกันไม่ให้ผู้ใช้ใช้งานอุปกรณ์ซึ่งมีเนื้อหาที่ไม่พึงประสงค์

อุปกรณ์ภายนอกที่สนับสนุน:

- พื้นที่เก็บข้อมูลดิสก์ (HDD, USB ดิสก์ที่ถอดเข้าออกได้)
- ซีดี/ดีวีดี
- USB เครื่องพิมพ์
- FireWireพื้นที่จัดเก็บข้อมูล
- Bluetooth อุปกรณ์
- เครื่องอ่านสมาร์ทการ์ด
- อุปกรณ์ภาพ
- โมเด็ม
- LPT/COM พอร์ต
- อุปกรณ์พกพา (อุปกรณ์ที่ใช้พลังงานจากแบตเตอรี่ เช่น เครื่องเล่นสื่อ, สมาร์ทโฟน, อุปกรณ์ Plug and Play เป็นต้น)
- อุปกรณ์ทุกประเภท

ตัวเลือกการตั้งค่าการควบคุมอุปกรณ์นั้นสามารถแก้ไขได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **สื่อที่ถอดเข้าออกได้**

คลิกปุ่มสลับ **เปิดใช้การควบคุมอุปกรณ์** เพื่อเปิดใช้งานฟีเจอร์การควบคุมอุปกรณ์ใน ESET Endpoint Security คุณต้องรีสตาร์ทคอมพิวเตอร์เพื่อให้การเปลี่ยนแปลงนี้มีผล เมื่อเปิดใช้งานการควบคุมอุปกรณ์แล้ว คุณจะสามารถกำหนด **กฎ** ในหน้าต่าง ตัวแก้ไขกฎ ได้

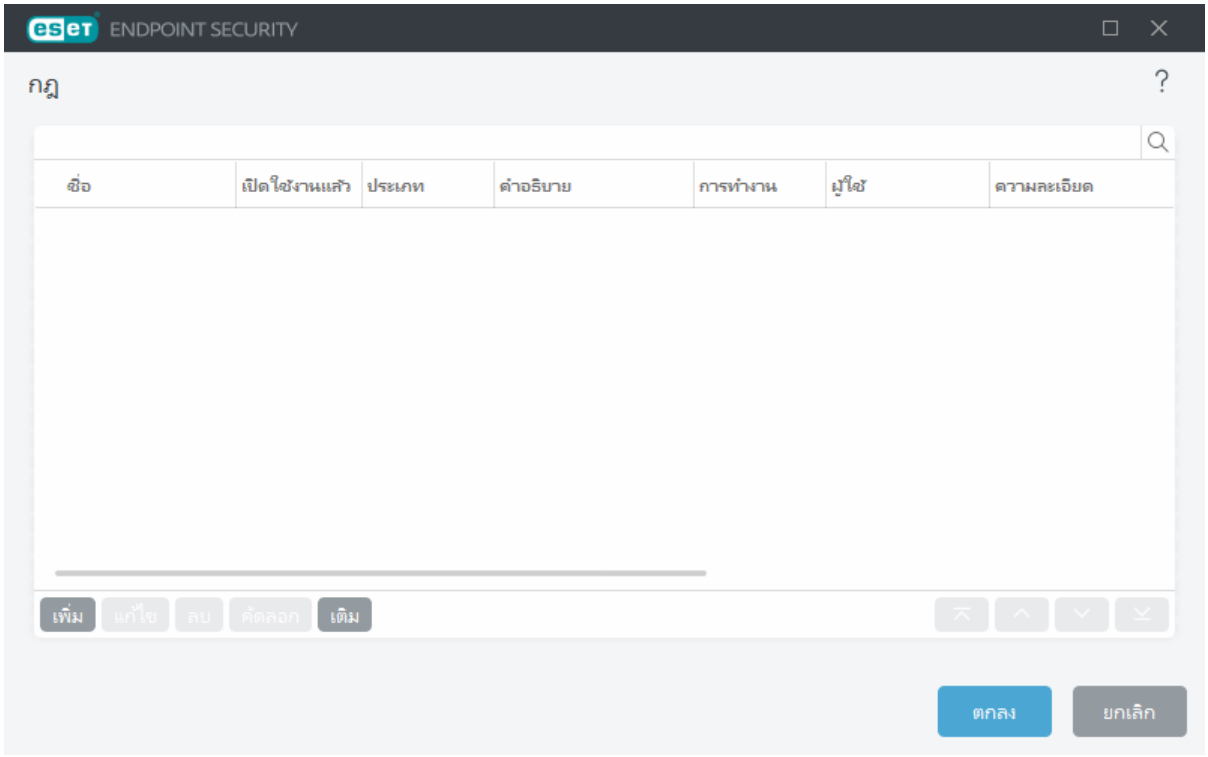
> คุณสามารถนำเข้ากลุ่มการควบคุมอุปกรณ์ที่มีกฎจากไฟล์ XML ได้โดยใช้เครื่องมือวางกำหนดการณ์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับและคู่มือแบบทีละขั้นตอน โปรดดู บทความฐานความรู้ ESET ของเรา

ถ้ามีการใส่อุปกรณ์ที่ถูกปิดกั้นโดยกฎที่มีอยู่ จะมีหน้าต่างการแจ้งเตือนปรากฏและไม่ได้รับสิทธิ์ให้เข้าถึงอุปกรณ์

เครื่องมือแก้ไขกฎการควบคุมอุปกรณ์

หน้าต่าง **เครื่องมือแก้ไขกฎการควบคุมอุปกรณ์** จะแสดงกฎที่มีอยู่ และช่วยให้สามารถทำการควบคุมอุปกรณ์ภายนอกที่ผู้ใช้ใช้ในการเชื่อมต่อกับคอมพิวเตอร์ได้อย่างแม่นยำ โปรดดูที่ การเพิ่มกฎการควบคุมอุปกรณ์

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
เพิ่มและแก้ไขกฎการควบคุมอุปกรณ์โดยใช้ผลิตภัณฑ์เอ็นพอยต์ ESET

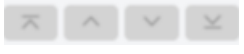


สามารถทำการอนุญาตหรือปิดกั้นอุปกรณ์ที่ระบุตามผู้ใช้ กลุ่มผู้ใช้ หรือตามพารามิเตอร์อุปกรณ์เพิ่มเติมใดๆ ที่สามารถระบุไว้ในการกำหนดค่ากฎได้ รายการของกฎประกอบด้วยคำอธิบายของกฎหลายรายการ เช่น ชื่อ ประเภทอุปกรณ์ภายนอก การดำเนินการที่จะทำหลังจากเชื่อมต่ออุปกรณ์ภายนอกกับคอมพิวเตอร์ของคุณ และความรุนแรงของบันทึก

คลิกที่ **เพิ่ม** หรือ **แก้ไข** เพื่อจัดการกฎ ยกเลิกการเลือกช่องทำเครื่องหมาย **เปิดใช้งานแล้ว** ที่อยู่ถัดจากกฎเพื่อปิดใช้งานกฎนั้นจนกว่าคุณจะต้องการใช้อีกครั้งในอนาคต เลือกกฎหนึ่งข้อหรือหลายข้อ แล้วคลิก **ลบ** เพื่อลบกฎถาวร

คัดลอก – สร้างกฎใหม่โดยมีตัวเลือกที่กำหนดไว้ล่วงหน้า ซึ่งใช้สำหรับกฎอื่นที่เลือกไว้

คลิก **เติม** เพื่อเติมพารามิเตอร์ของอุปกรณ์สื่อที่ถอดเข้าออกได้สำหรับอุปกรณ์ที่เชื่อมต่อกับคอมพิวเตอร์ของคุณโดยอัตโนมัติ

กฎจะได้รับการเรียงตามความสำคัญ โดยกฎที่สำคัญที่สุดจะอยู่ใกล้ด้านบนสุดที่สุด สามารถย้ายกฎได้ด้วยการคลิก  **บนสุด/ขึ้น/ลง/ล่างสุด** และสามารถย้ายกฎทีละข้อหรือย้ายเป็นกลุ่มได้

บันทึกการควบคุมอุปกรณ์ จะบันทึกเหตุการณ์ทั้งหมดที่ได้ทริกเกอร์การควบคุมอุปกรณ์ สามารถดูรายการบันทึกจากหน้าต่างหลักของโปรแกรม ESET Endpoint Security ใน **เครื่องมือ** > **ไฟล์บันทึก**

อุปกรณ์ที่ตรวจพบ

ปุ่ม **เติม** จะแสดงภาพรวมของอุปกรณ์ทั้งหมดที่เชื่อมต่อในปัจจุบันพร้อมข้อมูลเกี่ยวกับ: ประเภทอุปกรณ์ เกี่ยวกับผู้ขายอุปกรณ์ รุ่นและหมายเลขซีเรียล (หากมี)

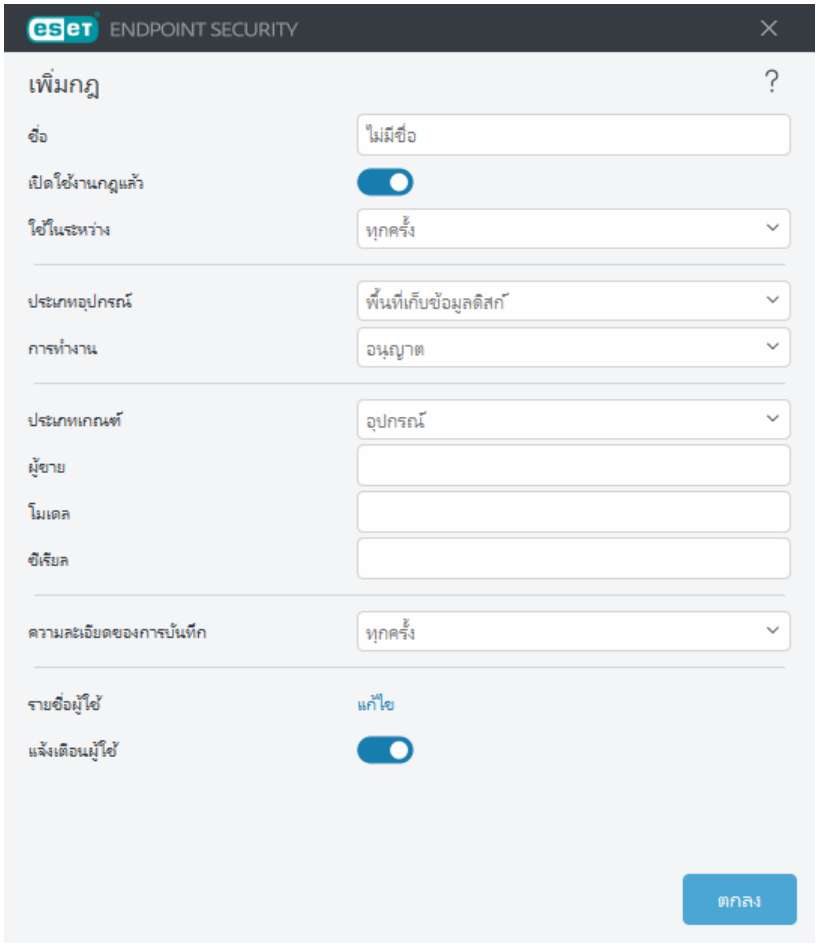
เลือกอุปกรณ์จากรายการอุปกรณ์ที่ตรวจพบ แล้วคลิก **ตกลง** เพื่อ เพิ่มกฎการควบคุมอุปกรณ์ ที่มีข้อมูลที่กำหนดไว้ล่วงหน้า (คุณสามารถปรับการตั้งค่าทุกค่าได้)

อุปกรณ์ในโหมดพลังงานต่ำ (พักการทำงาน) จะมีไอคอนคำเตือน ระบุไว้ หากต้องการเปิดใช้งานปุ่ม **ตกลง** และเพิ่มกฎสำหรับอุปกรณ์ ให้ดำเนินการดังต่อไปนี้:

- เชื่อมต่อกับอุปกรณ์อีกครั้ง
- ใช้อุปกรณ์ (ตัวอย่างเช่น เริ่มแอพกล้องใน Windows เพื่อปลุกเว็บแคม)

การเพิ่มกฎการควบคุมอุปกรณ์

กฎการควบคุมอุปกรณ์จะกำหนดการทำงานเมื่ออุปกรณ์ที่ตรงตามเกณฑ์กฎเชื่อมต่อกับคอมพิวเตอร์



ป้อนคำอธิบายของกฎในช่อง **ชื่อ** เพื่อคำอธิบายที่ดีขึ้น คลิกปุ่มสลับถัดจาก **เปิดใช้งานกฎแล้ว** เพื่อปิดใช้หรือเปิดใช้กฎนี้ ซึ่งอาจเป็นประโยชน์หากคุณไม่ต้องการลบกฎอย่างถาวร

ใช้ในระหว่าง – ช่วยให้คุณปรับใช้กฎที่สร้างในระหว่างช่วงเวลาหนึ่ง จากเมนูแบบเลื่อนลง ให้เลือกสล็อตเวลาที่สร้าง ดูข้อมูลเพิ่มเติมเกี่ยวกับ สล็อตเวลา

ประเภทอุปกรณ์

เลือกประเภทอุปกรณ์ภายนอกจากเมนูแบบเลื่อนลง (พื้นที่เก็บข้อมูลดิสก์/อุปกรณ์แบบพกพา/Bluetooth/FireWire/ฯลฯ) จะมีการรวบรวมข้อมูลประเภทอุปกรณ์จากระบบปฏิบัติการ และสามารถมองเห็นได้ในโปรแกรมจัดการอุปกรณ์ของระบบหากอุปกรณ์นั้นเชื่อมต่อกับคอมพิวเตอร์อยู่ อุปกรณ์เก็บข้อมูลจะรวมไปถึงดิสก์ภายนอกหรือเครื่องอ่านการ์ดหน่วยความจำทั่วไปที่เชื่อมต่อผ่าน USB หรือ FireWire เครื่องอ่านสมาร์ทการ์ดจะรวมถึงเครื่องอ่านสมาร์ทการ์ดทั้งหมดที่มีวงจรแบบฝังภายใน เช่น SIM การ์ด หรือการ์ดการตรวจสอบสิทธิ์ ตัวอย่างของอุปกรณ์ภาพได้แก่ เครื่องมือสแกนหรือกล้อง เนื่องจากอุปกรณ์เหล่านี้จะแสดงเฉพาะข้อมูลที่เกี่ยวกับการกระทำของอุปกรณ์ และไม่ได้เปิดเผยข้อมูลเกี่ยวกับผู้ใช้ การปิดกั้นอุปกรณ์เหล่านั้นจึงเป็นการปิดกั้นแบบทั้งหมดเท่านั้น

> ฟังก์ชันรายชื่อผู้ใช้จะไม่สามารถใช้ได้กับอุปกรณ์ประเภทโมเด็ม กฎจะใช้กับผู้ใช้ทุกคนและรายชื่อผู้ใช้ปัจจุบันจะถูกลบออก

การทำงาน

สามารถอนุญาตหรือปิดกั้นการเข้าถึงอุปกรณ์ที่ไม่ใช่อุปกรณ์เก็บข้อมูลได้ ในทางตรงกันข้าม กฎสำหรับอุปกรณ์เก็บข้อมูลช่วยให้คุณสามารถเลือกได้จากหนึ่งในการตั้งค่าสิทธิ์ต่อไปนี้:

- **อนุญาต** – อนุญาตให้เข้าถึงอุปกรณ์ได้อย่างสมบูรณ์
- **ปิดกั้น** – การเข้าถึงอุปกรณ์จะถูกปิดกั้น
- **เขียนบล็อก** – อนุญาตเฉพาะสิทธิ์ในการอ่านอุปกรณ์เท่านั้น
- **เตือน** – ในแต่ละครั้งที่เชื่อมต่ออุปกรณ์ ระบบจะแจ้งให้ผู้ใช้ทราบว่าอุปกรณ์นั้นได้รับอนุญาต/ถูกปิดกั้น และจะมีการจัดทำรายการบันทึกขึ้น อุปกรณ์ไม่ได้รับการจดจำ การแจ้งเตือนจะยังปรากฏขึ้นเมื่อมีการเชื่อมต่อกับอุปกรณ์เดิมนั้นอีกในภายหลัง

โปรดทราบว่ามีบางการทำงาน (การอนุญาต) เท่านั้นที่สามารถใช้งานได้กับอุปกรณ์ทุกประเภท หากอุปกรณ์เป็นอุปกรณ์เก็บข้อมูล การทำงานทั้งสี่อย่างนี้สามารถใช้งานได้ สำหรับอุปกรณ์ที่ไม่ใช่อุปกรณ์เก็บข้อมูล จะมีการทำงานเพียงสามอย่างเท่านั้นที่สามารถใช้งานได้ (เช่น **เขียนบล็อก** ไม่สามารถทำงานกับ Bluetooth ดังนั้น อุปกรณ์

Bluetooth สามารถเลือกได้เพียงอนุญาต ปิดกั้นหรือเตือนเท่านั้น)

ประเภทเกณฑ์

เลือก **กลุ่มอุปกรณ์** หรือ **อุปกรณ์**

พารามิเตอร์เพิ่มเติมที่แสดงด้านล่างสามารถใช้เพื่อปรับแต่งกฎสำหรับอุปกรณ์ต่างๆ ได้ พารามิเตอร์ทั้งหมดจะต้องตรงตามตัวพิมพ์ใหญ่-เล็กและรองรับอักขระตัวแทน (*,?):

- **ผู้ขาย** – กรองตามชื่อหรือ ID ของผู้ขาย
- **รุ่น** – ชื่อของอุปกรณ์ที่กำหนด
- **ซีเรียล** – อุปกรณ์ภายนอกมักจะมีหมายเลขซีเรียลของตนเอง ในกรณีของ CD/DVD หมายถึงหมายเลขซีเรียลของสื่อ ไม่ใช่ไดรฟ์ CD

> หากไม่ได้ระบุพารามิเตอร์เหล่านี้ กฎจะละเว้นช่องเหล่านี้ขณะที่จับคู่ พารามิเตอร์การกรองในช่องข้อความทั้งหมดจะต้องตรงตามตัวพิมพ์ใหญ่-เล็กและรองรับอักขระตัวแทน (เครื่องหมายคำถาม (?) จะแทนอักขระตัวเดียว ในขณะที่เครื่องหมายดอกจัน (*) จะแทนสตริงที่มีศูนย์อักขระหรือมากกว่า)

> หากต้องการดูข้อมูลเกี่ยวกับอุปกรณ์ ให้สร้างกฎสำหรับอุปกรณ์ประเภทนั้น เชื่อมต่ออุปกรณ์กับคอมพิวเตอร์ของคุณ และตรวจสอบรายละเอียดของอุปกรณ์ใน บันทึกการควบคุมอุปกรณ์

ความละเอียดของการบันทึก

- **เสมอ** – บันทึกเหตุการณ์ทั้งหมด
- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม
- **ข้อมูล** – บันทึกข้อความแจ้งข้อมูล รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน แล้วส่งไปที่ ERA Server
- **ไม่มี** – จะไม่มีการบันทึกใดๆ

สามารถจำกัดกฎสำหรับผู้ใช้บางคนหรือกลุ่มผู้ใช้บางกลุ่มได้โดยการเพิ่มกฎลงใน **รายชื่อผู้ใช้**:

- **เพิ่ม** – เปิด**ประเภทวัตถุ: ผู้ใช้หรือกลุ่ม** หน้าต่างโต้ตอบที่อนุญาตให้คุณเลือกผู้ใช้ที่ต้องการ
- **ลบออก** – ลบผู้ใช้ที่เลือกออกจากตัวกรอง

ข้อจำกัดของรายชื่อผู้ใช้
ไม่สามารถกำหนดรายชื่อผู้ใช้สำหรับกฎที่กำหนดตาม ประเภทอุปกรณ์ ต่อไปนี้:
- เครื่องพิมพ์ USB
- อุปกรณ์ Bluetooth
- เครื่องอ่านสมาร์ทการ์ด
- อุปกรณ์ภาพ
- โมเด็ม
- พอร์ต LPT/COM

แจ้งเตือนผู้ใช้ – หากอุปกรณ์ถูกปิดกั้นด้วยการแทรกกฎที่มีอยู่แล้ว หน้าต่างการแจ้งเตือนจะปรากฏขึ้น

กลุ่มอุปกรณ์

อุปกรณ์ที่ต่อเข้ากับคอมพิวเตอร์ของคุณอาจก่อให้เกิดความเสี่ยงด้านความปลอดภัย

หน้าต่างกลุ่มอุปกรณ์แบ่งออกเป็นสองส่วน ด้านขวาของหน้าต่างแสดงรายชื่ออุปกรณ์ที่เป็นของกลุ่มที่เกี่ยวข้อง และด้านซ้ายของหน้าต่างประกอบด้วยกลุ่มที่สร้างขึ้น เลือกกลุ่มเพื่อแสดงอุปกรณ์ในบานหน้าต่างด้านขวา

เมื่อคุณเปิดหน้าต่างกลุ่มอุปกรณ์และเลือกกลุ่ม คุณจะสามารถเพิ่มหรือย้ายอุปกรณ์ออกจากรายชื่อ วิธีเพิ่มอุปกรณ์ลงในกลุ่มอีกวิธีหนึ่งคือนำเข้าอุปกรณ์จากไฟล์ หรือคุณสามารถเลือกคลิกปุ่ม **เติม** และอุปกรณ์ทั้งหมดที่ต่อเข้ากับคอมพิวเตอร์ของคุณจะแสดงในหน้าต่าง **อุปกรณ์ที่ตรวจพบ** เลือกอุปกรณ์จากรายการที่เพิ่มใหม่เพื่อเพิ่มอุปกรณ์เหล่านั้นลงในกลุ่มได้ด้วยการคลิก **ตกลง**

องค์ประกอบการควบคุม

เพิ่ม – คุณสามารถเพิ่มกลุ่มโดยการพิมพ์ชื่อหรืออุปกรณ์ลงในกลุ่มที่มีอยู่ ทั้งนี้ขึ้นอยู่กับว่าคุณคลิกปุ่มที่ส่วนใดของหน้าต่าง

แก้ไข – ให้คุณเปลี่ยนชื่อของกลุ่มที่เลือกหรือพารามิเตอร์ของอุปกรณ์ (ผู้ขาย รุ่น หมายเลขซีเรียล)

ลบ – ลบกลุ่มหรืออุปกรณ์ที่เลือกโดยขึ้นอยู่กับว่าคุณคลิกปุ่มที่ส่วนใดของหน้าต่าง

นำเข้า – นำเข้ารายการอุปกรณ์จากไฟล์ข้อความ การนำเข้าอุปกรณ์จากไฟล์ข้อความต้องมีการจัดรูปแบบที่ถูกต้อง:

- อุปกรณ์แต่ละเครื่องจะเริ่มต้นที่บรรทัดใหม่
- จะต้องแสดงรายการ **ผู้ขาย รุ่น** และ **หมายเลขประจำเครื่อง** สำหรับอุปกรณ์แต่ละเครื่อง และคั่นด้วยเครื่องหมายจุลภาค

ตัวอย่างของเนื้อหาไฟล์ข้อความได้แก่:
```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

ส่งออก – ส่งออกรายการอุปกรณ์ไปยังไฟล์

ปุ่ม **เติม** จะแสดงภาพรวมของอุปกรณ์ทั้งหมดที่เชื่อมต่อในปัจจุบันพร้อมข้อมูลเกี่ยวกับ: ประเภทอุปกรณ์ เกี่ยวกับผู้ขายอุปกรณ์ รุ่นและหมายเลขซีเรียล (หากมี)

คุณสามารถนำเข้ากลุ่มการควบคุมอุปกรณ์ที่มีกฎจากไฟล์ XML ได้โดยใช้เครื่องมือวางกำหนดการณ์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับและคู่มือแบบทีละขั้นตอน โปรดดู บทความฐานความรู้ ESET ของเรา

เพิ่มอุปกรณ์

คลิก เพิ่ม ในหน้าต่างด้านขวาเพื่อเพิ่มอุปกรณ์ไปยังกลุ่มที่มีอยู่ พารามิเตอร์เพิ่มเติมที่แสดงด้านล่างสามารถใช้เพื่อปรับแต่งกฎสำหรับอุปกรณ์ต่างๆ ได้ พารามิเตอร์ทั้งหมดจะต้องตรงตามตัวพิมพ์ใหญ่-เล็กและรองรับอักขระตัวแทน (*,?):

- **ผู้ขาย** – กรองตามชื่อหรือ ID ของผู้ขาย
- **รุ่น** – ชื่อของอุปกรณ์ที่กำหนด
- **ซีเรียล** – อุปกรณ์ภายนอกมักจะมีหมายเลขซีเรียลของตนเอง ในกรณีของ CD/DVD หมายถึงหมายเลขซีเรียลของสื่อ ไม่ใช่ไดรฟ์ CD
- **คำอธิบาย** คำอธิบายเกี่ยวกับอุปกรณ์เพื่อการจัดระเบียบที่ดีขึ้น

หากไม่ได้ระบุพารามิเตอร์เหล่านี้ กฎจะละเว้นช่องเหล่านี้ขณะที่จับคู่ พารามิเตอร์การกรองในช่องข้อความทั้งหมดจะต้องตรงตามตัวพิมพ์ใหญ่-เล็กและรองรับอักขระตัวแทน (เครื่องหมายคำถาม (?) จะแทนอักขระตัวเดียว ในขณะที่เครื่องหมายดอกจัน (*) จะแทนสตริงที่มีศูนย์อักขระหรือมากกว่า)

คลิกที่ **ตกลง** เพื่อบันทึกการเปลี่ยนแปลง คลิก **ยกเลิก** ถ้าคุณต้องการออกจากหน้าต่าง **กลุ่มอุปกรณ์** โดยไม่บันทึกการเปลี่ยนแปลง

หลังจากสร้างกลุ่มอุปกรณ์ คุณต้อง เพิ่มกฎการควบคุมอุปกรณ์ใหม่ สำหรับกลุ่มอุปกรณ์ที่สร้างขึ้นและเลือกการทำงานที่จะเกิดขึ้น

โปรดทราบว่ามีบางการทำงาน (การอนุญาต) เท่านั้นที่สามารถใช้งานได้กับอุปกรณ์ทุกประเภท หากอุปกรณ์เป็นอุปกรณ์เก็บข้อมูล การทำงานทั้งสี่อย่างนี้สามารถใช้งานได้ สำหรับอุปกรณ์ที่ไม่ใช่อุปกรณ์เก็บข้อมูล จะมีการทำงานเพียงสามอย่างเท่านั้นที่สามารถใช้งานได้ (เช่น **เขียนบล็อก** ไม่สามารถทำงานกับ Bluetooth ดังนั้น อุปกรณ์ Bluetooth สามารถเลือกได้เพียงอนุญาต ปิดกั้นหรือเตือนเท่านั้น)

ThreatSense

ThreatSense ประกอบด้วยวิธีการตรวจหาภัยคุกคามที่ซับซ้อนหลายรูปแบบ เทคโนโลยีนี้เป็นการป้องกันในเชิงรุก ซึ่งหมายความว่าจะมีการป้องกันตั้งแต่ช่วงต้นที่มีการแพร่กระจายของภัยคุกคามใหม่ เทคโนโลยีนี้จะใช้การผสมผสานของการวิเคราะห์รหัส การจำลองรหัส ฐานข้อมูลทั่วไป และฐานข้อมูลไวรัส ซึ่งทำงานร่วมกันอย่างสอดคล้องเพื่อเพิ่มประสิทธิภาพของการรักษาความปลอดภัยให้กับระบบได้อย่างมาก กลไกการสแกนสามารถควบคุมสตรีมข้อมูลต่างๆ ได้พร้อมกัน ซึ่งเพิ่มประสิทธิภาพและอัตราการตรวจพบสูงสุด นอกจากนี้ เทคโนโลยี ThreatSense ยังช่วยกำจัดรูทคิทด้วย

ตัวเลือกการตั้งค่าของเทคโนโลยี ThreatSense ช่วยให้ผู้ใช้สามารถระบุพารามิเตอร์การสแกนต่างๆ ได้:

- ประเภทไฟล์และนามสกุลที่จะสแกน
- การใช้วิธีการตรวจหาต่างๆ ร่วมกัน
- ระดับการกำจัด เป็นต้น

หากต้องการเข้าสู่หน้าต่างการตั้งค่า ให้คลิก **ThreatSense** ใน การตั้งค่าขั้นสูง สำหรับโมดูลที่ใช้เทคโนโลยี ThreatSense (โปรดดูด้านล่าง) สถานการณ์ของการรักษาความปลอดภัยที่ต่างกันอาจต้องใช้การกำหนดค่าที่ต่างกัน โปรดทราบว่า ThreatSense สามารถกำหนดค่าแยกกันได้สำหรับโมดูลการป้องกันต่อไปนี้:

- การป้องกันระบบไฟล์แบบเรียลไทม์
- การสแกนขณะอยู่ในสถานะไม่ใช้งาน
- การสแกนเมื่อเริ่มต้น
- การป้องกันเอกสาร
- การป้องกันอีเมลไคลเอ็นต์
- การป้องกันการเข้าถึงเว็บ
- การสแกนคอมพิวเตอร์

พารามิเตอร์ ThreatSense มีการปรับให้เหมาะสำหรับแต่ละโมดูลมากที่สุด อีกทั้งการแก้ไขเหล่านี้จะมีผลกับการทำงานของระบบมากด้วยเช่นกัน ตัวอย่างเช่น การเปลี่ยนพารามิเตอร์เพื่อให้สแกนรันไทม์แพ็คเกอร์เสมอ หรือเปิดใช้การวิเคราะห์พฤติกรรมขั้นสูงในโมดูลการป้องกันระบบไฟล์แบบเรียลไทม์อาจทำให้ระบบทำงานช้าลง (โดยปกติโปรแกรมจะสแกนเฉพาะไฟล์ที่สร้างขึ้นใหม่โดยใช้วิธีการเหล่านี้) เราขอแนะนำให้คุณคงพารามิเตอร์ ThreatSense เริ่มต้นไว้สำหรับโมดูลทั้งหมด ยกเว้นการสแกนคอมพิวเตอร์

วัตถุที่จะสแกน

ส่วนนี้จะช่วยให้คุณสามารถกำหนดว่าจะสแกนหาการแฝงตัวจากองค์ประกอบและไฟล์คอมพิวเตอร์ใด

หน่วยความจำที่ใช้งาน – สแกนหาภัยคุกคามที่โจมตีหน่วยความจำที่ใช้งานของระบบ

ส่วนการบูต/UEFI – การสแกนบูตเซคเตอร์สำหรับมัลแวร์ที่มีอยู่ในบันทึกการบูตหลัก อ่านเพิ่มเติมเกี่ยวกับ UEFI ในประมวลศัพท์

ไฟล์อีเมล – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: DBX (Outlook Express) และ EML

อาร์ไคฟ์ – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE และอื่นๆ อีกมากมาย

อาร์ไคฟ์แบบคลายตัวเอง - อาร์ไคฟ์แบบคลายตัวเอง หรือ Self-extracting archives (SFX) คืออาร์ไคฟ์ที่สามารถคลายตัวเองได้

รันไทม์แพ็คเกอร์ – หลังจากเรียกใช้แล้ว รันไทม์แพ็คเกอร์ (ไม่เหมือนกับประเภทที่เก็บเอกสารมาตรฐาน) จะคลายออกในหน่วยความจำ นอกเหนือจากแพ็คเกอร์คงที่แบบมาตรฐาน (UPX, yoda, ASPack, FSG เป็นต้น) เครื่องมือสแกนจะสามารถจดจำประเภทหรือแพ็คเกอร์อื่นๆ เพิ่มเติมผ่านการใช้การจำลองรหัส

ตัวเลือกการสแกน

เลือกวิธีที่ใช้เมื่อสแกนหาการแฝงตัวบนระบบ ตัวเลือกที่ใช้ได้มีดังนี้:

การวิเคราะห์พฤติกรรม – การวิเคราะห์พฤติกรรมเป็นอัลกอริทึมที่วิเคราะห์การทำงาน (ที่เป็นอันตราย) ของโปรแกรม ข้อได้เปรียบสำคัญของเทคโนโลยีนี้คือความสามารถในการระบุซอฟต์แวร์ที่เป็นอันตรายซึ่งไม่มีอยู่ก่อนหน้านั้น หรือไม่เป็นที่รู้จักของกลไกตรวจหาก่อนหน้า ข้อเสียคือมีโอกาสที่จะเกิดการเตือนผิดพลาด (แม้จะน้อยมากก็ตาม)

วิเคราะห์พฤติกรรมขั้นสูง/ลายเซ็น DNA - การวิเคราะห์พฤติกรรมขั้นสูงเป็นอัลกอริทึมการวิเคราะห์พฤติกรรมขั้นสูงที่พัฒนาโดย ESET ปรับให้เหมาะสมกับการตรวจหาเวิร์มของคอมพิวเตอร์และม้าโทรจัน และเขียนในภาษาที่ใช้เขียนโปรแกรมระดับสูง การใช้การวิเคราะห์พฤติกรรมขั้นสูงจะช่วยเพิ่มความสามารถในการตรวจหาภัยคุกคามของผลิตภัณฑ์ ESET ได้เป็นอย่างมาก ฐานข้อมูลไวรัสสามารถตรวจหาและระบุไวรัสได้อย่างเชื่อถือได้ การใช้ระบบอัพเดทอัตโนมัติ ทำให้ฐานข้อมูลใหม่ใช้ได้หลังจากค้นพบภัยคุกคามเพียงไม่กี่ชั่วโมง ข้อเสียของฐานข้อมูลไวรัสคือระบบจะตรวจหาไวรัสเฉพาะที่รู้จักเท่านั้น (หรือเวอร์ชันที่มีการแก้ไขเล็กน้อยของไวรัสเหล่านี้)

การกำจัด

การตั้งค่าการกำจัด จะเป็นตัวกำหนดการทำงานของ ESET Endpoint Security ขณะกำจัดวัตถุ

การยกเว้น

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่า ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะสแกน

อื่นๆ

เมื่อกำหนดค่ากลไก ThreatSense สำหรับการสแกนคอมพิวเตอร์ จะสามารถใช้ตัวเลือกในส่วน **อื่นๆ** ได้ดังต่อไปนี้:

สแกนสตรีมข้อมูลสำรอง (ADS) – สตรีมข้อมูลสำรองที่ใช้งานโดยระบบไฟล์ NTFS เป็นการเชื่อมโยงไฟล์และโฟลเดอร์ซึ่งจะไม่ปรากฏสำหรับเทคนิคการสแกนทั่วไป การแฝงตัวจำนวนมากพยายามหลีกเลี่ยงการตรวจหานี้ โดยปลอมแปลงตัวเองเป็นสตรีมข้อมูลสำรอง

เรียกใช้การสแกนเบื้องหลังโดยมีลำดับความสำคัญต่ำ – ลำดับการสแกนแต่ละลำดับจะใช้ทรัพยากรของระบบจำนวนหนึ่ง หากคุณทำงานกับโปรแกรมที่ใช้ทรัพยากรระบบจำนวนมาก คุณสามารถเปิดใช้การสแกนเบื้องหลังที่มีลำดับความสำคัญต่ำ และประหยัดทรัพยากรไว้สำหรับแอพพลิเคชันของคุณ

บันทึกวัตถุทั้งหมด – บันทึกการสแกน จะแสดงไฟล์ที่สแกนแล้วทั้งหมดในอาร์ไคฟ์ที่ขยายในตัว รวมถึงไฟล์ที่ไม่ติดไวรัส (อาจสร้างข้อมูลบันทึกการสแกนจำนวนมากและเพิ่มขนาดไฟล์บันทึกการสแกน)

เปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท – เมื่อเปิดใช้การเพิ่มประสิทธิภาพแบบสมาร์ท ระบบจะใช้การตั้งค่าที่มีประสิทธิภาพที่สุดเพื่อให้แน่ใจว่าการสแกนจะมีประสิทธิภาพและความเร็วสูงสุดไปพร้อมกัน ซึ่งโมดูลการป้องกันต่างๆ จะสแกนข้อมูลอย่างชาญฉลาด โดยใช้ประโยชน์จากวิธีการสแกนต่างๆ และนำมาใช้งานกับประเภทไฟล์ที่ระบุ หากคุณปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท เราจะใช้เฉพาะการตั้งค่าที่ผู้ใช้กำหนดไว้ในแกน ThreatSense ของโมดูลเฉพาะเมื่อทำการสแกนเท่านั้น

เก็บบันทึกการลงเวลาเข้าถึงล่าสุด – เลือกตัวเลือกนี้เพื่อเก็บเวลาแรกเริ่มที่เข้าถึงไฟล์ที่สแกนแทนการอัพเดทเวลาเหล่านั้น (ตัวอย่างเช่น สำหรับใช้กับระบบสำรองข้อมูล)

ขีดจำกัด

ส่วนขีดจำกัดช่วยให้คุณสามารถระบุขนาดสูงสุดของวัตถุ และระดับของอาร์ไคฟ์ที่ซ้อนที่จะสแกน:

การตั้งค่าวัตถุ

ขนาดวัตถุสูงสุด – กำหนดขนาดสูงสุดของวัตถุที่จะสแกน โมดูลป้องกันไวรัสที่กำหนดจะสแกนเฉพาะวัตถุที่เล็กกว่าขนาดที่ระบุเท่านั้น ผู้ที่สามารถแก้ไขตัวเลือกนี้ควรเป็นผู้ใช้ขั้นสูง ซึ่งอาจมีเหตุผลบางอย่างสำหรับการยกเว้นวัตถุขนาดใหญ่จากการสแกน ค่าเริ่มต้น: ไม่จำกัด

เวลาสแกนสูงสุดสำหรับวัตถุ (วินาที) – กำหนดค่าสูงสุดสำหรับสแกนไฟล์ในวัตถุที่มีการบรรจุ (เช่น อาร์ไคฟ์ RAR/ZIP หรืออีเมลที่มีไฟล์แนบหลายรายการ) การตั้งค่านี้จะไม่ถูกปรับใช้สำหรับไฟล์สแตนด์อโลน การสแกนจะหยุดทันทีหากมีการป้อนค่าที่ผู้ใช้กำหนดและพ้นระยะเวลาดังกล่าว โดยไม่คำนึงว่าการสแกนแต่ละไฟล์ในวัตถุที่มีการบรรจุจะเสร็จสิ้นแล้วหรือไม่ ในกรณีที่อาร์ไคฟ์บรรจุไฟล์ขนาดใหญ่ การสแกนจะหยุดช้ากว่าไฟล์ที่ถูกดึงข้อมูลจากอาร์ไคฟ์ (ตัวอย่างเช่น เมื่อตัวแปรที่ผู้ใช้กำหนดคือ 3 วินาที แต่การดึงข้อมูลของไฟล์คือ 5 วินาที) ไฟล์ที่เหลือในอาร์ไคฟ์จะไม่ถูกสแกนเมื่อพ้นระยะเวลาดังกล่าว หากต้องการจำกัดเวลาในการสแกน ซึ่งรวมถึงอาร์ไคฟ์ขนาดใหญ่ ให้ใช้ **ขนาดวัตถุสูงสุด** และ **ขนาดไฟล์สูงสุดในอาร์ไคฟ์** (ไม่แนะนำให้ใช้เนื่องจากความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นได้) ค่าเริ่มต้น: ไม่จำกัด

ตั้งค่าการสแกนอาร์ไคฟ์

ระดับการซ้อนของอาร์ไคฟ์ – ระบุความลึกสูงสุดของการสแกนอาร์ไคฟ์ ค่าเริ่มต้น: 10

ขนาดไฟล์สูงสุดในอาร์ไคฟ์ – ตัวเลือกนี้ช่วยให้คุณสามารถระบุขนาดไฟล์สูงสุดสำหรับไฟล์ที่อยู่ในอาร์ไคฟ์ (เมื่อดึงข้อมูล) ที่จะสแกนได้ ค่าเริ่มต้น: ไม่จำกัด ค่าสูงสุดคือ 3 GB

เราไม่แนะนำให้แก้ไขค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดที่จะต้องแก้ไขค่านี้ในสถานการณ์ปกติ

ระดับการกำจัด

หากต้องการเปลี่ยนการตั้งค่าระดับการกำจัดไวรัสสำหรับโมดูลการป้องกันที่ต้องการ ให้ขยายส่วน **ThreatSense** (เช่น **การป้องกันระบบไฟล์แบบเรียลไทม์**) จากนั้นเลือก **ระดับการทำกำจัดไวรัส** จากเมนูแบบเลื่อนลง

ThreatSense มีระดับการปรับปรุงแก้ไข (เช่น การกำจัด) ดังต่อไปนี้

การปรับปรุงแก้ไขใน ESET Endpoint Security

ระดับการกำจัด	คำอธิบาย
แก้ไขการตรวจหาเสมอ	ให้พยายามปรับปรุงแก้ไขการตรวจหาขณะล้างวัตถุโดยไม่มีการแทรกแซงจากผู้ใช้ปลายทาง ในบางกรณีที่เกิดได้ยาก (ตัวอย่างเช่น ไฟล์ระบบ) หากการตรวจหาไม่สามารถปรับปรุงแก้ไขได้ วัตถุที่รายงานจะถูกทิ้งไว้ในตำแหน่งเดิม แนะนำให้ตั้ง แนะนำให้ตั้ง **ปรับปรุงแก้ไขการตรวจหาเสมอ** เป็นการตั้งค่าเริ่มต้นใน สภาพแวดล้อมที่มีการจัดการ
ปรับปรุงแก้ไขการตรวจหาว่าปลอดภัยหรือไม่นอกเหนือจากนั้นให้เก็บไว้	การพยายามปรับปรุงแก้ไขการตรวจหาขณะกำจัดวัตถุโดยไม่มีการแทรกแซงจากผู้ใช้ปลายทาง ในบางกรณี (ตัวอย่างเช่น ไฟล์ระบบหรือไฟล์เก็บถาวร ที่มีทั้งไฟล์ที่ไม่ติดและติดไวรัส) หากการตรวจหาไม่สามารถปรับปรุงแก้ไขได้ วัตถุที่รายงานจะถูกทิ้งไว้ในตำแหน่งเดิม
ปรับปรุงแก้ไขการตรวจหาว่าปลอดภัยหรือไม่นอกเหนือจากนั้นให้ถาม	การพยายามแก้ไขการตรวจหาขณะล้างวัตถุ ในบางกรณี หากไม่มีการกระทำใดสามารถทำได้ ผู้ใช้ปลายทางจะได้รับหน้าต่างโต้ตอบและต้องเลือกการดำเนินการการปรับปรุงแก้ไข (ตัวอย่างเช่น ลบ หรือ เพิกเฉย) แนะนำให้ใช้การตั้งค่านี้ในกรณีทั่วไป
ถามผู้ใช้ปลายทางเสมอ	ผู้ใช้ปลายทางจะได้รับหน้าต่างโต้ตอบขณะล้างวัตถุและต้องเลือกการดำเนินการการปรับปรุงแก้ไข (ตัวอย่างเช่น ลบ หรือ เพิกเฉย) ระดับนี้ได้รับการออกแบบสำหรับผู้ใช้ขั้นสูงขึ้นซึ่งรู้ว่าควรใช้วิธีใดเมื่อมีการตรวจหา

รายการที่อยู่ที่ยกเว้นจากการตรวจสอบ

นามสกุลไฟล์ที่ได้รับการยกเว้นเป็นส่วนหนึ่งของ ThreatSense หากต้องการกำหนดค่านามสกุลไฟล์ที่ได้รับการยกเว้น ให้คลิก **ThreatSense** ในการตั้งค่าขั้นสูง สำหรับ โมดูลที่ใช้เทคโนโลยี ThreatSense

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่า ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะสแกน

อย่าสับสนกับ การยกเว้นกระบวนการ, การยกเว้น HIPS หรือ การยกเว้นไฟล์/โฟลเดอร์

ทุกไฟล์จะถูกสแกนตามค่าเริ่มต้น คุณสามารถเพิ่มนามสกุลในรายการไฟล์ที่จะยกเว้นจากการสแกน

ในบางครั้ง การยกเว้นไฟล์จากการสแกนจะเป็นสิ่งจำเป็น หากไฟล์บางประเภทของการสแกนป้องกันโปรแกรมที่ใช้นามสกุลบางประเภทเพื่อไม่ให้ทำงานอย่างถูกต้อง ตัวอย่างเช่น อาจมีการแนะนำให้ยกเว้นนามสกุล `.edb`, `.eml` และ `.tmp` เมื่อใช้เซิร์ฟเวอร์ Microsoft Exchange

หากต้องการเพิ่มนามสกุลใหม่ลงในรายการ ให้คลิก **เพิ่ม** แล้วพิมพ์นามสกุลลงในช่องว่าง (ตัวอย่างเช่น tmp) จากนั้นคลิก **ตกลง** เมื่อคุณเลือก **ป้อนค่าหลายค่า** คุณสามารถเพิ่มนามสกุลไฟล์หลายนามสกุลโดยคั่นด้วยเส้นบรรทัด คอมมาหรือเซมิโคลอนได้ (ตัวอย่างเช่น เลือก **เซมิโคลอน** จากเมนูแบบเลื่อนลงให้เป็นตัวแบ่ง แล้วพิมพ์ `edb;eml;tmp`)
คุณสามารถใช้ สัญลักษณ์พิเศษ ? (เครื่องหมายคำถาม) เครื่องหมายคำถามแสดงถึงสัญลักษณ์ต่างๆ (ตัวอย่างเช่น `?db`).

หากต้องการดูส่วนขยาย (ถ้ามี) ของแฟ้มในระบบปฏิบัติการ Windows คุณต้องเลือกช่องทำเครื่องหมาย**ส่วนขยายของชื่อแฟ้ม**ใน **Windows Explorer** > **มุมมอง** (แท็บ)

พารามิเตอร์ ThreatSense เพิ่มเติม

หากต้องการแก้ไขการตั้งค่าเหล่านี้ ให้เปิดการตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันระบบไฟล์แบบเรียลไทม์** > **พารามิเตอร์ ThreatSense เพิ่มเติม**

พารามิเตอร์ ThreatSense เพิ่มเติมสำหรับไฟล์ที่สร้างใหม่และแก้ไข

ไฟล์ที่สร้างใหม่หรือแก้ไขมีความเป็นไปได้ที่จะติดไวรัสมากกว่าไฟล์ที่มีอยู่ ด้วยเหตุผลนี้ โปรแกรมจะตรวจสอบไฟล์เหล่านี้ด้วยพารามิเตอร์การสแกนเพิ่มเติม ESET Endpoint Security จะใช้การวิเคราะห์พฤติกรรมขั้นสูงที่สามารถตรวจหาภัยคุกคามใหม่ก่อนที่จะมีการปล่อยการอัพเดทกลไกการตรวจจับพร้อมกับวิธีสแกนโดยใช้ฐานข้อมูล

นอกจากไฟล์ที่สร้างใหม่แล้ว การสแกนยังทำงานใน **อาร์ไคฟ์แบบคลายตัวเอง** (.sfx) และ **รันไทม์แพ็คเกอร์** (ไฟล์ที่เรียกใช้ซึ่งบีบอัดภายใน) โดยปกติแล้ว ที่เก็บเอกสารจะถูกสแกนถึงระดับการซ้อนที่ 10 และจะได้รับการตรวจสอบโดยไม่พิจารณาขนาดที่แท้จริง หากต้องการแก้ไขการตั้งค่าการสแกนอาร์ไคฟ์ ให้ยกเลิกการเลือก **การตั้งค่าการสแกนอาร์ไคฟ์เริ่มต้น**

พารามิเตอร์ ThreatSense เพิ่มเติมสำหรับไฟล์ที่เรียกใช้

การวิเคราะห์พฤติกรรมขั้นสูงเมื่อเรียกใช้ไฟล์ - ตามค่าเริ่มต้น จะใช้ การวิเคราะห์พฤติกรรมขั้นสูง เมื่อเรียกใช้ไฟล์ เมื่อเปิดใช้งาน เราขอแนะนำให้เปิดใช้งาน การเพิ่มประสิทธิภาพแบบสมาร์ท และ ESET LiveGrid® ต่อไปเพื่อลดผลกระทบต่อประสิทธิภาพของระบบ

การวิเคราะห์พฤติกรรมขั้นสูงเมื่อเรียกใช้ไฟล์จากสื่อที่ถอดเข้าออกได้ - การวิเคราะห์พฤติกรรมขั้นสูงจะจำลองรหัสในสิ่งแวดล้อมเสมือนและประเมินพฤติกรรมก่อนจะให้อนุญาตให้ใช้งานรหัสจากสื่อที่ถอดออกได้

เครื่องมือ

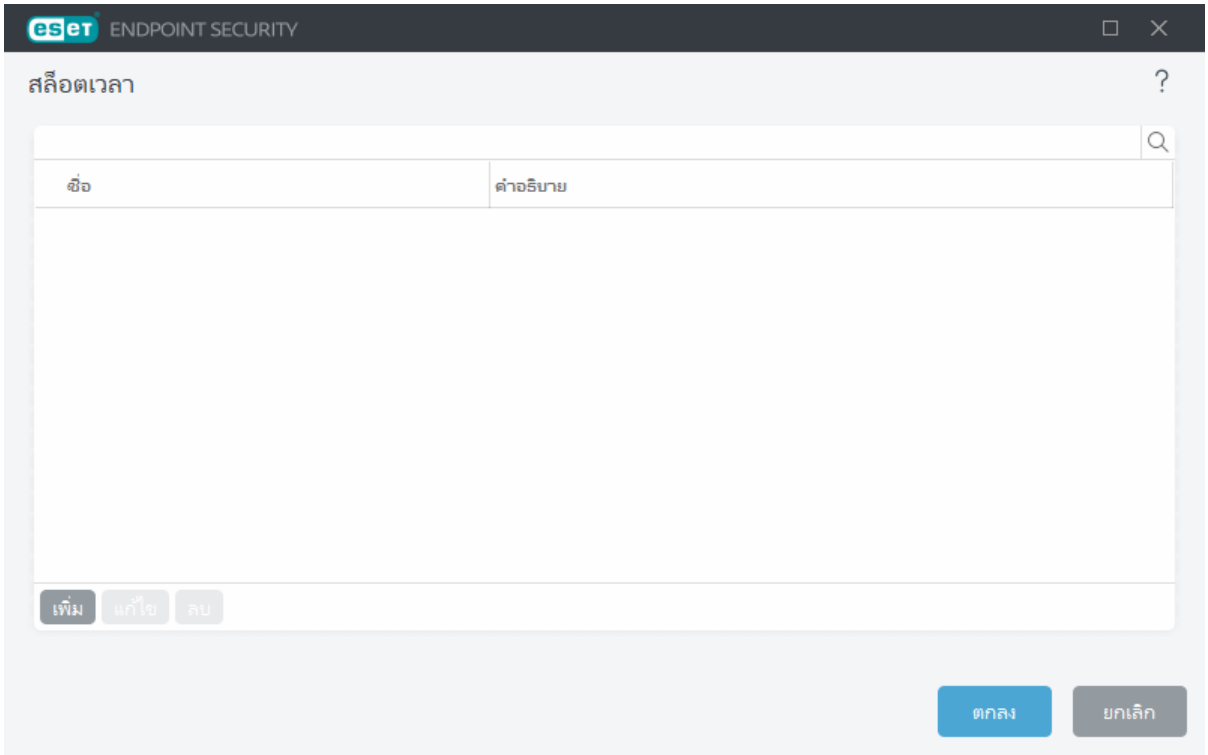
คุณสามารถกำหนดการตั้งค่าขั้นสูงสำหรับฟีเจอร์ที่มีความปลอดภัยเพิ่มเติม และช่วยลดความยุ่งยากในการดูแลระบบของ ESET Endpoint Security ใน การตั้งค่าขั้นสูง > **เครื่องมือ**

- สล็อตเวลา

- อัพเดท Microsoft Windows®
- ESET CMD
- การตรวจสอบและการจัดการระยะไกล
- การตรวจสอบช่วงเวลาของใบอนุญาต
- ไฟล์บันทึก
- โหมดการนำเสนอ
- การวินิจฉัย

สล็อตเวลา

สามารถสร้างช่วงเวลาและกำหนดไปยังกฎสำหรับ **การควบคุมอุปกรณ์** และ **การควบคุมการเข้าถึงเว็บไซต์** สามารถพบการตั้งค่า **สล็อตเวลา** ได้ใน การตั้งค่าขั้นสูง > **เครื่องมือ** ซึ่งจะทำให้คุณสามารถระบุสล็อตเวลาที่ใช้บ่อยๆ (เช่น เวลาทำงาน วันสุดสัปดาห์ ฯลฯ) และนำกลับมาใช้อีกครั้งได้อย่างง่ายดายโดยไม่ต้องระบุช่วงเวลาสำหรับทุกกฎอีกครั้ง สล็อตเวลาสามารถนำไปใช้ได้กับกฎทุกประเภทที่เกี่ยวข้องที่รองรับการควบคุมตามเวลา



หากต้องการสร้างสล็อตเวลา ให้ทำสิ่งต่างๆ ต่อไปนี้:

1. คลิก**แก้ไข** > **เพิ่ม**
2. พิมพ์ชื่อและ **รายละเอียด** ของสล็อตเวลาและคลิก **เพิ่ม**
3. ระบุวันและเวลาเริ่มต้น/สิ้นสุดของสล็อตเวลาหรือเลือก **ตลอดทั้งวัน**

4. คลิก **ตกลง** เพื่อยืนยัน

สามารถระบุช่วงเวลาของสล็อตเวลาหนึ่งรายการได้ตั้งแต่หนึ่งช่วงเวลาขึ้นไปตามวันและเวลา เมื่อสร้างแล้ว ช่วงเวลาจะปรากฏในเมนูแบบเลื่อนลงสำหรับตัวเลือก **ใช้ในระหว่าง** ใน หน้าต่างตัวแก้ไขกฎการควบคุมอุปกรณ์ หรือ หน้าต่างตัวแก้ไขกฎการควบคุมการเข้าถึงเว็บไซต์

อัพเดท Microsoft Windows®

คุณลักษณะการอัพเดท Windows เป็นองค์ประกอบสำคัญสำหรับการป้องกันผู้ใช้ให้พ้นจากซอฟต์แวร์ที่เป็นอันตราย ด้วยเหตุผลนี้ การติดตั้งการอัพเดทของ Microsoft Windows ให้เร็วที่สุดเมื่อมีการเผยแพร่จึงเป็นสิ่งที่สำคัญ ESET Endpoint Security จะแจ้งคุณเกี่ยวกับการอัพเดทที่ขาดหายไป ตามระดับที่คุณระบุ ระดับที่ใช้ได้มีดังนี้:

- **ไม่มีการอัพเดท** – ไม่มีการเสนอการอัพเดทเพื่อให้ดาวน์โหลด
- **การอัพเดทที่เป็นตัวเลือก** – ระบบจะเสนอการอัพเดทที่ทำเครื่องหมายว่าเป็นอัพเดทมีความสำคัญต่ำและสูงกว่าให้ดาวน์โหลด
- **การอัพเดทที่แนะนำ** – ระบบจะเสนอการอัพเดทที่ทำเครื่องหมายว่าเป็นอัพเดททั่วไปและสูงกว่าให้ดาวน์โหลด
- **การอัพเดทสำคัญ** – ระบบจะเสนอการอัพเดทที่ทำเครื่องหมายว่าเป็นอัพเดทสำคัญและสูงกว่าให้ดาวน์โหลด
- **การอัพเดทที่สำคัญมาก** – ระบบจะเสนอเฉพาะการอัพเดทที่สำคัญมากให้ดาวน์โหลด

คลิกที่ **ตกลง** เพื่อบันทึกการเปลี่ยนแปลง หน้าต่างการอัพเดทระบบจะปรากฏหลังการตรวจสอบสถานะกับเซิร์ฟเวอร์การอัพเดท ดังนั้น ข้อมูลการอัพเดทระบบอาจไม่ปรากฏทันทีหลังจากบันทึกการเปลี่ยนแปลง

หน้าต่างข้อความ – การอัพเดทระบบปฏิบัติการ

หากมีรายการอัพเดทสำหรับระบบปฏิบัติการของคุณ หน้าต่างหน้าแรกของ ESET Endpoint Security จะแสดงการแจ้งเตือน คลิก **ข้อมูลเพิ่มเติม** เพื่อเปิดหน้าต่างการอัพเดทระบบ

หน้าต่างการอัพเดทระบบจะแสดงรายการอัพเดทที่พร้อมสำหรับการดาวน์โหลดและติดตั้ง ประเภทการอัพเดทจะปรากฏถัดจากชื่อของการอัพเดทนั้น

คลิกสองครั้งที่แถวของการอัพเดทแถวใดก็ได้เพื่อแสดงหน้าต่างข้อมูลการอัพเดทที่มีข้อมูลเพิ่มเติม

คลิก **เรียกใช้การอัพเดทระบบปฏิบัติการ** เพื่อดาวน์โหลดและติดตั้งการอัพเดทระบบปฏิบัติการที่แสดงในรายการ

ข้อมูลการอัพเดท

หน้าต่างการอัพเดทระบบจะแสดงรายการอัพเดทที่พร้อมสำหรับการดาวน์โหลดและติดตั้ง ระดับความสำคัญของการอัพเดทจะปรากฏถัดจากชื่อของการอัพเดทนั้น

คลิกที่ **เรียกใช้การอัพเดทระบบ** เพื่อเริ่มต้นดาวน์โหลดและติดตั้งการอัพเดทระบบปฏิบัติการ

คลิกขวาที่แถวการอัพเดท และคลิก**แสดงข้อมูล**เพื่อแสดงหน้าต่างใหม่พร้อมด้วยข้อมูลเพิ่มเติม

ESET CMD

นี่เป็นคุณลักษณะที่ทำให้สามารถใช้คำสั่ง ecmd แบบขั้นสูงได้ คุณสามารถส่งออกและนำเข้าการตั้งค่าได้โดยใช้บรรทัดคำสั่ง (ecmd.exe) ตอนนี้ คุณจะสามารถส่งออกการตั้งค่าได้โดยใช้ GUI เท่านั้น ส่วนการกำหนดค่า ESET Endpoint Security สามารถส่งออกไปเป็นไฟล์ *.xml* ได้

เมื่อคุณเปิดใช้งาน ESET CMD แล้ว จะสามารถใช้วิธีการให้สิทธิ์ได้ทั้งหมดสองวิธี

- **ไม่มี** - ไม่มีสิทธิ์ เราไม่แนะนำให้คุณใช้วิธีการนี้เนื่องจากวิธีการดังกล่าวอนุญาตให้มีการนำเข้าการกำหนดค่าใดๆ ที่ไม่ได้ลงชื่อ ซึ่งค่อนข้างมีความเสี่ยง
- **รหัสผ่านการตั้งค่าขั้นสูง** – ต้องใช้รหัสผ่านเพื่อนำเข้าการกำหนดค่าจากไฟล์ *.xml* ไฟล์นี้จะต้องลงชื่อ (ดูการลงชื่อการกำหนดค่าไฟล์ *.xml* ด้านล่าง) รหัสผ่านที่ระบุใน ตั้งค่าการเข้าถึง จะต้องใส่ก่อนที่จะสามารถนำเข้าการกำหนดค่าใหม่ได้ หากไม่ได้เปิดใช้งานการตั้งค่าการเข้าถึงไว้ รหัสผ่านไม่ตรงกัน หรือไม่มีการลงชื่อไฟล์การกำหนดค่า *.xml* การกำหนดค่าจะไม่ถูกนำเข้า

เมื่อเปิดใช้งาน ESET CMD อยู่ คุณจะสามารถใช้บรรทัดคำสั่งสำหรับส่งออกหรือนำเข้าการกำหนดค่า ESET Endpoint Security ได้ คุณสามารถทำขั้นตอนนี้ได้ด้วยตนเอง หรือสร้างสคริปต์เพื่อจุดประสงค์ด้านระบบอัตโนมัติ

หากต้องการใช้คำสั่ง ecmd ขั้นสูง คุณต้องใช้งานคำสั่งเหล่านั้นด้วยสิทธิ์ของผู้ดูแลระบบ หรือเปิด Windows Command Prompt (cmd) โดยใช้ **เรียกใช้ในฐานะผู้ดูแล** มิฉะนั้น คุณจะได้รับข้อความ **Error executing command** และเมื่อส่งออกการกำหนดค่า จะต้องมีโฟลเดอร์ปลายทางด้วย คำสั่งส่งออกจะยังคงทำงานได้เมื่อการตั้งค่า ESET CMD ถูกปิด

คำสั่ง ecmd ขั้นสูงสามารถเรียกใช้ในระบบได้เท่านั้น การหยุดคำสั่ง ecmd ชั่วคราวสามารถเรียกใช้ผ่านงานไคลเอ็นต์ **เรียกใช้คำสั่ง** โดยใช้ ESET PROTECT เท่านั้น

คำสั่งส่งออกการตั้งค่า:
`ecmd /getcfg c:\config\settings.xml`
คำสั่งนำเข้าการตั้งค่า:
`ecmd /setcfg c:\config\settings.xml`

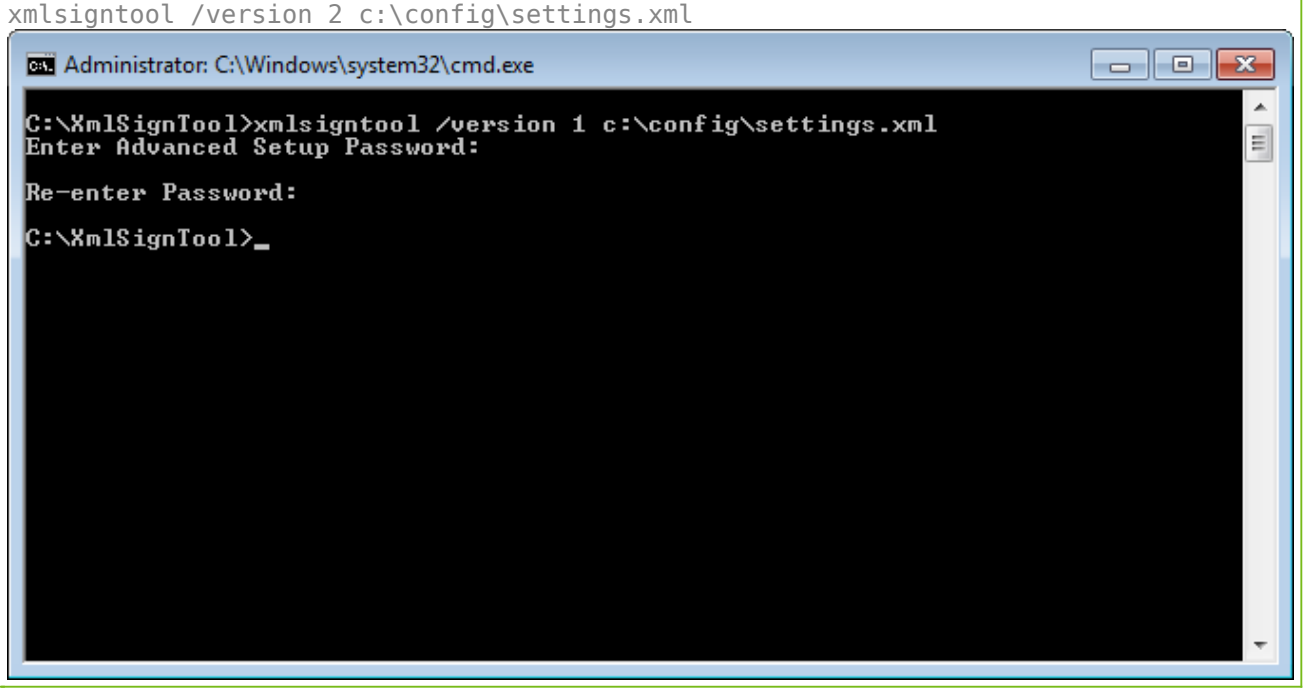
การลงชื่อไฟล์การกำหนดค่า *.xml*:

1. ดาวน์โหลดไฟล์ที่เรียกใช้ XmlSignTool
2. เปิด Windows Command Prompt (cmd) โดยใช้ **เรียกใช้ในฐานะผู้ดูแล**
3. ไปที่ตำแหน่งที่บันทึก `xmlsigntool.exe`
4. ดำเนินการคำสั่งเพื่อลงชื่อไฟล์การกำหนดค่า *.xml* การใช้งาน: `xmlsigntool /version 1|2 <xml_file_path>`

ค่าพารามิเตอร์ของ `/version` จะขึ้นอยู่กับเวอร์ชันของ ESET Endpoint Security ใช้ `/version 2` สำหรับเวอร์ชัน 7 และรุ่นใหม่กว่า

5. ป้อนแล้วป้อนรหัสผ่านของ การตั้งค่าขั้นสูง อีกครั้งตามที่ได้รับแจ้งจาก XmlSignTool ไฟล์การกำหนดค่า *.xml* ของคุณได้รับการลงชื่อแล้วตอนนี้ และสามารถใช้นำเข้าในอีกอินสแตนซ์หนึ่งของ ESET Endpoint Security ด้วย ESET CMD ได้โดยใช้วิธีการให้สิทธิ์รหัสผ่าน

คำสั่งลงชื่อไฟล์การกำหนดค่าที่ส่งออก:
`xmlsigntool /version 2 c:\config\settings.xml`



หากรหัสผ่าน ตั้งค่าการเข้าถึง ของคุณเปลี่ยนและคุณต้องการนำเข้าการกำหนดค่าที่ลงชื่อไว้ก่อนหน้าด้วยรหัสเก่า คุณจะต้องลงชื่อไฟล์การตั้งค่า *.xml* อีกครั้งโดยใช้รหัสผ่านปัจจุบันของคุณ การดำเนินการนี้จะทำให้คุณสามารถใช้ไฟล์การกำหนดค่าเก่าโดยไม่ต้องส่งออกไปอีกเครื่องที่กำลังเรียกใช้ ESET Endpoint Security ก่อนที่จะนำเข้า

ไม่แนะนำให้เปิดใช้งาน ESET CMD โดยไม่ใช้วิธีการให้สิทธิ์ เนื่องจากวิธีนี้จะอนุญาตการนำเข้าการกำหนดค่าใดๆ ที่ไม่ได้ลงชื่อ ตั้งรหัสผ่านใน การตั้งค่าขั้นสูง > **ส่วนติดต่อผู้ใช้** > **ตั้งค่าการเข้าถึง** เพื่อป้องกันไม่ให้มีการแก้ไขโดยไม่ได้รับอนุญาตจากผู้ใช้

รายการของคำสั่ง ecmd

สามารถเปิดใช้งานคุณลักษณะการรักษาความปลอดภัยแต่ละส่วนได้ และปิดใช้งานคำสั่ง ESET PROTECT Client Task Run ชั่วคราวได้ คำสั่งจะไม่เขียนทับการตั้งค่านโยบายและการตั้งค่าต่างๆ ที่หยุดชั่วคราวจะย้อนกลับไปเป็นสถานะดั้งเดิมหลังจากที่คำสั่งถูกใช้งานหรือหลังจากเครื่องเริ่มต้นระบบใหม่ ในการใช้งานคุณลักษณะนี้ ให้ระบุบรรทัดคำสั่งเพื่อเรียกใช้ในช่องของชื่อเดียวกัน

ดูรายการของคำสั่งตางๆ สำหรับคุณลักษณะการรักษาความปลอดภัยด้านล่าง:

คุณลักษณะการรักษาความปลอดภัย	คำสั่งหยุดชั่วคราว	เปิดใช้งานคำสั่ง
การป้องกันระบบไฟล์แบบเรียลไทม์	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
การป้องกันเอกสาร	ecmd /setfeature document pause	ecmd /setfeature document enable
การควบคุมอุปกรณ์	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
โหมดการนำเสนอ	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
ไฟร์วอลล์ส่วนบุคคล	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
เปิดใช้งานการป้องกันการโจมตีเครือข่าย (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
การป้องกันบอทเน็ต	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
การควบคุมการเข้าถึงเว็บไซต์	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
การป้องกันการเข้าถึงเว็บ	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
การป้องกันอีเมลไคลเอ็นต์	ecmd /setfeature email pause	ecmd /setfeature email enable
การป้องกันสแปมอีเมลไคลเอ็นต์	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
การป้องกันฟิชชิ่ง	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

การตรวจสอบและการจัดการระยะไกล

การตรวจสอบและการจัดการระยะไกล (RMM) เป็นกระบวนการในการดูแลและควบคุมระบบซอฟต์แวร์โดยใช้ตัวแทนที่ติดตั้งในระบบที่ผู้ให้บริการด้านการจัดการสามารถเข้าถึงได้

ERMM - ปลั๊กอิน ESET สำหรับ RMM

- การติดตั้ง ESET Endpoint Security เริ่มต้นจะประกอบด้วยไฟล์ `ermm.exe` ที่อยู่ในแอพพลิเคชันของอุปกรณ์ปลายทางภายในไดเรกทอรี:
  C:\Program Files\ESET\ESET Security\ermm.exe
- `ermm.exe` คือยูทิลิตี้บรรทัดคำสั่งที่ออกแบบมาเพื่ออำนวยความสะดวกในการจัดการผลิตภัณฑ์อุปกรณ์ปลายทางและการสื่อสารกับปลั๊กอิน RMM

- `ermm.exe` จะแลกเปลี่ยนข้อมูลกับปลั๊กอิน RMM ซึ่งสื่อสารกับเอเจนท์ RMM ที่เชื่อมโยงกับเซิร์ฟเวอร์ RMM โดยเครื่องมือ RMM ของ ESET จะถูกปิดใช้งาน ตามค่าเริ่มต้น

ทรัพยากรเพิ่มเติม

- บรรทัดคำสั่ง ERMM
- รายการคำสั่ง ERMM JSON
- วิธีเปิดใช้งานการตรวจสอบและการจัดการระยะไกลESET Endpoint Security

ปลั๊กอิน ESET Direct Endpoint Management สำหรับโซลูชัน RMM ของบริษัทอื่น

เซิร์ฟเวอร์ RMM จะทำงานเป็นบริการบนเซิร์ฟเวอร์ของบริษัทอื่น สำหรับข้อมูลเพิ่มเติมให้ดูคู่มือผู้ใช้แบบออนไลน์ของ ESET Direct Endpoint Management ดังต่อไปนี้:

- ปลั๊กอิน ESET Direct Endpoint Management สำหรับ ConnectWise Automate
- ปลั๊กอิน ESET Direct Endpoint Management สำหรับ DattoRMM
- ESET Direct Endpoint Management สำหรับ Solarwinds N-Central
- ESET Direct Endpoint Management สำหรับ NinjaRMM

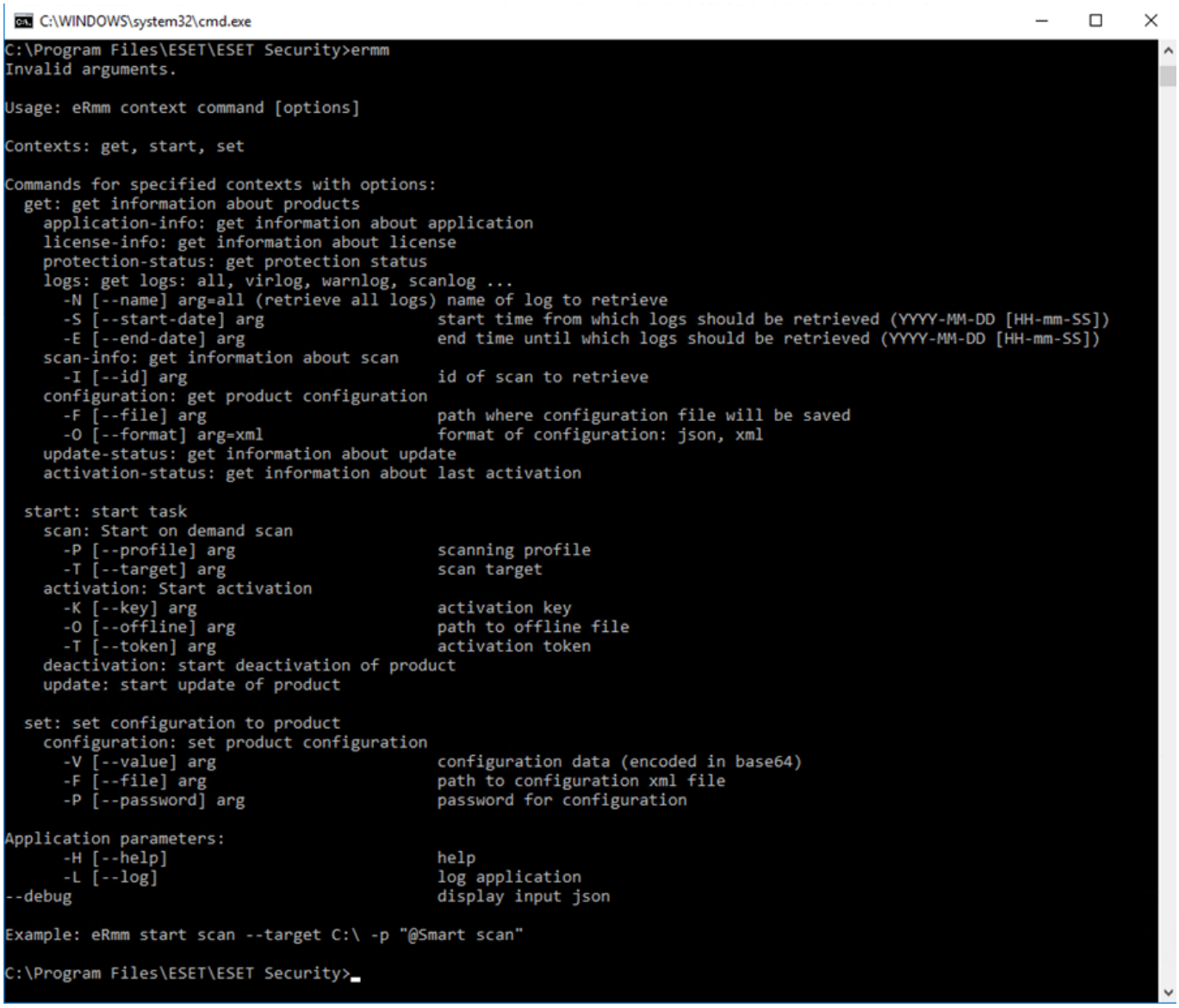
บรรทัดคำสั่ง ERMM

การจัดการการตรวจสอบระยะไกลดำเนินการโดยใช้ส่วนติดต่อของบรรทัดคำสั่ง การติดตั้ง ESET Endpoint Security เริ่มต้นจะประกอบด้วยไฟล์ ermm.exe ที่อยู่ในแอพพลิเคชันของอุปกรณ์ปลายทางภายในไดเรกทอรี *c:\Program Files\ESET\ESET Security*

เรียกใช้ Command Prompt (cmd.exe) ในฐานะผู้ดูแลระบบและไปยังพาธดังกล่าว (กดปุ่ม Windows + R บนแป้นพิมพ์ แล้วพิมพ์ cmd ลงในหน้าต่าง Run แล้วกด Enter เพื่อเปิด Command Prompt)

โครงสร้างภาษาของคำสั่งคือ: `ermm context command [options]`

พารามิเตอร์บันทึกต้องตรงตามตัวพิมพ์เล็กและพิมพ์ใหญ่



ermm.exe ใช้สามบริบทพื้นฐาน: รับ เริ่มต้น และตั้งค่า สามารถดูตัวอย่างโครงสร้างภาษาของคำสั่งได้ในตารางด้านล่าง คลิกลิงก์ในคอลัมน์คำสั่งเพื่อดูตัวเลือก พารามิเตอร์ และตัวอย่างการใช้งานเพิ่มเติม หลังจากการดำเนินคำสั่งสำเร็จ ส่วนเอาท์พุต (ผลลัพธ์) จะแสดงขึ้น หากต้องการดูส่วนอินพุต ให้เพิ่มพารามิเตอร์ `--debug` ที่คำสั่ง

บริบท	คำสั่ง	คำอธิบาย
get		**รับข้อมูลเกี่ยวกับผลิตภัณฑ์**
	application-info	รับข้อมูลเกี่ยวกับผลิตภัณฑ์
	license-info	รับข้อมูลเกี่ยวกับใบอนุญาต
	protection-status	สถานะของการป้องกัน
	logs	ขอบันทึก
	scan-info	รับข้อมูลเกี่ยวกับการเรียกใช้การสแกน
	configuration	รับการกำหนดค่าผลิตภัณฑ์
	update-status	รับข้อมูลเกี่ยวกับการอัพเดท
	activation-status	รับข้อมูลเกี่ยวกับการเปิดใช้งานครั้งล่าสุด
start		**เริ่มงาน**

บริบท	คำสั่ง	คำอธิบาย
	scan	เริ่มสแกนตามความต้องการ
	activation	เริ่มการเปิดใช้งานผลิตภัณฑ์
	deactivation	เริ่มการปิดใช้งานผลิตภัณฑ์
	update	เริ่มการอัพเดทผลิตภัณฑ์
set		**ตั้งค่าตัวเลือกสำหรับผลิตภัณฑ์**
	configuration	ตั้งค่าการกำหนดค่าไปยังผลิตภัณฑ์

ในผลลัพธ์เอาท์พุตของทุกคำสั่ง ข้อมูลแรกที่แสดงเป็น ID ผลลัพธ์ โปรดตรวจสอบตาราง ID ด้านล่างเพื่อให้เข้าใจข้อมูลผลลัพธ์ได้ดียิ่งขึ้น

ID ข้อผิดพลาด	ข้อผิดพลาด	คำอธิบาย
0	Success	
1	Command node not present	โหนด “คำสั่ง” ไม่อยู่ใน JSON อินพุต
2	Command not supported	ไม่รองรับคำสั่ง
3	General error executing the command	เกิดข้อผิดพลาดระหว่างกำลังดำเนินการคำสั่ง
4	Task already running	งานที่ขอกำลังดำเนินการอยู่แล้วและยังไม่ได้เริ่ม
5	Invalid parameter for command	การป้อนข้อมูลของผู้ใช้ไม่ถูกต้อง
6	Command not executed because it's disabled	RMM ไม่ได้เปิดใช้งานในการตั้งค่าขั้นสูงหรือเริ่มในฐานะผู้ดูแลระบบ

รายการคำสั่ง ERMM JSON

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status
- get scan-info
- get configuration
- get update-status
- start scan
- start activation
- start deactivation
- start update
- set configuration

get protection-status

Get the list of application statuses and the global application status

บรรทัดคำสั่ง

```
ermm.exe get protection-status
```

พารามิเตอร์

None

ตัวอย่าง

call

```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```

get application-info

Get information about the installed application

บรรทัดคำสั่ง

```
ermm.exe get application-info
```

พารามิเตอร์

None

ตัวอย่าง

call

```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

บรรทัดคำสั่ง

```
ermm.exe get license-info
```

พารามิเตอร์

None

ตัวอย่าง

call

```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```

get logs

Get logs of the product

บรรทัดคำสั่ง

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

พารามิเตอร์

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

ตัวอย่าง

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be { success, running, failure }

บรรทัดคำสั่ง

```
ermm.exe get activation-status
```

พารามิเตอร์

None

ตัวอย่าง

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

รับข้อมูลเกี่ยวกับการเรียกใช้การสแกน

บรรทัดคำสั่ง

```
ermm.exe get scan-info
```

พารามิเตอร์

ไม่มี

ตัวอย่าง

เรียก

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

ผลลัพธ์


```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

บรรทัดคำสั่ง

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

พารามิเตอร์

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

ตัวอย่าง

call

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

บรรทัดคำสั่ง

```
ermm.exe get update-status
```

พารามิเตอร์

None

ตัวอย่าง

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

บรรทัดคำสั่ง

```
ermm.exe start scan --profile "profile name" --target "path"
```

พารามิเตอร์

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

ตัวอย่าง

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

บรรทัดคำสั่ง

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

พารามิเตอร์

Name	Value
key	Activation key
offline	Path to offline file

ตัวอย่าง

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start deactivation

Start deactivation of the product

บรรทัดคำสั่ง

```
ermm.exe start deactivation
```

พารามิเตอร์

None

ตัวอย่าง

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

บรรทัดคำสั่ง

```
ermm.exe start update
```

พารามิเตอร์

None

ตัวอย่าง

call

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

บรรทัดคำสั่ง

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

พารามิเตอร์

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

ตัวอย่าง

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

การตรวจสอบช่วงเวลาของใบอนุญาต

ESET Endpoint Security จำเป็นต้องเชื่อมต่อกับเซิร์ฟเวอร์ของ ESET โดยอัตโนมัติ คุณสามารถจำกัดจำนวนการเชื่อมต่อกับเซิร์ฟเวอร์ใบอนุญาต ESET ได้ใน การตั้งค่าขั้นสูง > **เครื่องมือ** > **ใบอนุญาต** ตามค่าเริ่มต้น **ช่วงการตรวจสอบ** จะตั้งค่าเป็น **อัตโนมัติ** และระบบจะสร้างการเชื่อมต่อสองสามครั้งทุกๆ ชั่วโมง ในกรณีที่มีปริมาณการรับส่งข้อมูลเครือข่ายมาก ให้เปลี่ยน **ช่วงการตรวจสอบ** เป็น **จำกัด** เพื่อลดการโอเวอร์โหลด เมื่อการ **จำกัด** ถูกเลือก ESET Endpoint Security จะตรวจสอบเซิร์ฟเวอร์เพียงวันละครั้ง หรือเมื่อรีสตาร์ทคอมพิวเตอร์

หากการตั้งค่า **การตรวจสอบช่วงเวลา** ได้ตั้งค่าเป็น **จำกัด** การเปลี่ยนแปลงทั้งหมดซึ่งเกี่ยวข้องกับใบอนุญาตที่เสร็จสิ้นผ่าน ESET HUB /ESET MSP Administrator อาจใช้เวลาถึงหนึ่งวันในการปรับใช้การตั้งค่า ESET Endpoint Security ดังกล่าว

ไฟล์บันทึก

คุณสามารถเข้าถึงการกำหนดค่าการบันทึกของ ESET Endpoint Security ได้ใน การตั้งค่าขั้นสูง > **เครื่องมือ** > **ไฟล์บันทึก** ส่วนบันทึกนี้ใช้เพื่อกำหนดวิธีจัดการบันทึก โปรแกรมจะลบบันทึกเก่าโดยอัตโนมัติ เพื่อประหยัดพื้นที่บนฮาร์ดดิสก์ คุณสามารถระบุตัวเลือกต่อไปนี้สำหรับไฟล์บันทึก:

ความละเอียดขั้นต่ำในการบันทึก – ระบุระดับความละเอียดขั้นต่ำของเหตุการณ์ที่จะบันทึก:

- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- **มีข้อมูล** – บันทึกข้อความแจ้งข้อมูล รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน
- **ข้อผิดพลาด** – ข้อผิดพลาด เช่น "เกิดข้อผิดพลาดขณะดาวน์โหลดไฟล์" และข้อผิดพลาดร้ายแรงจะถูกบันทึก
- **ร้ายแรง** – บันทึกเฉพาะข้อผิดพลาดร้ายแรง (ข้อผิดพลาดในการเริ่มต้นการป้องกันไวรัส, ไฟร์วอลล์แบบติดตั้งในตัว เป็นต้น)

การเชื่อมต่อที่ปิดกั้นจะบันทึกไว้เมื่อคุณเลือกระดับค่าความละเอียดของ **การวินิจฉัย**

รายการบันทึกที่เก่ากว่าจำนวนวันที่ระบุในช่อง **ลบอัตโนมัติสำหรับบันทึกที่เก่ากว่า (วัน)** จะถูกลบโดยอัตโนมัติ

ปรับปรุงประสิทธิภาพไฟล์บันทึกโดยอัตโนมัติ – เมื่อเริ่มใช้งานแล้ว ไฟล์บันทึกจะถูกจัดเรียงข้อมูลโดยอัตโนมัติถ้ามีเปอร์เซ็นต์การกระจายตัวมากกว่าค่าที่ระบุในช่อง **ถ้าจำนวนบันทึกที่ไม่ได้ใช้งานเกิน (%)**

คลิก **ปรับปรุงประสิทธิภาพ** เพิ่มเริ่มต้นการจัดระเบียบบันทึกไฟล์ใหม่ รายการบันทึกที่ว่างเปล่าทั้งหมดจะถูกลบออกเพื่อช่วยปรับปรุงประสิทธิภาพและความเร็วของการประมวลผลบันทึก การปรับปรุงนี้จะเห็นได้ชัดโดยเฉพาะถ้าบันทึกมีรายการจำนวนมาก

เปิดใช้งานโปรโตคอลข้อความ เปิดใช้งานการบันทึกในรูปแบบอื่นแยกจาก ไฟล์บันทึก:

- **ไดเรกทอรีเป้าหมาย** – เลือกไดเรกทอรีที่จะจัดเก็บไฟล์บันทึก (ใช้เฉพาะกับ Text/CSV) คุณสามารถคัดลอกพาธหรือเลือกไดเรกทอรีอื่นโดยคลิก **ล้าง** แต่ละส่วนบันทึกมีไฟล์และชื่อไฟล์ที่กำหนดไว้ล่วงหน้าเป็นของตัวเอง (ตัวอย่างเช่น *virlog.txt* สำหรับส่วน **ภัยคุกคามที่พบ** ของไฟล์บันทึก ถ้าคุณใช้ไฟล์รูปแบบข้อความธรรมดาในการจัดเก็บบันทึก)
- **ประเภท** – ถ้าคุณเลือกรูปแบบไฟล์เป็น **ข้อความ** บันทึกจะจัดเก็บเป็นไฟล์ข้อความและข้อมูลจะคั่นด้วยแท็บต่างๆ การดำเนินการเดียวกันนี้ใช้เครื่องหมายจุลภาคเพื่อคั่นรูปแบบไฟล์ประเภท **CSV** ถ้าคุณเลือก **เหตุการณ์** การบันทึกจะจัดเก็บในบันทึก Windows Event (สามารถดูผ่าน Event Viewer ใน Control panel ได้) แทนที่จะเก็บไปยังไฟล์
- **ลบไฟล์บันทึกทั้งหมด** – ลบบันทึกที่เก็บไว้ทั้งหมดที่เลือกในปัจจุบันในเมนูแบบเลื่อนลง **ประเภท** การแจ้งเตือนเกี่ยวกับการลบบันทึกได้สำเร็จจะปรากฏขึ้น

เปิดใช้งานการติดตามการกำหนดค่าการเปลี่ยนแปลงในบันทึกการตรวจสอบ – ซึ่งแจ้งคุณเกี่ยวกับการเปลี่ยนแปลงการกำหนดค่าในแต่ละครั้ง โปรดดู บันทึกการตรวจสอบ สำหรับข้อมูลเพิ่มเติม

> i เพื่อให้สามารถแก้ไขปัญหาได้เร็วยิ่งขึ้น ESET อาจขอให้คุณมอบบันทึกจากคอมพิวเตอร์ของคุณ ESET Log Collector ช่วยให้คุณสามารถเก็บข้อมูลที่จำเป็นได้ง่ายยิ่งขึ้น สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ESET Log Collector ให้ไปที่ บทความฐานความรู้ ESET ของเรา

โหมดการนำเสนอ

โหมดการนำเสนอเป็นฟีเจอร์สำหรับผู้ใช้ที่ต้องการใช้ซอฟต์แวร์อย่างต่อเนื่องไม่ขาดสาย ไม่ต้องการถูกรบกวนจากหน้าต่างแจ้งเตือน/เตือนภัย และต้องการลดการใช้งาน CPU ลง โหมดการนำเสนอสามารถใช้ระหว่างการนำเสนอที่ไม่ควรมีการขัดจังหวะโดยกิจกรรมการป้องกันไวรัส เมื่อเปิดใช้งานคุณลักษณะนี้ หน้าต่างป๊อปอัปทั้งหมดจะถูกปิดใช้งาน และกิจกรรมของเครื่องมือวางกำหนดการจะหยุดทำงานโดยสิ้นเชิง การป้องกันระบบจะยังทำงานอยู่ในพื้นหลัง แต่ผู้ใช้ไม่ต้องดำเนินการใดๆ

คุณสามารถเปิดหรือปิดใช้งานโหมดการนำเสนอได้ใน หน้าต่างโปรแกรมหลัก ในส่วน **การตั้งค่า** > **คอมพิวเตอร์** โดยคลิก หรือ ที่อยู่ถัดจาก **โหมดการนำเสนอ** การเปิดใช้งานโหมดการนำเสนออาจทำให้เกิดความเสี่ยงด้านความปลอดภัย ดังนั้นไอคอนสถานะการป้องกันที่ทาสก์บาร์จะเปลี่ยนเป็นสีส้มพร้อมกับการเตือน คุณ

ยังจะเห็นคำเตือนนี้ใน หน้าต่างโปรแกรมหลัก ซึ่งคุณจะเห็น **โหมดการนำเสนอเปิดใช้งานอยู่** เป็นสีส้ม

เปิดใช้งาน **เปิดใช้งานโหมดการนำเสนอเมื่อเรียกใช้แอพพลิเคชันในโหมดเต็มหน้าจอโดยอัตโนมัติ** > การตั้งค่าขั้นสูง > **เครื่องมือ** > **โหมดการนำเสนอ** เพื่อเริ่มโหมดการนำเสนอเมื่อใดก็ตามที่คุณเริ่มใช้งานแอพพลิเคชันแบบเต็มหน้าจอและหยุดหลังจากที่คุณออกจากแอพพลิเคชันนั้น

เปิดใช้ตัวเลือก **ปิดโหมดการนำเสนออัตโนมัติหลังจาก** เพื่อกำหนดระยะเวลาที่จะให้ปิดใช้งานโหมดการนำเสนอโดยอัตโนมัติเมื่อเวลาผ่านไป

ถ้าไฟร์วอลล์อยู่ในโหมดตอบสนอง และมีการเปิดใช้งานโหมดการนำเสนอ คุณอาจพบปัญหาในการเชื่อมต่อกับอินเทอร์เน็ต ซึ่งอาจเป็นปัญหาถ้าคุณเริ่มต้นเกมที่เชื่อมต่อกับอินเทอร์เน็ต โดยปกติแล้ว ระบบจะสอบถามเพื่อให้คุณยืนยันการทำงานดังกล่าว (ถ้าไม่ได้กำหนดกฎการสื่อสารหรือการยกเว้นไว้) แต่การดำเนินการของผู้ใช้จะถูกปิดใช้งานในโหมดการนำเสนอ การแก้ไขปัญหานี้คือให้กำหนดกฎการสื่อสารสำหรับทุกแอพพลิเคชันที่อาจขัดแย้งกับการทำงานนี้ หรือให้ใช้ โหมดการกรอง อื่นๆ ในไฟร์วอลล์ โปรดทราบว่าถ้าเปิดใช้งานโหมดการนำเสนอ และคุณไปยังหน้าเว็บหรือแอพพลิเคชันที่อาจเกิดความเสี่ยงด้านความปลอดภัย ระบบอาจปิดกั้นหน้าเว็บหรือแอพพลิเคชันเหล่านี้ แต่คุณจะไม่เห็นคำอธิบายหรือการเตือน เนื่องจากการดำเนินการของผู้ใช้ถูกปิดใช้งาน

การวินิจฉัย

การวินิจฉัยจะให้บันทึกข้อมูลความล้มเหลวของแอพพลิเคชันของกระบวนการ ESET (ekrn เป็นต้น) หากแอพพลิเคชันล่ม บันทึกข้อมูลความล้มเหลวจะถูกสร้างขึ้น สิ่งนี้สามารถช่วยให้นักพัฒนาแก้ไขปัญหาและปรับแก้ปัญหาต่างๆ ของ ESET Endpoint Security ได้

คลิกเมนูแบบเลื่อนลงที่อยู่ถัดจาก **ชนิดดัมพ์** แล้วเลือกหนึ่งในสามตัวเลือกที่มีให้:

- เลือก**ปิดใช้งาน** เพื่อปิดใช้งานคุณลักษณะนี้
- **เล็ก** ค่าเริ่มต้น – บันทึกข้อมูลที่เป็นประโยชน์ไว้ในปริมาณที่น้อยที่สุด ซึ่งอาจช่วยระบุสาเหตุที่ทำให้แอพพลิเคชันเสียหายโดยไม่คาดหมาย ไฟล์ดัมพ์ชนิดนี้จะมีประโยชน์เมื่อมีพื้นที่ว่างจำกัด แต่เนื่องจากมีข้อมูลที่จำกัด การวิเคราะห์ไฟล์นี้อาจไม่พบข้อผิดพลาดที่ไม่ได้เกิดโดยตรงจากเธรดที่ทำงานอยู่เมื่อเกิดปัญหา
- **เต็ม** - บันทึกเนื้อหาทั้งหมดของหน่วยความจำระบบเมื่อแอพพลิเคชันหยุดทำงานโดยไม่คาดคิด ดัมพ์หน่วยความจำแบบสมบูรณ์อาจมีข้อมูลจากกระบวนการที่ทำงานอยู่เมื่อมีการรวบรวมดัมพ์หน่วยความจำ

ไดเรกทอรีเป้าหมาย – ไดเรกทอรีที่ดัมพ์ในระหว่างที่เกิดความเสียหายถูกสร้างขึ้น

เปิดโฟลเดอร์การวินิจฉัย – คลิก **เปิด** เพื่อเปิดไดเรกทอรีนี้ในหน้าต่าง *Windows explorer* ใหม่

สร้างดัมพ์การวินิจฉัย - คลิก **สร้าง** เพื่อสร้างไฟล์ดัมพ์การวินิจฉัยใน **ไดเรกทอรีเป้าหมาย**

การบันทึกขั้นสูง

เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันสแปม – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นระหว่างการสแกนสแปม ซึ่งจะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับกลไก ESET Antispam

เปิดใช้งานการบันทึกขั้นสูงของการป้องกันเบราว์เซอร์: บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในเบราว์เซอร์ปลอดภัยเพื่ออนุญาตการวินิจฉัยและการแก้ไขปัญหา

เปิดใช้งานเครื่องมือสแกนการบันทึกขั้นสูง – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นระหว่างการสแกนไฟล์และโฟลเดอร์โดยการสแกนคอมพิวเตอร์หรือการป้องกันระบบไฟล์แบบเรียลไทม์

เปิดใช้งานการบันทึกขั้นสูงสำหรับการควบคุมเนื้อหา – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการควบคุมอุปกรณ์ ซึ่งจะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับการควบคุมอุปกรณ์ได้

เปิดใช้งานการบันทึกขั้นสูงของ Direct Cloud: บันทึกการสื่อสารของผลิตภัณฑ์ทั้งหมดระหว่างผลิตภัณฑ์และเซิร์ฟเวอร์ Direct Cloud

เปิดใช้งานการบันทึกขั้นสูงของการป้องกันเอกสาร – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการป้องกันเอกสารเพื่ออนุญาตการวินิจฉัยและการแก้ไขปัญหา

เปิดใช้งานการบันทึกขั้นสูงของการป้องกันอีเมลไคลเอ็นต์ - บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการป้องกันอีเมลไคลเอ็นต์และปลั๊กอินอีเมลไคลเอ็นต์เพื่อให้สามารถดำเนินการวินิจฉัยและแก้ปัญหาได้

เปิดใช้งานเคอร์เนลการบันทึกขั้นสูง – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในบริการ ESET Kernel (ekrn) เพื่อช่วยวินิจฉัยและแก้ไขปัญหา

เปิดใช้งานการอนุญาตการบันทึกขั้นสูง – บันทึกการสื่อสารทั้งหมดของผลิตภัณฑ์ด้วยการเปิดใช้งาน ESET และเซิร์ฟเวอร์การอนุญาต

เปิดใช้งานการติดตามหน่วยความจำ - บันทึกเหตุการณ์ทั้งหมดซึ่งจะช่วยนักพัฒนาในการวินิจฉัยปัญหาหน่วยความจำรั่ว

เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันเครือข่าย - บันทึกข้อมูลทั้งหมดในเครือข่ายที่ส่งผ่านไฟร์วอลล์ในรูปแบบ PCAP เพื่อช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวข้องกับไฟร์วอลล์ได้

เปิดใช้การบันทึกขั้นสูงของเครื่องมือสแกนการรับส่งข้อมูลเครือข่าย – บันทึกข้อมูลทั้งหมดที่ส่งผ่านเครื่องมือสแกนการรับส่งข้อมูลเครือข่ายในรูปแบบ PCAP เพื่อช่วยให้นักพัฒนาวินิจฉัยและแก้ไขปัญหาที่เกี่ยวข้องกับเครื่องมือสแกนการรับส่งข้อมูลเครือข่าย

เปิดใช้งานการบันทึกขั้นสูงสำหรับระบบปฏิบัติการ – ข้อมูลเพิ่มเติมเกี่ยวกับระบบปฏิบัติการ เช่น กระบวนการที่ทำงานอยู่ กิจกรรม CPU การทำงานของดิสก์จะถูกเก็บรวบรวม สิ่งนี้สามารถช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับผลิตภัณฑ์ ESET ที่ทำงานอยู่ในระบบปฏิบัติการของคุณได้

เปิดใช้งานการบันทึกขั้นสูงของการส่งข้อความแบบพุช: บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในระหว่างการส่งข้อความแบบพุชเพื่ออนุญาตการวินิจฉัยและการแก้ปัญหา

เปิดใช้งานการบันทึกขั้นสูงของการป้องกันระบบไฟล์แบบเรียลไทม์ – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการป้องกันระบบไฟล์แบบเรียลไทม์เพื่ออนุญาตให้ระบบทำการวินิจฉัยและแก้ไขปัญหา

เปิดใช้งานการบันทึกขั้นสูงสำหรับกลไกอัพเดท – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในกระบวนการอัพเดท ซึ่งการทำเช่นนี้จะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวข้องกับกลไกการอัพเดทได้

เปิดใช้งานการบันทึกขั้นสูงสำหรับการจัดการจุดอ่อนและแพทช์ – บันทึกเหตุการณ์ทั้งหมดในการจัดการจุดอ่อนและแพทช์ การตั้งค่านี้จะแสดงก็ต่อเมื่อเปิดใช้งานการจัดการจุดอ่อนและแพทช์ในสภาพแวดล้อมการทำงานของคุณ (เปิดใช้งานใน ESET PROTECT Cloud)

เปิดใช้งานการบันทึกขั้นสูงสำหรับการควบคุมการเข้าถึงเว็บไซต์ – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการควบคุมการเข้าถึงเว็บไซต์ ซึ่งจะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับการควบคุมการเข้าถึงเว็บไซต์ได้

แฟ้มบันทึกจะอยู่ใน *C:\ProgramData\ESET\ESET Security\Diagnostics*

ฝ่ายสนับสนุนด้านเทคนิค

เมื่อ ติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET จาก ESET Endpoint Security แล้ว คุณสามารถส่งข้อมูลการกำหนดค่าระบบได้ เลือก **ส่งเสมอ** จากเมนูแบบเลื่อนลง **ส่งข้อมูลการกำหนดค่าระบบ** เพื่อส่งข้อมูลโดยอัตโนมัติ หรือเลือก **ถามก่อนส่ง** เพื่อให้ได้รับข้อความเตือนก่อนจะส่งข้อมูล

การเชื่อมต่อ

ในบางรูปแบบเครือข่าย พร็อกซีเซิร์ฟเวอร์สามารถควบคุมการสื่อสารระหว่างคอมพิวเตอร์ของคุณกับอินเทอร์เน็ตได้ หากคุณต้องการใช้พร็อกซีเซิร์ฟเวอร์ คุณต้องกำหนดการตั้งค่าต่อไปนี้ มิฉะนั้น ESET Endpoint Security และโมดูลจะไม่อัพเดทได้โดยอัตโนมัติ ใน ESET Endpoint Security การตั้งค่าพร็อกซีเซิร์ฟเวอร์จะพร้อมให้ใช้งานในส่วนสองส่วนของการตั้งค่าขั้นสูง

โดยการตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วมสามารถกำหนดได้ใน การตั้งค่าขั้นสูง > **การเชื่อมต่อ** > **พร็อกซีเซิร์ฟเวอร์** การระบุพร็อกซีเซิร์ฟเวอร์ที่ระดับนี้จะกำหนดการตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วมสำหรับ ESET Endpoint Security ทั้งหมด พารามิเตอร์ในที่นี้จะถูกนำมาใช้โดยโมดูลทั้งหมดที่ต้องการการเชื่อมต่ออินเทอร์เน็ต

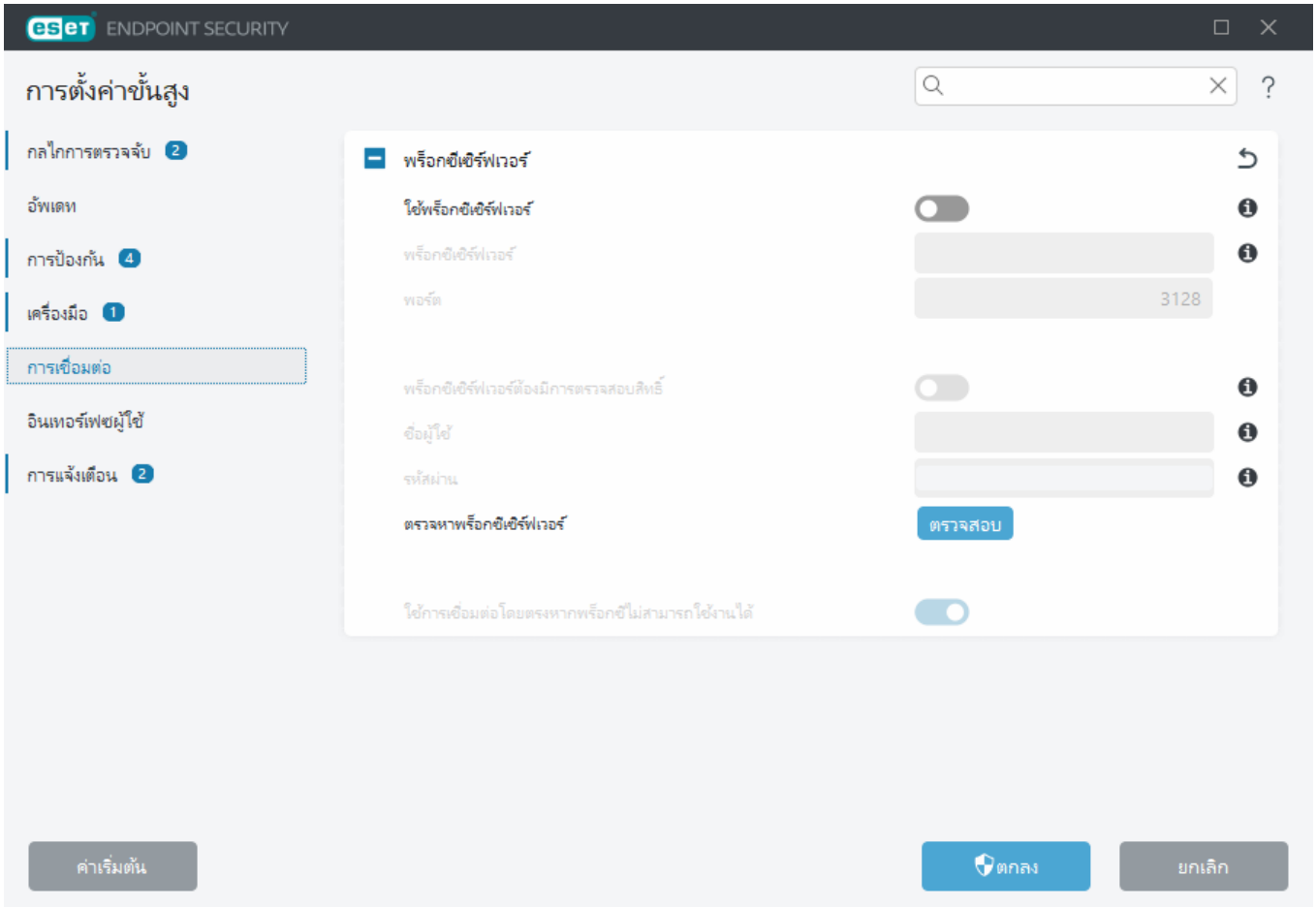
หากต้องการระบุการตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วมแบบเฉพาะเจาะจง ให้เปิดใช้ **ใช้พร็อกซีเซิร์ฟเวอร์** และพิมพ์ที่อยู่ของ**พร็อกซีเซิร์ฟเวอร์**พร้อมกับหมายเลข**พอร์ต**ของพร็อกซีเซิร์ฟเวอร์

หากการสื่อสารกับพร็อกซี่เซิร์ฟเวอร์ที่จำเป็นต้องมีการตรวจสอบสิทธิ์ ให้เลือก**พร็อกซี่เซิร์ฟเวอร์ต้องมีการตรวจสอบสิทธิ์** แล้วป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** ที่ถูกต้องลงในช่องที่สอดคล้องกัน คลิก **ตรวจหาพร็อกซีเซิร์ฟเวอร์** เพื่อตรวจหาและเติมการตั้งค่าพร็อกซีเซิร์ฟเวอร์โดยอัตโนมัติ หากต้องการค้นหาการตั้งค่าพร็อกซีในระบบปฏิบัติการของคุณ ให้กดปุ่มลัด **Windows + I** และคลิก **เครือข่ายและอินเทอร์เน็ต** > **พร็อกซี** ESET Endpoint Security จะคัดลอกพารามิเตอร์ที่ระบุไว้ในตัวเลือกอินเทอร์เน็ตสำหรับ Internet Explorer หรือ Google Chrome

> คุณต้องป้อนชื่อผู้ใช้และรหัสผ่านของคุณลงในการตั้งค่า **พร็อกซีเซิร์ฟเวอร์** ด้วยตัวเอง

ใช้การเชื่อมต่อโดยตรงหากพร็อกซีไม่สามารถใช้งานได้ – หาก ESET Endpoint Security ถูกกำหนดค่าผ่านพร็อกซี่และไม่สามารถเข้าถึงพร็อกซี่ได้ESET Endpoint Security จะข้ามพร็อกซี่และสื่อสารกับเซิร์ฟเวอร์ ESET โดยตรง

นอกจากนี้ ยังสามารถกำหนดการตั้งค่าพร็อกซีเซิร์ฟเวอร์เริ่มต้นได้โดยไปที่ การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์** > **อัพเดท** > **ตัวเลือกการเชื่อมต่อ** แล้วเลือก **การเชื่อมต่อผ่านพร็อกซีเซิร์ฟเวอร์** จากเมนูแบบเลื่อนลงสำหรับ **โหมดพร็อกซี** การกำหนดค่านี้ใช้ได้กับการอัพเดทเท่านั้น และแนะนำสำหรับแล็ปท็อปที่ได้รับการอัพเดทโมดูลจากตำแหน่งระยะไกล อ่านข้อมูลเพิ่มเติมได้ที่ การตั้งค่าการอัพเดทขั้นสูง



ส่วนติดต่อกับผู้ใช้

หากต้องการกำหนดค่าอินเทอร์เฟซผู้ใช้แบบกราฟิก (GUI) ของโปรแกรม ให้เปิด การตั้งค่าขั้นสูง > **อินเทอร์เฟซผู้ใช้**

คุณสามารถปรับรูปลักษณ์และเอฟเฟ็กต์ของโปรแกรมได้ใน องค์ประกอบส่วนติดต่อกับผู้ใช้ ของหน้าจอการตั้งค่าขั้นสูง

เพื่อให้มีการรักษาความปลอดภัยสูงสุดจากซอฟต์แวร์การรักษาความปลอดภัย คุณสามารถป้องกันการถอนการติดตั้งหรือการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตได้โดยปกป้องการตั้งค่าด้วยรหัสผ่านโดยใช้เครื่องมือ ตั้งค่าการเข้าถึง

หากต้องการกำหนดค่าลักษณะการทำงานของการแจ้งเตือนระบบ การเตือนการตรวจหา และสถานะแอพพลิเคชัน ให้ดูที่ส่วน การแจ้งเตือน

โหมดการนำเสนอ จะเป็นประโยชน์สำหรับผู้ที่ต้องการทำงานกับแอพพลิเคชัน ไม่ต้องการถูกรบกวนโดยหน้าต่างป๊อปอัป งานตามกำหนดการ และองค์ประกอบใดๆ ที่ทำให้ตัวประมวลผลและ RAM ทำงานหนักเกินไป

โปรดดู วิธีการย่อส่วนติดต่อกับผู้ใช้ของ ESET Endpoint Security (มีประโยชน์สำหรับสภาพแวดล้อมที่ได้รับการจัด

การ)

องค์ประกอบของส่วนติดต่อผู้ใช้

ตัวเลือกการกำหนดค่าส่วนติดต่อผู้ใช้ใน ESET Endpoint Security จะช่วยให้คุณสามารถปรับระบบการทำงานเพื่อให้เหมาะกับความต้องการของคุณ ตัวเลือกการกำหนดค่าเหล่านี้สามารถเข้าถึงได้ใน **การตั้งค่าขั้นสูง** (F5) > **ส่วนติดต่อผู้ใช้** > **องค์ประกอบของส่วนติดต่อผู้ใช้**

ในส่วน **องค์ประกอบของส่วนติดต่อผู้ใช้** คุณสามารถปรับสภาพแวดล้อมการทำงานได้ ใช้เมนูแบบเลื่อนลง **โหมดเริ่ม** เพื่อเลือกจากโหมดเริ่มส่วนติดต่อผู้ใช้แบบกราฟิก (GUI) ต่อไปนี้:

เต็ม – ระบบจะแสดง GUI ที่สมบูรณ์

อย่างน้อย – ส่วน GUI กำลังทำงาน แต่ผู้ใช้จะเห็นเฉพาะการแจ้งเตือนเท่านั้น

คู่มือ – GUI จะไม่เริ่มโดยอัตโนมัติเมื่อเข้าสู่ระบบ ผู้ใช้ทุกคนสามารถเริ่มต้นด้วยตัวเองได้

เงียบ – จะไม่แสดงการแจ้งเตือนหรือการเตือน GUI สามารถเริ่มต้นโดยผู้ดูแลระบบเท่านั้น โหมดนี้จะมีประโยชน์ในสภาพแวดล้อมที่ได้รับการจัดการหรือในสถานการณ์ที่คุณจำเป็นต้องรักษาทรัพยากรของระบบ

> เมื่อเลือกโหมดเริ่ม GUI ในโหมดอย่างน้อยและคุณได้เริ่มต้นระบบคอมพิวเตอร์ใหม่แล้ว การแจ้งเตือนจะปรากฏขึ้นแต่ส่วนติดต่อกับผู้ใช้แบบกราฟฟิกจะไม่ปรากฏขึ้น หากต้องการแปลงเป็นโหมดส่วนติดต่อผู้ใช้แบบกราฟิกที่สมบูรณ์แบบ ให้เรียกใช้ GUI จากเมนู Start ใต้ **โปรแกรมทั้งหมด** > **ESET** > ESET Endpoint Security ในฐานะผู้ดูแลระบบ หรือคุณสามารถทำขั้นตอนนี้ผ่าน ESET PROTECT โดยใช้นโยบายได้

โหมดสี เลือกโทนสีของ ESET Endpoint Security GUI จากเมนูแบบเลื่อนลง:

- **เหมือนกับสีของระบบ**—โทนสีของ ESET Endpoint Security จะได้รับการตั้งค่าตามการตั้งค่าระบบปฏิบัติการของคุณ
- **มืด** ESET Endpoint Security จะมีโทนสีเข้ม (โหมดมืด)
- **สว่าง** ESET Endpoint Security จะมีโทนสีสว่าง ซึ่งเป็นโทนสีมาตรฐาน

> นอกจากนี้คุณยังสามารถเลือกโทนสีของ ESET Endpoint Security GUI ได้ที่มุมขวาบนของหน้าต่างโปรแกรมหลัก

ถ้าคุณต้องการปิดใช้งานหน้าจอเริ่มต้นของ ESET Endpoint Security ให้ยกเลิกการเลือก **แสดงหน้าจอเริ่มต้น**

เมื่อต้องการให้ ESET Endpoint Security เล่นเสียงเมื่อมีเหตุการณ์สำคัญเกิดขึ้นระหว่างสแกน ตัวอย่างเช่น เมื่อค้นพบภัยคุกคามหรือเมื่อสแกนเสร็จสมบูรณ์ ให้เลือก **ใช้สัญญาณเสียง**

รวมเข้ากับเมนูบริบท – รวมองค์ประกอบการควบคุม ESET Endpoint Security ไว้ในเมนูบริบท

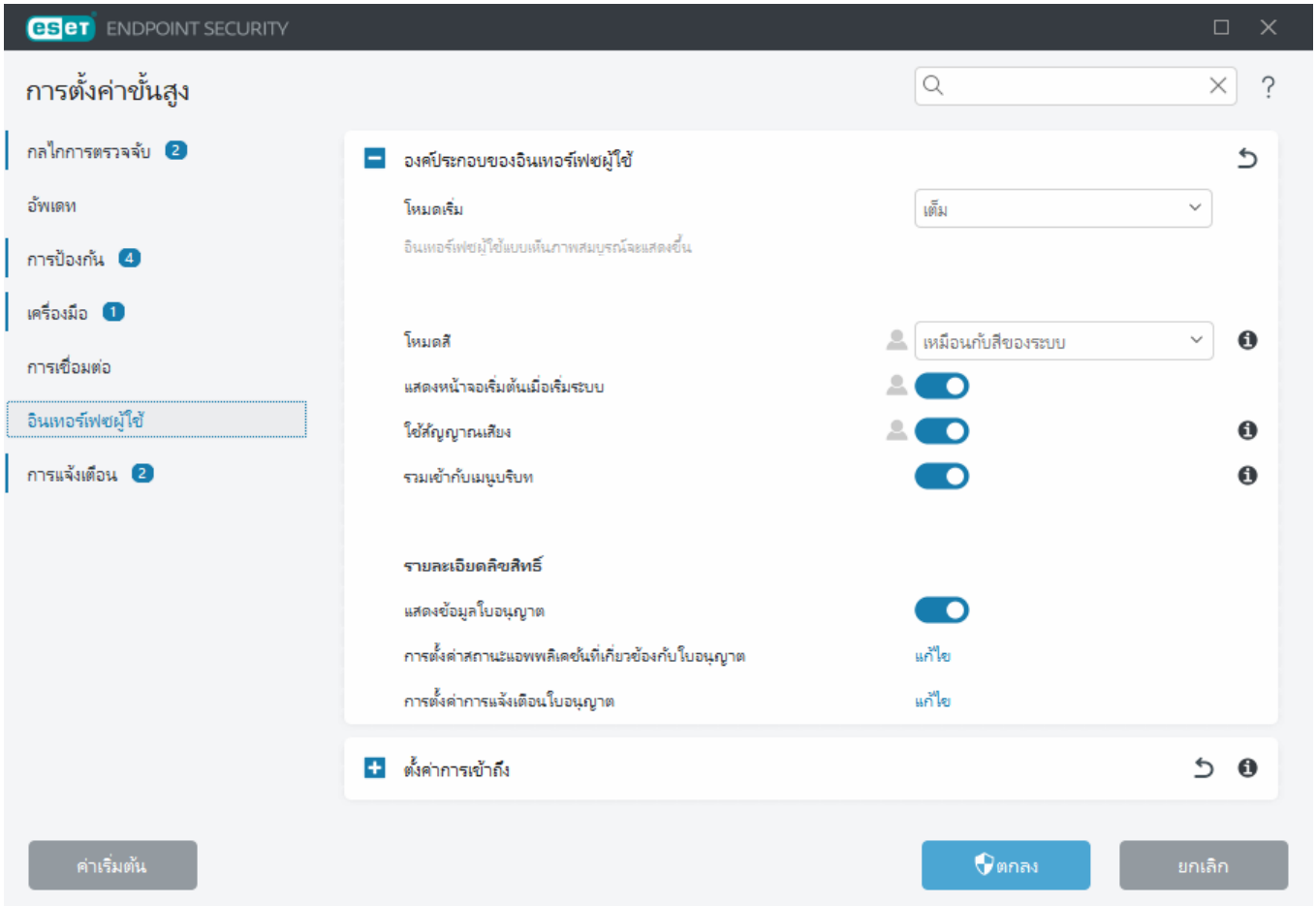
รายละเอียดลิขสิทธิ์

แสดงข้อมูลใบอนุญาต – เมื่อปิดใช้งานอยู่ จะไม่แสดงหน้าจอใบอนุญาตหมดอายุใน **สถานะของการป้องกัน** และ **วิธีใช้และการสนับสนุน**

การตั้งค่าสถานะแอพพลิเคชันที่เกี่ยวข้องกับใบอนุญาต–เปิดรายการสถานะแอพพลิเคชันที่เกี่ยวข้องกับใบอนุญาต

กำหนดค่าการแจ้งเตือนใบอนุญาต – เปิดรายการการแจ้งเตือนที่เกี่ยวข้องกับใบอนุญาต

การตั้งค่าข้อมูลใบอนุญาตจะถูกปรับใช้แต่จะไม่สามารถเข้าถึงได้สำหรับ ESET Endpoint Security ที่เปิดใช้งานด้วยใบอนุญาต MSP



ตั้งค่าการเข้าถึง

การตั้งค่า ESET Endpoint Security เป็นส่วนสำคัญของนโยบายรักษาความปลอดภัย การแก้ไขโดยไม่ได้รับอนุญาตอาจเป็นอันตรายต่อเสถียรภาพและการป้องกันระบบของคุณ เมื่อต้องการหลีกเลี่ยงการแก้ไขที่ไม่ได้รับอนุญาต คุณสามารถป้องกันพารามิเตอร์การตั้งค่าและการลบการติดตั้ง ESET Endpoint Security ด้วยรหัสผ่านได้ สามารถกำหนดการตั้งค่าการเข้าถึงได้ใน การตั้งค่าขั้นสูง > **อินเทอร์เฟซผู้ใช้** > **การตั้งค่าการเข้าถึง**

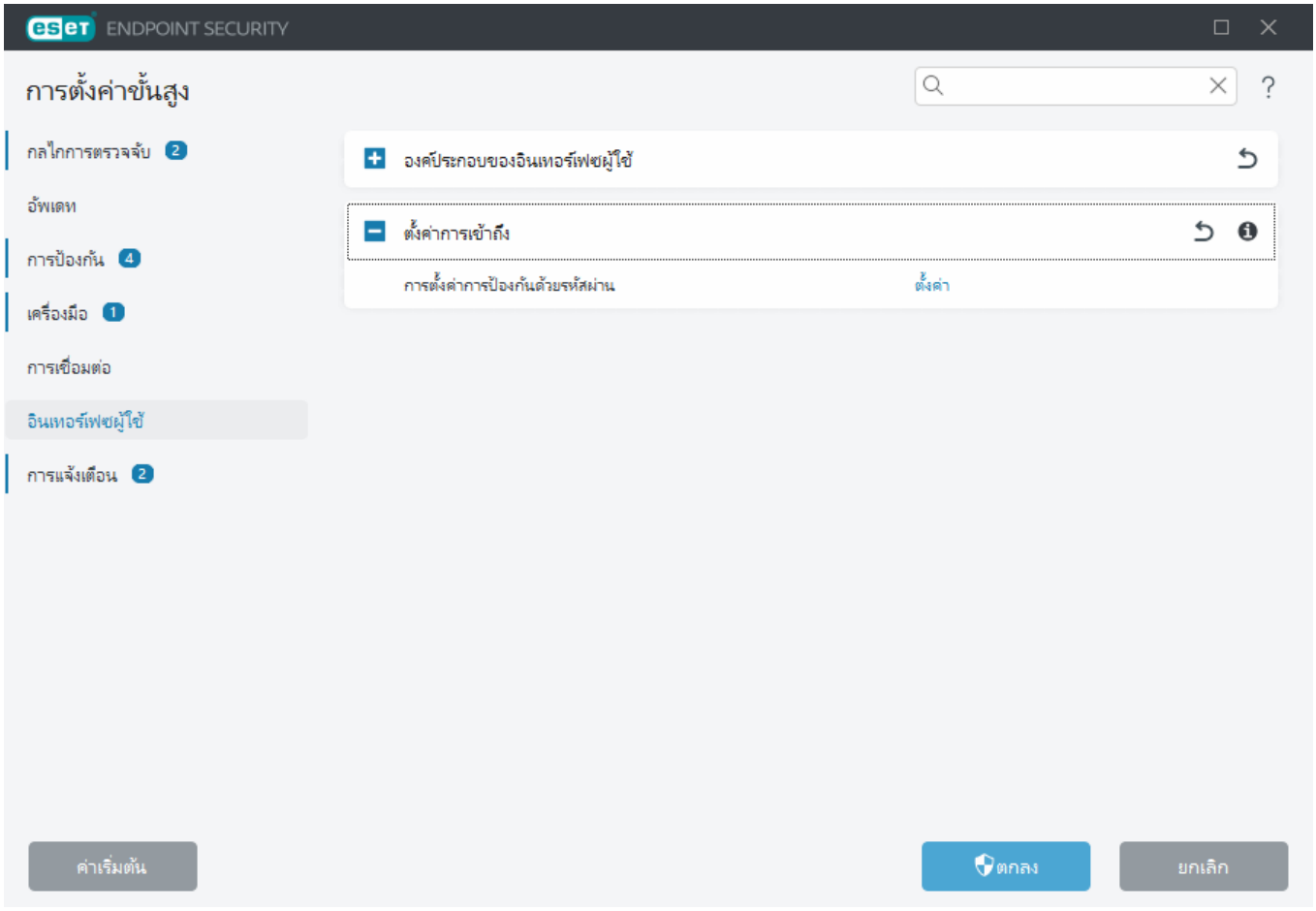
หากต้องการตั้งรหัสผ่านเพื่อป้องกันพารามิเตอร์การตั้งค่าและการลบการติดตั้ง ESET Endpoint Security ให้คลิก **ตั้งค่า** ถัดจาก **การตั้งค่าการป้องกันด้วยรหัสผ่าน**

หากต้องการเปลี่ยนรหัสผ่าน ให้คลิก **เปลี่ยนรหัสผ่าน** ถัดจาก **การตั้งค่าการป้องกันด้วยรหัสผ่าน**

หากต้องการลบรหัสผ่าน ให้คลิก **ลบออก** ถัดจาก **การตั้งค่าการป้องกันด้วยรหัสผ่าน**

สภาพแวดล้อมที่ได้รับการจัดการ

ผู้ดูแลระบบสามารถสร้างนโยบายเพื่อใช้รหัสผ่านป้องกันการตั้งค่าสำหรับ ESET Endpoint Security บนคอมพิวเตอร์ไคลเอ็นต์ที่เชื่อมต่อได้ หากต้องการสร้างนโยบายใหม่ ดูที่การตั้งค่าที่ป้องกันด้วยรหัสผ่าน



รหัสผ่านสำหรับการตั้งค่าขั้นสูง

ในการปกป้องการตั้งค่า ESET Endpoint Security ขั้นสูงและเพื่อหลีกเลี่ยงการแก้ไขโดยไม่ได้รับอนุญาต ให้พิมพ์รหัสผ่านใหม่ของคุณในช่อง **รหัสผ่านใหม่** และช่อง **ยืนยันรหัสผ่าน** คลิก**ตกลง**

สภาพแวดล้อมที่ได้รับการจัดการ

ผู้ดูแลระบบสามารถสร้างนโยบายเพื่อใช้รหัสผ่านป้องกันการตั้งค่าสำหรับ ESET Endpoint Security บนคอมพิวเตอร์ไคลเอ็นต์ที่เชื่อมต่อได้ หากต้องการสร้างนโยบายใหม่ ดูที่การตั้งค่าที่ป้องกันด้วยรหัสผ่าน

ไม่ได้รับการจัดการ

เมื่อคุณต้องการเปลี่ยนแปลงรหัสผ่านที่มีอยู่แล้ว:

1. พิมพ์รหัสผ่านเดิมของคุณในช่อง **รหัสผ่านเดิม**
2. ป้อนรหัสผ่านใหม่ของคุณในช่อง **รหัสผ่านใหม่** และ **ยืนยันรหัสผ่าน**
3. คลิก**ตกลง**

รหัสผ่านนี้จำเป็นต้องใช้ในการแก้ไขใดๆ ในอนาคตสำหรับ ESET Endpoint Security

หากคุณลืมรหัสผ่าน โปรดดู ปลดล็อครหัสผ่านการตั้งค่าของคุณในผลิตภัณฑ์เอ็นพอยต์ ESET

ในการกู้คืนรหัสใบอนุญาต ESET ที่สูญหาย, วันหมดอายุของใบอนุญาตของคุณ หรือข้อมูลใบอนุญาตอื่นๆ สำหรับ ESET Endpoint Security โปรดดู ฉันทำชื่อผู้ใช้ และรหัสผ่าน / รหัสใบอนุญาตของฉันหาย

รหัสผ่าน

เมื่อต้องการหลีกเลี่ยงการแก้ไขที่ไม่ได้รับอนุญาต คุณสามารถป้องกันพารามิเตอร์การตั้งค่าของ ESET Endpoint Security ด้วยรหัสผ่าน

โหมดปลอดภัย

หากส่วนติดต่อแบบกราฟิกของ ESET Endpoint Security ถูกเปิดในโหมดปลอดภัย หน้าต่างข้อความจะปรากฏขึ้นเพื่อแจ้งว่าแอพพลิเคชันจะทำงานในโหมดปลอดภัย เนื่องจากอยู่ในโหมดปลอดภัย การทำงานของโปรแกรมทั้งหมดจะจำกัด ดังนั้นจึงไม่สามารถเปิดส่วนติดต่อแบบกราฟิกของ ESET Endpoint Security ได้เหมือนในโหมดมาตรฐาน

หน้าต่างที่แสดงจะช่วยให้คุณเรียกใช้การสแกนคอมพิวเตอร์ได้ หากคุณต้องการตรวจสอบหารหัสที่เป็นอันตรายในคอมพิวเตอร์ ให้เลือกตัวเลือก **ใช่**

การเลือกดังกล่าวจะเปิดใช้การสแกนในหน้าต่างที่แยกต่างหาก โดยใช้พารามิเตอร์เดียวกับโปรไฟล์การสแกนคอมพิวเตอร์ที่เป็นค่าเริ่มต้น หลังการติดตั้ง ESET Endpoint Security

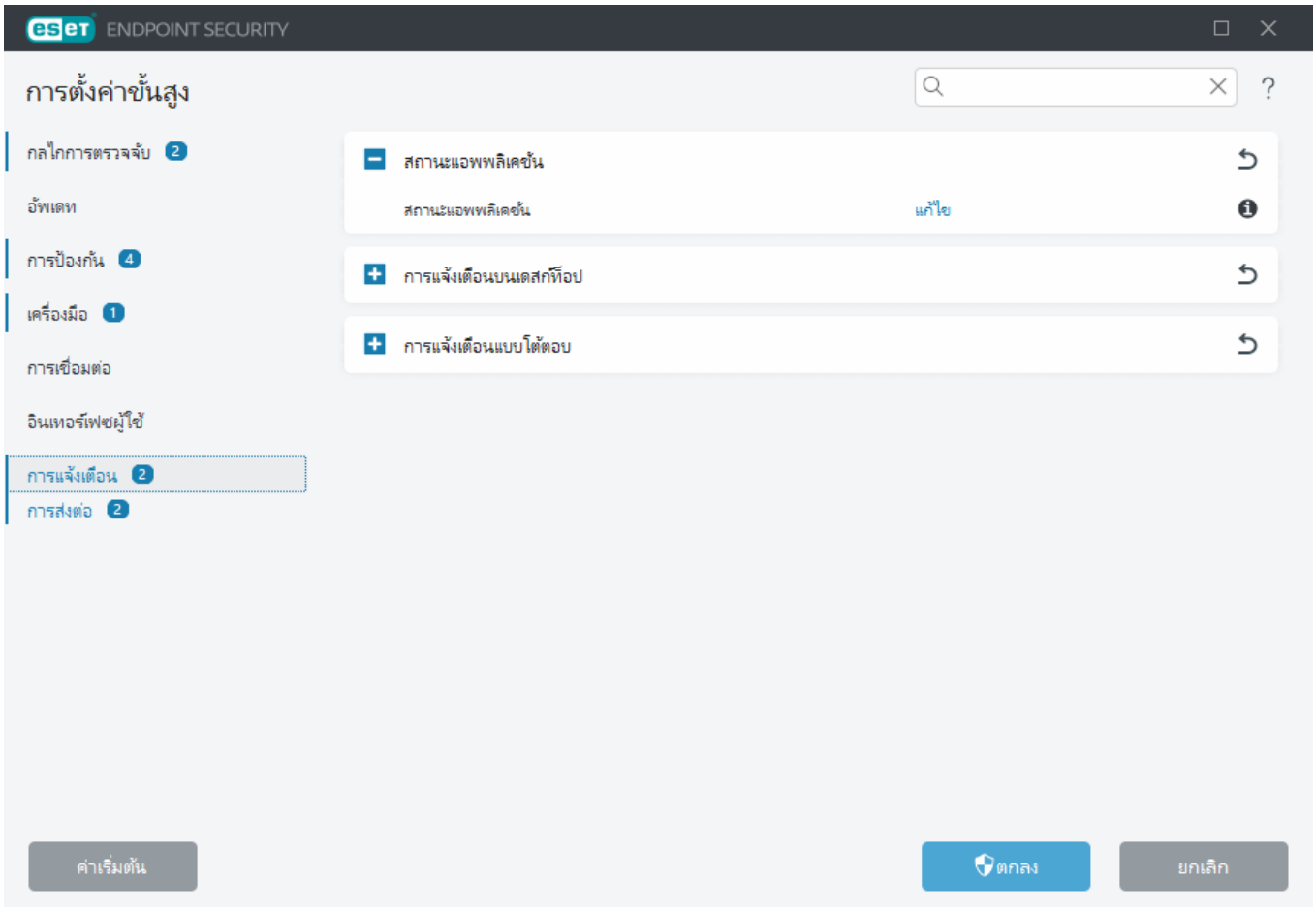
เลือกตัวเลือก **ไม่** เพื่อปิดหน้าต่างข้อความ ESET Endpoint Security จะไม่ทำงาน

การแจ้งเตือน

ในการจัดการการแจ้งเตือนใน ESET Endpoint Security ให้เปิด การตั้งค่าขั้นสูง > **การแจ้งเตือน** คุณสามารถกำหนดค่าการแจ้งเตือนประเภทต่อไปนี้ได้:

- สถานะแอพพลิเคชัน – การแจ้งเตือนที่แสดงในส่วนหน้าแรกของหน้าต่างโปรแกรมหลัก
- การแจ้งเตือนบนเดสก์ท็อป – การแจ้งเตือนขนาดเล็กถัดจากแถบงานของระบบ
- การแจ้งเตือนแบบโต้ตอบ – หน้าต่างการเตือนและกล่องข้อความที่ต้องการการโต้ตอบของผู้ใช้

- การส่งต่อ การแจ้งเตือนทางอีเมล – การแจ้งเตือนทางอีเมลจะถูกส่งไปยังที่อยู่อีเมลที่ระบุ
- การปรับแต่งของการแจ้งเตือน – เพิ่มข้อความที่กำหนดเองไปยัง เช่น การแจ้งเตือนบนเดสก์ท็อป



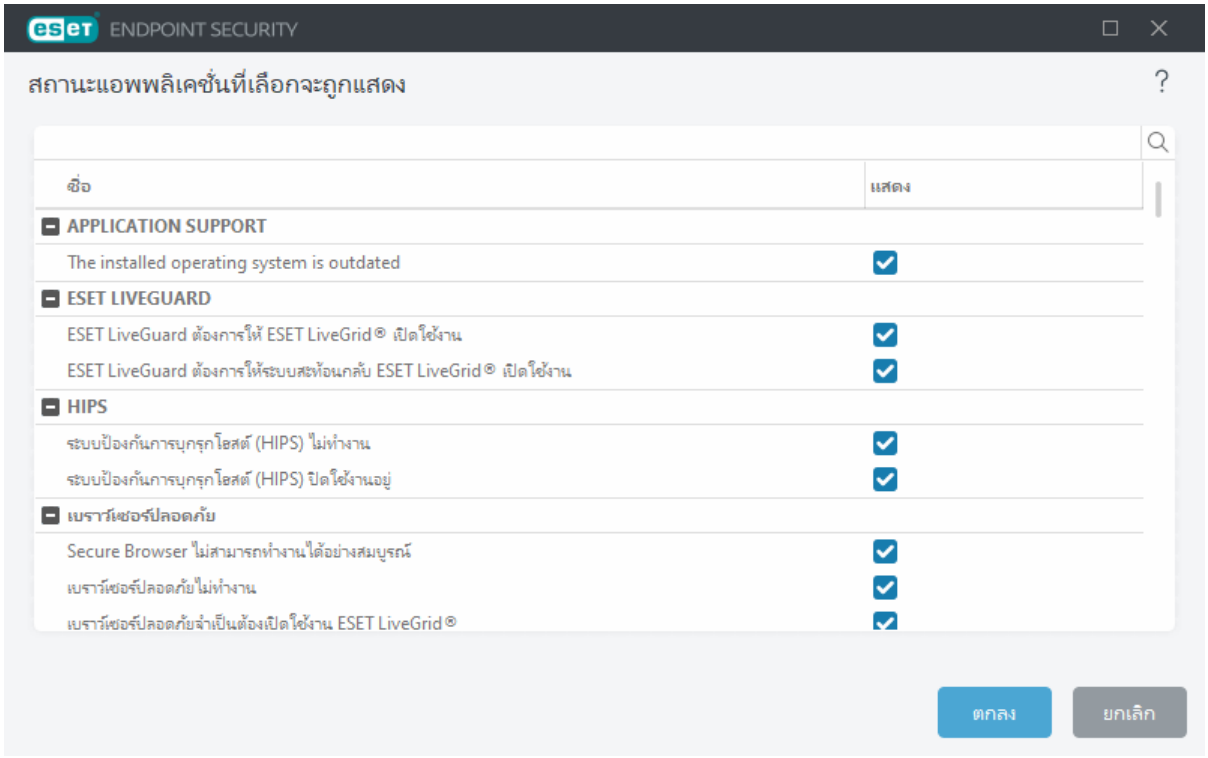
สถานะแอพพลิเคชัน

สถานะแอพพลิเคชัน – คลิก **แก้ไข** เพื่อเลือกสถานะแอพพลิเคชันที่จะแสดงในส่วนหน้าแรกของหน้าต่างโปรแกรมหลัก

สถานะแอพพลิเคชัน

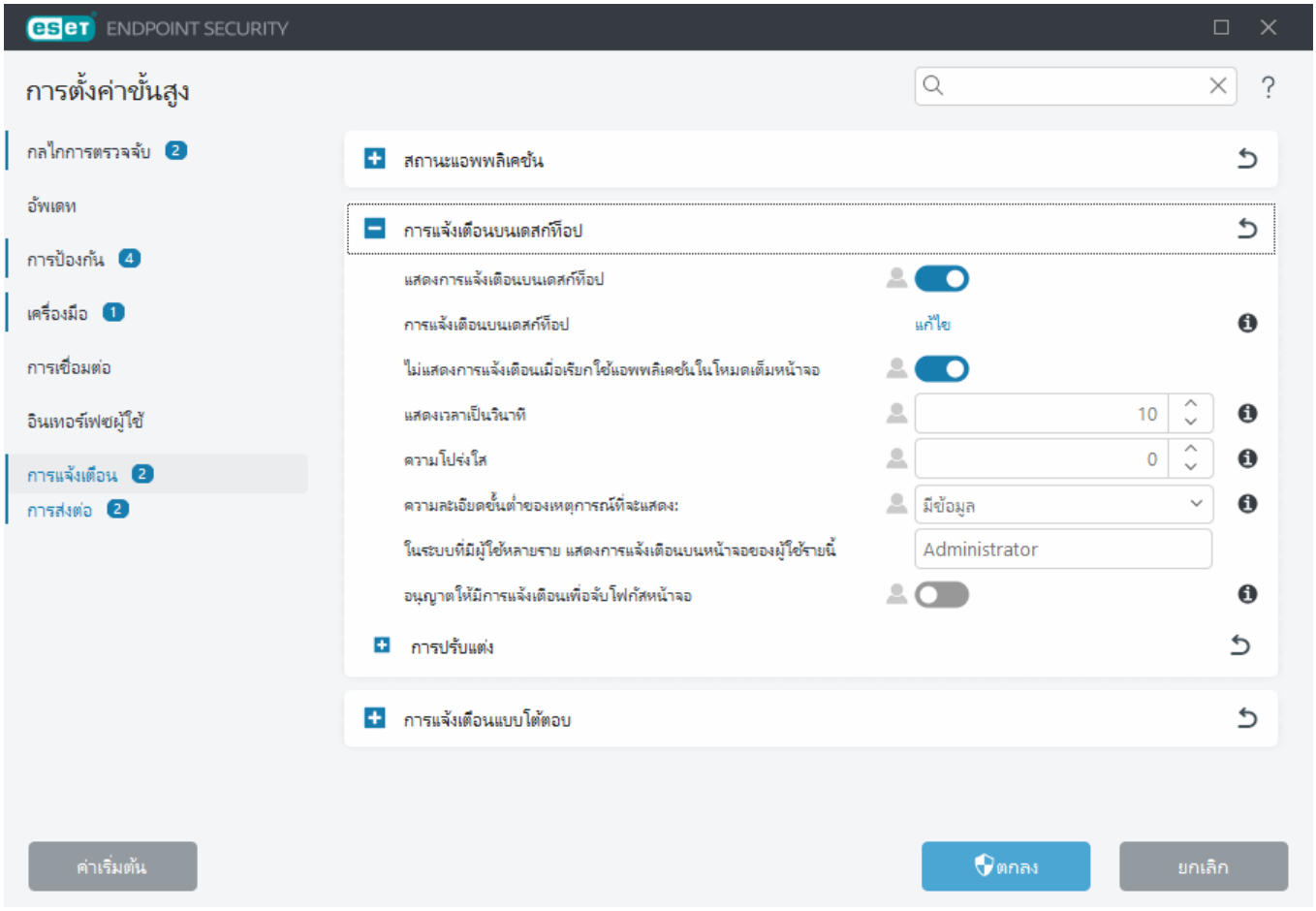
ในการกำหนดค่าสถานะแอพพลิเคชันที่จะแสดง (ตัวอย่างเช่น เมื่อคุณหยุดการป้องกันไวรัสและสปายแวร์ชั่วคราว หรือเปิดใช้งานโหมดการนำเสนอ) ให้เปิด การตั้งค่าขั้นสูง > **การแจ้งเตือน** แล้วคลิก **แก้ไข** ที่อยู่ถัดจาก **สถานะแอพพลิเคชัน**

สถานะแอพพลิเคชันจะแสดงขึ้นเช่นกันหากผลิตภัณฑ์ของคุณไม่ได้เปิดใช้งานหรือใบอนุญาตของคุณหมดอายุ การตั้งค่านี้สามารถเปลี่ยนแปลงได้ผ่านนโยบาย ESET PROTECT



การแจ้งเตือนบนเดสก์ท็อป

การแจ้งเตือนบนเดสก์ท็อปจะแสดงด้วยหน้าต่างการแจ้งเตือนขนาดเล็กซึ่งอยู่ถัดจากแถบงานระบบ ซึ่งถูกตั้งค่าให้แสดงเป็นเวลา 10 วินาทีโดยค่าเริ่มต้น ก่อนจะค่อยๆ หายไปอย่างช้าๆ นี่คือวิธีหลักที่ ESET Endpoint Security ใช้สื่อสารกับผู้ใช้ เพื่อแจ้งเตือนเกี่ยวกับการอัพเดทผลิตภัณฑ์ที่เสร็จสิ้น อุปกรณ์ใหม่ที่เชื่อมต่อ งานด้านการสแกนไวรัสที่เสร็จสมบูรณ์หรือการค้นพบภัยคุกคามใหม่



แสดงการแจ้งเตือนบนเดสก์ท็อป – เราขอแนะนำให้เปิดใช้งานตัวเลือกนี้เพื่อให้ผลิตภัณฑ์สามารถแจ้งให้คุณทราบเมื่อมีเหตุการณ์ใหม่เกิดขึ้น

การแจ้งเตือนบนเดสก์ท็อป – คลิก **แก้ไข** เพื่อเปิดใช้งานหรือปิดใช้งาน การแจ้งเตือนบนเดสก์ท็อป ที่ต้องการ

อย่าแสดงการแจ้งเตือนเมื่อเรียกใช้แอพพลิเคชันในโหมดเต็มหน้าจอ – ระงับการแจ้งเตือนที่ไม่โต้ตอบทั้งหมดเมื่อเรียกใช้แอพพลิเคชันในโหมดเต็มหน้าจอ

หมดเวลาเป็นวินาที – ตั้งค่าระยะเวลาที่สามารถมองเห็นการแจ้งเตือนได้ โดยค่านี้จะต้องอยู่ระหว่าง 3-30 วินาที

ความโปร่งใส – ตั้งค่าเปอร์เซ็นต์ความโปร่งใสของการแจ้งเตือน ค่านี้จะรองรับช่วงตั้งแต่ 0 (ไม่โปร่งใส) ไปจนถึง 80 (ความโปร่งใสสูงมาก)

ความละเอียดขั้นต่ำของเหตุการณ์ที่จะแสดง – ตั้งค่าระดับความรุนแรงเริ่มต้นของการแจ้งเตือนที่จะแสดง จากเมนูแบบเลื่อนลง ให้เลือกตัวเลือกต่อไปนี้:

- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- **มีข้อมูล** – บันทึกข้อความแจ้งข้อมูล เช่น กิจกรรมเครือข่ายที่ไม่ได้มาตรฐาน รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น

- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน (เช่น อัพเดทไม่สำเร็จ)
- **ข้อผิดพลาด** – ข้อผิดพลาด (ไม่ได้เริ่มต้นการป้องกันเอกสาร) และข้อผิดพลาดร้ายแรงจะถูกบันทึก
- **ร้ายแรง** – บันทึกเฉพาะข้อผิดพลาดร้ายแรงเมื่อเริ่มต้นการป้องกันไวรัสหรือระบบที่ติดไวรัส

ในระบบที่มีผู้ใช้หลายราย แสดงการแจ้งเตือนบนหน้าจอของผู้ใช้รายนี้ – อนุญาตให้บัญชีที่เลือกสามารถรับการแจ้งเตือนบนเดสก์ท็อปได้ ตัวอย่างเช่น หากคุณไม่ได้ใช้บัญชีผู้ดูแลระบบ ให้พิมพ์ชื่อเต็มของบัญชี จากนั้นระบบจะแสดงการแจ้งเตือนบนเดสก์ท็อปสำหรับบัญชีที่ระบุ โดยจะมีเพียงบัญชีเดียวเท่านั้นที่สามารถรับการแจ้งเตือนบนเดสก์ท็อปได้

อนุญาตให้การแจ้งเตือนจับโฟกัสหน้าจอ – การแจ้งเตือนจะจับโฟกัสหน้าจอและจะสามารถเข้าถึงได้โดย Alt+Tab

การปรับแต่งการแจ้งเตือน

ในหน้าต่างนี้ คุณสามารถปรับแต่งการส่งข้อความที่ใช้ในการแจ้งเตือน

ข้อความแจ้งเตือนตามค่าเริ่มต้น – ข้อความตามค่าเริ่มต้นที่จะแสดงตรงส่วนท้ายของการแจ้งเตือน

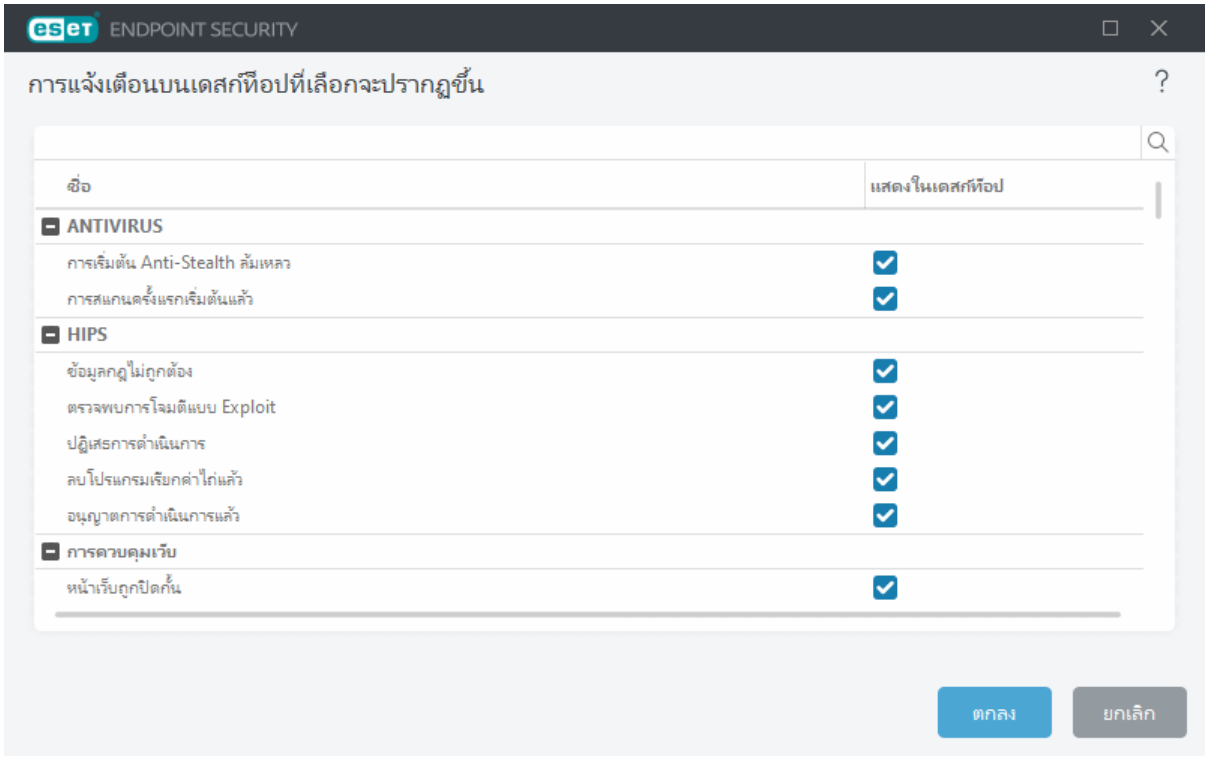
การตรวจหา

เปิดใช้งาน **อย่าปิดการแจ้งเตือนมัลแวร์โดยอัตโนมัติ** เพื่อให้การแจ้งเตือนมัลแวร์ยังคงอยู่บนหน้าจอ จนกว่าคุณจะปิดการแจ้งเตือนเหล่านี้ด้วยตนเอง

ปิดใช้งาน **ใช้ข้อความตามค่าเริ่มต้น** และป้อนข้อความของคุณเองในช่อง **ข้อความแจ้งเตือนการตรวจหา** เพื่อใช้การส่งข้อความการแจ้งเตือนที่ปรับแต่งเอง

หน้าต่างข้อความ – การแจ้งเตือนบนเดสก์ท็อป

หากต้องการปรับการมองเห็นการแจ้งเตือนบนเดสก์ท็อป (แสดงอยู่ที่ด้านล่างขวาของหน้าจอ) ให้เปิด การตั้งค่าขั้นสูง > **การแจ้งเตือน** > **การแจ้งเตือนบนเดสก์ท็อป** คลิก **แก้ไข** ถัดจาก **การแจ้งเตือนบนเดสก์ท็อป** แล้วเลือกช่องทำเครื่องหมาย **แสดงบนเดสก์ท็อป** ที่เหมาะสม



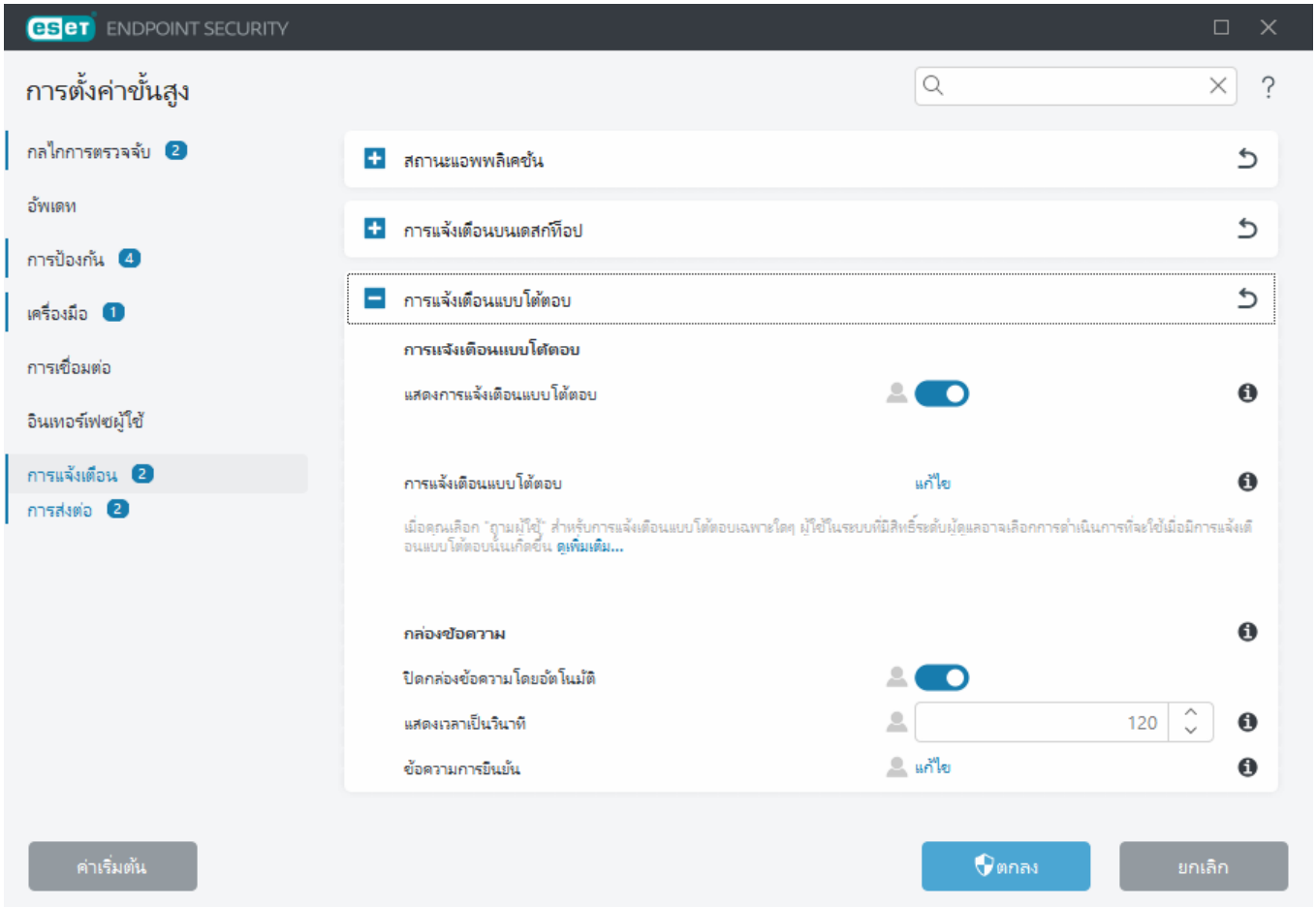
หากคุณต้องการตั้งค่าการแจ้งเตือนว่า**วิเคราะห์ไฟล์แล้ว** และ **ยังไม่ได้วิเคราะห์ไฟล์** ระหว่างใช้ ESET LiveGuard การป้องกันเชิงรุกจะต้องตั้งค่าเป็น **บล็อกการเรียกใช้จนกว่าจะได้รับผลการวิเคราะห์**

การแจ้งเตือนแบบโต้ตอบ

มองหาข้อมูลเกี่ยวกับการเตือนและการแจ้งเตือนทั่วไปอยู่ใช่ไหม

- พบภัยคุกคาม
- ที่อยู่ถูกปิดกั้นแล้ว
- ยังไม่ได้เปิดใช้งานผลิตภัณฑ์
- มีรายการอัปเดตให้ใช้งานได้
- ข้อมูลการอัพเดทไม่ตรงกัน
- การแก้ไขปัญหาสำหรับข้อความ "อัพเดทโมดูลไม่สำเร็จ"
- 'ไฟล์เสียหาย' หรือ 'ไม่สามารถเปลี่ยนชื่อไฟล์ได้'
- ใบรับรองเว็บไซต์ที่ยกเลิก
- ปิดกั้นภัยคุกคามเครือข่ายแล้ว
- ไฟล์ถูกปิดกั้นเนื่องจากการวิเคราะห์

ส่วน **การแจ้งเตือนแบบโต้ตอบ** ใน การตั้งค่าขั้นสูง > **การแจ้งเตือน** ช่วยให้คุณสามารถกำหนดค่าวิธีการที่กล่องข้อความและการแจ้งเตือนแบบโต้ตอบสำหรับการตรวจจับ ซึ่งจำเป็นต้องมีการตัดสินใจโดยผู้ใช้ (ตัวอย่างเช่น เว็บไซต์ที่อาจเป็นการฟิชชิ่ง) จะได้รับการจัดการโดย ESET Endpoint Security



การแจ้งเตือนแบบโต้ตอบ

การปิดใช้งาน **แสดงการแจ้งเตือนแบบโต้ตอบ** จะซ่อนหน้าต่างการเตือนและข้อความในเบราว์เซอร์ทั้งหมด และจะเหมาะสำหรับสถานการณ์เฉพาะที่มีจำนวนจำกัดเท่านั้น

- สำหรับผู้ใช้ที่ไม่ได้รับการจัดการ เราแนะนำว่าให้ทิ้งตัวเลือกนี้ไว้ตามการตั้งค่าเริ่มต้น (เปิดใช้งาน)
- สำหรับผู้ใช้ที่ได้รับการจัดการ สามารถเปิดใช้งานการตั้งค่านี้ไว้และเลือกการกระทำที่กำหนดไว้ล่วงหน้าสำหรับผู้ใช้ในรายการการแจ้งเตือนแบบโต้ตอบได้

การแจ้งเตือนแบบโต้ตอบ–คลิก **แก้ไข** เพื่อเลือกว่า การแจ้งเตือนแบบโต้ตอบ ใดที่จะแสดง

กล่องข้อความ

หากต้องการปิดกล่องข้อความโดยอัตโนมัติหลังจากปรากฏมาเป็นระยะเวลาหนึ่ง ให้เลือก **ปิดกล่องข้อความโดยอัตโนมัติ** หากไม่ปิดหน้าต่างดังกล่าวด้วยตนเอง หน้าต่างการเตือนจะปิดโดยอัตโนมัติหลังจากหมดเวลาตามที่กำหนด

หมดเวลาเป็นวินาที – ตั้งค่าระยะเวลาที่สามารถมองเห็นการเตือนได้ โดยค่านี้จะต้องอยู่ระหว่าง 10-999 วินาที

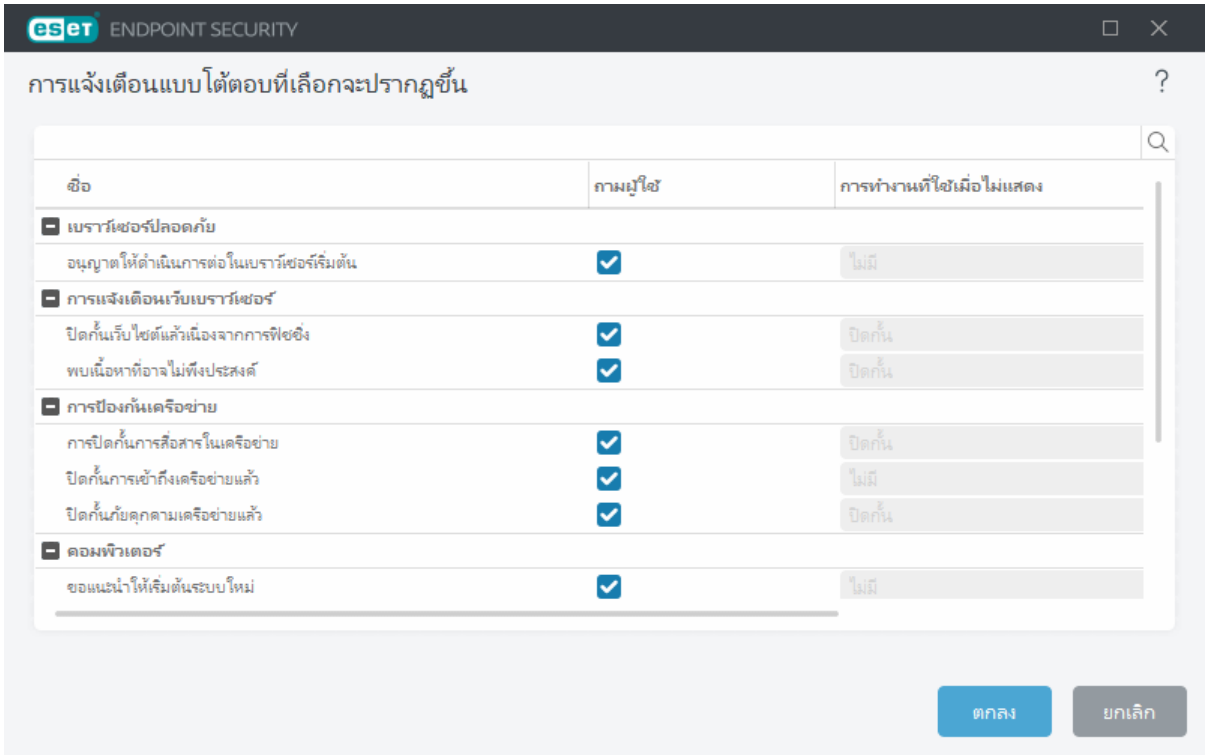
ข้อความการยืนยัน – คลิก **แก้ไข** เพื่อแสดง รายการของข้อความการยืนยัน ซึ่งคุณสามารถเลือกให้แสดงหรือไม่แสดงก็ได้

รายการการแจ้งเตือนแบบโต้ตอบ

ส่วนนี้จะสรุปหน้าต่างการเตือนแบบโต้ตอบบางหน้าต่างที่ ESET Endpoint Security จะแสดงก่อนที่จะทำการกระทำใดๆ

หากต้องการปรับพฤติกรรมสำหรับการแจ้งเตือนแบบโต้ตอบที่กำหนดค่าได้ ให้เปิด การตั้งค่าขั้นสูง > **การแจ้งเตือน** > **การแจ้งเตือนแบบโต้ตอบ** และคลิก **แก้ไข** ถัดจาก **การแจ้งเตือนแบบโต้ตอบ**

มีประโยชน์สำหรับสภาพแวดล้อมที่ได้รับการจัดการที่ผู้ดูแลระบบสามารถยกเลิกการเลือก **ถามผู้ใช้** ได้ทุกที่ และเลือกการกระทำที่กำหนดไว้ล่วงหน้าที่ใช้เมื่อมีหน้าต่างการเตือนแบบโต้ตอบแสดงอยู่



ตรวจสอบส่วนวิธีใช้อื่นสำหรับการอ้างอิงถึงหน้าต่างการเตือนแบบโต้ตอบเฉพาะ:

สื่อที่ถอดเข้าออกได้

- ตรวจพบอุปกรณ์ใหม่

เบราว์เซอร์ที่ปลอดภัย

- อนุญาตให้ดำเนินการต่อในเบราว์เซอร์เริ่มต้น

การป้องกันเครือข่าย

- การเข้าถึงเครือข่ายถูกปิดกั้น จะแสดงขึ้นเมื่องาน **แยกคอมพิวเตอร์ออกจากเครือข่าย** ของลูกค้าในเวิร์กสเตชันจาก ESET PROTECT ถูกเรียกใช้
- การปิดกั้นการสื่อสารในเครือข่าย
- ปิดกั้นภัยคุกคามเครือข่ายแล้ว

การแจ้งเตือนเว็บเบราว์เซอร์

- พบเนื้อหาที่อาจไม่พึงประสงค์
- ปิดกั้นเว็บไซต์แล้วเนื่องจากการฟิชชิ่ง

คอมพิวเตอร์

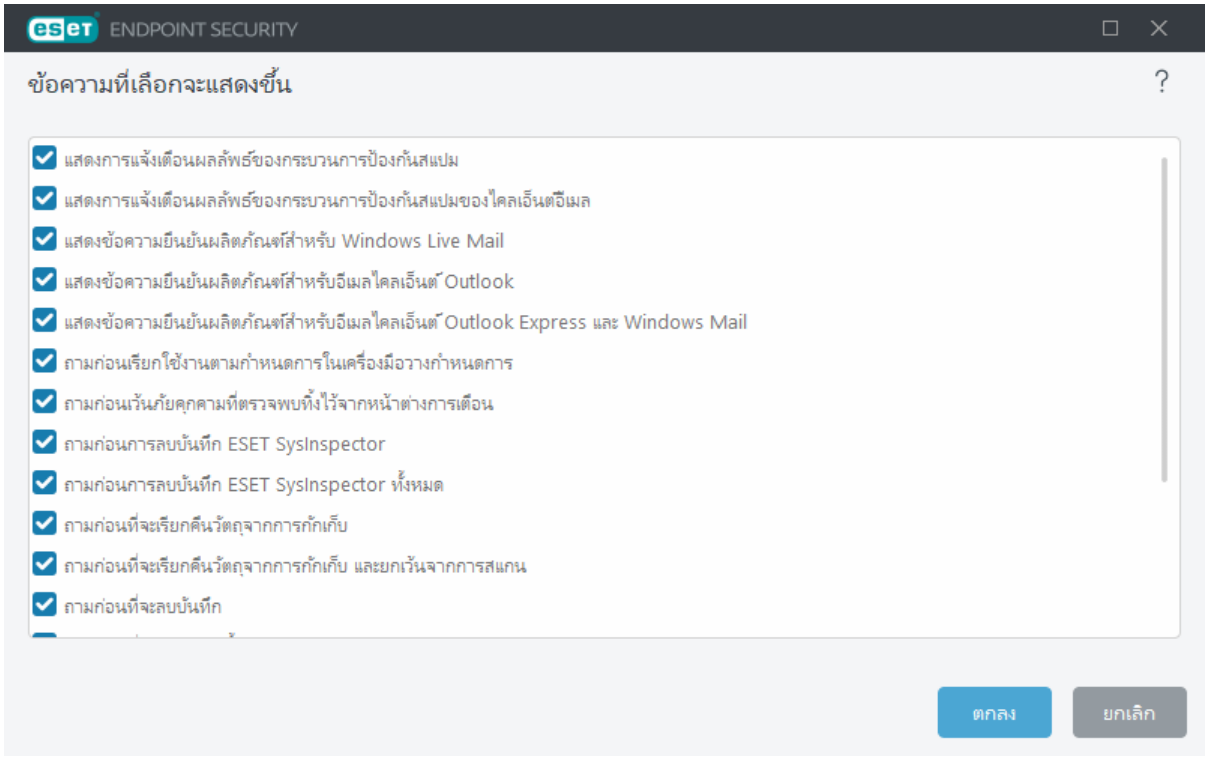
การแสดงผลการแจ้งเตือนเหล่านี้จะเปลี่ยนสีส่วนติดต่อกับผู้ใช้:

- เริ่มต้นคอมพิวเตอร์ใหม่ (จำเป็น)
- เริ่มต้นคอมพิวเตอร์ใหม่ (แนะนำ)

> การแจ้งเตือนแบบโต้ตอบไม่มีกลไกการตรวจจับ HIPS หรือหน้าต่างไฟร์วอลล์แบบโต้ตอบ เนื่องจากพฤติกรรมเหล่านี้สามารถกำหนดค่าแยกกันในคุณสมบัติที่เฉพาะเจาะจงได้

ข้อความการยืนยัน

ในการปรับข้อความการยืนยัน ให้ไปที่ การตั้งค่าขั้นสูง > **การแจ้งเตือน** > **การแจ้งเตือนแบบโต้ตอบ** และคลิก **แก้ไข** ถัดจาก **ข้อความการยืนยัน**



หน้าต่างข้อความนี้แสดงข้อความการยืนยันที่ ESET Endpoint Security จะแสดงขึ้นมาก่อนที่จะดำเนินการทำงานใดๆ เลือกหรือยกเลิกการเลือกกล่องทำเครื่องหมายที่อยู่ถัดจากแต่ละข้อความการยืนยันเพื่ออนุญาตหรือปิดใช้งานข้อความเหล่านั้น

เรียนรู้เพิ่มเติมเกี่ยวกับคุณลักษณะเฉพาะที่เกี่ยวข้องกับข้อความการยืนยัน:

- ถามก่อนที่จะลบบันทึก ESET SysInspector
- ถามก่อนที่จะลบบันทึก ESET SysInspector ทั้งหมด
- ถามก่อนที่จะลบวัตถุจากการกักเก็บ
- ถามก่อนที่จะละทิ้งการตั้งค่าในการตั้งค่าขั้นสูง
- ถามก่อนเว้นภัยคุกคามที่ตรวจพบทิ้งไว้จากหน้าต่างการเตือน
- ถามก่อนที่จะลบบันทึก
- ถามก่อนลบงานตามกำหนดการในเครื่องมือวางกำหนดการ
- ถามก่อนที่จะลบบันทึกทั้งหมด
- ถามก่อนรีเซ็ตสถิติ
- ถามก่อนที่จะเรียกคืนวัตถุจากการกักเก็บ
- ถามก่อนที่จะเรียกคืนวัตถุจากการกักเก็บ และยกเว้นจากการสแกน
- ถามก่อนเรียกใช้งานตามกำหนดการในเครื่องมือวางกำหนดการ
- แสดงการแจ้งเตือนผลลัพธ์ของกระบวนการป้องกันสแปม
- แสดงการแจ้งเตือนผลลัพธ์ของกระบวนการป้องกันสแปมของไคลเอ็นต์อีเมล

- แสดงข้อความยืนยันผลิตภัณฑ์สำหรับอีเมลไคลเอ็นต์ Outlook Express และ Windows Mail
- แสดงข้อความยืนยันผลิตภัณฑ์สำหรับ Windows Live Mail
- แสดงข้อความยืนยันผลิตภัณฑ์สำหรับอีเมลไคลเอ็นต์ Outlook

ข้อผิดพลาดของข้อขัดแย้งในการตั้งค่าขั้นสูง

ข้อผิดพลาดนี้อาจเกิดขึ้นหากองค์ประกอบบางอย่าง (เช่น HIPS หรือไฟร์วอลล์) และผู้ใช้สร้างกฎในโหมดโต้ตอบหรือโหมดการเรียนรู้พร้อมกัน

เราแนะนำให้ผู้ใช้เปลี่ยนโหมดการกรองเป็น **โหมดอัตโนมัติ** ตามค่าเริ่มต้นถ้าคุณต้องการสร้างกฎของคุณเอง อ่านเพิ่มเติมเกี่ยวกับ โหมดการเรียนรู้ ESET Firewall อ่านเพิ่มเติมเกี่ยวกับ โหมดการกรอง HIPS และ HIPS

อนุญาตให้ดำเนินการต่อในเบราว์เซอร์เริ่มต้น

การแจ้งเตือนแบบโต้ตอบเฉพาะจะแสดงเมื่อมีข้อผิดพลาดในการเริ่มต้นเบราว์เซอร์ปลอดภัยอย่างถูกต้องเท่านั้น

ต้องเริ่มต้นระบบใหม่

จำเป็นต้องรีสตาร์ทคอมพิวเตอร์หลังจากอัพเกรด ESET Endpoint Security เป็นเวอร์ชันใหม่ หรือใช้แพทช์กับแอพพลิเคชันผ่าน การจัดการจุดอ่อนและแพทช์ ESET Endpoint Security เวอร์ชันใหม่ได้ออกมาเพื่อปรับปรุงประสิทธิภาพหรือแก้ไขปัญหาที่การอัพเดทอัตโนมัติของโมดูลโปรแกรมไม่สามารถแก้ไขได้

คลิก **รีสตาร์ททันที** เพื่อรีสตาร์ทคอมพิวเตอร์ของคุณ หากคุณวางแผนจะรีสตาร์ทคอมพิวเตอร์ของคุณในภายหลัง ให้คลิก **เตือนฉันในภายหลัง** คุณสามารถรีสตาร์ทคอมพิวเตอร์ด้วยตนเองในภายหลังได้จากส่วน**สถานะการป้องกัน**ในหน้าต่างโปรแกรมหลัก

ในการปิดใช้งานการเตือน "ต้องเริ่มต้นระบบใหม่" หรือ "ขอแนะนำให้เริ่มต้นระบบใหม่" โปรดทำตามขั้นตอนด้านล่างนี้:

1. เปิด **การตั้งค่าขั้นสูง** (F5) > **การแจ้งเตือน** > **การแจ้งเตือนแบบโต้ตอบ**
2. คลิก **แก้ไข** ถัดจาก **การแจ้งเตือนแบบโต้ตอบ** ในส่วน **คอมพิวเตอร์** ให้เลิกเลือกกล่องกาเครื่องหมายถัดจาก **เริ่มต้นคอมพิวเตอร์ใหม่ (จำเป็น)** และ **เริ่มต้นคอมพิวเตอร์ใหม่ (แนะนำ)**
3. คลิก **ตกลง** เพื่อบันทึกการเปลี่ยนแปลงของคุณในทั้งสองหน้าต่างที่เปิดอยู่

4. การแจ้งเตือนจะไม่แสดงขึ้นในเครื่องเอ็นพอยต์อีกต่อไป
5. (ไม่บังคับ) ในการปิดใช้งานสถานะแอพพลิเคชันในหน้าต่างโปรแกรมหลักของ ESET Endpoint Security จากหน้าต่างสถานะแอพพลิเคชัน ให้เลิกเลือกกล่องกาเครื่องหมายถัดจาก **ต้องเริ่มต้นคอมพิวเตอร์ใหม่** และ **ขอแนะนำให้เริ่มต้นคอมพิวเตอร์ใหม่**

ขอแนะนำให้เริ่มต้นระบบใหม่

จำเป็นต้องรีสตาร์ทคอมพิวเตอร์หลังจากอัพเดท ESET Endpoint Security เป็นเวอร์ชันใหม่ ESET Endpoint Security เวอร์ชันใหม่ได้ออกมาเพื่อปรับปรุงประสิทธิภาพหรือแก้ไขปัญหาที่การอัพเดทอัตโนมัติของโมดูลโปรแกรมไม่สามารถแก้ไขได้

คลิก **รีสตาร์ททันที** เพื่อรีสตาร์ทคอมพิวเตอร์ของคุณ หากคุณวางแผนจะรีสตาร์ทคอมพิวเตอร์ของคุณในภายหลัง ให้คลิก **เตือนฉันในภายหลัง** คุณสามารถรีสตาร์ทคอมพิวเตอร์ด้วยตนเองในภายหลังได้จากส่วน**สถานะการป้องกัน**ในหน้าต่างโปรแกรมหลัก

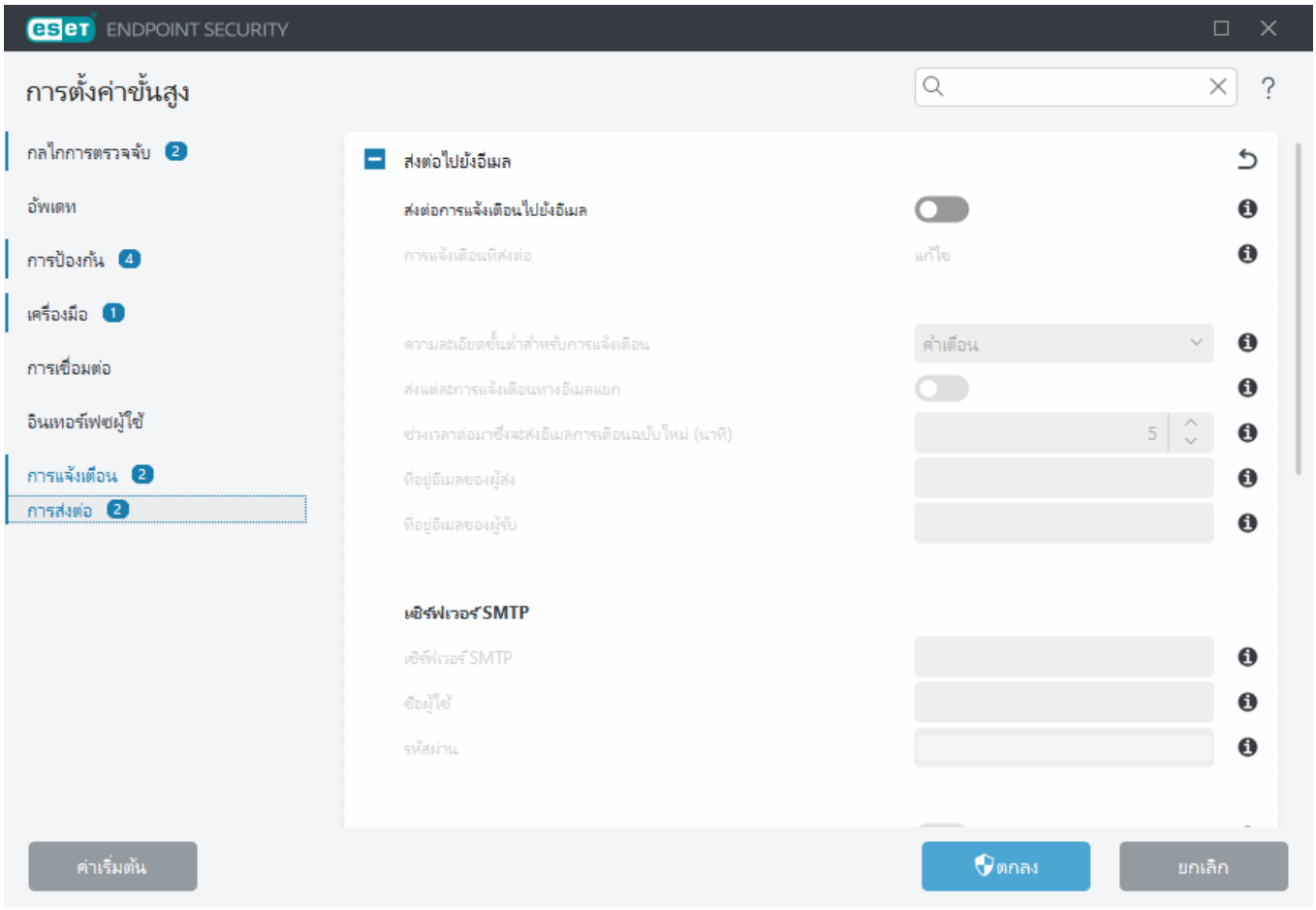
ในการปิดใช้งานการเตือน "ต้องเริ่มต้นระบบใหม่" หรือ "ขอแนะนำให้เริ่มต้นระบบใหม่" โปรดทำตามขั้นตอนด้านล่างนี้:

1. เปิด **การตั้งค่าขั้นสูง** (F5) > **การแจ้งเตือน** > **การแจ้งเตือนแบบโต้ตอบ**
2. คลิก **แก้ไข** ถัดจาก **การแจ้งเตือนแบบโต้ตอบ** ในส่วน **คอมพิวเตอร์** ให้เลิกเลือกกล่องกาเครื่องหมายถัดจาก **เริ่มต้นคอมพิวเตอร์ใหม่ (จำเป็น)** และ **เริ่มต้นคอมพิวเตอร์ใหม่ (แนะนำ)**
3. คลิก **ตกลง** เพื่อบันทึกการเปลี่ยนแปลงของคุณในทั้งสองหน้าต่างที่เปิดอยู่
4. การแจ้งเตือนจะไม่แสดงขึ้นในเครื่องเอ็นพอยต์อีกต่อไป
5. (ไม่บังคับ) ในการปิดใช้งานสถานะแอพพลิเคชันในหน้าต่างโปรแกรมหลักของ ESET Endpoint Security จากหน้าต่างสถานะแอพพลิเคชัน ให้เลิกเลือกกล่องกาเครื่องหมายถัดจาก **ต้องเริ่มต้นคอมพิวเตอร์ใหม่** และ **ขอแนะนำให้เริ่มต้นคอมพิวเตอร์ใหม่**

การส่งต่อ

ESET Endpoint Security สามารถส่งอีเมลแจ้งเตือนได้โดยอัตโนมัติหากมีเหตุการณ์ที่มีระดับความละเอียดที่เลือกไว้เกิดขึ้น ในส่วน การตั้งค่าขั้นสูง > **การแจ้งเตือน** > **การส่งต่อ** > **ส่งต่อไปยังอีเมล** ให้เปิดใช้งาน **ส่งต่อการแจ้งเตือนไปยังอีเมล** เพื่อเปิดใช้งานการแจ้งเตือนทางอีเมล

การแจ้งเตือนที่ส่งต่อ – เลือกการแจ้งเตือนบนเดสก์ท็อปที่ต้องการส่งต่อทางอีเมล



จากเมนูแบบเลื่อนลง **ความละเอียดขั้นต่ำสำหรับการแจ้งเตือน** คุณสามารถเลือกระดับความรุนแรงเริ่มต้นของการแจ้งเตือนที่จะส่ง

- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- **มีข้อมูล** – บันทึกข้อความแจ้งข้อมูล เช่น กิจกรรมเครือข่ายที่ไม่ได้มาตรฐาน รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน (เช่น อัพเดทไม่สำเร็จ)
- **ข้อผิดพลาด** – ข้อผิดพลาด (ไม่ได้เริ่มต้นการป้องกันเอกสาร) และข้อผิดพลาดร้ายแรงจะถูกบันทึก
- **ร้ายแรง** – บันทึกเฉพาะข้อผิดพลาดร้ายแรง (เช่น พบข้อผิดพลาดในการเริ่มต้นการป้องกันไวรัส หรือ พบภัยคุกคาม)

ส่งการแจ้งเตือนแต่ละรายการทางอีเมลแยก – เมื่อเปิดใช้งาน ผู้รับจะได้รับอีเมลใหม่สำหรับแต่ละการแจ้งเตือน ซึ่งอาจส่งผลให้ได้รับอีเมลจำนวนมากในระยะเวลาอันสั้น

ช่วงเวลาต่อมาซึ่งจะส่งอีเมลการเตือนฉบับใหม่ (นาที) – ช่วงเวลาต่อมาเป็นนาทีซึ่งจะส่งการเตือนฉบับใหม่ไปยังอีเมล ช่วงเวลาต่อมาซึ่ฉบับใหม่ไปยังอีเมล หากคุณตั้งค่านี้เป็น 0 การแจ้งเตือนเหล่านั้นจะถูกส่งในทันที

ที่อยู่ของผู้ส่ง – ระบุที่อยู่ของผู้ส่งซึ่งจะแสดงที่ส่วนหัวของอีเมลการแจ้งเตือน

ที่อยู่ของผู้รับ – ระบุที่อยู่ของผู้รับที่จะแสดงในส่วนหัวของอีเมลการแจ้งเตือน รองรับหลายค่า ใช้เครื่องหมายอัฒภาคเป็นตัวคั่น

เซิร์ฟเวอร์ SMTP

เซิร์ฟเวอร์ SMTP – เซิร์ฟเวอร์ SMTP ที่ใช้สำหรับส่งการแจ้งเตือน (เช่น *smtp.provider.com:587* พอร์ตที่กำหนดไว้ล่วงหน้าคือ พอร์ต 25)

เซิร์ฟเวอร์ SMTP ที่มีการเข้ารหัส TLS นั้น ได้รับการสนับสนุนโดย ESET Endpoint Security

ชื่อผู้ใช้ และ รหัสผ่าน – ถ้าเซิร์ฟเวอร์ SMTP ต้องมีการตรวจสอบสิทธิ์ ผู้ใช้ควรป้อนชื่อผู้ใช้และรหัสผ่านที่ถูกต้องในช่องเหล่านี้เพื่อเข้าถึงเซิร์ฟเวอร์ SMTP

ที่อยู่ของผู้ส่ง – ช่องนี้ระบุที่อยู่ของผู้ส่งซึ่งจะแสดงที่ส่วนหัวของอีเมลการแจ้งเตือน

ที่อยู่ของผู้รับ – ช่องนี้ระบุที่อยู่ของผู้รับซึ่งจะแสดงที่ส่วนหัวของอีเมลการแจ้งเตือน ใช้เครื่องหมายเซมิโคลอน ";" เพื่อแบ่งที่อยู่อีเมลหลายอีเมล

เปิดใช้งาน TLS – เปิดใช้งานการส่งข้อความการเตือนและข้อความการแจ้งเตือนที่การเข้ารหัส TLS รองรับ

รูปแบบข้อความ

การสื่อสารระหว่างโปรแกรมและผู้ใช้หรือผู้ดูแลระบบระยะไกลจะกระทำผ่านอีเมลหรือข้อความ LAN (โดยใช้บริการส่งข้อความของ Windows) รูปแบบเริ่มต้นของข้อความเตือนและข้อความแจ้งเตือน เป็นรูปแบบที่เหมาะกับสถานการณ์ส่วนใหญ่ แต่ในบางกรณี คุณอาจต้องการเปลี่ยนรูปแบบข้อความของข้อความเหตุการณ์

รูปแบบของข้อความเหตุการณ์ – รูปแบบข้อความของเหตุการณ์ที่แสดงบนคอมพิวเตอร์ระยะไกล

รูปแบบของข้อความเตือนภัยคุกคาม – ข้อความการเตือนและข้อความการแจ้งเตือนภัยคุกคามจะมีรูปแบบเริ่มต้นที่กำหนดไว้ล่วงหน้า เราไม่แนะนำให้เปลี่ยนรูปแบบนี้ แต่ในบางกรณี (ตัวอย่างเช่น หากคุณมีระบบประมวลผลอีเมลอัตโนมัติ) คุณอาจต้องการเปลี่ยนรูปแบบข้อความ

Charset – แปลงข้อความอีเมลเป็นการเข้ารหัสอักขระแบบ ANSI ตามการตั้งค่า Windows Regional (ตัวอย่างเช่น windows-1250, Unicode (UTF-8), ACSII 7-bit หรือภาษาญี่ปุ่น (ISO-2022-JP)) ซึ่งทำให้ "á" จะถูกเปลี่ยนเป็น "a" และสัญลักษณ์ที่ไม่รู้จักจะเปลี่ยนเป็น "?"

ใช้การเข้ารหัสในรูปแบบ Quoted-printable - ที่มาของข้อความอีเมลจะถูกเข้ารหัสในรูปแบบ Quoted-printable (QP) ซึ่งใช้อักขระ ASCII และสามารถส่งอักขระพิเศษของภาษาทางอีเมลได้อย่างถูกต้องในรูปแบบ 8 บิต (áéíóú)

คำหลัก (สตริงที่คั่นด้วยเครื่องหมาย %) ในข้อความจะถูกแทนที่ด้วยข้อมูลตามจริงที่ระบุไว้ คำหลักที่ใช้ได้มีดังนี้:

- **%TimeStamp%** - วันที่และเวลาของเหตุการณ์
- **%Scanner%** -โมดูลที่เกี่ยวข้อง
- **%ComputerName%** - ชื่อคอมพิวเตอร์ซึ่งมีการเตือนเกิดขึ้น
- **%ProgramName%** - โปรแกรมที่สร้างการเตือน
- **%InfectedObject%** - ชื่อของไฟล์ ข้อความ หรือรายการอื่นๆ ที่ติดไวรัส
- **%VirusName%** - การระบุการติดไวรัส
- **%Action%** – การทำงานที่ควบคุมการแฝงตัว
- **%ErrorDescription%** - คำอธิบายเหตุการณ์ที่ไม่ใช่ไวรัส

คำหลัก **%InfectedObject%** และ **%VirusName%** จะใช้เฉพาะสำหรับข้อความเตือนภัยคุกคามเท่านั้น และ **%ErrorDescription%** จะใช้เฉพาะในข้อความของเหตุการณ์

คืนค่าทั้งหมดกลับเป็นค่าเริ่มต้น

คลิก **ค่าเริ่มต้น** การตั้งค่าขั้นสูง เพื่อแปลงการตั้งค่าโปรแกรมทั้งหมดสำหรับโมดูลทั้งหมดกลับ สิ่งนี้จะถูกรีเซ็ตกลับเป็นสถานะที่เคยมีหลังการติดตั้งใหม่

โปรดดู การตั้งค่าการนำเข้าและส่งออก

แปลงกลับการตั้งค่าทุกอย่างในส่วนปัจจุบัน

คลิกลูกศรโค้ง เพื่อแปลงกลับการตั้งค่าทุกอย่างในส่วนปัจจุบันไปเป็นการตั้งค่าเริ่มต้นที่กำหนดโดย ESET

โปรดทราบว่า การเปลี่ยนแปลงใดๆ ที่ดำเนินการไว้จะสูญหายหลังจากที่คุณคลิก **แปลงกลับเป็นค่าเริ่มต้น**

แปลงกลับสารบัญ – เมื่อเปิดใช้งานตัวเลือกนี้ กฎ งานหรือโปรไฟล์ที่ได้เพิ่มด้วยตนเองหรือโดยอัตโนมัติจะสูญหาย

โปรดดู การตั้งค่าการนำเข้าและส่งออก

เกิดข้อผิดพลาดขณะบันทึกการกำหนดค่า

ข้อความแสดงข้อผิดพลาดนี้ระบุว่าระบบไม่ได้บันทึกการตั้งค่าอย่างถูกต้อง เนื่องจากเกิดข้อผิดพลาด

ซึ่งมักหมายความว่าผู้ใช้ที่พยายามจะปรับแต่งพารามิเตอร์โปรแกรมจะ:

- มีสิทธิ์การเข้าถึงไม่เพียงพอหรือไม่มีสิทธิ์พิเศษของระบบปฏิบัติการที่จำเป็นต้องใช้ในการปรับแต่งไฟล์การกำหนดค่าและรีจิสทรีระบบ
  > ในการดำเนินการแก้ไขตามต้องการ ผู้ดูแลระบบต้องลงชื่อเข้า
- ได้เปิดใช้งานโหมดการเรียนรู้ใน HIPS หรือไฟร์วอลล์ และพยายามจะเปลี่ยนแปลงการตั้งค่าขั้นสูง
  > ในการบันทึกการกำหนดค่าและหลีกเลี่ยงข้อขัดแย้งในการกำหนดค่า ให้ปิดการตั้งค่าขั้นสูงโดยไม่บันทึกและพยายามเปลี่ยนแปลงตามต้องการอีกครั้ง

สาเหตุทั่วไปลำดับที่สองอาจเป็นการที่โปรแกรมไม่สามารถทำงานได้อย่างถูกต้อง เกิดความเสียหาย และต้องติดตั้งใหม่

เครื่องมือสแกนของบรรทัดคำสั่ง

โมดูลป้องกันไวรัสของ ESET Endpoint Security นั้นสามารถเรียกใช้ผ่านบรรทัดคำสั่ง ทั้งด้วยตนเอง (โดยใช้คำสั่ง "ecls") หรือใช้ไฟล์แบทช์ ("bat")

การใช้เครื่องสแกนบรรทัดคำสั่งของ ESET:

```
ecls [ตัวเลือก..] ไฟล์..
```

คุณสามารถใช้พารามิเตอร์และสวิตช์ต่อไปนี้ขณะที่เรียกใช้เครื่องมือสแกนตามต้องการจากบรรทัดคำสั่ง:

ตัวเลือก

/base-dir=โฟลเดอร์	โหลดโมดูลจากโฟลเดอร์
/quar-dir=โฟลเดอร์	โฟลเดอร์กักเก็บ
/exclude=มาสก์	ยกเว้นไฟล์ที่ตรงกับมาสก์ในการสแกน
/subdir	สแกนโฟลเดอร์ย่อย (เริ่มต้น)
/no-subdir	ไม่สแกนโฟลเดอร์ย่อย
/max-subdir-level=LEVEL	จำนวนระดับย่อยสูงสุดของโฟลเดอร์ภายในโฟลเดอร์ที่จะสแกน

/symlink	ตามลิงค์สัญลักษณ์ (เริ่มต้น)
/no-symlink	ข้ามลิงค์สัญลักษณ์
/ads	สแกน ADS (เริ่มต้น)
/no-ads	ไม่สแกน ADS
/log-file=ไฟล์	บันทึกผลลัพธ์ไปที่ไฟล์
/log-rewrite	เขียนทับไฟล์ผลลัพธ์ (เริ่มต้น - ต่อท้าย)
/log-console	บันทึกผลลัพธ์ไปที่คอนโซล (เริ่มต้น)
/no-log-console	ไม่บันทึกผลลัพธ์ไปที่คอนโซล
/log-all	บันทึกไฟล์ที่ไม่ติดไวรัส
/no-log-all	ไม่บันทึกไฟล์ที่ไม่ติดไวรัส (เริ่มต้น)
/aind	แสดงสัญลักษณ์ของการทำงาน
/auto	สแกนและกำจัดโดยอัตโนมัติดิสก์ภายในเครื่องทั้งหมด

ตัวเลือกเครื่องมือสแกน

/files	สแกนไฟล์ (เริ่มต้น)
/no-files	ไม่สแกนไฟล์
/memory	สแกนหน่วยความจำ
/boots	สแกนบูตเซคเตอร์
/no-boots	ไม่สแกนบูตเซคเตอร์ (เริ่มต้น)
/arch	สแกนที่เก็บเอกสาร (เริ่มต้น)
/no-arch	ไม่สแกนที่เก็บเอกสาร
/max-obj-size=ขนาด	สแกนเฉพาะไฟล์ที่เล็กกว่า SIZE เมกะไบต์ (เริ่มต้น 0 = ไม่จำกัด)
/max-arch-level=LEVEL	จำนวนระดับย่อยสูงสุดของที่เก็บเอกสารภายในที่เก็บเอกสาร (ที่เก็บเอกสารซ้อน) ที่จะสแกน
/scan-timeout=จำกัด	สแกนที่เก็บเอกสารเป็นเวลาสูงสุดไม่เกิน LIMIT วินาที
/max-arch-size=ขนาด	สแกนไฟล์ในที่เก็บเอกสารเฉพาะเมื่อไฟล์มีขนาดเล็กกว่า SIZE (เริ่มต้น 0 = ไม่จำกัด)
/max-sfx-size=ขนาด	สแกนเฉพาะไฟล์ในที่เก็บเอกสารที่ขยายในตัว ถ้ามีขนาดเล็กกว่า SIZE เมกะไบต์ (เริ่มต้น 0 = ไม่จำกัด)
/mail	สแกนไฟล์อีเมล (เริ่มต้น)
/no-mail	ไม่สแกนไฟล์อีเมล
/mailbox	สแกนกล่องจดหมาย (เริ่มต้น)
/no-mailbox	ไม่สแกนกล่องจดหมาย
/sfx	สแกนที่เก็บเอกสารที่ขยายในตัว (เริ่มต้น)
/no-sfx	ไม่สแกนที่เก็บเอกสารที่ขยายในตัว
/rtp	สแกนรันไทม์แพ็คเกอร์ (เริ่มต้น)
/no-rtp	ไม่สแกนรันไทม์แพ็คเกอร์
/unsafe	สแกนหาแอพพลิเคชันที่อาจไม่ปลอดภัย
/no-unsafe	ไม่สแกนหาแอพพลิเคชันที่อาจไม่ปลอดภัย (เริ่มต้น)
/unwanted	สแกนหาแอพพลิเคชันที่อาจไม่พึงประสงค์

/no-unwanted	ไม่สแกนหาแอพพลิเคชันที่อาจไม่พึงประสงค์ (เริ่มต้น)
/suspicious	สแกนหาแอพพลิเคชันที่น่าสงสัย (ค่าเริ่มต้น)
/no-suspicious	ไม่สแกนหาแอพพลิเคชันที่อาจน่าสงสัย
/pattern	ใช้ฐานข้อมูล (เริ่มต้น)
/no-pattern	ไม่ใช้ฐานข้อมูล
/heur	เปิดใช้งานการวิเคราะห์พฤติกรรม (เริ่มต้น)
/no-heur	ปิดใช้งานการวิเคราะห์พฤติกรรม
/adv-heur	เปิดใช้งานการวิเคราะห์พฤติกรรมขั้นสูง (เริ่มต้น)
/no-adv-heur	ปิดใช้งานการวิเคราะห์พฤติกรรมขั้นสูง
/ext-exclude=ส่วนขยาย	ไม่รวมไฟล์ EXTENSIONS ที่คั่นด้วยเครื่องหมายโคลอนในการสแกน
/clean-mode=โหมด	ใช้โหมดการกำจัดสำหรับวัตถุที่ติดไวรัส ตัวเลือกที่ใช้ได้มีดังนี้: • none (ค่าเริ่มต้น) – จะไม่มีการกำจัดโดยอัตโนมัติ • standard – ecls.exe จะพยายามกำจัดหรือลบไฟล์ที่ติดไวรัสโดยอัตโนมัติ • เข้มงวด - ecls.exe จะพยายามกำจัดหรือลบไฟล์ที่ติดไวรัสโดยอัตโนมัติโดยไม่ต้องมีการดำเนินการโดยผู้ใช้ (คุณจะไม่ได้รับข้อความก่อนที่ไฟล์จะถูกลบ) • เคร่งครัด – ecls.exe จะลบไฟล์โดยไม่พยายามกำจัดไม่ว่าจะเป็นไฟล์อะไรก็ตาม • ลบ - ecls.exe จะลบไฟล์โดยไม่พยายามกำจัดแต่จะระงับการลบไฟล์ที่ละเอียดอ่อน เช่น ไฟล์ระบบ Windows
/quarantine	คัดลอกไฟล์ที่ติดไวรัส (ถ้ากำจัดแล้ว) ไปยังส่วนกักเก็บ (เสริมการทำงานที่ดำเนินการขณะกำจัด)
/no-quarantine	ไม่คัดลอกไฟล์ที่ติดไวรัสไปยังส่วนกักเก็บ

ตัวเลือกทั่วไป

/help	แสดงวิธีใช้และออก
/version	แสดงข้อมูลเวอร์ชันและออก
/preserve-time	เก็บบันทึกการลงเวลาเข้าถึงล่าสุด

รหัสการออกจากการทำงาน

0	ไม่พบภัยคุกคาม
1	พบภัยคุกคามและกำจัดแล้ว
10	ไม่สามารถสแกนบางไฟล์ได้ (อาจเป็นภัยคุกคาม)
50	พบภัยคุกคาม
100	ข้อผิดพลาด

รหัสการออกจากการทำงานที่มากกว่า 100 หมายความว่าไม่มีการสแกนไฟล์และอาจมีการติดไวรัส

คำถามทั่วไป

บทนี้จะครอบคลุมคำถามที่พบบ่อยและปัญหาที่พบเกือบทั้งหมด คลิกที่ชื่อหัวข้อเพื่อค้นหาวิธีแก้ไขปัญหา:

- วิธีอัพเดท ESET Endpoint Security
- วิธีเปิดใช้งาน ESET Endpoint Security
- ESET Endpoint Security ตรวจพบภัยคุกคาม
- วิธีลบไวรัสออกจากคอมพิวเตอร์
- วิธีอนุญาตการสื่อสารสำหรับแอพพลิเคชัน
- วิธีสร้างงานใหม่ในเครื่องมือวางกำหนดการ
- วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์
- วิธีการจัดการการแจ้งเตือนและการแจ้งเตือนแบบโต้ตอบ
- วิธีเชื่อมต่อผลิตภัณฑ์ของฉันกับ ESET PROTECT
  - วิธีการใช้โหมดเขียนทับ
  - วิธีนำนโยบายที่แนะนำไปใช้สำหรับ ESET Endpoint Security
- วิธีกำหนดค่ามิเรอร์
- ฉันจะอัพเกรดเป็น Windows 10 ด้วย ESET Endpoint Security ได้อย่างไร
- วิธีเปิดใช้งานการตรวจสอบและการจัดการระยะไกล
- วิธีการปิดกั้นการดาวน์โหลดของประเภทไฟล์บางประเภทจากอินเทอร์เน็ต
- วิธีการย่อส่วนติดต่อกับผู้ใช้ของ ESET Endpoint Security

หากปัญหาของคุณไม่ได้รวมอยู่ในหน้าวิธีใช้ที่แสดงไว้ที่ด้านบนนี้ ให้ลองค้นหาจากคำหลักหรือวลีที่อธิบายถึงปัญหาของคุณในหน้าวิธีใช้ของ ESET Endpoint Security

หากคุณไม่พบทางแก้ไขปัญหา/คำถามของคุณในหน้าวิธีใช้ โปรดไปที่ ฐานความรู้ของ ESET ที่ซึ่งจะมีคำตอบสำหรับคำถามและปัญหาที่พบบ่อย

- วิธีถอนการติดตั้ง ESET Endpoint Security
- แนวทางปฏิบัติในการป้องกันมัลแวร์ไฟล์โค้ดเดอร์ (โปรแกรมเรียกค่าไถ่)
- ESET Endpoint Security และ ESET Endpoint Antivirus FAQ
- ฉันควรเปิดที่อยู่และพอร์ตใดในไฟร์วอลล์ที่ไม่ได้เชื่อมต่อโดยตรงเพื่ออนุญาตให้ผลิตภัณฑ์ ESET ของฉันทำงานได้อย่างสมบูรณ์

หากจำเป็น คุณสามารถติดต่อศูนย์การสนับสนุนด้านเทคนิคทางออนไลน์ได้โดยตรง พร้อมทั้งแจ้งปัญหาหรือคำถามของคุณ คุณจะพบลิงค์ไปยังแบบฟอร์มการติดต่อออนไลน์ของเราได้ในช่อง **วิธีใช้และการสนับสนุน** ในหน้าต่างโปรแกรมหลัก

คำถามที่พบบ่อยเกี่ยวกับการอัพเดทอัตโนมัติ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการอัพเดทผลิตภัณฑ์ใน ESET Endpoint Security โปรดอ่านบทความฐานความรู้ของ ESET ดังต่อไปนี้

- อะไรคือความแตกต่างระหว่างผลิตภัณฑ์ของ ESET ประเภทอัพเดทและประเภทที่เผยแพร่ให้ใช้งาน

คอมพิวเตอร์จะอัพเดทโดยอัตโนมัติหรือไม่ และระบบจะดาวน์โหลดการอัพเดทก่อนหรือหลังรีสตาร์ท

ระบบจะดาวน์โหลดการอัพเดทก่อนที่จะรีสตาร์ท โดยจะจัดเตรียมไฟล์อัพเดทไปพร้อมกันด้วยในขั้นตอนนี้ และเมื่อรีสตาร์ทเสร็จแล้ว ไฟล์ที่ได้รับการอัพเดทนี้จะเพียงแต่อยู่ในสถานะพร้อมใช้งานเท่านั้น ไฟล์เวอร์ชันที่ติดตั้งอยู่ในปัจจุบันจะยังคงให้การป้องกันได้ต่อไปโดยไม่ถูกขัดจังหวะ ระบบจะปรับใช้การเปลี่ยนแปลงเหล่านี้เมื่อเริ่มต้น ESET Endpoint Security ครั้งถัดไป

ฉันมีคอมพิวเตอร์ประมาณ 3000 เครื่อง คอมพิวเตอร์ทุกเครื่องจะดาวน์โหลดการอัพเดทพร้อมกันหรือไม่ และฉันสามารถใช้พร็อกซี่สำหรับการอัพเดทอัตโนมัติสำหรับคอมพิวเตอร์จำนวนมากขนาดนั้นได้หรือไม่

ESET มีเครื่องมือมิเรอร์และโซลูชันพร็อกซี่สำหรับเครือข่ายขนาดใหญ่ให้ ด้วยเหตุนี้ ระบบจึงต้องดาวน์โหลดการอัพเดทผ่านทางอินเทอร์เน็ตเพียงครั้งเดียวเท่านั้นก่อนที่จะนำไปแจกจ่ายภายในเครือข่าย การอัพเดทต่างๆ เหล่านี้จะมีขนาดเล็กกว่า โดยทั่วไปแล้วจะมีขนาดเพียง 5–10 MB นอกจากนี้ ESET ยังจะคอยควบคุมปริมาณการอัพเดทในช่วงสัปดาห์แรกที่รายการเหล่านี้พร้อมให้ดาวน์โหลด ไคลเอนต์ทุกเครื่องจึงจะไม่เริ่มดาวน์โหลดพร้อมกันเมื่อเชื่อมต่อกับเซิร์ฟเวอร์ ESET โดยตรง

ฉันสามารถตัดสินใจได้หรือไม่ว่าคอมพิวเตอร์เครื่องใดจะอัพเดทโดยอัตโนมัติ ฉันไม่ต้องการดาวน์โหลดคอมพิวเตอร์มากกว่าสิบเครื่องต่อชั่วโมง หรือฉันต้องการอัพเดทคอมพิวเตอร์เพียงสิบเครื่องในตอนนี้และอัพเดทคอมพิวเตอร์เครื่องอื่นหลังจากผ่านไปสองสามวัน

สภาพแวดล้อมที่ได้รับการจัดการมีนโยบายการอัพเดทอัตโนมัติซึ่งคุณสามารถระบุเวอร์ชันล่าสุดที่ต้องการได้ และยังรองรับสัญลักษณ์แทน (ตัวอย่างเช่น 9.0.2032.*) อีกด้วย หากต้องการข้อมูลเพิ่มเติม โปรดดูบทการอัพเดทอัตโนมัติในตัวช่วยออนไลน์สำหรับ ESET PROTECT หรือ ESET PROTECT Cloud และเราต้องขออภัยด้วยที่ขณะนี้ยังไม่มีตัวเลือกอื่นสำหรับจำกัดการอัพเดทอัตโนมัติให้ใช้งาน แต่คุณสามารถกำหนดหลายนโยบายให้กับหลายกลุ่มได้

สามารถกำหนดค่าการอัพเดทอัตโนมัติด้วยวิธีอื่นนอกจากการดำเนินการด้วยนโยบายหรือไม่ และสามารถปิดใช้งานนโยบายนี้ได้หรือไม่ หากฉันไม่ต้องการให้ผลิตภัณฑ์ของ ESET ได้รับการอัพเดท

หากเราได้ออกฮอตฟิกซ์เกี่ยวกับความปลอดภัยและความเสถียรสำหรับผลิตภัณฑ์ ESET Endpoint ผลิตภัณฑ์นี้จะทำการอัพเดทแม้ว่าคุณจะปิดใช้งานการอัพเดทโดยอัตโนมัติไว้ ซึ่งเป็นไปตามข้อกำหนดที่มีผลบังคับใช้ในข้อตกลงและการใช้งานใบอนุญาต ESET ใช้ ฮอตฟิกซ์เกี่ยวกับความปลอดภัยและความเสถียร เพื่อแก้ไขปัญหาที่มีความร้ายแรงและเพื่อให้แน่ใจว่าคุณจะได้รับความปลอดภัยและความเสถียรขั้นสูงสุดสำหรับผลิตภัณฑ์ ESET

คุณสามารถกำหนดนโยบายการอัพเดทอัตโนมัติให้กับกลุ่มเอ็นพอยต์ใดก็ได้ โดยไม่คำนึงถึงการกำหนดค่าการอัพเดทอัตโนมัติในปัจจุบัน ในสภาพแวดล้อมที่ไม่ได้รับการจัดการ ผู้ใช้สามารถกำหนดค่าการอัพเดทอัตโนมัติภายในเครื่องได้ในหน้าจอการตั้งค่าขั้นสูงของผลิตภัณฑ์ ESET Endpoint

จะเกิดอะไรขึ้นหากฉันกำหนดค่านโยบายให้ใช้เวอร์ชันแรกสุดที่มี ESET จะยังอัพเดทผลิตภัณฑ์ของฉันหรือไม่

ฮอตฟิกซ์และฮอตฟิกซ์สำหรับปัญหาร้ายแรง (การอัพเดทการรักษาความปลอดภัยและความเสถียร) เป็นประเภทการอัพเดทที่แตกต่างกันเล็กน้อย โดยเมื่อยอมรับการตั้งค่าจากผู้ใช้ ระบบจะกำหนดให้ฮอตฟิกซ์ทั่วไปดำเนินการอัพเดทโดยอัตโนมัติโดยมีลำดับความสำคัญมาตรฐาน แต่จะปรับใช้ฮอตฟิกซ์สำหรับปัญหาร้ายแรงด้วยลำดับความสำคัญสูงสุดโดยไม่คำนึงถึงการตั้งค่าของผู้ใช้

การอัพเดทจะทำงานอย่างไรเมื่อออฟไลน์ และผู้ใช้จะต้องใช้ Repository ออฟไลน์เมื่อใด

Repository ออฟไลน์นั้นจะมีไฟล์ .dup และ .fup โดยเครื่องมือที่ทำหน้าที่ดาวน์โหลดส่วน Repository จะเป็นเครื่องมือมิเรอร์ ไม่ใช่การอัพเดทโมดูล ดูข้อมูลเพิ่มเติมได้ที่หัวข้อ Repository แบบออฟไลน์ ในวิธีใช้แบบออนไลน์สำหรับ ESET PROTECT

ผลิตภัณฑ์ ESET รู้ได้อย่างไรว่าต้องได้รับการอัพเดท ได้รับข้อมูลจาก Repository ใช่ไหม มีการส่งข้อมูลไปยังเซิร์ฟเวอร์หรือไม่ หาก ESET วางแผนว่าจะอัพเดทหลังจากที่มีการเผยแพร่เวอร์ชันไปแล้วหนึ่งเดือน ทางเซิร์ฟเวอร์ของ ESET จะสามารถรองรับการเปิดให้ใช้ทั่วโลกได้หรือไม่

ผลิตภัณฑ์ ESET จะดาวน์โหลดการอัพเดทอัตโนมัติจาก Repository โดยเซิร์ฟเวอร์จะพร้อมรับมือเสมอเนื่องจากการอัพเดทที่สำคัญนั้นมีขนาดเพียงไม่กี่ KB และ ESET จะไม่ทำให้เกิดการควบคุมปริมาณการอัพเดทที่สำคัญบนเซิร์ฟเวอร์ Repository อย่างไรก็ตาม มีตัวเลือกที่จะเปิดใช้งานการจำกัดปริมาณบนเซิร์ฟเวอร์ได้หากการอัพเดทอัตโนมัติมีขนาดใหญ่ คุณสามารถดูตัวอย่างขนาดฮอตฟิกซ์ในการอัพเดทส่วนต่างอัตโนมัติได้ในตารางด้านล่าง:

เวอร์ชันก่อนหน้า	เวอร์ชันใหม่	ขนาด
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

ผลิตภัณฑ์ ESET ของคุณอาจจะเริ่มต้นการอัพเดทแบบเต็มหากการอัพเดทส่วนต่างอัตโนมัติล้มเหลว โดยจะยังคงเป็นการอัพเดทอัตโนมัติที่มีการรับประกันฟังก์ชันการทำงาน แต่จะดาวน์โหลดไฟล์ .fup ซึ่งมีขนาดใหญ่กว่าแทนไฟล์ .dup โดยสำหรับเวอร์ชัน 9.0.2032.2 จะมีขนาด 27 MB อย่างไรก็ตาม สถานการณ์ดังกล่าวเกิดขึ้นได้ยาก

การอัพเดท ESET Endpoint Security จะเปิดให้ใช้พร้อมกับการควบคุมปริมาณหรือไม่ หากมี การควบคุมปริมาณจะดำเนินการหลังเปิดให้ใช้

นานเท่าใด

ESET จะควบคุมปริมาณการอัพเดทในช่วงสองสามสัปดาห์แรกเมื่อมีการเปิดเวอร์ชันใหม่ให้ใช้งาน เพื่อเป็นการลดภาระให้เซิร์ฟเวอร์และทำให้แจกจ่ายเวอร์ชันใหม่ได้อย่างทั่วถึง

การอัพเดทอัตโนมัติกำลังจะกลายเป็นหนึ่งในวิธีอัพเกรดหลัก จะมีการดำเนินการโดยละเอียดอย่างไร

ESET ต้องการให้ลูกค้าอัพเดทผ่านการอัพเดทอัตโนมัติให้มากที่สุดเท่าที่จะเป็นไปได้ เนื่องจากการเปิดให้สามารถใช้เวอร์ชันเก่าได้เป็นจำนวนมากทำให้เราสนับสนุนได้ยาก คุณลักษณะการอัพเดทอัตโนมัตินั้นจะมีวิธีการทำงานที่ไม่ซับซ้อน – นั่นคือระบบจะดาวน์โหลดไฟล์ .dup ในระหว่างการตรวจสอบการอัพเดทโมดูลครั้งแรก โดยผลิตภัณฑ์จะทำงานได้อย่างสมบูรณ์และจะปกป้องเครื่องคอมพิวเตอร์ตลอดเวลาในระหว่างขั้นตอนการอัพเดทดังกล่าว จากนั้นระบบจะเปิดใช้งานเวอร์ชันใหม่หลังจากรีสตาร์ท คุณสามารถใช้นโยบายเพื่อระบุเวอร์ชันสูงสุดที่ต้องการอัพเดทใน ESET PROTECT (ฝั่งเซิร์ฟเวอร์) ได้ และยังสามารถใช้อักขระตัวแทนได้อีกด้วย หากต้องการข้อมูลเพิ่มเติม โปรดดูบทการอัพเดทอัตโนมัติในตัวช่วยออนไลน์สำหรับ ESET PROTECT หรือ ESET PROTECT Cloud

การอัพเดทอัตโนมัติทำงานบน 1/10 ถูกต้องหรือไม่ ฉันกำลังใช้ ESET Endpoint Security 8.0.2028.1 ในขณะนี้ หากการอัพเดทอัตโนมัติทำงานจะทำการอัพเดทเป็นเวอร์ชันใด

การอัพเดทผลิตภัณฑ์โดยใช้การอัพเดทอัตโนมัติอาจล่าช้าเนื่องจากการควบคุมปริมาณบนเซิร์ฟเวอร์ Repository หากการอัพเดทผลิตภัณฑ์มีการเปิดให้ใช้งานพร้อมการควบคุมปริมาณ ระบบตรวจสอบการอัพเดทอัตโนมัติอาจไม่ได้รับรายการดังกล่าวโดยทันที และหากระบบกำหนดว่าการอัพเดทนั้นปลอดภัยและมีความเสถียร การควบคุมปริมาณอาจลดลงหรือถูกนำออกทั้งหมดเพื่อให้ไคลเอ็นต์ที่เหลือทั้งหมดได้รับการอัพเดท

ขั้นตอนการควบคุมปริมาณอาจใช้เวลาแตกต่างกันสำหรับการอัพเดทแต่ละครั้ง โดยจะขึ้นอยู่กับจำนวนไคลเอ็นต์ที่ร้องขอการอัพเดท ปริมาณการรับส่งข้อมูลบนเซิร์ฟเวอร์ของเรา และปัจจัยอื่นๆ โดยขั้นตอนดังกล่าวจะมีการเปลี่ยนแปลงอยู่เสมอ

ระบบจะดำเนินการอัพเดทอัตโนมัติเมื่อใด ถ้าฉันเปิดเครื่องคอมพิวเตอร์เวลา 8.45 น. และปิดเครื่องในเวลา 17.00 น.

การอัพเดทอัตโนมัติจะเริ่มเมื่อมีการอัพเดทโมดูลตามกำหนดการครั้งถัดไปที่ประสบความสำเร็จ สูงสุดหนึ่งครั้งทุก 2 4 ชั่วโมง

การอัพเดทจะทำงานครั้งต่อไปเมื่อใดหากคอมพิวเตอร์ปิดลงในขณะที่การอัพเดทอัตโนมัติกำลังทำงานอยู่

การอัพเดทจะทำงานตามกำหนดการครั้งถัดไป โดยมีกลไกป้องกันภัยที่แข็งแกร่งสำหรับขั้นตอนการอัพเดทอัตโนมัติ (เดิมเรียกว่า uPCU) หลังจากดาวน์โหลดการอัพเดทและรีสตาร์ทคอมพิวเตอร์แล้ว ไฟล์ที่ได้รับการอัพเดทนี้จะเพียงอยู่ในสถานะพร้อมใช้งานเท่านั้น โดยไฟล์เวอร์ชันที่ติดตั้งอยู่ในปัจจุบันจะยังคงให้การป้องกันได้ต่อไปโดยไม่ถูกขัดจังหวะ และระบบจะปรับใช้การเปลี่ยนแปลงเหล่านี้เมื่อเริ่มต้นผลิตภัณฑ์ ESET Endpoint ครั้งถัดไป

ฉันจะสามารถเรียกใช้การอัพเดทอัตโนมัติทันทีโดยไม่ต้องรอการเชื่อมต่อตามปกติทุกๆ 24 ชั่วโมงได้อย่างไร มีวิธีอื่นใดในการคลิกตรวจหาการอัพเดทหรือไม่

คุณสามารถเริ่มต้นขั้นตอนการอัพเดทอัตโนมัติด้วยตนเองได้ด้วยการเปิดหน้าต่างโปรแกรมหลักแล้วคลิก **อัพเดท** > **ตรวจหาการอัพเดท** เท่านั้น วิธีเริ่มต้นการอัพเดทโมดูลอื่นๆ ทั้งหมดจะเป็นไปตามนโยบายเครื่องมือวางกำหนดการณ์การอัพเดทอัตโนมัติ 24 ชั่วโมง และคุณจะยังไม่สามารถเริ่มดาวน์โหลดการอัพเดทอัตโนมัติจากระยะไกลได้ในขณะนี้ เราจะเพิ่มคุณลักษณะนี้ในอนาคต

วิธีอัพเดท ESET Endpoint Security

การอัพเดท ESET Endpoint Security สามารถดำเนินการได้ทั้งด้วยตนเองหรือโดยอัตโนมัติ ในการเรียกการอัพเดทให้คลิก **อัพเดท** ในหน้าต่างโปรแกรมหลักแล้วคลิก **ตรวจหาการอัพเดท**

การตั้งค่าการติดตั้งเริ่มต้นจะสร้างงานการอัพเดทอัตโนมัติ ซึ่งสามารถทำงานเป็นประจำในแต่ละชั่วโมง เมื่อต้องการเปลี่ยนช่วงเวลา ให้ไปที่ **เครื่องมือ** > เครื่องมือวางกำหนดการ

วิธีลบไวรัสออกจากคอมพิวเตอร์

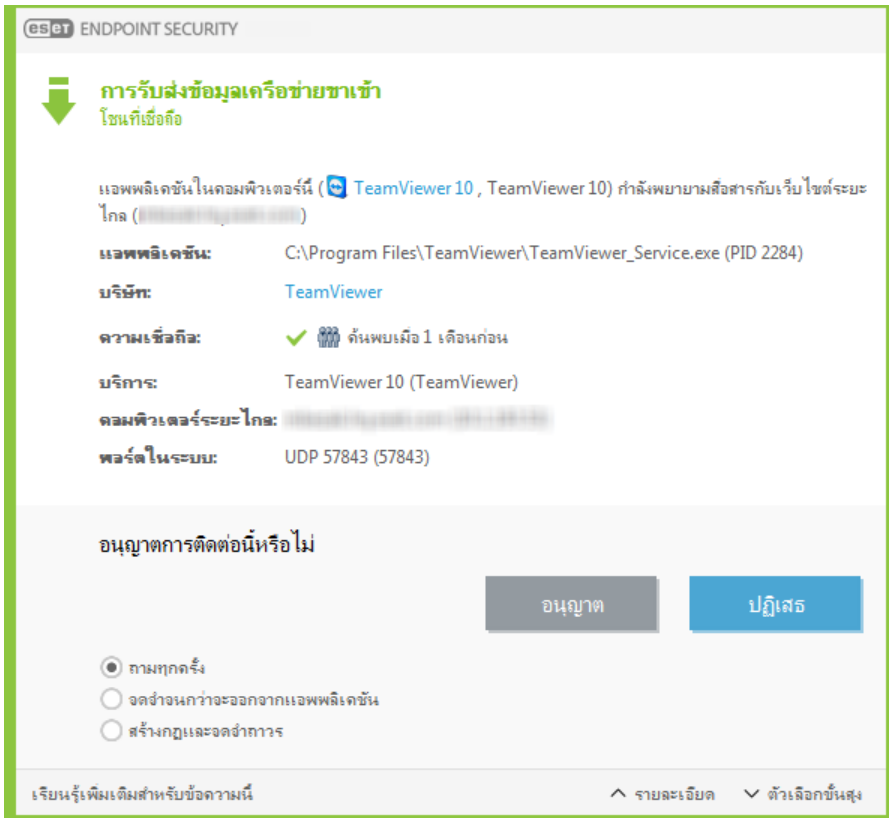
ถ้าคอมพิวเตอร์ของคุณแสดงอาการการติดไวรัสจากมัลแวร์ ตัวอย่างเช่น ทำงานช้า ค้างบ่อยๆ เราขอแนะนำให้คุณดำเนินการดังนี้:

1. ใน หน้าต่างโปรแกรมหลัก ให้คลิก **การสแกนคอมพิวเตอร์**
2. คลิก **การสแกนแบบสมาร์ท** เพื่อเริ่มต้นการสแกนระบบ
3. หลังจากสแกนเสร็จสิ้นแล้ว ให้ตรวจดูบันทึกสำหรับจำนวนไฟล์ที่สแกน ไฟล์ที่ติดไวรัส และไฟล์ที่กำจัด
4. หากคุณต้องการสแกนเฉพาะบางส่วนของดิสก์ ให้คลิก **การสแกนที่กำหนดเอง** และเลือกเป้าหมายที่จะสแกนไวรัส

สำหรับข้อมูลเพิ่มเติม โปรดดู บทความฐานความรู้ของ ESET ของเราที่มีการอัพเดทเป็นประจำ

วิธีอนุญาตการสื่อสารสำหรับแอพพลิเคชัน

ถ้าตรวจพบการเชื่อมต่อใหม่ในโหมดตอบสนอง และไม่มีกฎการจับคู่ คุณจะได้รับข้อความเพื่อให้อนุญาตหรือปฏิเสธการเชื่อมต่อ ถ้าคุณต้องการให้ ESET Endpoint Security ทำงานเหมือนกันทุกครั้งที่แอพพลิเคชันพยายามเริ่มต้นการเชื่อมต่อ ให้เลือกช่องทำเครื่องหมาย **จดจำการทำงาน (สร้างกฎ)**



คุณสามารถสร้างกฎไฟร์วอลล์ใหม่สำหรับแอปพลิเคชันก่อนที่ ESET Endpoint Security จะตรวจพบในหน้าต่างการตั้งค่าของไฟร์วอลล์ โดยเปิดหน้าต่างโปรแกรมหลัก > **การตั้งค่า** > **เครือข่าย** > **ไฟร์วอลล์** > คลิกที่ล้อเฟือง > **กำหนดค่า** > **ขั้นสูง** > **กฎ** โดยการคลิก **แก้ไข**

คลิก **เพิ่ม** เพื่อเพิ่มกฎ คลิกปุ่ม เพิ่ม และในแท็บ **ทั่วไป** ให้ป้อนชื่อ คำสั่ง และโปรโตคอลการสื่อสารสำหรับกฎ หน้าต่างนี้ช่วยให้คุณสามารถกำหนดการกระทำที่จะดำเนินการเมื่อใช้กฎ

ป้อนพาธไปยังไฟล์ที่เรียกใช้ของแอพพลิเคชันและพอร์ตการสื่อสารในระบบในแท็บ **ในระบบ** คลิกแท็บ **ระยะไกล** เพื่อป้อนที่อยู่และพอร์ตระยะไกล (ถ้ามี) กฎที่สร้างใหม่จะถูกนำไปใช้เมื่อแอพพลิเคชันพยายามสื่อสารอีกครั้ง

วิธีสร้างงานใหม่ในเครื่องมือวางกำหนดการ

เมื่อต้องการสร้างงานใหม่ใน **เครื่องมือ** > **เครื่องมือวางกำหนดการ** ให้คลิก **เพิ่มงาน** หรือคลิกขวาและเลือก **เพิ่ม** ที่เมนูบริบท มีงานตามกำหนดการห้าประเภท:

- **เรียกใช้แอพพลิเคชันภายนอก** – วางกำหนดการเรียกใช้แอพพลิเคชันภายนอก
- **การบำรุงรักษาบันทึก** – ไฟล์บันทึกยังมีข้อมูลที่หลงเหลือจากบันทึกที่ลบแล้วอีกด้วย งานนี้จะช่วยเพิ่มประสิทธิภาพการบันทึกในไฟล์บันทึกเป็นประจำเพื่อให้มีประสิทธิภาพการทำงานเพิ่มขึ้น
- **การตรวจสอบไฟล์เมื่อเริ่มต้น** – ตรวจสอบไฟล์ที่อนุญาตให้เรียกใช้ได้เมื่อเริ่มต้นระบบหรือเข้าสู่ระบบ
- **สร้างสแนปชอตสถานะของคอมพิวเตอร์** – สร้างสแนปชอตคอมพิวเตอร์ของ ESET SysInspector โดยรวบรวมข้อมูลโดยละเอียดเกี่ยวกับองค์ประกอบของระบบ (ตัวอย่างเช่น ไดรเวอร์ แอพพลิเคชัน) และประเมินระดับความเสี่ยงขององค์ประกอบแต่ละรายการ
- **การสแกนคอมพิวเตอร์ตามต้องการ** – ดำเนินการสแกนคอมพิวเตอร์ของไฟล์และโฟลเดอร์บนคอมพิวเตอร์ของคุณ
- **อัพเดท** – ตารางเวลาและอัพเดทงานโดยการอัพเดทโมดูลเหล่านี้

เนื่องจาก **อัพเดท** เป็นงานตามกำหนดการที่ใช้บ่อยที่สุดงานหนึ่ง ดังนั้นเราจะอธิบายวิธีเพิ่มงานการอัพเดทใหม่ดังด้านล่างนี้:

จากเมนูแบบหล่นลง **งานที่มีกำหนดการ** เลือก **อัพเดท** ป้อนชื่อของงานลงในช่อง **ชื่องาน** แล้วคลิก **ถัดไป** เลือกความถี่ของงาน ตัวเลือกที่ใช้ได้มีดังนี้: **หนึ่งครั้ง ซ้ำ รายวัน รายสัปดาห์** และ **ตามเหตุการณ์ เลือก ข้ามงานเมื่อทำงานด้วยแบตเตอรี่** เพื่อลดการใช้ทรัพยากรของระบบในขณะที่แล็ปท็อปทำงานด้วยพลังงานแบตเตอรี่ งานจะถูกเรียกใช้ตามวันที่และเวลาที่ระบุในช่อง **การเรียกใช้งาน** ขั้นตอนถัดไป ให้กำหนดการทำงานที่ต้องการหากไม่สามารถดำเนินการกับงานหรือทำงานให้สำเร็จตามเวลาในกำหนดกา ตัวเลือกที่ใช้ได้มีดังนี้:

- **เมื่อเวลาที่กำหนดไว้ครั้งต่อไป**
- **เร็วที่สุดเท่าที่ทำได้**
- **ทันที หากเวลาตั้งแต่ครั้งที่แล้วมากกว่าค่าที่ระบุ** (สามารถกำหนดระยะเวลาได้โดยใช้ช่องเลื่อน **เวลาตั้งแต่การใช้งานครั้งล่าสุด**)

ในขั้นถัดไป โปรแกรมจะแสดงข้อมูลสรุปพร้อมด้วยข้อมูลเกี่ยวกับงานตามกำหนดการปัจจุบัน คลิก **สิ้นสุด** เมื่อคุณแก้ไขจนเสร็จสิ้นแล้ว

หน้าต่างข้อความจะปรากฏ เพื่อให้คุณเลือกโปรไฟล์ที่จะใช้สำหรับงานตามกำหนดการ ในที่นี้คุณจะสามารถตั้งค่าโปรไฟล์หลักและโปรไฟล์รอง โปรไฟล์รองจะใช้ในกรณีที่ไม่สามารถทำงานให้เสร็จสมบูรณ์โดยใช้โปรไฟล์หลัก ยืนยันด้วยการคลิก **สิ้นสุด** และงานตามกำหนดการใหม่จะถูกเพิ่มในรายการของงานตามกำหนดการปัจจุบัน

วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์

หากต้องการวางกำหนดการงานทั่วไป ให้เปิดหน้าต่างโปรแกรมหลัก > **เครื่องมือ** > **เครื่องมือวางกำหนดการณ์** ที่ด้านล่างคือคู่มือสั้นๆ เกี่ยวกับวิธีการวางกำหนดงานที่จะสแกนไดรฟ์ในระบบของคุณในทุกสัปดาห์ ให้ดู บทความฐานความรู้ สำหรับคำแนะนำอย่างละเอียดเพิ่มเติม

เมื่อต้องการวางกำหนดการงานสแกน:

1. คลิก **เพิ่มงาน** ในหน้าจอเครื่องมือวางกำหนดการหลัก
2. เลือก **การสแกนคอมพิวเตอร์ตามต้องการ** จากเมนูแบบเลื่อนลง
3. ป้อนชื่อสำหรับงานแล้วเลือก **รายสัปดาห์สำหรับความถี่ของการทำงาน**
4. ตั้งวันและเวลาที่จะทำงาน
5. เลือก **เรียกใช้งานให้เร็วที่สุดเท่าที่ทำได้** เพื่อทำงานในภายหลังในกรณีที่การเรียกใช้งานตามกำหนดการไม่ทำงานด้วยสาเหตุใดก็ตาม (ตัวอย่างเช่น หากคอมพิวเตอร์ถูกปิดในเวลานั้น)
6. ดูข้อมูลสรุปของงานตามกำหนดการ และคลิกที่ **สิ้นสุด**
7. จากเมนูแบบเลื่อนลง **เป้าหมาย** ให้เลือก **ไดรฟ์ในระบบ**
8. คลิก **สิ้นสุด** เพื่อใช้งาน

วิธีเชื่อมต่อ ESET Endpoint Security กับ ESET PROTECT

เมื่อคุณได้ติดตั้ง ESET Endpoint Security บนคอมพิวเตอร์ของคุณและคุณต้องการเชื่อมต่อผ่าน ESET PROTECT ตรวจสอบให้แน่ใจว่าคุณได้ติดตั้งเอเจนท์ ESET Management บนเวิร์กสเตชันไคลเอ็นต์ไว้แล้วด้วย โดยนี่เป็นส่วนที่จำเป็นของโซลูชันไคลเอ็นต์ทั้งหมดที่สื่อสารกับเซิร์ฟเวอร์ ESET PROTECT

- ติดตั้งหรือปรับใช้เอเจนท์ ESET Management บนเวิร์กสเตชันไคลเอ็นต์

โปรดดู:

- เอกสารประกอบสำหรับอุปกรณ์ปลายทางที่จัดการจากระยะไกล
- วิธีการใช้โหมดเขียนทับ
- วิธีนำนโยบายที่แนะนำไปใช้สำหรับ ESET Endpoint Security

วิธีการใช้โหมดเขียนทับ

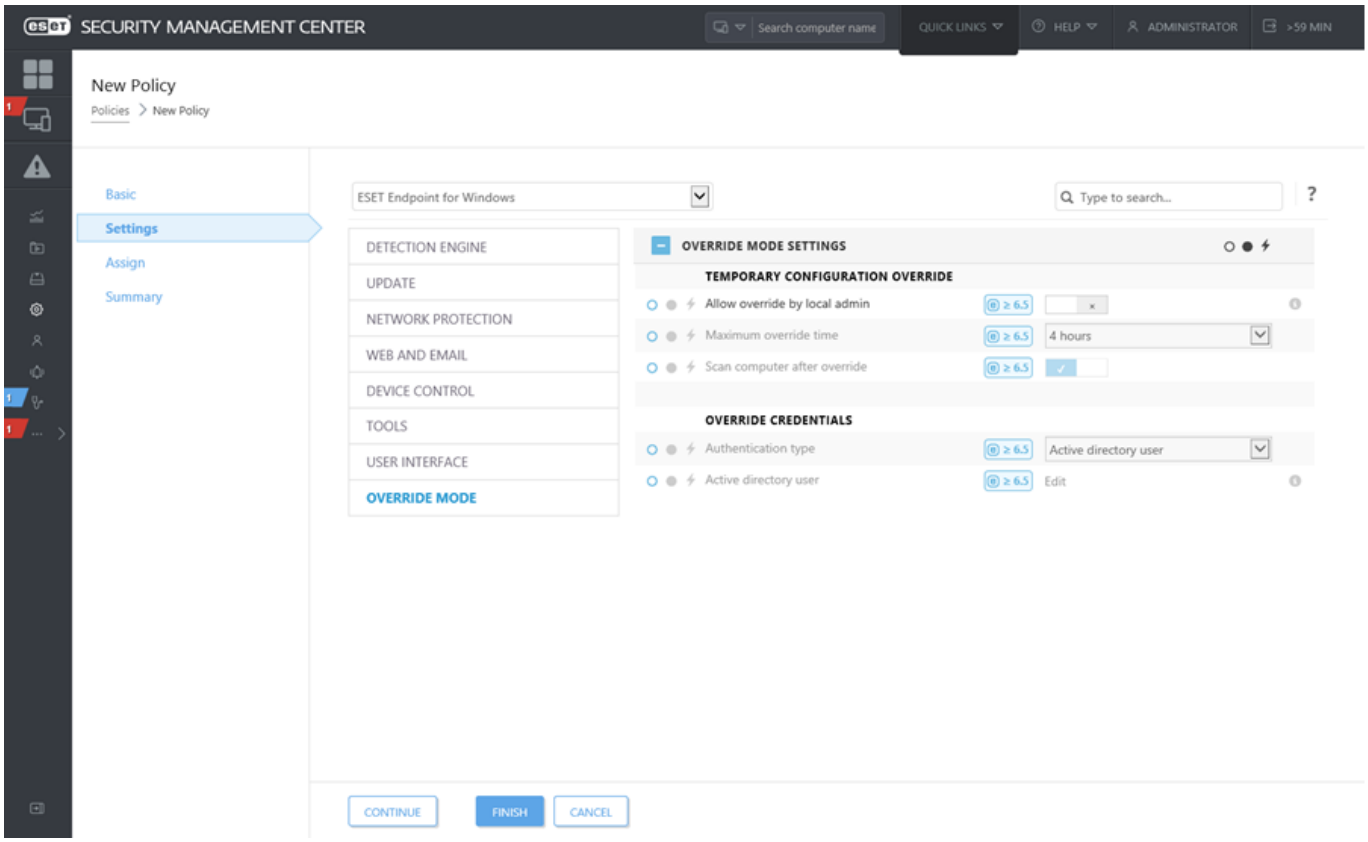
ผู้ใช้ที่มีผลิตภัณฑ์ ESET Endpoint (เวอร์ชัน 6.5 ขึ้นไป) สำหรับ Windows ที่ติดตั้งในเครื่องของผู้ใช้เหล่านั้นจะสามารถใช้คุณลักษณะเขียนทับได้ โหมดเขียนทับจะอนุญาตให้ผู้ใช้ที่อยู่ในระดับคอมพิวเตอร์ไคลเอ็นต์เปลี่ยนแปลงการตั้งค่าในผลิตภัณฑ์ ESET ที่ติดตั้งไว้ แม้ว่าจะมีการใช้นโยบายกับการตั้งค่าเหล่านี้ สามารถเปิดใช้งานโหมดเขียนทับสำหรับผู้ใช้ AD บางรายได้ หรือสามารถป้องกันด้วยรหัสผ่านได้ ฟังก์ชันนี้สามารถเปิดใช้งานได้ครั้งละไม่เกินสี่ชั่วโมง

เมื่อเปิดใช้โหมดเขียนทับแล้วนั้นจะไม่สามารถหยุดการทำงานจากเว็บคอนโซล ESET PROTECT ได้ โหมดเขียนทับจะปิดใช้งานโดนอัตโนมัติเมื่อสิ้นสุดระยะเวลาการเขียนทับ โดยสามารถปิดได้จากเครื่องไคลเอ็นต์เช่นเดียวกัน
ผู้ใช้ที่ใช้โหมดเขียนทับจำเป็นต้องมีสิทธิ์ของผู้แลระบบ Windows ด้วยเช่นกัน มิฉะนั้นผู้ใช้จะไม่สามารถบันทึกการเปลี่ยนแปลงในการตั้งค่าของ ESET Endpoint Security ได้
ระบบรองรับการเปิดใช้งานการตรวจสอบสิทธิ์กลุ่ม Active Directory

หากต้องการตั้งค่า**โหมดเขียนทับ** ให้ทำดังนี้:

1. ไปที่ **นโยบาย** > **นโยบายใหม่**
2. ใน ส่วน**พื้นฐาน** ให้ป้อน**ชื่อ** และ**คำอธิบาย** สำหรับนโยบายนี้
3. ใน ส่วน**การตั้งค่า** ให้เลือก **ESET Endpoint สำหรับ Windows**
4. คลิก **โหมดเขียนทับ** แล้วกำหนดค่ากฎสำหรับโหมดเขียนทับ
5. ใน ส่วน**กำหนด** ให้เลือกคอมพิวเตอร์หรือกลุ่มคอมพิวเตอร์ที่จะใช้กับนโยบายนี้

6. ตรวจดูการตั้งค่าใน ส่วน**ข้อมูลสรุป** แล้วคลิก **สิ้นสุด** เพื่อใช้นโยบาย



หาก *John* มีปัญหาเกี่ยวกับการตั้งค่าอุปกรณ์ปลายทางของเขา ซึ่งปิดกั้นฟังก์ชันการทำงานหรือการเข้าถึงเว็บที่สำคัญบางอย่างในเครื่อง ผู้ดูแลสามารถอนุญาตให้ *John* เขียนทับนโยบายอุปกรณ์ปลายทางที่มีอยู่ของเขาและปรับแต่งการตั้งค่าด้วยตัวเองในเครื่องได้ หลังจากนั้น ESET PROTECT จะสามารถร้องขอการตั้งค่าใหม่เหล่านี้ได้ ดังนั้นผู้ดูแลจะสามารถสร้างนโยบายใหม่ขึ้นจากการตั้งค่าเหล่านั้นได้
หากต้องการทำเช่นนั้น ให้ทำตามขั้นตอนด้านล่าง:
1. ไปที่ **นโยบาย** > **นโยบายใหม่**
2. กรอกลงในช่อง**ชื่อ**และ**คำอธิบาย**ให้เสร็จสมบูรณ์ ใน ส่วน**การตั้งค่า** ให้เลือก **ESET Endpoint สำหรับ Windows**
3. คลิก **โหมดเขียนทับ** เปิดใช้งานโหมดเขียนทับเป็นเวลาหนึ่งชั่วโมง แล้วเลือก *John* เป็นผู้ใช้ AD
4. กำหนดนโยบายไปที่ คอมพิวเตอร์ของ *John* แล้วคลิก **สิ้นสุด** เพื่อบันทึกนโยบาย
5. *John* จำเป็นต้องเปิดใช้งาน **โหมดเขียนทับ** ใน ESET Endpoint ของเขา และเปลี่ยนการตั้งค่าด้วยตัวเองในเครื่องของเขา
6. ในเว็บคอนโซล ESET PROTECT ให้ไปที่ **คอมพิวเตอร์** เลือก คอมพิวเตอร์ของ *John* แล้วคลิก **แสดงรายละเอียด**
7. ในส่วน**การกำหนดค่า** ให้คลิก **ขอการกำหนดค่า** เพื่อวางกำหนดการงานไคลเอ็นต์เพื่อรับการกำหนดค่าจากไคลเอ็นต์ ASAP
8. หลังผ่านไปสักครู่หนึ่ง การกำหนดค่ารายการใหม่จะปรากฏขึ้น คลิกที่ผลิตภัณฑ์ที่มีการตั้งค่าที่คุณต้องการบันทึก จากนั้นคลิก **เปิดการกำหนดค่า**
9. คุณสามารถตรวจดูการตั้งค่า แล้วคลิก **แปลงเป็นนโยบาย** ได้
10. กรอกลงในช่อง**ชื่อ**และ**คำอธิบาย**ให้เสร็จสมบูรณ์
11. ในส่วน**การตั้งค่า** คุณจะสามารถแก้ไขการตั้งค่าได้หากจำเป็น
12. ในส่วน**กำหนด** คุณสามารถกำหนดนโยบายนี้ไปที่คอมพิวเตอร์ของ *John* (หรือบุคคลอื่น) ได้
13. คลิก **สิ้นสุด** เพื่อบันทึกการติดตั้งได้
14. อย่าลืมลบนโยบายเขียนทับเมื่อไม่ต้องการใช้อีกต่อไปแล้ว

วิธีนำนโยบายที่แนะนำไปใช้สำหรับ ESET Endpoint Security

แนวทางปฏิบัติหลังการเชื่อมต่อ ESET Endpoint Security กับ ESET PROTECT คือการนำนโยบายที่แนะนำไปใช้หรือใช้นโยบายที่กำหนดเอง

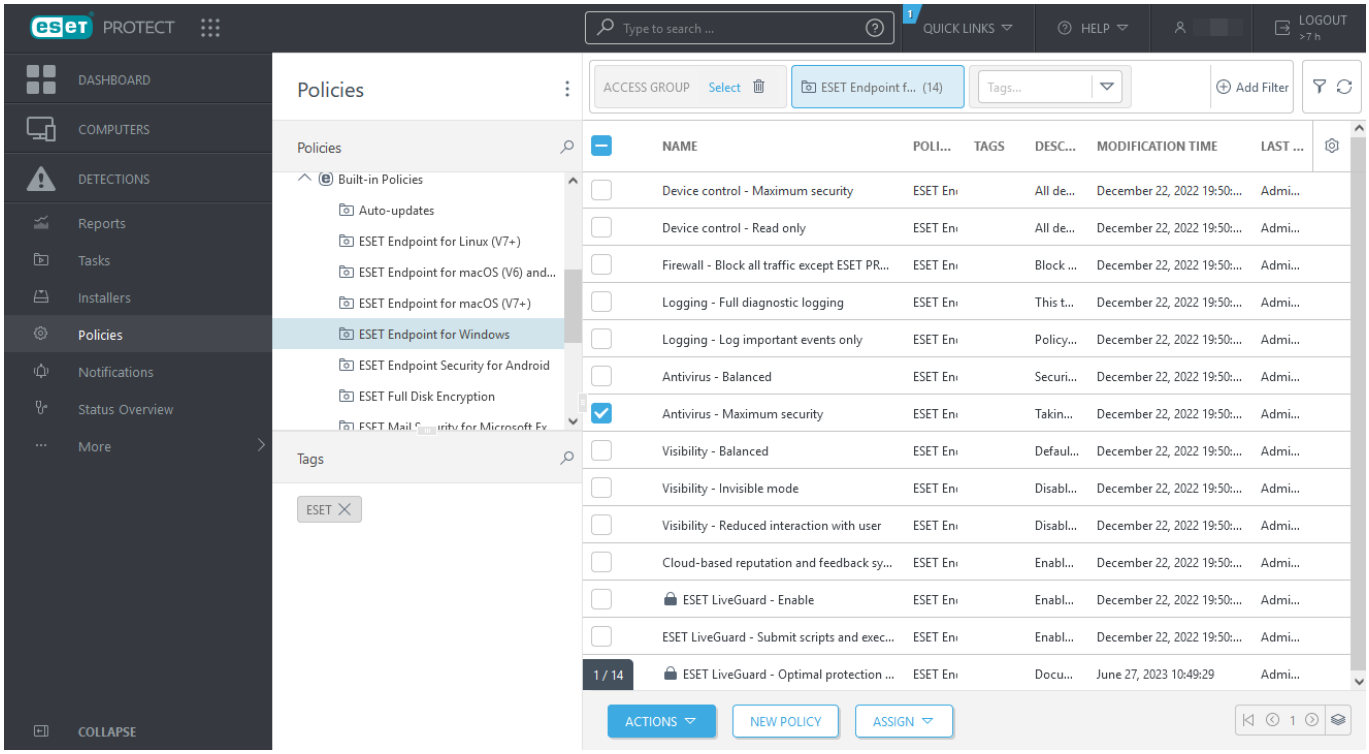
โดยมีนโยบายภายในตัวที่หลากหลายสำหรับ ESET Endpoint Security:

นโยบาย	คำอธิบาย
การป้องกันไวรัส - สมดุล	การกำหนดค่าความปลอดภัยที่แนะนำสำหรับการตั้งค่าส่วนใหญ่
การป้องกันไวรัส - ความปลอดภัยสูงสุด	ใช้ประโยชน์จากการเรียนรู้ของเครื่อง การตรวจสอบการทำงานเชิงลึก และการกรอง SSL การตรวจหาแอพพลิเคชันที่อาจไม่ปลอดภัย อาจไม่พึงประสงค์ และน่าสงสัยจะได้รับผลกระทบ
ระบบความเชื่อถือที่อ้างอิงระบบคลาวด์และระบบคำติชม	เปิดใช้งานระบบความเชื่อถือที่อ้างอิงระบบคลาวด์ ESET LiveGrid® เช่นเดียวกับระบบคำติชมเพื่อปรับปรุงการตรวจหาภัยคุกคามล่าสุดและช่วยแบ่งปันสิ่งที่อาจเป็นภัยคุกคามที่ไม่รู้จักหรือเป็นอันตรายสำหรับการวิเคราะห์เพิ่มเติม
การควบคุมอุปกรณ์ - ความปลอดภัยสูงสุด	อุปกรณ์ทั้งหมดจะถูกปิดกั้น เมื่อมีอุปกรณ์ใดๆ ก็ตามต้องการเชื่อมต่อ อุปกรณ์นั้นต้องได้รับอนุญาตจากผู้ดูแลระบบก่อน
การควบคุมอุปกรณ์ - อ่านอย่างเดียว	อุปกรณ์ทั้งหมดสามารถอ่านได้อย่างเดียวเท่านั้น โดยจะไม่ได้รับอนุญาตให้เขียน
ไฟร์วอลล์ - ปิดกั้นการรับส่งข้อมูลทั้งหมดยกเว้นการเชื่อมต่อของ ESET PROTECT และ ESET Inspect	ปิดกั้นการรับส่งข้อมูลทั้งหมดยกเว้นการเชื่อมต่อกับ ESET PROTECT และ เซิร์ฟเวอร์ ESET Inspect (เฉพาะ ESET Endpoint Security)
การบันทึก - การบันทึกสำหรับการวินิจฉัยเต็มรูปแบบ	เทมเพลตนี้เป็นการทำให้แน่ใจว่าผู้ดูแลระบบจะมีบันทึกทั้งหมดให้ใช้งานเมื่อต้องการ โดยทุกเหตุการณ์จะถูกบันทึกไว้ทั้งหมดตั้งแต่เหตุการณ์ความละเอียดขั้นต่ำซึ่งประกอบด้วย HIPS และThreatSense รวมถึงไฟร์วอลล์ โดยบันทึกจะถูกลบโดยอัตโนมัติหลังผ่านไป 90 วัน
การบันทึก - บันทึกเหตุการณ์สำคัญเท่านั้น	นโยบายเป็นการทำให้แน่ใจว่าคำเตือน ข้อผิดพลาด และเหตุการณ์ร้ายแรงจะได้รับการบันทึก โดยบันทึกจะถูกลบโดยอัตโนมัติหลังผ่านไป 90 วัน
การมองเห็น - สมดุล	ค่าเริ่มต้นสำหรับการมองเห็น เปิดใช้งานสถานะและการแจ้งเตือนแล้ว
การมองเห็น - โหมดมองไม่เห็น	ปิดใช้งานการแจ้งเตือน, การเตือน, GUI, การรวมเข้ากับเมนูบริบท ไม่มี egui.exe ที่จะเรียกใช้ได้ เหมาะสำหรับการจัดการจาก ESET PROTECT Cloudเพียงอย่างเดียว
การมองเห็น - ลดการโต้ตอบกับผู้ใช้	ปิดใช้งานสถานะแล้ว, ปิดใช้งานการแจ้งเตือนแล้ว, GUI ปรากฏ

หากต้องการกำหนดนโยบายที่มีชื่อว่า **การป้องกันไวรัส - ความปลอดภัยสูงสุด** ซึ่งบังคับใช้การตั้งค่าที่แนะนำมากกว่า 50 รายการสำหรับ ESET Endpoint Security ที่ติดตั้งบนเวิร์กสเตชันของคุณ ให้ดำเนินการตามขั้นตอนต่อไปนี้:

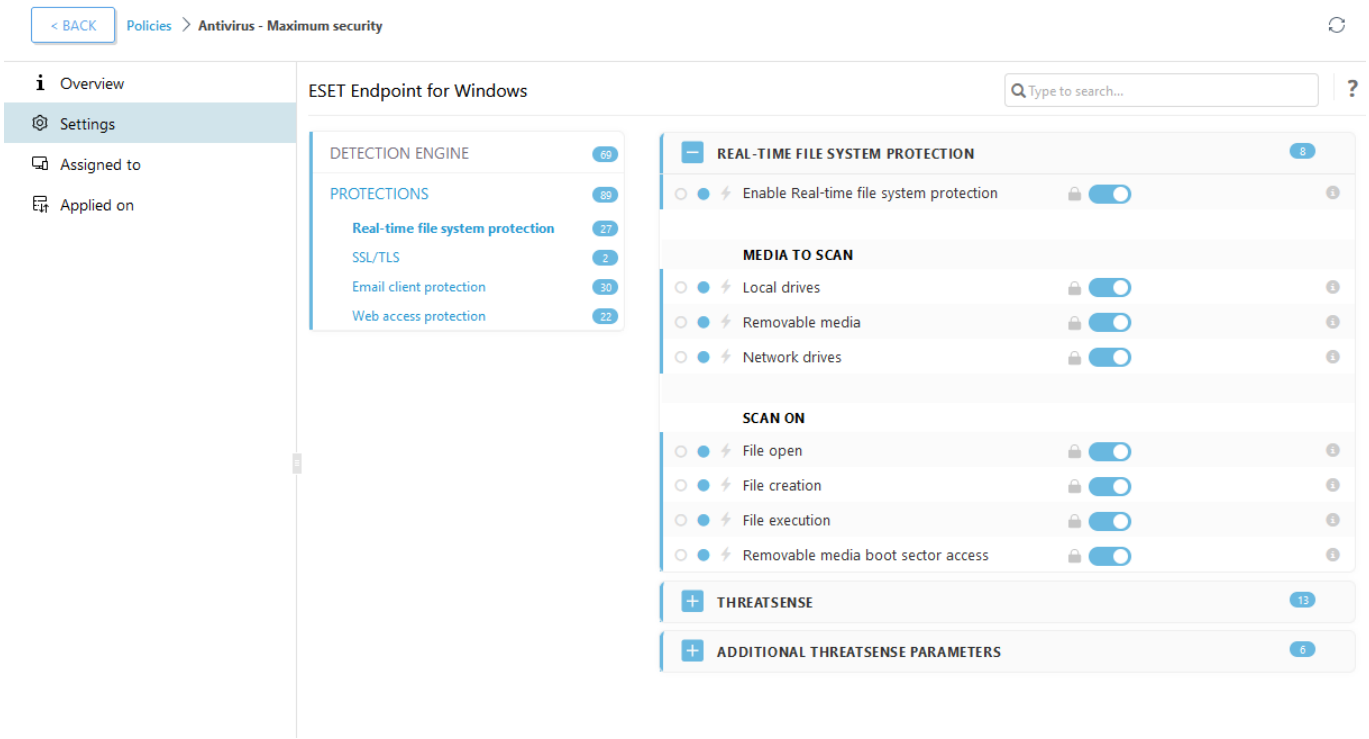
บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
นำนโยบายที่แนะนำหรือที่กำหนดไว้ล่วงหน้าไปใช้สำหรับ ESET Endpoint Security โดยใช้ ESET PROTECT

1. เปิดเว็บคอนโซล ESET PROTECT
2. ไปที่ **นโยบาย** และขยาย **นโยบายภายในตัว** > **ESET Endpoint สำหรับ Windows**
3. คลิก **การป้องกันไวรัส – ความปลอดภัยสูงสุด – แนะนำ**
4. ในแท็บ **กำหนดไปยัง** แล้วคลิก **กำหนดไคลเอ็นต์** หรือ **กำหนดกลุ่ม** และเลือกคอมพิวเตอร์ที่เหมาะสมซึ่งคุณต้องการปรับใช้นโนบายนี้



หากต้องการดูว่าการตั้งค่าใดที่ใช้กับนโยบายนี้ ให้คลิกแท็บ **การตั้งค่า** และขยายโครงสร้างการตั้งค่าขั้นสูง

- จุดสีฟ้าจะแสดงการตั้งค่าที่มีการแก้ไขสำหรับนโยบายนี้
- หมายเลขในกรอบสีฟ้าจะแสดงจำนวนของการตั้งค่าที่มีการแก้ไขโดยนโยบายนี้
- อ่านเพิ่มเติมเกี่ยวกับนโยบาย ESET PROTECT ได้ที่นี่



วิธีกำหนดค่ามิเรอร์

คุณสามารถกำหนดค่า ESET Endpoint Security ให้เก็บสำเนาของไฟล์อัพเดทกลไกการตรวจจับและแจกจ่ายการอัพเดทไปยังเวิร์กสเตชันอื่นที่เรียกใช้ ESET Endpoint Antivirus หรือ ESET Endpoint Security ได้

มิเรอร์อัพเดทจะสร้างสำเนาไฟล์อัพเดทที่ใช้ในการอัพเดทเวิร์กสเตชันที่กำลังเรียกใช้ ESET Endpoint Security รุ่นเดียวกันสำหรับ Windows (ตัวอย่างเช่น ESET Endpoint Security สำหรับ Windows เวอร์ชัน 10.x จะสร้างไฟล์อัพเดทเฉพาะสำหรับเวอร์ชัน 10.x ESET Endpoint Antivirus สำหรับ Windows และ ESET Endpoint Security สำหรับ Windows)

การกำหนดค่า ESET Endpoint Security เป็นเซิร์ฟเวอร์มิเรอร์เพื่อให้การอัพเดทผ่านเซิร์ฟเวอร์ HTTP ภายใน

1. กด **F5** เพื่อเข้าถึงการตั้งค่าขั้นสูง แล้วขยาย **อัพเดท** > **โปรไฟล์** > **มิเรอร์การอัพเดท**
2. ขยาย **อัพเดท** และทำให้มั่นใจว่าตัวเลือก **เลือกโดยอัตโนมัติ** ใต้ **การอัพเดทโมดูล** ถูกเปิดใช้งานแล้ว
3. ขยาย **มิเรอร์การอัพเดท** และเปิดใช้งาน **สร้างการอัพเดทมิเรอร์** และ **เปิดใช้งานเซิร์ฟเวอร์ HTTP**

หากต้องการข้อมูลเพิ่มเติม โปรดดู
- มิเรอร์การอัพเดท
- การอัพเดทจากมิเรอร์

การกำหนดค่าเซิร์ฟเวอร์มิเรอร์เพื่อให้การอัพเดทผ่านโฟลเดอร์เครือข่ายที่ใช้ร่วมกัน

1. สร้างโฟลเดอร์ที่ใช้งานร่วมกันบนอุปกรณ์ในระบบหรืออุปกรณ์เครือข่าย ผู้ใช้ทุกคนที่เรียกใช้โซลูชันรักษาความปลอดภัย ESET ต้องสามารถอ่านโฟลเดอร์นี้ได้ และบัญชีของระบบภายในต้องสามารถเขียนโฟลเดอร์นี้ได้
2. เปิดใช้งาน **สร้างอัพเดทมิเรอร์** ใต้ **การตั้งค่าขั้นสูง** > **อัพเดท** > **โปรไฟล์** > **มิเรอร์การอัพเดท**
3. สร้าง **โฟลเดอร์พื้นที่เก็บข้อมูล** ที่เหมาะสม โดยการคลิก **ล้าง** จากนั้น **แก้ไข** เรียกดูและเลือกโฟลเดอร์ที่ใช้ร่วมกันที่สร้างไว้

หากคุณไม่ต้องการให้การอัพเดทโมดูลผ่านทางเซิร์ฟเวอร์ HTTP ภายใน ให้ปิดใช้งาน**เปิดใช้งานเซิร์ฟเวอร์ HTTP**

ฉันจะอัพเกรดเป็น Windows 10 ด้วย ESET Endpoint Security ได้อย่างไร

เราแนะนำเป็นอย่างยิ่งให้คุณอัพเกรดผลิตภัณฑ์ ESET เป็นเวอร์ชันล่าสุด จากนั้นจึงดาวน์โหลดการอัพเดทโมดูลล่าสุดก่อนอัพเกรดเป็น Windows 10 การกระทำนี้จะทำให้ได้การป้องกันระดับสูงสุดและจะเก็บรักษาการตั้งค่าโปรแกรมและข้อมูลใบอนุญาตของคุณระหว่างอัพเกรดเป็น Windows 10

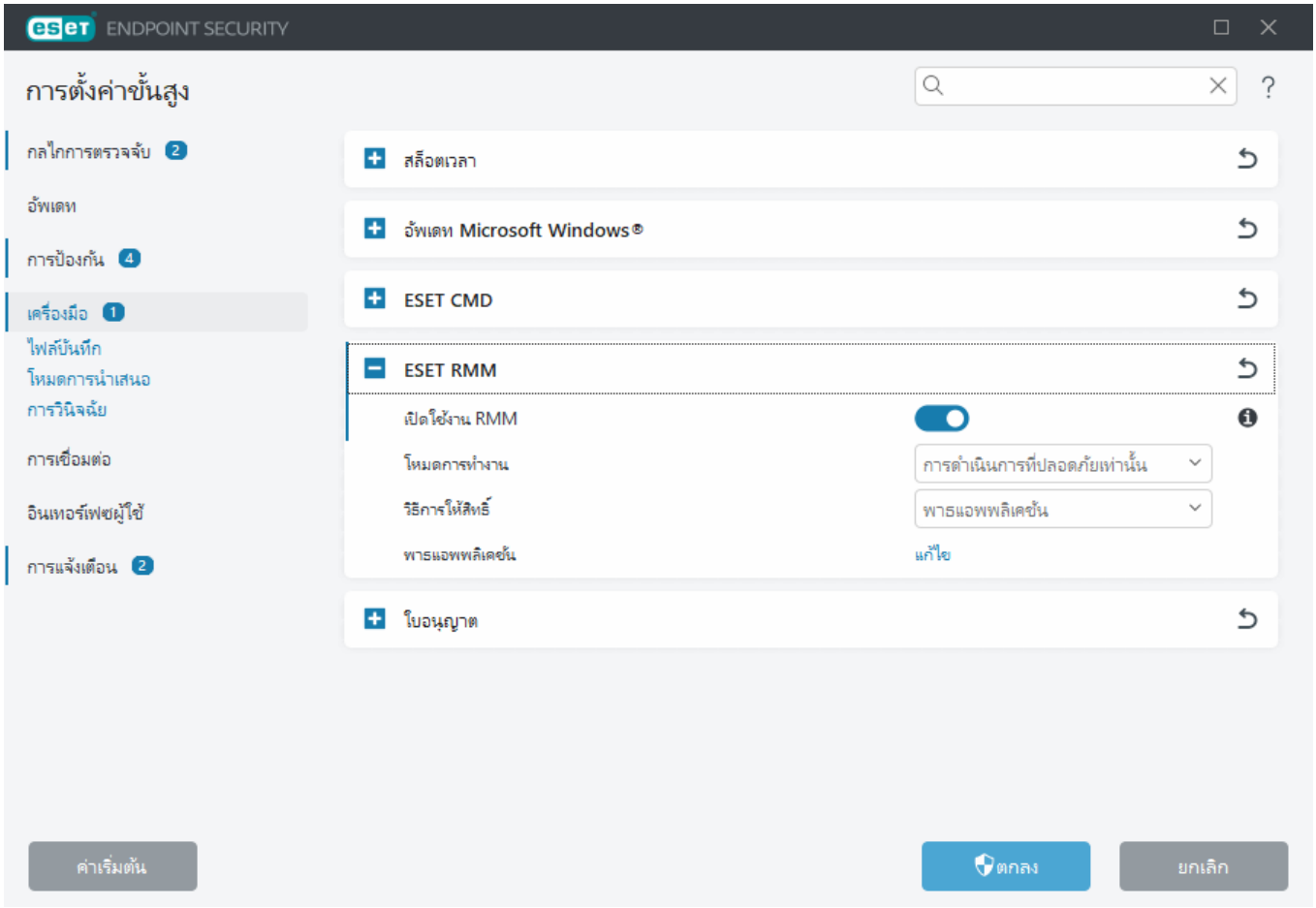
เวอร์ชันสำหรับภาษาอื่นๆ :

หากคุณกำลังมองหาผลิตภัณฑ์เอ็นพอยต์ ESET ในเวอร์ชันภาษาอื่น ให้ไปที่ หน้าดาวน์โหลด ของเรา

ข้อมูลเพิ่มเติมเกี่ยวกับความเข้ากันได้ของผลิตภัณฑ์ ESET สำหรับธุรกิจกับ Windows 10

วิธีเปิดใช้งานการตรวจสอบและการจัดการระยะไกล

การตรวจสอบและการจัดการระยะไกล (RMM) เป็นกระบวนการในการดูแลและควบคุมระบบซอฟต์แวร์ (เช่น ระบบซอฟต์แวร์ที่อยู่บนเดสก์ท็อป เซิร์ฟเวอร์ และอุปกรณ์เคลื่อนที่ต่างๆ) โดยใช้ตัวแทนที่ติดตั้งในระบบที่ผู้ให้บริการด้านการจัดการสามารถเข้าถึงได้ ESET Endpoint Security สามารถจัดการได้โดย RMM ตั้งแต่เวอร์ชัน 6.6.2028.0



ESET RMM จะปิดใช้งานตามค่าเริ่มต้น หากต้องการเปิดใช้งาน ESET RMM ให้เปิด **การตั้งค่าขั้นสูง** > **เครื่องมือ** > **ESET RMM** และเปิดใช้งานปุ่มสลับถัดจาก เปิดใช้งาน RMM

โหมดการทำงาน – เลือก **การดำเนินการที่ปลอดภัยเท่านั้น** หากคุณต้องการเปิดใช้งานอินเทอร์เฟซ RMM สำหรับการดำเนินการแบบอ่านอย่างเดียวและปลอดภัยเท่านั้น ให้เลือก **การดำเนินการทั้งหมด** หากคุณต้องการเปิดใช้งานอินเทอร์เฟซ RMM สำหรับการดำเนินการทั้งหมด

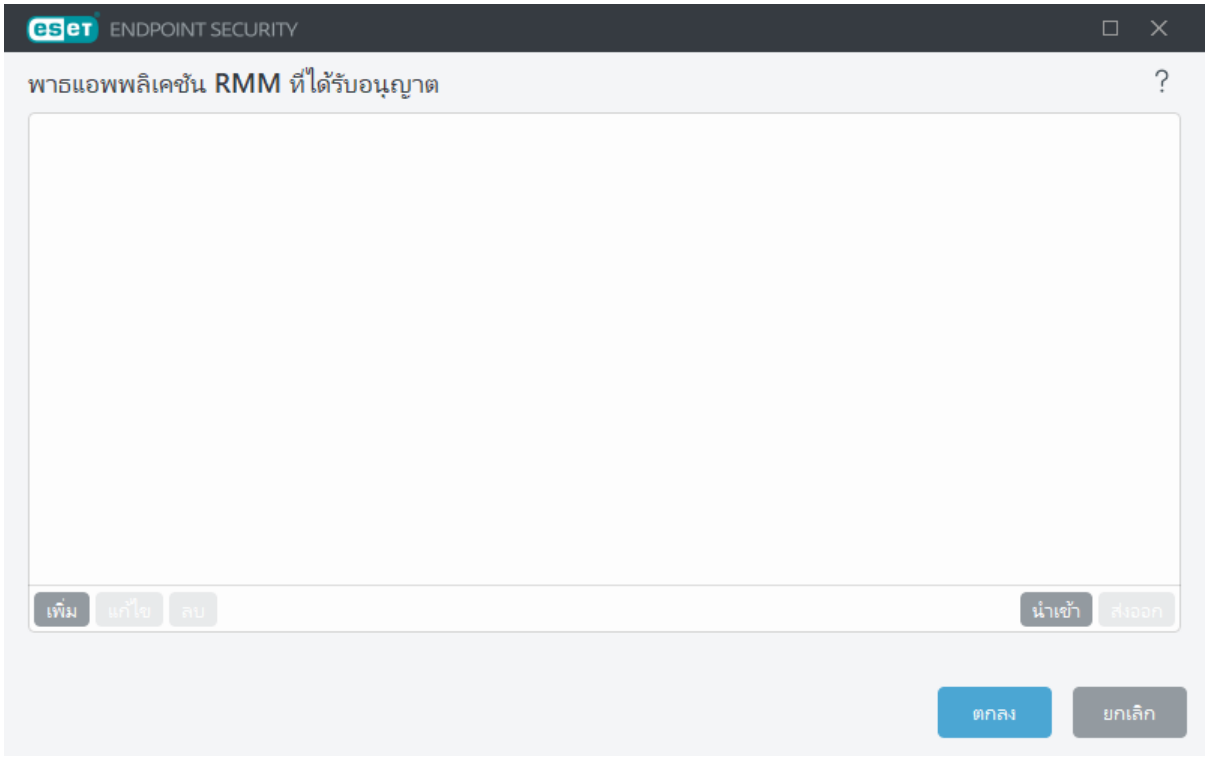
การดำเนินการ	โหมดการดำเนินการที่ปลอดภัยเท่านั้น	โหมดการดำเนินการทั้งหมด
ขอข้อมูลแอพพลิเคชัน	✔	✔
ขอการกำหนดค่า	✔	✔
ขอข้อมูลใบอนุญาต	✔	✔
ขอบันทึก	✔	✔
สถานะของการป้องกัน	✔	✔
ขอสถานะการอัพเดท	✔	✔
ตั้งค่าการกำหนดค่า		✔
เริ่มเปิดการใช้งาน		✔
เริ่มสแกน	✔	✔
เริ่มอัพเดท	✔	✔

วิธีการให้สิทธิ์ – ตั้งค่าวิธีการให้สิทธิ์ RMM ถ้าต้องการใช้การให้สิทธิ์ ให้เลือก **พาธแอพพลิเคชัน** จากเมนูแบบ

เลื่อนลง หรือเลือก **ไม่มี**

RMM ควรใช้การให้สิทธิ์ทุกครั้งเพื่อป้องกันซอฟต์แวร์ที่เป็นอันตรายไม่ให้ปิดใช้งานหรือหลีกเลี่ยงการป้องกันของ ESET Endpoint

พาธแอพพลิเคชัน – แอพพลิเคชันที่เจาะจงซึ่งได้รับอนุญาตให้เรียกใช้ RMM ถ้าคุณได้เลือก **พาธแอพพลิเคชัน** เป็นวิธีการให้สิทธิ์ ให้คลิก **แก้ไข** เพื่อเปิดหน้าต่างการกำหนดค่า **พาธแอพพลิเคชัน RMM ที่ได้รับอนุญาต**



เพิ่ม – สร้างพาธแอพพลิเคชัน RMM ที่ได้รับอนุญาตใหม่ ป้อนพาธหรือคลิกปุ่ม **...** เพื่อเลือกพาธที่เรียกใช้ได้

แก้ไข – แก้ไขพาธที่ได้รับอนุญาตที่มีอยู่ ใช้ **แก้ไข** ถ้าตำแหน่งของพาธที่เรียกใช้ได้เปลี่ยนเป็นโฟลเดอร์อื่น

ลบ – ลบพาธที่ได้รับอนุญาตที่มีอยู่

การติดตั้ง ESET Endpoint Security เริ่มต้นประกอบด้วยไฟล์ ermm.exe ที่อยู่ในไดเรกทอรีแอพพลิเคชัน Endpoint (พาธเริ่มต้น C:*Program Files**ESET**ESET Security*) ไฟล์ ermm.exe แลกเปลี่ยนข้อมูลกับปลั๊กอิน RMM ซึ่งสื่อสารกับ RMM Agent โดยลิงค์ไปที่เซิร์ฟเวอร์ RMM

- ermm.exe – ยูทิลิตีบรรทัดคำสั่งที่พัฒนาโดย ESET ซึ่งอนุญาตให้มีการจัดการผลิตภัณฑ์ Endpoint และการสื่อสารกับปลั๊กอิน RMM
- ปลั๊กอิน RMM เป็นแอพพลิเคชันของบริษัทอื่นที่ทำงานบนระบบ Endpoint Windows ปลั๊กอินได้รับการออกแบบมาเพื่อสื่อสารกับ RMM Agent ที่ระบุ (เช่น Kaseya เท่านั้น) และกับ ermm.exe
- RMM Agent เป็นแอพพลิเคชันของบริษัทอื่น (เช่น จาก Kaseya) ที่ทำงานบนระบบ Endpoint Windows Agent

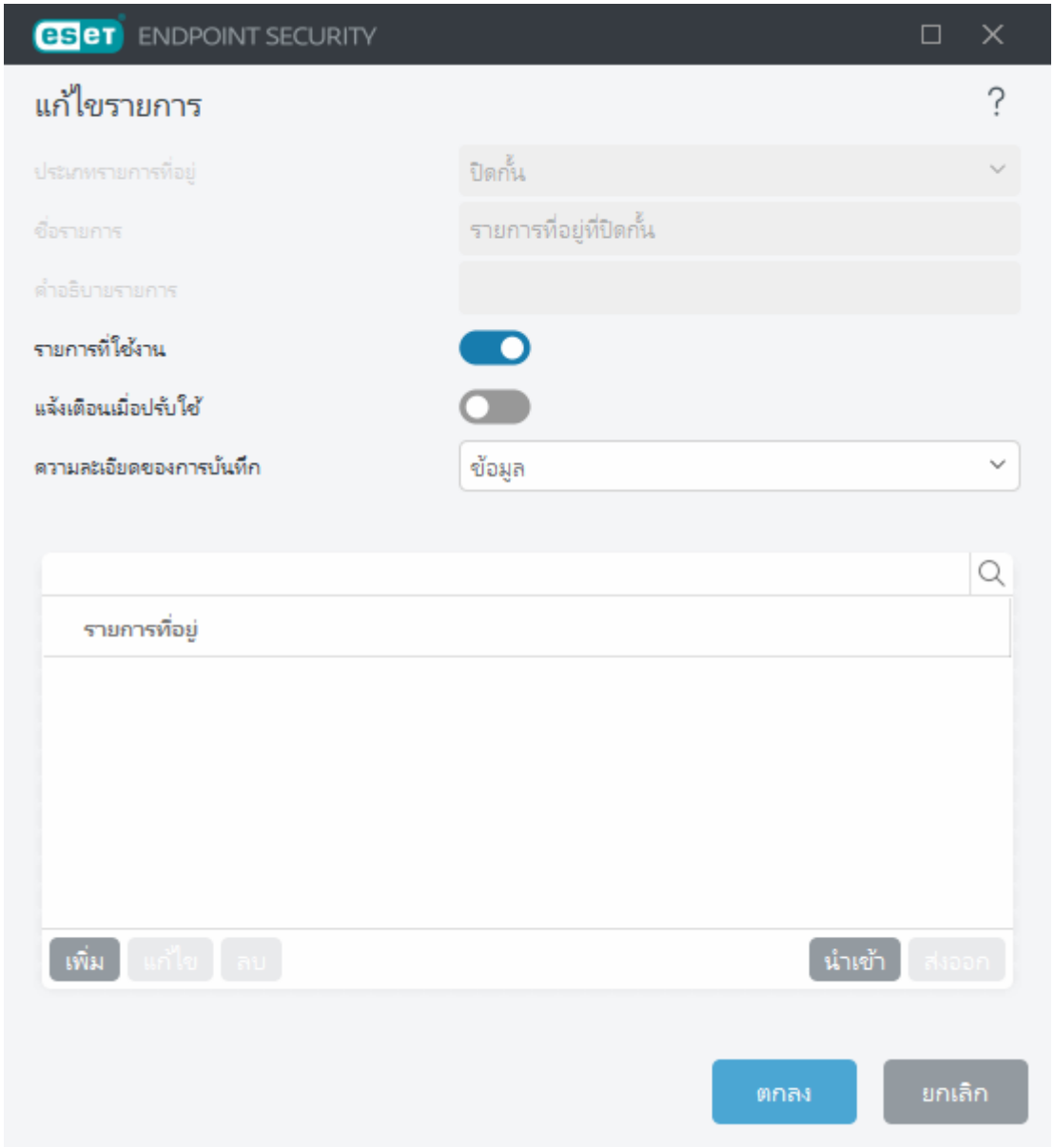
วิธีการปิดกั้นการดาวน์โหลดของประเภทไฟล์บางประเภทจากอินเทอร์เน็ต

หากคุณไม่ต้องการให้ดาวน์โหลดประเภทไฟล์บางประเภท (เช่น exe, pdf หรือ zip) จากอินเทอร์เน็ต ให้ใช้ การจัดการที่อยู่ URL พร้อมอักขระตัวแทนต่างๆ รวมกัน กดแป้น F5 เพื่อเข้าถึง **การตั้งค่าขั้นสูง** คลิก **เว็บและอีเมล** > **การป้องกันการเข้าถึงเว็บ** แล้วขยาย **การจัดการที่อยู่ URL** คลิก **แก้ไข** ที่อยู่ถัดจาก **รายการที่อยู่**

ในหน้าต่าง **รายการที่อยู่** ให้เลือก**รายการที่อยู่ที่ถูกบล็อก** และคลิก **แก้ไข** หรือ **เพิ่ม** เพื่อสร้าง/แก้ไขรายการ หน้าต่างใหม่เปิดขึ้น หากคุณต้องการสร้างรายการใหม่ ให้เลือก**ที่ปิดกั้น**จากเมนู**ประเภทรายการที่อยู่**และเลื่อนลงและตั้งชื่อรายการ หากคุณต้องการรับการแจ้งเตือนเมื่อเข้าถึงไฟล์ที่ประเภทของไฟล์ดังกล่าวแสดงอยู่ในรายการปัจจุบัน ให้เปิดใช้งานปุ่มสลับ **แจ้งเตือนเมื่อเกี่ยวข้อง** เลือก **ระดับความรุนแรงของการบันทึก** จากเมนูแบบเลื่อนลง ESET PROTECT สามารถเก็บรวบรวมข้อมูลบันทึกได้ด้วยการจัดให้อยู่ในประเภท **คำเตือน**

ความละเอียดการบันทึก ข้อมูล และ คำเตือน จะมีให้ใช้งานสำหรับกฎที่มีองค์ประกอบที่ไม่มีอักขระตัวแทนอย่างน้อยสององค์ประกอบภายในโดเมนเท่านั้น ตัวอย่างเช่น:

- *.domain.com/*
- *www.domain.com/*



คลิก **เพิ่ม** เพื่อป้อนมาสก์ที่ระบุประเภทไฟล์ที่คุณต้องการปิดกั้นไม่ให้ดาวน์โหลด ป้อน URL แบบเต็มหากต้องการปิดกั้นการดาวน์โหลดไฟล์บางประเภทจากเว็บไซต์บางเว็บ ตัวอย่างเช่น *http://example.com/file.exe* คุณสามารถใช้อักขระตัวแทนเพื่อแทนกลุ่มของไฟล์ เครื่องหมายคำถาม (?) แสดงถึงอักขระตัวแปรเดียว โดยที่เครื่องหมายดอกจัน (*) แสดงถึงสตริงตัวแปรตั้งแต่ศูนย์อักขระขึ้นไป ตัวอย่างเช่น มาสก์ **/*.zip* จะบล็อกไฟล์ zip ที่บีบอัดทั้งหมดจากการดาวน์โหลด

โปรดทราบว่าคุณสามารถปิดกั้นเฉพาะการดาวน์โหลดประเภทของไฟล์ที่เฉพาะเจาะจงได้โดยใช้วิธีนี้เมื่อส่วนขยายของไฟล์เป็นส่วนหนึ่งของ URL ของไฟล์ หากหน้าเว็บใช้ URL สำหรับการดาวน์โหลดไฟล์ ตัวอย่างเช่น *www.example.com/download.php?fileid=42* ไฟล์ใดๆ ก็ตามที่อยู่ในลิงค์นี้จะดาวน์โหลดเสมอแม้ว่าไฟล์นั้นจะมีส่วนขยายที่ถูกคุณปิดกั้นก็ตาม

วิธีการย่อส่วนติดต่อกับผู้ใช้ของ ESET Endpoint Security

เมื่อจัดการจากระยะไกล คุณสามารถนำนโยบาย "การมองเห็น" ที่กำหนดไว้ล่วงหน้าไปใช้ได้

หากไม่เช่นนั้น ให้ทำขั้นตอนต่อไปนี้ด้วยตนเอง:

1. กด **F5** เพื่อเข้าถึงการตั้งค่าขั้นสูงและขยาย **ส่วนติดต่อกับผู้ใช้** > **องค์ประกอบของส่วนติดต่อกับผู้ใช้**
2. ตั้งค่า**โหมดเริ่ม**ให้เป็นค่าที่ต้องการ ข้อมูลเพิ่มเติมเกี่ยวกับโหมดเริ่ม
3. ปิดใช้งาน**แสดงหน้าจอเริ่มต้นเมื่อเริ่มระบบ**และ**ใช้สัญญาณเสียง**
4. กำหนดค่าการแจ้งเตือน
5. กำหนดค่าสถานะแอพพลิเคชัน
6. กำหนดค่าข้อความการยืนยัน
7. กำหนดค่ากล่องการแจ้งเตือนและกล่องข้อความ

ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง

มีผลตั้งแต่วันที่ 19 ตุลาคม 2021

ข้อมูลสำคัญ: โปรดอ่านข้อกำหนดและเงื่อนไขของการใช้งานผลิตภัณฑ์ที่กำหนดไว้ด้านล่างนี้อย่างถี่ถ้วนก่อนที่จะดาวน์โหลด ติดตั้ง คัดลอก หรือใช้งาน **เมื่อคุณดาวน์โหลด ติดตั้ง คัดลอก หรือใช้ซอฟต์แวร์นี้ จะถือว่าคุณแสดงความยินยอมตามข้อกำหนดและเงื่อนไขเหล่านี้และคุณยอมรับ นโยบายความเป็นส่วนตัว**

ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง

ภายใต้ข้อตกลงการอนุญาตใช้งานสำหรับผู้ใช้ปลายทาง ("ข้อตกลง") นี้ ดำเนินการโดยและระหว่าง ESET, spol. s r. o. ซึ่งมีสำนักงานที่จดทะเบียนอยู่ที่ Einsteinova 24, 85101 Bratislava, Slovak Republic และจดทะเบียนในทะเบียนการค้าที่ได้รับการควบคุมดูแลโดย Bratislava I District Court, Section Sro, เลขที่ 3586/B หมายเลขทะเบียนธุรกิจ: 31333532 ("ESET" หรือ “ผู้ให้บริการ”) กับคุณ ซึ่งเป็นบุคคลธรรมดาหรือนิติบุคคล (“คุณ" หรือ "ผู้ใช้ปลายทาง”) คุณได้รับสิทธิ์ให้สามารถใช้ซอฟต์แวร์ที่กำหนดในข้อ 1 ของข้อตกลงนี้ ซอฟต์แวร์ที่กำหนดในข้อ 1 ของข้อตกลงนี้อาจจัดเก็บอยู่ในสื่อจัดเก็บข้อมูล ส่งทางอีเมล ดาวน์โหลดจากอินเทอร์เน็ต ดาวน์โหลดจากเซิร์ฟเวอร์ของผู้ให้บริการ หรือได้รับจากแหล่งอื่นๆ ตามข้อกำหนดและเงื่อนไขที่ระบุไว้ด้านล่างนี้

ข้อตกลงนี้เป็นข้อตกลงเกี่ยวกับสิทธิของผู้ใช้ปลายทางและไม่ใช่ข้อตกลงสำหรับการจำหน่าย ผู้ให้บริการยังคงเป็นเจ้าของสำเนาของซอฟต์แวร์ และสื่อทางกายภาพที่บรรจุในบรรจุภัณฑ์เชิงพาณิชย์ รวมถึงสำเนาอื่นๆ ของซอฟต์แวร์ที่ผู้ใช้ปลายทางได้รับอนุญาตตามข้อตกลงนี้

เมื่อคลิกที่ตัวเลือก "ฉันยอมรับ" หรือ "ฉันยอมรับ..." ในระหว่างการติดตั้ง ดาวน์โหลด คัดลอก หรือใช้ซอฟต์แวร์ จะถือว่าคุณยอมรับข้อกำหนดและเงื่อนไขของข้อตกลงนี้และรับทราบถึงนโยบายความเป็นส่วนตัว ถ้าคุณไม่ยอมรับข้อกำหนดและเงื่อนไขทั้งหมดของข้อตกลงนี้และ/หรือนโยบายความเป็นส่วนตัว โปรดคลิกที่ตัวเลือกการยกเลิกทันที ยกเลิกการติดตั้งหรือการดาวน์โหลด หรือทำลายหรือส่งคืนซอฟต์แวร์ สื่อการติดตั้ง รวมทั้งเอกสารประกอบ และใบเสร็จจากการจำหน่ายให้แก่ผู้ให้บริการหรือสถานที่ซึ่งคุณได้รับซอฟต์แวร์

คุณยอมรับว่าการใช้ซอฟต์แวร์ของคุณแสดงว่าคุณได้อ่านข้อตกลงนี้ ทำความเข้าใจและยอมรับที่จะมีข้อผูกพันตามข้อกำหนดและเงื่อนไขของข้อตกลงนี้

1. **ซอฟต์แวร์** ในข้อตกลงนี้ "ซอฟต์แวร์" หมายถึง (i) โปรแกรมคอมพิวเตอร์ที่มากับข้อตกลงนี้และองค์ประกอบทั้งหมดของโปรแกรม; (ii) เนื้อหาทั้งหมดของดิสก์ CD-ROM, DVD อีเมลและไฟล์แนบใดๆ หรือสื่ออื่นๆ ที่ข้อตกลงนี้มีให้ รวมถึงรหัสวัตถุของซอฟต์แวร์ที่มาพร้อมกับสื่อจัดเก็บข้อมูล ผ่านอีเมลหรือดาวน์โหลดผ่านอินเทอร์เน็ต; (iii) สื่อสิ่งพิมพ์ประกอบการอธิบายใดๆ และเอกสารอื่นๆ ใดๆ ที่เกี่ยวข้องกับซอฟต์แวร์ นอกเหนือจากคำอธิบายใดๆ ของซอฟต์แวร์ ข้อมูลทางเทคนิค คำอธิบายคุณสมบัติหรือการใช้งานซอฟต์แวร์ใดๆ คำอธิบายถึงสภาพแวดล้อมในการใช้งานซอฟต์แวร์ คำแนะนำสำหรับการใช้งานหรือการติดตั้งซอฟต์แวร์หรือคำอธิบายใดๆ ถึงวิธีการใช้งานซอฟต์แวร์ ("เอกสารประกอบ"); (iv) สำเนาของซอฟต์แวร์ การแก้ไขข้อผิดพลาดที่เป็นไปได้ในซอฟต์แวร์ ส่วนเพิ่มเติมซอฟต์แวร์ ส่วนขยาย เวอร์ชันดัดแปลงของซอฟต์แวร์ และการอัพเดทส่วนประกอบซอฟต์แวร์ ถ้ามี ตามที่ผู้ให้บริการให้อนุญาตแก่คุณตามข้อ 3 ของข้อตกลงนี้ ซอฟต์แวร์จะมีให้ในรูปแบบของรหัสวัตถุที่เรียกใช้งานได้เท่านั้น

2. **การติดตั้ง คอมพิวเตอร์ และรหัสใบอนุญาต ซอฟต์แวร์ที่อยู่ในสื่อจัดเก็บข้อมูล** ส่งทางอีเมล ดาวน์โหลดจากอินเทอร์เน็ต ดาวน์โหลดจากเซิร์ฟเวอร์ของผู้ให้บริการ หรือได้รับจากแหล่งอื่นๆ จะต้องมีการติดตั้ง คุณจะต้องติดตั้งซอฟต์แวร์ในคอมพิวเตอร์ที่ได้รับการกำหนดค่าอย่างถูกต้อง ตามข้อกำหนดขั้นต่ำที่ระบุไว้ในเอกสารประกอบ วิธีการติดตั้งจะมีระบุไว้ในเอกสารประกอบ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์หรือฮาร์ดแวร์ที่อาจมีผลเสียต่อซอฟต์แวร์ไว้ในคอมพิวเตอร์ที่คุณติดตั้งซอฟต์แวร์ คอมพิวเตอร์หมายถึงฮาร์ดแวร์ ซึ่งรวมถึงแต่ไม่จำกัดเพียง คอมพิวเตอร์ส่วนบุคคล แล็ปท็อป เวิร์กสเตชัน ปาล์มท็อปคอมพิวเตอร์ สมาร์ทโฟน อุปกรณ์อิเล็กทรอนิกส์แบบถือหรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆ ที่ซอฟต์แวร์ถูกออกแบบมาให้ใช้งานด้วย หรือที่ซอฟต์แวร์ถูกติดตั้งและ/หรือใช้งาน รหัสใบอนุญาตหมายถึงชุดของสัญลักษณ์ อักขระ หมายเลข หรือสัญลักษณ์พิเศษที่ไม่ซ้ำกันซึ่งจัดหาให้แก่ผู้ใช้ปลายทางเพื่ออนุญาตให้ใช้งานซอฟต์แวร์ เวอร์ชั่นเฉพาะ หรือส่วนขยายของข้อกำหนดของใบอนุญาตได้อย่างถูกกฎหมาย สอดคล้องกับข้อตกลงนี้

3. **ใบอนุญาต** ตามเงื่อนไขที่คุณยอมรับตามข้อกำหนดของข้อตกลงนี้ คุณจะต้องชำระค่าใบอนุญาตภายในระยะเวลาที่ครบกำหนด และคุณจะต้องปฏิบัติตามข้อกำหนดและเงื่อนไขทั้งหมดที่ระบุไว้ในที่นี้ ผู้ให้บริการจะให้สิทธิ์ ("ใบอนุญาต") ต่อไปนี้แก่คุณ:

ก) **การติดตั้งและการใช้งาน** คุณจะมีสิทธิที่ไม่จำกัดเฉพาะตัวและไม่สามารถโอนสิทธิได้ในการติดตั้งซอฟต์แวร์ในฮาร์ดดิสก์ของคอมพิวเตอร์ หรือสื่อถาวรอื่นๆ สำหรับการจัดเก็บข้อมูล การติดตั้ง และการจัดเก็บซอฟต์แวร์ในหน่วยความจำของระบบคอมพิวเตอร์ และในการปรับใช้งาน จัดเก็บ และแสดงซอฟต์แวร์

ข) **ข้อกำหนดของจำนวนใบอนุญาต** สิทธิในการใช้ซอฟต์แวร์จะมีข้อผูกพันตามจำนวนของผู้ใช้ปลายทาง ผู้ใช้ปลายทางหนึ่งราย จะมีความหมายดังนี้: (i) การติดตั้งซอฟต์แวร์ในระบบคอมพิวเตอร์หนึ่งระบบ หรือ (ii) ถ้าขอบเขตของใบอนุญาตเชื่อมโยงกับจำนวนกล่องจดหมาย คำว่า ผู้ใช้ปลายทางหนึ่งราย จะมีความหมายว่าผู้ใช้คอมพิวเตอร์หนึ่งรายที่ยอมรับอีเมลผ่านทางโปรแกรมตัวแทนผู้ใช้อีเมล (“MUA”) ถ้า MUA ยอมรับอีเมลและส่งต่อไปยังผู้ใช้หลายรายโดยอัตโนมัติ จำนวนของผู้ใช้ปลายทางจะพิจารณาตามจำนวนผู้ใช้ตามจริงที่มีการส่งอีเมลถึง ถ้าอีเมลเซิร์ฟเวอร์ดำเนินการเป็นเกตเวย์ของอีเมล จำนวนผู้ใช้ปลายทางจะต้องเท่ากับจำนวนผู้ใช้อีเมลเซิร์ฟเวอร์ที่เกตเวย์นั้นให้บริการอยู่ ถ้ามีการส่งอีเมลสำหรับที่อยู่อีเมลที่ไม่ได้ระบุจำนวนไปยังและยอมรับโดยผู้ใช้รายเดียว (เช่น ผ่านชื่อแทน) และข้อความนั้นไม่มีการส่งต่อโดยอัตโนมัติโดยไคลเอ็นต์ไปยังผู้ใช้จำนวนมาก จะต้องใช้ใบอนุญาตสำหรับคอมพิวเตอร์เครื่องเดียว คุณจะต้องไม่ใช้ใบอนุญาตเดียวกันในเวลาเดียวกันในคอมพิวเตอร์มากกว่าหนึ่งเครื่อง ผู้ใช้ปลายทางได้รับสิทธิ์ให้ป้อนรหัสใบอนุญาตไปยังซอฟต์แวร์ได้เฉพาะในขอบเขตเท่าที่ผู้ใช้ปลายทางมีสิทธิ์ใช้งานซอฟต์แวร์ ซึ่งสอดคล้องกับข้อจำกัดที่มีผลบังคับใช้จากจำนวนใบอนุญาตที่ได้รับจากผู้ให้บริการ รหัสใบอนุญาตจะถือว่าเป็นความลับ คุณต้องไม่แบ่งปันใบอนุญาตกับบุคคลที่สามหรืออนุญาติให้บุคคลที่สามใช้รหัสใบอนุญาตเว้นแต่จะได้รับอนุญาตจากข้อตกลงนี้หรือจากผู้ให้บริการ หากรหัสใบอนุญาตของคุณถูกบุกรุก โปรดแจ้งผู้ให้บริการทันที

ค) **เวอร์ชั่นใช้กับบ้าน/ธุรกิจ** ซอฟต์แวร์เวอร์ชั่นใช้กับบ้านจะใช้เฉพาะในสภาพแวดล้อมการแบบส่วนบุคคลและ/หรือแบบไม่ใช่เชิงพาณิชย์ในบ้านและในครอบครัวเท่านั้น การรับซอฟต์แวร์เวอร์ชั่นใช้กับธุรกิจต้องเป็นไปเพื่อนำไปใช้ในสภาพแวดล้อมเชิงพาณิชย์ และเพื่อใช้ซอฟต์แวร์ในอีเมลเซิร์ฟเวอร์ เมลรีเลย์ เมลเกตเวย์ หรืออินเทอร์เน็ตเกตเวย์

ง) **ระยะเวลาของใบอนุญาต** สิทธิในการใช้ซอฟต์แวร์จะมีระยะเวลาจำกัด

จ) **ซอฟต์แวร์ของ OEM** ซอฟต์แวร์ที่จัดประเภทว่าเป็น "OEM" จะจำกัดเฉพาะคอมพิวเตอร์ที่คุณได้รับซอฟต์แวร์มาด้วย ไม่สามารถโอนซอฟต์แวร์ไปยังคอมพิวเตอร์เครื่องอื่นได้

ฉ) **NFR, ซอฟต์แวร์ทดลองใช้** ซอฟต์แวร์ที่ถูกจัดเป็น "ไม่ใช่สำหรับจำหน่าย" ซึ่งเรียกว่า NFR หรือทดลองใช้ ไม่สามารถกำหนดไว้สำหรับการชำระเงิน และต้องใช้สำหรับการสาธิตหรือการทดสอบคุณลักษณะของซอฟต์แวร์เท่านั้น

ช) **การยุติใบอนุญาต** ใบอนุญาตจะยุติโดยอัตโนมัติเมื่อสิ้นสุดระยะเวลาที่ได้รับสิทธิ ถ้าคุณไม่ปฏิบัติตามบทบัญญัติของข้อตกลงนี้ ผู้ให้บริการจะได้รับสิทธิให้เพิกถอนจากข้อตกลงนี้ โดยไม่มีผลกระทบต่อสิทธิหรือการเยียวยาทางกฎหมายที่เปิดไว้ให้กับผู้ให้บริการสำหรับกรณีดังกล่าว ในกรณีของการยกเลิกใบอนุญาต คุณจะต้องลบ ทำลาย หรือส่งคืนซอฟต์แวร์และสำเนาการสำรองข้อมูลทั้งหมดแก่ ESET หรือสถานที่ซึ่งคุณได้รับซอฟต์แวร์ โดยเป็นผู้ออกค่าใช้จ่ายเอง เมื่อสิ้นสุดระยะเวลาที่ได้รับสิทธิใช้ใบอนุญาต ผู้ให้บริการมีสิทธิในการยกเลิกการให้สิทธิของผู้ใช้ปลายทางสำหรับการใช้ฟังก์ชันของซอฟต์แวร์ที่ต้องเชื่อมต่อกับเซิร์ฟเวอร์ของผู้ให้บริการหรือเซิร์ฟเวอร์ของบุคคลที่สาม

4. **ฟังก์ชันที่ต้องใช้การรวบรวมข้อมูลและการเชื่อมต่ออินเทอร์เน็ต** เพื่อให้การทำงานถูกต้อง ซอฟต์แวร์ต้องมีการเชื่อมต่ออินเทอร์เน็ต และต้องเชื่อมต่อกับเซิร์ฟเวอร์ของผู้ให้บริการหรือเซิร์ฟเวอร์ของบุคคลที่สามและการรวบรวมข้อมูลที่เกี่ยวข้องเป็นประจำตามนโยบายความเป็นส่วนตัว การเชื่อมต่อกับอินเทอร์เน็ตและการรวบรวมข้อมูลที่เกี่ยวข้องมีความสำคัญสำหรับคุณลักษณะของซอฟต์แวร์ดังต่อไปนี้:

ก) **การอัพเดทซอฟต์แวร์** ผู้ให้บริการจะได้รับสิทธิ์ตั้งแต่เวลาออกการอัพเดทหรืออัพเกรดซอฟต์แวร์ ("การอัพเดท") แต่จะไม่มีภาระหน้าที่ในการให้การอัพเดท ฟังก์ชันนี้จะถูกเปิดใช้งานภายใต้การตั้งค่ามาตรฐานของซอฟต์แวร์และจะได้รับการติดตั้งการอัพเดทโดยอัตโนมัติ ยกเว้นผู้ใช้ปลายทางจะปิดใช้งานการติดตั้งการอัพเดทโดยอัตโนมัติสำหรับการจัดหาการอัพเดท จะต้องใช้การตรวจสอบความถูกต้องของใบอนุญาต ซึ่งรวมถึงข้อมูลเกี่ยวกับคอมพิวเตอร์และ/หรือแพลตฟอร์มที่ติดตั้งซอฟต์แวร์นั้นตามนโยบายความเป็นส่วนตัว

การจัดหาการอัพเดทใดๆ อาจอยู่ภายใต้นโยบายการสิ้นสุดอายุการใช้งาน ("นโยบาย EOL") ซึ่งมีอยู่ใน https://go.eset.com/eol_business จะไม่มีการอัพเดทใดๆ หลังจากซอฟต์แวร์หรือคุณลักษณะใดๆ ของซอฟต์แวร์ถึงวันสิ้นสุดอายุการใช้งานที่กำหนดไว้ในนโยบาย EOL

ข) **การส่งต่อการแฝงตัวและข้อมูลแก่ผู้ให้บริการ** ซอฟต์แวร์นี้มีฟังก์ชันที่ทำหน้าที่เก็บตัวอย่างของไวรัสคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ที่เป็นอันตรายอื่นๆ และสิ่งที่น่าสงสัยซึ่งเป็นปัญหา ที่อาจไม่พึงประสงค์หรืออาจไม่ปลอดภัย เช่น ไฟล์ URL แพ็คเก็ต IP และค่าเฟรมอีเธอร์เน็ต (“การแฝงตัว”) และจะส่งตัวอย่างเหล่านี้ให้กับผู้ให้บริการ รวมถึงแต่ไม่จำกัดเฉพาะข้อมูลเกี่ยวกับกระบวนการติดตั้ง คอมพิวเตอร์และ/หรือแพลตฟอร์มที่ติดตั้งซอฟต์แวร์นั้น และข้อมูลเกี่ยวกับระบบปฏิบัติการและการทำงานของซอฟต์แวร์ ("ข้อมูล") ข้อมูลและการแฝงตัวอาจประกอบด้วยข้อมูล (รวมถึงข้อมูลส่วนบุคคลที่ได้รับโดยการสุ่มหรือโดยบังเอิญ) เกี่ยวกับผู้ใช้ปลายทางหรือผู้ใช้อื่นๆ ที่ใช้คอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ และไฟล์ที่ได้รับผลกระทบจากการแฝงตัวรวมถึงเมตาดาต้าที่เกี่ยวข้อง

ข้อมูลและการแฝงตัวอาจรวบรวมได้โดยฟังก์ชันซอฟต์แวร์ต่อไปนี้:

i. ฟังก์ชันระบบความเชื่อถือ LiveGrid ประกอบด้วยการรวบรวมและการส่งแฮชที่เกี่ยวข้องกับการแฝงตัวแบบทางเดียวให้กับผู้ให้บริการ โดยฟังก์ชันนี้จะถูกเปิดใช้งานภายใต้การตั้งค่ามาตรฐานของซอฟต์แวร์

ii. ฟังก์ชันระบบตรวจสอบป้อนกลับของ LiveGrid ประกอบด้วยการรวบรวมและการส่งข้อมูลการบุกรุกพร้อมด้วยเมตาดาต้าและข้อมูลที่เกี่ยวข้องให้กับผู้ให้บริการ โดยฟังก์ชันนี้จะถูกเปิดใช้งานโดยผู้ใช้ปลายทางระหว่างกระบวนการติดตั้งซอฟต์แวร์

ผู้ให้บริการจะใช้ข้อมูลและการบุกรุกที่ได้รับเพื่อการวิเคราะห์และการวิจัยเกี่ยวกับการบุกรุก การปรับปรุงซอฟต์แวร์ และการตรวจสอบความถูกต้องของใบอนุญาต และจะใช้มาตรการที่เหมาะสมเพื่อดำเนินการให้มั่นใจว่าการบุกรุกและข้อมูลที่ได้รับจะคงปลอดภัย เมื่อเปิดใช้งานฟังก์ชันนี้ของซอฟต์แวร์ ผู้ให้บริการจะเก็บรวบรวมและดำเนินการกับการบุกรุกและข้อมูลตามที่ระบุไว้ในนโยบายความเป็นส่วนตัวและตามระเบียบข้อบังคับตามกฎหมายที่เกี่ยวข้อง คุณสามารถปิดการทำงานของฟังก์ชันนี้ได้ทุกเมื่อ

สำหรับวัตถุประสงค์ของข้อตกลงนี้ จะจำเป็นต้องเก็บรวบรวม ประมวลผล และจัดเก็บข้อมูล เพื่อให้ผู้ให้บริการสามารถระบุตัวคุณได้ตามที่ระบุไว้ในนโยบายความเป็นส่วนตัว คุณรับทราบว่าผู้ให้บริการสามารถตรวจสอบว่าคุณใช้ซอฟต์แวร์ตามบทบัญญัติของข้อตกลงนี้หรือไม่ โดยใช้วิธีการของผู้ให้บริการเอง ในที่นี้จะถือว่าคุณรับทราบว่าตามวัตถุประสงค์ของข้อตกลงนี้แล้ว จำเป็นที่จะต้องถ่ายโอนข้อมูลของคุณขณะที่มีการสื่อสารระหว่างซอฟต์แวร์และระบบคอมพิวเตอร์ของผู้ให้บริการ หรือกับหุ้นส่วนธุรกิจที่เป็นส่วนหนึ่งของภาคการจัดจำหน่ายของผู้ให้บริการ ตลอดจนเครือข่ายที่รองรับ ทั้งนี้เพื่อตรวจสอบถึงฟังก์ชันการใช้งานและการได้รับอนุญาตให้ใช้ซอฟต์แวร์และเพื่อคุ้มครองสิทธิ์ของผู้ให้บริการ

ตามข้อสรุปของข้อตกลงนี้ ผู้ให้บริการหรือหุ้นส่วนธุรกิจที่เป็นส่วนหนึ่งของภาคการจัดจำหน่ายของผู้ให้บริการและเครือข่ายที่รองรับจะได้รับสิทธิ์ให้โอน ประมวลผล และจัดเก็บข้อมูลสำคัญที่จะระบุตัวคุณ เพื่อการเรียกเก็บเงินและการปฏิบัติตามข้อตกลงนี้ รวมถึงการส่งการแจ้งเตือนในคอมพิวเตอร์ของคุณ

สามารถดูรายละเอียดเกี่ยวกับการป้องกันความเป็นส่วนตัว ข้อมูลส่วนบุคคล และสิทธิ์ของคุณในแง่ของข้อมูลได้ในนโยบายความเป็นส่วนตัวซึ่งอยู่ในเว็บไซต์ของผู้ให้บริการและสามารถเข้าถึงได้โดยตรงจากกระบวนการติดตั้ง คุณสามารถดูจากส่วนวิธีใช้ของซอฟต์แวร์ได้เช่นกัน

5. **การใช้สิทธิ์ของผู้ใช้ปลายทาง** คุณต้องใช้สิทธิ์ของผู้ใช้ปลายทางในนามบุคคลหรือผ่านพนักงาน คุณได้รับสิทธิ์ให้ใช้ซอฟต์แวร์เฉพาะเพื่อปกป้องการทำงานของคุณและคุ้มครองคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่คุณได้รับใบอนุญาตเท่านั้น

6. **ข้อจำกัดเกี่ยวกับสิทธิ์** คุณไม่สามารถคัดลอก แจกจ่าย ดึงข้อมูลจากองค์ประกอบ หรือทำผลงานที่ต่อเนื่องของซอฟต์แวร์นี้ เมื่อใช้ซอฟต์แวร์ จะถือว่าคุณต้องปฏิบัติตามข้อจำกัดต่อไปนี้:

ก) คุณสามารถสร้างสำเนาของซอฟต์แวร์เก็บไว้หนึ่งฉบับในสื่อสำหรับการจัดเก็บข้อมูลถาวร เพื่อเป็นสำเนาสำรองข้อมูลแบบถาวร ซึ่งจะทำให้ไม่มีการติดตั้งหรือใช้สำเนาสำรองข้อมูลอาร์ไคฟ์ในคอมพิวเตอร์เครื่องอื่น สำเนาอื่นๆ ที่

คุณดำเนินการจากซอฟต์แวร์จะถือว่าเป็นการละเมิดข้อตกลงนี้

ข) คุณไม่สามารถใช้ ปรับเปลี่ยน แปล หรือสร้างซอฟต์แวร์ซ้ำ หรือถ่ายโอนสิทธิ์ในการใช้ซอฟต์แวร์หรือสำเนาของซอฟต์แวร์ในลักษณะใดๆ นอกเหนือจากที่ระบุไว้ในข้อตกลงนี้

ค) คุณไม่สามารถจำหน่าย อนุญาตช่วง เช่าซื้อหรือเช่า หรือขอยืมซอฟต์แวร์ หรือใช้ซอฟต์แวร์เพื่อให้บริการในเชิงพาณิชย์

ง) คุณไม่สามารถทำวิศวกรรมย้อนกลับ ย้อนการคอมไพล์ หรือแยกส่วนประกอบของซอฟต์แวร์ หรือพยายามค้นหารหัสที่มาของซอฟต์แวร์ ยกเว้นจะอยู่ภายในขอบเขตของกฎหมายว่าห้ามมีข้อจำกัดนี้อย่างชัดเจน

จ) คุณยอมรับว่าคุณจะใช้ซอฟต์แวร์นี้เฉพาะในลักษณะที่เป็นไปตามกฎหมายที่มีผลบังคับใช้ทั้งหมดในเขตอำนาจศาลที่คุณใช้ซอฟต์แวร์ ซึ่งจะรวมถึง แต่ไม่จำกัดเพียงข้อจำกัดที่มีผลบังคับใช้เกี่ยวกับลิขสิทธิ์และสิทธิในทรัพย์สินทางปัญญา

ฉ) คุณยอมรับว่าคุณจะใช้ซอฟต์แวร์และฟังก์ชันในลักษณะที่ไม่จำกัดโอกาสของผู้ใช้ปลายทางคนอื่นในการเข้าถึงบริการเหล่านี้ ผู้ให้บริการสงวนสิทธิ์ในการจำกัดขอบเขตของบริการที่ให้แก่ผู้ใช้ปลายทางแต่ละราย เพื่อให้มีผู้ใช้ปลายทางสามารถใช้บริการได้เป็นจำนวนมากที่สุด การจำกัดขอบเขตของบริการจะหมายถึงการยุติการให้บริการโดยสมบูรณ์ สำหรับฟังก์ชันใดๆ ของซอฟต์แวร์ และการลบข้อมูลและสารสนเทศในเซิร์ฟเวอร์ของผู้ให้บริการหรือเซิร์ฟเวอร์ของบุคคลที่สามที่เกี่ยวข้องกับฟังก์ชันของซอฟต์แวร์

ช) คุณยอมรับว่าจะไม่กระทำกิจกรรมใดๆ ที่มีการใช้รหัสใบอนุญาตมาเกี่ยวข้อง ขัดกับข้อกำหนดของข้อตกลงนี้ หรือชี้นำไปสู่การมอบรหัสใบอนุญาตให้บุคคลที่ไม่มีสิทธิ์ใช้งานซอฟต์แวร์ เช่น การส่งทอดรหัสใบอนุญาตที่ใช้แล้วหรือยังไม่ได้ใช้ ไม่ว่าจะในรูปแบบใดก็ตาม รวมถึงการทำซ้ำโดยไม่ได้รับอนุญาต หรือแจกจ่ายรหัสใบอนุญาตที่ทำซ้ำหรือสร้างขึ้น หรือใช้งานซอฟต์แวร์โดยที่ใช้รหัสใบอนุญาตซึ่งได้รับมาจากแหล่งอื่นๆ ที่ไม่ใช่จากผู้ให้บริการ

7. **ลิขสิทธิ์** ซอฟต์แวร์และสิทธิทั้งปวง รวมถึงแต่ไม่จำกัดเพียงสิทธิในกรรมสิทธิและสิทธิในทรัพย์สินทางปัญญาเป็นของ ESET และ/หรือผู้ให้การอนุญาตของ ESET ESET และผู้ให้การอนุญาตของ ESET จะได้รับความคุ้มครองตามบทบัญญัติของสนธิสัญญาระหว่างประเทศ และโดยกฎหมายระดับชาติที่มีอำนาจบังคับอื่นๆ ทั้งหมดของประเทศที่ใช้ซอฟต์แวร์นี้ โครงสร้าง การจัดระเบียบ และรหัสของซอฟต์แวร์เป็นความลับทางการค้าที่เป็นประโยชน์และข้อมูลลับเฉพาะของ ESET และ/หรือผู้ที่ให้การอนุญาตของ ESET คุณต้องไม่คัดลอกซอฟต์แวร์ ยกเว้นตามที่ระบุไว้ในข้อ 6(ก) สำเนาที่คุณได้รับอนุญาตให้ดำเนินการตามข้อตกลงนี้จะต้องมีคำชี้แจงลิขสิทธิ์และกรรมสิทธิ์อื่นๆ เช่นเดียวกับที่ปรากฏในซอฟต์แวร์ ถ้าคุณทำวิศวกรรมย้อนกลับ ย้อนการคอมไพล์ แยกส่วนประกอบ หรือพยายามค้นหารหัสที่มาของซอฟต์แวร์ ในลักษณะที่เป็นการละเมิดบทบัญญัติของข้อตกลงนี้ จะถือว่าคุณยอมรับในที่นี้ว่าข้อมูลใดๆ ที่ได้รับจะถือว่าเป็นกรรมสิทธิ์ของผู้ให้บริการ และเป็นของผู้ให้บริการโดยสมบูรณ์ นับจากที่ได้รับข้อมูลดังกล่าว

เป็นต้นไป โดยปริยายและไม่สามารถเพิกถอนได้ โดยไม่คำนึงถึงสิทธิของผู้ให้บริการเกี่ยวกับการละเมิดข้อตกลงนี้

8. **การสงวนสิทธิ์** ผู้ให้บริการขอสงวนสิทธิทั้งหมดสำหรับซอฟต์แวร์ ยกเว้นสิทธิที่มีการให้สิทธิแก่คุณอย่างชัดเจนภายใต้ข้อกำหนดของข้อตกลงนี้ ในฐานะที่คุณเป็นผู้ใช้ปลายทางของซอฟต์แวร์

9. **เวอร์ชันหลายภาษา ซอฟต์แวร์ที่รองรับสื่อสองชนิด หลายสำเนา** ในกรณีที่ซอฟต์แวร์รองรับหลายแพลตฟอร์มหรือหลายภาษา หรือถ้าคุณได้รับซอฟต์แวร์หลายสำเนา คุณสามารถใช้ซอฟต์แวร์ได้เฉพาะสำหรับระบบคอมพิวเตอร์จำนวนหนึ่ง และสำหรับเวอร์ชันที่คุณได้รับใบอนุญาต คุณไม่สามารถจำหน่าย ให้เช่า เช่าซื้อ อนุญาตช่วง ให้หยิบยืม หรือโอนเวอร์ชันหรือสำเนาของซอฟต์แวร์ที่คุณไม่ได้ใช้งาน

10. **การเริ่มต้นและการยุติข้อตกลง** ข้อตกลงนี้มีผลนับจากวันที่คุณยอมรับข้อกำหนดของข้อตกลงนี้ คุณสามารถยุติข้อตกลงนี้เมื่อใดก็ได้ ด้วยการถอนการติดตั้งอย่างถาวร การทำลาย หรือการส่งคืนซอฟต์แวร์ สำเนาการสำรองข้อมูลทั้งหมด ตลอดจนเอกสารที่เกี่ยวข้องทั้งหมดที่คุณได้รับจากผู้ให้บริการหรือจากหุ้นส่วนธุรกิจของผู้ให้บริการ โดยเป็นผู้ออกค่าใช้จ่ายเอง สิทธิ์ในการใช้ซอฟต์แวร์และคุณลักษณะใดๆ ของซอฟต์แวร์อาจอยู่ภายใต้นโยบาย EOL สิทธิ์ในการใช้ซอฟต์แวร์ของคุณจะสิ้นสุดลงหลังจากซอฟต์แวร์หรือคุณลักษณะใดๆ ของซอฟต์แวร์ถึงวันสิ้นสุดอายุการใช้งานที่กำหนดไว้ในนโยบาย EOL ไม่ว่าการยุติข้อตกลงนี้จะเกิดขึ้นด้วยสาเหตุใด บทบัญญัติของข้อ 7, 8, 11, 13, 19 และ 21 จะยังคงมีผลบังคับโดยไม่จำกัดเวลา

11. **ประกาศของผู้ใช้ปลายทาง** ในฐานะที่เป็นผู้ใช้ปลายทาง คุณรับทราบว่าซอฟต์แวร์นี้มีให้แก่คุณแบบ "ตามสภาพ" โดยไม่มีการรับประกันทั้งโดยชัดแจ้งหรือโดยนัย ไม่ว่าในประเภทใดภายในขอบเขตสูงสุดที่กฎหมายอนุญาต ผู้ให้บริการ ผู้ให้การอนุญาตแก่ผู้ให้บริการหรือบริษัทในเครือ หรือผู้ถือลิขสิทธิ์ ไม่ได้ให้การรับรองหรือรับประกันทั้งโดยชัดแจ้งและโดยนัย ซึ่งจะรวมถึง แต่ไม่จำกัดเพียงการรับประกันการขาย หรือความเหมาะสมกับวัตถุประสงค์อย่างใดอย่างหนึ่งเป็นการเฉพาะ หรือการรับประกันว่าซอฟต์แวร์ไม่ได้ละเมิดสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้าหรือสิทธิอื่นๆ ของบุคคลที่สาม ผู้ให้บริการหรือบุคคลอื่นไม่มีการรับประกันใดๆ ว่าฟังก์ชันที่มีอยู่ในซอฟต์แวร์นี้จะเป็นไปตามความต้องการ หรือการทำงานของซอฟต์แวร์จะทำงานต่อเนื่องและปราศจากข้อผิดพลาด คุณต้องรับผิดชอบและรับความเสี่ยงทั้งหมดสำหรับการเลือกซอฟต์แวร์ เพื่อให้ได้ผลลัพธ์ตามเจตนารมณ์ของคุณ และสำหรับการติดตั้ง การใช้งาน และผลที่จะได้รับจากซอฟต์แวร์

12. **ไม่มีข้อผูกมัดอื่น** ข้อตกลงนี้ไม่ได้แสดงถึงภาระหน้าที่อื่นใดในส่วนของผู้ให้บริการและผู้ให้การอนุญาตแก่ผู้ให้บริการ ยกเว้นจะระบุไว้อย่างชัดเจนในที่นี้

13. **ข้อจำกัดความรับผิด** ภายในขอบเขตสูงสุดที่กฎหมายอนุญาต ไม่ว่าในกรณีใดๆ ผู้ให้บริการ พนักงาน หรือผู้ให้การอนุญาตจะไม่มีความรับผิดต่อการสูญเสียผลกำไร รายได้ การขาย ข้อมูล หรือค่าใช้จ่ายที่เกิดขึ้นเพื่อจัดหาสินค้าหรือบริการทดแทน ความเสียหายของสินทรัพย์ การบาดเจ็บของบุคคล การหยุดชะงักของธุรกิจ การสูญเสีย

ข้อมูลธุรกิจหรือความเสียหายเป็นกรณีพิเศษ ทางตรง ทางอ้อม เกิดขึ้นเอง ทางเศรษฐกิจ การชดเชย บทลงโทษ หรือความเสียหายที่เป็นพิเศษหรือที่เกิดขึ้นในภายหลัง อันเกิดขึ้นด้วยวิธีใดๆ ก็ตามจากการทำสัญญา การละเมิด ความประมาทหรือข้อเท็จจริงอื่นๆ ที่แสดงถึงความรับผิด อันเกิดจากการติดตั้ง การใช้หรือไม่สามารถใช้ซอฟต์แวร์ แม้ในกรณีที่ผู้ให้บริการหรือผู้ให้การอนุญาตแก่ผู้ให้บริการหรือบริษัทในเครือได้รับแจ้งถึงโอกาสที่จะเกิดความเสียหายนั้นแล้วก็ตาม เนื่องจากในบางประเทศและบางเขตอำนาจศาลไม่อนุญาตให้มีการยกเว้นความรับผิด แต่อาจอนุญาตให้มีการจำกัดความรับผิด ในกรณีดังกล่าว ความรับผิดของผู้ให้บริการ พนักงาน หรือผู้ให้การอนุญาตหรือบริษัทในเครือจะจำกัดอยู่เพียงไม่เกินจำนวนเงินที่คุณชำระเป็นค่าใบอนุญาตเท่านั้น

14. ในข้อตกลงนี้จะไม่มีผลกระทบต่อสิทธิตามกฎหมายของฝ่ายใดที่มีฐานะเป็นผู้บริโภคถ้าเกิดข้อขัดแย้งในการทำงาน

15. **การสนับสนุนด้านเทคนิค** ESET หรือบุคคลที่สามที่กำหนดโดย ESET จะใช้ดุลยพินิจในการให้บริการสนับสนุนด้านเทคนิค โดยไม่มีการรับประกันหรือการประกาศใดๆ จะไม่มีการสนับสนุนด้านเทคนิคใดๆ หลังจากซอฟต์แวร์หรือคุณลักษณะใดๆ ของซอฟต์แวร์ถึงวันสิ้นสุดอายุการใช้งานดังที่กำหนดไว้ในนโยบาย EOL ผู้ใช้ปลายทางจะต้องสำรองข้อมูล ซอฟต์แวร์ และโปรแกรมที่มีอยู่ทั้งหมดก่อนการให้การสนับสนุนด้านเทคนิค ESET และ/หรือบุคคลที่สามที่กำหนดโดย ESET จะไม่ยอมรับการรับผิดสำหรับความเสียหายหรือการสูญเสียของข้อมูล สินทรัพย์ ซอฟต์แวร์หรือฮาร์ดแวร์ หรือการสูญเสียผลกำไร อันเนื่องมาจากการให้การสนับสนุนด้านเทคนิค ESET และ/หรือบุคคลที่สามที่กำหนดโดย ESET ขอสงวนสิทธิ์ที่จะพิจารณาว่าการแก้ไขปัญหาอยู่นอกขอบเขตของการสนับสนุนด้านเทคนิค ESET ขอสงวนสิทธิ์ในการใช้ดุลยพินิจเพื่อปฏิเสธ พัก หรือยุติการให้การสนับสนุนด้านเทคนิค อาจจำเป็นต้องใช้ข้อมูลใบอนุญาต ข้อมูล และข้อมูลอื่นๆ ตามที่ระบุไว้ในนโยบายความเป็นส่วนตัว เพื่อวัตถุประสงค์ในการให้บริการสนับสนุนด้านเทคนิค

16. **การโอนใบอนุญาต** ซอฟต์แวร์สามารถโอนจากระบบคอมพิวเตอร์หนึ่งไปยังอีกระบบหนึ่ง ยกเว้นจะขัดกับข้อกำหนดของข้อตกลง ถ้าไม่ขัดกับข้อกำหนดของข้อตกลง ผู้ใช้ปลายทางจะได้รับสิทธิเฉพาะสำหรับการโอนใบอนุญาตอย่างถาวร และสิทธิทั้งหมดที่มาจากข้อตกลงนี้ไปยังผู้ใช้ปลายทางรายอื่น โดยมีความยินยอมของผู้ให้บริการ ตามเงื่อนไขว่า (i) ผู้ใช้ปลายทางเดิมต้องไม่เก็บสำเนาของซอฟต์แวร์ไว้ (ii) การโอนสิทธิจะต้องเป็นโดยตรง เช่น จากผู้ใช้ปลายทางเดิมไปยังผู้ใช้ปลายทางรายใหม่ (iii) ผู้ใช้ปลายทางรายใหม่ต้องถือสิทธิและภาระหน้าที่ทั้งหมดที่เป็นหน้าที่รับผิดชอบของผู้ใช้ปลายทางเดิมภายใต้ข้อกำหนดของข้อตกลงนี้ (iv) ผู้ใช้ปลายทางเดิมต้องให้เอกสารประกอบแก่ผู้ใช้ปลายทางรายใหม่ ซึ่งจะช่วยตรวจสอบซอฟต์แวร์ที่เป็นของแท้ดังที่ระบุภายใต้ข้อ 17

17. **การตรวจสอบซอฟต์แวร์ที่เป็นของแท้** ผู้ใช้ปลายทางสามารถพิสูจน์สิทธิ์ในการใช้ซอฟต์แวร์ได้โดยใช้วิธีการใดวิธีการหนึ่งต่อไปนี้: (i) ผ่านใบรับรองของใบอนุญาตที่ออกโดยผู้ให้บริการหรือบุคคลที่สามที่มีการกำหนดโดยผู้ให้บริการ (ii) ผ่านข้อตกลงใบอนุญาตที่เป็นลายลักษณ์อักษร ถ้ามีการสรุปข้อตกลงดังกล่าวไว้ (iii) ผ่านการส่งอีเมลที่ส่ง

ไปยังผู้ให้บริการซึ่งมีรายละเอียดของการอนุญาต (ชื่อผู้ใช้และรหัสผ่าน) อาจจำเป็นต้องใช้ข้อมูลใบอนุญาตและข้อมูลอัตลักษณ์ผู้ใช้ปลายทางตามที่ระบุไว้ในนโยบายความเป็นส่วนตัว เพื่อวัตถุประสงค์ในการตรวจสอบความเป็นของแท้ของซอฟต์แวร์

18. **การอนุญาตสำหรับหน่วยงานของรัฐที่มีอำนาจและรัฐบาลของสหรัฐอเมริกา** หน่วยงานของรัฐที่มีอำนาจ รวมถึงรัฐบาลของสหรัฐอเมริกา จะได้รับซอฟต์แวร์นี้พร้อมด้วยสิทธิการอนุญาตและข้อจำกัดที่อธิบายไว้ในข้อตกลงนี้

19. **การปฏิบัติตามการควบคุมด้านการค้า**

ก) คุณจะไม่ส่งออก ส่งออกซ้ำ ถ่ายโอนหรือทำให้บุคคลใดๆ ใช้งานซอฟต์แวร์นี้ได้ ไม่ว่าทางตรงหรือทางอ้อม หรือใช้งานในลักษณะใด ๆ หรือมีส่วนร่วมในการกระทำใด ๆ ที่อาจส่งผลให้ ESET หรือบริษัทผู้ถือหุ้น กิจการในเครือของบริษัทผู้ถือหุ้น รวมถึงหน่วยงานที่ควบคุมโดยบริษัทผู้ถือหุ้น (ซึ่งต่อไปนี้จะเรียกว่า "บริษัทในเครือ") มีการล่วงละเมิดหรือได้รับผลกระทบด้านลบภายใต้กฎหมายการควบคุมการค้าซึ่งรวมถึง

i. กฎหมายใด ๆ ที่ควบคุม จำกัด หรือบังคับใช้ข้อกำหนดด้านใบอนุญาตเกี่ยวกับการส่งออก การส่งออกซ้ำหรือโอนย้ายสินค้า ซอฟต์แวร์ เทคโนโลยี หรือบริการที่ออกหรือนำไปใช้โดยรัฐบาล ภาครัฐ หรือหน่วยงานซึ่งมีอำนาจกำกับดูแลของสหรัฐอเมริกา สิงคโปร์ สหราชอาณาจักร สหภาพยุโรป หรือประเทศสมาชิกหรือประเทศใด ๆ ที่มีข้อผูกพันภายใต้ข้อตกลงที่จะต้องดำเนินการหรือที่ ESET หรือบริษัทในเครือใด ๆ จัดตั้งขึ้นหรือดำเนินการ และ

ii. การลงโทษทางเศรษฐกิจ การเงิน การค้าหรือทางด้านอื่น ๆ การจำกัด คำสั่งห้ามค้าขาย การห้ามนำเข้าหรือส่งออก การห้ามโอนเงินหรือทรัพย์สินหรือการให้บริการ หรือมาตรการที่เทียบเท่าที่กำหนดโดยรัฐบาล ภาครัฐ หรือหน่วยงานซึ่งมีอำนาจกำกับดูแลของสหรัฐอเมริกา สิงคโปร์ สหราชอาณาจักร สหภาพยุโรป หรือประเทศสมาชิกใด ๆ หรือประเทศใด ๆ ที่มีข้อผูกพันภายใต้ข้อตกลงที่จะต้องดำเนินการหรือที่ ESET หรือบริษัทในเครือใด ๆ จัดตั้งขึ้นหรือดำเนินการ

(การกระทำทางกฎหมายที่อ้างถึงในจุดที่ i และ ii ข้างต้นร่วมกัน เรียกว่า “กฎหมายการควบคุมการค้า”)

ข) ESET มีสิทธิ์ระงับข้อผูกพันภายใต้ หรือยุติข้อกำหนดเหล่านี้โดยมีผลทันทีในกรณีที่:

i. ESET พิจารณาโดยอิงจากความเห็นที่สมเหตุสมผลว่าผู้ใช้ละเมิดหรือมีแนวโน้มที่จะละเมิดบทบัญญัติของข้อ 19 ก ของข้อตกลง หรือ

ii. ผู้ใช้ปลายทางและ/หรือซอฟต์แวร์ต้องอยู่ภายใต้กฎหมายควบคุมการค้าและ ด้วยเหตุนี้ ESET จะพิจารณาโดยอิงจากความเห็นที่สมเหตุสมผลว่า การปฏิบัติตามภาระหน้าที่ภายใต้ข้อตกลงนี้ต่อไปอาจส่งผลให้ ESET หรือ บริษัทในมีการล่วงละเมิดหรือได้รับผลกระทบด้านลบภายใต้กฎหมายควบคุมการค้า

ค) ไม่มีสิ่งใดในข้อตกลงที่มีจุดมุ่งหมาย และไม่มีสิ่งใดที่ควรแปลความหมายหรือตีความ ไปในทางชักชวนหรือกำหนดให้ฝ่ายหนึ่งฝ่ายใดกระทำการหรืองดเว้นการกระทำ (หรือตกลงที่จะกระทำหรือละเว้นจากการกระทำ) ในลักษณะใด ๆ ซึ่งไม่สอดคล้องกับ ผิดหรือต้องห้ามภายใต้กฎหมายควบคุมการค้าใดๆ ที่บังคับใช้

20. **การแจ้งเตือน** การแจ้งเตือนและการส่งคืนซอฟต์แวร์และเอกสารประกอบทั้งหมดจะต้องส่งถึง: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic โดยไม่กระทบต่อสิทธิ์ของ ESET ในการแจ้งการเปลี่ยนแปลงใดๆ ในข้อตกลงนี้ นโยบายความเป็นส่วนตัว นโยบาย EOL และเอกสารประกอบ ตามข้อ 22 ของข้อตกลงนี้ ESET อาจส่งอีเมลถึงคุณ แจ้งเตือนในแอพผ่านซอฟต์แวร์ หรือโพสต์การสื่อสารบนเว็บไซต์ของเรา คุณตกลงที่จะรับการสื่อสารทางกฎหมายจาก ESET ในรูปแบบอิเล็กทรอนิกส์ รวมถึงการสื่อสารใดๆ เกี่ยวกับการเปลี่ยนแปลงข้อกำหนด ข้อกำหนดพิเศษ หรือนโยบายความเป็นส่วนตัว ข้อเสนอสัญญา/การยอมรับ หรือคำเชิญใดๆ ในการดำเนินการ ประกาศ หรือการสื่อสารทางกฎหมายอื่นๆ โดยจะถือว่าได้รับการสื่อสารทางอิเล็กทรอนิกส์ดังกล่าวในรูปแบบเป็นลายลักษณ์อักษร เว้นแต่กฎหมายที่บังคับใช้จะกำหนดให้มีการสื่อสารในรูปแบบอื่นโดยเฉพาะ

21. **กฎหมายที่มีผลบังคับใช้** ข้อตกลงนี้อยู่ภายใต้อำนาจและมีการตีความตามกฎหมายของสาธารณรัฐสโลวัก ผู้ใช้ปลายทางและผู้ให้บริการยอมรับในที่นี้ว่าหลักการด้านข้อขัดแย้งของกฎหมายและอนุสัญญาสหประชาชาติว่าด้วยสัญญาการขายสินค้าระหว่างประเทศจะไม่มีผลบังคับ คุณยอมรับโดยชัดเจนว่าการพิพาทหรือการเรียกร้องที่มาจากข้อตกลงนี้กับผู้ให้บริการ หรือการพิพาทหรือการเรียกร้องที่เกี่ยวข้องกับการใช้ซอฟต์แวร์จะอยู่ภายใต้อำนาจของศาลเขต Bratislava I และคุณยอมรับอย่างชัดเจนต่อการใช้อำนาจศาลในศาลเขตดังกล่าว

22. **บทบัญญัติทั่วไป** ถ้าบทบัญญัติใดของข้อตกลงนี้ไม่มีผลบังคับหรือเป็นโมฆะ ข้อตกลงนี้จะไม่มีผลต่อความถูกต้องของบทบัญญัติอื่นๆ ในข้อตกลง ซึ่งจะมีผลบังคับและถูกต้องตามเงื่อนไขที่ระบุไว้ในที่นี้ ข้อตกลงนี้ดำเนินการเป็นภาษาอังกฤษ ในกรณีที่การแปลข้อตกลงนี้จัดทำขึ้นเพื่อความสะดวกหรือวัตถุประสงค์อื่นใด หรือในกรณีที่มีความแตกต่างในระหว่างเวอร์ชันภาษาต่างๆ ของข้อตกลงนี้ ให้ยึดถือเวอร์ชันภาษาอังกฤษเป็นหลัก

ESET ขอสงวนสิทธิ์ในการเปลี่ยนแปลงซอฟต์แวร์ เช่นเดียวกับสงวนสิทธิ์ในการแก้ไขข้อตกลง ส่วนเพิ่มเติม ภาคผนวก นโยบายความเป็นส่วนตัว นโยบาย EOL และเอกสารเพิ่มเติม หรือส่วนใดส่วนหนึ่งของรายการดังกล่าวได้ตลอดเวลาโดยอัพเดทเอกสารที่เกี่ยวข้อง (i) เพื่อสะท้อนถึงการเปลี่ยนแปลงซอฟต์แวร์หรือวิธีที่ ESET ดำเนินธุรกิจ (ii) ด้วยเหตุผลด้านกฎหมาย ด้านข้อบังคับหรือความปลอดภัย หรือ (iii) เพื่อป้องกันการละเมิดหรืออันตราย คุณจะได้รับการแจ้งล่วงหน้าถึงการเปลี่ยนแปลงใดๆ ของข้อตกลงนี้ทางอีเมล การแจ้งเตือนภายในแอพ หรือทางอิเล็กทรอนิกส์ในรูปแบบอื่นๆ หากคุณไม่เห็นด้วยกับการเปลี่ยนแปลงที่เสนอในข้อตกลงคุณ สามารถยกเลิกข้อตกลงได้ตามข้อ 10 ภายใน 30 วันหลังจากได้รับหนังสือแจ้งการเปลี่ยนแปลง การเปลี่ยนแปลงที่เสนอจะถือว่าได้รับการยอมรับและมีผลบังคับใช้ต่อคุณ ณ วันที่คุณได้รับแจ้งการเปลี่ยนแปลง เว้นแต่คุณจะยุติข้อตกลงภายในระยะเวลาที่กำหนดไว้นี้

ข้อตกลงทั้งหมดนี้เป็นข้อตกลงระหว่างผู้ให้บริการกับคุณเกี่ยวกับซอฟต์แวร์ และมีผลเหนือกว่าการรับรอง การแลกเปลี่ยนความคิดเห็น ภาระหน้าที่ การสื่อสาร หรือโฆษณาที่เกี่ยวข้องกับซอฟต์แวร์ทั้งหมดที่เกิดขึ้นก่อนหน้านี้

EULAID: EULA-PRODUCT-LG; 3537.0

นโยบายความเป็นส่วนตัว

ESET, spol. s r. o., มีสำนักงานอยู่ที่ Einsteinova 24, 851 01 Bratislava, Slovak Republic ซึ่งจดทะเบียนในทะเบียนการค้าที่ได้รับการควบคุมดูแลโดย Bratislava I District Court, Section Sro, เลขที่ 3586/B หมายเลขทะเบียนธุรกิจ: 31333532 ในฐานะผู้ควบคุมข้อมูล ("ESET" หรือ "เรา") ต้องการให้มีความโปร่งใสในด้านการประมวลผลข้อมูลส่วนบุคคลและความเป็นส่วนตัวของลูกค้าของเรา เพื่อให้บรรลุเป้าหมายนี้ เราเผยแพร่นโยบายความเป็นส่วนตัวนี้โดยมีวัตถุประสงค์เพื่อแจ้งข้อมูลลูกค้าของเราเท่านั้น ("ผู้ใช้ปลายทาง" หรือ "คุณ") เกี่ยวกับหัวข้อต่อไปนี้:

- การประมวลผลข้อมูลส่วนบุคคล,
- การรักษาความลับของข้อมูล,
- สิทธิ์ของข้อมูล

การประมวลผลข้อมูลส่วนบุคคล

บริการที่ ESET นำเสนอในผลิตภัณฑ์ของเรามีให้ภายใต้ข้อกำหนดของข้อตกลงใบอนุญาตผู้ใช้ปลายทาง ("EULA") แต่บางผลิตภัณฑ์อาจต้องให้ความสนใจเป็นพิเศษ ราต้องการให้รายละเอียดเพิ่มเติมเกี่ยวกับการรวบรวมข้อมูลที่เกี่ยวข้องกับการให้บริการของเรา เราให้บริการต่างๆ ตามที่ได้อธิบายไว้ใน EULA และเอกสารเกี่ยวกับผลิตภัณฑ์ เช่น บริการอัพเดต/อัพเกรด ESET LiveGrid® การป้องกันการใช้ข้อมูลที่ไม่ถูกต้อง การสนับสนุน ฯลฯ เพื่อให้การทำงานทั้งหมด เราจำเป็นต้องรวบรวมข้อมูลต่อไปนี้:

- รายการอัพเดทและสถิติอื่นๆ ที่ครอบคลุมข้อมูลเกี่ยวกับกระบวนการติดตั้งและคอมพิวเตอร์ของคุณ รวมทั้งแพลตฟอร์มที่ติดตั้งผลิตภัณฑ์ของเราและข้อมูลเกี่ยวกับการดำเนินงานและฟังก์ชันการทำงานของผลิตภัณฑ์ของเรา เช่น ระบบปฏิบัติการ ข้อมูลฮาร์ดแวร์ ไอดีการติดตั้ง ไอดีใบอนุญาต ที่อยู่ IP ที่อยู่ MAC การตั้งค่าของผลิตภัณฑ์
- แฮชแบบวันเวย์ที่เกี่ยวกับการแทรกซึมที่เป็นส่วนหนึ่งของ ESET LiveGrid® Reputation System ซึ่งปรับปรุงประสิทธิภาพของโซลูชันการป้องกันมัลแวร์ของเราโดยการเปรียบเทียบไฟล์ที่ถูกสแกนกับฐานข้อมูลของรายการที่อยู่ในบัญชีขาวและบัญชีดำในคลาวด์

• ตัวอย่างและเมตาดาต้าที่น่าสงสัยจากภายนอกที่เป็นส่วนหนึ่งของ ESET LiveGrid® Feedback System ซึ่งช่วยให้ ESET สามารถตอบสนองต่อความต้องการของผู้ใช้ปลายทางของเราได้ทันที และช่วยให้เราสามารถตอบสนองต่อภัยคุกคามล่าสุดได้ เราจำเป็นต้องพึ่งพาข้อมูลที่คุณส่งให้เรา

o การแทรกซึมต่างๆ เช่น ตัวอย่างของไวรัสและโปรแกรมที่เป็นอันตรายอื่นๆ และที่น่าสงสัย ปัญหา วัตถุที่อาจไม่เป็นที่ต้องการหรืออาจไม่ปลอดภัย เช่น ไฟล์ที่สามารถเปิดใช้งานได้ ข้อความอีเมลที่คุณเป็นผู้รายงานว่าเป็นสแปมหรือที่ผลิตภัณฑ์ของเราปักธงเตือน

o ข้อมูลเกี่ยวกับอุปกรณ์ในเครือข่ายภายใน เช่น ประเภท, ผู้จำหน่าย รุ่นและ/หรือชื่อของอุปกรณ์

o ข้อมูลที่เกี่ยวกับการใช้อินเทอร์เน็ต เช่น ที่อยู่ IP และข้อมูลเกี่ยวกับภูมิศาสตร์, แพ็คเกจ IP, URL และเฟรมอีเธอร์เน็ต

o ไฟล์แครชดัมป์และข้อมูลต่างๆ ที่มีอยู่

ไม่ไม่ได้ประสงค์ที่จะรวบรวมข้อมูลของคุณนอกเหนือจากขอบเขตที่ระบุนี้ แต่ในบางเวลาเราก็ไม่สามารถที่จะป้องกันได้ ข้อมูลที่เก็บรวบรวมโดยไม่ได้ตั้งใจอาจรวมอยู่ในตัวของมัลแวร์เอง (เก็บรวบรวมโดยไม่ได้แจ้งให้คุณทราบหรือคุณไม่ได้อนุมัติ) หรือที่ถูกเก็บรวบรวมโดยเป็นส่วนหนึ่งของชื่อไฟล์หรือ URL และเรามิได้ต้องการข้อมูลเหล่านั้นมาเป็นส่วนหนึ่งของระบบของเราหรือประมวลผลข้อมูลเหล่านั้นตามวัตถุประสงค์ที่แจ้งไว้ในนโยบายความเป็นส่วนตัวนี้

• การดูข้อมูลเช่นไอดีใบอนุญาตและข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล ที่อยู่ ที่อยู่อีเมล นั้นจำเป็นสำหรับวัตุประสงค์ในการเรียกเก็บเงิน ตรวจสอบว่าใบอนุญาตเป็นของแท้หรือไม่ และจัดเตรียมการให้บริการของเรา

• ข้อมูลติดต่อและข้อมูลที่อยู่ในคำขอการสนับสนุนของคุณอาจจำเป็นสำหรับการให้บริการสนับสนุน โดยขึ้นอยู่กับช่องทางที่คุณเลือกในการติดต่อเรา เราอาจเก็บรวบรวมข้อมูลที่อยู่อีเมล หมายเลขโทรศัพท์ ข้อมูลใบอนุญาต รายละเอียดผลิตภัณฑ์ และคำอธิบายของกรณีการสนับสนุนของคุณ คุณอาจถูกขอให้ระบุข้อมูลอื่นๆ เพื่อให้บริการสนับสนุนรวดเร็วมากยิ่งขึ้น

การรักษาความลับข้อมูล

ESET เป็นบริษัทที่ดำเนินธุรกิจทั่วโลกผ่านทางหน่วยงานในเครือหรือคู่ค้าเป็นส่วนหนึ่งของเครือข่ายการกระจาย การให้บริการ และการสนับสนุนของเรา ข้อมูลที่ ESET เป็นผู้ประมวลผลอาจได้รับการถ่ายโอนไปยังและจากหน่วยงานในเครือหรือคู่ค้าสำหรับประสิทธิภาพของ EULA เช่นการให้บริการหรือการสนับสนุนหรือการเรียกเก็บเงิน โดยขึ้นอยู่กับตำแหน่งและบริการของคุณที่คุณเลือกที่จะใช้ เราอาจจำเป็นต้องถ่ายโอนข้อมูลของคุณไปยังประเทศที่จำเป็นต้องได้รับการตัดสินใจจากคณะกรรมาธิการยุโรป แม้ในกรณีนี้ การถ่ายโอนข้อมูลทั้งหมดจะต้องเป็นไปตามข้อกำหนดของ

กฎหมายการป้องกันข้อมูลและจะเกิดขึ้นเฉพาะเมื่อจำเป็นเท่านั้น ข้อตกลงตามสัญญามาตรฐาน ข้อบังคับของบริษัทที่ผูกมัด หรือมาตรการป้องกันที่เหมาะสมอื่นๆ จะต้องมีการจัดตั้งขึ้นโดยไม่มีข้อยกเว้นใดๆ

เรากำลังทำอย่างสุดความสามารถเพื่อป้องกันไม่ให้ข้อมูลถูกจัดเก็บนานเกินความจำเป็น ในขณะที่สามารถให้บริการตามมาตรฐานของ EULA ได้ ระยะเวลาการเก็บรักษาข้อมูลของเราอาจยาวนานกว่าอายุของใบอนุญาตของคุณ ก็เพียงเพื่อให้คุณมีเวลาสำหรับการต่ออายุที่ง่ายดายและสะดวกสบาย สถิติและข้อมูลอื่นๆ จาก ESET LiveGrid® ที่ย่อลงให้เล็กที่สุดและไม่ได้ระบุชื่ออาจได้รับการประมวลผลเพิ่มเติมเพื่อวัตถุประสงค์ทางด้านสถิติ

ESET ใช้มาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมเพื่อให้แน่ใจว่ามีระดับความปลอดภัยที่เหมาะสมกับความเสี่ยงที่อาจเกิดขึ้น เรากำลังพยายามอย่างเต็มที่เพื่อให้มั่นใจได้ถึงการรักษาความลับที่ต่อเนื่อง ความสมบูรณ์ ความพร้อมใช้งาน และความยืดหยุ่นของระบบและบริการด้านการประมวลผล อย่างไรก็ตาม ในกรณีที่ข้อมูลถูกละเมิดจนเป็นผลทำให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของคุณ เราพร้อมที่จะแจ้งให้หน่วยงานกำกับดูแลทราบรวมถึงเจ้าของข้อมูลด้วย ในฐานะเจ้าของข้อมูล คุณมีสิทธิที่จะยื่นเรื่องร้องเรียนต่อหน่วยงานกำกับดูแล

สิทธิของเจ้าของข้อมูล

ESET มีหน้าที่ต้องปฏิบัติตามกฎหมายของประเทศสโลวาเกียและเราต้องปฏิบัติตามกฎหมายว่าด้วยการปกป้องข้อมูลในฐานะส่วนหนึ่งของสหภาพยุโรป คุณมีสิทธิ์ที่จะติดตามสิทธิ์ในฐานะเจ้าของข้อมูลภายใต้เงื่อนไขที่กำหนดโดยกฎหมายคุ้มครองข้อมูลที่บังคับใช้:

- สิทธิ์ในการขอเข้าถึงข้อมูลส่วนบุคคลของคุณจาก ESET
- สิทธิ์ในการแก้ไขข้อมูลส่วนบุคคลของคุณหากไม่ถูกต้อง (คุณมีสิทธิ์ที่จะกรอกข้อมูลส่วนตัวที่ไม่สมบูรณ์)
- สิทธิ์ในการขอลบข้อมูลส่วนบุคคลของคุณ
- สิทธิ์ในการขอข้อจำกัดในการประมวลผลข้อมูลส่วนบุคคลของคุณ
- สิทธิ์ในการคัดค้านการประมวลผล
- สิทธิ์ในการยื่นเรื่องร้องเรียนและ
- สิทธิ์ในการเคลื่อนย้ายข้อมูล

เราเชื่อว่าทุกข้อมูลที่เราประมวลผลมีค่าและมีความจำเป็นต่อจุดประสงค์ด้านผลประโยชน์ตามกฎหมาย ซึ่งคือการให้บริการของผลิตภัณฑ์และมอบผลิตภัณฑ์ให้แก่ลูกค้าของเรา

หากคุณประสงค์ที่จะใช้สิทธิ์ของคุณในฐานะที่เป็นเจ้าของข้อมูล หรือหากคุณมีข้อสงสัยหรือข้อกังวล โปรดส่ง

ข้อความมาที่:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk