ESET Smart Security Premium

คู่มือผลิตภัณฑ์

คลิกที่นี่เพื่อแสดงเวอร์ชันออนไลน์ของเอกสารนี้

Digital Security
Progress. Protected.

ESET Smart Security Premium ได้รับการพัฒนาจาก ESET, spol. s r.o.

สำหรับข้อมูลเพิ่มเติม โปรดไปที่ https://www.eset.com

ฝ่ายสนับสนุนด้านเทคนิค: https://support.eset.com

REV. 12/4/2024

ESET Smart Security Premium

ESET Smart Security Premium เป็นวิธีการใหม่ในการรักษาความปลอดภัยคอมพิวเตอร์ที่ผสานรวมอย่างแท้จริง กลไกการสแกนเวอร์ชันใหม่ล่าสุดของ ESET LiveGrid® ที่ผสมผสานกับไฟร์วอลล์ที่กำหนดเองและโมดูลการป้องกันสแปม ใช้ความเร็วและความแม่นยำในการทำให้คอมพิวเตอร์ของคุณปลอดภัยอยู่เสมอ เป็นผลให้เกิดระบบอัจฉริยะที่ตื่นตัวอยู่เสมอต่อการโจมตีและซอฟต์แวร์ที่เป็นอันตรายซึ่งอาจก่อให้เกิดอันตรายต่อคอมพิวเตอร์ของคุณ

ESET Smart Security Premium เป็นโซลูชันการรักษาความปลอดภัยแบบสมบูรณ์ซึ่งผสมผสานการป้องกันขั้นสูงสุดและการใช้ทรัพยากรของระบบน้อยที่สุด เทคโนโลยีขั้นสูงของเราใช้ปัญญาประดิษฐ์เพื่อป้องกันการแฝงตัวจากไวรัส สปายแวร์ ม้าโทรจัน เวิร์ม แอดแวร์ รูทคิท และการโจมตีอื่นๆ โดยไม่ขัดขวางประสิทธิภาพการทำงานของระบบหรือรบกวนคอมพิวเตอร์ของคุณ

คุณลักษณะและคุณประโยชน์

ส่วนติดต่อผู้ใช้รูปแบบใหม่	ส่วนติดต่อผู้ใช้ในเวอร์ชันนี้ ได้รับการปรับรูปแบบใหม่อย่างเห็นได้ชัดและถูกทำให้ใช้ง่ายขึ้นซึ่งเป็นไปตามผลการทดสอบการใช้งาน การใช้คำและการแจ้งเตือนของ GUI ได้รับการทบทวนอย่างระมัดระวังและส่วนติดต่อให้การสนับสนุนภาษาที่อ่านจากขวาไปซ้ายเช่นฮิบรูและอารบิกแล้วในตอนนี้ ตัวช่วยออนไลน์ รวมเข้ากับ ESET Smart Security Premium แล้วในตอนนี้และให้เนื้อหาสนับสนุนที่ได้รับการอัพเดทอย่างต่อเนื่อง
การป้องกันไวรัสและสปายแวร์	ตรวจหาและกำจัดไวรัส เวิร์ม โทรจัน และรูทคิท ทั้งที่รู้จักและไม่รู้จักในเชิงรุกได้มากกว่า การวิเคราะห์พฤติกรรมขั้นสูงจะกำหนดสถานะแม้กระทั่งมัลแวร์ที่ไม่เคยพบเห็นมาก่อน ซึ่งจะช่วยป้องกันคุณจากภัยคุกคามที่ไม่รู้จักและลดประสิทธิภาพภัยคุกคามก่อนที่จะก่อให้เกิดอันตราย การป้องกันการเข้าถึงเว็บ และ การป้องกันฟิชชิ่งทำงานโดยการตรวจสอบการสื่อสารระหว่างเบราว์เซอร์เว็บและเซิร์ฟเวอร์ระยะไกล (รวมถึง SSL) การป้องกันไคลเอ็นต์อีเมล ให้การควบคุมการสื่อสารทางอีเมลที่ได้รับผ่านโปรโตคอล POP3(S) และ IMAP(S)
การอัพเดทเป็นประจำ	การอัพเดทกลไกตรวจหา (ก่อนหน้านี้เรียกว่า "ฐานข้อมูลไวรัส") และโมดูลโปรแกรมเป็นประจำเป็นวิธีที่ดีที่สุดเพื่อให้แน่ใจว่าคอมพิวเตอร์ของคุณจะมีระดับการรักษาความปลอดภัยสูงสุด
ESET LiveGrid® (ความเชื่อถือที่อ้างอิงคลาวด์)	คุณ สามารถตรวจสอบความเชื่อถือของกระบวนการและไฟล์ที่ทำงานอยู่ได้โดยตรงจาก ESET Smart Security Premium
การควบคุมอุปกรณ์	สแกนอุปกรณ์ USB การ์ดหน่วยความจำ และซีดี/ดีวีดีทั้งหมดโดยอัตโนมัติ ปิดกั้นสื่อที่ถอดเข้าออกได้ตามประเภทของสื่อ ผู้ผลิต ขนาด และแอตทริบิวต์อื่นๆ
ฟังก์ชันการทำงานของ HIPS	คุณสามารถปรับแต่งการทำงานของระบบได้ละเอียดมากขึ้น ไม่ว่าจะเป็นระบุกฎสำหรับรีจิสตรีของระบบ กระบวนการและโปรแกรมที่ใช้งาน และปรับแต่งลักษณะการรักษาความปลอดภัยของคุณ
โหมดผู้เล่นเกม	เลื่อนหน้าต่างป๊อปอัปทั้งหมด การอัพเดท หรือกิจกรรมอื่นๆ ที่ต้องใช้ทรัพยากรระบบอย่างมากเพื่อเล่นเกมและทำกิจกรรมแบบเต็มหน้าจออื่นๆ

คุณลักษณะใน ESET Smart Security Premium

การป้องกันการธนาคารและการชำระเงิน	การป้องกันทางด้านธนาคารและการชำระเงินจะมอบเบราว์เซอร์ที่มีการป้องกันสำหรับใช้เมื่อเข้าถึงเกตเวย์การธนาคารออนไลน์หรือการชำระเงินออนไลน์เพื่อให้มั่นใจว่าธุรกรรมออนไลน์ทั้งหมดทำขึ้นในสภาพแวดล้อมที่น่าเชื่อถือและปลอดภัย
รองรับฐานข้อมูลเครือข่าย	ฐานข้อมูลเครือข่ายให้การระบุอย่างรวดเร็วและปิดกั้นการรับส่งข้อมูลที่เป็นอันตรายที่ส่งไปที่หรือมาจากอุปกรณ์ของผู้ใช้เช่นบอตและแพ็คการหาจุดอ่อน คุณลักษณะอาจถูกพิจารณาให้เป็นการปรับปรุงการป้องกันบอตเน็ต
ไฟร์วอลล์อัจฉริยะ	ป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตเพื่อไม่ให้เข้าถึงคอมพิวเตอร์และใช้ประโยชน์จากข้อมูลส่วนบุคคลของคุณ
การป้องกันสแปมของ ESET	โดยมีสัดส่วนร้อยละ 50 ของการสื่อสารทางอีเมลทั้งหมด การป้องกันสแปมจะช่วยป้องกันปัญหานี้
การป้องกันการโจรกรรม	การป้องกันการโจรกรรม ขยายความปลอดภัยของระดับของผู้ใช้ในกรณีที่คอมพิวเตอร์สูญหายหรือถูกโขมย เมื่อผู้ใช้ติดตั้ง ESET Smart Security Premium และ การป้องกันการโจรกรรม อุปกรณ์ของผู้ใช้จะปรากฏในส่วนติดต่อทางเว็บ ส่วนติดต่อทางเว็บจะอนุญาตให้ผู้ใช้จัดการการกำหนดค่า การป้องกันการโจรกรรม ของพวกเขาและดูแลคุณลักษณะการป้องกันการโจรกรรมในอุปกรณ์ของพวกเขา
การควบคุมเนื้อหา	ปกป้องครอบครัวของคุณจากเนื้อหาทางเว็บที่อาจไม่เหมาะสมด้วยการปิดกั้นเว็บไซต์หลายประเภท
Password Manager	Password Manager จะปกป้องและจัดเก็บรหัสผ่านและข้อมูลส่วนตัวของคุณ
Secure Data	โดยอนุญาตให้คุณเข้ารหัสข้อมูลบนคอมพิวเตอร์และ USB ไดรฟ์ของคุณเพื่อป้องกันการใช้งานข้อมูลส่วนตัวที่เป็นความลับในทางที่ผิด
ESET LiveGuard	ค้นพบและหยุดภัยคุกคามที่ไม่เคยเห็นมาก่อน และประมวลผลข้อมูลเพื่อการตรวจจับในอนาคต

ต้องใช้ใบอนุญาตเพื่อให้คุณลักษณะของ ESET Smart Security Premium สามารถทำงานได้ ขอแนะนำให้คุณต่ออายุใบอนุญาตล่วงหน้าหลายสัปดาห์ก่อนที่ใบอนุญาตสำหรับ ESET Smart Security Premium จะหมดอายุ

มีอะไรใหม่

มีอะไรใหม่ใน ESET Smart Security Premium 15

ตัวตรวจสอบเครือข่าย (เดิมเรียกว่า อุปกรณ์ภายในบ้านที่เชื่อมต่ออยู่) ที่ปรับปรุงแล้ว

ช่วยปกป้องเครือข่ายและอุปกรณ์ IoT ของคุณ และแสดงอุปกรณ์ที่เชื่อมต่อกับเราเตอร์ ดูวิธีการ ตรวจสอบเครือข่ายที่คุณกำลังใช้และอุปกรณ์ที่เชื่อมต่ออยู่

ESET HOME (เดิมชื่อ myESET)

เพิ่มการมองเห็นและการควบคุมความปลอดภัยของคุณ ติดตั้งการป้องกันสำหรับอุปกรณ์ใหม่ เพิ่มและแบ่งปันใบ

อนุญาต และรับการแจ้งเตือนที่สำคัญผ่านแอพโทรศัพท์มือถือและเว็บพอร์ทัล สำหรับข้อมูลเพิ่มเติม โปรดเยี่ยมชม คู่มือความช่วยเหลือออนไลน์ ESET HOME

ระบบป้องกันการบุกรุกที่ใช้โฮสต์ (HIPS) ที่ปรับปรุงแล้ว

สแกนพื้นที่หน่วยความจำที่สามารถแก้ไขได้ด้วยเทคนิคการปล่อยมัลแวร์เข้าระบบที่ซับซ้อน การปรับปรุงนี้จะช่วยขยายความสามารถทางเทคโนโลยีในการตรวจจับการบุกรุกโดยมัลแวร์ที่มีความซับซ้อนมากที่สุดได้

ESET LiveGuard

เทคโนโลยีการป้องกันระดับเฟิร์สคลาสที่ปรับให้เหมาะกับคุณ ชั้นความปลอดภัยใหม่ที่มีการกำหนดค่าโดยอัตโนมัตินี้จะค้นหาและหยุดภัยคุกคามที่ไม่เคยเห็นมาก่อน และประมวลผลข้อมูลเพื่อการตรวจจับในอนาคตได้ ดูข้อมูล เพิ่มเติมเกี่ยวกับ LiveGuard

---

สำหรับรูปภาพและข้อมูลเพิ่มเติมเกี่ยวกับคุณลักษณะใหม่ใน ESET Smart Security Premium โปรดดู มีอะไรใหม่ในผลิตภัณฑ์ ESET สำหรับใช้งานในบ้านเวอร์ชันล่าสุด

> หากต้องการปิดใช้งาน **การแจ้งเตือนมีอะไรใหม่** ให้คลิก **การตั้งค่าขั้นสูง** > **การแจ้งเตือน** > **การแจ้งเตือนบนเดสก์ท็อป** คลิก **แก้ไข** ถัดจาก **การแจ้งเตือนบนเดสก์ท็อป** และยกเลิกการเลือกช่องทำเครื่องหมาย **แสดงการแจ้งเตือนมีอะไรใหม่** สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการแจ้งเตือน โปรดดูส่วน การแจ้งเตือน

ฉันมีผลิตภัณฑ์ใดอยู่

ESET มีความปลอดภัยหลากหลายชั้นให้เลือกสรร พร้อมผลิตภัณฑ์ใหม่ๆ ตั้งแต่โซลูชันป้องกันไวรัสที่ทรงพลังและรวดเร็วไปจนถึงโซลูชันป้องกันไวรัสแบบครบวงจรซึ่งใช้ทรัพยากรของระบบน้อยที่สุด ดังนี้:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

เพื่อระบุว่าคุณติดตั้งผลิตภัณฑ์ใดเอาไว้ ให้เปิด หน้าต่างโปรแกรมหลัก แล้วคุณจะเห็นชื่อของผลิตภัณฑ์ที่ด้านบนสุดของหน้าต่าง (โปรดดู บทความฐานความรู้)

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
กลไกการตรวจจับ	✔	✔	✔
การเรียนรู้ของเครื่องขั้นสูง	✔	✔	✔
การป้องกันการโจมตีแบบ Exploit	✔	✔	✔
การป้องกันการโจมตีที่ใช้สคริปต์	✔	✔	✔
การป้องกันฟิชชิ่ง	✔	✔	✔
การป้องกันการเข้าถึงเว็บ	✔	✔	✔
HIPS (รวมถึง การป้องกันแรนซั่มแวร์)	✔	✔	✔
การป้องกันสแปม		✔	✔
ไฟร์วอลล์		✔	✔
ตัวตรวจสอบเครือข่าย		✔	✔
การป้องกัน Webcam		✔	✔
การป้องกันการโจมตีเครือข่าย		✔	✔
การป้องกันบอตเน็ต		✔	✔
การป้องกันการธนาคารและการชำระเงิน		✔	✔
การควบคุมเนื้อหา		✔	✔
การป้องกันการโจรกรรม		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

ผลิตภัณฑ์ข้างต้นบางรายการอาจไม่สามารถใช้ได้สำหรับภาษา/ภูมิภาคของคุณ

ความต้องการของระบบ

เพื่อให้สามารถทำงานได้อย่างเหมาะสม ระบบของคุณควรเป็นไปตามข้อกำหนดด้านฮาร์ดแวร์และซอฟต์แวร์สำหรับ ESET Smart Security Premium ดังต่อไปนี้:

ตัวประมวลผลที่รองรับ

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

ตัวประมวลผล ARM64, 1 GHz หรือสูงกว่า

ระบบปฏิบัติการที่สนับสนุน*

Microsoft® Windows® 11
Microsoft® Windows® 10
Microsoft® Windows® 8.1

Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 ที่มีการอัพเดท Windows ล่าสุด

Microsoft® Windows® Home Server 2011 64-bit

โปรดพยายามอัพเดทระบบปฏิบัติการของคุณให้ทันสมัยเสมอ

การป้องกันการโจรกรรม ไม่รองรับการทำงานของ Microsoft Windows Home Server

อื่นๆ

ต้องใช้การเชื่อมต่ออินเทอร์เน็ตในการเปิดใช้งานและอัพเดท ESET Smart Security Premium เพื่อให้ทำงานได้อย่างปกติ

โปรแกรมป้องกันไวรัสสองโปรแกรมที่ทำงานพร้อมกันบนอุปกรณ์เดียวทำให้เกิดความขัดแย้งของทรัพยากรระบบที่หลีกเลี่ยงไม่ได้ เช่น การชะลอตัวของระบบเพื่อให้ไม่สามารถทำงานได้

*ESET จะไม่สามารถมอบการป้องกันให้แก่ระบบปฏิบัติการที่ไม่รองรับได้หลังเดือนกุมภาพันธ์ 2021

Windows 7 เวอร์ชันของคุณไม่ได้อัพเดท

ปัญหา

คุณกำลังใช้ระบบปฏิบัติการเวอร์ชันที่ไม่ได้อัพเดท หากต้องการให้มีการป้องกันต่อไป โปรดพยายามอัพเดทระบบปฏิบัติการของคุณให้ทันสมัยเสมอ

โซลูชัน

คุณได้ติดตั้ง ESET Smart Security Premium ที่ใช้งาน {GET_OSNAME} {GET_BITNESS}

ตรวจสอบว่าคุณได้ติดตั้ง Windows 7 Service Pack 1 (SP1) ที่มีการอัพเดท Windows ล่าสุด (KB4474419 และ KB4490628 เป็นอย่างน้อย)

หาก Windows 7 ของคุณไม่ได้รับการกำหนดค่าให้อัพเดทโดยอัตโนมัติ ให้คลิก**เมนูเริ่มต้น** > **แผงควบคุม** > **ระบบและความปลอดภัย** > **Windows Update** > **ตรวจหาอัพเดต** แล้วจากนั้นให้คลิก **ติดตั้งการปรับปรุง**

ทั้งนี้โปรดดู Windows 7 ไม่ได้รับการสนับสนุนจาก Microsoft อีกต่อไป

Windows 7 ไม่ได้รับการสนับสนุนจาก Microsoft อีกต่อไป

ปัญหา

การสนับสนุน Windows 7 ของ Microsoft ได้หมดลงแล้วในวันที่ 14 มกราคม 2020 หมายความว่าอย่างไร

หากคุณยังคงใช้ Windows 7 หลังจากการสนับสนุนได้สิ้นสุดลงแล้ว พีซีของคุณจะยังคงทำงานอยู่แต่อาจเสี่ยงต่อความเสี่ยงด้านความปลอดภัยและไวรัสมากขึ้น พีซีของคุณจะไม่ได้รับ Windows Update อีกต่อไป (รวมถึงการอัพเดทด้านความปลอดภัย)

โซลูชัน

ต้องการปรับรุ่นจาก Windows 7 เป็น Windows 10 หรือไม่ อัพเดทผลิตภัณฑ์ ESET ของคุณ

กระบวนการปรับรุ่นจะค่อนข้างง่าย และในหลายกรณีคุณสามารถทำได้โดยไม่สูญเสียไฟล์ของคุณ: ก่อนการอัพเกรดเป็น Windows 10:

1. ตรวจสอบ/อัพเดทผลิตภัณฑ์ ESET ของคุณ
2. การสำรองข้อมูลสำคัญ
3. อ่านคำถามที่ถามบ่อยเกี่ยวกับการปรับรุ่นเป็น Windows 10 ของ Microsoft และอัพเดทระบบปฏิบัติการ Windows ของคุณ

มีคอมพิวเตอร์หรืออุปกรณ์เครื่องใหม่ใช่ไหม โปรดโอนผลิตภัณฑ์ ESET

หากคุณกำลังจะซื้อหรือได้ซื้อคอมพิวเตอร์หรืออุปกรณ์เครื่องใหม่แล้ว โปรดเรียนรู้เกี่ยวกับ วิธีโอนผลิตภัณฑ์ ESET ไปยังอุปกรณ์เครื่องใหม่

> โปรดดู การสนับสนุนสำหรับ Windows 7 สิ้นสุดลงแล้ว ด้วยเช่นกัน

Windows Vista ไม่ได้รับการสนับสนุนอีกต่อไป

ปัญหา

เนื่องจากข้อจำกัดด้านเทคนิคใน Windows Vista ESET Smart Security Premium จึงไม่สามารถมอบการป้องกันได้หลังจาก **เดือนกุมภาพันธ์ 2021** ผลิตภัณฑ์ ESET จะ **ไม่สามารถทำงานได้** ซึ่งอาจทำให้ระบบของคุณเสี่ยงต่อการถูกบุกรุก

การสนับสนุน Windows Vista ของ Microsoft ได้หมดลงแล้วในวันที่ 11 เมษายน 2017 หมายความว่าอย่างไร

หากคุณยังคงใช้ Windows Vista หลังจากการสนับสนุนได้สิ้นสุดลงแล้ว พีซีของคุณจะยังคงทำงานอยู่แต่อาจเสี่ยงต่อความเสี่ยงด้านความปลอดภัยและไวรัสมากขึ้น พีซีของคุณจะไม่ได้รับ Windows Update อีกต่อไป (รวมถึงการอัพเดทด้านความปลอดภัย)

โซลูชัน

จะอัพเกรดจาก Windows Vista เป็น Windows 10 ใช่ไหม โปรดซื้อคอมพิวเตอร์หรืออุปกรณ์เครื่องใหม่และถ่ายโอนผลิตภัณฑ์ ESET

ก่อนการอัพเกรดเป็น Windows 10:

1. การสำรองข้อมูลสำคัญ
2. อ่านคำถามที่ถามบ่อยเกี่ยวกับการปรับรุ่นเป็น Windows 10 ของ Microsoft และอัพเดทระบบปฏิบัติการ Windows ของคุณ
3. ติดตั้งหรือ ถ่ายโอนผลิตภัณฑ์ ESET ไปยังอุปกรณ์เครื่องใหม่

> โปรดดู การสนับสนุนสำหรับ Windows Vista สิ้นสุดลงแล้ว ด้วยเช่นกัน

การป้องกัน

เมื่อคุณทำงานกับคอมพิวเตอร์ของคุณ และโดยเฉพาะเมื่อคุณเรียกใช้อินเทอร์เน็ต โปรดระลึกไว้ว่าไม่มีระบบป้องกันไวรัสใดในโลกที่สามารถกำจัดความเสี่ยงจากการตรวจหา และ การโจมตีระยะไกล เมื่อต้องการเพิ่มการป้องกันและความสะดวกสูงสุด จึงจำเป็นที่คุณต้องใช้โซลูชันป้องกันไวรัสอย่างถูกต้องและปฏิบัติตามกฎที่มีประโยชน์ต่างๆ:

อัพเดทเป็นประจำ

ตามสถิติจาก ESET LiveGrid® การแฝงตัวแบบใหม่และไม่ซ้ำกันหลายพันแบบจะถูกสร้างขึ้นทุกวันเพื่อให้สามารถผ่านการวัดความปลอดภัยที่มีอยู่และสร้างผลกำไรให้กับผู้เขียนได้ โดยสร้างความเสียหายให้เกิดขึ้นกับผู้ใช้อื่น ผู้เชี่ยวชาญที่ห้องปฏิบัติการไวรัสของ ESET จะวิเคราะห์การคุกคามเหล่านี้ทุกวัน และจัดเตรียมและเผยแพร่การอัพเดทเพื่อปรับปรุงระดับการป้องกันอย่างต่อเนื่องสำหรับผู้ใช้ของเรา เพื่อให้แน่ใจว่าการอัพเดทเหล่านี้มีประสิทธิภาพสูงสุด จึงจำเป็นต้องกำหนดค่าการอัพเดทอย่างถูกต้องในระบบของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีกำหนดค่าการอัพเดท โปรดดูในบท การตั้งค่าการอัพเดท

ดาวน์โหลดโปรแกรมแก้ไขด้านความปลอดภัย

ผู้เขียนซอฟต์แวร์ที่เป็นอันตรายมักใช้จุดอ่อนของระบบต่างๆ เพื่อเพิ่มประสิทธิภาพของการแพร่รหัสที่เป็นอันตราย เมื่อทราบเช่นนี้แล้ว บริษัทซอฟต์แวร์จึงต้องติดตามจุดอ่อนต่างๆ อย่างใกล้ชิดในแอพพลิเคชันของตน เพื่อแสดงและเผยแพร่การอัพเดทการรักษาความปลอดภัยที่จะกำจัดการคุกคามที่อาจเกิดขึ้นเป็นประจำ จึงเป็นสิ่งจำเป็นที่ต้องดาวน์โหลดการอัพเดทการรักษาความปลอดภัยเหล่านี้เมื่อมีการเผยแพร่ Microsoft Windows และเว็บเบราว์เซอร์ เช่น Internet Explorer คือตัวอย่างของสองโปรแกรมที่มีการเผยแพร่การอัพเดทการรักษาความปลอดภัยตามกำหนดการเป็นประจำ

การสำรองข้อมูลสำคัญ

ผู้เขียนมัลแวร์จะไม่สนใจเกี่ยวกับความจำเป็นของผู้ใช้ และการทำงานของโปรแกรมที่เป็นอันตรายมักจะนำไปสู่การทำงานไม่ถูกต้องทั้งหมดของระบบปฏิบัติการและการสูญหายของข้อมูลสำคัญ ดังนั้นจึงต้องสำรองข้อมูลสำคัญและที่เป็นความลับของคุณไปยังแหล่งที่มาภายนอกอยู่เสมอ เช่น DVD หรือฮาร์ดไดรฟ์ภายนอก ซึ่งจะทำให้กู้คืนข้อมูลของคุณได้ง่ายดายและรวดเร็วยิ่งขึ้นในกรณีที่ระบบล้มเหลว

สแกนคอมพิวเตอร์เพื่อหาไวรัสเป็นประจำ

การตรวจหาไวรัส เวิร์ม โทรจัน และรูทคิทที่รู้จักและไม่รู้จักได้มากขึ้นจะมีการจัดการโดยโมดูลการป้องกันระบบไฟล์แบบเรียลไทม์ ซึ่งหมายความว่าทุกครั้งที่คุณเข้าถึงหรือเปิดไฟล์ ระบบจะสแกนเพื่อหากิจกรรมของมัลแวร์ เราขอแนะนำให้คุณเรียกใช้การสแกนคอมพิวเตอร์แบบเต็มรูปแบบอย่างน้อยเดือนละครั้ง เนื่องจากฐานข้อมูลมัลแวร์อาจหลากหลายและกลไกตรวจหาจะอัพเดทตัวเองทุกวัน

ปฏิบัติตามกฎการรักษาความปลอดภัยพื้นฐาน

กฎนี้เป็นกฎที่มีประโยชน์และมีประสิทธิภาพมากที่สุด ซึ่งผู้ใช้ควรให้ความสนใจอยู่เสมอ ในปัจจุบัน การบุกรุกจำนวนมากต้องการการดำเนินการของผู้ใช้เพื่อให้ระบบทำงานและกระจายการบุกรุก หากคุณมีความระมัดระวังเมื่อเปิดไฟล์ใหม่ คุณจะสามารถประหยัดเวลาและความพยายามที่จะต้องใช้ในการกำจัดการบุกรุกได้เป็นอย่างมาก คำแนะนำที่มีประโยชน์มีดังนี้:

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

หน้าวิธีใช้

ยินดีต้อนรับสู่คู่มือผู้ใช้ ESET Smart Security Premium ข้อมูลที่ให้มานี้จะช่วยสร้างความคุ้นเคยเกี่ยวกับผลิตภัณฑ์ให้คุณ และช่วยทำให้คอมพิวเตอร์มีความปลอดภัยมากยิ่งขึ้น

การเริ่มต้นใช้งาน

ก่อนใช้ ESET Smart Security Premium เราแนะนำให้คุณทำความคุ้นเคยกับ ประเภทของการตรวจหา และ การโจมตีระยะไกล หลายประเภท คุณอาจพบเมื่อใช้คอมพิวเตอร์ของคุณ

นอกจากนี้ เรายังคอมไพล์รายการของ คุณลักษณะใหม่ ที่มีใน ESET Smart Security Premium และคำแนะนำเพื่อช่วยคุณกำหนดการตั้งค่าพื้นฐานต่างๆ

วิธีใช้หน้าวิธีใช้ของ ESET Smart Security Premium

หัวข้อวิธีใช้ต่างๆ จะแบ่งออกเป็นหลายบทและหลายบทแยกย่อย กด **F1** เพื่อดูข้อมูลเกี่ยวกับหน้าต่างที่คุณกำลังเปิดอยู่

โปรแกรมช่วยให้คุณค้นหาหัวข้อวิธีใช้ด้วยคำหลัก หรือค้นหาเนื้อหาโดยพิมพ์คำหรือวลี ความแตกต่างระหว่างสองวิธีนี้ก็คือ คำหลักนั้นอาจมีเนื้อหาเกี่ยวข้องกับหน้าวิธีใช้ที่ไม่ได้มีคำหลักนั้นๆ อยู่ในข้อความก็ได้ การค้นหาตามคำและวลีจะค้นหาเนื้อหาของหน้าวิธีใช้ทั้งหมด และแสดงเฉพาะที่มีคำหรือวลีนั้นๆ ในข้อความเท่านั้น

เพื่อความสอดคล้องและช่วยป้องกันการสับสน ศัพท์บัญญัติที่ใช้ในคำแนะนำนี้จะไปเป็นตามชื่อศัพท์บัญญัติพารามิเตอร์ของ ESET Smart Security Premium นอกจากนี้เรายังใช้ชุดรูปแบบสัญลักษณ์ชุดหนึ่งเพื่อเน้นหัวข้อต่างๆ ที่น่าสนใจเป็นพิเศษหรือมีความสำคัญ

บันทึกย่อเป็นเพียงการสำรวจสั้นๆ เท่านั้น ถึงแม้ว่าคุณจะสามารถข้ามได้ แต่บันทึกย่อมีข้อมูลที่มีประโยชน์อย่างยิ่ง เช่น คุณสมบัติที่เฉพาะเจาะจงหรือลิงก์ไปที่หัวข้อบางหัวข้อ

ซึ่งคุณควรให้ความใส่ใจกับบันทึกนี้ เราจึงขอแนะนำไม่ให้คุณข้าม ปกติแล้ว ในบันทึกจะมีข้อมูลที่ไม่จำเป็น แต่มีความสำคัญ

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

การติดตั้ง

สามารถติดตั้ง ESET Smart Security Premium ในคอมพิวเตอร์ของคุณได้หลายวิธี วิธีการติดตั้งอาจแตกต่างกันไปทั้งนี้ขึ้นอยู่กับประเทศและวิธีการแจกจ่าย:

- Live Installer — ดาวน์โหลดจากเว็บไซต์ของ ESET หรือ CD/DVD แพ็คเกจติดตั้งจะเหมือนกันสำหรับทุกภาษา (เลือกภาษาที่เหมาะสม) Live Installer เป็นไฟล์ขนาดเล็ก ไฟล์เพิ่มเติมที่จำเป็นในการติดตั้ง ESET Smart Security Premium จะถูกดาวน์โหลดโดยอัตโนมัติ

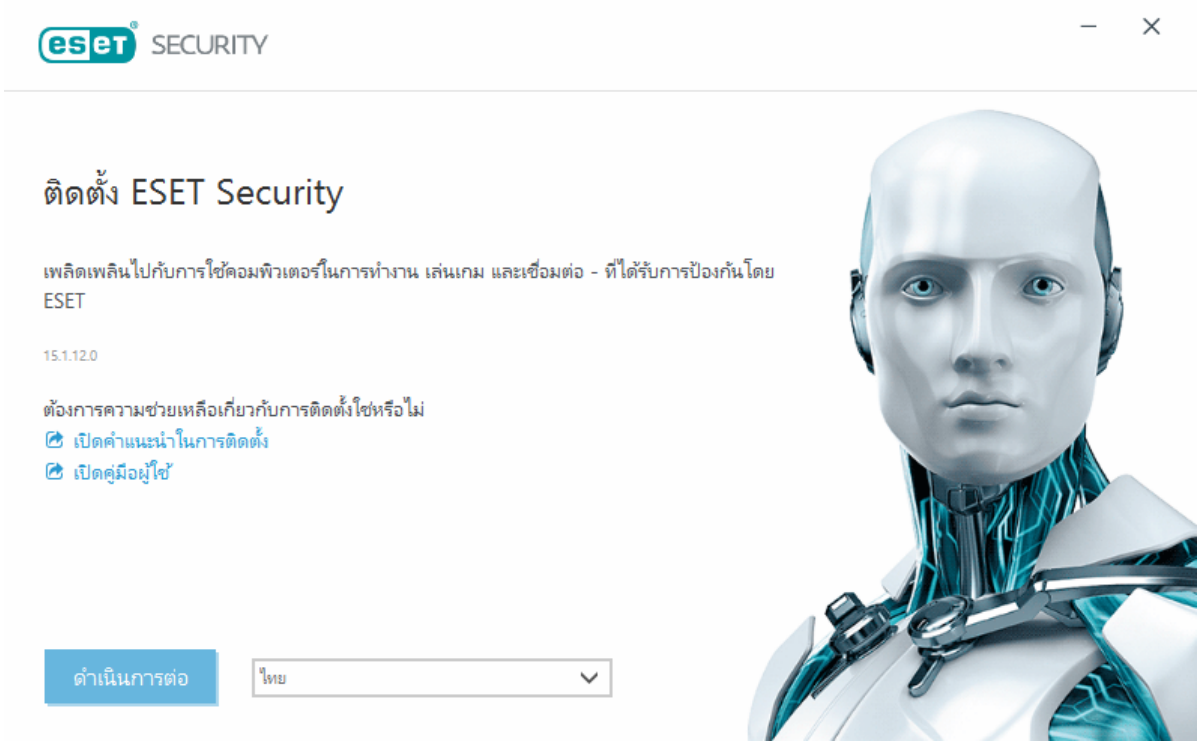
• การติดตั้งแบบออฟไลน์ – ใช้ไฟล์ .exe ที่มีขนาดใหญ่กว่าไฟล์ Live Installer และไม่จำเป็นต้องเชื่อมต่ออินเทอร์เน็ตหรือไฟล์เพิ่มเติมเพื่อดำเนินการติดตั้งให้เสร็จสมบูรณ์

โปรดตรวจสอบให้แน่ใจว่าไม่มีโปรแกรมป้องกันไวรัสอื่นติดตั้งอยู่บนคอมพิวเตอร์ของคุณก่อนที่คุณจะติดตั้ง ESET Smart Security Premium ถ้ามีการติดตั้งโซลูชันการป้องกันไวรัสสองชนิดขึ้นไปบนคอมพิวเตอร์เครื่องเดียว อาจมีการทำงานที่ขัดแย้งกัน ขอแนะนำให้คุณลบการติดตั้งโปรแกรมป้องกันไวรัสอื่นในระบบของคุณ โปรดดู บทความฐานความรู้ของ ESET สำหรับรายการของเครื่องมือถอนการติดตั้งสำหรับซอฟต์แวร์ป้องกันไวรัสที่ใช้กันทั่วไป (ให้บริการเป็นภาษาอังกฤษและภาษาอื่นๆ อีกมากมาย)

โปรแกรมติดตั้งที่ใช้งานออนไลน์

เมื่อคุณได้ดาวน์โหลด แพ็คเกจการติดตั้ง Live installer ให้คลิกสองครั้งที่ไฟล์การติดตั้งและทำตามคำแนะนำแบบทีละขั้นตอนในวิซาร์ดตัวติดตั้ง

สำหรับการติดตั้งประเภทนี้ คุณต้องเชื่อมต่ออินเทอร์เน็ต



1.เลือกภาษาที่เหมาะสมจากเมนูแบบเลื่อนลงแล้วคลิก **ดำเนินการต่อ**

หากคุณกำลังติดตั้งเวอร์ชันที่ใหม่กว่าทับเวอร์ชันก่อนหน้าที่มีการตั้งค่าที่ป้องกันด้วยรหัสผ่าน ให้ป้อนรหัสผ่านของคุณด้วย คุณสามารถกำหนดค่ารหัสผ่านการตั้งค่าได้ใน การตั้งค่าการเข้าถึง

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

- ESET LiveGrid® ระบบคำติชม
- แอพพลิเคชันที่อาจไม่พึงประสงค์
- โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า

เมื่อคลิก **ดำเนินการต่อ** หรือ **อนุญาตทั้งหมดและดำเนินการต่อ** จะถือว่าคุณยอมรับข้อตกลงการอนุญาตใช้งานสำหรับผู้ใช้ปลายทางและรับทราบนโยบายความเป็นส่วนตัวแล้ว

3. หากต้องการเปิดใช้งาน จัดการ และดูความปลอดภัยของอุปกรณ์โดยใช้ ESET HOME ให้ เชื่อมต่ออุปกรณ์ของคุณกับบัญชี ESET HOME คลิก **ข้ามการล็อคอิน** เพื่อดำเนินการต่อโดยไม่ต้องเชื่อมต่อ ESET HOME คุณสามารถเชื่อมต่ออุปกรณ์เข้ากับบัญชี ESET HOME ของคุณได้ในภายหลัง

4. หากคุณดำเนินการต่อโดยไม่เชื่อมต่อกับ ESET HOME ให้เลือกตัวเลือกการเปิดใช้งาน หากคุณกำลังติดตั้งเวอร์ชันล่าสุดทับเวอร์ชันก่อนหน้า รหัสใบอนุญาตจะถูกป้อนโดยอัตโนมัติ

5. วิซาร์ดการติดตั้งจะกำหนดผลิตภัณฑ์ของ ESET ที่ติดตั้งตามใบอนุญาตของคุณ เวอร์ชันที่มีคุณลักษณะด้านความปลอดภัยมากที่สุดจะถูกเลือกไว้ล่วงหน้าเสมอ คลิก **เปลี่ยนผลิตภัณฑ์** หากคุณต้องการ ติดตั้งผลิตภัณฑ์ ESET เวอร์ชันอื่น คลิก **ดำเนินการต่อ** เพื่อเริ่มกระบวนการติดตั้ง ซึ่งอาจใช้เวลาสักครู่

หากมีรายการที่เหลือ (ไฟล์หรือโฟลเดอร์) จากผลิตภัณฑ์ของ ESET ที่ถูกถอนการติดตั้งในอดีต ระบบจะขอให้คุณอนุญาตเพื่อลบออก คลิก **ติดตั้ง** เพื่อดำเนินการต่อ

6. คลิก**เสร็จสิ้น** เพื่อออกจากวิซาร์ดการติดตั้ง

การติดตั้งตัวแก้ไขปัญหา

หลังจากที่ผลิตภัณฑ์ถูกติดตั้งและเปิดใช้งาน โมดูลจะเริ่มดาวน์โหลด การป้องกันกำลังเริ่มต้นและคุณสมบัติอาจยังทำงานได้ไม่เต็มที่จนกว่าการดาวน์โหลดจะเสร็จสมบูรณ์

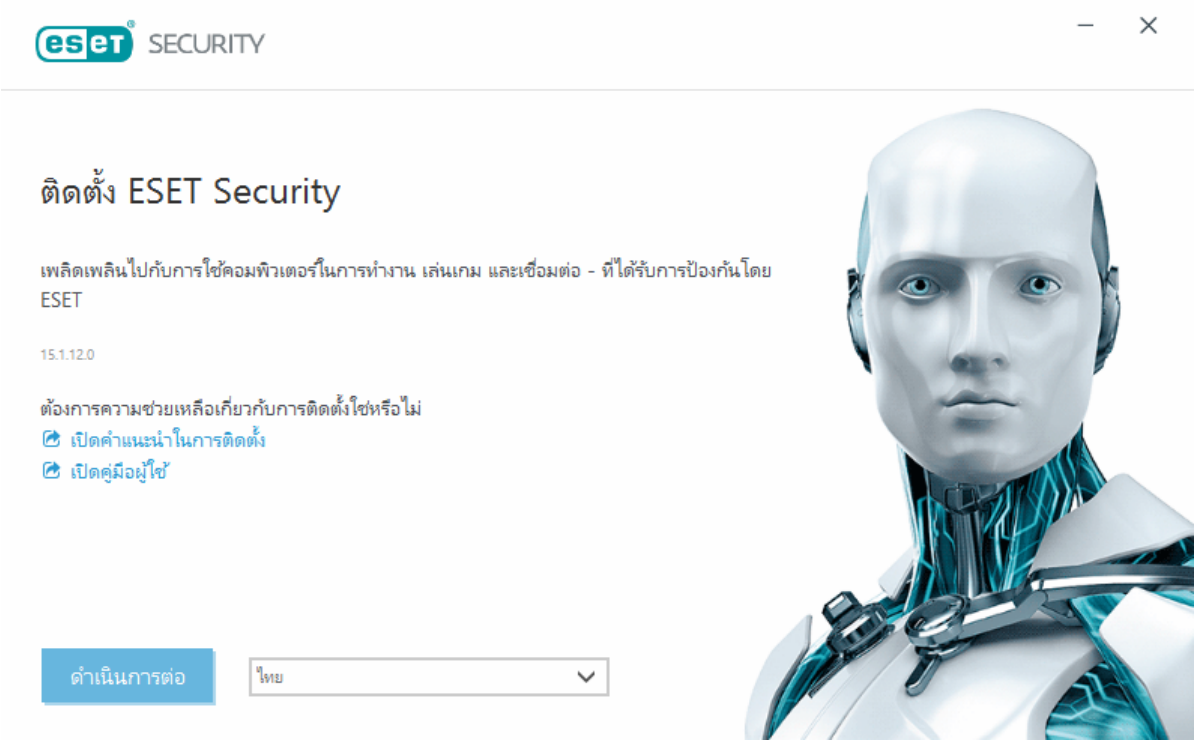
การติดตั้งแบบออฟไลน์

ดาวน์โหลดและติดตั้งผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้านโดยใช้ตัวติดตั้งแบบออฟไลน์ (.exe) ด้านล่าง เลือกเวอร์ชันของผลิตภัณฑ์ ESET สำหรับใช้ในบ้านที่จะดาวน์โหลด (32 บิต, 64 บิต หรือ ARM)

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
ดาวน์โหลด 64 บิต ดาวน์โหลด 32 บิต ดาวน์โหลด ARM	ดาวน์โหลด 64 บิต ดาวน์โหลด 32 บิต ดาวน์โหลด ARM	ดาวน์โหลด 64 บิต ดาวน์โหลด 32 บิต ดาวน์โหลด ARM

หากคุณมีการเชื่อมต่ออินเทอร์เน็ตที่ใช้งานอยู่ ให้ ติดตั้งผลิตภัณฑ์ ESET ของคุณโดยใช้ Live Installer

เมื่อคุณเริ่มต้นตัวติดตั้งแบบออฟไลน์ (.exe) วิซาร์ดการติดตั้งจะนำคุณเข้าสู่กระบวนการตั้งค่า



1.เลือกภาษาที่เหมาะสมจากเมนูแบบเลื่อนลงแล้วคลิก **ดำเนินการต่อ**

> หากคุณกำลังติดตั้งเวอร์ชันที่ใหม่กว่าทับเวอร์ชันก่อนหน้าที่มีการตั้งค่าที่ป้องกันด้วยรหัสผ่าน ให้ป้อนรหัสผ่านของคุณด้วย คุณสามารถกำหนดค่ารหัสผ่านการตั้งค่าได้ใน การตั้งค่าการเข้าถึง

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

- ESET LiveGrid® ระบบคำติชม
- แอพพลิเคชันที่อาจไม่พึงประสงค์
- โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า

> เมื่อคลิก **ดำเนินการต่อ** หรือ **อนุญาตทั้งหมดและดำเนินการต่อ** จะถือว่าคุณยอมรับข้อตกลงการอนุญาตใช้งานสำหรับผู้ใช้ปลายทางและรับทราบนโยบายความเป็นส่วนตัวแล้ว

3. คลิก **ข้ามการล็อคอิน** เมื่อคุณมีการเชื่อมต่ออินเทอร์เน็ต คุณสามารถ เชื่อมต่ออุปกรณ์ของคุณกับบัญชี ESET HOME ได้

4. คลิก **ข้ามการเปิดใช้งาน** โดย ESET Smart Security Premium ต้องเปิดใช้งานหลังจากการติดตั้งเพื่อให้สามารถทำงานได้อย่างสมบูรณ์ การเปิดใช้งานผลิตภัณฑ์ ต้องมีการเชื่อมต่ออินเทอร์เน็ตที่ใช้งานอยู่

5. วิซาร์ดการติดตั้งจะแสดงผลิตภัณฑ์ ESET ที่จะติดตั้งตามตัวติดตั้งแบบออฟไลน์ที่ดาวน์โหลดมา คลิก **ดำเนินการต่อ** เพื่อเริ่มกระบวนการติดตั้ง ซึ่งอาจใช้เวลาสักครู่

> i หากมีรายการที่เหลือ (ไฟล์หรือโฟลเดอร์) จากผลิตภัณฑ์ของ ESET ที่ถูกถอนการติดตั้งในอดีต ระบบจะขอให้คุณอนุญาตเพื่อลบออก คลิก **ติดตั้ง** เพื่อดำเนินการต่อ

6. คลิก**เสร็จสิ้น** เพื่อออกจากวิซาร์ดการติดตั้ง

⚠ การติดตั้งตัวแก้ไขปัญหา

การเปิดใช้งานผลิตภัณฑ์

มีวิธีเปิดใช้งานผลิตภัณฑ์ของคุณอยู่หลากหลายวิธี ตัวเลือกในการเปิดใช้งานในหน้าต่างการเปิดใช้งานอาจแตกต่างกันไปตามแต่ละประเทศ และวิธีการแจกจ่าย (ซีดี/ดีวีดี หน้าเว็บ ESET เป็นต้น):

• หากคุณซื้อผลิตภัณฑ์ที่อยู่ในกล่องจากร้านค้าปลีกหรือได้รับอีเมลที่มีรายละเอียดใบอนุญาต ให้เปิดใช้งานผลิตภัณฑ์ของคุณโดยการคลิก **ใช้รหัสใบอนุญาตที่ซื้อมา** รหัสใบอนุญาตมักจะอยู่ในด้านในหรือบนด้านหลังแพ็คเกจของผลิตภัณฑ์ ต้องป้อนรหัสใบอนุญาตตามที่ได้รับมาเพื่อให้สามารถเปิดใช้งานได้ รหัสใบอนุญาต– สายอักขระเฉพาะตัวในรูปแบบ XXXX-XXXX-XXXX-XXXX-XXXX หรือ XXXX-XXXXXXXX ซึ่งใช้เพื่อยืนยันตัวตนของเจ้าของใบอนุญาตและการเปิดใช้งานใบอนุญาตของคุณ

• หลังจากเลือก ใช้บัญชี ESET HOME ระบบจะขอข้อมูลให้คุณเข้าสู่ระบบบัญชี ESET HOME ของคุณ

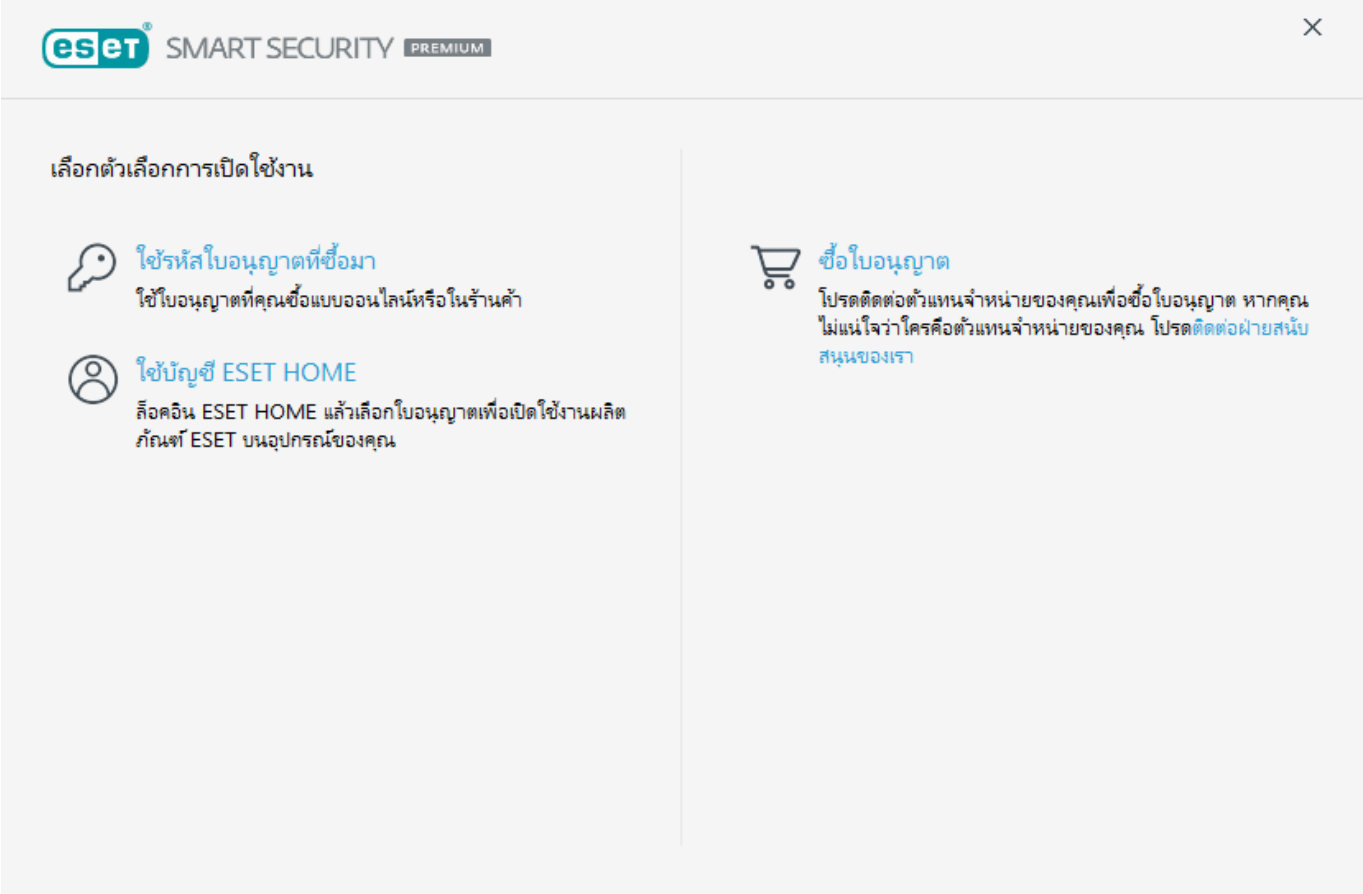
• หากคุณต้องการประเมิน ESET Smart Security Premium ก่อนตัดสินใจซื้อ ให้เลือก ทดลองใช้ฟรี ป้อนที่อยู่อีเมลและประเทศของคุณเพื่อเปิดใช้งาน ESET Smart Security Premium ในระยะเวลาที่จำกัด ใบอนุญาตรุ่นทดลองใช้ของคุณจะถูกส่งอีเมลไปถึงคุณ ใบอนุญาตรุ่นทดลองใช้จะสามารถเปิดใช้งานได้หนึ่งครั้งต่อลูกค้าหนึ่งรายเท่านั้น

• หากคุณไม่มีใบอนุญาตและต้องการซื้อ ให้คลิก**ซื้อใบอนุญาต** การดำเนินการนี้จะเปลี่ยนเส้นทางคุณไปยังเว็บไซต์ของตัวแทนจำหน่าย ESET ในพื้นที่ของคุณ ใบอนุญาตแบบเต็มของผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้านนั้น ไม่สามารถใช้งานได้ฟรี

คุณสามารถเปลี่ยนแปลงใบอนุญาตผลิตภัณฑ์เมื่อใดก็ได้ หากต้องการดำเนินการดังกล่าว ให้คลิก **วิธีใช้และการสนับสนุน** > **เปลี่ยนใบอนุญาต** ใน หน้าต่างหลักของโปรแกรม คุณจะเห็น ID ใบอนุญาตสาธารณะที่ใช้เพื่อระบุใบอนุญาตของคุณกับฝ่ายสนับสนุน ESET

หากคุณมีชื่อผู้ใช้และรหัสผ่านที่ใช้สำหรับการเปิดใช้งานของผลิตภัณฑ์ ESET ก่อนหน้านี้และไม่ทราบว่าจะเปิดใช้งานอย่างไร ESET Smart Security Premium จะแปลงข้อมูลการเข้าสู่ระบบอันเก่าของคุณให้เป็นรหัสใบอนุญาต

⚠ ไม่สามารถเปิดใช้งานผลิตภัณฑ์ได้ใช่หรือไม่



การป้อนรหัสใบอนุญาตของคุณระหว่างการเปิดใช้งาน

การอัพเดทอัตโนมัติมีความสำคัญต่อความปลอดภัยของคุณ ESET Smart Security Premium จะรับรายการอัพเดทต่างๆ หลังจากที่เปิดใช้งานแล้วเท่านั้น

เมื่อเข้าสู่ **รหัสใบอนุญาต** เป็นสิ่งสำคัญมากที่จะต้องป้อนให้ตรงตามที่ได้เขียนไว้:

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

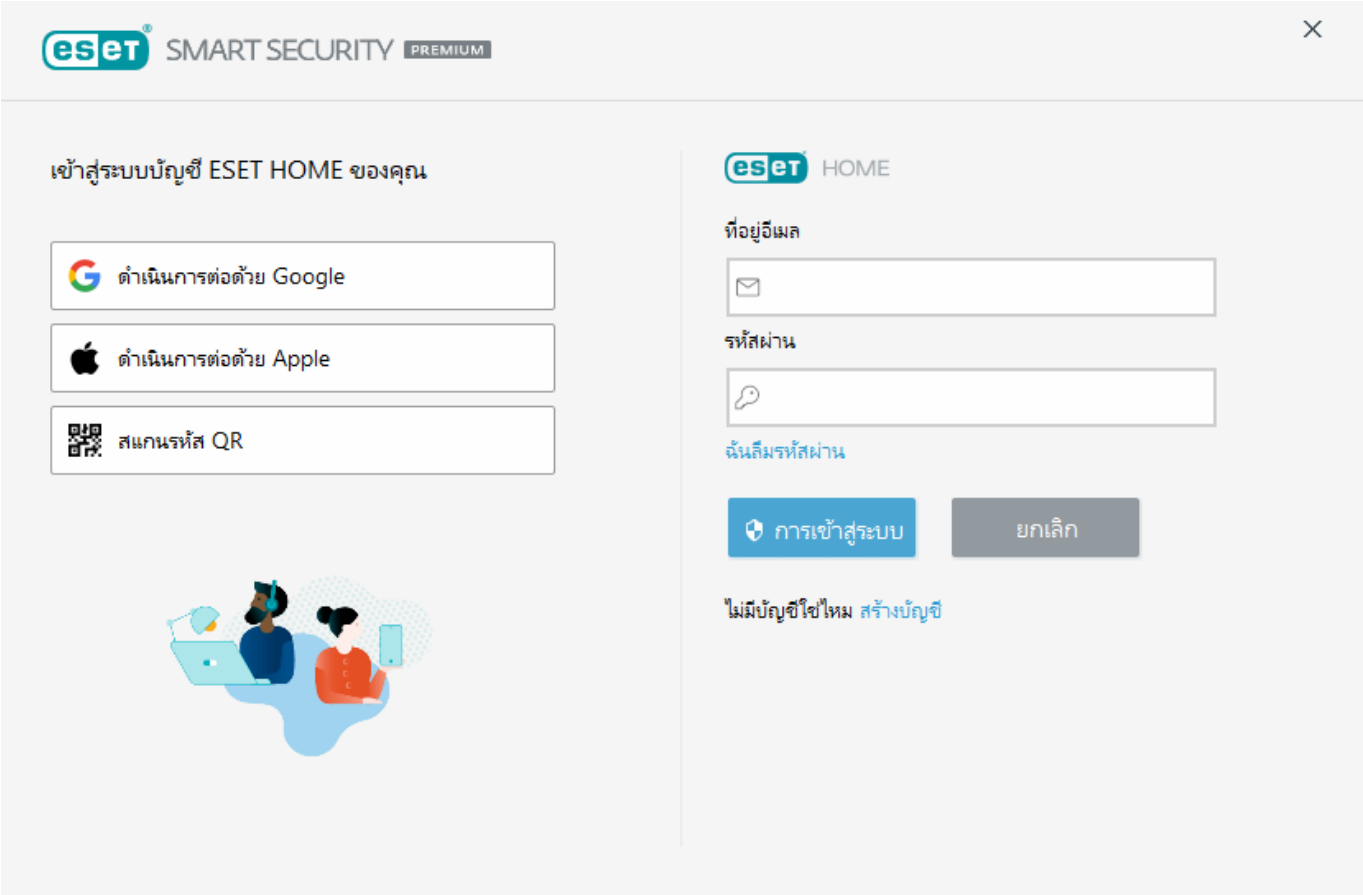
เราขอแนะนำให้คุณคัดลอกและวางรหัสใบอนุญาตของคุณจากอีเมลลงทะเบียนของคุณเพื่อให้มั่นใจว่าถูกต้อง

หากคุณไม่ป้อนรหัสใบอนุญาตหลังการติดตั้ง ผลิตภัณฑ์ของคุณจะไม่ถูกเปิดใช้งาน คุณสามารถเปิดใช้งาน ESET Smart Security Premium ใน หน้าต่างโปรแกรมหลัก > **วิธีใช้และการสนับสนุน** > **เปิดใช้งานใบอนุญาต**

ใบอนุญาตแบบเต็มของผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้านนั้น ไม่สามารถใช้งานได้ฟรี

ใช้บัญชี ESET HOME

เชื่อมต่ออุปกรณ์ของคุณกับ ESET HOME เพื่อดูและจัดการใบอนุญาตและอุปกรณ์ทั้งหมดของ ESET ที่เปิดใช้งานของคุณ คุณสามารถต่ออายุ อัพเกรด หรือขยายใบอนุญาต และดูรายละเอียดใบอนุญาตที่สำคัญได้ ในพอร์ทัลการจัดการ ESET HOME หรือแอพโทรศัพท์มือถือ คุณสามารถ แก้ไขการตั้งค่า Anti-Theft เพิ่มใบอนุญาตอื่นๆ ดาวน์โหลดผลิตภัณฑ์ไปยังอุปกรณ์ ตรวจสอบสถานะความปลอดภัยของผลิตภัณฑ์ หรือแบ่งปันใบอนุญาตผ่านอีเมลของคุณได้ สำหรับข้อมูลเพิ่มเติมให้ไปที่หน้าช่วยเหลือออนไลน์ของ ESET HOME



หลังจากเลือก **ใช้บัญชี ESET HOME** เป็นวิธีการเปิดใช้งานหรือเมื่อเชื่อมต่อกับบัญชี ESET HOME ระหว่างการติดตั้ง:

1. ล็อคอินเข้าสู่บัญชี ESET HOME ของคุณ

หากคุณไม่มีบัญชี ESET HOME ให้คลิก **สร้างบัญชี** เพื่อลงทะเบียนหรือดูคำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME
หากคุณลืมรหัสผ่าน ให้คลิก **ฉันลืมรหัสผ่าน** และทำตามขั้นตอนบนหน้าจอหรือดู คำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME

2. ตั้ง **ชื่ออุปกรณ์** สำหรับอุปกรณ์ของคุณที่จะใช้ในบริการ ESET HOME ทั้งหมดแล้วคลิก **ดำเนินการต่อ**

3. เลือกใบอนุญาตสำหรับการเปิดใช้งานหรือ เพิ่มใบอนุญาตใหม่ คลิก **ดำเนินการต่อ** เพื่อเปิดใช้งาน ESET Smart Security Premium

เปิดใช้งานใบอนุญาตรุ่นทดลองใช้

หากต้องการเปิดใช้งาน ESET Smart Security Premium เวอร์ชันทดลอง ให้ป้อนที่อยู่อีเมลที่ถูกต้องในช่อง **ที่อยู่อีเมล** และช่อง **ยืนยันที่อยู่อีเมล** หลังจากเปิดใช้งานแล้ว ระบบจะสร้างใบอนุญาตของ ESET และส่งให้คุณทางอีเมล ที่อยู่อีเมลนี้ยังจะใช้สำหรับการแจ้งเตือนเกี่ยวกับการหมดอายุของผลิตภัณฑ์และการสื่อสารอื่นๆ กับ ESET อีกด้วย เวอร์ชั่นทดลองสามารถเปิดใช้งานได้เพียงครั้งเดียวเท่านั้น

เลือกประเทศของคุณจากเมนูแบบเลื่อนลง **ประเทศ** เพื่อลงทะเบียน ESET Smart Security Premium กับตัวแทนจำหน่ายในท้องถิ่นของคุณซึ่งจะให้การสนับสนุนด้านเทคนิค

รหัสใบอนุญาตฟรีของ ESET

ใบอนุญาตเต็มรูปแบบสำหรับ ESET Smart Security Premium นั้นไม่ฟรี

รหัสใบอนุญาตของ ESET คือชุดของอักขระและหมายเลขที่แยกด้วยเครื่องหมายขีดยาว ซึ่งจัดหาให้โดย ESET เพื่ออนุญาตให้ใช้งาน ESET Smart Security Premium ได้อย่างถูกกฎหมายตามที่ระบุไว้ใน ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง ผู้ใช้ปลายทางทุกรายมีสิทธิ์ในการใช้รหัสใบอนุญาตได้เฉพาะในขอบเขตเท่าที่มีสิทธิ์ใช้งาน ESET Smart Security Premium ซึ่งอิงจากจำนวนใบอนุญาตที่ ESET มอบให้ รหัสใบอนุญาตถือว่าเป็นความลับและไม่สามารถแบ่งปันได้ อย่างไรก็ตาม คุณสามารถ แชร์ที่นั่งของใบอนุญาตโดยใช้ ESET HOME ได้

อาจมีแหล่งข้อมูลทางอินเทอร์เน็ตที่ให้รหัสใบอนุญาตของ ESET ในรูปแบบ "ฟรี" แต่โปรดจำไว้ว่า:

- การคลิกที่โฆษณา "ใบอนุญาตฟรีของ ESET" อาจทำให้คอมพิวเตอร์หรืออุปกรณ์ของคุณติดไวรัสมัลแวร์ได้ มัลแวร์สามารถซ่อนตัวอยู่ในคอนเทนต์โซเชียลมีเดียที่ไม่เป็นทางการ (เช่น วิดีโอ) เว็บไซต์ที่แสดงโฆษณาเพื่อรับเงินตามการเยี่ยมชมของคุณ และอื่นๆ โดยปกติแล้วเว็บไซต์เหล่านี้จะเป็นกับดัก

• ESET สามารถปิดใช้งานใบอนุญาตที่ละเมิดลิขสิทธิ์ได้

• การใช้รหัสใบอนุญาตที่ละเมิดลิขสิทธิ์นั้นไม่สอดคล้องกับ ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง ที่คุณต้องยอมรับเพื่อติดตั้ง ESET Smart Security Premium

• ซื้อใบอนุญาต ESET ผ่านช่องทางอย่างเป็นทางการเท่านั้น เช่น www.eset.com ตัวแทนจำหน่ายหรือผู้ค้าปลีกของ ESET (อย่าซื้อใบอนุญาตจากเว็บไซต์ของบุคคลภายนอกที่ไม่เป็นทางการเช่น eBay หรือใบอนุญาตที่ใช้งานร่วมกันของบุคคลภายนอก)

• การดาวน์โหลด ESET Smart Security Premium นั้นฟรี แต่การเปิดใช้งานระหว่างการติดตั้งจำเป็นต้องใช้รหัสใบอนุญาตของ ESET ที่ถูกต้อง (คุณสามารถดาวน์โหลดและติดตั้งได้ตามปกติ แต่ถ้าไม่มีการเปิดใช้งานผลิตภัณฑ์จะไม่ทำงาน)

• อย่าแบ่งปันใบอนุญาตของคุณในอินเทอร์เน็ตหรือสื่อสังคมออนไลน์ (เพราะอาจทำให้ใบอนุญาตแพร่กระจายไปถึงมือผู้อื่นได้)

หากต้องการระบุหรือรายงานใบอนุญาตของ ESET ที่ละเมิดลิขสิทธิ์ โปรดไปที่บทความฐานความรู้ สำหรับคำแนะนำ

หากคุณมีความไม่แน่ใจเกี่ยวกับการซื้อผลิตภัณฑ์ด้านการรักษาความปลอดภัยของ ESET คุณสามารถใช้เวอร์ชั่นทดลองใช้ระหว่างตัดสินใจได้:

1. เปิดใช้งาน ESET Smart Security Premium โดยใช้ใบอนุญาตเวอร์ชันทดลองใช้ฟรี

2. เข้าร่วมในโปรแกรมเบต้าของ ESET

3. ติดตั้ง ESET Mobile Security หากคุณใช้อุปกรณ์โทรศัพท์มือถือ Android โดยสามารถใช้งานในรูปแบบพรีเมียมได้ฟรี

หากต้องการรับส่วนลด / ยืดอายุใบอนุญาตของคุณ:

- แนะนำ ESET Smart Security Premium ให้เพื่อนของคุณ
- ต่ออายุ ESET ของคุณ (หากคุณเคยเปิดใช้งานใบอนุญาตมาก่อน) หรือเปิดใช้งานเป็นระยะเวลานานขึ้น

การเปิดใช้งานล้มเหลว-สถานการณ์ทั่วไป

หากการเปิดใช้งาน ESET Smart Security Premium ไม่ประสบความสำเร็จ สถานการณ์ที่พบมากที่สุดคือ:

- รหัสใบอนุญาตมีการใช้งานอยู่แล้ว
- รหัสใบอนุญาตไม่ถูกต้อง เกิดข้อผิดพลาดกับฟอร์มการเปิดใช้งานผลิตภัณฑ์
- ไม่มีข้อมูลเสริมสำหรับการเปิดใช้งาน หรือข้อมูลไม่ถูกต้อง
- การสื่อสารกับฐานข้อมูลการเปิดใช้งานล้มเหลว โปรดลองเปิดใช้งานอีกครั้งภายในอีก 15 นาที
- ไม่มีหรือปิดใช้งานการเชื่อมต่อไปยังเซิร์ฟเวอร์การเปิดใช้งาน ESET

ตรวจสอบว่าคุณได้ป้อนรหัสใบอนุญาตที่ถูกต้องแล้วและลองเปิดใช้งานอีกครั้ง หากคุณใช้บัญชี ESET HOME สำหรับการเปิดใช้งาน โปรดดู การจัดการใบอนุญาต ESET HOME - วิธีใช้ออนไลน์

หากคุณยังคงไม่สามารถเปิดใช้งานได้ ตัวแก้ไขปัญหาการเปิดใช้งานของ ESET จะนำคุณไปรู้จักกับคำถามทั่วไป ข้อผิดพลาด ปัญหาที่เกี่ยวกับการเปิดใช้งานและการอนุญาต (พร้อมให้ใช้งานในรูปแบบภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษา)

การเปิดใช้งานล้มเหลวเนื่องจากมีการใช้ใบอนุญาตเกินจำนวน

ปัญหา

- ใบอนุญาตของคุณอาจถูกใช้เกินจำนวนหรือถูกใช้ในทางที่ผิด
- การเปิดใช้งานล้มเหลวเนื่องจากมีการใช้ใบอนุญาตเกินจำนวน

โซลูชัน

มีอุปกรณ์ที่ใช้ใบอนุญาตนี้เกินกว่าจำนวนที่อนุญาต คุณอาจตกเป็นเหยื่อของการปลอมแปลงหรือการละเมิดสิทธิ์ซอฟต์แวร์ ใบอนุญาตจะไม่สามารถใช้เพื่อเปิดใช้งานผลิตภัณฑ์อื่นๆ ของ ESET ได้ คุณสามารถแก้ปัญหานี้ได้โดยตรง

หากคุณได้รับอนุญาตให้จัดการใบอนุญาตในบัญชี ESET HOME ของคุณหรือซื้อใบอนุญาตจากแหล่งที่ถูกต้องตามกฎหมาย ถ้าคุณยังไม่มีบัญชี ให้สร้างบัญชี

หากคุณเป็นเจ้าของใบอนุญาตและคุณไม่ได้รับแจ้งให้ป้อนที่อยู่อีเมลของคุณ:

1. ในการจัดการใบอนุญาต ESET ของคุณ ให้เปิดเว็บเบราว์เซอร์และไปยัง https://home.eset.com เข้าถึง ESET License Manager แล้วลบหรือปิดใช้งานที่นั่ง สำหรับข้อมูลเพิ่มเติม โปรดดู สิ่งที่ควรทำในกรณีที่มีการใช้ใบอนุญาตเกินจำนวน

2. หากต้องการระบุหรือรายงานใบอนุญาตของ ESET ที่ละเมิดลิขสิทธิ์ โปรดไปที่บทความระบุและรายงานใบอนุญาต ESET ที่ละเมิดสิทธิ์ สำหรับคำแนะนำ

3. หากคุณไม่มั่นใจ คลิกย้อน **กลับ** และ ส่งอีเมลหาการสนับสนุนด้านเทคนิคของ ESET

หากคุณไม่ใช่เจ้าของใบอนุญาต ให้ติดต่อเจ้าของใบอนุญาตนี้เพื่อแจ้งข้อมูลว่าคุณไม่สามารถเปิดใช้งานผลิตภัณฑ์ ESET ได้เนื่องจากมีการใช้ใบอนุญาตเกินจำนวน เจ้าของใบอนุญาตสามารถแก้ไขปัญหาได้ในพอร์ทัล ESET HOME

หากได้รับแจ้งให้ยืนยันที่อยู่อีเมลของคุณ (ในบางกรณีเท่านั้น) ให้ป้อนที่อยู่อีเมลที่ใช้ซื้อหรือเปิดใช้งาน ESET Smart Security Premium ของคุณ

การอัพเกรดใบอนุญาต

หน้าต่างการแจ้งเตือนนี้จะปรากฏขึ้นเมื่อใบอนุญาตที่ใช้เปิดใช้งานผลิตภัณฑ์ ESET ของคุณมีการเปลี่ยนแปลง ใบอนุญาตที่มีการเปลี่ยนแปลงของคุณทำให้สามารถเปิดใช้งานผลิตภัณฑ์ที่มีคุณสมบัติความปลอดภัยมากขึ้นได้ หากไม่มีการดำเนินการใดๆ ESET Smart Security Premium จะแสดงหน้าต่างการแจ้งเตือนหนึ่งครั้ง ซึ่งเรียกว่า **เปลี่ยนไปใช้ผลิตภัณฑ์ที่มีคุณสมบัติมากกว่า**

ใช่ (แนะนำ) – จะติดตั้งผลิตภัณฑ์ที่มีคุณสมบัติความปลอดภัยมากกว่าให้โดยอัตโนมัติ

ไม่ ขอบคุณ –จะไม่ทำการเปลี่ยนแปลงใดๆ และการแจ้งเตือนจะหายไปอย่างถาวร

หากต้องการเปลี่ยนผลิตภัณฑ์ภายหลัง โปรดดูบทความฐานความรู้ ESET ของเรา สำหรับข้อมูลเพิ่มเติมเกี่ยวกับใบอนุญาต ESET โปรดดูที่ คำถามที่พบบ่อยเกี่ยวกับการอนุญาต

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
กลไกการตรวจจับ	✔	✔	✔
การเรียนรู้ของเครื่องขั้นสูง	✔	✔	✔
การป้องกันการโจมตีแบบ Exploit	✔	✔	✔
การป้องกันการโจมตีที่ใช้สคริปต์	✔	✔	✔
การป้องกันฟิชชิ่ง	✔	✔	✔
การป้องกันการเข้าถึงเว็บ	✔	✔	✔
HIPS (รวมถึง การป้องกันแรนซั่มแวร์)	✔	✔	✔
การป้องกันสแปม		✔	✔
ไฟร์วอลล์		✔	✔
ตัวตรวจสอบเครือข่าย		✔	✔
การป้องกัน Webcam		✔	✔
การป้องกันการโจมตีเครือข่าย		✔	✔
การป้องกันบอตเน็ต		✔	✔
การป้องกันการธนาคารและการชำระเงิน		✔	✔
การควบคุมเนื้อหา		✔	✔
การป้องกันการโจรกรรม		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

การอัพเกรดผลิตภัณฑ์

คุณได้ดาวน์โหลดโปรแกรมติดตั้งตามค่าเริ่มต้นและตัดสินใจเปลี่ยนแปลงผลิตภัณฑ์ที่จะเปิดใช้งาน หรือคุณต้องการเปลี่ยนผลิตภัณฑ์ที่ติดตั้งเป็นผลิตภัณฑ์ที่มีคุณสมบัติความปลอดภัยมากกว่า

เปลี่ยนแปลงผลิตภัณฑ์ในระหว่างการติดตั้ง

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
กลไกการตรวจจับ	✔	✔	✔
การเรียนรู้ของเครื่องขั้นสูง	✔	✔	✔
การป้องกันการโจมตีแบบ Exploit	✔	✔	✔
การป้องกันการโจมตีที่ใช้สคริปต์	✔	✔	✔
การป้องกันฟิชชิ่ง	✔	✔	✔
การป้องกันการเข้าถึงเว็บ	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
HIPS (รวมถึง การป้องกันแรนซั่มแวร์)	✔	✔	✔
การป้องกันสแปม		✔	✔
ไฟร์วอลล์		✔	✔
ตัวตรวจสอบเครือข่าย		✔	✔
การป้องกัน Webcam		✔	✔
การป้องกันการโจมตีเครือข่าย		✔	✔
การป้องกันบอตเน็ต		✔	✔
การป้องกันการธนาคารและการชำระเงิน		✔	✔
การควบคุมเนื้อหา		✔	✔
การป้องกันการโจรกรรม		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

การดาวน์เกรดใบอนุญาต

หน้าต่างโต้ตอบนี้จะปรากฏขึ้นเมื่อใบอนุญาตที่ใช้เปิดใช้งานผลิตภัณฑ์ ESET ของคุณมีการเปลี่ยนแปลง ใบอนุญาตที่มีการเปลี่ยนแปลงของคุณสามารถใช้ได้กับผลิตภัณฑ์ ESET รุ่นอื่นที่มีคุณสมบัติความปลอดภัยน้อยกว่าเท่านั้น ผลิตภัณฑ์นี้จะได้รับการเปลี่ยนโดยอัตโนมัติเพื่อไม่ให้คุณสูญเสียการป้องกัน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับใบอนุญาต ESET โปรดดูที่ คำถามที่พบบ่อยเกี่ยวกับการอนุญาต

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
กลไกการตรวจจับ	✔	✔	✔
การเรียนรู้ของเครื่องขั้นสูง	✔	✔	✔
การป้องกันการโจมตีแบบ Exploit	✔	✔	✔
การป้องกันการโจมตีที่ใช้สคริปต์	✔	✔	✔
การป้องกันฟิชชิ่ง	✔	✔	✔
การป้องกันการเข้าถึงเว็บ	✔	✔	✔
HIPS (รวมถึง การป้องกันแรนซั่มแวร์)	✔	✔	✔
การป้องกันสแปม		✔	✔
ไฟร์วอลล์		✔	✔
ตัวตรวจสอบเครือข่าย		✔	✔
การป้องกัน Webcam		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
การป้องกันการโจมตีเครือข่าย		✔	✔
การป้องกันบอตเน็ต		✔	✔
การป้องกันการธนาคารและการชำระเงิน		✔	✔
การควบคุมเนื้อหา		✔	✔
การป้องกันการโจรกรรม		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

การดาวน์เกรดผลิตภัณฑ์

ผลิตภัณฑ์ที่คุณได้ติดตั้งในตอนนี้มีคุณสมบัติความปลอดภัยมากกว่าผลิตภัณฑ์ที่คุณกำลังจะเปิดใช้งาน Secure Data และ Password Manager ไม่ใช่ส่วนหนึ่งของผลิตภัณฑ์นี้ คุณจะไม่สามารถสร้างไฟล์ที่เข้ารหัสได้

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
กลไกการตรวจจับ	✔	✔	✔
การเรียนรู้ของเครื่องขั้นสูง	✔	✔	✔
การป้องกันการโจมตีแบบ Exploit	✔	✔	✔
การป้องกันการโจมตีที่ใช้สคริปต์	✔	✔	✔
การป้องกันฟิชชิ่ง	✔	✔	✔
การป้องกันการเข้าถึงเว็บ	✔	✔	✔
HIPS (รวมถึง การป้องกันแรนซั่มแวร์)	✔	✔	✔
การป้องกันสแปม		✔	✔
ไฟร์วอลล์		✔	✔
ตัวตรวจสอบเครือข่าย		✔	✔
การป้องกัน Webcam		✔	✔
การป้องกันการโจมตีเครือข่าย		✔	✔
การป้องกันบอตเน็ต		✔	✔
การป้องกันการธนาคารและการชำระเงิน		✔	✔
การควบคุมเนื้อหา		✔	✔
การป้องกันการโจรกรรม		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

การติดตั้งตัวแก้ไขปัญหา

หากพบปัญหาในระหว่างการติดตั้ง วิซาร์ดการติดตั้งจะให้ตัวแก้ไขปัญหาที่จะช่วยแก้ปัญหาหากเป็นไปได้

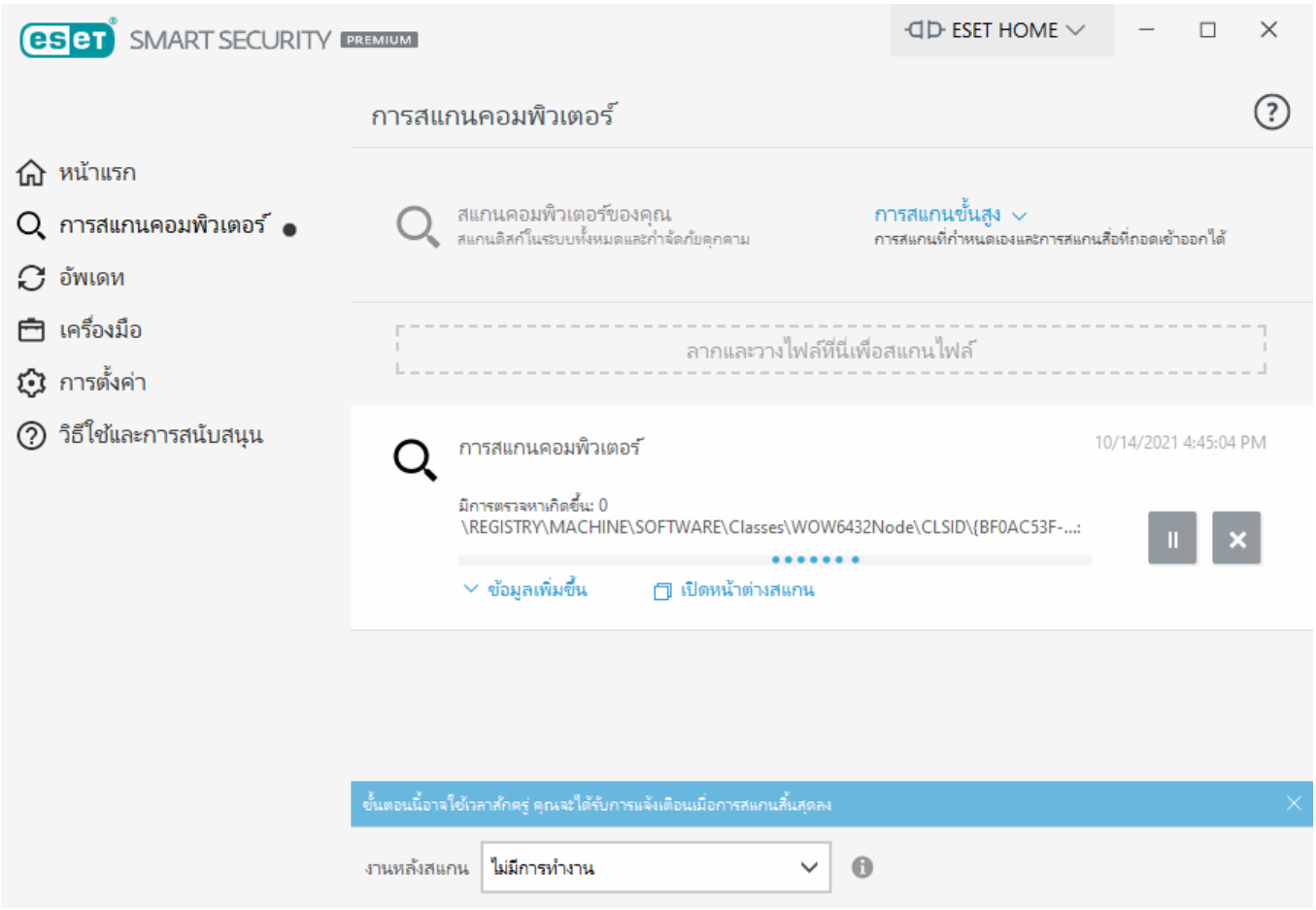
คลิก **เรียกใช้ตัวแก้ไขปัญหา** เพื่อให้ตัวแก้ไขปัญหาเริ่มทำงาน เมื่อดำเนินการเสร็จสิ้น โปรดดำเนินการตามโซลูชันที่แนะนำ

หากปัญหายังคงอยู่ โปรดดูรายการ ข้อผิดพลาดทั่วไปของการติดตั้งและวิธีแก้ไข

สแกนครั้งแรกหลังจากการติดตั้ง

หลังจากที่ติดตั้ง ESET Smart Security Premium การสแกนคอมพิวเตอร์จะเริ่มโดยอัตโนมัติหลังจากที่อัปเดตสำเร็จ เพื่อตรวจสอบรหัสที่เป็นอันตราย

คุณยังสามารถเริ่มการสแกนคอมพิวเตอร์ด้วยตัวเองได้จาก หน้าต่างโปรแกรมหลัก โดยการคลิกที่ **การสแกนคอมพิวเตอร์** > **สแกนคอมพิวเตอร์ของคุณ** สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการสแกนคอมพิวเตอร์ ให้ดูที่ส่วน การสแกนคอมพิวเตอร์



การอัพเกรดเป็นเวอร์ชันล่าสุด

ESET Smart Security Premium เวอร์ชันใหม่ได้ออกมาเพื่อปรับปรุงประสิทธิภาพหรือแก้ไขปัญหาที่ไม่สามารถแก้ไขได้โดยการอัพเดทอัตโนมัติของโมดูลโปรแกรม การอัพเกรดเป็นเวอร์ชันใหม่กว่าสามารถทำได้หลายวิธี:

1. อัตโนมัติ โดยใช้การอัพเดทโปรแกรม
เนื่องจากมีการแจกจ่ายการอัพเกรดโปรแกรมให้กับผู้ใช้ทั้งหมดและอาจมีผลกับการกำหนดค่าบางอย่างในระบบ การอัพเกรดนี้จึงออกมาหลังจากผ่านการทดสอบเป็นระยะเวลานานเพื่อให้มั่นใจว่าสามารถทำงานกับการกำหนดค่าระบบทั้งหมดได้ หากคุณต้องการอัพเกรดเป็นเวอร์ชันใหม่ทันทีเมื่อมีการออก ให้ใช้วิธีหนึ่งจากด้านล่างนี้ ตรวจสอบให้แน่ใจว่าคุณได้เปิดใช้งาน **การอัพเดทคุณลักษณะของแอพพลิเคชัน** ใน **การตั้งค่าขั้นสูง** (F5) > **อัพเดท** > **โปรไฟล์** > **การอัพเดท** แล้ว

2. ด้วยตนเอง ใน หน้าต่างโปรแกรมหลัก โดยคลิก **ตรวจสอบการอัพเดท** ในส่วน **อัพเดท**

3. ด้วยตนเอง โดยการดาวน์โหลดและ เวอร์ชันใหม่กว่าทับเวอร์ชันที่มีอยู่ก่อนหน้า

สำหรับข้อมูลเพิ่มเติมและคำแนะนำพร้อมภาพประกอบสามารถดูได้ที่:

- อัพเดทผลิตภัณฑ์ของ ESET—ตรวจสอบโมดูลผลิตภัณฑ์ล่าสุด
- อะไรคือความแตกต่างระหว่างผลิตภัณฑ์ของ ESET ประเภทอัพเดทและประเภทที่เผยแพร่ให้ใช้งาน

การอัพเกรดอัตโนมัติสำหรับผลิตภัณฑ์ดั้งเดิม

เวอร์ชันผลิตภัณฑ์ ESET ของคุณไม่รองรับอีกต่อไป และผลิตภัณฑ์ของคุณได้รับการอัพเกรดให้เป็นเวอร์ชันล่าสุด

⚠ ปัญหาการติดตั้งทั่วไป

ℹ ผลิตภัณฑ์ ESET เวอร์ชันใหม่ในแต่ละเวอร์ชันจะมีการแก้ไขบั๊กและปรับปรุงหลายประการ ลูกค้าเดิมที่มีใบอนุญาตที่ถูกต้องของผลิตภัณฑ์ ESET จะสามารถอัพเกรดผลิตภัณฑ์เดิมให้เป็นเวอร์ชันล่าสุดได้ฟรี

หากต้องการทำการติดตั้งให้เสร็จสิ้น:

1. ให้คลิก **ยอมรับและดำเนินการต่อ** เพื่อยอมรับ ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง และยอมรับนโยบายความเป็นส่วนตัว หากคุณไม่ยอมรับข้อตกลงผู้ใช้ปลายทาง ให้คลิก **ถอนการติดตั้ง** โดยคุณจะไม่

สามารถคืนค่าเป็นเวอร์ชันก่อนหน้าได้อีกต่อไป

2. คลิก **อนุญาตทั้งหมดและดำเนินการต่อ** เพื่ออนุญาตทั้ง ระบบสะท้อนกลับ ESET LiveGrid® และ โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า หรือคลิก **ดำเนินการต่อ** หากคุณไม่ต้องการมีส่วนร่วม

3. หลังเปิดใช้งานผลิตภัณฑ์ ESET ใหม่ด้วยรหัสใบอนุญาตของคุณ หน้าแรกจะปรากฏขึ้น หากไม่พบข้อมูลใบอนุญาต ให้ดำเนินการต่อไปด้วยใบอนุญาตทดลองใหม่ หากใบอนุญาตของคุณที่ใช้กับผลิตภัณฑ์ก่อนหน้านี้ไม่ถูกต้อง ให้ เปิดใช้งานผลิตภัณฑ์ ESET ของคุณ

4. ต้องรีสตาร์ทอุปกรณ์เพื่อดำเนินการติดตั้งให้เสร็จสมบูรณ์

การแนะนำผลิตภัณฑ์ ESET ให้เพื่อน

ตอนนี้ ESET Smart Security Premium ในเวอร์ชันนี้จะมีข้อเสนอโบนัสสำหรับการแนะนำ คุณจึงสามารถแบ่งปันประสบการณ์ผลิตภัณฑ์ ESET กับเพื่อนหรือครอบครัวของคุณได้ คุณยังสามารถแบ่งปันแม้กระทั่งผลิตภัณฑ์ที่เปิดใช้งานแล้วได้ด้วยใบอนุญาตรุ่นทดลองใช้ เมื่อคุณใช้งานในฐานะผู้ใช้งานแบบทดลองใช้ ทุกครั้งที่คุณแนะนำสำเร็จและส่งผลลัพธ์ในการเปิดใช้งานผลิตภัณฑ์ ทั้งคุณและเพื่อนของคุณจะได้รับการขยายเวลาพิเศษสำหรับใบอนุญาตรุ่นทดลองใช้

คุณสามารถทำการแนะนำโดยใช้ ESET Smart Security Premium ที่ติดตั้งได้ ผลิตภัณฑ์ที่คุณสามารถแนะนำได้จะขึ้นอยู่กับผลิตภัณฑ์ที่คุณใช้แนะนำ ดูตารางต่อไปนี้

ผลิตภัณฑ์ที่ติดตั้งของคุณ	ผลิตภัณฑ์ที่คุณแนะนำได้
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

ผลิตภัณฑ์ที่แนะนำ

หากต้องการส่งลิงก์แนะนำ **แนะนำเพื่อน** ในเมนูหลักของ ESET Smart Security Premium ให้คลิก **แบ่งปันลิงก์ที่อ้างอิง** ผลิตภัณฑ์ของคุณจะสร้างลิงก์ที่แนะนำที่จะแสดงในหน้าต่างใหม่ คัดลอกลิงค์นี้แล้วส่งไปให้ครอบครัวและเพื่อนๆ ของคุณ คัดลอกลิงก์แล้วส่งไปให้ครอบครัวและเพื่อนๆ ของคุณ คุณสามารถแบ่งปันลิงก์ที่แนะนำได้โดยตรงจากผลิตภัณฑ์ ESET โดยใช้ตัวเลือกต่างๆ ดังนี้ **แบ่งปันบน Facebook แนะนำรายชื่อติดต่อ Gmail** และ **แบ่งปันบน Twitter**

เมื่อเพื่อนของคุณคลิกลิงก์แนะนำที่คุณส่ง ระบบจะเปลี่ยนเส้นทางไปยังหน้าเว็บที่เพื่อนของคุณสามารถดาวน์โหลดผลิตภัณฑ์และสามารถใช้งานการป้องกันแบบฟรีได้เพิ่มอีกหนึ่งเดือน ในฐานะผู้ใช้งานแบบทดลองใช้ คุณจะได้รับการแจ้งเตือนสำหรับทุกๆ ลิงก์แนะนำที่เปิดใช้งานสำเร็จ และใบอนุญาตของคุณจะยืดอายุการปกป้องแบบฟรีเพิ่มอีกหนึ่งเดือนโดยอัตโนมัติ ซึ่งวิธีนี้ทำให้คุณสามารถยืดอายุการปกป้องแบบฟรีได้สูงสุดถึง 5 เดือน คุณสามารถตรวจสอบจำนวนลิงก์แนะนำที่เปิดใช้งานสำเร็จได้ในหน้าต่าง **แนะนำเพื่อน** ในผลิตภัณฑ์ ESET ของคุณ

คุณลักษณะการอ้างอิงอาจไม่พร้อมใช้งานสำหรับภาษา/ภูมิภาคของคุณ

ESET Smart Security Premium จะถูกติดตั้ง

หน้าต่างข้อความนี้สามารถแสดงได้:

- ระหว่างขั้นตอนการติดตั้ง – คลิก **ดำเนินการต่อ** เพื่อติดตั้ง ESET Smart Security Premium
- เมื่อเปลี่ยนใบอนุญาตใน ESET Smart Security Premium – คลิก **เปิดใช้งาน** เพื่อเปลี่ยนใบอนุญาตและเปิดใช้งาน ESET Smart Security Premium

ตัวเลือก **เปลี่ยนผลิตภัณฑ์** ช่วยให้คุณสามารถสลับระหว่างผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้านตามใบอนุญาต ESET ของคุณ ดูข้อมูลเพิ่มเติมได้ที่ ฉันมีผลิตภัณฑ์ใดบ้าง

เปลี่ยนเป็นสายผลิตภัณฑ์ที่ต่างออกไป

ตามใบอนุญาต ESET ของคุณ คุณสามารถสลับไปมาระหว่างหลายๆ ผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้านได้ ดูข้อมูลเพิ่มเติมได้ที่ ฉันมีผลิตภัณฑ์ใดบ้าง

การลงทะเบียน

โปรดลงทะเบียนใบอนุญาตของคุณโดยกรอกช่องในแบบฟอร์มการลงทะเบียนให้เสร็จสมบูรณ์แล้วคลิก เปิดใช้งาน โดยต้องกรอกช่องที่ทำเครื่องหมายว่าจำเป็นในวงเล็บ ข้อมูลนี้จะถูกใช้สำหรับกรณีที่เกี่ยวข้องกับใบอนุญาต ESET ของคุณเท่านั้น

ความคืบหน้าของการเปิดใช้งาน

โปรดรอสักสองสามวินาทีเพื่อให้กระบวนการเปิดใช้งานเสร็จสมบูรณ์ (เวลาที่ต้องรออาจแตกต่างกันไปตามความเร็วของการเชื่อมต่ออินเทอร์เน็ตหรือคอมพิวเตอร์)

เปิดใช้งานสำเร็จแล้ว

กระบวนการเปิดใช้งานเสร็จสมบูรณ์ ปฏิบัติตามวิซาร์ดที่เลือกหลังการติดตั้งโปรแกรมเพื่อตั้งค่า ESET Smart Security Premium ให้เสร็จสิ้น

การอัพเดตโมดูลจะเริ่มขึ้นในอีกไม่กี่วินาที การอัพเดทปกติของ ESET Smart Security Premium จะเริ่มต้นทันที

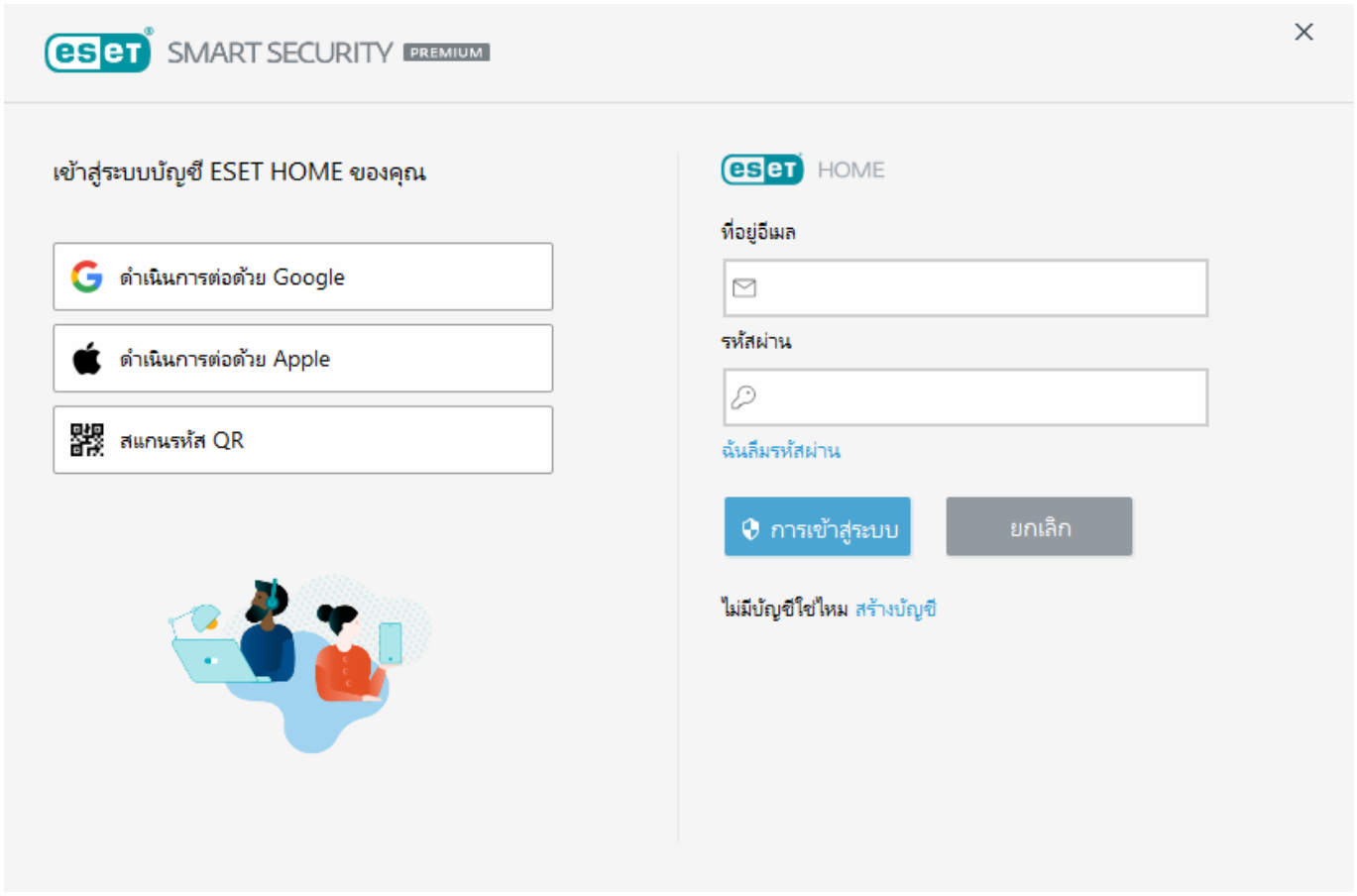
การสแกนครั้งแรกจะเริ่มโดยอัตโนมัติภายใน 20 นาทีหลังจากการอัพเดทโมดูลนี้

คู่มือสำหรับผู้เริ่มต้น

บทนี้จะให้ภาพรวมเริ่มต้นของ ESET Smart Security Premium และการตั้งค่าพื้นฐานของโปรแกรม

เชื่อมต่อกับ ESET HOME

เชื่อมต่ออุปกรณ์ของคุณกับ ESET HOME เพื่อดูและจัดการใบอนุญาตและอุปกรณ์ทั้งหมดของ ESET ที่เปิดใช้งานของคุณ คุณสามารถต่ออายุ อัพเกรด หรือขยายใบอนุญาต และดูรายละเอียดใบอนุญาตที่สำคัญได้ ในพอร์ทัลการจัดการ ESET HOME หรือแอพโทรศัพท์มือถือ คุณสามารถ แก้ไขการตั้งค่า Anti-Theft เพิ่มใบอนุญาตอื่นๆ ดาวน์โหลดผลิตภัณฑ์ไปยังอุปกรณ์ ตรวจสอบสถานะความปลอดภัยของผลิตภัณฑ์ หรือแบ่งปันใบอนุญาตผ่านอีเมลของคุณได้ สำหรับข้อมูลเพิ่มเติมให้ไปที่หน้าช่วยเหลือออนไลน์ของ ESET HOME



หากต้องการเชื่อมต่ออุปกรณ์ของคุณกับ ESET HOME:

หากคุณกำลังเชื่อมต่อกับ ESET HOME ในระหว่างการติดตั้งหรือเมื่อเลือก **ใช้บัญชี ESET HOME** เป็นวิธีการเปิดใช้งาน ให้ทำตามคำแนะนำในหัวข้อ ใช้บัญชี ESET HOME
หากคุณได้ติดตั้ง ESET Smart Security Premium ไว้และได้เปิดใช้งานด้วยใบอนุญาตที่เพิ่มเข้าในบัญชี ESET HOME ของคุณแล้ว คุณจะสามารถเชื่อมต่ออุปกรณ์ของคุณเข้ากับ ESET HOME ได้โดยใช้พอร์ทัล ESET HOME โปรดดำเนินการตามคำแนะนำใน คู่มือความช่วยเหลือออนไลน์สำหรับ ESET HOME และ อนุญาตการเชื่อมต่อใน ESET Smart Security Premium

1.ใน หน้าต่างโปรแกรมหลัก ให้คลิก **ESET HOME** > **เชื่อมต่อกับ ESET HOME** หรือคลิก **เชื่อมต่อกับ ESET HOME** ใน **เชื่อมต่ออุปกรณ์นี้กับการแจ้งเตือนบัญชี ESET HOME**

2.ล็อคอินเข้าสู่บัญชี ESET HOME ของคุณ

หากคุณไม่มีบัญชี ESET HOME ให้คลิก **สร้างบัญชี** เพื่อลงทะเบียนหรือดูคำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME
หากคุณลืมรหัสผ่าน ให้คลิก **ฉันลืมรหัสผ่าน** และทำตามขั้นตอนบนหน้าจอหรือดู คำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME

3.ตั้ง **ชื่ออุปกรณ์** และคลิก **ดำเนินการต่อ**

4.หลังจากการเชื่อมต่อสำเร็จหน้าต่างรายละเอียดจะปรากฏขึ้น ให้คลิก **เสร็จสิ้น**

ล็อคอินเข้าสู่ ESET HOME

คุณสามารถล็อคอินเข้าสู่บัญชี ESET HOME ของคุณ ได้หลายวิธีดังนี้:

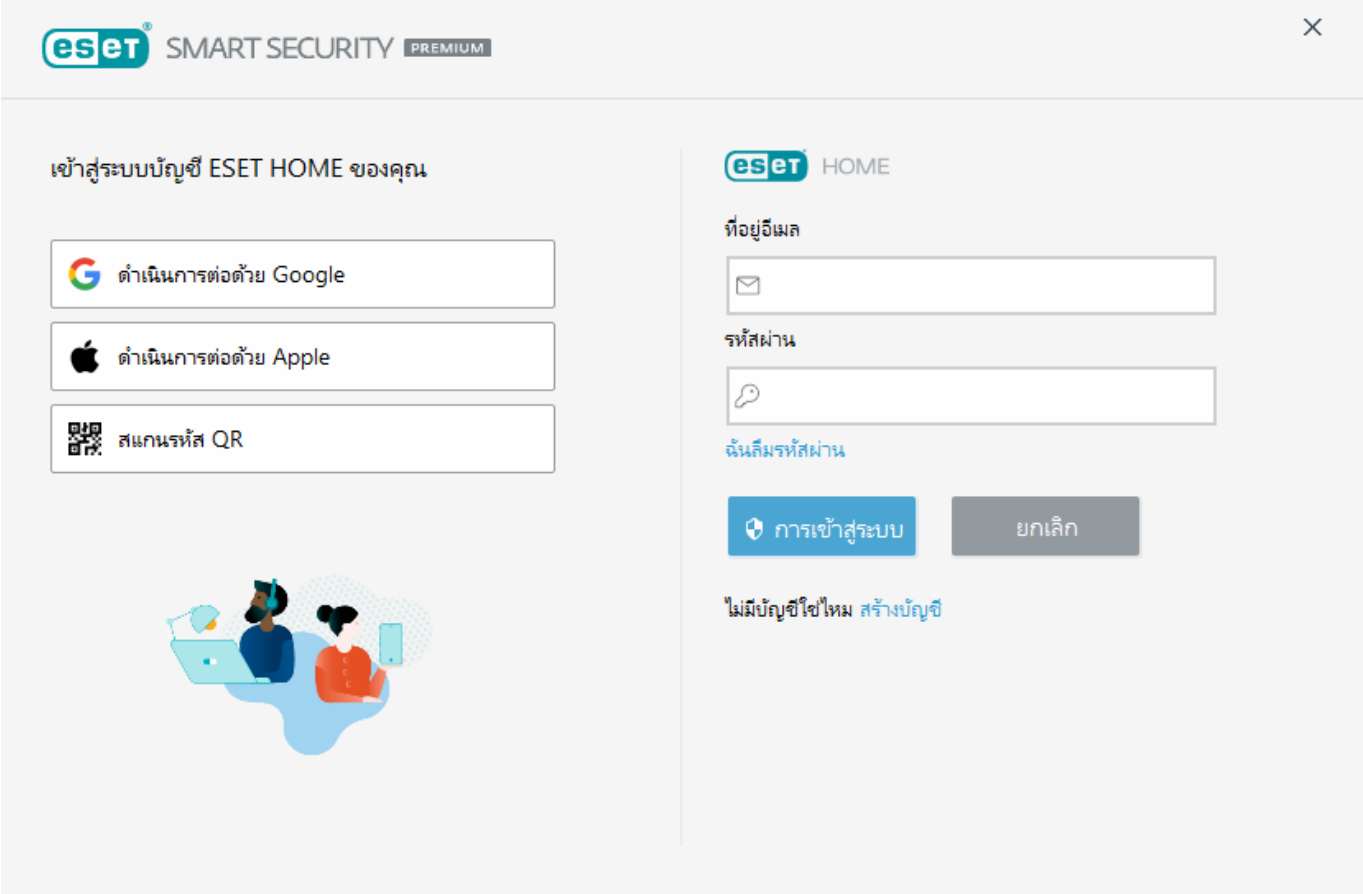
• **ใช้ที่อยู่อีเมล ESET HOME และรหัสผ่านของคุณ** – พิมพ์ **ที่อยู่อีเมล** และ **รหัสผ่าน** ที่คุณใช้สร้างบัญชี ESET HOME แล้วคลิก **ล็อคอิน**

• **ใช้บัญชี Google/AppleID** – คลิก **ดำเนินการต่อด้วย Google** หรือ **ดำเนินการต่อด้วย Apple** แล้วล็อคอินด้วยบัญชีที่ถูกต้อง หลังจากล็อคอินได้สำเร็จระบบจะเปลี่ยนเส้นทางคุณไปยังหน้าเว็บยืนยันของ ESET HOME หากต้องการดำเนินการต่อให้สลับกลับไปยังหน้าต่างผลิตภัณฑ์ ESET ของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการล็อคอินด้วยบัญชี Google /AppleID โปรดดูคำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME

• **สแกนรหัส QR** – คลิก **สแกนรหัส QR** เพื่อแสดงรหัส QR โปรดเปิดแอพโทรศัพท์มือถือ ESET HOME แล้วสแกนรหัส QR หรือหันกล้องบนอุปกรณ์ของคุณไปที่รหัส QR สำหรับข้อมูลเพิ่มเติม โปรดดูคำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME

หากคุณไม่มีบัญชี ESET HOME ให้คลิก **สร้างบัญชี** เพื่อลงทะเบียนหรือดูคำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME
หากคุณลืมรหัสผ่าน ให้คลิก **ฉันลืมรหัสผ่าน** และทำตามขั้นตอนบนหน้าจอหรือดู คำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME

⚠ ล็อคอินล้มเหลว - ข้อผิดพลาดทั่วไป



ล็อคอินล้มเหลว - ข้อผิดพลาดทั่วไป

เราไม่พบบัญชีที่ตรงกับที่อยู่อีเมลที่ป้อน

ที่อยู่อีเมลที่คุณป้อนไม่ตรงกับบัญชี ESET HOME ใดๆ เลย คลิก **ย้อนกลับ** แล้วพิมพ์ที่อยู่อีเมลและรหัสผ่านที่ถูกต้อง

หากต้องการล็อคอิน คุณจะต้องสร้างบัญชี ESET HOME หากคุณไม่มีบัญชี ESET HOME ให้คลิก **ย้อนกลับ** > **สร้างบัญชี** หรือดู สร้างบัญชี ESET HOME ใหม่

ชื่อผู้ใช้และรหัสผ่านไม่ตรงกัน

รหัสผ่านที่ป้อนไม่ตรงกับที่อยู่อีเมลที่ป้อน คลิก **ย้อนกลับ** จากนั้นป้อนรหัสผ่านที่ถูกต้องและตรวจสอบให้แน่ใจว่าที่อยู่อีเมลที่ป้อนถูกต้อง หากคุณยังไม่สามารถล็อคอินได้ ให้คลิก **ย้อนกลับ** > **ฉันลืมรหัสผ่าน** เพื่อรีเซ็ตรหัสผ่านแล้วปฏิบัติตามขั้นตอนบนหน้าจอหรือดู ฉันลืมรหัสผ่าน ESET HOME

ตัวเลือกการเข้าสู่ระบบที่เลือกไม่ตรงกับบัญชีของคุณ

บัญชีของคุณลิงก์อยู่กับบัญชีสื่อสังคม หากต้องการล็อคอิน ESET HOME ให้คลิก **ดำเนินการต่อด้วย Google** หรือ **ดำเนินการต่อด้วย Apple** แล้วล็อคอินบัญชีที่ถูกต้อง หลังจากล็อคอินได้สำเร็จแล้วระบบจะเปลี่ยนเส้นทางคุณไปยังหน้าเว็บยืนยันของ ESET HOME คุณสามารถยกเลิกการเชื่อมต่อสื่อสังคมออกจากบัญชี ESET HOME ของคุณได้ในพอร์ทัล ESET HOME

รหัสผ่านไม่ถูกต้อง

ข้อผิดพลาดนี้จะเกิดขึ้นเฉพาะเมื่อ ESET Smart Security Premium เชื่อมต่ออยู่กับ ESET HOME อยู่แล้วและคุณได้ทำการเปลี่ยนแปลงที่จำเป็นต้องใช้การล็อคอิน (ตัวอย่างเช่น การปิดใช้งาน Anti-Theft) และรหัสผ่านที่คุณป้อนไม่ตรงกับบัญชี คลิก **ย้อนกลับ** แล้วป้อนรหัสผ่านที่ถูกต้อง หากคุณยังไม่สามารถล็อคอินได้ ให้คลิก **ย้อนกลับ** > **ฉันลืมรหัสผ่าน** เพื่อรีเซ็ตรหัสผ่านแล้วปฏิบัติตามขั้นตอนบนหน้าจอหรือดู ฉันลืมรหัสผ่าน ESET HOME

เพิ่มอุปกรณ์ใน ESET HOME

หากคุณได้ติดตั้ง ESET Smart Security Premium ไว้และได้เปิดใช้งานด้วยใบอนุญาตที่เพิ่มเข้าในบัญชี ESET HOME ของคุณแล้ว คุณจะสามารถเพิ่มอุปกรณ์ของคุณเข้ากับ ESET HOME ได้โดยใช้พอร์ทัล ESET HOME:

1. ส่งคำขอเชื่อมต่อไปยังอุปกรณ์ของคุณ

2. ESET Smart Security Premium จะแสดงหน้าต่างข้อความ **เชื่อมต่ออุปกรณ์นี้เข้ากับบัญชี ESET HOME** พร้อมชื่อบัญชี ESET HOME โปรดคลิก **อนุญาต** เพื่อเชื่อมต่ออุปกรณ์เข้ากับบัญชี ESET HOME ที่กล่าวถึงนั้น

i หากไม่ได้ดำเนินการ คำขอเชื่อมต่อจะถูกยกเลิกโดยอัตโนมัติหลังจากประมาณ 30 นาที

หน้าต่างโปรแกรมหลัก

หน้าต่างหลักของโปรแกรม ESET Smart Security Premium จะถูกแบ่งออกเป็นสองส่วนหลัก หน้าต่างหลักที่ด้านขวาจะแสดงข้อมูลที่เกี่ยวข้องกับตัวเลือกที่เลือกจากเมนูหลักทางด้านซ้าย

i **คำแนะนำพร้อมภาพประกอบ**
โปรดดู เปิดหน้าต่างโปรแกรมหลักของผลิตภัณฑ์ ESET สำหรับ Windows เพื่อดูคำแนะนำพร้อมภาพประกอบของเราซึ่งมีให้แบบภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษา

ESET HOME – เชื่อมต่ออุปกรณ์ของคุณเข้ากับ ESET HOME ใช้ ESET HOME เพื่อดูและจัดการ การตั้งค่า Anti-Theft และ อุปกรณ์และใบอนุญาต ESET ที่เปิดใช้งานของคุณ

ข้อมูลต่อไปนี้จะเป็นคำอธิบายของตัวเลือกภายในเมนูหลัก:

หน้าแรก - ให้ข้อมูลเกี่ยวกับสถานะการป้องกันของ ESET Smart Security Premium

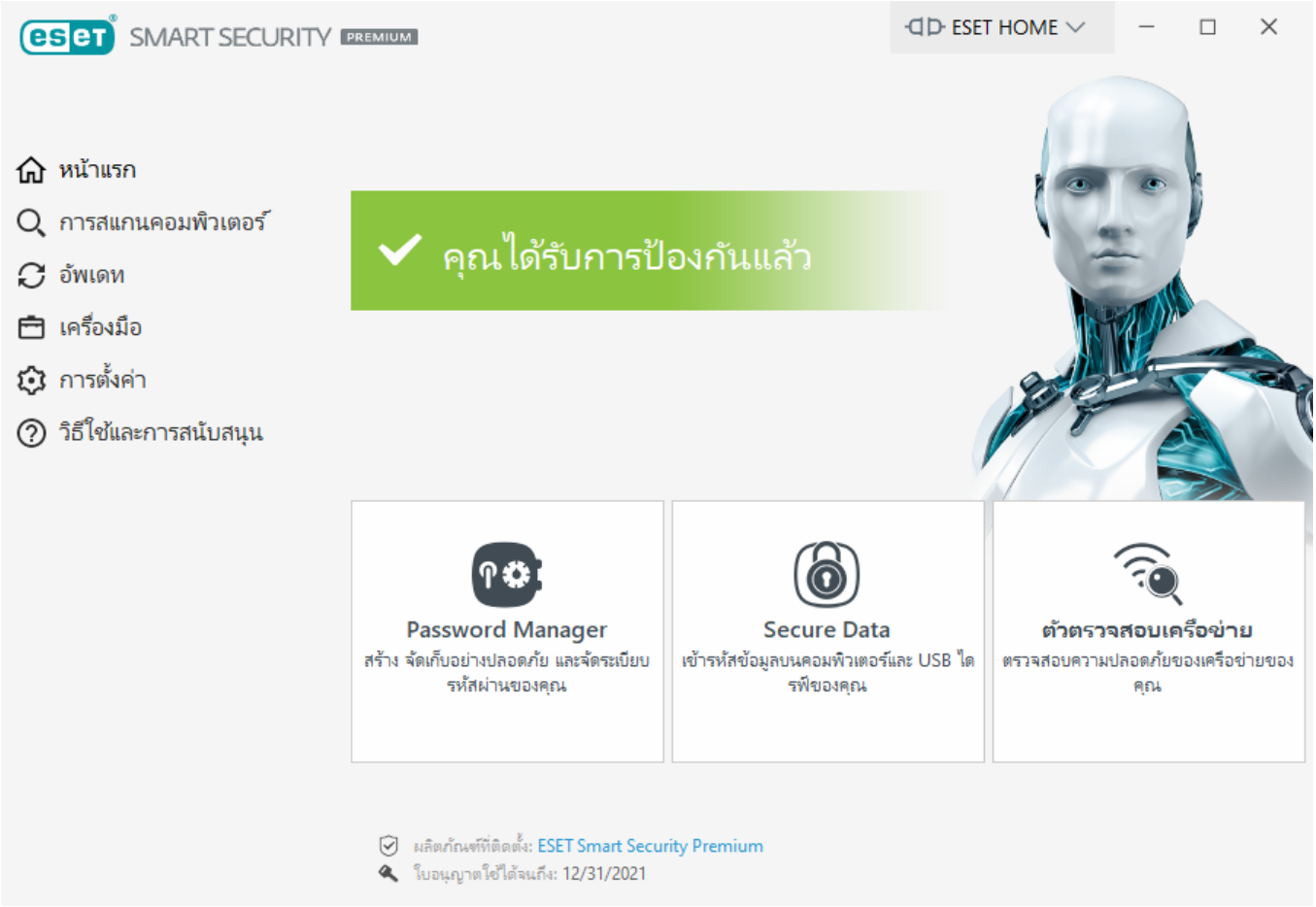
การสแกนคอมพิวเตอร์ - กำหนดค่าและเริ่มต้นสแกนคอมพิวเตอร์ของคุณหรือสร้างการสแกนแบบกำหนดเอง

อัพเดท - แสดงข้อมูลเกี่ยวกับการอัพเดทกลไกตรวจหา

เครื่องมือ – ให้การเข้าถึง Password Manager, Secure Data, ตัวตรวจสอบเครือข่าย, การป้องกันทางด้านธนาคารและการชำระเงิน, Anti-Theft และอื่นๆ โมดูลที่ช่วยให้การดูแลโปรแกรมง่ายขึ้นและให้ตัวเลือกเพิ่มเติมสำหรับผู้ใช้ขั้นสูง สำหรับข้อมูลเพิ่มเติม โปรดดู เครื่องมือใน ESET Smart Security Premium

การตั้งค่า - เลือกตัวเลือกนี้เพื่อปรับระดับความปลอดภัยสำหรับคอมพิวเตอร์ อินเทอร์เน็ตการป้องกันเครือข่ายและเครื่องมือความปลอดภัย.

วิธีใช้และการสนับสนุน - ให้การเข้าถึงไฟล์วิธีใช้ ฐานความรู้ของ ESET เว็บไซต์ของ ESET และลิงก์เพื่อส่งคำขอรับการสนับสนุน



หน้าจอหลัก ประกอบด้วยข้อมูลสำคัญเกี่ยวกับระดับการป้องกันปัจจุบันของคอมพิวเตอร์ของคุณ หน้าต่างสถานะจะแสดงคุณลักษณะที่ใช้บ่อยใน ESET Smart Security Premium ข้อมูลเกี่ยวกับผลิตภัณฑ์ที่ติดตั้งและวันที่หมดอายุของใบอนุญาตจะอยู่ที่นี่ด้วยเช่นกัน ให้คลิก **ESET Smart Security Premium** หากต้องการติดตั้งผลิตภัณฑ์ ESET เวอร์ชันอื่น ข้อมูลเพิ่มเติมเกี่ยวกับคุณลักษณะในแต่ละผลิตภัณฑ์ที่เฉพาะเจาะจง

ไอคอนสีเขียวและสถานะ **คุณได้รับการป้องกันแล้ว** สีเขียวแสดงว่ามีการป้องกันขั้นสูงสุด

ควรทำอย่างไรเมื่อโปรแกรมทำงานไม่ถูกต้อง

หากโมดูลการป้องกันที่ทำงานอยู่กำลังทำงานอย่างถูกต้อง ไอคอนสถานะการป้องกันจะเป็นสีเขียว เครื่องหมายอัศเจรีย์สีแดงหรือไอคอนการแจ้งเตือนสีส้มแสดงว่าไม่มีการป้องกันขั้นสูงสุด ข้อมูลเพิ่มเติมเกี่ยวกับสถานะการป้องกันของแต่ละโมดูล รวมทั้งทางแก้ไขที่แนะนำสำหรับการเรียกคืนการป้องกันแบบเต็มรูปแบบ จะปรากฏขึ้นใต้ **หน้าแรก** ในการเปลี่ยนสถานะของแต่ละโมดูล ให้คลิก **การตั้งค่า** แล้วเลือกโมดูลที่ต้องการ

ไอคอนสีแดงและสถานะ **แจ้งเตือนเรื่องความปลอดภัย** สีแดงจะหมายถึงปัญหาร้ายแรง มีเหตุผลหลายประการที่อาจทำให้สถานะนี้แสดงขึ้น ตัวอย่างเช่น:

- **ผลิตภัณฑ์ไม่ได้เปิดใช้งาน**หรือ**ใบอนุญาตหมดอายุแล้ว**– สิ่งนี้จะระบุโดยไอคอนสถานะการป้องกันเป็นสีแดง โปรแกรมจะไม่สามารถอัพเดทได้หลังจากใบอนุญาตของคุณหมดอายุ ปฏิบัติตามคำแนะนำต่อไปนี้ในหน้าต่างการเตือนเพื่อต่ออายุใบอนุญาต
- **กลไกตรวจหาไม่อัพเดท** – ข้อผิดพลาดจะปรากฏขึ้นหลังจากการพยายามอัพเดทกลไกตรวจหาที่ล้มเหลวหลายครั้ง ขอแนะนำให้คุณตรวจสอบการตั้งค่าการอัพเดท สาเหตุทั่วไปสำหรับข้อผิดพลาดนี้คือข้อมูลการตรวจสอบสิทธิ์ที่ป้อนไม่ถูกต้องหรือ การตั้งค่าการเชื่อมต่อ ที่กำหนดค่าไม่ถูกต้อง
- **การป้องกันระบบไฟล์แบบเรียลไทม์ถูกปิดใช้งาน** – การป้องกันระบบไฟล์แบบเรียลไทม์ถูกปิดใช้งานโดยผู้ใช้ คอมพิวเตอร์ของคุณไม่ได้รับการป้องกันจากภัยคุกคาม คลิก **เปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์** เพื่อเปิดใช้งานการทำงานนี้อีกครั้ง
- **การป้องกันไวรัสและการป้องกันสปายแวร์ถูกปิดใช้งาน** - คุณสามารถเปิดใช้งานการป้องกันไวรัสและการป้องกันสปายแวร์ใดอีกครั้งโดยคลิก **เปิดใช้งานการป้องกันไวรัสและสปายแวร์**
- **ไฟร์วอลล์ของ ESET ถูกปิดใช้งานอยู่** - ปัญหานี้ยังได้รับการระบุจากการแจ้งเตือนความปลอดภัยที่

อยู่ถัดจากรายการ **เครือข่าย** บนเดสก์ท็อปของคุณอีกด้วย คุณสามารถเปิดใช้งานการป้องกันเครือข่ายใหม่อีกครั้งได้โดยการคลิกที่ **เปิดใช้งานไฟร์วอลล์**

ไอคอนสีส้มระบุถึงการป้องกันที่จำกัด ตัวอย่างเช่น อาจเกิดปัญหาของการอัพเดทโปรแกรมหรือใบอนุญาตของคุณใกล้ถึงวันหมดอายุ

มีเหตุผลหลายประการที่อาจทำให้สถานะนี้แสดงขึ้น ตัวอย่างเช่น:

- **คำเตือนของการปรับการป้องกันการโจรกรรมให้เหมาะสม** - อุปกรณ์นี้ไม่ได้รับการปรับให้เหมาะสมสำหรับ การป้องกันการโจรกรรม ตัวอย่างเช่น บัญชีหลอก (คุณลักษณะความปลอดภัยที่ทำงานโดยอัตโนมัติเมื่อคุณระบุว่าอุปกรณ์สูญหาย) อาจไม่ได้สร้างขึ้นด้วยคอมพิวเตอร์ของคุณ คุณสามารถสร้างบัญชีหลอกได้โดยใช้คุณลักษณะ การปรับให้เหมาะสม ในส่วนติดต่อของเว็บไซต์ การป้องกันการโจรกรรม
- **โหมดผู้เล่นเกมเปิดใช้งานอยู่** - การเปิดใช้งาน โหมดผู้เล่นเกม อาจเกิดความเสี่ยงด้านความปลอดภัย การเปิดใช้งานคุณลักษณะนี้จะปิดใช้งานหน้าต่างป๊อปอัปทั้งหมดและหยุดงานตามกำหนดเวลาใดๆ
- **ใบอนุญาตของคุณใกล้หมดอายุแล้ว** - สามารถทราบปัญหานี้ได้จากไอคอนสถานะการป้องกันซึ่งจะแสดงเครื่องหมายอัศเจรีย์ใกล้กับนาฬิการะบบ หลังจากใบอนุญาตหมดอายุ โปรแกรมจะไม่สามารถอัพเดทและไอคอนสถานะการป้องกันจะเปลี่ยนเป็นสีแดง

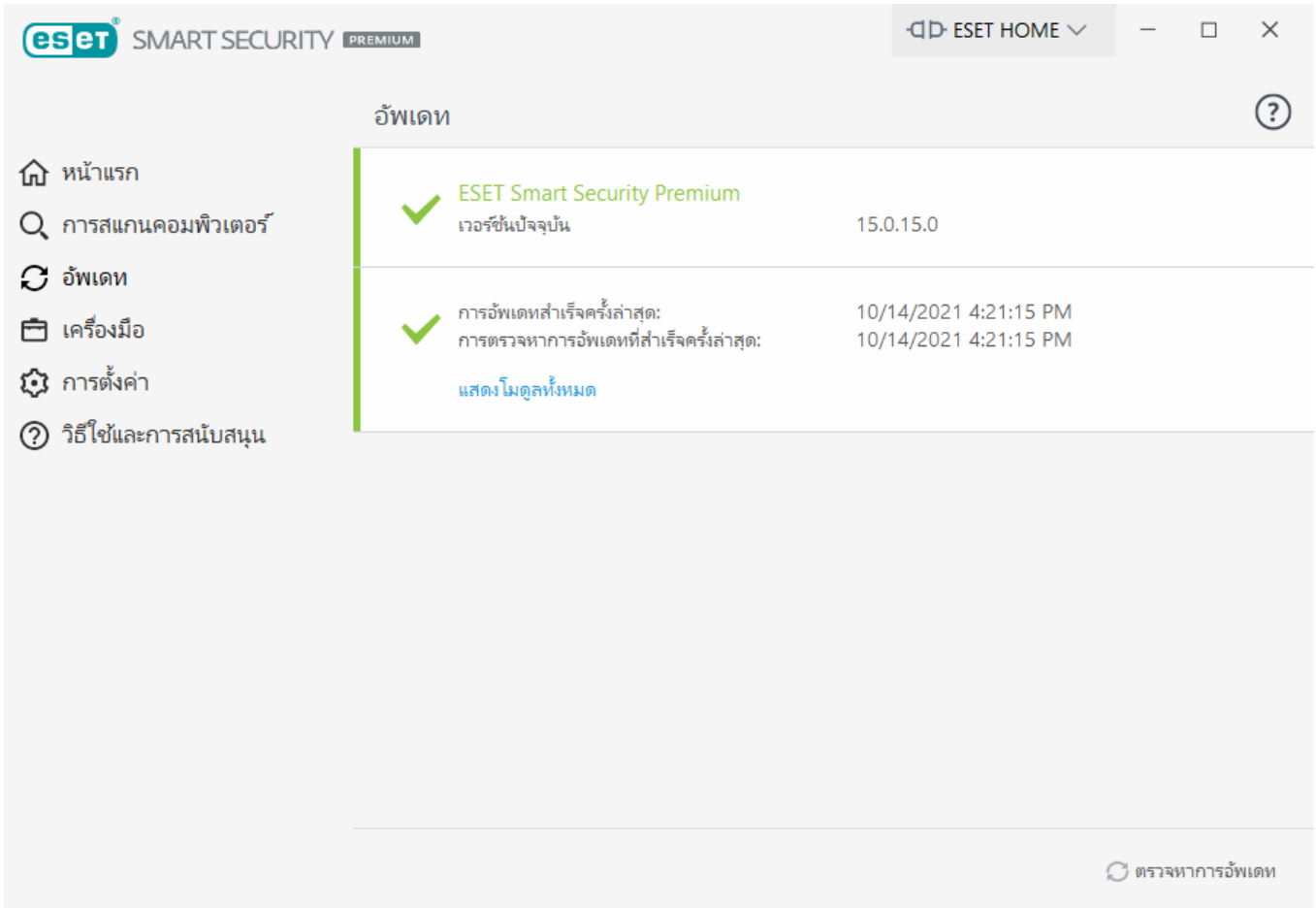
หากคุณไม่สามารถแก้ไขปัญหาโดยใช้วิธีแก้ไขที่แนะนำได้ ให้คลิก **วิธีใช้และการสนับสนุน** เพื่อเข้าถึงไฟล์วิธีใช้หรือค้นหา ฐานความรู้ ESET หากคุณยังคงต้องการความช่วยเหลือ คุณสามารถส่งคำร้องขอรับการสนับสนุนได้ ฝ่ายสนับสนุนทางเทคนิคของ ESET จะตอบคำถามของคุณอย่างรวดเร็วและค้นหาการแก้ไขปัญหา

การอัพเดท

การอัพเดท ESET Smart Security Premium เป็นประจำเป็นวิธีการที่ดีที่สุดเพื่อให้มั่นใจว่าคอมพิวเตอร์มีระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัพเดทจะช่วยให้มั่นใจได้ว่าทั้งโมดูลโปรแกรมและส่วนประกอบของระบบจะอัพเดทอยู่เสมอ

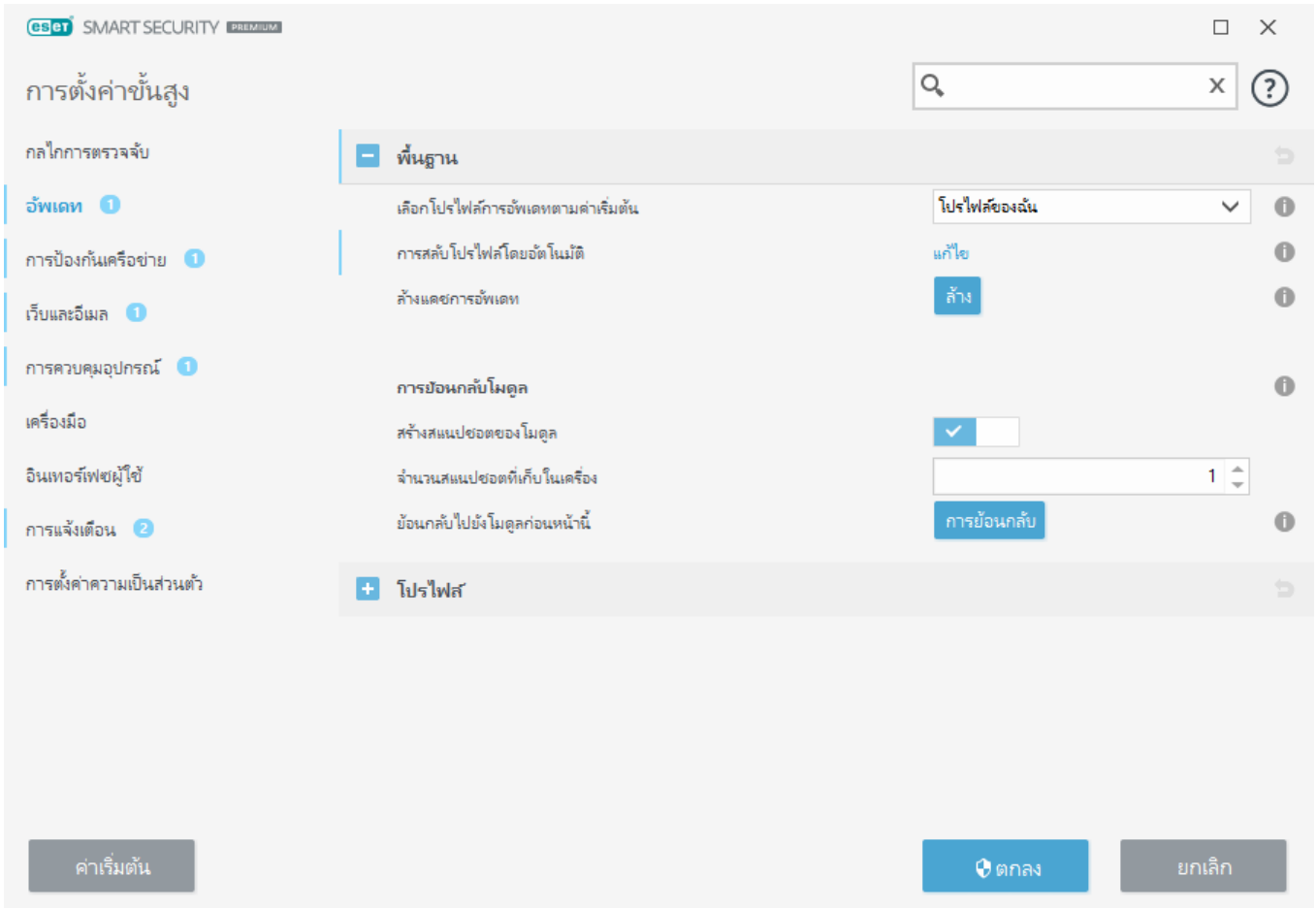
เมื่อคลิก **อัพเดท** ในหน้าต่างโปรแกรมหลัก คุณสามารถดูสถานะการอัพเดทในปัจจุบัน รวมถึงวันที่และเวลาของการอัพเดทที่สำเร็จครั้งล่าสุด และดูว่าจะต้องมีการอัพเดทหรือไม่ได้

นอกเหนือจากการอัพเดทอัตโนมัติแล้ว คุณยังสามารถคลิก **ตรวจหาการอัพเดท** เพื่อเรียกใช้การอัพเดทด้วยตนเองได้



หน้าต่างการตั้งค่าขั้นสูง (คลิก **การตั้งค่า** ในเมนูหลัก จากนั้นคลิก **การตั้งค่าขั้นสูง** หรือกด **F5** ในแป้นพิมพ์ของคุณ) มีตัวเลือกการอัพเดทเพิ่มเติม ในการกำหนดค่าตัวเลือกการอัพเดทขั้นสูง เช่น โหมดการอัพเดท การเข้าถึงเซิร์ฟเวอร์พร็อกซีและการเชื่อมต่อ LAN ให้คลิก **การอัพเดท** ในโครงสร้างการตั้งค่าขั้นสูง

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



ตั้งค่าเครื่องมือความปลอดภัย ESET เพิ่มเติม

ก่อนที่จะเริ่มใช้ ESET Smart Security Premium คุณสามารถตั้งค่าเครื่องมือความปลอดภัยเพิ่มเติมเพื่อเพิ่มการป้องกันให้มากที่สุดได้:

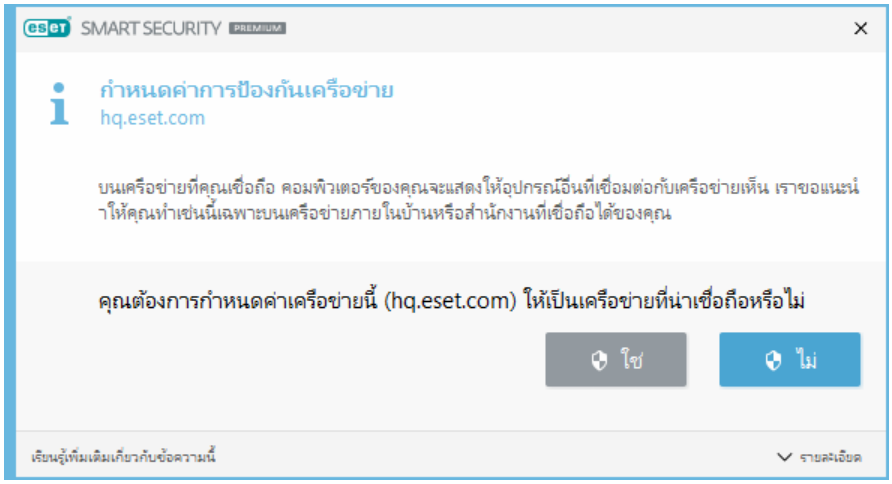
- Password Manager
- ESET Secure Data
- การควบคุมเนื้อหา
- การป้องกันการโจรกรรม

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าเครื่องมือความปลอดภัยใน ESET Smart Security Premium โปรดอ่านบทความฐานความรู้ของ ESET ต่อไปนี้

กำหนดค่าการป้องกันเครือข่าย

การกำหนดค่าเครือข่ายที่เชื่อมต่อถือเป็นสิ่งที่จำเป็น เพื่อป้องกันคอมพิวเตอร์ของคุณในสภาพแวดล้อมการทำงานของเครือข่าย คุณสามารถอนุญาตให้ผู้ใช้รายอื่นๆ เข้าถึงคอมพิวเตอร์ของคุณได้โดยกำหนดค่าการป้องกันเครือข่ายให้อนุญาตให้ใช้งานร่วมกัน คลิก **การตั้งค่า** > **การป้องกันเครือข่าย** > **เครือข่ายที่เชื่อมต่อ** แล้วคลิกลิงก์ด้านล่างเครือข่ายที่เชื่อมต่อ หน้าต่างป๊อปอัปจะแสดงตัวเลือกสำหรับกำหนดค่าเครือข่ายที่เลือกให้เป็นเครือข่ายที่เชื่อถือ

โดยค่าเริ่มต้น ESET Smart Security Premium จะใช้การตั้งค่า Windows เมื่อมีการตรวจพบเครือข่ายใหม่ หากต้องการให้แสดงหน้าต่างข้อความเมื่อตรวจพบเครือข่ายใหม่ ให้เปลี่ยนประเภทการป้องกันของเครือข่ายใหม่ใน เครือข่ายที่รู้จัก เป็นถามผู้ใช้ การกำหนดค่าการป้องกันเครือข่ายจะเกิดขึ้นเมื่อใดก็ตามที่คอมพิวเตอร์ของคุณเชื่อมต่อกับเครือข่ายใหม่ ดังนั้น ส่วนใหญ่แล้วจึงไม่จำเป็นต้องกำหนดโซนที่เชื่อถือ



มีโหมดการป้องกันเครือข่ายสองโหมดที่คุณสามารถเลือกได้จากในหน้าต่างการกำหนดค่าการป้องกันเครือข่าย ดังนี้:

• **ใช่** – สำหรับเครือข่ายที่เชื่อถือ (เครือข่ายในบ้านหรือที่ทำงาน) ผู้ใช้เครือข่ายรายอื่นสามารถมองเห็นคอมพิวเตอร์และไฟล์ที่ใช้ร่วมกันที่เก็บไว้ในคอมพิวเตอร์ของคุณได้ และผู้ใช้รายอื่นบนเครือข่ายสามารถเข้าถึงทรัพยากรระบบได้ เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าถึงเครือข่ายภายในที่ปลอดภัย

• **ไม่** – สำหรับเครือข่ายที่ไม่เชื่อถือ (เครือข่ายสาธารณะ) ไฟล์และโฟลเดอร์ในระบบของคุณจะไม่ถูกใช้ร่วมกันหรือมองเห็นได้สำหรับผู้ใช้รายอื่นบนเครือข่าย และการแบ่งปันทรัพยากรระบบจะถูกปิดใช้งาน เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าสู่เครือข่ายไร้สาย

การกำหนดค่าเครือข่ายที่ไม่ถูกต้องอาจทำให้เกิดความเสี่ยงด้านการรักษาความปลอดภัยของคอมพิวเตอร์ของคุณ

ตามค่าเริ่มต้น เวิร์กสเตชันจากเครือข่ายที่เชื่อถือจะสามารถเข้าถึงไฟล์และเครื่องพิมพ์ที่ใช้งานร่วมกันได้ เปิดใช้งานการสื่อสาร RPC ขาเข้า และทำให้การใช้เดสก์ท็อประยะไกลร่วมกันสามารถใช้งานได้

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับคุณลักษณะนี้ ให้อ่านบทความฐานความรู้ของ ESET ต่อไปนี้:

- เปลี่ยนแปลงการเชื่อมต่อเครือข่ายไฟร์วอลล์การตั้งค่าในผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้าน

เปิดใช้งาน การป้องกันการโจรกรรม

ในระหว่างที่เราเดินทางในชีวิตประจำวันจากที่บ้านไปที่ทำงาน หรือไปยังสถานที่สาธารณะอื่นๆ อุปกรณ์ส่วนบุคคลของเราจะมีความเสี่ยงต่อการสูญหายหรือถูกขโมยอยู่ตลอดเวลา การป้องกันการโจรกรรม เป็นคุณลักษณะที่ขยายการรักษาความปลอดภัยในระดับผู้ใช้ที่ครอบคลุมถึงกรณีอุปกรณ์สูญหายหรือถูกขโมย โดย การป้องกันการโจรกรรม ช่วยให้คุณสามารถตรวจสอบการใช้อุปกรณ์และติดตามอุปกรณ์ที่สูญหายได้โดยใช้การบอกตำแหน่งตามที่อยู่ IP ใน ESET HOME ซึ่งวิธีนี้จะช่วยให้คุณได้อุปกรณ์กลับคืนมาและช่วยปกป้องข้อมูลส่วนบุคคลของคุณได้

การใช้เทคโนโลยีที่ทันสมัย เช่น การค้นหาที่อยู่ IP ตามตำแหน่งทางภูมิศาสตร์ การบันทึกภาพจากกล้องทางเว็บ การป้องกันบัญชีผู้ใช้ และการตรวจสอบอุปกรณ์ การป้องกันการโจรกรรม อาจช่วยเหลือคุณและหน่วยงานผู้รักษากฎหมายในการค้นหาคอมพิวเตอร์หรืออุปกรณ์ของคุณ หากเกิดการสูญหายหรือถูกโจรกรรม ใน ESET HOME คุณสามารถดูกิจกรรมที่เกิดขึ้นในคอมพิวเตอร์หรืออุปกรณ์ของคุณได้

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับ การป้องกันการโจรกรรม ใน ESET HOME โปรดดูวิธีใช้ออนไลน์ของ ESET HOME

หากต้องการเปิดใช้งาน การป้องกันการโจรกรรม และปกป้องอุปกรณ์ของคุณในกรณีที่สูญหายหรือถูกโจรกรรม ให้เลือกตัวเลือกใดตัวเลือกหนึ่งต่อไปนี้:

- หลังจากติดตั้งผลิตภัณฑ์ ให้คลิก **เปิดใช้งาน การป้องกันการโจรกรรม** เพื่อเปิดใช้งาน การป้องกันการโจรกรรม
- หากคุณเห็นข้อความ "Anti-Theft พร้อมใช้งาน" ในหน้าต่างโปรแกรมหลัก > หน้าจอ**หลัก** ให้คลิก **เปิดใช้งาน การป้องกันการโจรกรรม**
- จากหน้าต่าง โปรแกรมหลัก ให้คลิก **เครื่องมือ** > **การป้องกันการโจรกรรม**
- จากหน้าต่างโปรแกรมหลัก ให้คลิก **การตั้งค่า** > **เครื่องมือความปลอดภัย** คลิกไอคอนแถบเลื่อน **การป้องกันการโจรกรรม** แล้วทำตามคำแนะนำบนหน้าจอ

หากอุปกรณ์ของคุณไม่ได้เชื่อมต่ออยู่กับ ESET HOME คุณจะต้อง:
1. ล็อคอินเข้าสู่บัญชี ESET HOME ของคุณเมื่อเปิดใช้งาน การป้องกันการโจรกรรม
2. ตั้งค่าชื่ออุปกรณ์

การป้องกันการโจรกรรม ไม่รองรับการทำงานของ Microsoft Windows Home Server

หลังจากที่คุณเปิดใช้งาน การป้องกันการโจรกรรม คุณสามารถปรับปรุงประสิทธิภาพการรักษาความปลอดภัยของอุปกรณ์ให้เหมาะสมได้ในหน้าต่างโปรแกรมหลัก > **เครื่องมือ** > **การป้องกันการโจรกรรม**

เครื่องมือการควบคุมเนื้อหา

หากคุณได้ เปิดใช้งานการควบคุมเนื้อหาเว็บไซต์ ใน ESET Smart Security Premium ไว้แล้ว คุณต้องตั้งค่าการควบคุมเนื้อหาเว็บไซต์ให้สำหรับบัญชีผู้ใช้ที่เกี่ยวข้องทุกบัญชีด้วย

เมื่อการควบคุมเนื้อหาเว็บไซต์ทำงานอยู่แต่ยังไม่มีการตั้งค่าบัญชีผู้ใช้ ข้อความ "ยังไม่มีการตั้งค่าการควบคุมเนื้อหาเว็บไซต์" จะปรากฏขึ้นบนหน้าจอ **หลัก** ให้คลิก **ตั้งค่ากฎ** แล้วดูส่วน การควบคุมเนื้อหาเว็บไซต์ สำหรับข้อมูลเพิ่มเติม

การทำงานกับ ESET Smart Security Premium

ตัวเลือกการตั้งค่าของ ESET Smart Security Premium ช่วยให้คุณสามารถปรับระดับการป้องกันคอมพิวเตอร์และเครือข่ายของคุณได้

เมนู **การตั้งค่า** แบ่งออกเป็นส่วนต่างๆ ดังต่อไปนี้:

การป้องกันคอมพิวเตอร์

การป้องกันอินเทอร์เน็ต

การป้องกันเครือข่าย

เครื่องมือความปลอดภัย

คลิกที่องค์ประกอบเพื่อปรับการตั้งค่าขั้นสูงของโมดูลการป้องกันที่เกี่ยวข้อง

การตั้งค่าการป้องกัน **คอมพิวเตอร์** จะช่วยให้คุณสามารถเปิดหรือปิดใช้งานองค์ประกอบต่อไปนี้:

- **การป้องกันระบบไฟล์แบบเรียลไทม์** – โปรแกรมจะสแกนไฟล์ทั้งหมดเพื่อหารหัสที่เป็นอันตรายเมื่อเปิด สร้าง หรือเรียกใช้ไฟล์
- **ESET LiveGuard** – เพิ่มชั้นการป้องกันแบบคลาวด์ซึ่งได้รับการออกแบบมาเป็นการเฉพาะเพื่อลดผลกระทบจากภัยคุกคามที่ไม่เคยพบมาก่อน

o**การป้องกันเชิงรุก** – ปิดกั้นการทำงานของไฟล์ใหม่จนกว่าจะได้รับได้รับผลการวิเคราะห์ ESET LiveGuard หากคุณต้องการยกเลิกการปิดกั้นไฟล์ที่กำลังอยู่ระหว่างการวิเคราะห์ ให้คลิกขาวแล้วคลิก **ยกเลิกการปิดกั้นไฟล์ที่ ESET LiveGuard กำลังวิเคราะห์**

• **การควบคุมอุปกรณ์** - โมดูลนี้อนุญาตให้คุณสแกน ปิดกั้น หรือปรับตัวกรอง/การอนุญาตเพิ่มเติมแล้วเลือกวิธีที่ผู้ใช้จะสามารถเข้าถึงและใช้อุปกรณ์ที่ให้ (ซีดี/ดีวีดี/USB...) ได้

• **HIPS** - ระบบHIPS จะตรวจสอบเหตุการณ์ภายในระบบปฏิบัติการและตอบสนองเหตุการณ์ตามชุดของกฎที่กำหนดเอง

• **โหมดผู้เล่นเกม** - เปิดหรือปิดใช้งาน โหมดผู้เล่นเกม คุณจะได้รับข้อความการเตือน (อาจทำให้เกิดความเสี่ยงด้านความปลอดภัย) และหน้าต่างหลักจะเปลี่ยนเป็น สีส้ม หลังจากเปิดใช้งานโหมดผู้เล่นเกม

• **การป้องกันเว็บแคม** - ควบคุมกระบวนการและแอพพลิเคชันซึ่งเข้าถึงกล้องที่เชื่อมต่อกับคอมพิวเตอร์

การตั้งค่า **การป้องกัน อินเทอร์เน็ต** จะช่วยคุณเปิดหรือปิดใช้งานองค์ประกอบต่อไปนี้:

• **การป้องกันการเข้าถึงเว็บ** – ถ้าเปิดใช้งานตัวเลือกนี้ ระบบจะสแกนการรับส่งทั้งหมดผ่าน HTTP หรือ HTTPS เพื่อหาซอฟต์แวร์ที่เป็นอันตราย

• **การป้องกันอีเมลไคลเอ็นต์** - ตรวจสอบการสื่อสารที่ได้รับผ่านทางโปรโตคอล POP3(S) และ IMAP(S)

• **การป้องกันสแปม** - สแกนอีเมลที่ไม่พึงประสงค์ เช่น สแปม

• **การป้องกันฟิชชิ่ง** - กรองเว็บไซต์ที่สงสัยว่ามีการแจกจ่ายเนื้อหาที่มุ่งจัดการผู้ใช้ให้ส่งข้อมูลที่เป็นความลับ

ส่วน **การป้องกันเครือข่าย** อนุญาตให้คุณเปิดหรือปิดใช้งาน ไฟร์วอลล์ การป้องกันการโจมตีเครือข่าย (IDS) และ การป้องกันบอตเน็ต

การตั้งค่า **เครื่องมือรักษาความปลอดภัย** ช่วยให้คุณสามารถปรับโมดูลต่อไปนี้:

• **การป้องกันทางด้านธนาคารและการชำระเงิน** – จะเพิ่มระดับการป้องกันเบราว์เซอร์เพิ่มเติมซึ่งออกแบบมาเพื่อปกป้องข้อมูลทางการเงินของคุณระหว่างการทำธุรกรรมออนไลน์ เปิดใช้งาน **ป้องกันเบราว์เซอร์ทั้งหมด** เพื่อเริ่มใช้งาน เว็บเบราว์เซอร์ที่รองรับ ในโหมดปลอดภัย สำหรับข้อมูลเพิ่มเติมโปรดดู การป้องกันทางด้านธนาคารและการชำระเงิน

• **การควบคุมเนื้อหาเว็บไซต์** – โมดูล การควบคุมเนื้อหาเว็บไซต์ จะช่วยปกป้องบุตรหลานของคุณโดยบล็อกเนื้อหาที่ไม่เหมาะสมหรือเป็นอันตรายบนอินเทอร์เน็ต

• **Anti-Theft** – เปิดใช้งาน การป้องกันการโจรกรรม เพื่อป้องกันคอมพิวเตอร์ของคุณในกรณีที่เกิดการสูญหายหรือถูกโจรกรรม

• **Secure Data** – เมื่อเปิดใช้งาน ESET Secure Data คุณสามารถเข้ารหัสข้อมูลของคุณเพื่อป้องกันการใช้ข้อมูลส่วนตัวที่เป็นความลับในทางที่ผิด

• **Password Manager** – Password Manager จะปกป้องและจัดเก็บรหัสผ่านและข้อมูลส่วนบุคคลของคุณ

การควบคุมเนื้อหาจะช่วยให้คุณปิดกั้นหน้าเว็บที่อาจมีเนื้อหาที่ไม่เหมาะสม นอกจากนี้ ผู้ปกครองสามารถห้ามการเข้าถึงเว็บไซต์ที่กำหนดไว้ล่วงหน้าได้มากกว่า 40 ประเภทและกว่า 140 ประเภทย่อย

เมื่อต้องการเปิดใช้งานองค์ประกอบด้านความปลอดภัยที่ถูกปิดใช้งานอีกครั้ง ให้คลิกแถบเลื่อน เพื่อแสดงเครื่องหมายถูกสีเขียว

เมื่อปิดใช้งานการป้องกันด้วยวิธีนี้ โมดูลการป้องกันที่ปิดใช้งานอยู่ทั้งหมดจะเปิดใช้งานหลังจากเริ่มต้นระบบคอมพิวเตอร์ใหม่

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

การป้องกันคอมพิวเตอร์

คลิก **การป้องกันคอมพิวเตอร์** จากหน้าต่าง **การตั้งค่า** เพื่อดูภาพรวมของโมดูลการป้องกันทั้งหมด

• การป้องกันระบบไฟล์แบบเรียลไทม์

• ESET LiveGuard

oการป้องกันเชิงรุก – ปิดกั้นการทำงานของไฟล์ใหม่จนกว่าจะได้รับได้รับผลการวิเคราะห์ ESET LiveGuard หากคุณต้องการยกเลิกการปิดกั้นไฟล์ที่กำลังอยู่ระหว่างการวิเคราะห์ ให้คลิกขาวแล้วคลิก **ยกเลิกการปิดกั้นไฟล์ที่ ESET LiveGuard กำลังวิเคราะห์**

• การควบคุมอุปกรณ์

• ระบบป้องกันการบุกรุกโฮสต์ (HIPS)

• โหมดผู้เล่นเกม

- การป้องกัน Webcam

หากต้องการหยุดชั่วคราวหรือปิดใช้งานโมดูลการป้องกันแต่ละโมดูล ให้คลิกไอคอนแถบเลื่อน 

> ⚠ การปิดโมดูลการป้องกันอาจลดระดับการป้องกันของคอมพิวเตอร์ของคุณ

คลิกไอคอนฟันเฟือง ⚙ ที่อยู่ถัดจากโมดูลการป้องกันเพื่อเข้าถึงการตั้งค่าขั้นสูงสำหรับโมดูลนั้น

สำหรับการ **ป้องกันระบบไฟล์แบบเรียลไทม์** ให้คลิกไอคอนฟันเฟือง ⚙ และเลือกจากตัวเลือกต่อไปนี้:

- **กำหนดค่า** – เปิดการตั้งค่าขั้นสูงสำหรับการป้องกันระบบไฟล์แบบเรียลไทม์
- **แก้ไขการยกเว้น** – เปิด หน้าต่างการตั้งค่าการยกเว้น เพื่อให้คุณสามารถยกเว้นไฟล์และโฟลเดอร์จากการสแกนได้

สำหรับการ **การป้องกันเว็บแคม** ให้คลิกไอคอนฟันเฟือง ⚙ และเลือกจากตัวเลือกต่อไปนี้:

- **กำหนดค่า** – เปิดการตั้งค่าขั้นสูงสำหรับการป้องกันเว็บแคม
- **ปิดกั้นการเข้าถึงทั้งหมดจนกว่าจะรีสตาร์ท** – ปิดกั้นการเข้าถึงเว็บแคมจนกว่าคอมพิวเตอร์จะรีสตาร์ท
- **ปิดกั้นการเข้าถึงทั้งหมดโดยถาวร** – ปิดกั้นการเข้าถึงเว็บแคมจนกว่าการตั้งค่านี้จะถูกปิดใช้งาน
- **หยุดปิดกั้นการเข้าถึงทั้งหมด** – ปิดการใช้งานความสามารถในการปิดกั้นการเข้าถึงเว็บแคม ตัวเลือกนี้จะใช้ได้เฉพาะเมื่อการเข้าถึงเว็บแคมถูกปิดกั้นอยู่เท่านั้น

หยุดการป้องกันไวรัสและสปายแวร์ - ปิดใช้งานโมดูลแอนตี้ไวรัสและสปายแวร์ทั้งหมด เมื่อคุณปิดใช้งานการป้องกัน หน้าต่างจะเปิดขึ้นซึ่งคุณสามารถกำหนดระยะเวลาการปิดใช้งานการป้องกันได้โดยใช้เมนูแบบเลื่อนลง **ช่วงเวลา** โปรดใช้หากคุณเป็นผู้ใช้ที่มีประสบการณ์หรือได้รับคำแนะนำจากฝ่ายสนับสนุนด้านเทคนิคของ ESET เท่านั้น

กลไกการตรวจจับ

กลไกการตรวจจับป้องกันการโจมตีของระบบที่ประสงค์ร้ายโดยการควบคุมไฟล์ อีเมล และการติดต่อสื่อสารทางอินเทอร์เน็ต ตัวอย่างเช่น หากวัตถุที่ถูกจัดประเภทเป็นมัลแวร์ถูกตรวจจับ การปรับปรุงแก้ไขจะเริ่มต้นขึ้น กลไกการตรวจจับสามารถลบวัตถุได้โดยการปิดกั้นวัตถุก่อน แล้วจึงกำจัด ลบ หรือย้ายไปยังการกักเก็บ

หากต้องการกำหนดการตั้งค่ากลไกการตรวจจับโดยละเอียด ให้คลิก **การตั้งค่าขั้นสูง** หรือกด **F5**

การเปลี่ยนเป็นการตั้งค่ากลไกการตรวจจับควรดำเนินการโดยผู้ใช้ที่มีประสบการณ์ในการใช้งานเท่านั้น การกำหนดค่าที่ไม่ถูกต้องของการตั้งค่าจะลดระดับความสามารถในการป้องกัน

ในส่วนนี้:

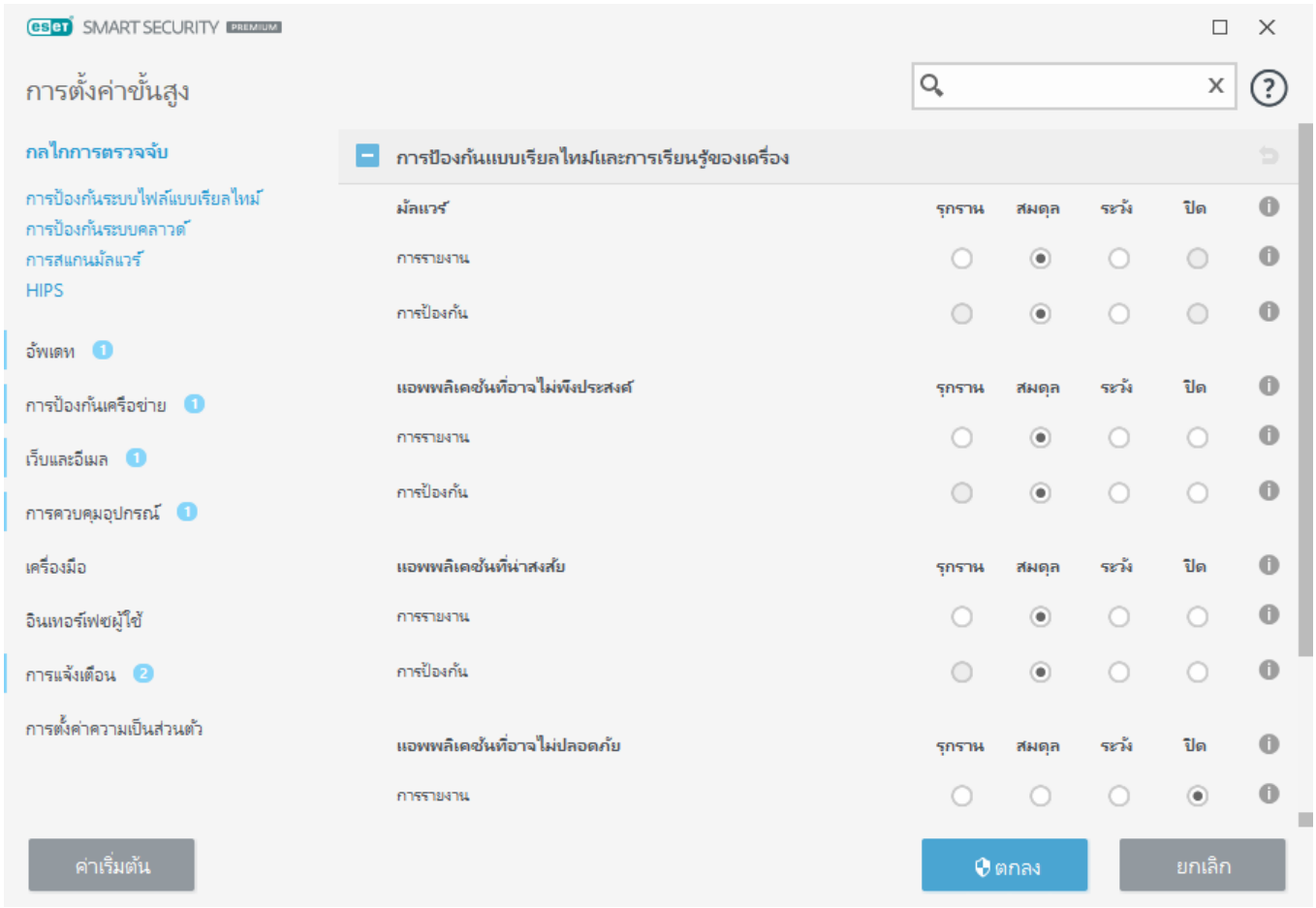
- ประเภทการป้องกันแบบเรียลไทม์และการเรียนรู้ของเครื่อง

- การสแกนมัลแวร์
- การตั้งค่าการรายงาน
- การตั้งค่าการป้องกัน

ประเภทการป้องกันแบบเรียลไทม์และการเรียนรู้ของเครื่อง

การป้องกันแบบเรียลไทม์และการเรียนรู้ของเครื่อง สำหรับโมดูลการป้องกันทั้งหมด (ตัวอย่างเช่น การป้องกันระบบไฟล์แบบเรียลไทม์,การป้องกันการเข้าถึงเว็บไซต์ ฯลฯ) อนุญาตให้คุณตั้งค่าการรายงานและระดับการป้องกันของประเภทต่อไปนี้:

- **มัลแวร์** – 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 การเรียนรู้ของเครื่องขั้นสูงเป็นส่วนหนึ่งของกลไกการตรวจจับในฐานะชั้นการป้องกันขั้นสูง ซึ่งช่วยปรับปรุงการตรวจหาโดยอิงจากการเรียนรู้ของเครื่อง อ่านข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้ใน ประมวลศัพท์

การสแกนมัลแวร์

การตั้งค่าเครื่องมือสแกนสามารถกำหนดค่าแยกกันสำหรับเครื่องมือสแกนแบบเรียลไทม์และเครื่องมือสแกนตามต้องการได้ โดยจะเปิดใช้งาน **ใช้การตั้งค่าการป้องกันแบบเรียลไทม์** ตามค่าเริ่มต้น เมื่อเปิดใช้งาน การตั้งค่าการสแกนตามต้องการ จะรับช่วงต่อจากส่วน **การป้องกันแบบเรียลไทม์และการเรียนรู้ของเครื่อง** หากต้องการดูข้อมูลเพิ่มเติม โปรดดูการสแกนมัลแวร์

การตั้งค่าการรายงาน

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

เกณฑ์การรายงานจะกำหนดค่าสำหรับแต่ละประเภท (เรียกว่า "ประเภท"):

1.มัลแวร์

2.แอพพลิเคชันที่อาจไม่พึงประสงค์

3.อาจไม่ปลอดภัย

4.แอพพลิเคชันที่น่าสงสัย

การรายงานจะทำงานด้วยกลไกการตรวจจับ รวมถึงองค์ประกอบการเรียนรู้ของเครื่อง สามารถตั้งค่าเกณฑ์การรายงานที่สูงกว่าเกณฑ์การป้องกันปัจจุบันได้ 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 Smart Security Premium

ความพร้อม (เปิดใช้งาน หรือ ปิดใช้งาน) ของโมดูลการป้องกันสำหรับเกณฑ์ประเภทที่เลือกมีดังต่อไปนี้:

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

* สามารถใช้งานได้ใน ESET Smart Security Premium เวอร์ชัน 13.1 และใหม่กว่า

**ไม่แนะนำ

ระบุเวอร์ชันผลิตภัณฑ์ โมดูลโปรแกรม และวันที่สร้าง

1.คลิก **วิธีใช้และการสนับสนุน** > **เกี่ยวกับ ESET Smart Security Premium**

2.ในหน้าจอ **เกี่ยวกับ** บรรทัดแรกของข้อความจะแสดงหมายเลขเวอร์ชันของผลิตภัณฑ์ ESET ของคุณ

3.คลิก **องค์ประกอบที่ติดตั้ง** เพื่อเข้าถึงข้อมูลเกี่ยวกับโมดูลเฉพาะ

Keynotes

Keynotes จำนวนหนึ่งเมื่อตั้งค่าเกณฑ์ที่เหมาะสมสำหรับสภาพแวดล้อมของคุณ:

- เกณฑ์**สมดุล**เป็นที่แนะนำสำหรับการตั้งค่าส่วนใหญ่
- เกณฑ์**ระวัง**แสดงถึงระดับการป้องกันที่เปรียบเทียบกันได้จากเวอร์ชันก่อนของ ESET Smart Security Premium (13.0 ลงไป) แนะนำให้ใช้สำหรับสภาพแวดล้อมที่มุ่งเน้นไปที่การลดวัตถุที่รายงานผิดพลาดโดยซอฟต์แวร์ด้านความปลอดภัยเป็นสำคัญ
- ยิ่งเกณฑ์การรายงานสูงเท่าใด อัตราการตรวจหาก็สูงเท่านั้น แต่ก็มีโอกาสที่จะเป็นวัตถุที่รายงานผิดพลาดได้มากกว่าเช่นเดียวกัน
- จากมุมมองของโลกแห่งความเป็นจริง ไม่มีการรับประกันอัตราการตรวจหา 100% เช่นเดียวกับที่มีโอกาส 0% ที่จะหลีกเลี่ยงไม่ให้มีการจัดประเภทวัตถุที่ไม่ติดไวรัสอย่างผิดๆ ว่าเป็นมัลแวร์
- ทำให้ ESET Smart Security Premium 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

ตารางการเปลี่ยนแปลงสำหรับ ESET Smart Security Premium 13.0 ลงไป

เมื่ออัปเกรดจากเวอร์ชัน 13.0 ลงไปเป็นเวอร์ชัน 13.1 และใหม่กว่า สถานะของเกณฑ์ใหม่จะเป็นดังต่อไปนี้:

สลับประเภทก่อนอัพเกรด	✓	✗
เกณฑ์ของประเภทใหม่หลังจากอัพเกรด	สมดุล	ปิด

ตัวเลือกขั้นสูงของกลไกการตรวจจับ

เทคโนโลยีการป้องกันการปกปิด เป็นระบบที่ก้าวหน้า ซึ่งสามารถตรวจหาโปรแกรมที่เป็นอันตราย เช่น รูทคิท ซึ่งสามารถซ่อนตัวจากระบบปฏิบัติการได้ ซึ่งหมายความว่า โปรแกรมไม่สามารถตรวจพบโดยใช้เทคนิคการทดสอบทั่วไป

เปิดใช้งานการสแกนขั้นสูงผ่าน AMSI – เครื่องมือ Microsoft Antimalware Scan Interface ที่ช่วยให้นักพัฒนาแอพพลิเคชันป้องกันมัลแวร์ใหม่ๆ ได้ (Windows 10 เท่านั้น)

ตรวจพบการแฝงตัว

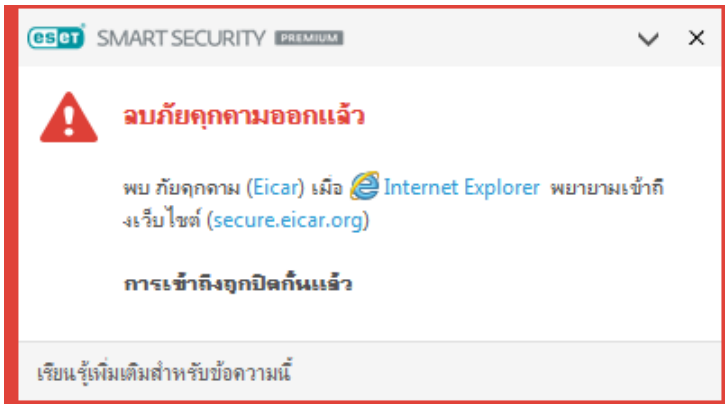
การบุกรุกสามารถเข้าสู่ระบบได้จากจุดเข้าใช้ต่างๆ เช่น หน้าเว็บ โฟลเดอร์ที่ใช้ร่วมกัน ผ่านอีเมล หรือจากอุปกรณ์ที่ถอดเข้าออกได้ (USB, ดิสก์ภายนอก, ซีดี, ดีวีดี เป็นต้น)

พฤติกรรมมาตรฐาน

สำหรับตัวอย่างทั่วไปของวิธีจัดการกับการบุกรุกโดย ESET Smart Security Premium ระบบจะตรวจพบการบุกรุกโดยใช้:

- การป้องกันระบบไฟล์แบบเรียลไทม์
- การป้องกันการเข้าถึงเว็บ
- การป้องกันอีเมลไคลเอ็นต์
- การสแกนคอมพิวเตอร์ตามต้องการ

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



การสแกนคอมพิวเตอร์เพื่อค้นหาไฟล์ที่ติดไวรัส

ถ้าคอมพิวเตอร์ของคุณแสดงสัญญาณการติดไวรัสจากมัลแวร์ เช่น ทำงานช้า ค้างบ่อยๆ เป็นต้น เราขอแนะนำให้คุณดำเนินการดังนี้:

1.เปิด ESET Smart Security Premium แล้วคลิก**การสแกนคอมพิวเตอร์**

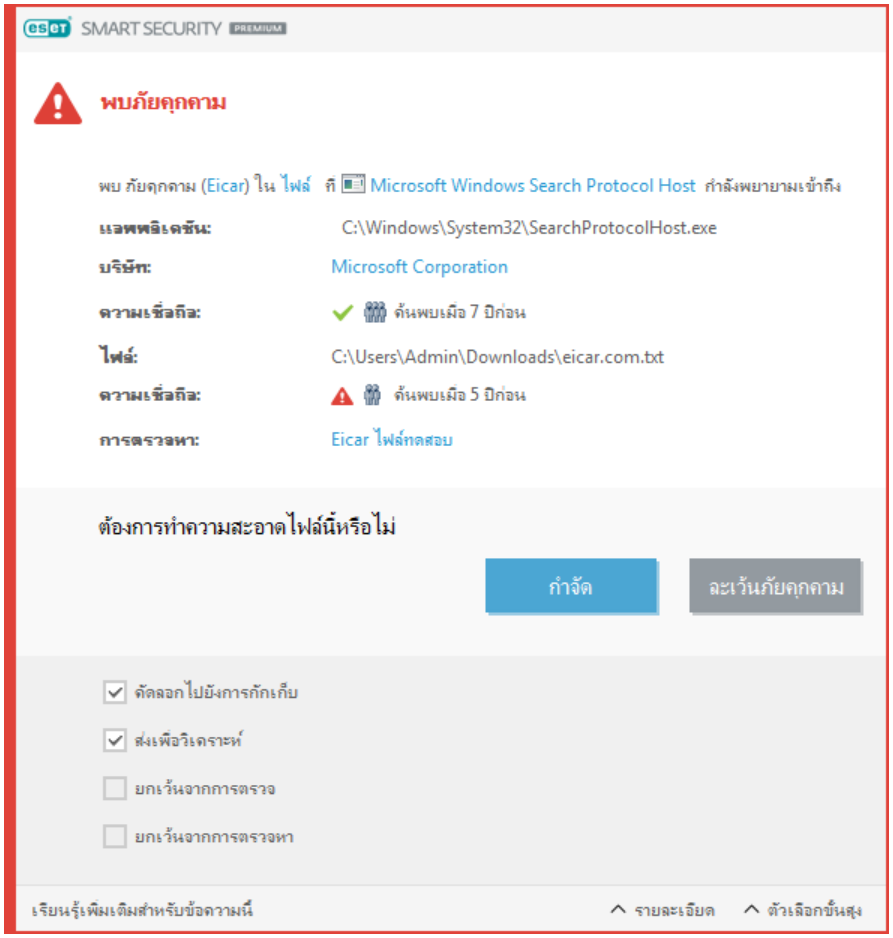
2.คลิก **สแกนคอมพิวเตอร์ของคุณ** (สำหรับข้อมูลเพิ่มเติม ให้ดูที่ การสแกนคอมพิวเตอร์)

3.หลังจากสแกนเสร็จสิ้นแล้ว ให้ตรวจดูบันทึกสำหรับจำนวนไฟล์ที่สแกน ไฟล์ที่ติดไวรัส และไฟล์ที่มีการกำจัดไวรัส

หากคุณต้องการสแกนเฉพาะบางส่วนของดิสก์ ให้คลิก **การสแกนที่กำหนดเอง** และเลือกเป้าหมายที่จะสแกนหาไวรัส

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

การกักเก็บนั้นสามารถเข้าถึงได้จากหน้าต่างโปรแกรมหลัก ESET Smart Security Premium โดยการคลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **การกักเก็บ**

นอกจากนี้ไฟล์ที่ถูกกักเก็บยังสามารถเรียกคืนไปยังตำแหน่งดั้งเดิมได้อีกด้วย:

• ใช้คุณสมบัติ **เรียกคืน** สำหรับการดำเนินการดังกล่าว ซึ่งสามารถใช้งานได้จากเมนูบริบทโดยคลิกไฟล์ที่ต้องการในการกักเก็บ

• หากไฟล์ถูกทำเครื่องหมายเป็น แอพพลิเคชันที่อาจไม่พึงประสงค์ ตัวเลือก **เรียกคืนและยกเว้นจากการสแกน** จะเปิดใช้งาน ทั้งนี้โปรดดู การยกเว้น

• นอกจากนี้เมนูบริบทยังมีตัวเลือก **เรียกคืนไปที่** ซึ่งช่วยให้คุณสามารถเรียกคืนไฟล์ไปยังตำแหน่งอื่นนอกเหนือจากตำแหน่งที่ถูกลบได้

• ในบางกรณีจะไม่สามารถใช้งานฟังก์ชันการเรียกคืนได้ ตัวอย่างเช่น ไฟล์ที่ตั้งอยู่ในการแชร์เครือข่ายที่อ่านได้อย่างเดียวเท่านั้น

มีภัยคุกคามหลายรายการ

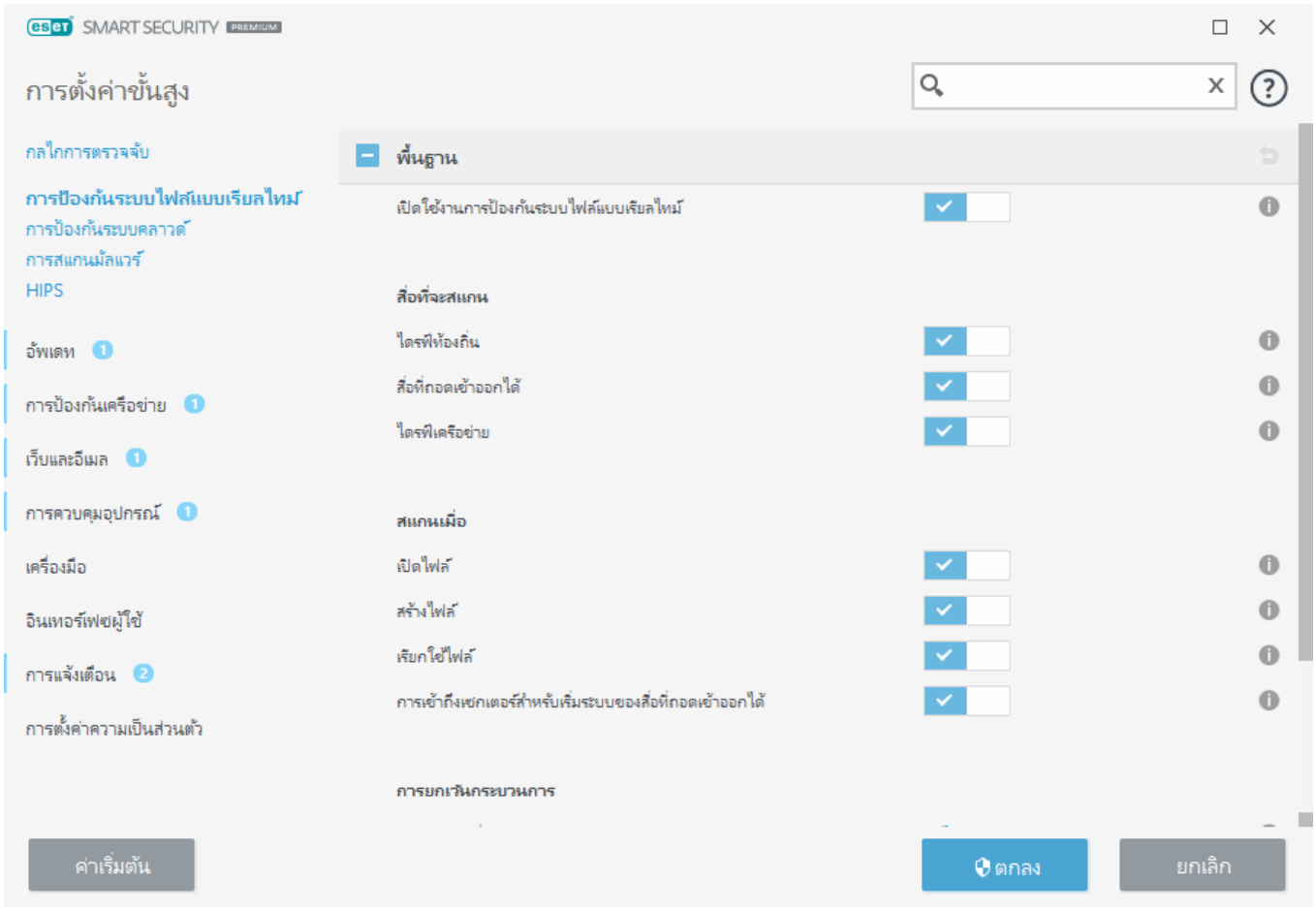
ถ้าไฟล์ที่ติดไวรัสไม่ได้รับการกำจัดในระหว่างการสแกนคอมพิวเตอร์ (หรือ ระดับการกำจัด ถูกกำหนดเป็น **ไม่มีการกำจัด**) ระบบจะแสดงหน้าต่างการเตือนให้คุณเลือกการทำงานสำหรับไฟล์เหล่านั้น เลือกการทำงานสำหรับไฟล์ (การทำงานจะได้รับการกำหนดให้ใช้กับไฟล์ในรายการได้ทีละไฟล์) จากนั้นคลิก **สิ้นสุด**

การลบไฟล์ในอาร์ไคฟ์

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

การป้องกันระบบไฟล์แบบเรียลไทม์

การป้องกันระบบไฟล์แบบเรียลไทม์จะควบคุมไฟล์ทั้งหมดในระบบสำหรับรหัสที่เป็นอันตรายเมื่อเปิด สร้าง หรือเรียกใช้



ตามค่าเริ่มต้น การป้องกันแบบเรียลไทม์จะเริ่มต้นทำงานเมื่อเริ่มต้นระบบและให้การสแกนทำงานต่อเนื่อง เราไม่แนะนำให้ปิดใช้งาน **เปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์** ใน **การตั้งค่าขั้นสูง** ภายใต้ **กลไกการตรวจจับ** > **การป้องกันระบบไฟล์แบบเรียลไทม์** > **พื้นฐาน**

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 โปรแกรมจะสแกนไฟล์ทั้งหมดเมื่อเปิด สร้าง หรือเรียกใช้ ขอแนะนำให้คุณคงการตั้งค่าเริ่มต้นเหล่านี้ไว้ เนื่องจากการตั้งค่าเหล่านี้จะให้การป้องกันแบบเรียลไทม์ในระดับสูงสุดสำหรับคอมพิวเตอร์ของคุณ:

- **เปิดไฟล์** – สแกนเมื่อไฟล์ถูกเปิด
- **สร้างไฟล์** – สแกนไฟล์ที่ถูกสร้างหรือแก้ไข
- **เรียกใช้ไฟล์** – สแกนเมื่อไฟล์ถูกเรียกใช้หรือทำงาน
- **การเข้าถึงบูตเซคเตอร์ของสื่อที่ถอดเข้าออกได้** – เมื่อสื่อที่ถอดเข้าออกได้ที่มีบูตเซคเตอร์เสียบเข้าไปในอุปกรณ์ บูตเซคเตอร์จะสแกนในทันที ตัวเลือกนี้ไม่ได้เปิดใช้งานการสแกนไฟล์สื่อที่ถอดเข้าออกได้ การสแกนไฟล์สื่อที่ถอดเข้าออกได้จะอยู่ใน **สื่อที่จะสแกน** > **สื่อที่ถอดเข้าออกได้** สำหรับการทำให้ **การเข้าถึงบูตเซคเตอร์ของสื่อที่ถอดเข้าออกได้** ทำงานอย่างถูกต้อง ให้เปิดใช้งาน **บูตเซคเตอร์/UEFI** ในพารามิเตอร์ ThreatSense

การป้องกันระบบไฟล์แบบเรียลไทม์จะตรวจสอบสื่อทุกประเภท และจะถูกเรียกใช้ตามเหตุการณ์ต่าง ๆ ของระบบ เช่น การเข้าถึงไฟล์ การใช้วิธีการตรวจหาของเทคโนโลยี ThreatSense (ดังที่อธิบายไว้ในส่วน ThreatSense การตั้งค่าพารามิเตอร์กลไก) สามารถกำหนดค่าการป้องกันระบบไฟล์แบบเรียลไทม์เพื่อปฏิบัติต่อไฟล์ที่สร้างใหม่แตกต่างจากไฟล์ที่มีอยู่แล้ว ตัวอย่างเช่น คุณสามารถกำหนดค่าการป้องกันระบบไฟล์แบบเรียลไทม์เพื่อตรวจสอบไฟล์ที่สร้างใหม่ได้อย่างใกล้ชิดมากขึ้น

เพื่อให้มีการใช้ทรัพยากรของระบบน้อยที่สุดเมื่อใช้การป้องกันระบบไฟล์แบบเรียลไทม์ ไฟล์ที่ผ่านการสแกนแล้วจะไม่มีการสแกนซ้ำอีก (ยกเว้นกรณีที่มีการแก้ไข) ไฟล์จะถูกสแกนอีกครั้งในทันทีหลังจากอัพเดทกลไกตรวจหาแต่ละครั้ง สามารถควบคุมการทำงานแบบนี้ได้ด้วยการใช้ **การเพิ่มประสิทธิภาพแบบสมาร์ท** หากปิดใช้งาน **การเพิ่มประสิทธิภาพแบบสมาร์ท** ไฟล์ทั้งหมดจะถูกสแกนในแต่ละครั้งที่มีการเข้าถึง หากต้องการแก้ไขการตั้งค่านี้ ให้กด **F5** เพื่อเปิด**การตั้งค่าขั้นสูง**และขยาย **กลไกตรวจหา** > **การป้องกันระบบไฟล์แบบเรียลไทม์** คลิก **พารามิเตอร์ ThreatSense**> **อื่น ๆ** แล้วเลือกหรือไม่เลือก **เปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท**

ระดับการกำจัด

หากต้องการเข้าถึงการตั้งค่าระดับการกำจัดสำหรับโมดูลการป้องกันที่ต้องการ ให้ขยาย **พารามิเตอร์ ThreatSense** (ตัวอย่างเช่น **การป้องกันระบบไฟล์แบบเรียลไทม์**) จากนั้นคลิก **การกำจัด > ระดับการกำจัด**

พารามิเตอร์ของ ThreatSense มีระดับการปรับปรุงแก้ไข (เช่น การกำจัด) ดังต่อไปนี้

การปรับปรุงแก้ไขใน ESET Smart Security Premium

ระดับการกำจัด	คำอธิบาย
แก้ไขการตรวจหาเสมอ	ให้พยายามปรับปรุงแก้ไขการตรวจหาขณะล้างวัตถุโดยไม่มีการแทรกแซงจากผู้ใช้ปลายทาง ในบางกรณีที่เกิดได้ยาก (ตัวอย่างเช่น ไฟล์ระบบ) หากการตรวจหาไม่สามารถปรับปรุงแก้ไขได้ วัตถุที่รายงานจะถูกทิ้งไว้ในตำแหน่งเดิม แนะนำให้ตั้ง
ปรับปรุงแก้ไขการตรวจหาว่าปลอดภัยหรือไม่ นอกเหนือจากนั้นให้เก็บไว้	การพยายามปรับปรุงแก้ไขการตรวจหาขณะกำจัดวัตถุโดยไม่มีการแทรกแซงจากผู้ใช้ปลายทาง ในบางกรณี (ตัวอย่างเช่น ไฟล์ระบบหรือไฟล์เก็บถาวร ที่มีทั้งไฟล์ที่ไม่ติดและติดไวรัส) หากการตรวจหาไม่สามารถปรับปรุงแก้ไขได้ วัตถุที่รายงานจะถูกทิ้งไว้ในตำแหน่งเดิม
ปรับปรุงแก้ไขการตรวจหาว่าปลอดภัยหรือไม่ นอกเหนือจากนั้นให้ถาม	การพยายามแก้ไขการตรวจหาขณะล้างวัตถุ ในบางกรณี หากไม่มีการกระทำใดสามารถทำได้ ผู้ใช้ปลายทางจะได้รับหน้าต่างโต้ตอบและต้องเลือกการดำเนินการรุการปรับปรุงแก้ไข (ตัวอย่างเช่น ลบ หรือ เพิกเฉย) แนะนำให้ใช้การตั้งค่านี้ในกรณีทั่วไป
ถามผู้ใช้ปลายทางเสมอ	ผู้ใช้ปลายทางจะได้รับหน้าต่างโต้ตอบขณะล้างวัตถุและต้องเลือกการดำเนินการการปรับปรุงแก้ไข (ตัวอย่างเช่น ลบ หรือ เพิกเฉย) ระดับนี้ได้รับการออกแบบสำหรับผู้ใช้ขั้นสูงขึ้นซึ่งรู้ว่าควรใช้วิธีใดเมื่อมีการตรวจหา

เมื่อใดควรแก้ไขการกำหนดค่าการป้องกันแบบเรียลไทม์

การป้องกันแบบเรียลไทม์เป็นองค์ประกอบที่สำคัญที่สุดในการรักษาระบบที่ปลอดภัย โปรดระมัดระวังเมื่อแก้ไขพารามิเตอร์ทุกครั้ง เราขอแนะนำให้คุณแก้ไขพารามิเตอร์ในกรณีพิเศษเท่านั้น

หลังจากการติดตั้ง ESET Smart Security Premium การตั้งค่าทั้งหมดจะได้รับการเพิ่มประสิทธิภาพเพื่อให้การรักษาความปลอดภัยให้กับระบบในระดับสูงสุดสำหรับผู้ใช้ หากต้องการเรียกคืนการตั้งค่าเริ่มต้น ให้คลิก ↩ ถัดจากแต่ละแท็บในหน้าต่าง (**การตั้งค่าขั้นสูง** > **กลไกตรวจหา** > **การป้องกันระบบไฟล์แบบเรียลไทม์**)

การตรวจสอบการป้องกันแบบเรียลไทม์

เมื่อต้องการตรวจสอบว่าการป้องกันแบบเรียลไทม์กำลังทำงานและตรวจหาไวรัส ให้ใช้ไฟล์ทดสอบจาก *www.eicar.com* ไฟล์ทดสอบนี้เป็นไฟล์ที่ปลอดภัยซึ่งสามารถตรวจพบโดยโปรแกรมป้องกันไวรัสทุกประเภท ไฟล์นี้สร้างขึ้นโดยบริษัท 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 **การป้องกันคอมพิวเตอร์** > **การป้องกันระบบไฟล์แบบเรียลไทม์**

ากการป้องกันแบบเรียลไทม์ไม่สามารถเริ่มต้นเมื่อระบบเริ่มต้น เป็นไปได้ว่าอาจเกิดจากการปิดใช้งานตัวเลือก **เปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์** หากต้องการทำให้แน่ใจว่าตัวเลือกนี้เปิดใช้งานอยู่ ให้ไปที่ **การตั้งค่าขั้นสูง (F5)** แล้วคลิก **กลไกตรวจหา** > **การป้องกันระบบไฟล์แบบเรียลไทม์**

ถ้าการป้องกันแบบเรียลไทม์ไม่พบหรือไม่กำจัดการแฝงตัว

ตรวจสอบว่าไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอื่นในคอมพิวเตอร์ของคุณ หากโปรแกรมป้องกันไวรัสสองโปรแกรมถูกติดตั้งในเวลาเดียวกัน อาจเกิดความขัดแย้งขึ้นได้ ขอแนะนำให้คุณลบการติดตั้งโปรแกรมป้องกันไวรัสอื่นในระบบของคุณก่อนติดตั้ง ESET

การป้องกันแบบเรียลไทม์ไม่เริ่มต้นทำงาน

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

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*)

คุณสามารถเพิ่มไฟล์ที่สามารถยกเว้นได้ในรายการของกระบวนการที่ได้รับการยกเว้นผ่าน **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจหา** > **การป้องกันระบบไฟล์แบบเรียลไทม์** > **กระบวนการการยกเว้น**

คุณลักษณะนี้ได้รับการออกแบบมาเพื่อแยกเครื่องมือการสำรองข้อมูล การยกเว้นกระบวนการของเครื่องมือสำรองข้อมูลจากการสแกนจะไม่ใช่เพียงทำให้มั่นใจเรื่องความมั่นคงของระบบเท่านั้น แต่ยังจะไม่มีผลกระทบต่อประสิทธิภาพของการสำรองข้อมูล ซึ่งการสำรองจะไม่ทำงานช้าลงในขณะที่กำลังใช้งานอยู่

คลิก **แก้ไข** เพื่อเปิดหน้าต่างการจัดการ **ข้อยกเว้นของกระบวนการ** ที่คุณสามารถ เพิ่มข้อยกเว้นต่างๆ และเรียกใช้ไฟล์ที่สามารถยกเว้นได้ (ตัวอย่างเช่น *Backup-tool.exe*) ซึ่งจะแยกออกจากการสแกน เมื่อไฟล์ *.exe* ถูกเพิ่มไปยังข้อยกเว้นแล้ว กิจกรรมของกระบวนการนี้จะไม่ใช่ได้รับการตรวจสอบโดย ESET Smart Security Premium 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... (ตัวอย่างเช่น C:\Program Files\Firefox\Firefox.exe) อย่าป้อนชื่อของแอพพลิเคชัน
เมื่อไฟล์ *.exe* ถูกเพิ่มไปยังข้อยกเว้นแล้ว กิจกรรมของกระบวนการนี้จะไม่ใช่ได้รับการตรวจสอบโดย ESET Smart Security Premium และจะไม่มีการสแกนเพื่อทำงานบนการปฏิบัติการของไฟล์ใดที่ดำเนินการโดยกระบวนการนี้

หากคุณไม่ใช้ฟังก์ชันเรียกดูเมื่อเลือกกระบวนการที่สามารถยกเว้นได้ คุณจำเป็นต้องป้อนพาธแบบเต็มให้เป็นแบบยกเว้นได้ด้วยตนเอง มิเช่นนั้น ข้อยกเว้นจะไม่ทำงานอย่างถูกต้องและ HIPS อาจรายงานข้อผิดพลาด

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

การป้องกันแบบคลาวด์

ESET LiveGrid® (สร้างจากระบบการเตือนล่วงหน้าขั้นสูง ESET ThreatSense.Net) จะใช้ข้อมูลที่ผู้ใช้ ESET ส่งมาจากทั่วโลกและส่งข้อมูลไปยัง ESET Research Lab ด้วยการให้ตัวอย่างที่น่าสงสัยและเมตาดาต้า ESET LiveGrid® ทำให้เราสามารถตอบสนองความต้องการของลูกค้าได้ทันทีและทำให้ ESET สามารถโต้ตอบภัยคุกคามล่าสุดได้อยู่เสมอ

ESET LiveGuard เป็นคุณลักษณะที่จะช่วยเพิ่มชั้นการป้องกันซึ่งได้รับการออกแบบมาเป็นการเฉพาะเพื่อลดผลกระทบจากภัยคุกคามที่ไม่เคยพบมาก่อน เมื่อเปิดใช้งาน ตัวอย่างที่น่าสงสัยที่ยังไม่ได้รับการยืนยันว่าเป็นรายการที่เป็นอันตรายและอาจมีมัลแวร์จะถูกส่งไปที่คลาวด์ของ ESET โดยอัตโนมัติ

ตัวเลือกที่ใช้ได้มีดังนี้:

เปิดใช้งานระบบความเชื่อถือของ ESET LiveGrid®, ระบบคำติชมของ ESET LiveGrid® และ ESET LiveGuard

ระบบความเชื่อของ ESET LiveGrid® ให้บัญชีปลอดภัยและบัญชีดำในระบบคลาวด์ โดยระบบคำติชมของ ESET LiveGrid® จะเก็บข้อมูลเกี่ยวกับคอมพิวเตอร์ของคุณที่เกี่ยวข้องกับภัยคุกคามที่ตรวจพบใหม่ คุณลักษณะ ESET LiveGuard จะตรวจหาภัยคุกคามใหม่ๆ ซึ่งไม่เคยเห็นมาก่อนด้วยการวิเคราะห์พฤติกรรมของภัยคุกคามเหล่านั้นใน

ตรวจสอบความเชื่อถือของกระบวนการที่ทำงานอยู่และไฟล์ได้โดยตรงจากส่วนติดต่อของโปรแกรมหรือเมนูบริบทที่มีข้อมูลเพิ่มเติมจาก ESET LiveGrid® เมื่อใช้ระบบป้องกันของ ESET LiveGuard ไฟล์ใหม่ต่างๆ จะถูกปิดกั้นไม่ให้ทำงานจนกว่าจะได้รับผลลัพธ์การวิเคราะห์

เปิดใช้งานระบบความเชื่อถือ ESET LiveGrid®

ระบบความเชื่อของ ESET LiveGrid® ให้บัญชีปลอดภัยและบัญชีดำในระบบคลาวด์

ตรวจสอบความเชื่อถือของกระบวนการที่ทำงานอยู่และไฟล์ได้โดยตรงจากส่วนติดต่อของโปรแกรมหรือเมนูบริบทที่มีข้อมูลเพิ่มเติมจาก ESET LiveGrid®

เปิดใช้งานระบบคำติชม ESET LiveGrid®

นอกจากระบบความเชื่อถือของ ESET LiveGrid® แล้ว ระบบคำติชมของ ESET LiveGrid® จะเก็บข้อมูลเกี่ยวกับคอมพิวเตอร์ของคุณที่เกี่ยวข้องกับภัยคุกคามที่ตรวจพบใหม่ โดยข้อมูลเหล่านี้อาจประกอบด้วย:

- ตัวอย่างหรือสำเนาของไฟล์ที่ภัยคุกคามปรากฏขึ้น
- พาธไปยังไฟล์
- ชื่อไฟล์:
- วันที่และเวลา
- กระบวนการที่ภัยคุกคามปรากฏบนคอมพิวเตอร์ของคุณ
- ข้อมูลเกี่ยวกับระบบปฏิบัติการของคอมพิวเตอร์ของคุณ

ตามค่าเริ่มต้น ESET Smart Security Premium จะได้รับการกำหนดค่าเพื่อส่งไฟล์ที่น่าสงสัยไปที่ห้องปฏิบัติการไวรัสของ ESET เพื่อวิเคราะห์โดยละเอียด ไฟล์ที่มีนามสกุลบางอย่าง เช่น *.doc* หรือ *.xls* จะถูกยกเว้นเสมอ นอกจากนี้คุณยังสามารถเพิ่มนามสกุลอื่นๆ ถ้ามีไฟล์ชนิดใดที่คุณหรือองค์กรของคุณไม่ต้องการส่ง

i อ่านเพิ่มเติมเกี่ยวกับการส่งข้อมูลที่เกี่ยวข้องใน นโยบายความเป็นส่วนตัว

คุณสามารถเลือกจะไม่เปิดใช้งาน ESET LiveGrid® ได้

คุณจะไม่สูญเสียฟังก์ชันการทำงานใดๆ ในซอฟต์แวร์ แต่ในบางกรณี ESET Smart Security Premium อาจสามารถตอบสนองต่อการคุกคามใหม่ได้เร็วขึ้นเมื่อคุณเปิดใช้งาน ESET LiveGrid® หากคุณเคยใช้ ESET LiveGrid® ก่อนหน้านี้และปิดใช้งานไปแล้ว อาจยังคงมีแพ็คเกจข้อมูลที่ต้องส่ง แม้ว่าจะปิดใช้งานแล้ว โปรแกรมจะส่งแพ็คเกจดังกล่าวไปยัง ESET เมื่อส่งข้อมูลปัจจุบันทั้งหมดแล้ว โปรแกรมจะไม่สร้างแพ็คเกจเพิ่มเติมอีก

i อ่านเพิ่มเติมเกี่ยวกับ ESET LiveGrid® ใน ประมวลศัพท์
โปรดดู คำแนะนำพร้อมภาพประกอบ ของเราซึ่งมีให้แบบภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษาเกี่ยวกับการเปิดหรือปิดใช้งาน ESET LiveGrid® ใน ESET Smart Security Premium

---

การกำหนดค่าการป้องกันแบบระบบคลาวด์ในการตั้งค่าขั้นสูง

หากต้องการเข้าถึงการตั้งค่าสำหรับ ESET LiveGrid® และ ESET LiveGuardให้เปิด **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจจับ** > **การป้องกันระบบคลาวด์**

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

• **เปิดใช้งานระบบคำติชม ESET LiveGrid®** – ส่งข้อมูลที่ส่งที่เกี่ยวข้อง (อธิบายในส่วน**การส่งตัวอย่าง**ด้านล่าง) พร้อมกับรายงานความผิดพลาดและสถิติไปยังห้องปฏิบัติการวิจัย ESET เพื่อวิเคราะห์เพิ่มเติม

• **เปิดใช้งาน ESET LiveGuard** – คุณลักษณะ ESET LiveGuard จะตรวจจับภัยคุกคามใหม่ๆ ซึ่งไม่เคยเห็นมาก่อนด้วยการวิเคราะห์พฤติกรรมของภัยคุกคามเหล่านั้นใน Sandbox คุณสามารถเปิดใช้งาน ESET LiveGuard ได้เมื่อได้เมื่อเปิดใช้งาน ESET LiveGrid® ไว้เท่านั้น

• **ส่งรายงานความล้มเหลวและข้อมูลการวินิจฉัย** – ส่งข้อมูลการวินิจฉัยที่เกี่ยวข้องของ ESET LiveGrid® เช่น รายงานความผิดพลาดและโมดูลดัมพ์หน่วยความจำ เราขอแนะนำให้เปิดใช้งานสิ่งนี้ไว้เพื่อช่วยให้ ESET วินิจฉัยปัญหา ปรับปรุงผลิตภัณฑ์และปกป้องผู้ใช้ปลายทางได้ดียิ่งขึ้น

• **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 เพื่อการวิเคราะห์และเพื่อปรับปรุงการตรวจหา (ขนาดสูงสุดของตัวอย่างตามค่าเริ่มต้นคือ 64MB) ในอนาคต ตัวเลือกที่ใช้ได้มีดังนี้:

• **ตัวอย่างไฟล์ที่ตรวจพบทั้งหมด** – วัตถุ ทั้งหมดตรวจจับโดย กลไกการตรวจจับ (ซึ่งรวมถึงแอพพลิเคชั่นที่อาจไม่พึงประสงค์เมื่อเปิดใช้งานในการตั้งค่าเครื่องมือสแกน)

• **ตัวอย่างไฟล์ทั้งหมดยกเว้นเอกสาร** – วัตถุต่างๆ ที่ตรวจพบทั้งหมดยกเว้น **เอกสาร** (ดูด้านล่าง)

• **ไม่ส่ง** – วัตถุต่างๆ ที่ตรวจพบจะไม่ส่งไปยัง ESET

ส่งตัวอย่างที่น่าสงสัยโดยอัตโนมัติ

ตัวอย่างเหล่านี้จะถูกส่งไปยัง ESET ในกรณีที่กลไกการตรวจจับตรวจไม่พบ ตัวอย่างเช่น ตัวอย่างที่เกือบจะพลาดการตรวจหาหรือหนึ่งใน โมดูลการป้องกัน ของ ESET Smart Security Premium พิจารณาตัวอย่างเหล่านี้ว่าน่าสงสัยหรือมีพฤติกรรมที่ไม่ชัดเจน (ขนาดสูงสุดของตัวอย่างตามค่าเริ่มต้นคือ 64 MB)

• **ไฟล์ที่เปิดใช้งานได้** – รวมถึงไฟล์ที่เปิดใช้งานได้ เช่น .exe, .dll, .sys

• **อาร์ไคฟ์** – รวมถึงประเภทไฟล์อาร์ไคฟ์ เช่น .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab

• **สคริปต์** – รวมถึงประเภทไฟล์สคริปต์ เช่น .bat, .cmd, .hta, .js, .vbs, .ps1

• **อื่นๆ** – รวมถึงประเภทไฟล์ เช่น .jar, .reg, .msi, .sfw, .lnk

• **อีเมลสแปมที่เป็นไปได้** – วิธีนี้จะช่วยในการส่งสแปมส่วนต่างๆ ที่เป็นไปได้ หรืออีเมลสแปมที่เป็นไปได้ทั้งหมดพร้อมกับเอกสารแนบไปที่ ESET เพื่อวิเคราะห์ต่อไป การเปิดใช้งานตัวเลือกนี้จะช่วยปรับปรุงการตรวจหาสแปมโดยรวม รวมถึงการปรับปรุงการตรวจหาสแปมในอนาคตอีกด้วย

• **ลบไฟล์ที่เรียกใช้ได้ อาร์ไคฟ์ สคริปต์ ตัวอย่างอื่นๆ และอีเมลที่อาจเป็นสแปมออกจากเซิร์ฟเวอร์ของ ESET** – กำหนดเวลาลบตัวอย่างหรือส่งไปรับการวิเคราะห์โดย ESET LiveGuard

• **เอกสาร** – รวมถึงเอกสาร Microsoft Office หรือ PDF ที่มีหรือไม่มีเนื้อหาที่กำลังใช้งานอยู่

• **ลบเอกสารออกจากเซิร์ฟเวอร์ของ ESET** – กำหนดเวลาลบเอกสารที่ส่งไปรับการวิเคราะห์โดย ESET LiveGuard

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** > **กลไกการตรวจจับ** > **การป้องกันแบบระบบคลาวด์** > **การส่งตัวอย่าง** แล้วคลิก **แก้ไข** ถัดจาก **การยกเว้น** เพิ่มการยกเว้น `download.domain.com`

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

ESET LiveGuard

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*

ESET LiveGuard

ESET LiveGuard เป็นคุณลักษณะที่จะช่วยเพิ่มชั้นการป้องกันแบบคลาวด์ซึ่งได้รับการออกแบบมาเป็นการเฉพาะเพื่อลดผลกระทบจากภัยคุกคามที่ไม่เคยพบมาก่อน

เมื่อเปิดใช้งาน ตัวอย่างที่น่าสงสัยที่ยังไม่ได้รับการยืนยันว่าเป็นรายการที่เป็นอันตรายและอาจมีมัลแวร์จะถูกส่งไปที่คลาวด์ของ ESET โดยอัตโนมัติ ซึ่งตัวอย่างที่ส่งจะถูกเรียกใช้ใน Sandbox และได้รับการประเมินโดยเครื่องมือตรวจจับมัลแวร์ขั้นสูงของเรา โดยตัวอย่างที่เป็นอันตรายหรืออีเมลสแปมที่น่าสงสัยจะถูกส่งไปยัง ESET LiveGrid® ไฟล์แนบอีเมลจะถูกจัดการแยกต่างหากและอาจมีการส่งไปยัง ESET LiveGuard คุณสามารถ กำหนดขอบเขตของไฟล์ที่ส่งและระยะเวลาการเก็บรักษาไฟล์ในระบบคลาวด์ของ ESET ได้ โดยตามค่าเริ่มต้นเอกสารและไฟล์ PDF ที่มีเนื้อหาที่ใช้งานอยู่ (macros, javascript) จะไม่ถูกส่ง

ESET LiveGuard สามารถเปิดใช้งานหรือปิดใช้งานได้ใน:

- หน้าต่างโปรแกรมหลัก > **การตั้งค่า การป้องกันคอมพิวเตอร์**
- **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจจับ** > **การป้องกันระบบคลาวด์**

เพื่อเข้าถึงการตั้งค่าขั้นสูงสำหรับ ESET LiveGuard ให้เปิด **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจจับ** > **การป้องกันระบบคลาวด์** > **ESET LiveGuard**

- **การดำเนินการหลังตรวจพบ** – เลือกการกระทำที่ต้องการให้ดำเนินการหลังจากวิเคราะห์ตัวอย่างแล้วและประเมินว่าเป็นภัยคุกคาม
- **การป้องกันเชิงรุก** – อนุญาตหรือปิดกั้นการทำงานของไฟล์ที่ ESET LiveGuard วิเคราะห์

หากคุณตั้งค่าการป้องกันเชิงรุกเป็น **ปิดกั้นการทำงานจนกว่าจะได้รับผลการวิเคราะห์** และคุณต้องการยกเลิกปิดกั้นไฟล์ที่กำลังอยู่ระหว่างการวิเคราะห์ ให้คลิกขวาที่ไฟล์แล้วคลิก **ยกเลิกการปิดกั้นไฟล์ที่ ESET LiveGuard กำลังวิเคราะห์**

- **ระยะเวลารอสูงสุดสำหรับผลการวิเคราะห์ (นาที)** – กำหนดเวลาให้ระบบยกเลิกการปิดกั้นไฟล์ที่กำลังอยู่ระหว่างการวิเคราะห์ไม่ว่าการวิเคราะห์จะเสร็จสมบูรณ์หรือไม่

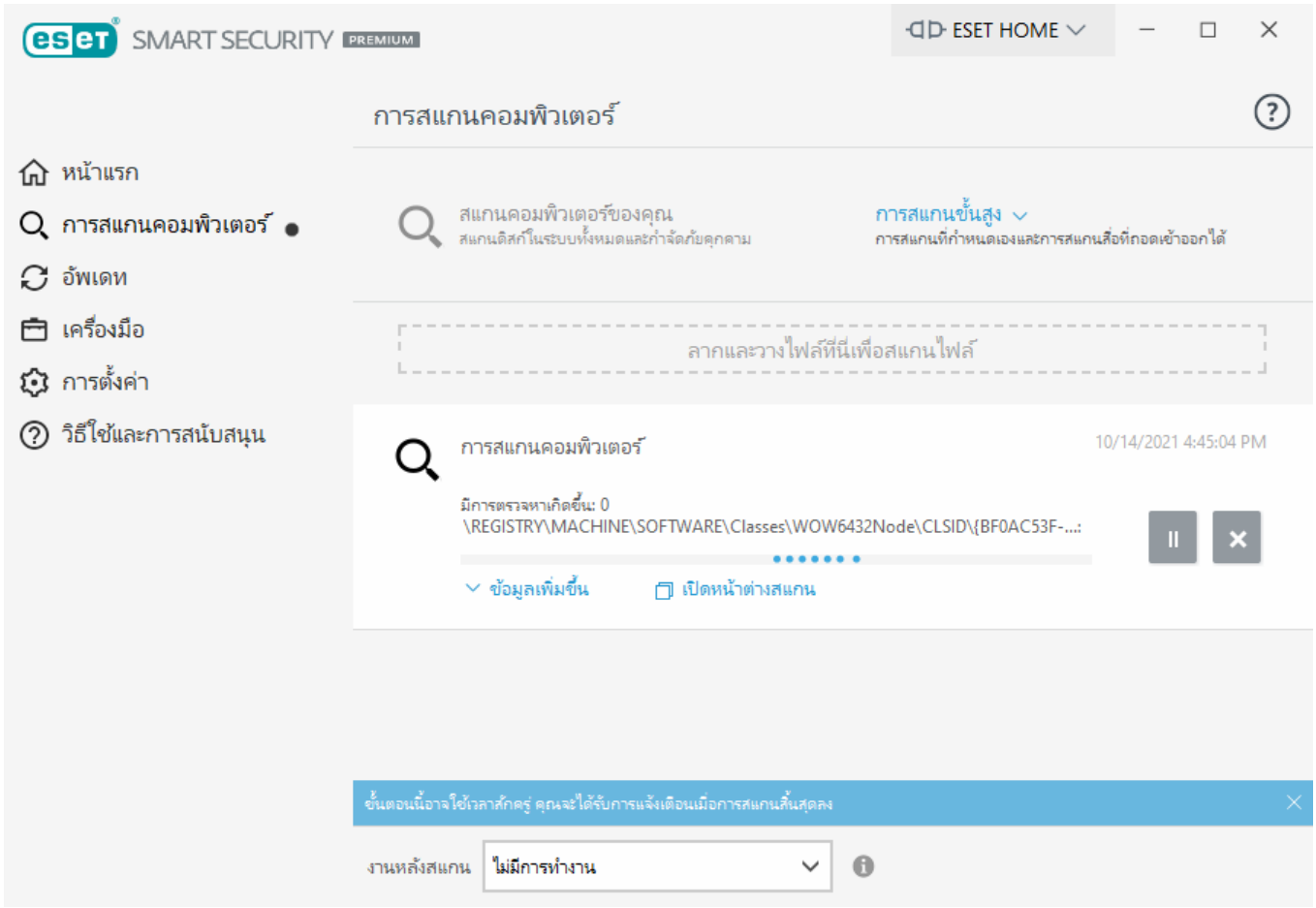
ESET LiveGuard จะแจ้งให้คุณทราบเกี่ยวกับสถานะการวิเคราะห์ โดยคุณสามารถดูการแจ้งเตือนที่มีด้านล่าง:

ชื่อการแจ้งเตือน	คำอธิบาย
ไฟล์ถูกปิดกั้นเนื่องจากกำลังอยู่ระหว่างการวิเคราะห์	ไฟล์นี้ถูกปิดกั้นโดย ESET LiveGuard เนื่องจาก ESET LiveGuard กำลังวิเคราะห์ไฟล์เพื่อให้แน่ใจว่าคุณจะสามารถใช้งานได้อย่างปลอดภัย คุณสามารถรอหรือเลือกตัวเลือกต่อไปนี้ได้: • **ยกเลิกการปิดกั้นไฟล์** – ยกเลิกการปิดกั้นแต่ ดำเนินการวิเคราะห์ต่อไป โดยคุณจะได้รับการแจ้งเตือนเกี่ยวกับผลลัพธ์ เราไม่แนะนำให้ใช้การดำเนินการนี้หากคุณไม่แน่ใจในความน่าเชื่อถือของไฟล์ • **เปลี่ยนการตั้งค่า** – เปิดหน้าต่างตั้งค่าการป้องกันคอมพิวเตอร์ซึ่งคุณสามารถปิดใช้งาน ESET LiveGuard และระบบการป้องกันเชิงรุกได้
ไฟล์ที่ยกเลิกการปิดกั้น	ระบบจะไม่ปิดกั้นไฟล์อีกต่อไป โดยการวิเคราะห์จะดำเนินการต่อและคุณจะได้รับการแจ้งเตือนเกี่ยวกับผลลัพธ์ และคุณสามารถเปิดไฟล์นี้ได้
ไฟล์กำลังอยู่ระหว่างการวิเคราะห์	ESET LiveGuard ต้องใช้เวลามากขึ้นในการวิเคราะห์ให้เสร็จสมบูรณ์ คุณสามารถเปิดไฟล์ได้หากจำเป็น
ลบภัยคุกคามออกแล้ว	ESET LiveGuard ได้ทำการวิเคราะห์เสร็จสมบูรณ์แล้วและไฟล์นี้มีภัยคุกคาม ไฟล์ถูกทำความสะอาดแล้ว
ไฟล์ปลอดภัยสามารถใช้ได้	ESET LiveGuard ได้เสร็จสิ้นการวิเคราะห์และไฟล์มีความปลอดภัยในการใช้งาน

หาก ESET LiveGuard ทำงานไม่ถูกต้อง คุณจะได้รับสถานะแอพพลิเคชันใน หน้าต่างโปรแกรมหลัก > แท็บ **หน้าแรก** ทำตามคำแนะนำในสถานะแอพพลิเคชันเพื่อแก้ไขปัญหา หากคุณไม่สามารถแก้ไขปัญหาได้ ให้ติดต่อฝ่ายสนับสนุนด้านเทคนิค

การสแกนคอมพิวเตอร์

เครื่องมือสแกนตามต้องการเป็นส่วนสำคัญของโซลูชันป้องกันไวรัส ซึ่งใช้เพื่อสแกนไฟล์และโฟลเดอร์ในคอมพิวเตอร์ของคุณ เมื่อพิจารณาถึงแง่ของความปลอดภัย การสแกนคอมพิวเตอร์ไม่ควรดำเนินการเฉพาะเวลาที่สงสัยว่ามีการติดไวรัสเท่านั้น แต่ควรดำเนินการอย่างสม่ำเสมอให้เป็นส่วนหนึ่งของมาตรการรักษาความปลอดภัย ขอแนะนำให้คุณสแกนข้อมูลของระบบโดยละเอียดเป็นประจำเพื่อตรวจหาไวรัส ซึ่งไม่พบโดย การป้องกันระบบไฟล์แบบเรียลไทม์ เมื่อเขียนลงในดิสก์ กรณีนี้สามารถเกิดขึ้นได้ถ้าการป้องกันระบบไฟล์แบบเรียลไทม์ถูกปิดใช้งานในขณะนี้ กลไกตรวจหาเก่าเกินไป หรือไฟล์ไม่ถูกตรวจพบว่าเป็นไวรัสเมื่อบันทึกลงในดิสก์



มี **การสแกนคอมพิวเตอร์** สองประเภท **สแกนคอมพิวเตอร์ของคุณ** จะสแกนระบบอย่างรวดเร็วโดยไม่ระบุค่าพารามิเตอร์การสแกน **การสแกนที่กำหนดเอง** (ภายใต้ การสแกนขั้นสูง) จะทำให้คุณสามารถเลือกโปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้า ซึ่งออกแบบมาเพื่อกำหนดตำแหน่งและเลือกเป้าหมายการสแกนอย่างเจาะจง

โปรดดู ความคืบหน้าของการสแกน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับกระบวนการสแกน

โดยค่าเริ่มต้น ESET Smart Security Premium จะพยายามทำความสะอาดหรือลบการตรวจหาที่พบในระหว่างการสแกนคอมพิวเตอร์โดยอัตโนมัติ ในบางกรณี หากไม่มีการกระทำใดสามารถทำได้ ผู้ใช้ปลายทางจะได้รับหน้าต่างโต้ตอบและต้องเลือกการดำเนินการทำความสะอาด (ตัวอย่างเช่น ลบ หรือ เพิกเฉย) หากต้องการเปลี่ยนแปลงระดับการทำความสะอาดและสำหรับข้อมูลแบบละเอียด โปรดดู การทำความสะอาด หากต้องการตรวจสอบการสแกนครั้งก่อนหน้า โปรดดู ไฟล์บันทึก

สแกนคอมพิวเตอร์

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

อาด

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

ตัวเลือกในการสแกนต่อไปนี้มีให้ใช้ที่ใต้ **การสแกนขั้นสูง**:

การสแกนที่กำหนดเอง

การสแกนที่กำหนดเองช่วยให้คุณสามารถระบุพารามิเตอร์การสแกน เช่น เป้าหมายและวิธีการสแกนได้ 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
- **เริ่มต้นระบบใหม่** – ปิดโปรแกรมที่เปิดอยู่ทั้งหมด แล้วเริ่มต้นคอมพิวเตอร์ใหม่หลังจากสแกนเสร็จสิ้น
- **เริ่มต้นระบบใหม่หากจำเป็น** – คอมพิวเตอร์จะเริ่มต้นใหม่หากจำเป็นเพื่อทำความสะอาดภัยคุกคามที่

ตรวจพบเท่านั้น

• **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

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

> i เราขอแนะนำให้คุณเรียกใช้การสแกนคอมพิวเตอร์อย่างน้อยเดือนละหนึ่งครั้ง การสแกนสามารถกำหนดค่าเป็นงานตามกำหนดการได้จาก **เครื่องมือ** > **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** (F5) > **กลไกตรวจหา** >

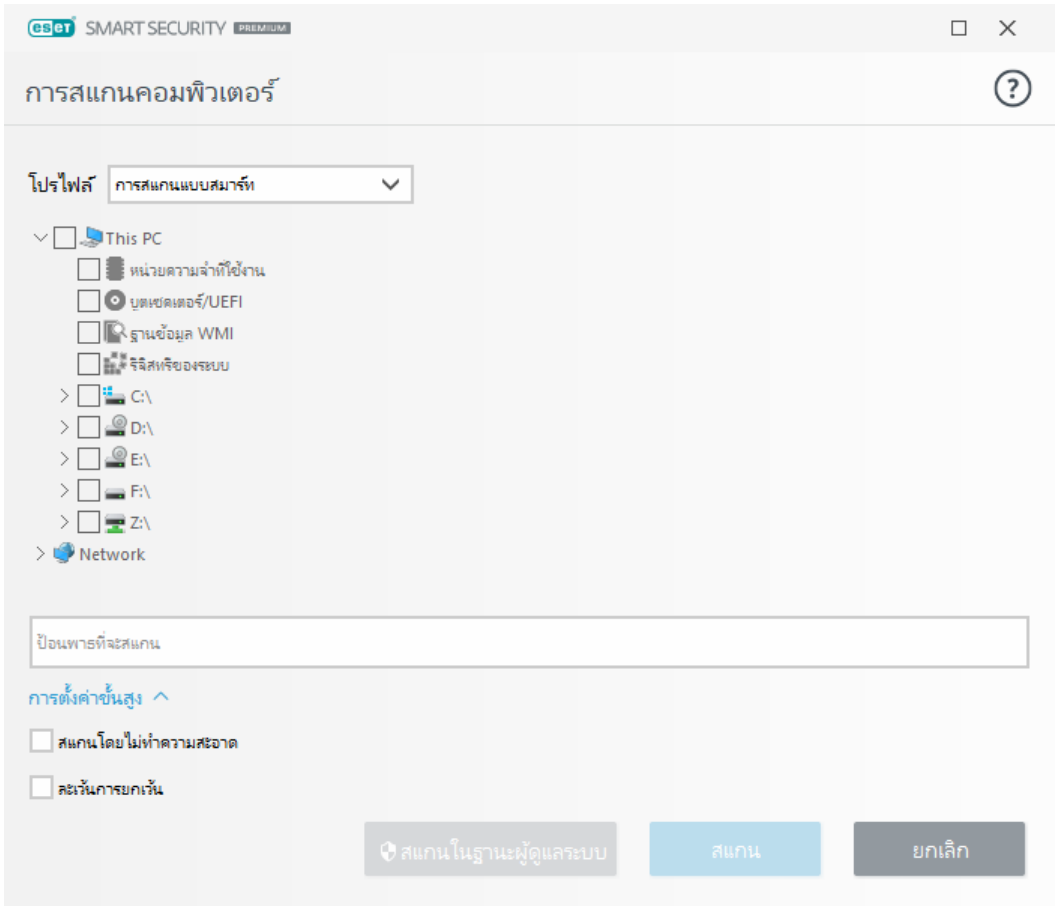
การสแกนมัลแวร์ > **การสแกนตามต้องการ** > พารามิเตอร์ ThreatSense

โครงสร้างโฟลเดอร์ (แบบต้นไม้) ยังมีเป้าหมายการสแกนที่เฉพาะเจาะจงอีกด้วย

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

หากต้องการไปยังเป้าหมายการสแกน (ไฟล์หรือโฟลเดอร์) อย่างรวดเร็ว ให้พิมพ์พาธของเป้าหมายดังกล่าวลงในช่องข้อความใต้ลำดับโครงสร้าง พาธต้องตรงตามตัวพิมพ์เล็กและใหญ่ โปรดเลือกกล่องกาเครื่องหมายในลำดับโครงสร้างหากต้องการให้ระบบสแกนเป้าหมายด้วย

> **วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์**
> หากต้องการกำหนดตารางงานทั่วไป ให้อ่านบท วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์



คุณสามารถกำหนดค่าพารามิเตอร์การทำความสะอาดสำหรับการสแกนภายใต้ **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจจับ** > **การสแกนตามต้องการ** > **ThreatSense พารามิเตอร์** > **การทำความสะอาด** ได้ หากต้องการเรียกใช้การสแกนโดยไม่ทำความสะอาด 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) คุณสามารถดูรายละเอียดเพิ่มเติมได้ใน บทความฐานความรู้ ของเรา

วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์
หากต้องการกำหนดตารางงานทั่วไป ให้อ่านบท วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์

ความคืบหน้าของการสแกน – แถบความคืบหน้าจะแสดงสถานะของวัตถุที่สแกนเสร็จแล้ว โดยเปรียบเทียบกับวัตถุที่รอสแกนอยู่ สถานะความคืบหน้าของการสแกนจะได้มาจากจำนวนวัตถุทั้งหมดที่รวมอยู่ในการสแกน

เป้าหมาย – ชื่อของวัตถุที่สแกนและตำแหน่งของวัตถุในปัจจุบัน

พบภัยคุกคาม - แสดงจำนวนทั้งหมดของไฟล์ที่สแกน ภัยคุกคามที่พบ และภัยคุกคามที่กำจัดระหว่างการสแกน

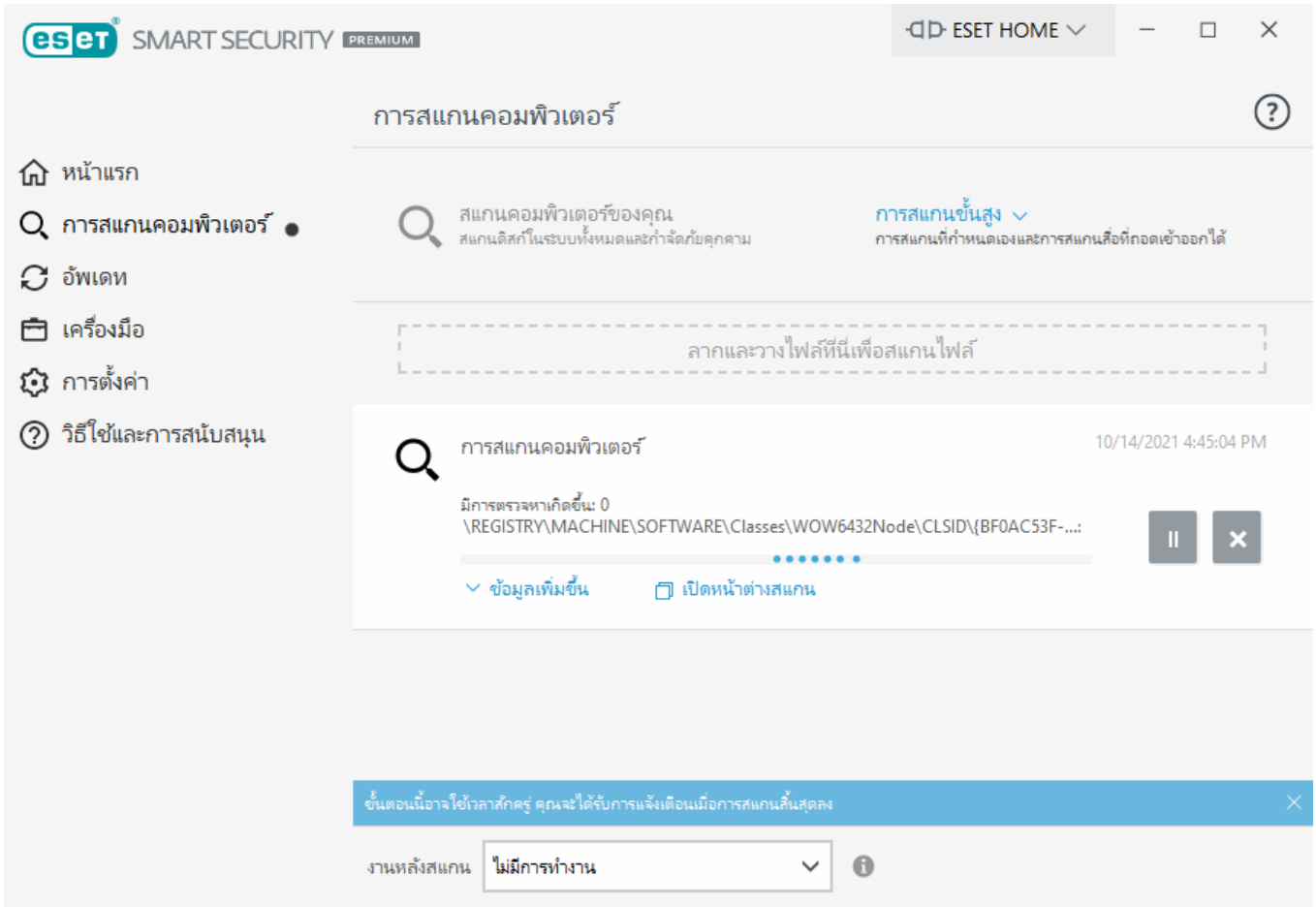
หยุดชั่วคราว – หยุดการสแกนชั่วคราว

ทำงานต่อ – ตัวเลือกนี้จะปรากฏขึ้นเมื่อหยุดความคืบหน้าของการสแกนไว้ชั่วคราว คลิกที่ **ทำงานต่อ** เพื่อเริ่มสแกนต่อ

หยุด – สิ้นสุดการสแกน

เลื่อนบันทึกการสแกน – ถ้าเปิดใช้งานตัวเลือกนี้ บันทึกการสแกนจะเลื่อนลงโดยอัตโนมัติเมื่อมีการเพิ่มรายการใหม่เพื่อให้รายการล่าสุดปรากฏขึ้น

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



เมนูแบบเลื่อนลง **การทำงานหลังสแกน** ทำให้คุณสามารถตั้งค่าการทำงานที่จะดำเนินการโดยอัตโนมัติหลังจากการสแกนเสร็จสิ้นได้:

• **ไม่มีการทำงาน** – หลังจากสแกนเสร็จสิ้น จะไม่มีการดำเนินการใดๆ

• **ปิดระบบ** – คอมพิวเตอร์จะปิดหลังจากสแกนเสร็จสิ้น

• **เริ่มต้นระบบใหม่** – ปิดโปรแกรมที่เปิดอยู่ทั้งหมด แล้วเริ่มต้นคอมพิวเตอร์ใหม่หลังจากสแกนเสร็จสิ้น

• **เริ่มต้นระบบใหม่หากจำเป็น** – คอมพิวเตอร์จะเริ่มต้นใหม่หากจำเป็นเพื่อทำความสะอาดภัยคุกคามที่ตรวจพบเท่านั้น

• **บังคับให้รีบูต** – บังคับให้ปิดโปรแกรมที่เปิดอยู่ทั้งหมดโดยไม่ต้องรอการโต้ตอบของผู้ใช้และรีสตาร์ทคอมพิวเตอร์หลังจากการสแกนเสร็จสิ้น

• **บังคับให้รีบูตเครื่องหากจำเป็น** – คอมพิวเตอร์จะเริ่มต้นใหม่หากจำเป็นเพื่อทำความสะอาดภัยคุกคามที่ตรวจพบเท่านั้น

• **พักเครื่อง** – บันทึกเซสชันของคุณและปรับคอมพิวเตอร์เข้าสู่สถานะการใช้พลังงานต่ำเพื่อให้คุณสามารถ

กลับมาทำงานต่อได้อย่างรวดเร็ว

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

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

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

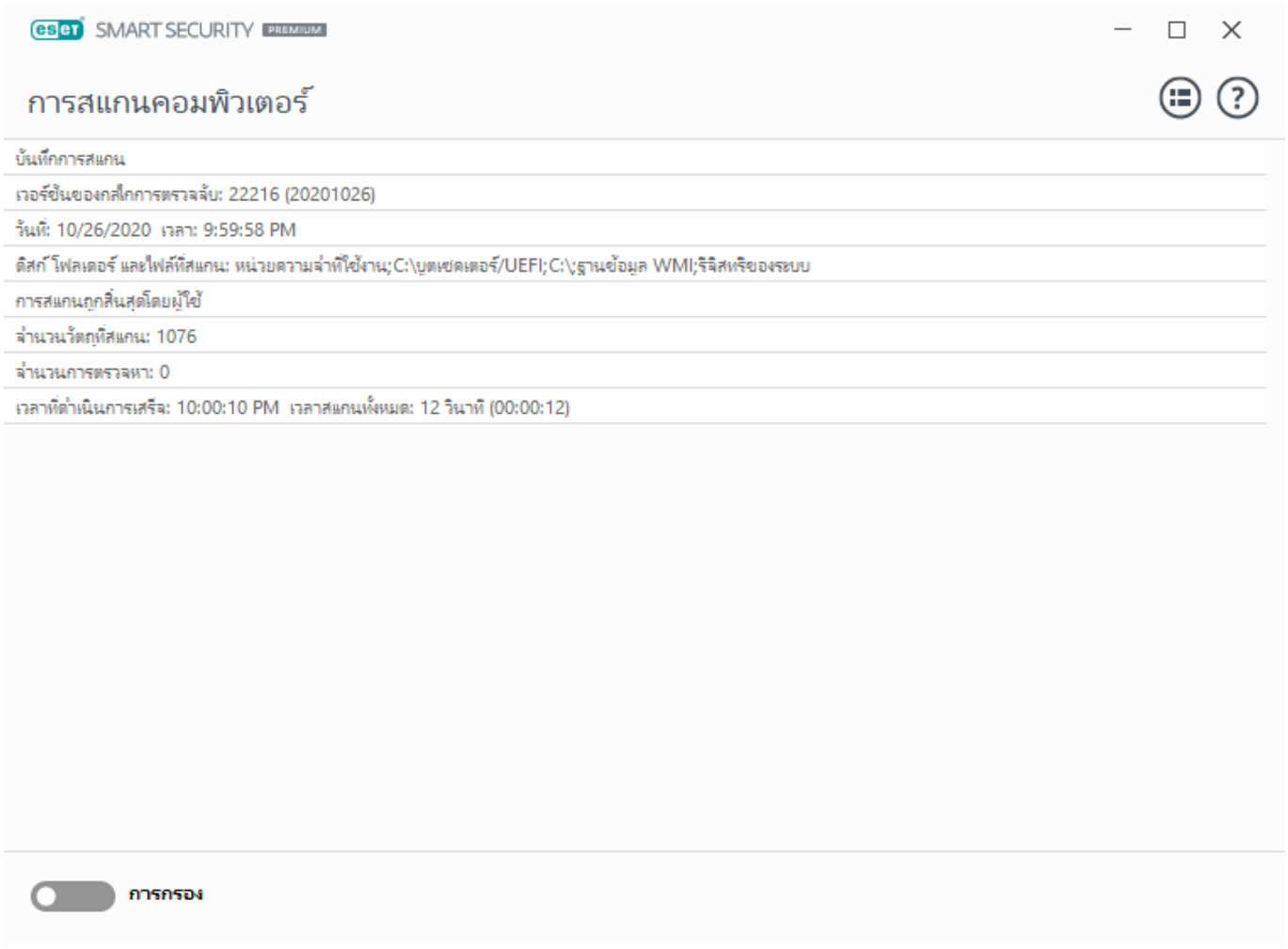
บันทึกการสแกนคอมพิวเตอร์

เมื่อการสแกนเสร็จสิ้น บันทึกการสแกนคอมพิวเตอร์ จะเปิดโดยมีข้อมูลที่เกี่ยวข้องทั้งหมดซึ่งเกี่ยวกับการสแกนนี้โดยเฉพาะ บันทึกการสแกนจะให้ข้อมูลต่างๆ แก่คุณ เช่น:

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

หากงานตามกำหนดการเดียวกันที่ถูกดำเนินการก่อนยังคงทำงานอยู่ การเริ่มต้นงานสแกนคอมพิวเตอร์ตามกำหนดการใหม่จะถูกข้าม งานสแกนตามกำหนดการที่ถูกข้ามไปจะสร้างบันทึกการสแกนคอมพิวเตอร์ที่มีวัตถุที่ถูกสแกน 0 รายการ พร้อมสถานะ **การสแกนไม่เริ่มต้นเนื่องจากการสแกนก่อนหน้านี้ยังคงทำงานอยู่**

ในการค้นหาบันทึกการสแกนก่อนหน้า ในหน้าต่างโปรแกรมหลัก ให้เลือก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก** ในเมนูแบบเลื่อนลง 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)

การทำงาน	การใช้งาน
คัดลอก	คัดลอกการบันทึกที่ไฮไลท์ไว้ลงในคลิปบอร์ด คำสั่งลัด: `Ctrl+C`
คัดลอกทั้งหมด	คัดลอกการบันทึกทั้งหมดไปยังหน้าต่าง
ส่งออก	ส่งการบันทึกที่ไฮไลท์ไว้ลงในคลิปบอร์ดออกไปยังไฟล์ XML
ส่งออกทั้งหมด	ตัวเลือกนี้จะส่งการบันทึกทั้งหมดออกไปยังไฟล์ XML
คำอธิบายการตรวจหา	เปิดสารานุกรมภัยคุกคามของ ESET ซึ่งมีข้อมูลโดยละเอียดเกี่ยวกับอันตรายและอาการของการแฝงตัวที่ทำไฮไลต์ไว้

การสแกนมัลแวร์

ส่วน**การสแกนมัลแวร์** สามารถเข้าถึงได้จาก **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจจับ** > **การสแกนมัลแวร์** และให้ตัวเลือกต่างๆ เพื่อเลือกการสแกนพารามิเตอร์ ส่วนนี้จะรวมถึงรายการต่อไปนี้:

โปรไฟล์ที่เลือก – ชุดพารามิเตอร์หนึ่งที่ใช้โดยเครื่องมือสแกนตามต้องการ เมื่อต้องการสร้างการสแกนใหม่ หากต้องการสร้างใหม่ ให้คลิก **แก้ไข** ถัดจาก **รายการของโปรไฟล์** ดู การสแกนโปรไฟล์ สำหรับรายละเอียดเพิ่มเติม

เป้าหมายการสแกน – หากต้องการสแกนเฉพาะเป้าหมายที่กำหนดเท่านั้น คุณสามารถคลิก **แก้ไข** ถัดจาก **เป้าหมายการสแกน** และเลือกตัวเลือกจากเมนูแบบเลื่อนลงหรือเลือกเป้าหมายที่กำหนดจากโครงสร้างโฟลเดอร์ ให้ดู เป้าหมายการสแกน สำหรับรายละเอียดเพิ่มเติม

พารามิเตอร์ThreatSense – ตัวเลือกการตั้งค่าขั้นสูงต่างๆ เช่น ข้อยกเว้นของไฟล์ที่คุณต้องการควบคุม วิธีการตรวจหาที่ใช้ เป็นต้น สามารถพบได้ในส่วนนี้ ให้คลิกเพื่อเปิดแท็บที่มีตัวเลือกขั้นสูง

การสแกนในสถานะไม่ใช้งาน

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

การสแกนในสถานะไม่ใช้งาน

เปิดใช้งานแถบเลื่อนที่อยู่ถัดจาก **เปิดใช้งานการสแกนในสถานะไม่ใช้งาน** เพื่อเปิดใช้งานคุณลักษณะนี้ เมื่อคอมพิวเตอร์อยู่ในสถานะที่ไม่ได้ใช้งาน การสแกนคอมพิวเตอร์แบบเงียบจะดำเนินการบนไดรฟ์ในระบบทั้งหมด

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

การตั้งค่าขั้นสูง

เปิดใช้งานแถบเลื่อนที่อยู่ถัดจาก **เปิดใช้งานการบันทึก** ในการตั้งค่าขั้นสูงเพื่อบันทึกผลการสแกนคอมพิวเตอร์ในส่วน ไฟล์บันทึก (จาก หน้าต่างโปรแกรมหลัก คลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก** แล้วเลือก **การสแกนคอมพิวเตอร์** จากเมนูแบบเลื่อนลง **บันทึก**)

การตรวจหาสภาวะไม่ใช้งาน

ดู การตรวจหาสภาวะไม่ใช้งาน สำหรับรายการแบบเต็มของเงื่อนไขที่จะต้องให้ตรง เพื่อเรียกใช้เครื่องเครื่องสแกนที่มีสถานะไม่ใช้งาน

คลิกการตั้งค่าพารามิเตอร์กลไก ThreatSense เพื่อแก้ไขพารามิเตอร์การสแกน (ตัวอย่างเช่น วิธีการตรวจหา) สำหรับเครื่องสแกนที่มีสถานะไม่ใช้งาน

โปรไฟล์การสแกน

โปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าใน ESET Smart Security Premium 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 ให้เปิดหน้าต่างการตั้งค่าขั้นสูง (F5) และคลิก **กลไกตรวจหา** > **การสแกนมัลแวร์** > **การสแกนตามต้องการ** > **รายการของโปรไฟล์** หน้าต่าง **ตัวจัดการโปรไฟล์** มีเมนูแบบเลื่อนลง **โปรไฟล์ที่เลือ**

ก ซึ่งแสดงโปรไฟล์การสแกนที่มีอยู่และตัวเลือกสำหรับสร้างโปรไฟล์ใหม่ เพื่อช่วยให้คุณสร้างโปรไฟล์การสแกนให้เหมาะสมกับความต้องการ โปรดไปที่ส่วน ThreatSenseการตั้งค่าพารามิเตอร์กลไก 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

การควบคุมอุปกรณ์

ESET Smart Security Premium ทำหน้าที่ในการควบคุมอุปกรณ์ (ซีดี/ดีวีดี/USB/...) โดยอัตโนมัติ โมดูลนี้จะช่วยให้คุณสามารถปิดกั้นหรือปรับตัวกรอง/สิทธิ์ที่ขยาย และกำหนดความสามารถของผู้ใช้ในการเข้าถึงและทำงานกับอุปกรณ์เหล่านี้ได้ คุณลักษณะนี้เป็นประโยชน์ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์ต้องการป้องกันไม่ให้ผู้ใช้ใช้งานอุปกรณ์ซึ่งมีเนื้อหาที่ไม่พึงประสงค์

อุปกรณ์ภายนอกที่สนับสนุน:

- พื้นที่เก็บข้อมูลดิสก์ (HDD, USB ดิสก์ที่ถอดเข้าออกได้)
- ซีดี/ดีวีดี
- USB เครื่องพิมพ์
- FireWireพื้นที่จัดเก็บข้อมูล
- Bluetooth อุปกรณ์
- เครื่องอ่านสมาร์ทการ์ด
- อุปกรณ์ภาพ
- โมเด็ม
- LPT/COM พอร์ต
- อุปกรณ์แบบพกพา
- อุปกรณ์ทุกประเภท

ตัวเลือกการตั้งค่าการควบคุมอุปกรณ์นั้นสามารถแก้ไขได้ใน **การตั้งค่าขั้นสูง** (F5) > **สื่อที่ถอดเข้าออกได้**

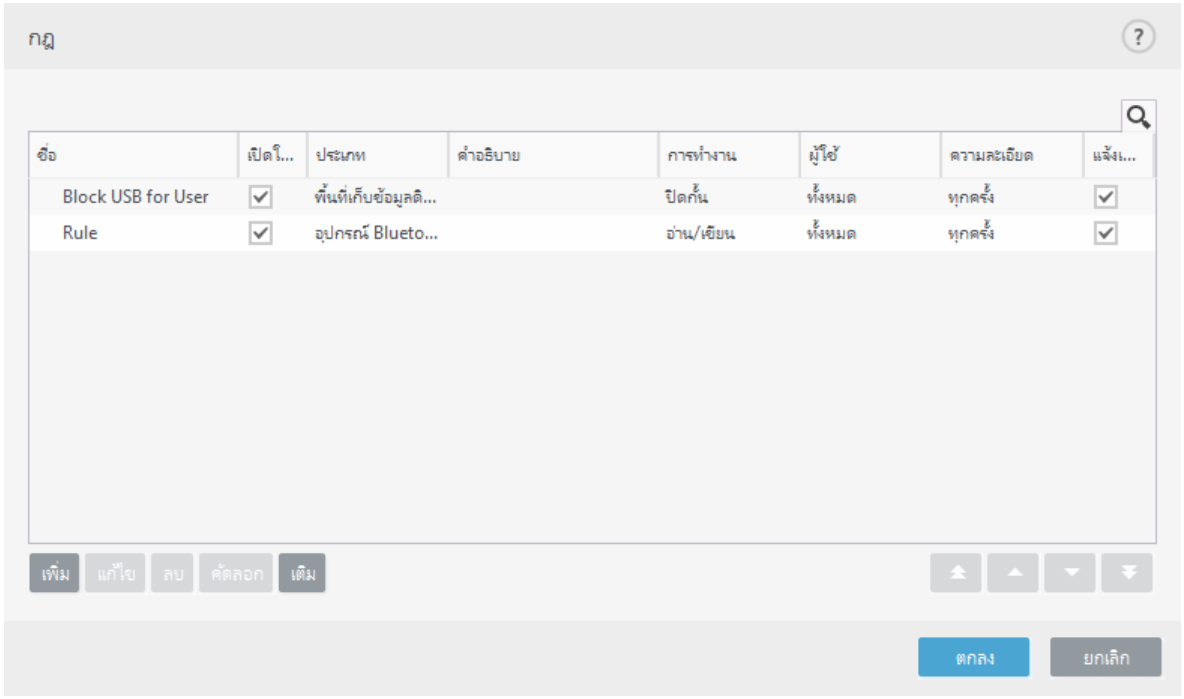
เปิดใช้งานแถบเลื่อนที่อยู่ถัดจาก **เปิดใช้งานการควบคุมอุปกรณ์** เพื่อเปิดใช้งานคุณลักษณะการควบคุมอุปกรณ์ใน ESET Smart Security Premium คุณจำเป็นต้องรีสตาร์ทคอมพิวเตอร์ของคุณเพื่อให้การเปลี่ยนแปลงนี้เกิดผล เมื่อเปิดใช้งานการควบคุมอุปกรณ์ **กฎ** จะเปิดใช้งาน และอนุญาตให้คุณเปิดหน้าต่าง ตัวแก้ไขกฎ

> คุณสามารถสร้างกลุ่มอุปกรณ์หลายๆ กลุ่มที่ปรับใช้กฎที่แตกต่างกัน คุณยังสามารถสร้างกลุ่มอุปกรณ์เพียงกลุ่มเดียวที่จะปรับใช้กฎพร้อมการดำเนินการ **อ่าน/เขียน** หรือ **อ่านอย่างเดียว** วิธีนี้จะช่วยปิดกั้นอุปกรณ์ที่การควบคุมอุปกรณ์ไม่รู้จักเมื่อต่อเข้ากับคอมพิวเตอร์ของคุณ

ถ้ามีการใส่อุปกรณ์ที่ถูกปิดกั้นโดยกฎที่มีอยู่ จะมีหน้าต่างการแจ้งเตือนปรากฏและไม่ได้รับสิทธิ์ให้เข้าถึงอุปกรณ์

เครื่องมือแก้ไขกฎการควบคุมอุปกรณ์

หน้าต่าง **เครื่องมือแก้ไขกฎการควบคุมอุปกรณ์** จะแสดงกฎที่มีอยู่ และช่วยให้สามารถทำการควบคุมอุปกรณ์ภายนอกที่ผู้ใช้ใช้ในการเชื่อมต่อกับคอมพิวเตอร์ได้อย่างแม่นยำ



สามารถทำการอนุญาตหรือปิดกั้นอุปกรณ์บางชนิดได้ตามผู้ใช้หรือกลุ่มผู้ใช้ และอิงตามพารามิเตอร์อุปกรณ์เพิ่มเติม ซึ่งสามารถระบุไว้ในการกำหนดค่ากฎได้ รายการของกฎประกอบด้วยคำอธิบายของกฎหลายรายการ เช่น ชื่อ ประเภทอุปกรณ์ภายนอก การดำเนินการที่จะทำหลังจากเชื่อมต่ออุปกรณ์ภายนอกกับคอมพิวเตอร์ของคุณ และความรุนแรงของบันทึก โปรดดูที่ การเพิ่มกฎการควบคุมอุปกรณ์

คลิกที่ **เพิ่ม** หรือ **แก้ไข** เพื่อจัดการกฎ คลิก **คัดลอก** เพื่อสร้างกฎใหม่โดยมีตัวเลือกที่กำหนดไว้ล่วงหน้า ซึ่งใช้สำหรับกฎอื่นที่เลือกไว้ สามารถคัดลอกสตริง XML ที่ปรากฏเมื่อคลิกกฎนั้นลงในคลิปบอร์ด เพื่อช่วยให้ผู้ดูแลระบบสามารถส่งออก/นำเข้าข้อมูลเหล่านี้และใช้งาน

โดยการกด **CTRL** และคลิก คุณสามารถเลือกหลายกฎและใช้การทำงานกับกฎที่เลือกไว้ทั้งหมด เช่น ลบ หรือเลื่อนขึ้นลงในรายการ ช่องทำเครื่องหมาย **เปิดใช้งาน** จะปิดใช้งานหรือเปิดใช้งานกฎนี้ ซึ่งจะมีประโยชน์ถ้าคุณไม่ต้องการลบกฎอย่างถาวร ในกรณีที่คุณต้องการใช้อีกในอนาคต

การควบคุมจะดำเนินการจนเสร็จสิ้นตามกฎที่จัดเรียงไว้ตามลำดับความสำคัญ โดยกฎที่มีลำดับความสำคัญสูงจะอยู่ด้านบนสุด

รายการบันทึกสามารถดูได้จากหน้าต่างหลักของ ESET Smart Security Premium ใน **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก**

บันทึกการควบคุมอุปกรณ์จะบันทึกรายการการเกิดขึ้นซ้ำทั้งหมดขณะที่การควบคุมอุปกรณ์ถูกเรียก

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)

กลุ่มอุปกรณ์

⚠ อุปกรณ์ที่ต่อเข้ากับคอมพิวเตอร์ของคุณอาจก่อให้เกิดความเสี่ยงด้านความปลอดภัย

หน้าต่างกลุ่มอุปกรณ์แบ่งออกเป็นสองส่วน ด้านขวาของหน้าต่างแสดงรายชื่ออุปกรณ์ที่เป็นของกลุ่มที่เกี่ยวข้อง และด้านซ้ายของหน้าต่างประกอบด้วยกลุ่มที่สร้างขึ้น เลือกกลุ่มที่มีรายชื่ออุปกรณ์ที่คุณต้องการแสดงไว้ในช่องด้านขวา

เมื่อคุณเปิดหน้าต่างกลุ่มอุปกรณ์และเลือกกลุ่ม คุณจะสามารถเพิ่มหรือย้ายอุปกรณ์ออกจากรายชื่อ วิธีเพิ่มอุปกรณ์

ลงในกลุ่มอีกวิธีหนึ่งคือนำเข้าอุปกรณ์จากไฟล์ หรือคุณสามารถเลือกคลิกปุ่ม **เติม** และอุปกรณ์ทั้งหมดที่ต่อเข้ากับคอมพิวเตอร์ของคุณจะแสดงในหน้าต่าง **อุปกรณ์ที่ตรวจพบ** เลือกอุปกรณ์จากรายการที่เพิ่มใหม่เพื่อเพิ่มอุปกรณ์นั้นลงในกลุ่มได้ด้วยการคลิก **ตกลง**

องค์ประกอบการควบคุม

เพิ่ม – คุณสามารถเพิ่มกลุ่มได้โดยป้อนชื่อหรืออุปกรณ์ไปยังกลุ่มที่มีอยู่ (อีกทางหนึ่งคือคุณสามารถระบุข้อมูล เช่น ชื่อผู้ขาย รุ่น และหมายเลขซีเรียลได้) โดยขึ้นอยู่กับว่าคุณคลิกปุ่มที่ส่วนใดของหน้าต่าง

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)

เมื่อปรับแต่งเสร็จแล้ว ให้คลิก **OK** คลิก **ยกเลิก** ถ้าคุณต้องการออกจากหน้าต่าง **กลุ่มอุปกรณ์** โดยไม่บันทึกการเปลี่ยนแปลง

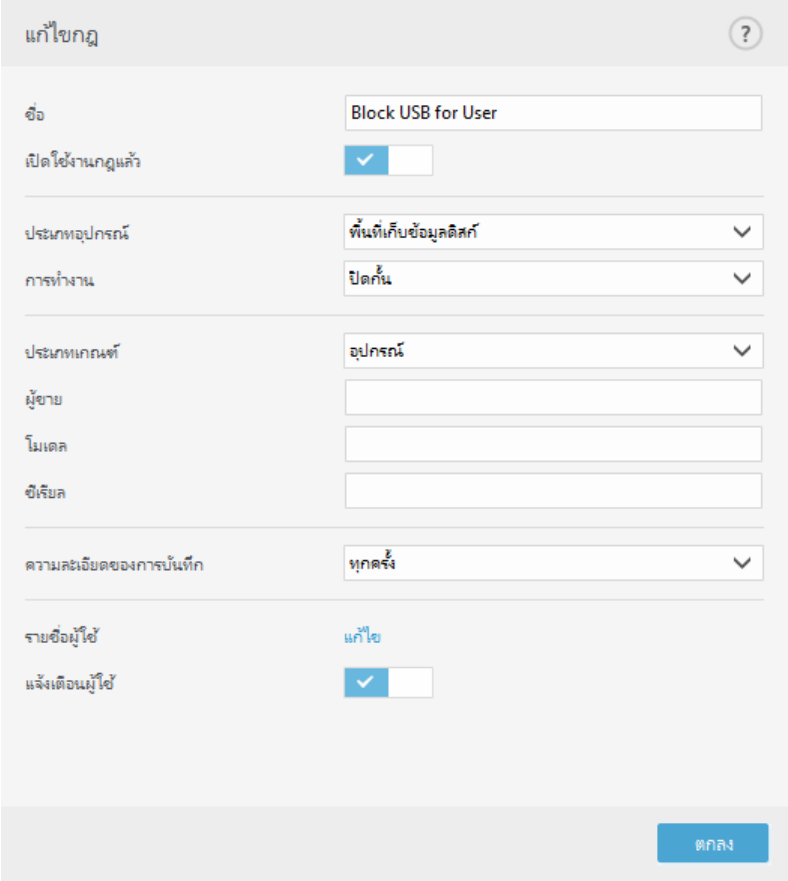
คุณสามารถสร้างกลุ่มอุปกรณ์หลายๆ กลุ่มที่ปรับใช้กฎที่แตกต่างกัน คุณยังสามารถสร้างกลุ่มอุปกรณ์เพียงกลุ่มเดียวที่จะปรับใช้กฎพร้อมการดำเนินการ **อ่าน/เขียน** หรือ **อ่านอย่างเดียว** วิธีนี้จะช่วยปิดกั้นอุปกรณ์ที่การควบคุมอุปกรณ์ไม่รู้จักเมื่อต่อเข้ากับคอมพิวเตอร์ของคุณ

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

Bluetooth สามารถเลือกได้เพียงอนุญาต ปิดกั้นหรือเตือนเท่านั้น)

การเพิ่มกฎการควบคุมอุปกรณ์

กฎการควบคุมอุปกรณ์จะกำหนดการทำงานที่จะดำเนินการเมื่ออุปกรณ์เชื่อมต่ออุปกรณ์ที่เป็นไปตามเกณฑ์ของกฎที่ตั้งไว้กับคอมพิวเตอร์



ป้อนคำอธิบายของกฎในช่อง **ชื่อ** เพื่อคำอธิบายที่ดีขึ้น คลิกแถบเลื่อนถัดจาก **เปิดใช้งานกฎแล้ว** เพื่อปิดใช้งานหรือเปิดใช้งานกฎนี้ ซึ่งอาจมีประโยชน์หากคุณไม่ต้องการลบกฎอย่างถาวร

ประเภทอุปกรณ์

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

ทำของอุปกรณ์ และไม่ได้เปิดเผยข้อมูลเกี่ยวกับผู้ใช้ การปิดกั้นอุปกรณ์เหล่านั้นจึงเป็นการปิดกั้นแบบทั้งหมดเท่านั้น

การทำงาน

สามารถอนุญาตหรือปิดกั้นการเข้าถึงอุปกรณ์ที่ไม่ใช่อุปกรณ์เก็บข้อมูลได้ ในทางตรงกันข้าม กฎสำหรับอุปกรณ์เก็บข้อมูลช่วยให้คุณสามารถเลือกได้จากหนึ่งในการตั้งค่าสิทธิ์ต่อไปนี้:

- **อ่าน/เขียน** – อนุญาตให้เข้าถึงอุปกรณ์ได้อย่างสมบูรณ์
- **ปิดกั้น** – การเข้าถึงอุปกรณ์จะถูกปิดกั้น
- **อ่านอย่างเดียว** – อนุญาตเฉพาะสิทธิ์ในการอ่านอุปกรณ์เท่านั้น
- **เตือน** – ในแต่ละครั้งที่เชื่อมต่ออุปกรณ์ ระบบจะแจ้งให้ผู้ใช้ทราบว่าอุปกรณ์นั้นได้รับอนุญาต/ถูกปิดกั้น และจะมีการจัดทำรายการบันทึกขึ้น อุปกรณ์ไม่ได้รับการจดจำ การแจ้งเตือนจะยังปรากฏขึ้นเมื่อมีการเชื่อมต่อกับอุปกรณ์เดิมนั้นอีกในภายหลัง

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

ประเภทเกณฑ์

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

พารามิเตอร์เพิ่มเติมซึ่งแสดงด้านล่างสามารถใช้เพื่อปรับแต่งและออกแบบกฎให้กับอุปกรณ์ พารามิเตอร์ทั้งหมดจะต้องตรงตามตัวพิมพ์เล็กและใหญ่:

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

> หากไม่ได้ระบุพารามิเตอร์เหล่านี้ กฎจะละเว้นช่องเหล่านี้ขณะที่จับคู่ พารามิเตอร์การกรองในช่องข้อความทั้งหมดไม่จำเป็นต้องตรงตามตัวพิมพ์เล็กและใหญ่และไม่สนับสนุนสัญลักษณ์แทน (*, ?)

หากต้องการดูข้อมูลเกี่ยวกับอุปกรณ์ ให้สร้างกฎสำหรับอุปกรณ์ประเภทนั้น เชื่อมต่ออุปกรณ์กับคอมพิวเตอร์ของคุณ และตรวจสอบรายละเอียดของอุปกรณ์ใน บันทึกการควบคุมอุปกรณ์

ความละเอียดของการบันทึก

ESET Smart Security Premium จะบันทึกเหตุการณ์สำคัญทั้งหมดไว้ในไฟล์บันทึก ซึ่งจะสามารถดูได้โดยตรงจากเมนูหลัก คลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก** จากนั้นเลือก**ควบคุมอุปกรณ์** จาก **บันทึก** ในเมนูแบบเลื่อนลง

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

รายชื่อผู้ใช้

สามารถจำกัดกฎสำหรับผู้ใช้บางคนหรือผู้ใช้บางกลุ่มได้โดยการเพิ่มกฎลงในรายชื่อผู้ใช้ โดยคลิกที่ **แก้ไข** ที่อยู่ถัดจาก **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

การป้องกัน Webcam

การป้องกันเว็บแคม ช่วยให้คุณสามารถดูกระบวนการและแอพพลิเคชันต่างๆ ที่เข้าถึงกล้องทางเว็บของคอมพิวเตอร์ของคุณได้ หน้าต่างแจ้งเตือนจะแสดงขึ้นหากมีแอพพลิเคชันที่ไม่ต้องการกำลังพยายามเข้าถึงกล้องของคุณ คุณสามารถ **อนุญาต** หรือ **ปิดกั้น** การเข้าถึง สีของหน้าต่างแจ้งเตือนจะขึ้นอยู่กับความเชื่อถือของแอพพลิเคชัน

ตัวเลือกการตั้งค่าการป้องกันเว็บแคมนั้นสามารถแก้ไขได้ใน **การตั้งค่าขั้นสูง**(F5) > **การควบคุมอุปกรณ์** > **การป้องกันเว็บแคม**

เพื่อเปิดใช้งานคุณลักษณะการป้องกันเว็บแคมใน ESET Smart Security Premium ให้เปิดใช้งานแถบเลื่อนถัดจาก **เปิดใช้งานการป้องกันเว็บแคม**

เมื่อเปิดใช้งานการป้องกันเว็บแคม **กฎ** จะทำงาน ทำให้คุณสามารถเปิดหน้าต่าง ตัวแก้ไขกฎ ได้

หากต้องการปิดใช้งานการแจ้งเตือนสำหรับแอพพลิเคชันที่มีกฎซึ่งถูกแก้ไขแต่ยังคงเป็นลายเซ็นดิจิทัลที่ถูกต้อง (เช่น รายการอัพเดทแอพพลิเคชัน) ให้เปิดใช้งานแถบเลื่อนที่อยู่ถัดจาก **ปิดใช้งานการเข้าถึงการแจ้งเตือนเว็บแคมสำหรับแอพพลิเคชันที่มีการแก้ไข**

ตัวแก้ไขกฎการป้องกัน Webcam

หน้าต่างจะแสดงกฎที่มีอยู่และอนุญาตให้ควบคุมแอพพลิเคชันและกระบวนการต่างๆ ที่เข้าถึงกล้องทางเว็บของคอมพิวเตอร์ของคุณได้ตามการดำเนินการที่คุณลงมือทำ

การทำงานที่ใช้ได้มีดังนี้:

- **อนุญาตการเข้าถึง**
- **บล็อกการเข้าถึง**
- **ถาม** (ถามผู้ใช้ทุกครั้งที่แอพพลิเคชันพยายามเข้าถึงเว็บแคม)

ยกเลิกการเลือกกล่องกาเครื่องหมายในคอลัมน์ **การแจ้งเตือน** เพื่อหยุดรับการแจ้งเตือนเมื่อแอพพลิเคชันเข้าถึงเว็บแคม

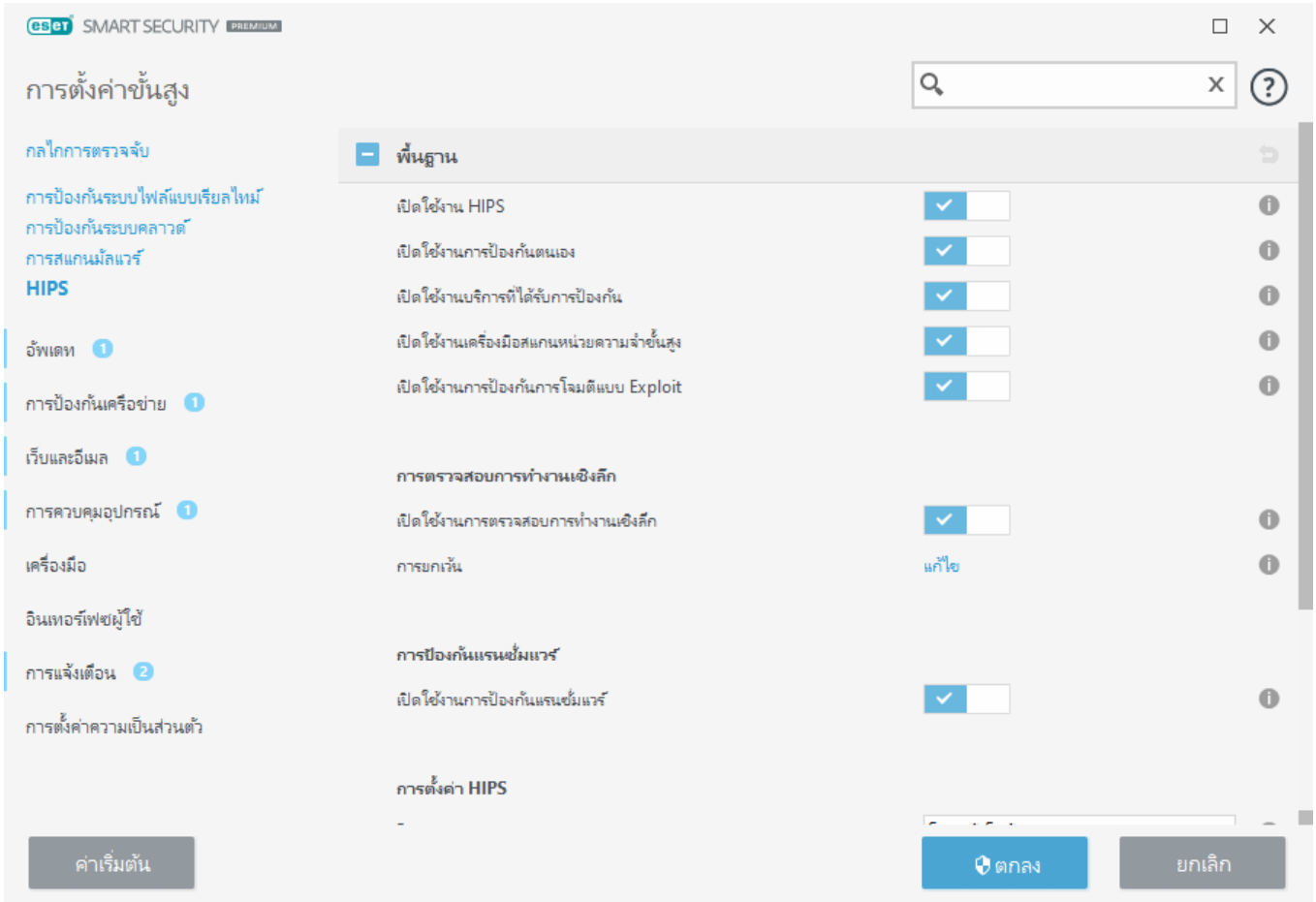
คำแนะนำพร้อมภาพประกอบ
วิธีสร้างและแก้ไขกฎเว็บแคมใน ESET Smart Security Premium

ระบบป้องกันการบุกรุกโฮสต์ (HIPS)

การเปลี่ยนเป็นการตั้งค่า HIPS ควรดำเนินการโดยผู้ใช้ที่มีประสบการณ์ในการใช้งานเท่านั้น การกำหนดค่าที่ไถูกต้องของการตั้งค่า HIPS จะทำให้ระบบมีปัญหาด้านเสถียรภาพ

ระบบ **ป้องกันการบุกรุกที่ใช้โฮสต์ (HIPS)** จะป้องกันระบบของคุณจากมัลแวร์และกิจกรรมที่ไม่พึงประสงค์ที่พยายามสร้างผลเสียต่อคอมพิวเตอร์ HIPS ใช้การวิเคราะห์การทำงานขั้นสูงร่วมกับความสามารถในการตรวจหาของการกรองเครือข่าย เพื่อตรวจสอบกระบวนการที่ทำงานอยู่ ไฟล์และรหัสรีจิสตรี HIPS แยกต่างหากจากการป้องกันระบบไฟล์แบบเรียลไทม์และไม่ใช่ไฟร์วอลล์ แต่จะติดตามเฉพาะกระบวนการที่ทำงานอยู่ภายในระบบปฏิบัติการเท่านั้น

การตั้งค่า HIPS สามารถทำได้ที่ใต้ **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจจับ** > **HIPS** > **พื้นฐาน** สถานะของ HIPS (เปิดใช้งาน/ปิดใช้งาน) จะปรากฏใน หน้าต่างโปรแกรมหลัก ESET Smart Security Premium ใต้ **การตั้งค่า** > **การป้องกันคอมพิวเตอร์**



พื้นฐาน

เปิดใช้งาน HIPS – เปิดใช้งาน HIPS เป็นค่าเริ่มต้นในESET Smart Security Premium การปิด HIPS จะปิดการใช้งานคุณลักษณะของ HIPS ที่เหลือ เช่น การป้องกันการโจมตีแบบ Exploit

เปิดใช้งานการป้องกันตนเอง – ESET Smart Security Premium ใช้เทคโนโลยี**การป้องกันตนเอง** ในตัว ซึ่งเป็นส่วนหนึ่งของ HIPS เพื่อป้องกันซอฟต์แวร์ที่เป็นอันตรายจากความเสียหายหรือการเปิดใช้งานการป้องกันไวรัสและสปายแวร์ การป้องกันตนเองจะป้องกันระบบที่สำคัญและกระบวนการของ ESET รหัสรีจิสตรีและไฟล์ต่างๆ จากการถูกเปลี่ยนแปลง

เปิดใช้งานบริการที่ได้รับการป้องกัน – เปิดใช้การป้องกันสำหรับ บริการ ESET (ekrn.exe) เมื่อเปิดใช้งานแล้ว บริการจะเริ่มต้นโดยเป็นกระบวนการ Windows ที่ได้รับการป้องกันเพื่อป้องกันการโจมตีจากมัลแวร์ โดยตัวเลือกนี้จะมีให้ใช้งานใน Windows 8.1 และรุ่นใหม่กว่า

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

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 คุณสามารถเลือกเพิ่ม แก้ไข หรือลบกฎได้ คุณสามารถดูรายละเอียดเพิ่มเติมเกี่ยวกับการสร้างกฎและการดำเนินการ HIPS ได้ใน แก้ไขกฎ HIPS

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)

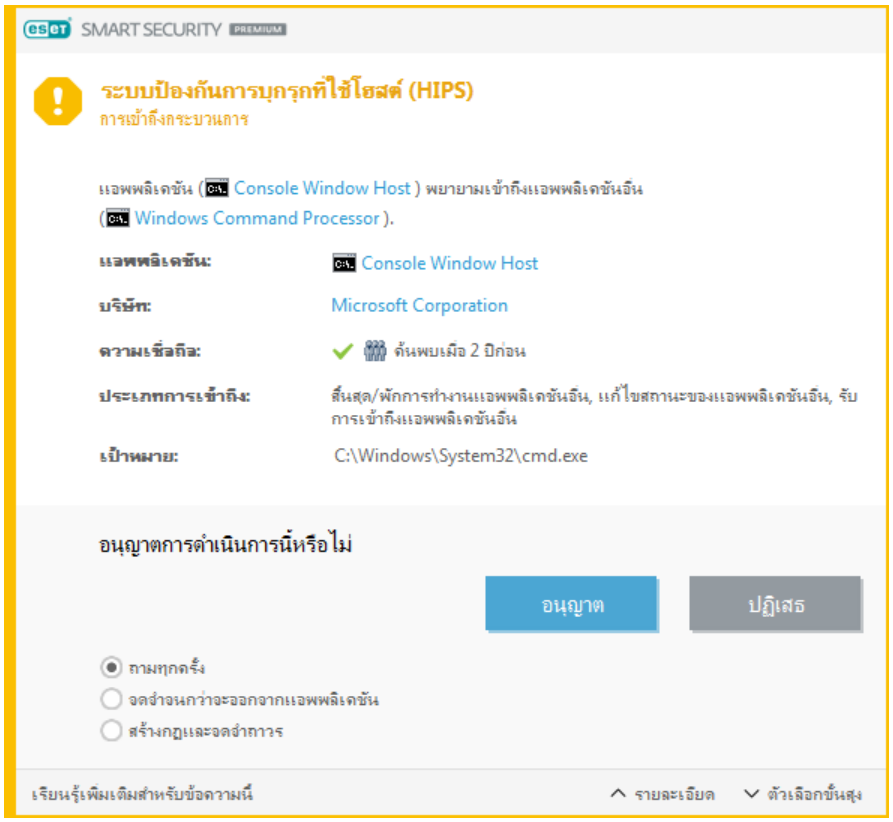
คลิก **รายละเอียด** ที่ด้านล่างสุดเพื่อดูสิ่งที่แอพพลิเคชันเรียกใช้การทำงาน ความเชื่อถือของไฟล์คืออะไร หรือการทำงานใดที่คุณถูกขอให้อนุญาตหรือปฏิเสธ

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

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

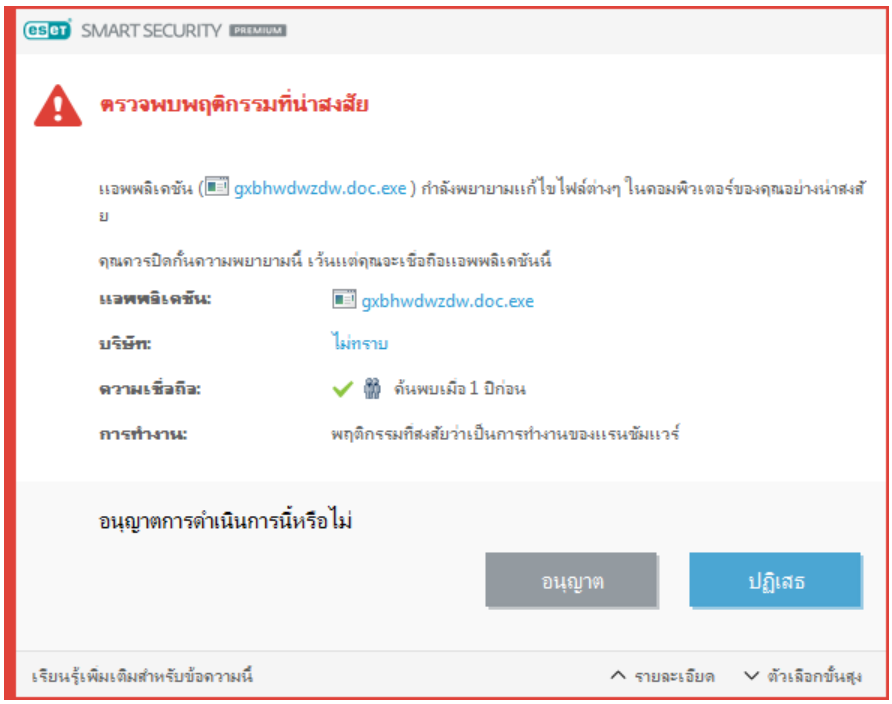
การแจ้งเตือน HIPS แบบไม่มีจุดสิ้นสุดหรือไม่

หากต้องการหยุดการแจ้งเตือนที่แสดง เปลี่ยนโหมดการกรองเป็น **โหมดอัตโนมัติ** ใน **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจหา** > **HIPS** > **พื้นฐาน**



ตรวจพบพฤติกรรมที่สงสัยว่าเป็นการทำงานของแรนซัมแวร์

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



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

ESET LiveGrid® ต้องเปิดใช้งานเอาไว้เพื่อให้สามารถใช้งานการป้องกันแรนซัมแวร์ได้อย่างถูกต้อง

การจัดการกฎ HIPS

รายการของกฎที่ผู้ใช้กำหนดและเพิ่มโดยอัตโนมัติจากระบบ HIPS สามารถดูรายละเอียดเพิ่มเติมเกี่ยวกับการสร้างกฎและการดำเนินการของ HIPS ได้ในบท การตั้งค่ากฎ HIPS ดูหลักการทั่วไปของ HIPS

คอลัมน์

กฎ – ชื่อกฎที่ผู้ใช้กำหนดหรือเลือกโดยอัตโนมัติ

เปิดใช้งาน – ปิดใช้งานแถบเลื่อนนี้หากคุณต้องการคงกฎไว้ในรายการแต่ไม่ต้องการใช้

การทำงาน – กฎระบุการทำงาน – **อนุญาต ปิดกั้น** หรือ **ถาม** – ที่ควรได้รับการดำเนินการถ้าตรงตามเงื่อนไข

ที่มา – ระบบจะใช้กฎนี้ต่อเมื่อแอพพลิเคชันเรียกเหตุการณ์

เป้าหมาย – จะมีการใช้กฎก็ต่อเมื่อการดำเนินการเกี่ยวข้องกับไฟล์ แอพพลิเคชัน หรือรายการรีจิสตรีบางรายการ

ความละเอียดของการบันทึก – ถ้าคุณเปิดใช้งานตัวเลือกนี้ ข้อมูลเกี่ยวกับกฎนี้จะถูกเขียนไปที่ บันทึก HIPS

แจ้ง – หน้าต่างป๊อปอัปขนาดเล็กจะปรากฏที่มุมล่างขวาถ้ามีการเรียกเหตุการณ์

องค์ประกอบการควบคุม

เพิ่ม – สร้างกฎใหม่

แก้ไข – ช่วยให้คุณสามารถแก้ไขรายการที่เลือกได้

ลบออก – ลบรายการที่เลือกออก

จัดอันดับความสำคัญของกฎ HIPS

ไม่มีตัวเลือกเพื่อปรับระดับความสำคัญของกฎ HIPS ที่ใช้ปุ่มบนสุด/ล่าสุด (ซึ่ง กฎของไฟร์วอลล์ ที่กฎถูกเรียกใช้จากบนลงล่าง).

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

แก้ไขกฎ HIPS

ดู การจัดการกฎ HIPS ก่อน

ชื่อกฎ – ชื่อกฎที่ผู้ใช้กำหนดหรือเลือกโดยอัตโนมัติ

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

การดำเนินการที่ได้ผล – คุณต้องเลือกประเภทของการดำเนินการที่กฎจะนำมาปรับใช้ ระบบจะใช้กฎนี้เฉพาะสำหรับการดำเนินการประเภทนี้เท่านั้นและสำหรับเป้าหมายที่เลือก

เปิดใช้งาน – ปิดใช้งานแถบเลื่อนนี้หากคุณต้องการคงกฎไว้ในรายการแต่ไม่ปรับใช้

ความละเอียดของการบันทึก – ถ้าคุณเปิดใช้งานตัวเลือกนี้ ข้อมูลเกี่ยวกับกฎนี้จะถูกเขียนไปที่ บันทึก HIPS

แจ้งเตือนผู้ใช้ – หน้าต่างป๊อปอัปขนาดเล็กจะปรากฏที่มุมล่างขวาถ้ามีการเรียกเหตุการณ์

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 **รายการเฉพาะ** จากเมนูแบบเลื่อนลงแล้วคลิก **เพิ่ม** เพื่อป้อนข้อมูลด้วยตัวเอง หรือคุณสามารถคลิก **เปิดตัวแก้ไขรีจิสตรี** เพื่อเลือกรหัสจากรีจิสตรี นอกจากนี้ คุณยังสามารถเลือก **รายการทั้งหมด** จากเมนูแบบเลื่อนลงเพื่อเพิ่มแอพพลิเคชันทั้งหมดได้

> **i** การดำเนินการของกฎบางอย่างที่กำหนดไว้ล่วงหน้าโดย HIPS จะไม่สามารถปิดกั้นหรืออนุญาตได้ตามค่าเริ่มต้น นอกจากนี้ HIPS จะไม่ตรวจสอบการดำเนินการทั้งหมดของระบบ HIPS ตรวจสอบการดำเนินการที่อาจพิจารณาว่าไม่ปลอดภัย

คำอธิบายของการดำเนินการที่สำคัญ:

การดำเนินการของไฟล์

- **ลบไฟล์** – แอพพลิเคชันจะสอบถามเกี่ยวกับการอนุญาตให้ลบไฟล์เป้าหมาย
- **เขียนไปยังไฟล์** – แอพพลิเคชันจะสอบถามเกี่ยวกับการอนุญาตให้เขียนไฟล์เป้าหมาย
- **การเข้าถึงดิสก์โดยตรง** – แอพพลิเคชันจะพยายามอ่านจากหรือเขียนไปยังดิสก์ด้วยวิธีที่ไม่เป็นมาตรฐาน ซึ่งจะหลีกเลี่ยงขั้นตอนทำงานทั่วไปของ Windows ซึ่งอาจส่งผลให้ไฟล์ได้รับการแก้ไขโดยไม่ใช้แอพพลิเคชันของกฎที่สอดคล้องกัน การดำเนินการนี้อาจมีสาเหตุจากการที่มัลแวร์พยายามหลบเลี่ยงการตรวจหาซอฟต์แวร์สำรองข้อมูลพยายามที่จะทำสำเนาของดิสก์ หรือโปรแกรมจัดการพาร์ติชันพยายามจัดระเบียบได

รฟ์ข้อมูลของดิสก์ใหม่

• **ติดตั้งฮุคร่วม** – อ้างถึงการเรียกฟังก์ชัน SetWindowsHookEx จากไลบรารี MSDN

• **โหลดไดรเวอร์** – การติดตั้งและการโหลดไดรเวอร์ลงในระบบ

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

ไม่สามารถดักรับข้อมูลการดำเนินการของกระบวนการของ Windows XP รุ่น 64 บิตได้

การดำเนินการของรีจิสตรี

• **แก้ไขการตั้งค่าการเริ่มต้น** – การเปลี่ยนแปลงในการตั้งค่า ซึ่งกำหนดแอพพลิเคชันที่จะถูกเรียกใช้เมื่อเริ่มต้น Windows ซึ่งจะสามารถพบได้ เช่น จากการค้นหารหัส Run ใน Windows Registry

• **ลบจากรีจิสตรี** – การลบรหัสรีจิสตรีหรือค่าของรหัสรีจิสตรี

• **เปลี่ยนชื่อรหัสรีจิสตรี** – การเปลี่ยนชื่อรหัสรีจิสตรี

• **แก้ไขรีจิสตรี** – การสร้างค่าใหม่ของรหัสรีจิสตรี การเปลี่ยนค่าที่มีอยู่ การย้ายข้อมูลในโครงสร้างฐานข้อมูล

หรือการตั้งค่าสิทธิ์ของผู้ใช้หรือกลุ่มสำหรับรหัสรีจิสตรี

> คุณสามารถใช้สัญลักษณ์แทนที่มีข้อจำกัดบางอย่างเมื่อป้อนเป้าหมาย แทนที่จะใช้รหัสหนึ่ง ระบบจะใช้สัญลักษณ์ * (ดอกจัน) ในพาธของรีจิสตรี ตัวอย่างเช่น *HKEY_USERS*\software* สามารถหมายถึง *HKEY_USER\.default\software* แต่ไม่ใช่ *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software* *HKEY_LOCAL_MACHINE\system\ControlSet** ไม่ใช่พาธของรหัสรีจิสตรีที่ถูกต้อง พาธของรหัสรีจิสตรีที่มี * หมายความว่า "พาธนี้หรือพาธใดๆ ในระดับใดก็ได้อยู่หลังสัญลักษณ์นี้" วิธีการนี้เป็นวิธีการเดียวในการใช้สัญลักษณ์แทนสำหรับเป้าหมายไฟล์ ขั้นแรก ระบบจะประเมินพาธบางส่วนก่อน จากนั้นจะประเมินพาธที่อยู่หลังสัญลักษณ์แทน (*)

> หากคุณสร้างกฎที่กว้างมาก คำเตือนเกี่ยวกับกฎประเภทนี้จะปรากฏขึ้น

ในตัวอย่างต่อไปนี้ เราจะสาธิตวิธีจำกัดการทำงานที่ไม่พึงประสงค์ของแอพพลิเคชันที่ระบุ:

1. ตั้งชื่อกฎและเลือก**ปิดกั้น** (หรือ **ถาม** หากคุณต้องการหรือเลือกภายหลัง) จากเมนู**การทำงาน** แบบเลื่อนลง

2. เลือกแถบตัวเลื่อนที่อยู่ถัดจาก **แจ้งเตือนผู้ใช้** เพื่อแสดงการแจ้งเตือนเมื่อมีการนำกฎไปใช้

3. เลือกการดำเนินการอย่างน้อยหนึ่งอย่าง ในส่วน**การดำเนินการที่ได้ผล** ว่าจะใช้กฎใด

4. คลิก**ถัดไป**

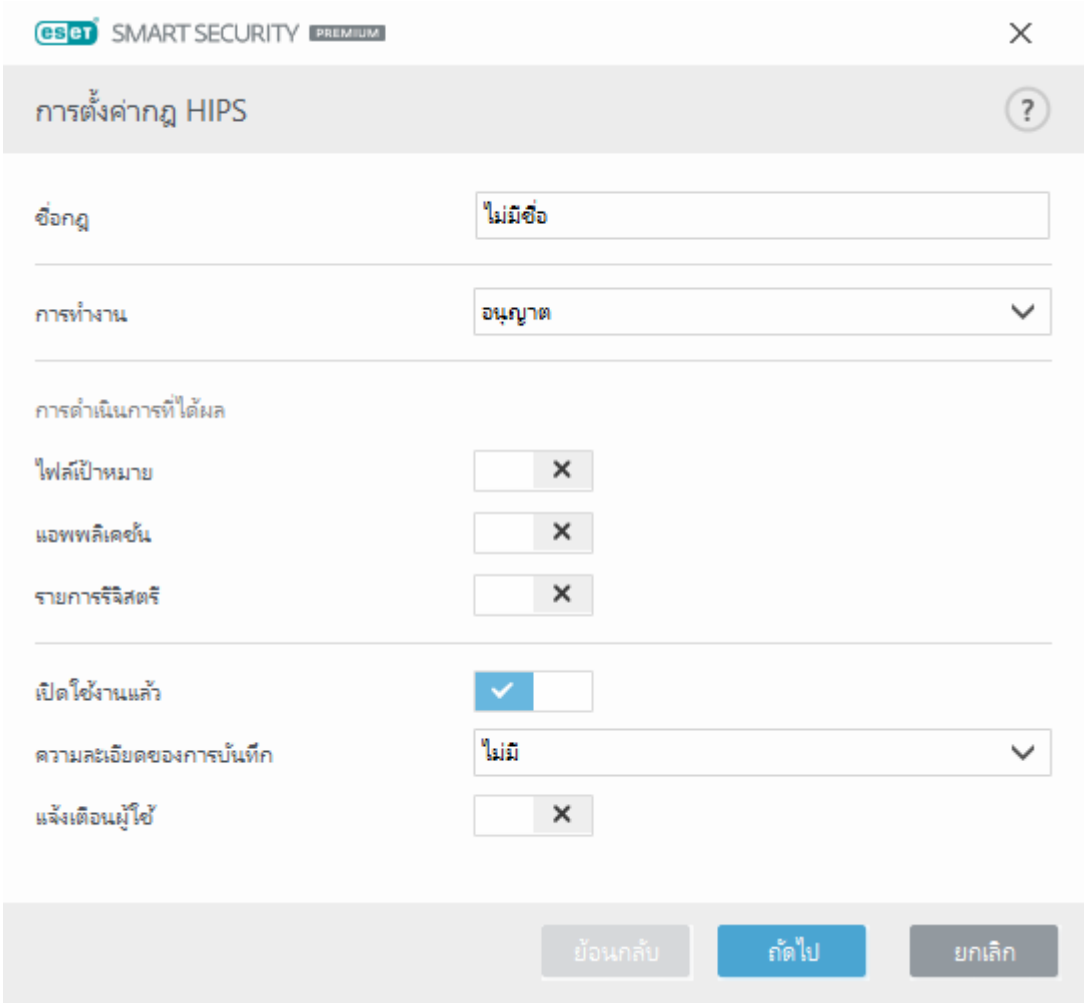
5. ในหน้าต่าง **แอพพลิเคชันที่มา** เลือก **แอพพลิเคชันที่เจาะจง** จากเมนูแบบเลื่อนลงเพื่อใช้กฎใหม่กับแอพพลิเคชันทั้งหมดที่พยายามจะทำงานกับแอพพลิเคชันที่เลือกไว้บนแอพพลิเคชันที่คุณระบุ

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*

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

โหมดผู้เล่นเกม

โหมดผู้เล่นเกมเป็นคุณลักษณะสำหรับผู้ใช้ที่ต้องการใช้ซอฟต์แวร์อย่างต่อเนื่องโดยไม่ถูกขัดขวาง ไม่ต้องการให้หน้าต่างป๊อปอัปมารบกวน และต้องการลดการใช้งาน CPU โหมดผู้เล่นเกมสามารถใช้ระหว่างการนำเสนอที่ไม่ควรมีการขัดจังหวะโดยกิจกรรมการป้องกันไวรัส เมื่อเปิดใช้งานคุณลักษณะนี้ หน้าต่างป๊อปอัปทั้งหมดจะถูกปิดใช้งาน

และกิจกรรมของเครื่องมือวางกำหนดการจะหยุดทำงานโดยสิ้นเชิง การป้องกันระบบจะยังทำงานอยู่ในพื้นหลัง แต่ผู้ใช้ไม่ต้องดำเนินการใดๆ

คุณสามารถเปิดหรือปิดใช้งานโหมดผู้เล่นเกมได้ใน หน้าต่างโปรแกรมหลัก ใต้ **การตั้งค่า** > **การป้องกันคอมพิวเตอร์** โดยคลิก  หรือ  ที่อยู่ถัดจาก **โหมดผู้เล่นเกม** การเปิดใช้งานโหมดผู้เล่นเกมอาจทำให้เกิดความเสี่ยงด้านความปลอดภัย ดังนั้นไอคอนสถานะการป้องกันที่ทาสก์บาร์จะเปลี่ยนเป็นสีส้มพร้อมกับการเตือน คุณยังจะเห็นคำเตือนนี้ใน หน้าต่างโปรแกรมหลัก ซึ่งคุณจะเห็น **โหมดผู้เล่นเกมเปิดใช้งานอยู่** เป็นสีส้ม

เปิดใช้งาน **เปิดใช้งานโหมดผู้เล่นเกมเมื่อเรียกใช้แอพพลิเคชันในโหมดเต็มหน้าจอโดยอัตโนมัติ** ใต้ **การตั้งค่าขั้นสูง** (F5) > **เครื่องมือ** > **โหมดผู้เล่นเกม** เพื่อให้โหมดผู้เล่นเกมเริ่มต้นเมื่อใดก็ตามที่คุณเริ่มใช้งานแอพพลิเคชันแบบเต็มหน้าจอและหยุดหลังจากที่คุณออกจากแอพพลิเคชันนั้น

เปิดใช้งาน **ปิดใช้งานโหมดผู้เล่นเกมโดยอัตโนมัติหลังจาก** เพื่อระบุช่วงเวลาที่โหมดผู้เล่นเกมจะปิดใช้งานโดยอัตโนมัติ

> **i** หากไฟร์วอลล์อยู่ในโหมดโต้ตอบ และมีการเปิดใช้งานโหมดผู้เล่นเกม คุณอาจพบปัญหาในการเชื่อมต่อกับอินเทอร์เน็ต ซึ่งอาจเป็นปัญหาถ้าคุณเริ่มต้นเกมที่เชื่อมต่อกับอินเทอร์เน็ต โดยปกติแล้ว ระบบจะสอบถามเพื่อให้คุณยืนยันการทำงานดังกล่าว (ถ้าไม่ได้กำหนดกฎการสื่อสารหรือการยกเว้นไว้) แต่การดำเนินการของผู้ใช้จะถูกปิดใช้งานในโหมดผู้เล่นเกม ในการอนุญาตการสื่อสาร ให้ระบุกฎสื่อสารสำหรับแอพพลิเคชันใดๆ ที่อาจพบปัญหานี้ หรือใช้ โหมดการกรอง ที่แตกต่างในไฟร์วอลล์ โปรดทราบว่าหากเปิดใช้งานโหมดผู้เล่นเกม และคุณไปยังหน้าเว็บหรือแอพพลิเคชันที่อาจเกิดความเสี่ยงด้านความปลอดภัย ระบบอาจปิดกั้นหน้าเว็บหรือแอพพลิเคชันเหล่านี้โดยไม่มีคำอธิบายหรือคำเตือนเนื่องจากการโต้ตอบของผู้ใช้ถูกปิดใช้งาน

การสแกนเมื่อเริ่มต้น

ตามค่าเริ่มต้น การตรวจสอบไฟล์เมื่อเริ่มต้นระบบอัตโนมัติจะดำเนินการเมื่อเริ่มต้นระบบและในระหว่างการอัพเดทกลไกตรวจหา การสแกนนี้จะขึ้นอยู่กับ การกำหนดค่าเครื่องมือวางกำหนดการและงาน

ตัวเลือกการสแกนเมื่อเริ่มต้น เป็นส่วนหนึ่งของงานของเครื่องมือวางกำหนดการ **การตรวจสอบไฟล์เมื่อเริ่มต้นระบบ** ในการแก้ไขการตั้งค่า ให้ไปที่ **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ตัววางกำหนดการ** แล้วคลิกที่ **การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้น** จากนั้น **แก้ไข** ในขั้นตอนสุดท้าย หน้าต่าง การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้น จะปรากฏขึ้น (ดูรายละเอียดเพิ่มเติมได้ในบทถัดไป)

สำหรับคำแนะนำโดยละเอียดเกี่ยวกับการสร้างและการจัดการงานของเครื่องมือวางกำหนดการ โปรดดูที่ การสร้างงานใหม่

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

การป้องกันเอกสาร

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

หากต้องการเปิดใช้งานการป้องกันไฟล์เอกสาร ให้เปิดหน้าต่าง **การตั้งค่าขั้นสูง** (F5)> **กลไกการตรวจจับ** > **การสแกนมัลแวร์** > **การป้องกันไฟล์เอกสาร** แล้วคลิกแถบเลื่อนถัดจาก **เปิดใช้งานการป้องกันไฟล์เอกสาร**

i คุณลักษณะนี้จะถูกเปิดใช้งานโดยแอพพลิเคชันที่ใช้ Microsoft Antivirus API (ตัวอย่างเช่น Microsoft Office 2000 และสูงกว่าหรือ Microsoft Internet Explorer 5.0 และสูงกว่า)

การยกเว้น

การยกเว้น จะช่วยให้คุณสามารถยกเว้นวัตถุจากกลไกการตรวจจับได้ ในการทำให้แน่ใจว่าจะมีการสแกนวัตถุทั้งหมด เราขอแนะนำให้สร้างข้อยกเว้นต่อเมื่อจำเป็นจริง ๆ เท่านั้น สถานการณ์ที่คุณอาจต้องยกเว้นวัตถุ ซึ่งอาจรวมถึงการสแกนรายการฐานข้อมูลขนาดใหญ่ที่จะทำให้คอมพิวเตอร์ทำงานช้าในระหว่างการสแกนหรือซอฟต์แวร์ที่ขัดแย้งกับการสแกน

การยกเว้นการทำงาน ช่วยให้คุณยกเว้นไฟล์และโฟลเดอร์จากการสแกน การยกเว้นการทำงานมีประโยชน์ในการยกเว้นการสแกนระดับไฟล์ของแอพพลิเคชันเกมหรือเมื่อเกิดพฤติกรรมของระบบที่ไม่ปกติหรือมีการทำงานเพิ่มขึ้น

การยกเว้นการตรวจหา ช่วยให้คุณยกเว้นวัตถุจากการตรวจหาโดยใช้ชื่อ พาธ หรือแฮชของการตรวจหา การยกเว้นการตรวจหาไม่ได้ยกเว้นไฟล์และโฟลเดอร์จากการสแกนเช่นเดียวกับการยกเว้นการทำงาน การยกเว้นการตรวจหาจะยกเว้นวัตถุเมื่อถูกตรวจจับโดยกลไกการตรวจจับและมีกฎที่เหมาะสมแสดงอยู่ในรายการการยกเว้นเท่านั้น

โปรดอย่าสับสนกับประเภทการยกเว้นอื่นๆ:

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

การยกเว้นการทำงาน

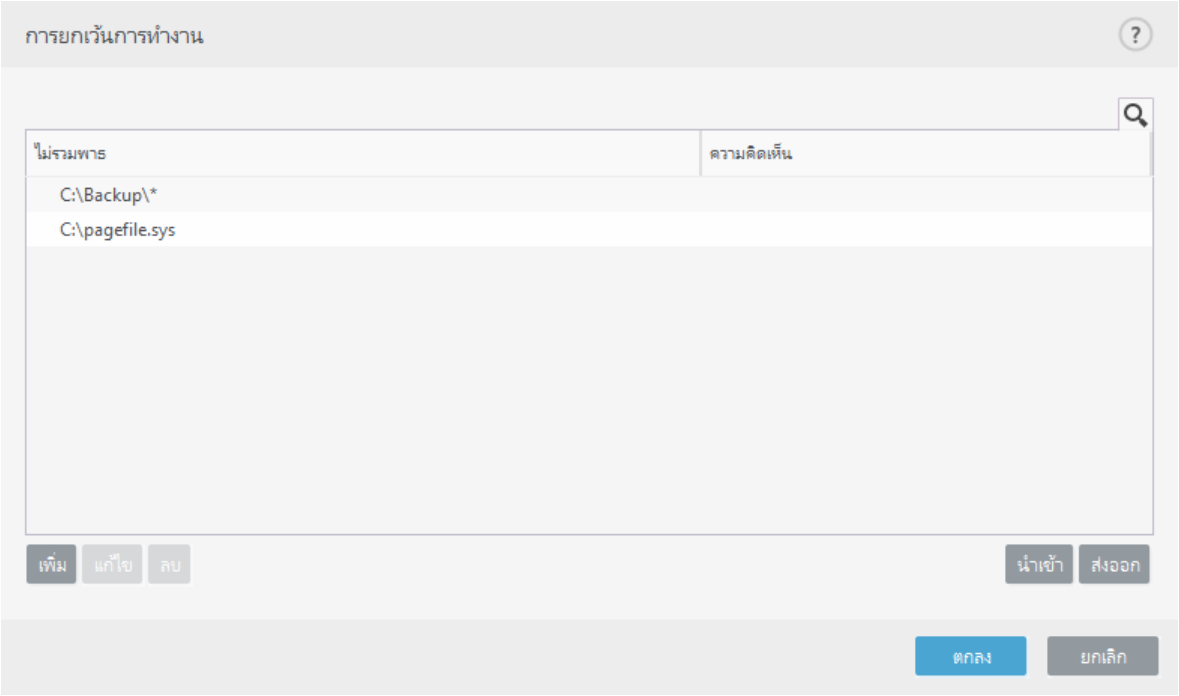
การยกเว้นการทำงาน ช่วยให้คุณยกเว้นไฟล์และโฟลเดอร์จากการสแกน

หากต้องการทำให้แน่ใจว่าจะมีการสแกนวัตถุทั้งหมดเพื่อหาภัยคุกคาม เราขอแนะนำให้สร้างการยกเว้นต่อเมื่อจำเป็นจริงๆ เท่านั้น แต่ยังมีบางสถานการณ์ที่คุณอาจจำเป็นต้องยกเว้นวัตถุ ตัวอย่างเช่น รายการฐานข้อมูลขนาดใหญ่ที่จะทำให้คอมพิวเตอร์ทำงานช้าในระหว่างการสแกนหรือซอฟต์แวร์ที่ขัดแย้งกับการสแกน

คุณสามารถเพิ่มไฟล์และโฟลเดอร์ให้ยกเว้นจากการสแกนในรายการการยกเว้นได้ผ่าน **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจจับ** > **การยกเว้น** > **การยกเว้นการทำงาน** > **แก้ไข**

> อย่าสับสนกับ การยกเว้นการตรวจหา นามสกุลไฟล์ที่ยกเว้น การยกเว้น HIPS หรือ การยกเว้นกระบวนการ

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



โมดูลการป้องกันระบบไฟล์แบบเรียลไทม์ หรือ**โมดูลการสแกนคอมพิวเตอร์** จะไม่สามารถตรวจพบภัยคุกคามภายในไฟล์ได้ถ้าไฟล์ตรงตามเกณฑ์สำหรับการยกเว้นจากการสแกน

องค์ประกอบการควบคุม

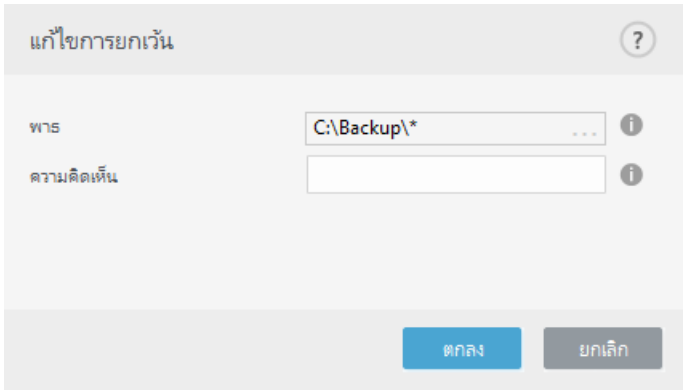
- **เพิ่ม** – ยกเว้นวัตถุจากการตรวจหา
- **แก้ไข** – ช่วยให้คุณสามารถแก้ไขรายการที่เลือกได้
- **ลบ** – ลบรายการต่างๆ ที่เลือกออก (CTRL + คลิกเพื่อเลือกรายการหลายรายการ)

เพิ่มหรือแก้ไขการยกเว้นการทำงาน

หน้าต่างข้อความนี้จะยกเว้นพาธแบบเฉพาะ (ไฟล์หรือไดเรกทอรี) สำหรับคอมพิวเตอร์เครื่องนี้

เลือกพาธหรือป้อนด้วยตัวเอง

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



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

รูปแบบของการยกเว้น

• 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

ตัวแปรของระบบในการยกเว้น

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

ไม่รองรับสัญลักษณ์แทนในช่วงกลางของพาธ

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

คำสั่งของการยกเว้น

- ไม่มีตัวเลือกเพื่อปรับระดับความสำคัญของการยกเว้นที่ใช้ปุ่มบนสุด/ล่างสุด (ซึ่ง กฎของไฟร์วอลล์ ที่กฎถูกเรียกใช้จากบนลงล่าง).
- เมื่อใช้กฎที่สามารถใช้ได้ครั้งแรกตรงกับเครื่องมือสแกน กฎที่สามารถใช้ได้ครั้งที่สองจะไม่ได้รับการประเมิน
- ยิ่งมีกฎน้อย ประสิทธิภาพการสแกนยิ่งดีขึ้น
- หลีกเลี่ยงการสร้างกฎที่ทำพร้อมกัน

รูปแบบของการยกเว้นพาธ

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

รูปแบบของการยกเว้น

- 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

ตัวแปรของระบบในการยกเว้น

คุณสามารถใช้ระบบตัวแปรได้ เช่น %PROGRAMFILES% เพื่อระบุข้อยกเว้นการสแกน

• หากไม่ต้องการรวมโฟลเดอร์ Program Files โดยใช้ระบบตัวแปร ให้ใช้พาธ *%PROGRAMFILES%** (จำไว้ว่าให้เพิ่มเครื่องหมายดั้นหลังและดอกจันที่ด้านหลังสุดของพาธ) 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

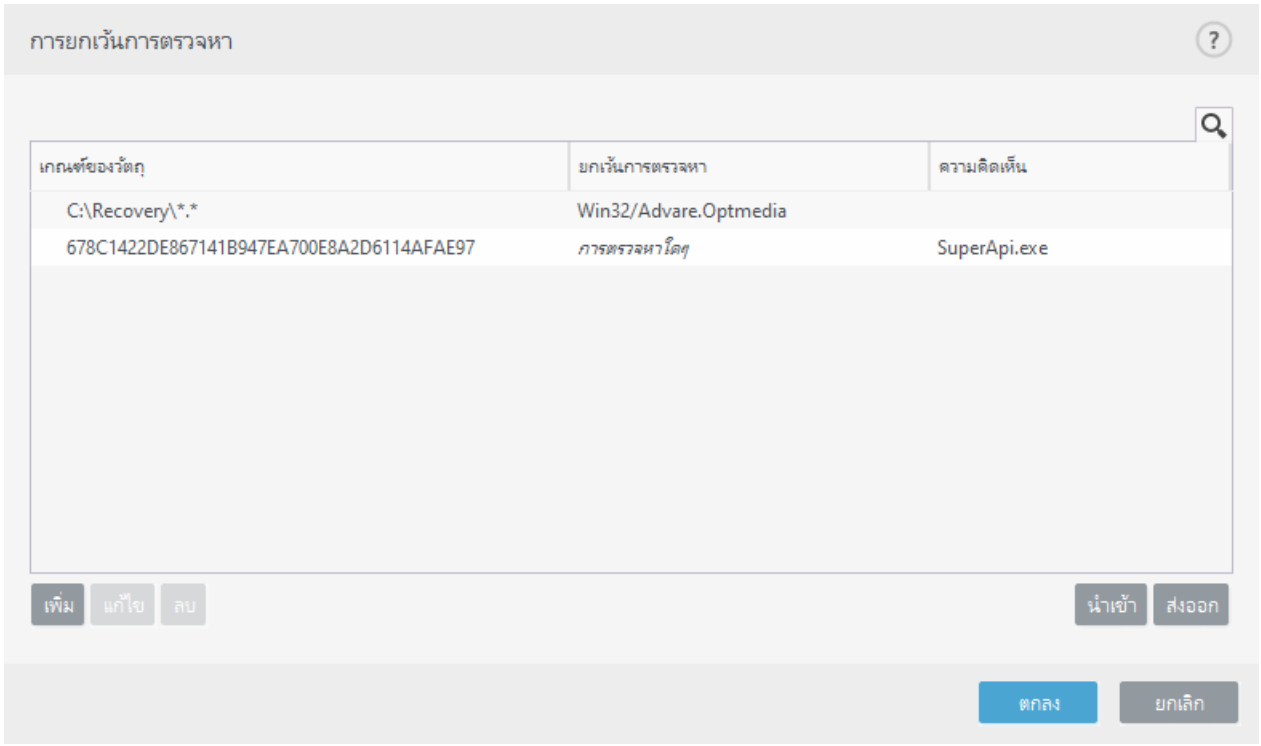
การยกเว้นการตรวจหา

การยกเว้นการตรวจหาช่วยให้คุณยกเว้นวัตถุจากการตรวจจับโดยการกรองชื่อการตรวจหา พาธของวัตถุ หรือแฮช

วิธีการทำงานของการยกเว้นการตรวจหา

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** (F5) > **กลไกการตรวจจับ** > **การยกเว้น** > **การยกเว้นการตรวจหา** > **แก้ไข**

อย่าสับสนกับ การยกเว้นการการทำงาน นามสกุลไฟล์ที่ยกเว้น การยกเว้น HIPS หรือ การยกเว้นกระบวนการ

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

สำหรับ แอพพลิเคชันที่อาจไม่พึงประสงค์ และ แอพพลิเคชันที่อาจไม่ปลอดภัย สามารถสร้างการยกเว้นด้วยชื่อการตรวจจับดังนี้:

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

เกณฑ์การยกเว้นการตรวจหาของวัตถุ

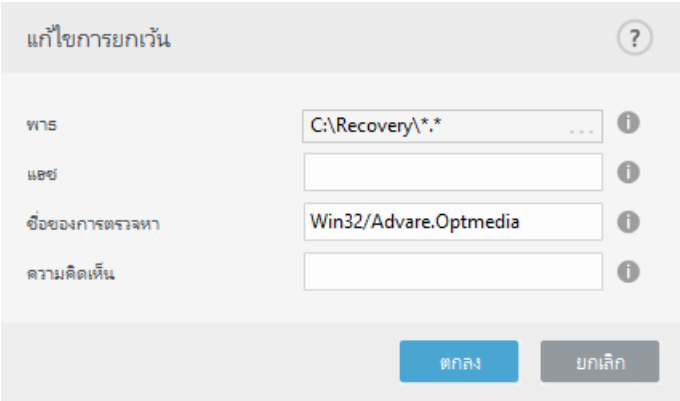
- **พาธ** – จำกัดการยกเว้นการตรวจหาสำหรับพาธเฉพาะ (หรือพาธใดๆ)
- **ชื่อของการตรวจหา** - หากมีชื่อของ การตรวจหา ถัดจากไฟล์ที่ยกเว้น หมายความว่า ไฟล์ดังกล่าวจะถูกยกเว้นสำหรับการตรวจหาที่กำหนดเท่านั้น แต่ไม่ใช่ทั้งหมด หากไฟล์นั้นติดไวรัสมัลแวร์อื่นๆ ในภายหลัง ไฟล์จะถูกตรวจพบ
- **แฮช** – ยกเว้นไฟล์ที่อิงจากแฮชที่ระบุไว้ SHA-1 ไม่ว่าจะเป็นประเภทของไฟล์ ตำแหน่ง ชื่อ หรือส่วนขยายของไฟล์

เพิ่มหรือแก้ไขการยกเว้นการตรวจหา

ยกเว้นการตรวจหา

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

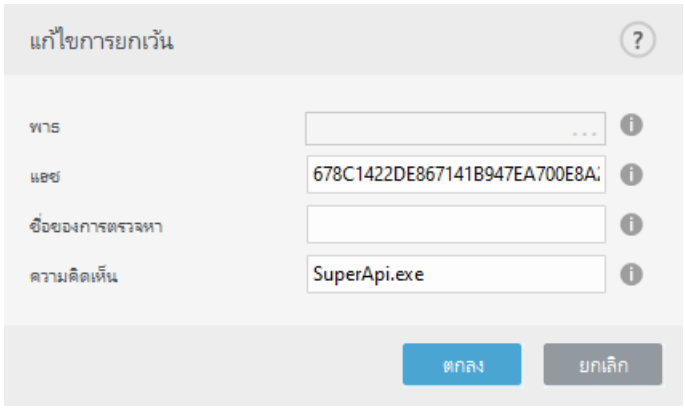
โปรดดู รูปแบบของการยกเว้นพาธ



โปรดดู ตัวอย่างการยกเว้นการตรวจหา ด้านล่าง

ไม่รวมแฮช

ยกเว้นไฟล์ที่อิงจากแฮชที่ระบุไว้ SHA-1 ไม่ว่าจะเป็นประเภทของไฟล์ ตำแหน่ง ชื่อ หรือส่วนขยายของไฟล์



การยกเว้นโดยอิงจากชื่อของการตรวจหา
หากต้องการยกเว้นการตรวจหาโดยอิงจากชื่อ ให้ป้อนชื่อของการตรวจหาที่ถูกต้อง:
Win32/Adware.Optmedia
คุณสามารถใช้รูปแบบต่อไปนี้ได้เมื่อคุณไม่รวมการตรวจหาจากหน้าต่างการเตือนESET Smart Security Premium:
@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):

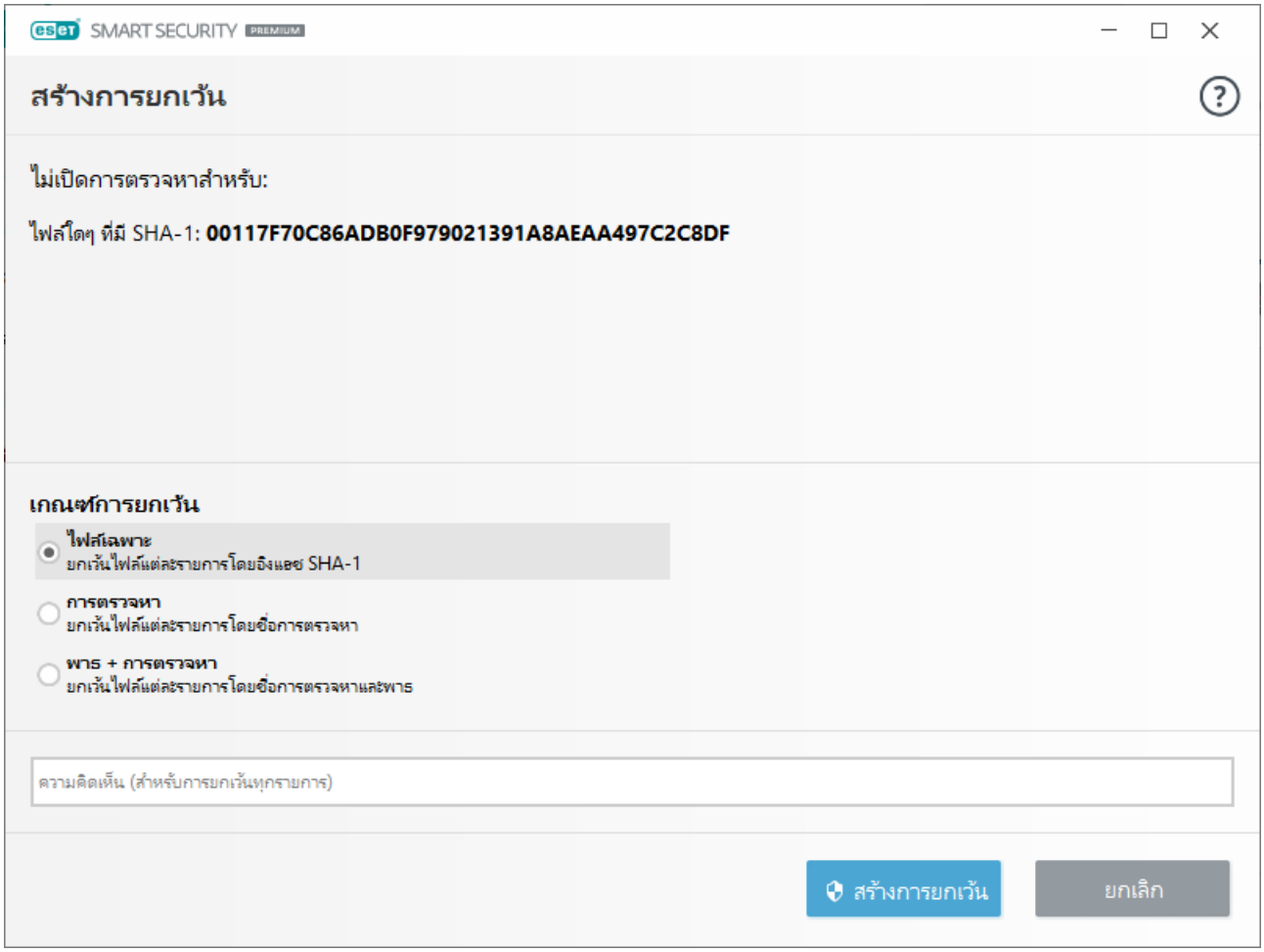
1. ใน หน้าต่างโปรแกรมหลัก ให้คลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก**.
2. คลิกขวาที่การตรวจหาใน **บันทึกการตรวจหา**
3. คลิก **สร้างการยกเว้น**

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



การยกเว้น HIPS

การยกเว้นทำให้คุณยกเว้นกระบวนการต่างๆ จากการตรวจสอบการทำงานเชิงลึกของ HIPS ได้

หากต้องการแก้ไขข้อยกเว้น HIPS ให้ไปยัง **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจจับ** > **HIPS** > **พื้นฐาน** > **การยกเว้น** > **แก้ไข**

อย่าสับสนกับ นามสกุลไฟล์ที่ยกเว้น การตรวจหานามสกุลไฟล์ การยกเว้นการทำงาน หรือ การยกเว้นกระบวนการ

หากต้องการยกเว้นวัตถุ ให้คลิก **เพิ่ม** แล้วป้อนพาธไปยังวัตถุหรือเลือกวัตถุในโครงสร้าง คุณยังสามารถแก้ไขหรือลบรายการที่เลือกไว้ได้

พารามิเตอร์ ThreatSense

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

ตัวเลือกการตั้งค่ากลไก ThreatSense อนุญาตให้คุณระบุพารามิเตอร์การสแกนต่าง ๆ ได้:

- ประเภทไฟล์และนามสกุลที่จะสแกน
- การใช้วิธีการตรวจหาต่างๆ ร่วมกัน
- ระดับการกำจัด เป็นต้น

ในการเข้าสู่หน้าต่างการตั้งค่า ให้คลิก **พารามิเตอร์ ThreatSense** ในหน้าต่างการตั้งค่าขั้นสูงสำหรับโมดูลใดๆ ที่ใช้เทคโนโลยี 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 (แม้จะน้อยมากก็

ตาม)

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

การกำจัด

การตั้งค่าการกำจัด จะเป็นตัวกำหนดการทำงานของ ESET Smart Security Premium ขณะกำจัดวัตถุ การกำจัดมี 4 ระดับ:

พารามิเตอร์ของ ThreatSense มีระดับการปรับปรุงแก้ไข (เช่น การกำจัด) ดังต่อไปนี้

การปรับปรุงแก้ไขใน ESET Smart Security Premium

ระดับการกำจัด	คำอธิบาย
แก้ไขการตรวจหาเสมอ	ให้พยายามปรับปรุงแก้ไขการตรวจหาขณะล้างวัตถุโดยไม่มีการแทรกแซงจากผู้ใช้ปลายทาง ในบางกรณีที่เกิดได้ยาก (ตัวอย่างเช่น ไฟล์ระบบ) หากการตรวจหาไม่สามารถปรับปรุงแก้ไขได้ วัตถุที่รายงานจะถูกทิ้งไว้ในตำแหน่งเดิม แนะนำให้ตั้ง
ปรับปรุงแก้ไขการตรวจหาว่าปลอดภัยหรือไม่ นอกเหนือจากนั้นให้เก็บไว้	การพยายามปรับปรุงแก้ไขการตรวจหาขณะกำจัดวัตถุโดยไม่มีการแทรกแซงจากผู้ใช้ปลายทาง ในบางกรณี (ตัวอย่างเช่น ไฟล์ระบบหรือไฟล์เก็บถาวร ที่มีทั้งไฟล์ที่ไม่ติดและติดไวรัส) หากการตรวจหาไม่สามารถปรับปรุงแก้ไขได้ วัตถุที่รายงานจะถูกทิ้งไว้ในตำแหน่งเดิม
ปรับปรุงแก้ไขการตรวจหาว่าปลอดภัยหรือไม่ นอกเหนือจากนั้นให้ถาม	การพยายามแก้ไขการตรวจหาขณะล้างวัตถุ ในบางกรณี หากไม่มีการกระทำใดสามารถทำได้ ผู้ใช้ปลายทางจะได้รับหน้าต่างโต้ตอบและต้องเลือกการดำเนินการการปรับปรุงแก้ไข (ตัวอย่างเช่น ลบ หรือ เพิกเฉย) แนะนำให้ใช้การตั้งค่านี้ในกรณีทั่วไป
ถามผู้ใช้ปลายทางเสมอ	ผู้ใช้ปลายทางจะได้รับหน้าต่างโต้ตอบขณะล้างวัตถุและต้องเลือกการดำเนินการการปรับปรุงแก้ไข (ตัวอย่างเช่น ลบ หรือ เพิกเฉย) ระดับนี้ได้รับการออกแบบสำหรับผู้ใช้ขั้นสูงขึ้นซึ่งรู้ว่าควรใช้วิธีใดเมื่อมีการตรวจหา

การยกเว้น

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่าพารามิเตอร์ ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะสแกน

อื่นๆ

เมื่อกำหนดค่าพารามิเตอร์กลไก ThreatSenseสำหรับการสแกนคอมพิวเตอร์ 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) ที่ต้องการสแกน ค่าสูงสุดคือ **3 GB**

เราไม่แนะนำให้แก้ไขค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดที่จะต้องแก้ไขค่านี้ในสถานการณ์ปกติ

รายการที่อยู่ที่ยกเว้นจากการตรวจสอบ

นามสกุลไฟล์ที่ได้รับการยกเว้นเป็นส่วนหนึ่งของ พารามิเตอร์ ThreatSense หากต้องการกำหนดค่านามสกุลไฟล์ที่ได้รับการยกเว้น ให้คลิก **พารามิเตอร์ ThreatSense** ในหน้าต่างการตั้งค่าขั้นสูงสำหรับ โมดูลที่ใช้เทคโนโลยี ThreatSense

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่าพารามิเตอร์ 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`).

หากต้องการดูส่วนขยายที่ถูกต้อง (หากมี) ของไฟล์ในระบบปฏิบัติการ Windows คุณต้องยกเลิกการทำเครื่องหมายตัวเลือก **ซ่อนส่วนขยายสำหรับประเภทไฟล์ที่รู้จัก** ที่ (แท็บ) **แผงการควบคุม** > **ตัวเลือกโฟลเดอร์** > **มุมมอง** แล้วใช้การเปลี่ยนแปลงนี้

พารามิเตอร์ ThreatSense เพิ่มเติม

หากต้องการแก้ไขการตั้งค่าเหล่านี้ ให้ไปยัง **การตั้งค่าขั้นสูง** (F5) > **กลไกการตรวจจับ** > **การป้องกันระบบไฟล์แบบเรียลไทม์** > **พารามิเตอร์ ThreatSense เพิ่มเติม**

พารามิเตอร์ ThreatSense เพิ่มเติมสำหรับไฟล์ที่สร้างใหม่และแก้ไข

ไฟล์ที่สร้างใหม่หรือแก้ไขมีความเป็นไปได้ที่จะติดไวรัสมากกว่าไฟล์ที่มีอยู่ ด้วยเหตุผลนี้ โปรแกรมจะตรวจสอบไฟล์เหล่านี้ด้วยพารามิเตอร์การสแกนเพิ่มเติม ESET Smart Security Premium 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 - การวิเคราะห์พฤติกรรมขั้นสูงจะ

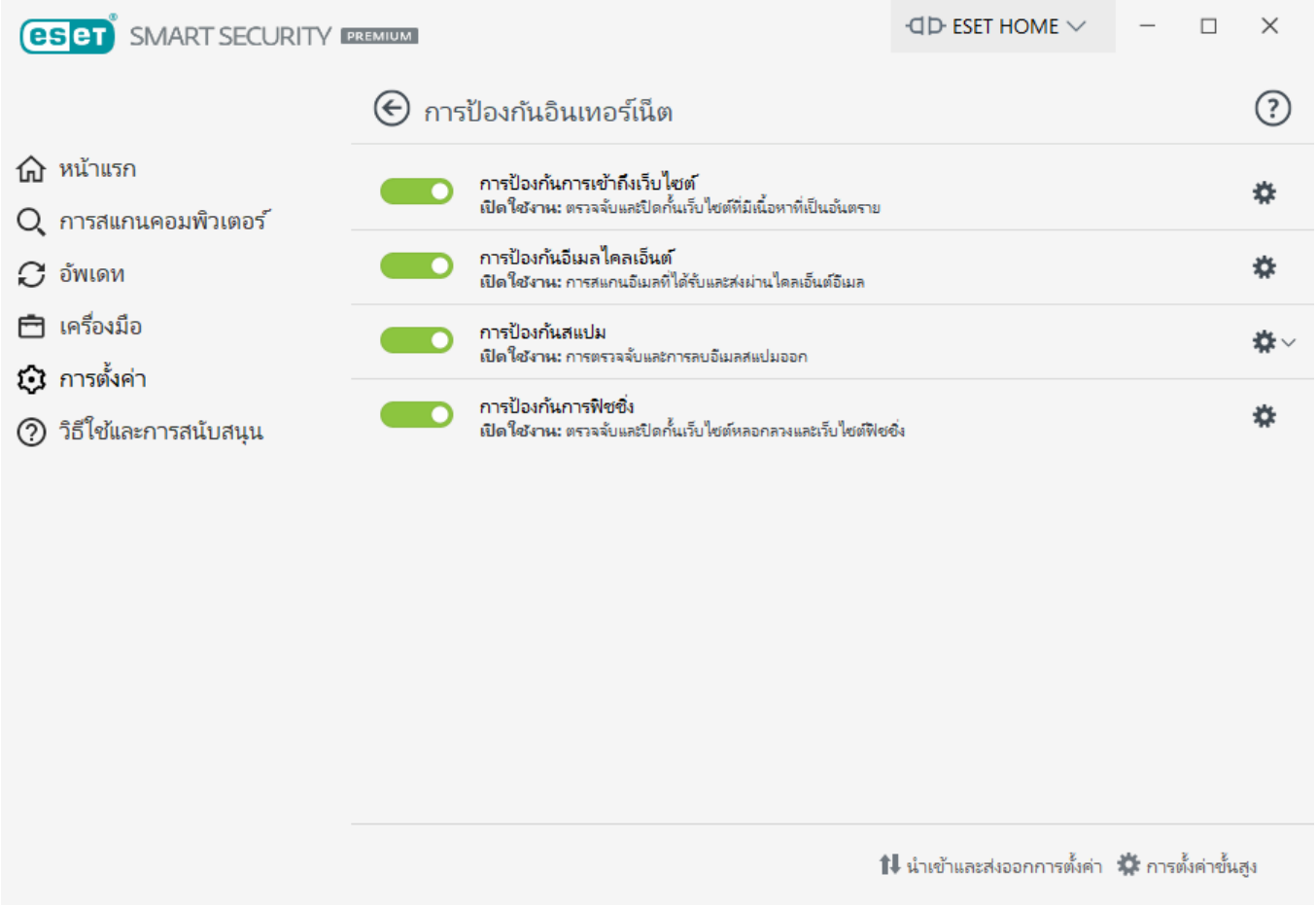
จำลองรหัสในสิ่งแวดล้อมเสมือนและประเมินพฤติกรรมก่อนจะให้อนุญาตให้ใช้งานรหัสจากสื่อที่ถอดออกได้

การป้องกันอินเทอร์เน็ต

หากต้องการกำหนดค่าการป้องกันเว็บและอีเมล ให้คลิก **การป้องกันอินเทอร์เน็ต** ในหน้าต่าง **การตั้งค่า** จากส่วนนี้ คุณสามารถเข้าถึงการตั้งค่าโปรแกรมที่ละเอียดมากขึ้น

หากต้องการหยุดชั่วคราวหรือปิดใช้งานโมดูลการป้องกันแต่ละโมดูล ให้คลิกไอคอนแถบเลื่อน

การปิดโมดูลการป้องกันอาจลดระดับการป้องกันของคอมพิวเตอร์ของคุณ



คลิกที่ไอคอนรูปเฟือง เพื่อเปิดเว็บ/อีเมล/การป้องกันฟิชชิ่ง/การป้องกันสแปม การตั้งค่าการป้องกันในการตั้งค่าขั้นสูง

การเชื่อมต่ออินเทอร์เน็ตเป็นคุณลักษณะมาตรฐานสำหรับคอมพิวเตอร์ส่วนบุคคล แต่น่าเสียดายที่อินเทอร์เน็ตกลายเป็นสื่อหลักสำหรับการกระจายรหัสที่เป็นอันตราย และด้วยเหตุผลนี้ จึงจำเป็นอย่างยิ่งที่คุณจะพิจารณาอย่างรอบคอบถึงการตั้งค่า การป้องกันการเข้าถึงเว็บ ของคุณ

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

การป้องกันฟิชชิ่ง จะกรองข้อความอีเมลที่ไม่พึงประสงค์

สำหรับการ **การป้องกันสแปม** ให้คลิกไอคอนฟันเฟือง ⚙ และเลือกจากตัวเลือกต่อไปนี้:

- **กำหนดค่า** – เปิดการตั้งค่าขั้นสูงสำหรับการป้องกันสแปมของอีเมลไคลเอ็นต์
- **รายการที่อยู่ของผู้ใช้** (หากเปิดใช้งานอยู่) – เปิดหน้าต่างข้อความที่คุณสามารถเพิ่ม แก้ไข หรือลบที่อยู่เพื่อกำหนดกฎการป้องกันสแปมได้ กฎในรายการนี้จะถูกนำไปใช้กับผู้ใช้ปัจจุบัน
- **รายการที่อยู่ร่วม** (หากเปิดใช้งานอยู่) – เปิดหน้าต่างข้อความที่คุณสามารถเพิ่ม แก้ไข หรือลบที่อยู่เพื่อกำหนดกฎการป้องกันสแปมได้ กฎในรายการนี้จะถูกนำไปใช้กับผู้ใช้ทั้งหมด

การป้องกันฟิชชิ่ง อนุญาตให้คุณปิดกั้นหน้าเว็บที่ทราบว่ามีการแจกจ่ายเนื้อหาการฟิชชิ่ง เราขอแนะนำให้คุณเปิดใช้งานการป้องกันฟิชชิ่งทิ้งไว้

การกรองโปรโตคอล

การป้องกันไวรัสสำหรับโปรโตคอลแอพพลิเคชันจะมีให้โดยเครื่องมือสแกน ThreatSense ซึ่งรวมเทคนิคการสแกนมัลแวร์ขั้นสูงทั้งหมดไว้ได้อย่างราบรื่น การกรองโปรโตคอลจะทำงานอัตโนมัติ โดยไม่คำนึงถึงเบราว์เซอร์อินเทอร์เน็ตหรืออีเมลไคลเอ็นต์ที่ใช้ ในการแก้ไขการตั้งค่าที่เข้ารหัส (SSL/TLS) ให้ไปที่ **การตั้งค่าขั้นสูง**(F5) >**เว็บและอีเมล์**> **SSL/TLS**

เปิดใช้การกรองเนื้อหาโปรโตคอลแอพพลิเคชัน – สามารถใช้เพื่อปิดใช้งานการกรองโปรโตคอลได้ โปรดทราบว่าองค์ประกอบ (การป้องกันการเข้าถึงเว็บ, การป้องกันโปรโตคอลอีเมล, การป้องกันฟิชชิ่ง, การควบคุมเนื้อหาเว็บไซต์) จำนวนมากของ ESET Smart Security Premium จะขึ้นอยู่กับส่วนนี้และจะไม่ทำงานถ้าไม่มีการกรอง

แอพพลิเคชันที่ยกเว้น – อนุญาตให้คุณยกเว้นแอพพลิเคชันที่ระบุจากการกรองโปรโตคอล ส่วนนี้จะเป็นประโยชน์เมื่อการกรองโปรโตคอลก่อให้เกิดปัญหาด้านการทำงานร่วมกัน

ที่อยู่ IP ที่ยกเว้น – อนุญาตให้คุณยกเว้นที่อยู่ระยะไกลที่ระบุจากการกรองโปรโตคอล ส่วนนี้จะเป็นประโยชน์เมื่อการกรองโปรโตคอลก่อให้เกิดปัญหาด้านการทำงานร่วมกัน

ส่วนที่เพิ่ม (ตัวอย่างเช่น *2001:718:1c01:16:214:22ff:fec9:ca5*)

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

ตัวอย่างของที่อยู่ IP ที่ไม่รวม

ที่อยู่ IPv4 และมาสก์:

- *192.168.0.10* - เพิ่มที่อยู่ IP ของคอมพิวเตอร์แต่ละเครื่องซึ่งจะใช้กฎ
- *192.168.0.1* ถึง *192.168.0.99* - ป้อนที่อยู่ IP แรกและสุดท้าย เพื่อระบุช่วง IP (ของคอมพิวเตอร์หลายเครื่อง) ซึ่งจะใช้กฎ
- ซับเน็ต (กลุ่มของคอมพิวเตอร์) กำหนดโดยที่อยู่ IP และมาสก์ ตัวอย่างเช่น *255.255.255.0* เป็นมาสก์เครือข่ายสำหรับคำนำหน้า *192.168.1.0/24* ซึ่งหมายถึงช่วงที่อยู่คือ *192.168.1.1* ถึง 192.168.1.254

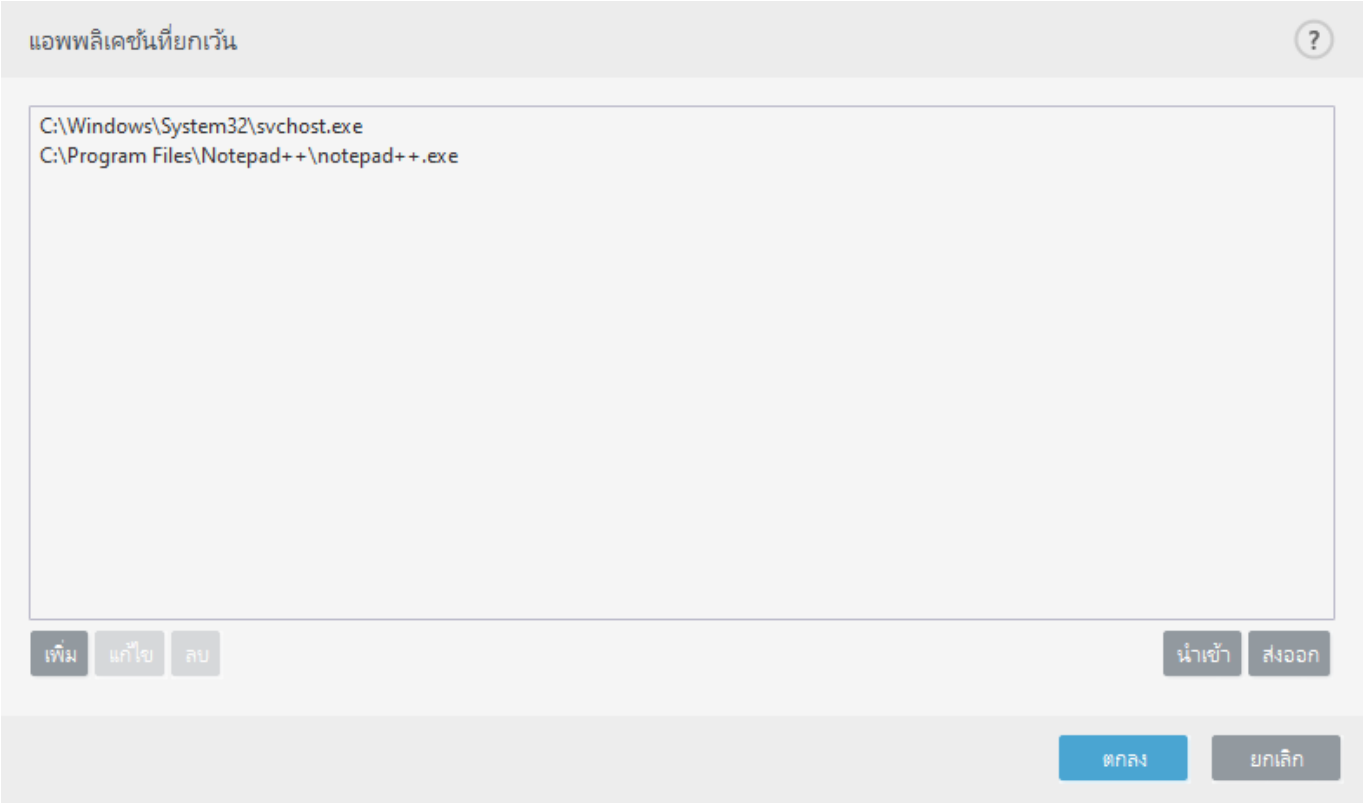
ที่อยู่ IPv6 และมาสก์:

- *2001:718:1c01:16:214:22ff:fec9:ca5* – ที่อยู่ IPv6 ของคอมพิวเตอร์แต่ละเครื่องที่จะใช้กฎ
- *2002:c0a8:6301:1::1/64* – ที่อยู่ IPv6 ที่มีความยาวคำนำหน้า 64 บิต ได้แก่ *2002:c0a8:6301:0001:0000:0000:0000:0000to2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

แอพพลิเคชันที่ยกเว้น

เมื่อต้องการยกเว้นการสื่อสารของแอพพลิเคชันที่ใช้งานเครือข่ายบางรายการจากการกรองเนื้อหา ให้เลือกแอพพลิเคชันในรายการ การสื่อสารของ HTTP/POP3/IMAP ของแอพพลิเคชันที่เลือกจะไม่ได้รับการตรวจสอบเพื่อหาภัยคุกคาม เราขอแนะนำให้ใช้ตัวเลือกนี้เฉพาะสำหรับแอพพลิเคชันที่ทำงานได้อย่างไม่ถูกต้องและการสื่อสารของแอพพลิเคชันเหล่านั้นกำลังถูกตรวจสอบอยู่

แอพพลิเคชันและบริการที่ทำงานอยู่จะสามารถใช้งานได้ที่นี่โดยอัตโนมัติ คลิก **เพิ่ม** เพื่อเพิ่มแอพพลิเคชันด้วยตัวเองหากไม่ปรากฏในรายการการกรองโปรโตคอล



ที่อยู่ IP ที่ไม่รวม

รายการที่อยู่ในรายการจะถูกยกเว้นจากการกรองเนื้อหาโปรโตคอล การสื่อสารของ HTTP/POP3/IMAP จาก/ไปยังที่อยู่ที่เลือกจะไม่ได้รับการตรวจสอบเพื่อหาภัยคุกคาม เราขอแนะนำให้คุณใช้ตัวเลือกนี้เฉพาะสำหรับที่อยู่ที่ทราบว่าเชื่อถือได้เท่านั้น

คลิก **เพิ่ม** เพื่อยกเว้นที่อยู่ IP/ช่วงของที่อยู่/ซับเน็ตของจุดเชื่อมต่อระยะไกลไม่ให้แสดงในรายการการกรองโปรโตคอล

คลิก**ลบออก** เพื่อลบรายการที่เลือกออกจากรายการ

เพิ่มที่อยู่ IPv4

ตัวเลือกนี้อนุญาตให้คุณเพิ่มที่อยู่ IP/ช่วงที่อยู่/ซับเน็ต ให้กับจุดระยะไกลซึ่งมีการใช้กฎ โปรโตคอลอินเทอร์เน็ตเวอร์ชัน 4 เป็นเวอร์ชันเก่า แต่ยังมีการใช้งานอย่างแพร่หลาย

ที่อยู่เดียว - เพิ่มที่อยู่ IP ของคอมพิวเตอร์แต่ละเครื่องซึ่งจะใช้กฎ (ตัวอย่างเช่น *192.168.0.10*)

ช่วงที่อยู่ - ป้อนที่อยู่ IP แรกและสุดท้าย เพื่อระบุช่วง IP (ของคอมพิวเตอร์หลายเครื่อง) ซึ่งจะใช้กฎ (ตัวอย่างเช่น *192.168.0.1* ถึง *192.168.0.99*)

ซับเน็ต - ซับเน็ต (กลุ่มของคอมพิวเตอร์) กำหนดโดยที่อยู่ IP และมาสก์

ตัวอย่างเช่น *255.255.255.0* เป็นมาสก์เครือข่ายสำหรับคำนำหน้า *192.168.1.0/24* ซึ่งหมายถึงช่วงที่อยู่คือ *192.168.1.1* ถึง 192.168.1.254

เพิ่มที่อยู่ IPv6

ตัวเลือกนี้อนุญาตให้คุณเพิ่มที่อยู่/ซับเน็ต IPv6 ของจุดระยะไกลซึ่งมีการใช้กฎ นี่คือเวอร์ชันใหม่สุดของโปรโตคอลอินเทอร์เน็ต และจะใช้แทนเวอร์ชัน 4 ซึ่งเป็นเวอร์ชันเก่า

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

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

SSL/TLS

ESET Smart Security Premium สามารถใช้เพื่อตรวจสอบภัยคุกคามในการสื่อสารที่ใช้โปรโตคอล SSL คุณสามารถใช้โหมดการกรองต่างๆ เพื่อตรวจสอบการสื่อสารที่ป้องกันด้วย SSL ด้วยใบรับรองที่เชื่อถือ ใบรับรองที่ไม่รู้จัก หรือใบรับรองที่ถูกยกเว้นจากการตรวจสอบของการสื่อสารที่ป้องกันด้วย SSL

เปิดใช้งานการกรองโปรโตคอล SSL/TLS – ถ้าปิดใช้งานการกรองโปรโตคอล โปรแกรมจะไม่สแกนการสื่อสารผ่าน SSL

โหมดการกรองโปรโตคอล SSL/TLS สามารถใช้งานได้ในตัวเลือกดังต่อไปนี้:

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

รายการแอพพลิเคชันที่กรอง SSL/TLS สามารถใช้เพื่อปรับแต่งการทำงานของ ESET Smart Security Premium สำหรับบางแอพพลิเคชันได้

รายการของใบรับรองที่รู้จัก อนุญาตให้คุณปรับแต่งพฤติกรรมของ ESET Smart Security Premium สำหรับใบรับรอง SSL บางใบได้

ยกเว้นการสื่อสารกับโดเมนที่เชื่อถือได้ – เมื่อเปิดใช้งาน การสื่อสารกับโดเมนที่เชื่อถือได้จะถูกยกเว้นจากการตรวจสอบ ความน่าเชื่อถือของโดเมนถูกกำหนดโดย Whitelist ในตัว

ปิดกั้นการสื่อสารที่เข้ารหัสโดยใช้โปรโตคอล SSL v2 ที่เลิกใช้แล้ว – โปรแกรมจะปิดกั้นการสื่อสารที่ใช้โปรโตคอล SSL เวอร์ชันก่อนหน้าโดยอัตโนมัติ

ใบรับรองหลัก

เพิ่มใบรับรองหลักลงในเบราว์เซอร์ที่รู้จัก - เพื่อให้การสื่อสาร SSL ทำงานอย่างถูกต้องในเบราว์เซอร์/อีเมลไคลเอ็นต์ของคุณ การเพิ่มใบรับรองหลักสำหรับ ESET ในรายการใบรับรองหลักที่รู้จัก (ผู้เผยแพร่) จึงเป็นสิ่งสำคัญ เมื่อเปิดใช้งาน ESET Smart Security Premium จะเพิ่มใบรับรอง ESET SSL Filter CA ลงในเบราว์เซอร์ที่รู้จักโดยอัตโนมัติ (ตัวอย่างเช่น Opera) สำหรับเบราว์เซอร์ที่ต้องใช้ที่เก็บใบรับรองของระบบ โปรแกรมจะเพิ่มใบรับรองโดยอัตโนมัติ ตัวอย่างเช่น Firefox จะกำหนดค่าการอนุญาต Trust Root ในที่เก็บใบรับรองของระบบโดยอัตโนมัติ

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

ความถูกต้องของใบรับรอง

หากไม่สามารถยืนยันความน่าเชื่อถือของใบรับรองได้ – ในบางกรณี ใบรับรองเว็บไซต์จะไม่สามารถยืนยันได้ด้วยการใช้ที่เก็บของ Trusted Root Certification Authorities (TRCA) ดังนั้นบุคคลหนึ่ง (ตัวอย่างเช่น ผู้ดูแลระบบของเว็บเซิร์ฟเวอร์หรือธุรกิจขนาดเล็ก) ได้ลงชื่อในใบรับรอง และการพิจารณาว่าใบรับรองนี้เชื่อถือได้จะไม่ใช่ความเสี่ยงเสมอไป ธุรกิจขนาดใหญ่ส่วนใหญ่ (เช่น ธนาคาร) ใช้ใบรับรองที่ลงชื่อโดย TRCA หากเลือก **ถามเกี่ยวกับความถูกต้องของใบรับรอง** (ที่เลือกไว้ตามค่าเริ่มต้น) ผู้ใช้จะได้รับข้อความให้เลือกการทำงานที่จะดำเนินการเมื่อมีการสร้างการสื่อสารที่เข้ารหัส คุณสามารถเลือก **ปิดกั้นการสื่อสารที่ใช้ใบรับรอง** เพื่อสิ้นสุดการเชื่อมต่อที่เข้ารหัสไปยังไซต์ที่มีใบรับรองที่ไม่ได้ยืนยันเสมอ

หากใบรับรองเสียหาย – หมายความว่าใบรับรองลงชื่อไม่ถูกต้องหรือเสียหาย ในกรณีนี้ ESET ขอแนะนำให้ให้เลือก **ปิดกั้นการสื่อสารที่ใช้ใบรับรอง** ไว้ หากเลือก **สอบถามเกี่ยวกับความถูกต้องของใบรับรอง** ผู้ใช้จะได้รับข้อความเตือนให้เลือกการดำเนินการที่จะเกิดขึ้นเมื่อมีการสร้างการสื่อสารที่เข้ารหัส

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

ใบรับรอง

เพื่อให้การสื่อสาร SSL ทำงานอย่างถูกต้องในเบราว์เซอร์/อีเมลไคลเอ็นต์ของคุณ จะต้องมีการเพิ่มใบรับรองหลักสำหรับ ESET ในรายการใบรับรองหลักที่รู้จัก (ผู้เผยแพร่) ควรเปิดใช้งาน **เพิ่มใบรับรองหลักในเบราว์เซอร์ที่รู้จัก**

เลือกตัวเลือกนี้เพื่อเพิ่มใบรับรองหลัก ESET ในเบราว์เซอร์ที่รู้จักโดยอัตโนมัติ (ตัวอย่างเช่น Opera และ Firefox) เมื่อต้องการเรียกดูโดยใช้ที่เก็บใบรับรองของระบบ โปรแกรมจะเพิ่มใบรับรองโดยอัตโนมัติ (เช่น Internet Explorer) เมื่อต้องการใช้ใบรับรองกับเบราว์เซอร์ที่ไม่สนับสนุน ให้คลิกที่ **ดูใบรับรอง** > **รายละเอียด** > **คัดลอกไปยังไฟล์...** จากนั้นนำเข้าสู่เบราว์เซอร์ด้วยตนเอง

ในบางกรณีอาจไม่สามารถยืนยันใบรับรองโดยใช้ที่เก็บของ Trusted Root Certification Authorities (เช่น VeriSign) ซึ่งหมายความว่าใบรับรองมีการลงชื่อด้วยตนเองโดยบุคคลหนึ่ง (เช่น ผู้ดูแลระบบของเว็บเซิร์ฟเวอร์หรือบริษัทธุรกิจขนาดเล็ก) และการพิจารณาว่าใบรับรองนี้เชื่อถือได้จะไม่ใช่ความเสี่ยงเสมอ ธุรกิจขนาดใหญ่ส่วนใหญ่ (เช่น ธนาคาร) ใช้ใบรับรองที่ลงชื่อโดย TRCA

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

คุณสามารถเลือก **ปิดกั้นการสื่อสารที่ใช้ใบรับรอง** เพื่อสิ้นสุดการเชื่อมต่อที่เข้ารหัสไปยังไซต์ที่ใช้ใบรับรองที่ไม่ได้ยืนยันเสมอ

ถ้าใบรับรองไม่ถูกต้องหรือเสียหาย หมายความว่าใบรับรองหมดอายุหรือมีการลงชื่อด้วยตนเองไม่ถูกต้อง ในกรณีนี้เราขอแนะนำให้ปิดกั้นการสื่อสารที่ใช้ใบรับรองดังกล่าว

การรับส่งข้อมูลทางเครือข่ายที่เข้ารหัส

ถ้าระบบของคุณได้รับการกำหนดค่าให้ใช้การสแกนโปรโตคอล SSL จะมีหน้าต่างข้อความที่แสดงข้อความให้คุณเลือกการดำเนินการปรากฏขึ้นมาในสองสถานการณ์ นั่นคือ:

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

สถานการณ์ที่สอง หาก **โหมดการกรองโปรโตคอล SSL** ถูกตั้งค่าเป็น **โหมดตอบสนอง** กล่องข้อความของแต่ละเว็บไซต์จะถามว่าจะ **สแกน** หรือ **ละเว้น** การรับส่งข้อมูล บางแอพพลิเคชันตรวจสอบว่าการรับส่งข้อมูล SSL ของตนไม่ได้รับการแก้ไขหรือตรวจสอบจากผู้ใดเลย ในกรณีนี้ ESET Smart Security Premium ต้อง **ละเว้น** การรับส่ง

ข้อมูลดังกล่าวและปล่อยให้แอพพลิเคชันทำงาน

> **ตัวอย่างพร้อมภาพประกอบ**
> บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
> • การแจ้งเตือนใบรับรองในผลิตภัณฑ์ ESET สำหรับใช้งานในบ้าน
> • "การรับส่งข้อมูลทางเครือข่ายที่เข้ารหัส: ใบรับรองที่ไม่เชื่อถือ" จะปรากฏขึ้นเมื่อเยี่ยมชมหน้าเว็บ

ในทั้งสองกรณี ผู้ใช้สามารถเลือกที่จะจดจำการทำงานที่เลือกได้ การทำงานที่บันทึกไว้จะจัดเก็บใน รายการของใบรับรองที่รู้จัก

รายการของใบรับรองที่รู้จัก

รายการของใบรับรองที่รู้จัก สามารถใช้เพื่อปรับแต่งพฤติกรรมของ ESET Smart Security Premium สำหรับใบรับรอง SSL ที่ต้องการ และเพื่อจดจำการดำเนินการที่เลือกหากเลือก **โหมดโต้ตอบ** ใน **โหมดการกรองโปรโตคอล SSL/TLS** สามารถดูและแก้ไขรายการนี้ได้ใน **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **SSL/TLS** > **รายการของใบรับรองที่รู้จัก**

หน้าต่าง **รายการของใบรับรองที่รู้จัก** ประกอบด้วย:

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

รายการแอพพลิเคชันที่กรอง SSL/TLS

รายการแอพพลิเคชันที่กรอง SSL/TLS สามารถใช้เพื่อปรับแต่งพฤติกรรมของ ESET Smart Security Premium สำหรับแอพพลิเคชันบางแอพพลิเคชัน และจดจำการดำเนินการที่เลือกเมื่อ **โหมดการกรองโปรโตคอล SSL/TLS** อยู่ใน **โหมดโต้ตอบ** คุณสามารถดูและแก้ไขรายการนี้ได้ใน **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **SSL/TLS** > **รายการของแอพพลิเคชันที่กรอง SSL/TLS**

หน้าต่าง **รายการของแอพพลิเคชันที่กรอง SSL/TLS** ประกอบด้วย:

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

การป้องกันอีเมลไคลเอ็นต์

ดู การรวม ESET Smart Security Premium เข้ากับอีเมลไคลเอ็นต์ของคุณ เพื่อกำหนดค่าการรวม

การตั้งค่าอีเมลไคลเอ็นต์จะอยู่ใน **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **การป้องกันอีเมลไคลเอ็นต์** > **อีเมลไคลเอ็นต์**

อีเมลไคลเอ็นต์

เปิดใช้งานการปกป้องอีเมลโดยปลั๊กอินไคลเอ็นต์ – เมื่อปิดใช้งาน การป้องกันโดยอีเมลปลั๊กอินไคลเอ็นต์จะปิด

อีเมลที่จะสแกน

เลือกอีเมลที่จะสแกน:

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

> เราขอแนะนำให้คุณเปิดใช้งาน **เปิดใช้งานการปกป้องอีเมลโดยปลั๊กอินไคลเอ็นต์** ไว้ แม้ว่าการรวมจะไม่ได้เปิดใช้งานหรือทำงานอยู่ การสื่อสารทางอีเมลจะยังมีการป้องกันด้วย การกรองโปรโตคอล (IMAP/IMAPS และ POP3/POP3S)

การทำงานที่จะมีการดำเนินการในอีเมลที่ติดไวรัส

ไม่มีการทำงาน – ถ้าเลือกตัวเลือกนี้ โปรแกรมจะระบุสิ่งที่แนบมาที่ติดไวรัส แต่จะคงอีเมลไว้โดยไม่ดำเนินการใดๆ

ลบอีเมล – โปรแกรมจะแจ้งให้ผู้ใช้ทราบเกี่ยวกับการแฝงตัว และลบข้อความ

ย้ายอีเมลไปยังโฟลเดอร์รายการที่ถูกลบ – โปรแกรมจะย้ายอีเมลที่ติดไวรัสไปยังโฟลเดอร์รายการที่ถูกลบโดยอัตโนมัติ

ย้ายอีเมลไปยังโฟลเดอร์ (การกระทำที่เป็นค่าเริ่มต้น) – อีเมลที่ติดไวรัสจะถูกย้ายไปยังโฟลเดอร์ที่ระบุโดยอัต

โนมัติ

โฟลเดอร์ – ระบุโฟลเดอร์แบบกำหนดเองที่คุณต้องการย้ายอีเมลที่ติดไวรัสเมื่อตรวจพบ

การรวมเข้ากับอีเมลไคลเอ็นต์

การรวม ESET Smart Security Premium กับอีเมลไคลเอ็นต์ของคุณจะเพิ่มระดับการป้องกันรหัสที่เป็นอันตรายในข้อความอีเมล หากไคลเอ็นต์อีเมลของคุณได้รับการสนับสนุน การรวมนี้จะสามารถเปิดใช้งานได้ใน ESET Smart Security Premium เมื่อรวมเข้าอีเมลไคลเอ็นต์ของคุณ แถบเครื่องมือของ ESET Smart Security Premium จะถูกแทรกลงในอีเมลไคลเอ็นต์ โดยตรง ซึ่งจะทำให้การป้องกันอีเมลมีประสิทธิภาพมากยิ่งขึ้น การตั้งค่าการรวมจะอยู่ใน **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **การป้องกันอีเมลไคลเอ็นต์** > **การรวมเข้ากับอีเมลไคลเอ็นต์**

อีเมลไคลเอ็นต์ที่ได้รับการสนับสนุนอยู่ในขณะนี้ ได้แก่ Microsoft Outlook, Outlook Express, Windows Mail และ Windows Live Mail การป้องกันอีเมลจะทำงานเป็นปลั๊กอินสำหรับโปรแกรมเหล่านี้ ประโยชน์สำคัญของปลั๊กอินคือการทำงานที่ไม่ขึ้นอยู่กับโปรโตคอลที่ใช้ เมื่ออีเมลไคลเอ็นต์ได้รับข้อความที่เข้ารหัส ระบบจะดำเนินการถอดรหัสและส่งไปยังเครื่องมือสแกนไวรัส โปรดดูบทความฐานความรู้ของ ESET สำหรับรายการอีเมลไคลเอ็นต์ที่สนับสนุนทั้งหมด ตลอดจนเวอร์ชันของอีเมลไคลเอ็นต์เหล่านั้น

ปิดใช้งาน **การปรับการจัดการสิ่งที่แนบมาให้เหมาะสม** และ **การประมวลผลอีเมลไคลเอ็นต์ขั้นสูง** หากคุณพบว่าระบบทำงานช้าลงขณะรับอีเมล

แถบเครื่องมือ Microsoft Outlook

การป้องกัน Microsoft Outlook ทำงานเป็นโมดูลปลั๊กอิน หลังจากติดตั้ง ESET Smart Security Premium ระบบจะเพิ่มแถบเครื่องมือนี้ ซึ่งมีตัวเลือกการป้องกันไวรัส/การป้องกันสแปม ไปยัง Microsoft Outlook:

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

ไม่ใช่สแปม – ทำเครื่องหมายข้อความที่เลือกว่าไม่ใช่สแปม

ที่อยู่สแปม (บัญชีดำ รายการของที่อยู่สแปม) – เพิ่มที่อยู่ของผู้ส่งใหม่ในบัญชีดำ ข้อความทั้งหมดที่ได้รับจากรายการนี้จะถูกจัดเป็นสแปมโดยอัตโนมัติ

โปรดระมัดระวัง การแอบอ้าง – การปลอมแปลงที่อยู่ของผู้ส่งในข้อความอีเมลเพื่อทำให้ผู้รับอีเมลเข้าใจผิดไปอ่านและตอบกลับข้อความนั้น

ที่อยู่ที่เชื่อถือ (บัญชีปลอดภัย รายการของที่อยู่ที่เชื่อถือ) – เพิ่มที่อยู่ของผู้ส่งใหม่ในบัญชีปลอดภัย ข้อความทั้งหมดที่ได้รับจากที่อยู่ในบัญชีปลอดภัยนี้จะไม่ถูกจัดเป็นสแปมโดยอัตโนมัติ

ESET Smart Security Premium – ดับเบิลคลิกที่ไอคอนเพื่อเปิดหน้าต่างหลักของ ESET Smart Security Premium

สแกนข้อความซ้ำ – ช่วยให้คุณสามารถเริ่มต้นการตรวจสอบอีเมลด้วยตนเองได้ คุณสามารถระบุข้อความที่จะตรวจสอบ และคุณสามารถเปิดใช้การสแกนซ้ำอีเมลที่ได้รับ สำหรับข้อมูลเพิ่มเติม โปรดดู การป้องกันอีเมลไคลเอ็นต์

ตั้งค่าเครื่องสแกน – แสดงตัวเลือกการตั้งค่า การป้องกันอีเมลไคลเอ็นต์

ตั้งค่าการป้องกันสแปม – แสดงตัวเลือกการตั้งค่า การป้องกันสแปม

สมุดที่อยู่ – เปิดหน้าต่างการป้องกันสแปม ซึ่งคุณจะสามารถเข้าถึงรายการของที่อยู่ที่ยกเว้น ที่เชื่อถือ และเป็นสแปมได้

แถบเครื่องมือสำหรับ Outlook Express และ Windows Mail

การป้องกัน Outlook Express และ Windows Mail ทำงานเป็นโมดูลปลั๊กอิน หลังจากติดตั้ง ESET Smart Security Premium ระบบจะเพิ่มแถบเครื่องมือนี้ ซึ่งมีตัวเลือกการป้องกันไวรัส/การป้องกันสแปม ไปยัง Outlook Express หรือ Windows Mail:

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

ไม่ใช่สแปม – ทำเครื่องหมายข้อความที่เลือกว่าไม่ใช่สแปม

ที่อยู่สแปม – เพิ่มที่อยู่ของผู้ส่งใหม่ใน บัญชีดำ ข้อความทั้งหมดที่ได้รับจากรายการนี้จะถูกจัดเป็นสแปมโดยอัตโนมัติ

โปรดระมัดระวัง การแอบอ้าง – การปลอมแปลงที่อยู่ของผู้ส่งในข้อความอีเมลเพื่อทำให้ผู้รับอีเมลเข้าใจผิดไปอ่านและตอบกลับข้อความนั้น

ที่อยู่ที่เชื่อถือ – เพิ่มที่อยู่ของผู้ส่งใหม่ในบัญชีปลอดภัย ข้อความทั้งหมดที่ได้รับจากที่อยู่ในบัญชีปลอดภัยนี้จะไม่ถูกจัดเป็นสแปมโดยอัตโนมัติ

ESET Smart Security Premium – ดับเบิลคลิกที่ไอคอนเพื่อเปิดหน้าต่างหลักของ ESET Smart Security Premium

สแกนข้อความซ้ำ – ช่วยให้คุณสามารถเริ่มต้นการตรวจสอบอีเมลด้วยตนเองได้ คุณสามารถระบุข้อความที่จะตรวจสอบ และคุณสามารถเปิดใช้การสแกนซ้ำอีเมลที่ได้รับ สำหรับข้อมูลเพิ่มเติม โปรดดู การป้องกันอีเมลไคลเอ็นต์

ตั้งค่าเครื่องสแกน – แสดงตัวเลือกการตั้งค่า การป้องกันอีเมลไคลเอ็นต์

ตั้งค่าการป้องกันสแปม – แสดงตัวเลือกการตั้งค่า การป้องกันสแปม

ส่วนติดต่อผู้ใช้

ปรับแต่งการใช้งาน – คุณสามารถปรับแต่งการใช้งานของแถบเครื่องมือสำหรับอีเมลไคลเอ็นต์ของคุณได้ ยกเลิกการเลือกตัวเลือกเพื่อปรับแต่งลักษณะที่ปรากฏโดยไม่ขึ้นอยู่กับพารามิเตอร์ของโปรแกรมอีเมล

แสดงข้อความ – แสดงคำอธิบายไอคอนต่างๆ

ข้อความอยู่ทางขวา – คำอธิบายตัวเลือกถูกย้ายจากด้านล่างสุดไปยังด้านขวาของไอคอน

ไอคอนขนาดใหญ่ – แสดงไอคอนขนาดใหญ่สำหรับตัวเลือกเมนู

ข้อความยืนยัน

การแจ้งเตือนนี้จะทำหน้าที่ตรวจสอบว่าผู้ใช้ต้องการดำเนินการที่เลือกจริงหรือไม่ ซึ่งจะช่วยป้องกันการดำเนินการผิดพลาดได้

แต่ในหน้าต่างข้อความนี้จะมีตัวเลือกเพื่อปิดใช้การยืนยันอยู่ด้วย

สแกนข้อความซ้ำ

แถบเครื่องมือของ ESET Smart Security Premium ที่รวมอยู่ในอีเมลไคลเอ็นต์จะช่วยให้ผู้ใช้สามารถระบุตัวเลือกต่างๆ สำหรับการตรวจสอบอีเมลได้ ตัวเลือก **สแกนข้อความซ้ำ** มีโหมดการสแกนอยู่สองโหมด:

ข้อความทั้งหมดในโฟลเดอร์ปัจจุบัน – สแกนข้อความในโฟลเดอร์ที่แสดงอยู่ในปัจจุบัน

เฉพาะข้อความที่เลือก – สแกนเฉพาะข้อความที่ผู้ใช้ทำเครื่องหมายเท่านั้น

ช่องทำเครื่องหมาย **สแกนข้อความที่สแกนแล้วซ้ำ** จะมีตัวเลือกให้ผู้ใช้สามารถเรียกใช้การสแกนข้อความที่ได้สแกนแล้วก่อนหน้านี้

ส่งอีเมลโปรโตคอล

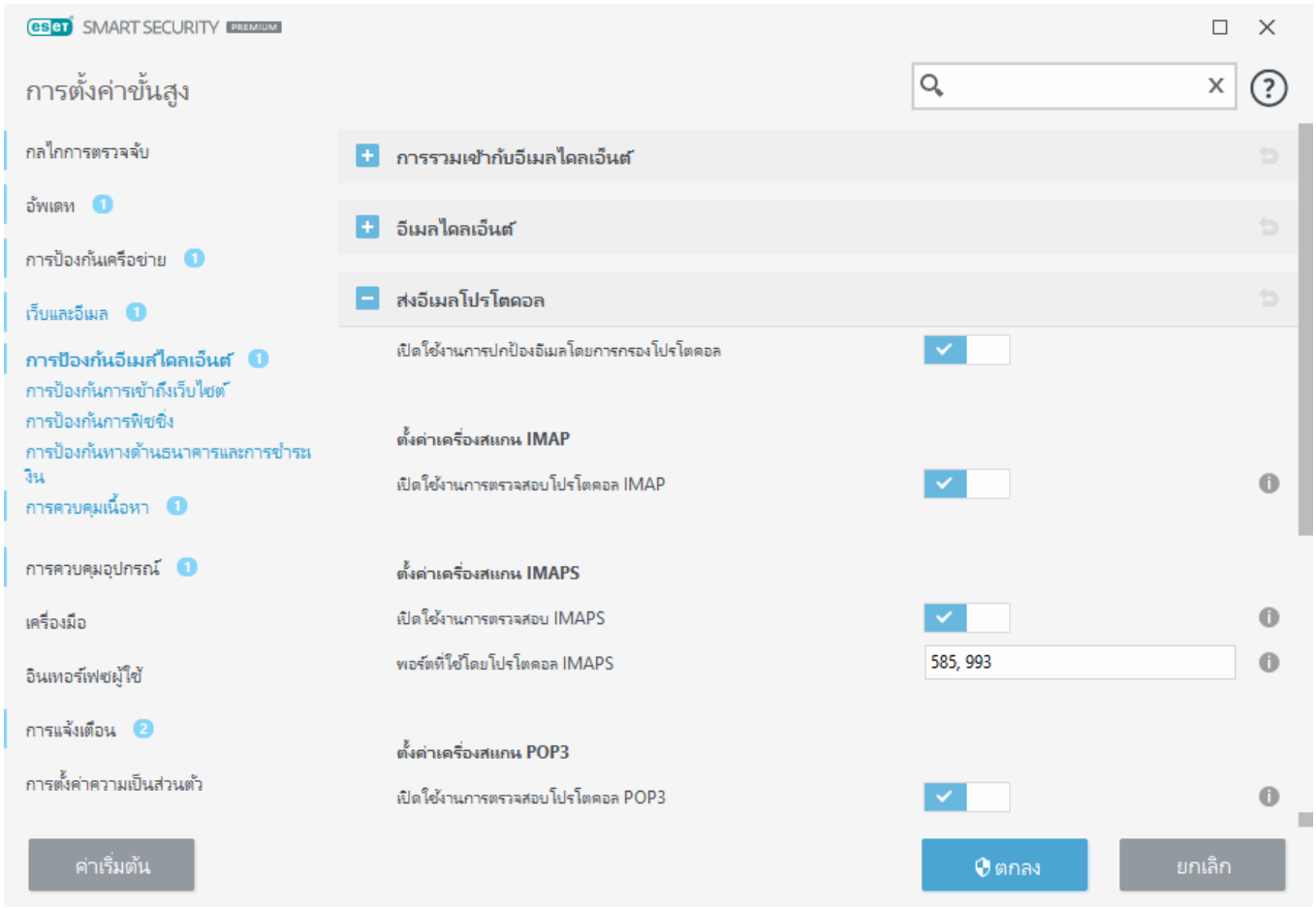
โปรโตคอล IMAP และ POP3 เป็นโปรโตคอลที่ใช้งานกันอย่างแพร่หลาย เพื่อรับการสื่อสารทางอีเมลในแอพพลิเคชันอีเมลไคลเอ็นต์ Internet Message Access Protocol (IMAP) เป็นโปรโตคอลอินเทอร์เน็ตหนึ่งสำหรับการเรียกคืนอีเมล IMAP มีข้อได้เปรียบบางอย่างที่เหนือกว่า POP3 ตัวอย่างเช่น หลายไคลเอ็นต์สามารถเชื่อมต่อพร้อมกันได้ในกล่องจดหมายเดียวกัน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

ESET Smart Security Premium มีการป้องกันโปรโตคอลเหล่านี้ โดยไม่พิจารณาถึงอีเมลไคลเอ็นต์ที่ใช้ และไม่ได้กำหนดให้ต้องกำหนดค่าอีเมลไคลเอ็นต์อีกครั้ง ตามค่าเริ่มต้น การติดต่อสื่อสารผ่านโปรโตคอล POP3 และ IMAP ทั้งหมดจะถูกสแกน โดยไม่คำนึงถึงค่าเริ่มต้นหมายเลขพอร์ต POP3/IMAP
โปรโตคอล IMAP ไม่ถูกสแกน อย่างไรก็ตาม การสื่อสารกับเซิร์ฟเวอร์ Microsoft Exchange สามารถสแกนได้โดยใช้ โมดูลการรวม ในอีเมลไคลเอ็นต์ เช่น Microsoft Outlook

เราขอแนะนำให้เปิดใช้งาน **เปิดใช้งานการป้องกันอีเมลโดยการกรองโปรโตคอล** ไว้ ในการกำหนดค่า IMAP/IMAPS และตรวจสอบโปรโตคอล POP3/POP3S ให้ไปที่ **การตั้งค่าขั้นสูง** > **เว็บและอีเมล** > **การป้องกันอีเมลไคลเอ็นต์** > **โปรโตคอลอีเมล**

ESET Smart Security Premium ยังสนับสนุนการสแกนโปรโตคอล IMAPS (585, 993) และ POP3S (995) ที่จะใช้ช่องทางที่เข้ารหัสเพื่อโอนข้อมูลระหว่างเซิร์ฟเวอร์กับไคลเอ็นต์ ESET Smart Security Premium จะตรวจสอบการสื่อสารโดยใช้โปรโตคอล SSL (Secure Socket Layer) และ TLS (Transport Layer Security) โปรแกรมจะสแกนเฉพาะการรับส่งในพอร์ตที่กำหนดใน **พอร์ตที่ใช้งานโดยโปรโตคอล IMAPS/POP3S** โดยไม่คำนึงถึงเวอร์ชันของระบบปฏิบัติการ สามารถเพิ่มพอร์ตการสื่อสารอื่นๆ ได้หากจำเป็น หมายเลขพอร์ตหลายพอร์ตจะต้องคั่นด้วยเครื่องหมายจุลภาค

การสื่อสารที่เข้ารหัสจะถูกสแกนตามค่าเริ่มต้น หากต้องการดูการตั้งค่าเครื่องมือสแกน ให้เปิดการตั้งค่าขั้นสูง > **เว็บและอีเมล์** > **SSL/TLS**



ตัวกรอง POP3, POP3S

โปรโตคอล POP3 เป็นโปรโตคอลที่มีการใช้งานอย่างแพร่หลายมากที่สุด โดยใช้เพื่อรับการสื่อสารทางอีเมลในแอพพลิเคชันของอีเมลไคลเอ็นต์ ESET Smart Security Premium มีการป้องกันสำหรับโปรโตคอลนี้ โดยไม่คำนึงถึงอีเมลไคลเอ็นต์ที่ใช้งาน

โมดูลการป้องกันที่มีการควบคุมนี้จะเริ่มต้นโดยอัตโนมัติเมื่อเริ่มต้นระบบ จากนั้นจะมีสถานะใช้งานในหน่วยความจำ เพื่อให้โมดูลทำงานอย่างถูกต้อง โปรดตรวจสอบว่ามีการเปิดใช้งานอยู่ การตรวจสอบโปรโตคอล POP3 จะทำงานโดยอัตโนมัติ โดยไม่ต้องมีการกำหนดค่าอีเมลไคลเอ็นต์ใหม่ โดยปกติ โปรแกรมจะสแกนการสื่อสารทั้งหมดในพอร์ต 110 แต่คุณสามารถเพิ่มพอร์ตการสื่อสารอื่นได้หากจำเป็น เลขที่พอร์ตหลายเลขที่ต้องคั่นด้วยเครื่องหมายคอมมา

การสื่อสารที่เข้ารหัสจะถูกสแกนตามค่าเริ่มต้น หากต้องการดูการตั้งค่าเครื่องมือสแกน ให้เปิดการตั้งค่าขั้นสูง > **เว็บและอีเมล์** > SSL/TLS

ในส่วนนี้ คุณสามารถกำหนดค่าการตรวจสอบโปรโตคอล POP3 และ POP3S

เปิดใช้งานการตรวจสอบโปรโตคอล POP3 - หากเปิดใช้งานตัวเลือกนี้ ระบบจะตรวจสอบการรับส่งข้อมูลทั้งหมดผ่าน POP3 เพื่อหาซอฟต์แวร์ที่เป็นอันตราย

พอร์ตที่ใช้งานโดยโปรโตคอล POP3 - รายการพอร์ตที่ใช้งานโดยโปรโตคอล POP3 (110 เป็นค่าเริ่มต้น)

ESET Smart Security Premium สนับสนุนการตรวจสอบโปรโตคอล POP3S ด้วย การสื่อสารประเภทนี้จะใช้ช่องทางที่เข้ารหัส เพื่อโอนข้อมูลระหว่างเซิร์ฟเวอร์กับไคลเอ็นต์ ESET Smart Security Premium จะตรวจสอบการสื่อสารโดยใช้วิธีการเข้ารหัส SSL (Secure Socket Layer) และ TLS (Transport Layer Security)

ไม่ใช้การตรวจสอบ POP3S - โปรแกรมจะไม่ตรวจสอบการสื่อสารที่เข้ารหัส

ใช้การตรวจสอบโปรโตคอล POP3S สำหรับพอร์ตที่เลือก - เลือกตัวเลือกนี้เพื่อเปิดใช้การตรวจสอบ POP3S เฉพาะสำหรับพอร์ตที่กำหนดใน **พอร์ตที่ใช้งานโดยโปรโตคอล POP3S**

พอร์ตที่ใช้งานโดยโปรโตคอล POP3S - รายการพอร์ต POP3S ที่จะตรวจสอบ (995 เป็นค่าเริ่มต้น)

แท็กอีเมล

ตัวเลือกสำหรับฟังก์ชันนี้สามารถใช้ได้ผ่าน **การตั้งค่าขั้นสูง** ภายใต้ **เว็บและอีเมล** > **การป้องกันอีเมลไคลเอ็นต์** > **การเตือนและการแจ้งเตือน**

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

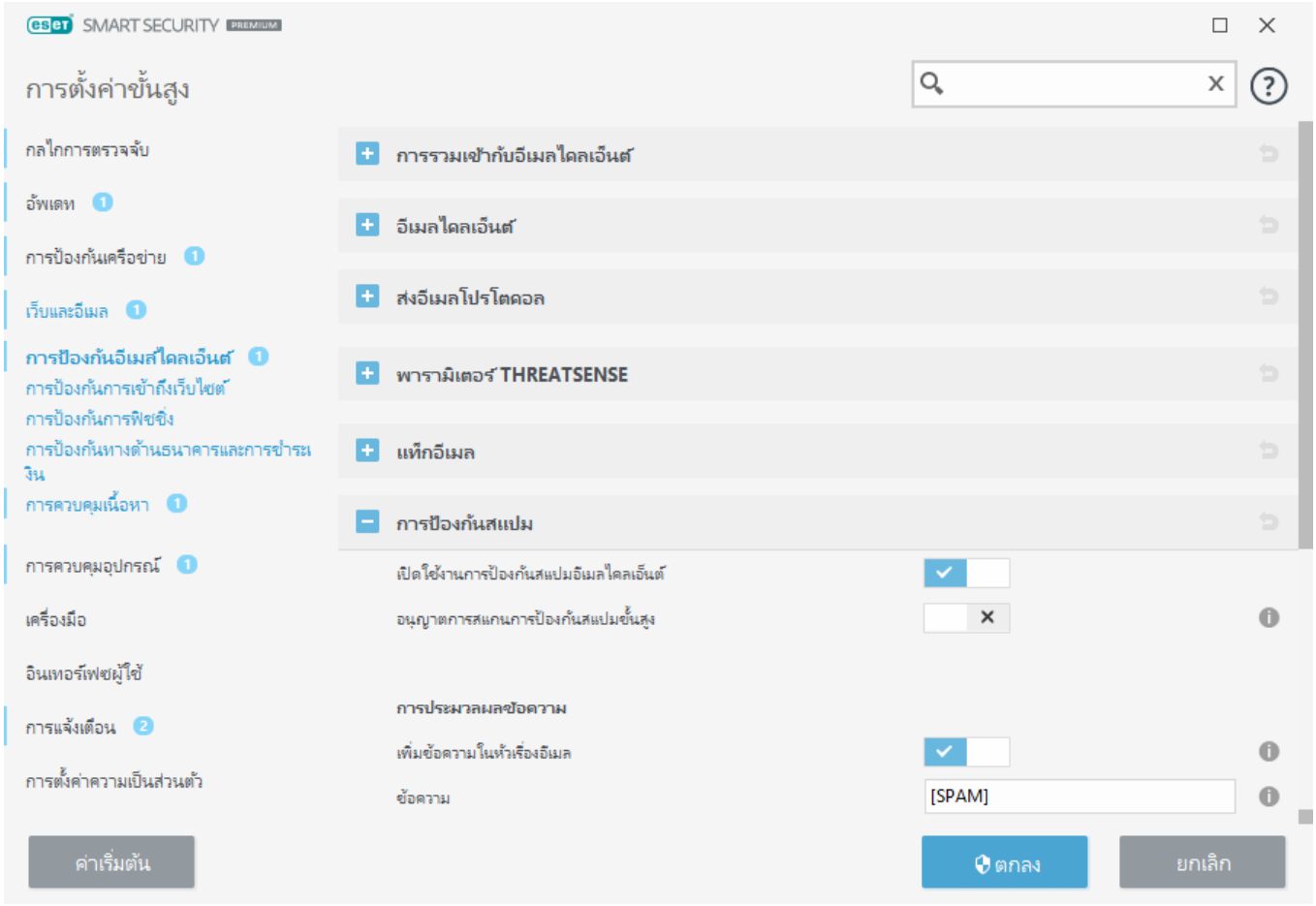
- **ไม่** - ไม่มีการเพิ่มข้อความแท็ก
- **เมื่อการตรวจหาเกิดขึ้น** – โปรแกรมจะทำเครื่องหมายเฉพาะข้อความที่มีซอฟต์แวร์ที่เป็นอันตรายว่าตรวจสอบแล้ว (ค่าเริ่มต้น)
- **ไปยังอีเมลทุกฉบับเมื่อสแกน** – โปรแกรมจะเพิ่มข้อความต่อท้ายอีเมลที่สแกนทั้งหมด

ข้อความที่จะเพิ่มลงในหัวเรื่องของอีเมลที่ตรวจพบ – แก้ไขแม่แบบนี้หากคุณต้องการแก้ไขรูปแบบคำนำหน้าของหัวเรื่องของอีเมลที่ติดไวรัส ฟังก์ชันนี้จะแทนที่หัวเรื่องของความ "สวัสดี" ด้วยรูปแบบต่อไปนี้: "สวัสดี [ชื่อการ

ตรวจพบไวรัส]" ตัวแปร %DETECTIONNAME% จะแสดงแทนการตรวจหา

การป้องกันสแปม

อีเมลที่ไม่พึงประสงค์ หรือสแปม จัดเป็นปัญหาการสื่อสารทางอิเล็กทรอนิกส์ลำดับต้นๆ โดยมีสัดส่วนร้อยละ 30 ของการสื่อสารทางอีเมลทั้งหมด การป้องกันสแปมจะช่วยป้องกันปัญหานี้ โมดูลป้องกันสแปมเป็นการกรองข้อมูลที่มีประสิทธิภาพ เพื่อทำให้กล่องขาเข้ามีความปลอดภัย เนื่องจากรวมหลักการต่างๆ ของการรักษาความปลอดภัยอีเมลไว้ด้วยกัน เมื่อต้องการกำหนดค่าการป้องกันสแปม ให้เปิด **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **การป้องกันอีเมลไคลเอ็นต์** > **การป้องกันสแปม**



สำหรับการตรวจหาสแปม หลักการสำคัญอย่างหนึ่งคือการจดจำอีเมลที่ไม่พึงประสงค์จากที่อยู่ที่เชื่อถือ (อนุญาตแล้ว) และที่อยู่สแปม (บล็อกแล้ว) ที่กำหนดไว้ล่วงหน้า

วิธีหลักที่ใช้เพื่อตรวจหาสแปมคือ การสแกนคุณสมบัติของข้อความอีเมล ระบบจะสแกนข้อความที่ได้รับตามเกณฑ์การป้องกันสแปมขั้นพื้นฐาน (การกำหนดข้อความ, การวิเคราะห์พฤติกรรมแบบสถิติ อัลกอริทึมในการรับรู้ และวิธีเฉพาะอื่นๆ) และค่าดัชนีผลลัพธ์จะเป็นตัวกำหนดว่าข้อความเป็นสแปมหรือไม่

เปิดใช้งานการป้องกันสแปมอีเมลไคลเอ็นต์ – เมื่อเปิดใช้งาน การป้องกันสแปมจะเปิดใช้งานโดยอัตโนมัติเมื่อเริ่มต้นระบบ

อนุญาตการสแกนการป้องกันสแปมขั้นสูง – ข้อมูลต่อต้านสแปมเพิ่มเติมจะถูกดาวน์โหลดเป็นระยะ ซึ่งจะเพิ่มความสามารถในการต่อต้านสแปมและให้ผลลัพธ์ที่ดียิ่งขึ้น

การป้องกันสแปมใน ESET Smart Security Premium จะทำให้คุณสามารถตั้งค่าพารามิเตอร์ต่างๆ สำหรับข้อความได้

การประมวลผลข้อความ

เพิ่มข้อความในหัวเรื่องอีเมล – ช่วยให้คุณสามารถเพิ่มสตริงคำนำหน้าที่กำหนดเองในบรรทัดหัวเรื่องของข้อความซึ่งจัดประเภทว่าเป็นสแปม ค่าเริ่มต้นคือ "[SPAM]"

ย้ายข้อความไปยังโฟลเดอร์สแปม – เมื่อเปิดใช้งาน ข้อความสแปมจะถูกย้ายไปยังโฟลเดอร์อีเมลขยะเริ่มต้นและข้อความที่จัดประเภทใหม่ว่าไม่ใช่สแปมจะถูกย้ายไปที่กล่องข้อความเข้าอีกด้วย เมื่อคุณคลิกขวาที่ข้อความอีเมลและเลือก ESET Smart Security Premium จากเมนูบริบท คุณจะสามารถเลือกจากตัวเลือกที่มีผลบังคับใช้

ใช้โฟลเดอร์ – ระบุโฟลเดอร์แบบกำหนดเองที่คุณต้องการย้ายอีเมลที่ติดไวรัสเมื่อตรวจพบ

ทำเครื่องหมายข้อความสแปมว่าอ่านแล้ว – เปิดใช้งานตัวเลือกนี้เพื่อทำเครื่องหมายสแปมว่าอ่านแล้วโดยอัตโนมัติ การทำเช่นนี้จะช่วยให้คุณให้ความสนใจกับข้อความที่ "ไม่ติดไวรัส" เท่านั้น

ทำเครื่องหมายข้อความที่จัดประเภทใหม่ว่ายังไม่ได้อ่าน – ข้อความเดิมที่จัดประเภทเป็นสแปม แต่ทำเครื่องหมายว่า "ไม่ติดไวรัส" ในภายหลัง จะแสดงเป็นข้อความที่ยังไม่ได้อ่าน

การบันทึกคะแนนสแปม – กลไกการป้องกันสแปมของ ESET Smart Security Premium จะระบุคะแนนสแปมไปที่ข้อความที่สแกนแล้วทุกข้อความ โดยข้อความจะถูกบันทึกไว้ใน บันทึกการป้องกันสแปม (หน้าต่างโปรแกรมหลัก > **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก** > **การป้องกันสแปม**)

- **ไม่มี** – คะแนนจากการสแกนเพื่อป้องกันสแปมจะไม่ถูกบันทึก
- **จัดประเภทใหม่และทำเครื่องหมายว่าเป็นสแปม** – เลือกตัวเลือกนี้ถ้าคุณต้องการบันทึกคะแนนสแปมสำหรับข้อความที่ทำเครื่องหมายว่าเป็น SPAM.
- **ทั้งหมด** - ข้อความทั้งหมดจะได้รับการบันทึกไปที่บันทึกพร้อมด้วยคะแนนสแปม

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

ESET Smart Security Premium สนับสนุนการป้องกันสแปมสำหรับ Microsoft Outlook, Outlook Express, Windows Mail และ Windows Live Mail

ผลการประมวลผลที่อยู่

เมื่อเพิ่มที่อยู่ใหม่หรือเปลี่ยนการทำงานที่ใช้สำหรับที่อยู่อีเมล ESET Smart Security Premium จะแสดงข้อความแจ้งเตือน เนื้อหาของข้อความการแจ้งเตือนจะแตกต่างกันไปตามการดำเนินการของคุณ

เลือกกล่องกาเครื่องหมาย **ไม่ต้องถามอีก** เพื่อดำเนินการอัตโนมัติโดยไม่ต้องแสดงข้อความในครั้งถัดไป

รายการที่อยู่การป้องกันสแปม

คุณลักษณะป้องกันสแปมใน ESET Smart Security Premium ช่วยให้คุณสามารถกำหนดค่าพารามิเตอร์ต่างๆ สำหรับรายการที่อยู่

เปิดใช้งานรายการที่อยู่ของผู้ใช้ – เปิดใช้งานตัวเลือกนี้เพื่อเปิดใช้งานรายการที่อยู่ของผู้ใช้

รายการที่อยู่ของผู้ใช้ – รายการที่อยู่อีเมลที่คุณสามารถเพิ่ม แก้ไข หรือลบที่อยู่เพื่อกำหนดกฎการป้องกันสแปมได้ กฎในรายการนี้จะถูกนำไปใช้กับผู้ใช้ปัจจุบัน

เปิดใช้งานรายการที่อยู่ร่วม – เปิดใช้งานตัวเลือกนี้เพื่อเปิดใช้งานรายการที่อยู่ร่วมซึ่งใช้ร่วมกันโดยผู้ใช้ทั้งหมดในอุปกรณ์เครื่องนี้

รายการที่อยู่ร่วม – รายการที่อยู่อีเมลที่คุณสามารถเพิ่ม แก้ไข หรือลบที่อยู่เพื่อกำหนดกฎการป้องกันสแปมได้ กฎในรายการนี้จะถูกนำไปใช้กับผู้ใช้ทั้งหมด

อนุญาตและเพิ่มไปยังรายการที่อยู่ของผู้ใช้โดยอัตโนมัติ

ถือว่าที่อยู่ต่างๆ จากสมุดที่อยู่เป็นแบบเชื่อถือได้ - ที่อยู่จากรายการติดต่อของคุณจะถือว่าเชื่อถือได้โดยไม่มีการเพิ่มลงในรายการที่ผู้ใช้อนุญาต

เพิ่มที่อยู่ของผู้รับจากข้อความขาออก – เพิ่มที่อยู่ของผู้รับจากข้อความที่ส่งไปยังรายการที่อยู่ของผู้ใช้เป็นอนุญาตแล้ว

เพิ่มที่อยู่จากข้อความที่จัดประเภทใหม่ว่าไม่ใช่สแปม – เพิ่มที่อยู่ของผู้ส่งจากข้อความที่จัดประเภทใหม่ว่า

ไม่ใช่สแปมไปยังรายการที่อยู่ของผู้ใช้เป็น อนุญาตแล้ว

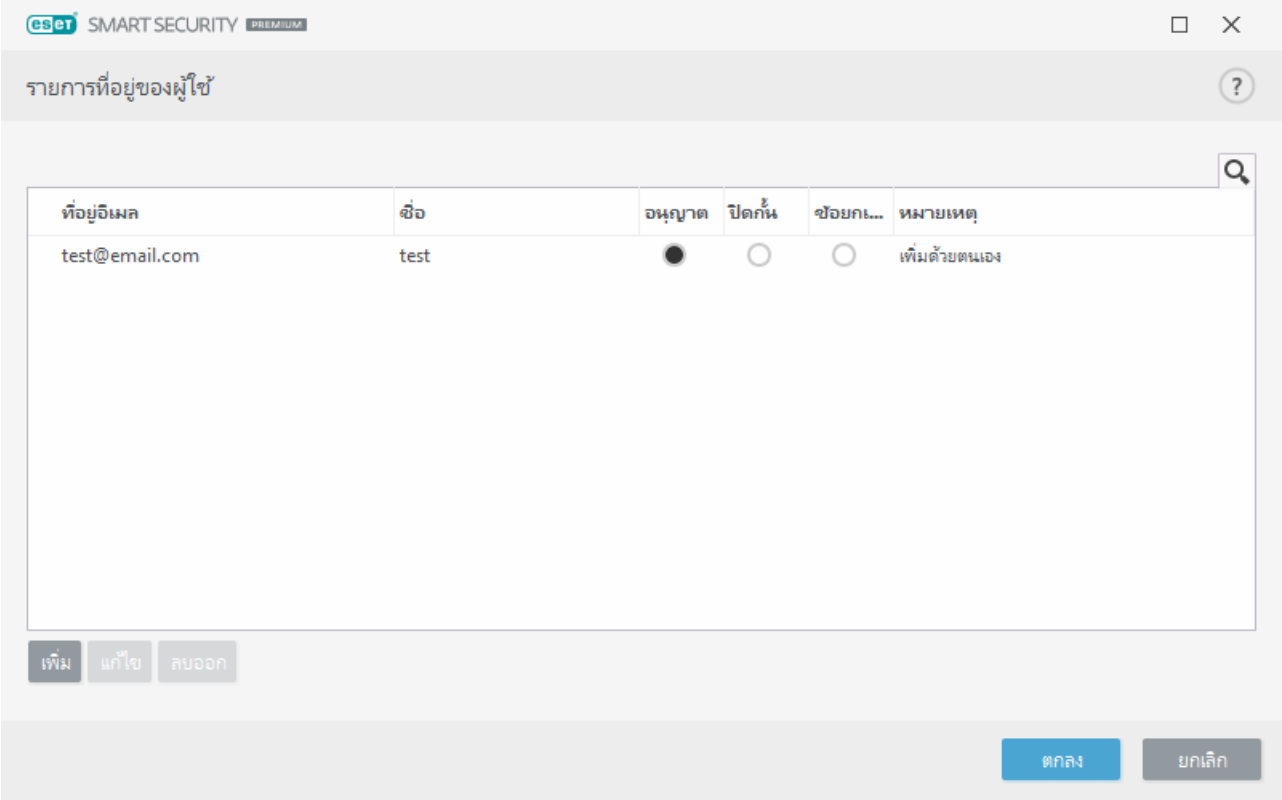
เพิ่มรายการที่อยู่ของผู้ใช้เป็นข้อยกเว้นโดยอัตโนมัติ

เพิ่มที่อยู่จากบัญชีของตนเอง – เพิ่มที่อยู่ของคุณจากบัญชีอีเมลไคลเอ็นต์ที่มีอยู่ไปยังรายการที่อยู่ของผู้ใช้เป็นข้อยกเว้น

รายการที่อยู่

เพื่อป้องกันอีเมลที่ไม่พึงประสงค์ ESET Smart Security Premium ทำให้คุณสามารถจำแนกที่อยู่อีเมลในรายการที่อยู่ได้

เมื่อต้องการแก้ไขรายการที่อยู่ ให้เปิด **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **การป้องกันอีเมลไคลเอ็นต์** > **รายการที่อยู่การป้องกันสแปม** 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

หน้าต่างนี้ช่วยให้คุณสามารถเพิ่มหรือแก้ไขที่อยู่ในรายการที่อยู่ป้องกันสแปมและกำหนดค่าการทำงานที่ใช้ได้:

ที่อยู่อีเมล – ที่อยู่ที่จะนำกฎไปใช้

ชื่อ – ชื่อกฎที่กำหนดเอง

การทำงาน – การทำงานที่จะใช้หากที่อยู่อีเมลของผู้ติดต่อตรงกับที่อยู่ที่ระบุในช่อง **ที่อยู่อีเมล**:

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

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

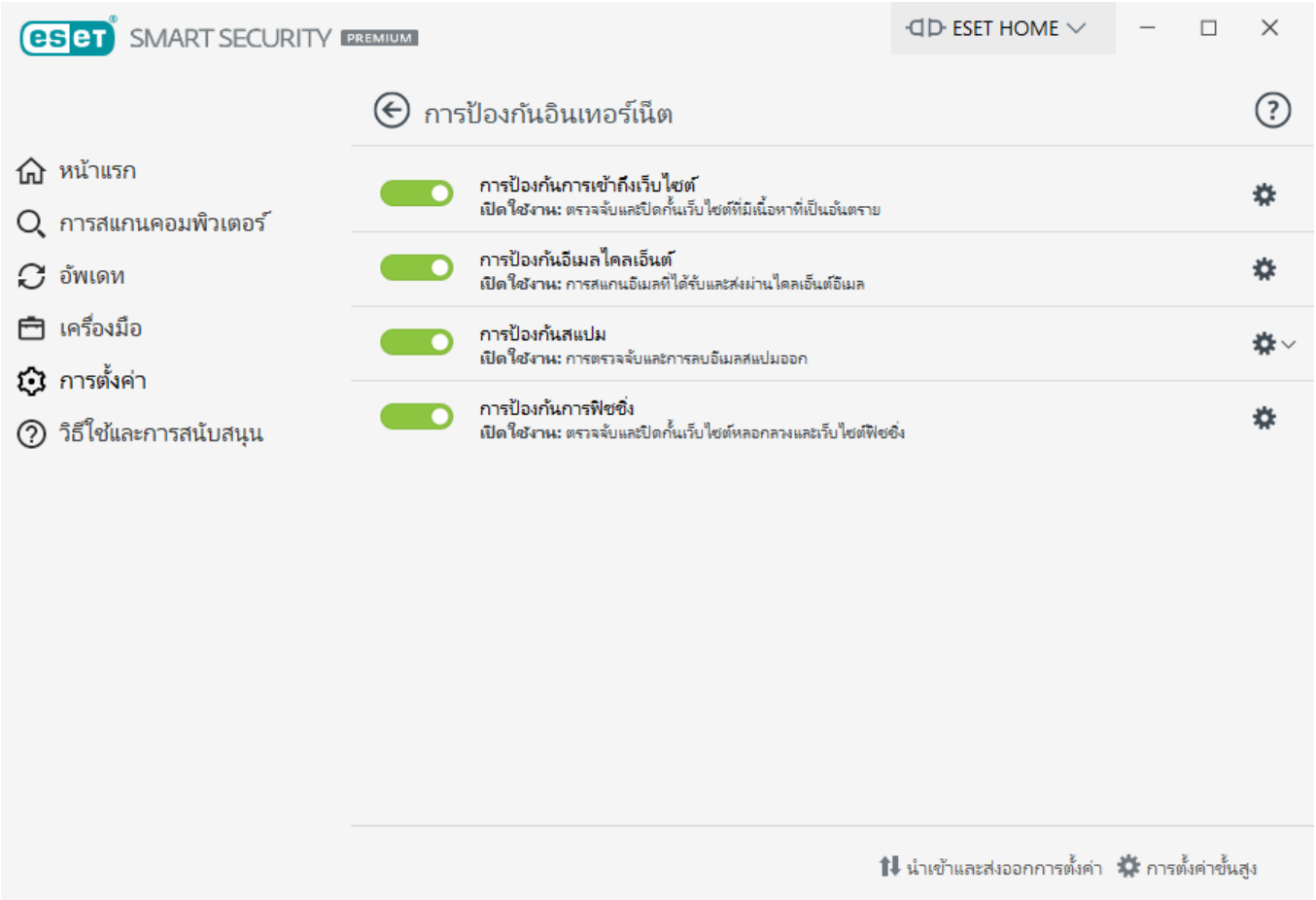
โดเมนระดับล่าง – เลือกตัวเลือกนี้เพื่อให้ใช้กฎกับโดเมนระดับล่างของผู้ติดต่อ (*address.info* คือโดเมน และ *my.address.info* คือโดเมนย่อย)

การป้องกันการเข้าถึงเว็บ

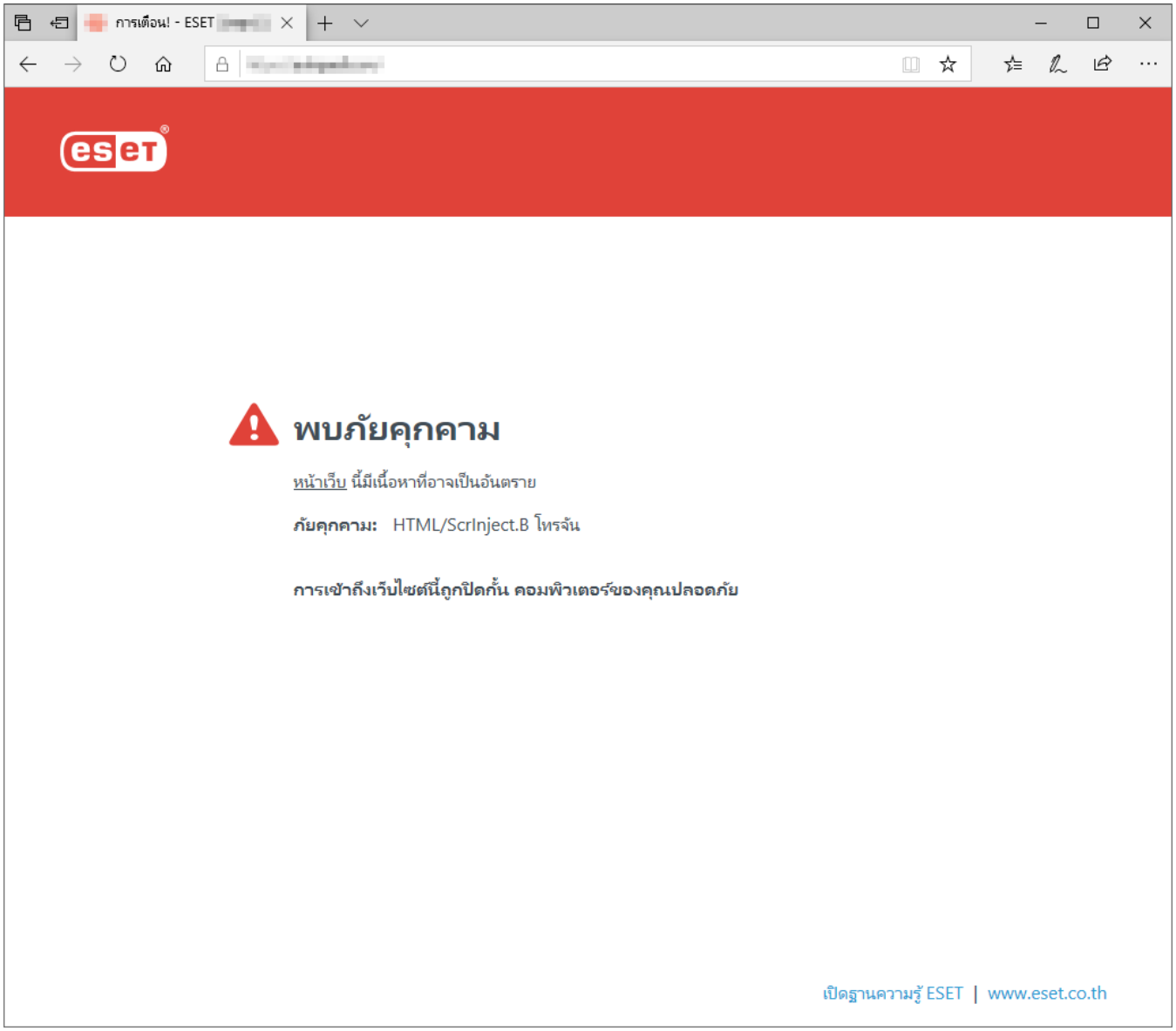
การเชื่อมต่ออินเทอร์เน็ตเป็นคุณลักษณะมาตรฐานในคอมพิวเตอร์ส่วนบุคคลส่วนใหญ่ แต่น่าเสียดายที่คุณลักษณะนี้กลายเป็นสื่อหลักสำหรับการถ่ายโอนรหัสที่เป็นอันตราย การป้องกันการเข้าถึงเว็บจะทำงานโดยตรวจสอบการสื่อสารระหว่างเว็บเบราว์เซอร์และเซิร์ฟเวอร์ระยะไกล และทำตามกฎ HTTP (Hypertext Transfer Protocol) และ HTTPS (การสื่อสารที่เข้ารหัส)

การเข้าถึงหน้าเว็บที่มีเนื้อหาที่เป็นอันตรายจะถูกปิดกั้นก่อนที่เนื้อหาจะได้รับการดาวน์โหลด หน้าเว็บอื่นๆ จะถูกสแกนด้วยกลไกการสแกน ThreatSense ขณะที่โหลดและจะถูกปิดกั้นถ้าตรวจพบเนื้อหาที่เป็นอันตราย การป้องกันการเข้าถึงเว็บจะให้การปกป้องสองระดับ คือการปิดกั้นตามบัญชีดำและปิดกั้นตามเนื้อหา

เราขอแนะนำอย่างยิ่งให้เปิดใช้งานตัวเลือกการป้องกันการเข้าถึงเว็บไซต์ ตัวเลือกนี้สามารถเข้าถึงได้จาก หน้าต่างหลักของโปรแกรม > **ตั้งค่า** > **การป้องกันอินเทอร์เน็ต** > **การป้องกันการเข้าถึงเว็บ**



การป้องกันการเข้าถึงเว็บไซต์จะแสดงข้อความต่อไปนี้ในเบราว์เซอร์ของคุณเมื่อเว็บไซต์ถูกปิดกั้น:



คำแนะนำพร้อมภาพประกอบ

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:

- ยกเว้นเว็บไซต์ที่ปลอดภัยไม่ให้ถูกบล็อกโดยการป้องกันการเข้าถึงเว็บไซต์
- บล็อกเว็บไซต์ที่ใช้ ESET Smart Security Premium

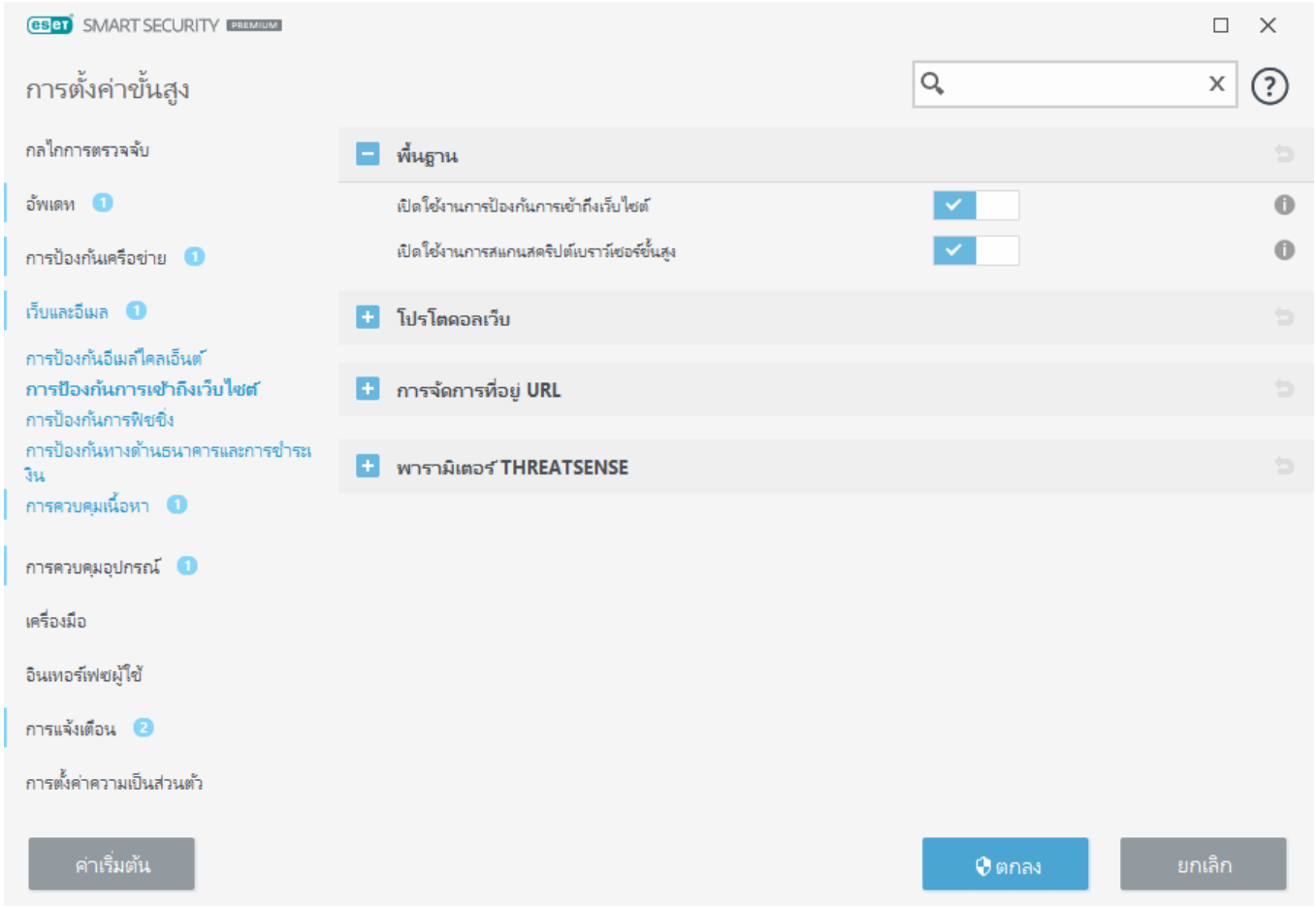
ตัวเลือกต่อไปนี้จะมีอยู่ใน **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **การป้องกันการเข้าถึงเว็บ**:

พื้นฐาน – เพื่อเปิดใช้งานหรือปิดใช้งานคุณสมบัตินี้จากการตั้งค่าขั้นสูง

โปรโตคอลเว็บ – ช่วยให้คุณสามารถกำหนดค่าการตรวจหาสำหรับโปรโตคอลมาตรฐานเหล่านี้ซึ่งเบราว์เซอร์อินเทอร์เน็ตส่วนใหญ่ใช้งาน

การจัดการที่อยู่ URL – ช่วยให้คุณสามารถระบุที่อยู่ URL ที่จะปิดกั้น อนุญาต หรือยกเว้นจากการตรวจสอบได้

พารามิเตอร์ ThreatSense - การตั้งค่าเครื่องมือสแกนไวรัสขั้นสูง - ช่วยให้คุณสามารถกำหนดค่าการตั้งค่าได้ เช่น ประเภทของวัตถุที่จะสแกน (อีเมล อาร์ไคฟ์ ฯลฯ) วิธีการตรวจหาของการป้องกันการเข้าถึงเว็บ ฯลฯ



การตั้งค่าขั้นสูงของการป้องกันการเข้าถึงเว็บไซต์

ตัวเลือกต่อไปนี้จะมีอยู่ใน **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **การป้องกันการเข้าถึงเว็บ** > **พื้นฐาน**:

เปิดใช้งานการป้องกันการเข้าถึงเว็บ – เมื่อปิดใช้งาน จะไม่มีการเรียกใช้การป้องกันการเข้าถึงเว็บไซต์และการป้องกันฟิชชิ่ง ตัวเลือกนี้จะมีให้ใช้เมื่อเปิดใช้งานการกรองโปรโตคอล SSL/TLS เท่านั้น

เปิดใช้งานการสแกนสคริปต์เบราว์เซอร์ขั้นสูง - เมื่อเปิดใช้งาน โปรแกรม JavaScript ทั้งหมดที่ใช้งานโดยเบราว์เซอร์อินเทอร์เน็ตจะถูกตรวจสอบโดยกลไกการตรวจจับ

เราขอแนะนำให้คุณคงการป้องกันการเข้าถึงเว็บให้มีสถานะเปิดใช้งาน

โปรโตคอลเว็บ

ตามค่าเริ่มต้น ESET Smart Security Premium ถูกกำหนดให้ตรวจสอบโปรโตคอล HTTP ที่อินเทอร์เน็ตเบราว์เซอร์ส่วนใหญ่ใช้

การตั้งค่าเครื่องสแกน HTTP

การรับส่งข้อมูล HTTP จะถูกตรวจสอบบนพอร์ตทั้งหมดสำหรับแอพพลิเคชั่นทั้งหมดเสมอ

การตั้งค่าเครื่องสแกน HTTP

ESET Smart Security Premium อีกทั้งสนับสนุนการตรวจสอบโปรโตรคอล HTTPS การสื่อสาร HTTPS จะใช้ช่องทางที่เข้ารหัส เพื่อโอนข้อมูลระหว่างเซิร์ฟเวอร์กับไคลเอ็นต์ ESET Smart Security Premium จะตรวจสอบการสื่อสารโดยใช้โปรโตคอล SSL (Secure Socket Layer) และ TLS (Transport Layer Security) โปรแกรมจะสแกนเฉพาะการรับส่งในพอร์ตที่กำหนดใน **พอร์ตที่ใช้งานโดยโปรโตคอล HTTPS** โดยไม่คำนึงถึงเวอร์ชันของระบบปฏิบัติการ

การสื่อสารที่เข้ารหัสจะถูกสแกนตามค่าเริ่มต้น หากต้องการดูการตั้งค่าเครื่องมือสแกน ให้เปิดการตั้งค่าขั้นสูง > **เว็บและอีเมล์** > **SSL/TLS**

การจัดการที่อยู่ URL

ส่วนการจัดการที่อยู่ URL จะช่วยให้คุณสามารถระบุที่อยู่ HTTP ที่จะปิดกั้น อนุญาต หรือยกเว้นจากการสแกนเนื้อหา

ต้องเลือก เปิดใช้งานการกรองโปรโตคอล SSL หากคุณต้องการกรองที่อยู่ HTTPS เพิ่มเติมจากหน้าเว็บ HTTP มิฉะนั้นจะเพิ่มเฉพาะโดเมนของไซต์ HTTPS ที่คุณเข้าชมเท่านั้น จะไม่เพิ่ม URL เต็ม

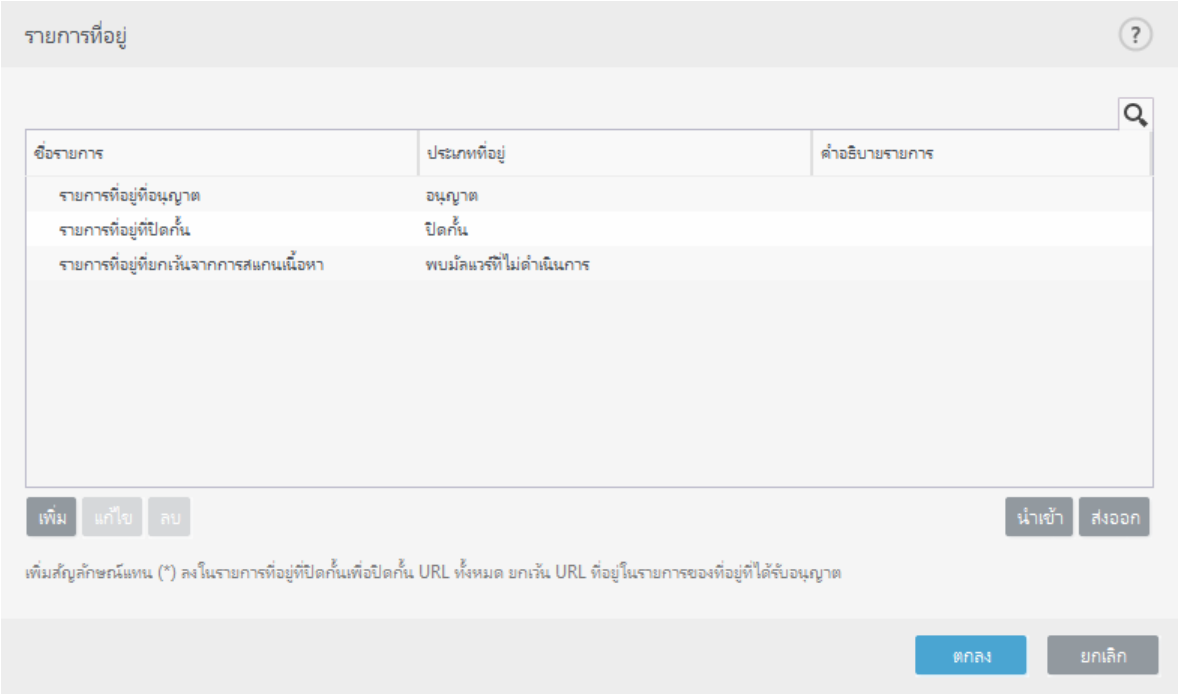
เว็บไซต์ใน **รายการที่อยู่ที่ปิดกั้น** จะไม่สามารถเข้าถึงได้เว้นแต่จะอยู่ใน **รายการที่อยู่ที่อนุญาต** ด้วยเช่นกัน เว็บไซต์ใน **รายการที่อยู่ที่ยกเว้นจากการสแกนเนื้อหา** จะไม่ถูกสแกนหารหัสที่เป็นอันตรายเมื่อเข้าถึง

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

คุณสามารถใช้สัญลักษณ์พิเศษ * (ดอกจัน) และ ? (เครื่องหมายคำถาม) ในรายการได้ (เครื่องหมายคำถาม) ได้ขณะสร้างรายการที่อยู่ โดยเครื่องหมายดอกจันจะแทนสตริงอักขระ และเครื่องหมายคำถามจะแทนสัญลักษณ์ ควร

พิจารณาอย่างรอบคอบเมื่อระบุที่อยู่ที่ยกเว้น เนื่องจากรายการดังกล่าวควรมีเฉพาะที่อยู่ที่เชื่อถือและปลอดภัยเท่านั้น ในทำนองเดียวกัน คุณควรตรวจสอบให้แน่ใจว่ามีการใช้สัญลักษณ์ * และ ? ในรายการนี้อย่างถูกต้อง โปรดดู เพิ่มที่อยู่ HTTP / มาสก์ของโดเมน เพื่อดูวิธีทำให้ทั้งโดเมนรวมถึงโดเมนย่อยทั้งหมดตรงกันได้อย่างปลอดภัย ในการเปิดใช้งานรายการ ให้เลือก **รายการที่ใช้งาน** หากคุณต้องการให้ระบบแจ้งเมื่อป้อนที่อยู่จากรายการปัจจุบัน ให้เลือก **แจ้งเมื่อนำไปใช้**

> **โดเมนที่เชื่อถือ**
> ที่อยู่จะไม่ถูกกรองหากการตั้งค่า **เว็บและอีเมล์** > **SSL/TLS** > **ยกเว้นการสื่อสารกับโดเมนที่เชื่อถือ** เปิดใช้งานอยู่และโดเมนถือเป็นโดเมนที่เชื่อถือได้



องค์ประกอบการควบคุม

เพิ่ม – สร้างรายการใหม่เพิ่มเติมจากรายการที่กำหนดไว้ล่วงหน้า ส่วนนี้จะมีประโยชน์เมื่อคุณต้องการแยกที่อยู่ออกเป็นกลุ่มๆ ตัวอย่างเช่น รายการของที่อยู่ที่ปิดกั้นรายการหนึ่งอาจประกอบด้วยที่อยู่จากบัญชีดำสาธารณะภายนอก และรายการถัดไปอาจประกอบด้วยบัญชีดำของคุณเอง ซึ่งทำให้ง่ายขึ้นต่อการอัพเดทรายการภายนอกในขณะที่เก็บส่วนของคุณไว้เหมือนเดิม

แก้ไข – แก้ไขรายการที่มีอยู่ ใช้สิ่งนี้ในการเพิ่มหรือลบที่อยู่ออก

ลบ – ลบรายการที่มีอยู่ สามารถใช้งานได้กับรายการที่สร้างด้วย **เพิ่ม** เท่านั้น ไม่สามารถใช้กับรายการตามค่าเริ่มต้นได้

รายการที่อยู่ URL

ในส่วนนี้ คุณสามารถระบุรายการของที่อยู่ HTTP ที่จะถูกปิดกั้น อนุญาต หรือยกเว้นจากการตรวจสอบ

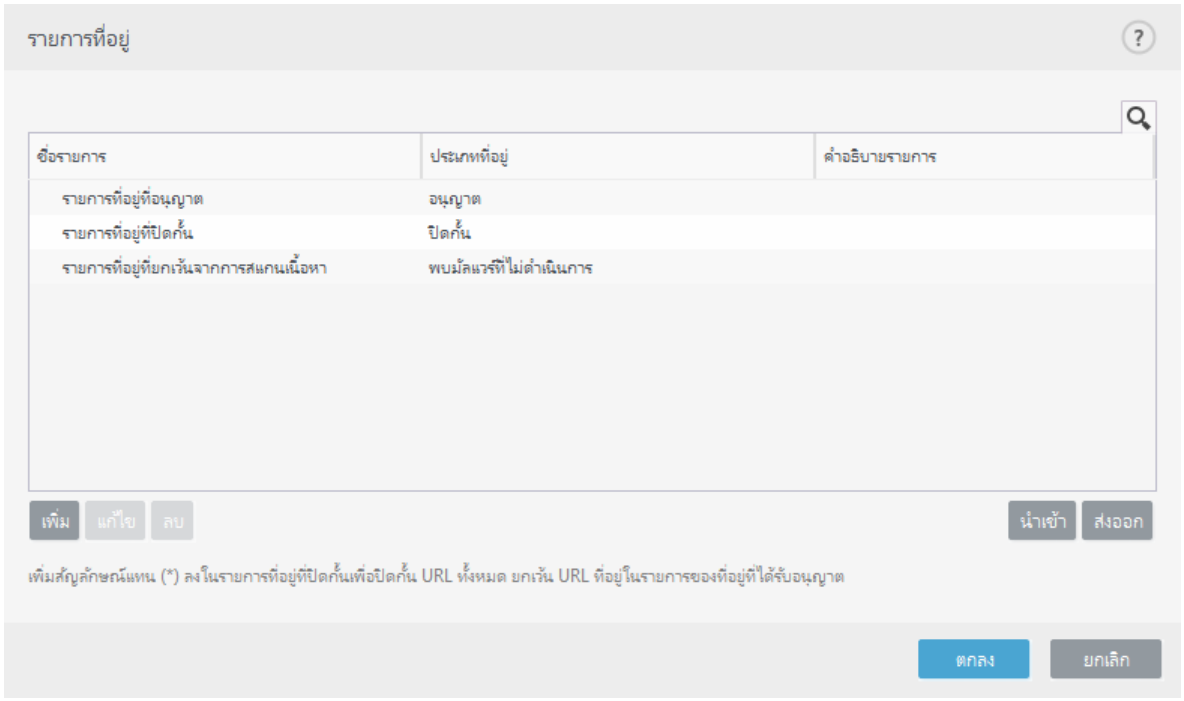
ตามค่าเริ่มต้นแล้ว จะมีสามรายการดังต่อไปนี้:

• **รายการที่อยู่ที่ยกเว้นจากการสแกนเนื้อหา** – ไม่มีการตรวจสอบรหัสที่เป็นอันตรายสำหรับที่อยู่ที่เพิ่มไว้ในรายการนี้

• **รายการที่อยู่ที่อนุญาต** – ถ้าเปิดใช้งานตัวเลือก อนุญาตการเข้าถึงเฉพาะที่อยู่ HTTP ในรายการของที่อยู่ที่อนุญาต และรายการของที่อยู่ที่ปิดกั้นประกอบด้วย * (จับคู่ทุกอย่าง) ผู้ใช้จะสามารถเข้าถึงที่อยู่ที่ระบุในรายการนี้ได้เท่านั้น ที่อยู่ในรายการนี้จะได้รับอนุญาตแม้ว่ารวมอยู่ในรายการที่อยู่ที่ปิดกั้น

• **รายการที่อยู่ที่ปิดกั้น** - ผู้ใช้จะไม่สามารถเข้าถึงที่อยู่ที่ระบุในรายการนี้เว้นแต่ที่อยู่นั้นอยู่ในรายการที่อยู่ที่อนุญาต

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



คำแนะนำพร้อมภาพประกอบ

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:

• ยกเว้นเว็บไซต์ที่ปลอดภัยไม่ให้ถูกบล็อกโดยการป้องกันการเข้าถึงเว็บไซต์

• ปิดกั้นเว็บไซต์โดยใช้งานผลิตภัณฑ์ ESET Windows สำหรับใช้งานในบ้าน

สำหรับข้อมูลเพิ่มเติม โปรดดูที่การจัดการที่อยู่ URL

สร้างรายการที่อยู่ URL ใหม่

ส่วนนี้ช่วยให้คุณสามารถระบุรายการของที่อยู่/มาสก์ URL ที่จะถูกปิดกั้น อนุญาต หรือยกเว้นจากการตรวจสอบ

เมื่อสร้างรายการใหม่ คุณจะสามารถกำหนดค่าตัวเลือกต่อไปนี้ได้:

ประเภทรายการที่อยู่ - มีประเภทรายการสามประเภท:

- **ยกเว้นจากการตรวจสอบ** – ไม่มีการตรวจสอบรหัสที่เป็นอันตรายสำหรับที่อยู่ที่เพิ่มในรายการนี้
- **รายการที่อยู่ที่ปิดกั้น** - ผู้ใช้จะไม่สามารถเข้าถึงที่อยู่ที่ระบุในรายการนี้
- **รายการที่อยู่ที่อนุญาต** - หากเปิดใช้งานตัวเลือก อนุญาตการเข้าถึงเฉพาะที่อยู่ HTTP ในรายการของที่อยู่ที่อนุญาต และรายการของที่อยู่ที่ปิดกั้นประกอบด้วย * (จับคู่ทุกอย่าง) ผู้ใช้จะสามารถเข้าถึงที่อยู่ที่ระบุในรายการนี้เท่านั้น ที่อยู่ในรายการนี้จะได้รับอนุญาตแม้ว่าจับคู่ด้วยรายการที่อยู่ที่ปิดกั้น

ชื่อรายการ – ระบุชื่อของรายการ ช่องจะกลายเป็นสีเทาขณะแก้ไขหนึ่งในสามรายการที่กำหนดไว้ล่วงหน้า

คำอธิบายรายการ - พิมพ์คำอธิบายโดยย่อสำหรับรายการ (ไม่จำเป็น) จะกลายเป็นสีเทาขณะแก้ไขหนึ่งในสามรายการที่กำหนดไว้ล่วงหน้า

เมื่อต้องการเปิดใช้งานรายการ ให้เลือก **รายการที่ใช้งาน** ถัดจากรายการนั้น ถ้าคุณต้องการรับการแจ้งเมื่อมีบางรายการถูกใช้เพื่อประเมินไซต์ HTTP ที่คุณเยี่ยมชม ให้เลือก **แจ้งเตือนเมื่อปรับใช้** ตัวอย่างเช่น จะมีการส่งการแจ้งเตือนถ้าเว็บไซต์ถูกปิดกั้นหรืออนุญาตเพราะเว็บไซต์นั้นอยู่ในรายการที่อยู่ที่ปิดกั้นหรืออนุญาต การแจ้งเตือนจะแจ้งชื่อของรายการที่มีเว็บไซต์ที่ระบุ

องค์ประกอบการควบคุม

เพิ่ม – เพิ่มที่อยู่ URL ใหม่ไปยังรายการ (ป้อนค่าได้หลายค่าโดยใส่ตัวคั่น)

แก้ไข – แก้ไขที่อยู่ที่มีอยู่ในรายการ ดำเนินการได้เฉพาะที่อยู่ที่สร้างด้วย **เพิ่ม**

ลบออก – ลบที่อยู่ที่มีอยู่ในรายการ ดำเนินการได้เฉพาะที่อยู่ที่สร้างด้วย **เพิ่ม**

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

วิธีการเพิ่มมาสก์ URL

โปรดดูคำแนะนำในหน้าต่างข้อความนี้ก่อนป้อนที่อยู่ที่ต้องการ/มาสก์ของโดเมน

ESET Smart Security Premium ให้ผู้ใช้สามารถปิดกั้นการเข้าถึงเว็บไซต์ที่ระบุ และป้องกันไม่ให้เบราว์เซอร์อินเทอร์เน็ตแสดงเนื้อหา นอกจากนี้ ยังให้ผู้ใช้สามารถระบุที่อยู่ ซึ่งต้องการยกเว้นจากการตรวจสอบ หากไม่ทราบชื่อเต็มของเซิร์ฟเวอร์ระยะไกล หรือผู้ใช้ต้องการระบุทั้งกลุ่มของเซิร์ฟเวอร์ระยะไกล คุณสามารถใช้มาสก์เพื่อระบุกลุ่มดังกล่าวได้ มาสก์นี้ได้แก่สัญลักษณ์ "?" และ "*":

- ใช้ ? เพื่อแทนสัญลักษณ์
- ใช้ * เพื่อแทนสตริงข้อความ

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

สัญลักษณ์ '*.' ที่อยู่ด้านหน้าของลำดับจะแสดงผลเป็นพิเศษหากใช้ขึ้นต้นชื่อโดเมน แรกสุด สัญลักษณ์แทน * ต้องไม่ตรงกับเครื่องหมายทับ ('/') ในกรณีนี้ ทั้งนี้เพื่อกันไม่ให้หลีกเลี่ยงมาสก์ 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* จะไม่ถูกต้อง เนื่องจากมาสก์ดังกล่าวจะไปตรงกับ *http://anotherdomain.com* เช่นกัน

การป้องกันฟิชชิ่ง

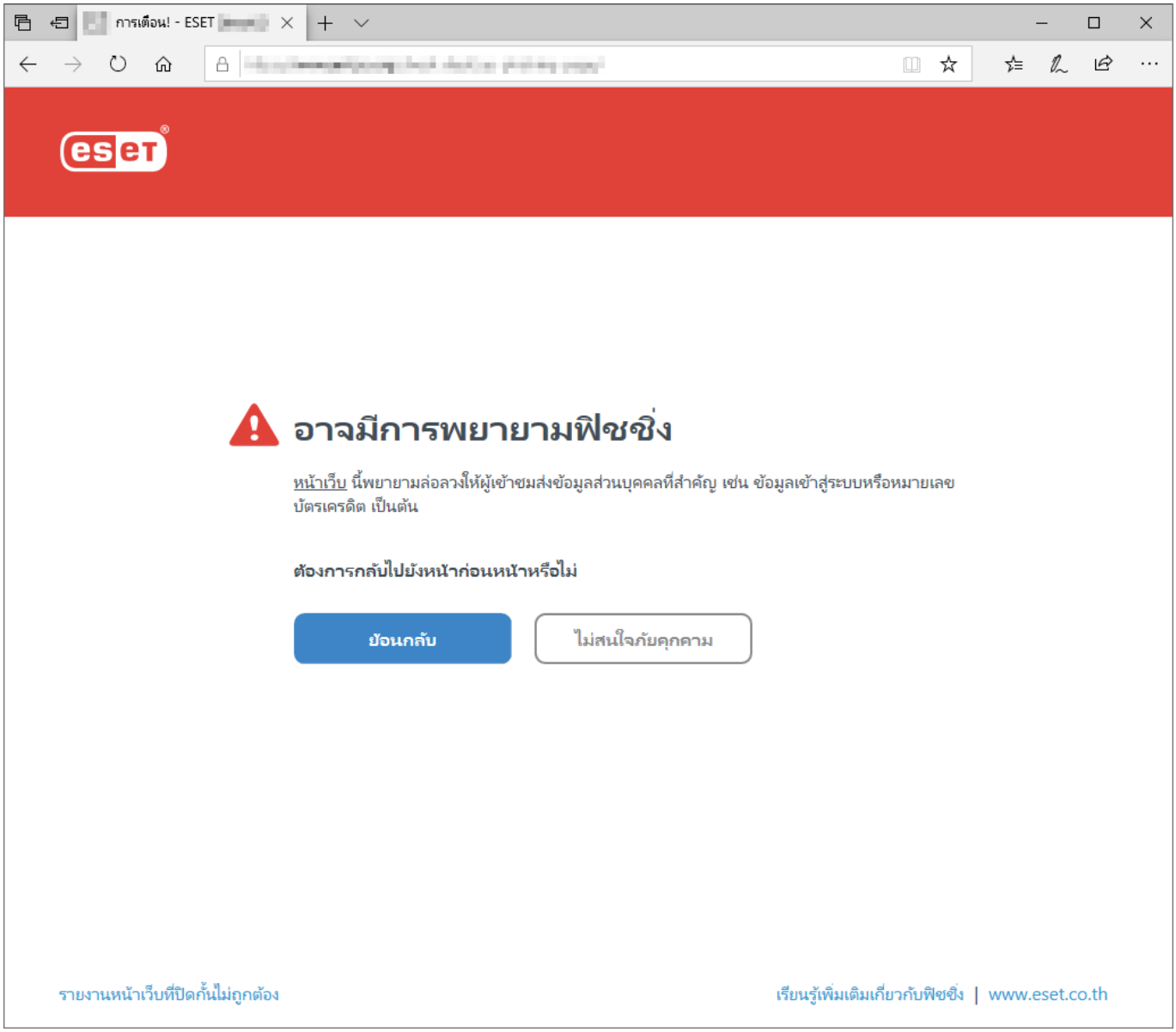
คำว่า ฟิชชิ่ง จะหมายถึงกิจกรรมที่ผิดกฎหมายซึ่งใช้กลลวงทางสังคม (การจัดการผู้ใช้เพื่อให้ได้ข้อมูลที่เป็นความลับ) การฟิชชิ่งมักนำมาใช้เพื่อให้ได้รับสิทธิ์การเข้าถึงข้อมูลสำคัญ เช่น หมายเลขบัญชีธนาคาร หมายเลข PIN เป็นต้น อ่านข้อมูลเพิ่มเติมเกี่ยวกับการทำงานนี้ใน ประมวลศัพท์ ESET Smart Security Premium รวมการป้องกันฟิชชิ่ง ซึ่งจะปิดกั้นหน้าเว็บที่เผยแพร่เนื้อหาดังกล่าว

เราขอแนะนำให้คุณเปิดใช้งานการป้องกันฟิชชิ่งใน ESET Smart Security Premium หากต้องการดำเนินการดังกล่าว ให้เปิด **การตั้งค่าขั้นสูง** (F5) และนำทางไปที่ **เว็บและอีเมล** > **การป้องกันฟิชชิ่ง**

โปรดไปที่ บทความฐานความรู้ ของเราหากต้องการข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันฟิชชิ่งใน ESET Smart Security Premium

การเข้าถึงเว็บไซต์ฟิชชิ่ง

เมื่อคุณเข้าถึงเว็บไซต์ฟิชชิ่งที่เป็นที่รู้จัก ข้อความต่อไปนี้จะปรากฏขึ้นในเว็บเบราว์เซอร์ของคุณ หากคุณยังต้องการเข้าถึงเว็บไซต์ ให้คลิก **ละเว้นภัยคุกคาม** (ไม่แนะนำ)



ตามค่าเริ่มต้น เว็บไซต์ที่อาจเป็นฟิชชิ่งซึ่งมีการกำหนดว่าเป็นบัญชีปลอดภัยจะหมดอายุหลังจากผ่านไปหลายชั่วโมง หากต้องการอนุญาตเว็บไซต์อย่างถาวร โปรดใช้เครื่องมือ การจัดการที่อยู่ URL จาก **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **การป้องกันการเข้าถึงเว็บ** > **การจัดการที่อยู่ URL** > **รายการที่อยู่** คลิก **แก้ไข** และเพิ่มเว็บไซต์ที่คุณต้องการแก้ไขลงในรายการ

การรายงานไซต์ฟิชชิ่ง

ลิงค์ **รายงาน** จะช่วยให้คุณสามารถรายงานเว็บไซต์ฟิชชิ่ง/ที่เป็นอันตรายไปยัง ESET เพื่อวิเคราะห์

ก่อนส่งเว็บไซต์ไปยัง ESET โปรดตรวจสอบว่าเว็บไซต์ตรงตามเกณฑ์อย่างน้อยหนึ่งข้อดังต่อไปนี้:
• ไม่มีการตรวจพบเว็บไซต์เลย
• มีการตรวจพบเว็บไซต์ว่าเป็นภัยคุกคามโดยเป็นข้อผิดพลาด ในกรณีนี้ คุณสามารถ รายงานหน้าที่ถูกปิดกั้นอย่างไม่ถูกต้อง

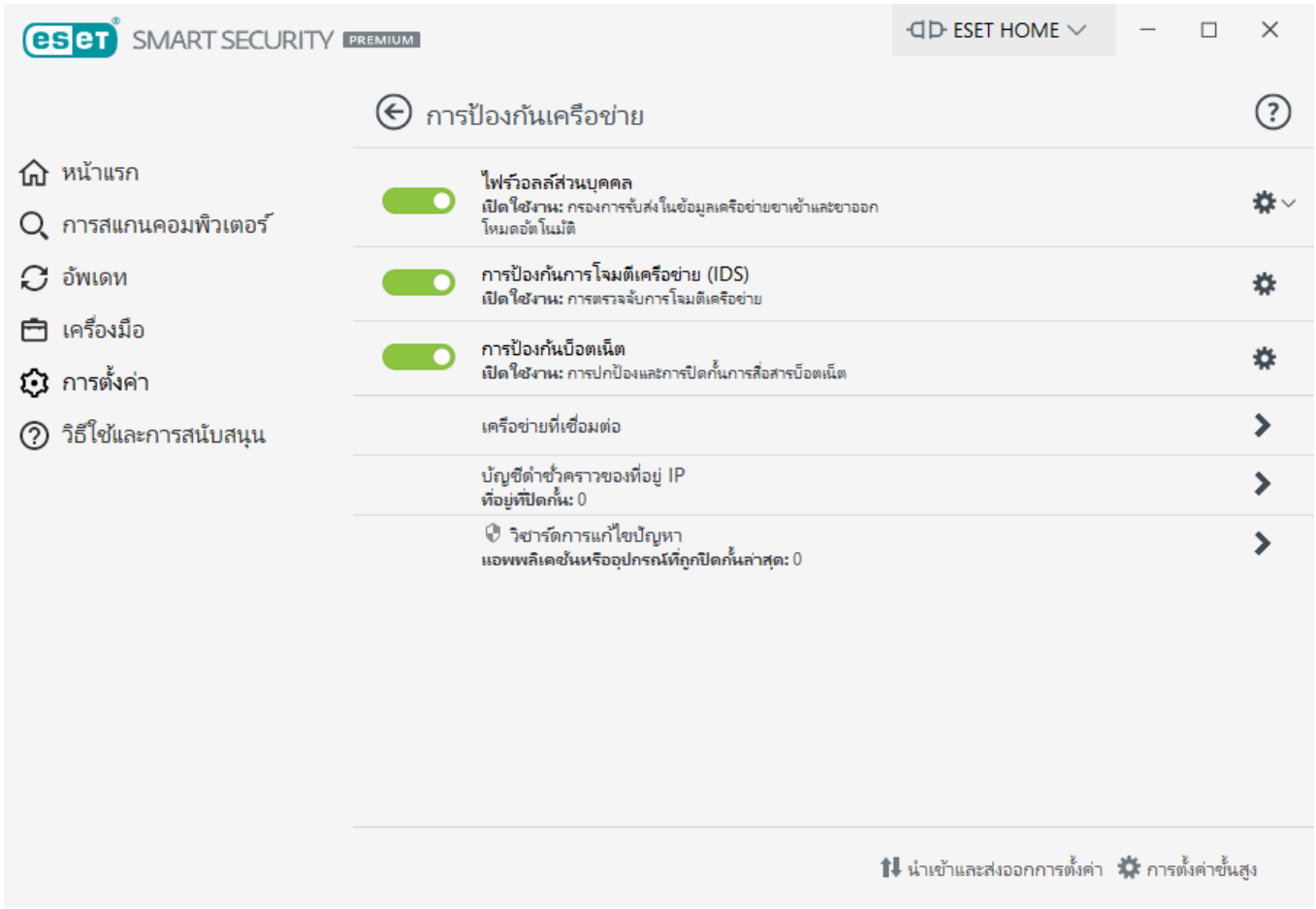
อีกวิธีหนึ่งคือ คุณสามารถส่งเว็บไซต์ทางอีเมล ส่งอีเมลไปที่ samples@eset.com โปรดใช้ชื่อเรื่องที่อธิบายชัดเจนและให้ข้อมูลเกี่ยวกับเว็บไซต์มากที่สุดเท่าที่จะเป็นไปได้ (ตัวอย่างเช่น เว็บไซต์ที่คุณใช้อ้างอิง คุณทราบเรื่องเว็บไซต์นี้ได้อย่างไร เป็นต้น)

การป้องกันเครือข่าย

การกำหนดค่าการป้องกันเครือข่ายจะพบได้ที่หน้าต่าง **การตั้งค่า** ใต้ **การป้องกันเครือข่าย**

หากต้องการหยุดชั่วคราวหรือปิดใช้งานโมดูลการป้องกันแต่ละโมดูล ให้คลิกไอคอนแถบเลื่อน 

การปิดโมดูลการป้องกันอาจลดระดับการป้องกันของคอมพิวเตอร์ของคุณ



ไฟร์วอลล์ – ในส่วนนี้ คุณสามารถปรับโหมดการกรองสำหรับไฟร์วอลล์ ESET หากต้องการเข้าถึงการตั้งค่าอย่างละเอียดยิ่งขึ้น ให้คลิกที่ล้อเฟือง ⚙ > **กำหนดค่า** ที่อยู่ถัดจาก **ไฟร์วอลล์** หรือกด **F5** เพื่อเข้าถึงการตั้งค่าขั้นสูง:

กำหนดค่า – เปิดหน้าต่างไฟร์วอลล์ในการตั้งค่าขั้นสูงซึ่งคุณจะสามารถระบุวิธีที่ไฟร์วอลล์จะจัดการการสื่อสารในเครือข่ายได้

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

ปิดกั้นการรับส่งทั้งหมด – การสื่อสารขาเข้าและขาออกทั้งหมดจะถูกปิดกั้นโดยไฟร์วอลล์ ใช้ตัวเลือกนี้เฉพาะเมื่อคุณสงสัยเกี่ยวกับความเสี่ยงด้านความปลอดภัยที่สำคัญ ซึ่งต้องการตัดการเชื่อมต่อระบบจากเครือข่าย ขณะที่การกรองการรับส่งข้อมูลของเครือข่ายอยู่ในโหมด **ปิดกั้นการรับส่งข้อมูลทั้งหมด** ให้คลิก **หยุดปิดกั้นการรับส่งข้อมูลทั้งหมด** เพื่อเรียกคืนการดำเนินการไฟร์วอลล์ปกติ

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

โหมดโต้ตอบ – (เมื่อโหมดการกรองอื่นเปิดใช้งานอยู่) – คลิกเพื่อเปลี่ยนโหมดการกรองเป็นโหมดการกรองเชิงโต้ตอบ

การป้องกันการโจมตีเครือข่าย (IDS) – วิเคราะห์เนื้อหาของการรับส่งข้อมูลเครือข่ายและป้องกันจากการโจมตีเครือข่าย การรับส่งข้อมูลใดๆ ที่พิจารณาแล้วว่าเป็นอันตรายจะถูกปิดกั้น ESET Smart Security Premium จะให้ข้อมูลคุณเมื่อคุณเชื่อมต่อกับเครือข่ายไร้สายที่ไม่ได้รับการป้องกันหรือเครือข่ายที่มีการป้องกันที่ไม่ปลอดภัย

การป้องกันบอตเน็ต - ตรวจหามัลแวร์บนระบบของคุณอย่างรวดเร็วและแม่นยำ

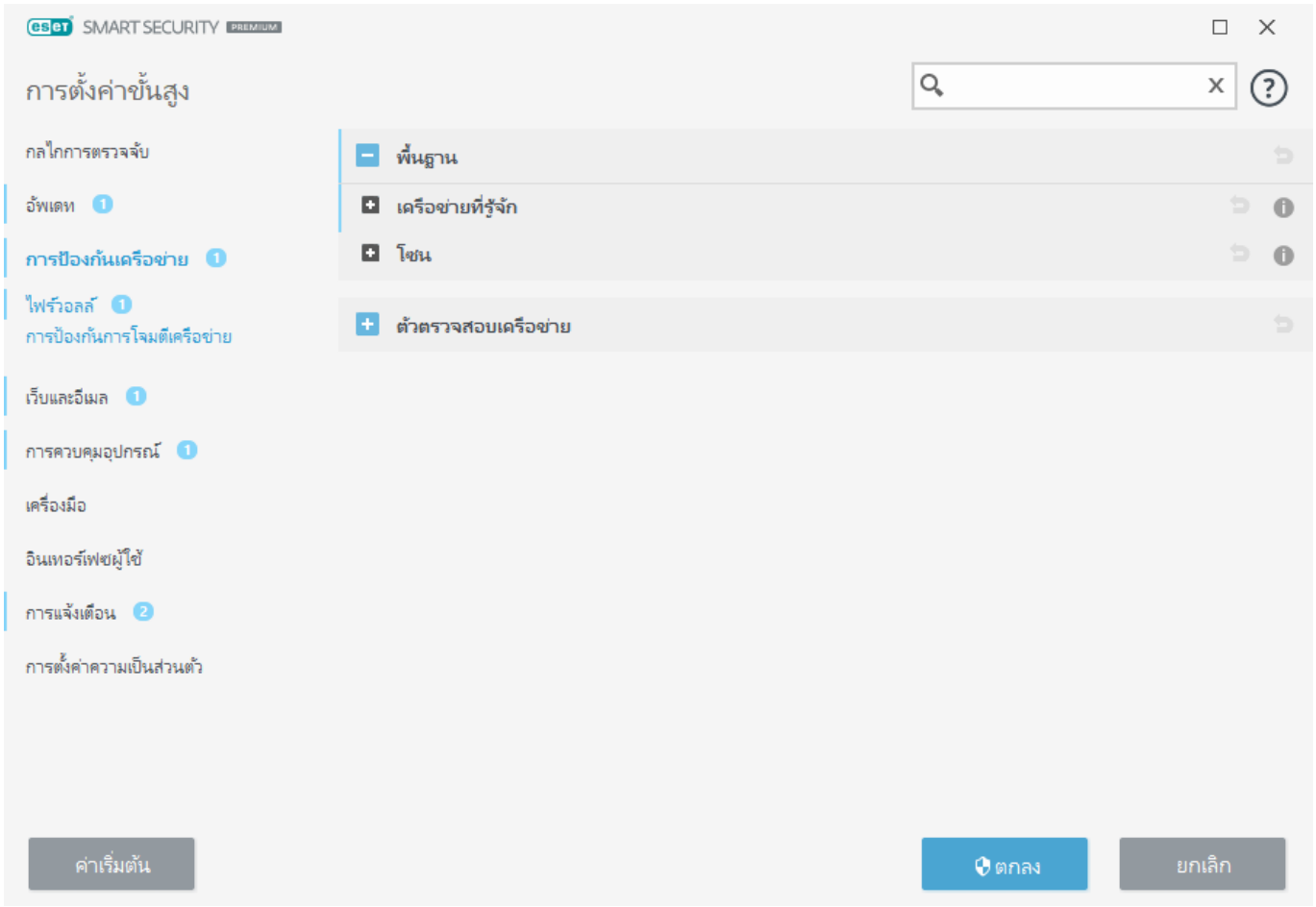
เครือข่ายที่เชื่อมต่อ - แสดงเครือข่ายที่อะแดปเตอร์เครือข่ายเชื่อมต่ออยู่ หลักจากคุณคลิกลิงก์ที่ใต้ชื่อเครือข่ายหน้าต่างป๊อปอัปจะทำให้คุณสามารถกำหนดค่าเครือข่ายให้เป็นเครือข่ายที่เชื่อถือได้

บัญชีดำชั่วคราวของที่อยู่ IP – ดูรายการของที่อยู่ IP ที่ถูกตรวจพบว่าเป็นแหล่งที่มาของการโจมตีและเพิ่มลงในบัญชีดำเพื่อปิดกั้นการเชื่อมต่อเป็นระยะเวลาหนึ่ง สำหรับข้อมูลเพิ่มเติม ให้คลิกที่ตัวเลือกนี้ จากนั้นกด F1

วิซาร์ดการแก้ไขปัญหา – ช่วยให้คุณแก้ไขปัญหาการเชื่อมต่อที่เกิดจากไฟร์วอลล์ของ ESET สำหรับข้อมูลเพิ่มเติม โปรดดูที่ วิซาร์ดการแก้ไขปัญหา

การตั้งค่าขั้นสูงสำหรับการป้องกันเครือข่าย

ในหน้าต่างโปรแกรมหลัก คลิก **ตั้งค่า** > **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย**



พื้นฐาน

เครือข่ายที่รู้จัก

สำหรับข้อมูลเพิ่มเติม โปรดดูเครือข่ายที่รู้จัก

โซน

โซนแสดงถึงชุดรวมของที่อยู่เครือข่ายที่สร้างกลุ่มลอจิคัลหนึ่งกลุ่ม สำหรับข้อมูลเพิ่มเติม โปรดดูที่ การกำหนดค่าโซน

ตัวตรวจสอบเครือข่าย

เปิดใช้งานตัวตรวจสอบเครือข่าย

ตัวตรวจสอบเครือข่ายจะช่วยระบุจุดอ่อนในเครือข่ายภายในบ้านของคุณ เช่น พอร์ตที่เปิดอยู่หรือรหัสผ่านเราเตอร์ที่มีความปลอดภัยต่ำ ทั้งยังให้รายการอุปกรณ์ที่เชื่อมต่อซึ่งจัดประเภทตามชนิดของอุปกรณ์

แจ้งเกี่ยวกับอุปกรณ์เครือข่ายที่เพิ่งค้นพบ

แจ้งให้คุณทราบเมื่อตรวจพบอุปกรณ์ใหม่บนเครือข่ายของคุณ

เครือข่ายที่รู้จัก

เมื่อใช้คอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายที่ไม่เชื่อถือหรือเครือข่ายที่อยู่นอกเครือข่ายที่เชื่อถือ (ซึ่งก็คือเครือข่ายบ้านหรือที่ทำงาน) ของคุณอยู่บ่อยครั้ง เราขอแนะนำให้ตรวจสอบความน่าเชื่อถือของเครือข่ายใหม่ที่คุณจะเชื่อมต่อ เมื่อกำหนดเครือข่ายแล้ว ESET Smart Security Premium จะสามารถจำเครือข่ายที่เชื่อถือ (บ้าน/ที่ทำงาน) โดยใช้พารามิเตอร์เครือข่ายที่กำหนดค่าใน **การระบุรหัสประจำตัวเครือข่าย** คอมพิวเตอร์มักจะเข้าสู่เครือข่ายโดยใช้ที่อยู่ IP คล้ายกับเครือข่ายที่เชื่อถือ ในกรณีดังกล่าว ESET Smart Security Premium อาจพิจารณาเครือข่ายที่ไม่รู้จักว่าไม่น่าเชื่อถือ (เครือข่ายบ้านหรือที่ทำงาน) เราขอแนะนำให้คุณใช้ **การตรวจสอบสิทธิ์เครือข่าย** เพื่อหลีกเลี่ยงสถานการณ์เช่นนี้ หากต้องการเข้าถึงการตั้งค่าเครือข่ายที่รู้จัก ให้ไปที่ **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **พื้นฐาน** > **เครือข่ายที่รู้จัก**

เมื่ออะแดปเตอร์เครือข่ายเชื่อมต่อกับเครือข่ายหนึ่งหรือการตั้งค่าเครือข่ายของอะแดปเตอร์เครือข่ายถูกกำหนดค่าใหม่ ESET Smart Security Premium จะค้นรายการเครือข่ายที่รู้จักเพื่อหาบันทึกที่ตรงกับเครือข่ายใหม่ ถ้าตรงกับ **การระบุรหัสประจำตัวเครือข่าย** และ **การตรวจสอบสิทธิ์เครือข่าย** (ไม่จำเป็น) เครือข่ายจะได้รับการทำเครื่องหมายเป็นเชื่อมต่อในอินเทอร์เฟซนี้ เมื่อไม่พบเครือข่ายใดๆ ที่รู้จัก การกำหนดค่ารหัสประจำตัวเครือข่ายจะสร้างการเชื่อมต่อเครือข่ายใหม่เพื่อใช้ระบุเครือข่ายในครั้งต่อไปที่คุณเชื่อมต่อ การเชื่อมต่อเครือข่ายใหม่จะใช้ประเภทการปกป้องตามที่ได้กำหนดไว้ในการตั้งค่า Windows ตามค่าเริ่มต้น หน้าต่างข้อความ **ตรวจพบการเชื่อมต่อเครือข่ายใหม่** จะแสดงข้อความให้คุณเลือกประเภทการป้องกันระหว่าง **เครือข่ายที่เชื่อถือ**, **เครือข่ายที่ไม่เชื่อถือ** หรือ **ใช้การตั้งค่า Windows** ถ้าอะแดปเตอร์เครือข่ายเชื่อมต่อกับเครือข่ายที่รู้จักและเครือข่ายนั้นได้รับการทำเครื่องหมายเป็น **เครือข่ายที่เชื่อถือ** ซับเน็ตในพื้นที่ของอะแดปเตอร์ดังกล่าวจะได้รับการเพิ่มไปยังโซนที่เชื่อถือ

ประเภทการปกป้องของเครือข่ายใหม่ – เลือกหนึ่งในตัวเลือกต่อไปนี้: **ใช้การตั้งค่า Windows**, **ถามผู้ใช้** หรือ **ทำเครื่องหมายว่าไม่เชื่อถือ** จะถูกใช้สำหรับเครือข่ายใหม่ตามค่าเริ่มต้น

เครือข่ายที่รู้จัก อนุญาตให้คุณกำหนดค่าชื่อเครือข่าย การระบุรหัสประจำตัวเครือข่าย ประเภทการปกป้อง เป็นต้น หากต้องการเข้าถึงตัวแก้เครือข่ายที่รู้จัก ให้คลิก **แก้ไข**

เมื่อคุณเลือก **ใช้การตั้งค่า Windows** จะ ไม่มีหน้าต่างข้อความปรากฏขึ้น และเครือข่ายที่คุณเชื่อมต่ออยู่จะถูกทำเครื่องหมายตามการตั้งค่า Windows ของคุณ นี่จะช่วยให้สามารถเข้าถึงบางคุณลักษณะ (ตัวอย่างเช่น การแบ่งปันไฟล์และรีโมทเดสก์ท็อป) จากเครือข่ายใหม่ได้

ตัวแก้เครือข่ายที่รู้จัก

กำหนดค่าเครือข่ายที่รู้จักได้ด้วยตนเองใน **การตั้งค่าขั้นสูง** > **การป้องกันเครือข่าย** > **พื้นฐาน** > **เครือข่ายที่รู้จัก** โดยคลิก **แก้ไข**

คอลัมน์

ชื่อ – ชื่อของเครือข่ายที่รู้จัก

ประเภทการปกป้อง – แสดงว่ามีการตั้งค่าเครือข่ายเป็น **เครือข่ายที่เชื่อถือ เครือข่ายที่ไม่เชื่อถือ** หรือ **ใช้การตั้งค่า Windows**

โปรไฟล์ของไฟร์วอลล์ – เลือกโปรไฟล์จากเมนูแบบเลื่อนลง **แสดงกฎที่ใช้ในโปรไฟล์** เพื่อแสดงตัวกรองกฎของโปรไฟล์

โปรไฟล์การอัพเดท – อนุญาตให้คุณใช้โปรไฟล์การอัพเดทที่สร้างขึ้นเมื่อเชื่อมต่อกับเครือข่ายนี้

องค์ประกอบการควบคุม

เพิ่ม – สร้างเครือข่ายที่รู้จักใหม่

แก้ไข – คลิกเพื่อแก้ไขเครือข่ายที่รู้จักที่มีอยู่

ลบออก – เลือกเครือข่ายและคลิก **ลบออก** เพื่อลบเครือข่ายนี้ออกจากรายการเครือข่ายที่รู้จัก

บนสุด/ขึ้น/ลง/ล่างสุด – อนุญาตให้คุณปรับระดับความสำคัญของเครือข่ายที่รู้จัก (เครือข่ายจะถูกประเมินจากบนลงล่าง)

การตั้งค่าการกำหนดค่าเครือข่าย จะจัดเรียงในแท็บดังต่อไปนี้:

เครือข่าย

ที่จุดนี้ คุณสามารถกำหนด **ชื่อเครือข่าย** และเลือก **ประเภทของการป้องกัน** (เครือข่ายที่เชื่อถือ, เครือข่ายที่ไม่เชื่อถือ หรือใช้การตั้งค่า Windows) ของเครือข่ายดังกล่าวได้ ใช้เมนูแบบเลื่อนลง **โปรไฟล์ของไฟร์วอลล์** เพื่อเลือกโปรไฟล์จากเครือข่ายนี้ หากเครือข่ายใช้ประเภทการป้องกันเป็น **ที่เชื่อถือ** เครือข่ายย่อยทั้งหมดที่เชื่อมต่อโดยตรง

จะได้รับการพิจารณาเป็นเชื่อถือ ตัวอย่างเช่น ถ้าอะแดปเตอร์เครือข่ายเชื่อมต่อกับเครือข่ายนี้ด้วยที่อยู่ IP 192.168.1.5 และซับเน็ตมาสก์ 255.255.255.0 ซับเน็ต 192.168.1.0/24 จะเพิ่มไปยังโซนที่เชื่อถือของอะแดปเตอร์นั้น ถ้าอะแดปเตอร์นั้นมีที่อยู่/ซับเน็ตเพิ่มเติม ทั้งหมดจะได้รับการเชื่อถือ โดยไม่คำนึงถึงการกำหนดค่า **การระบุรหัสประจำตัวเครือข่าย** ของเครือข่ายที่รู้จัก

นอกจากนี้ ที่อยู่ที่เพิ่มไปยัง **ที่อยู่ที่เชื่อถือเพิ่มเติม** จะได้รับเพิ่มไปยังโซนที่เชื่อถือของอะแดปเตอร์ของเครือข่ายนี้เสมอ (โดยไม่คำนึงถึงประเภทการปกป้องของเครือข่าย)

แจ้งเมื่อเชื่อมต่อเครือข่ายแบบไร้สายที่มีการป้องกันต่ำ – ESET Smart Security Premium จะแจ้งให้คุณทราบเมื่อเชื่อมต่อเครือข่ายแบบไร้สายที่ไม่ได้รับการป้องกันหรือเครือข่ายที่มีการป้องกันต่ำ

โปรไฟล์ไฟร์วอลล์ – เลือกโปรไฟล์ไฟร์วอลล์ที่จะใช้เมื่อเชื่อมต่อกับเครือข่ายนี้

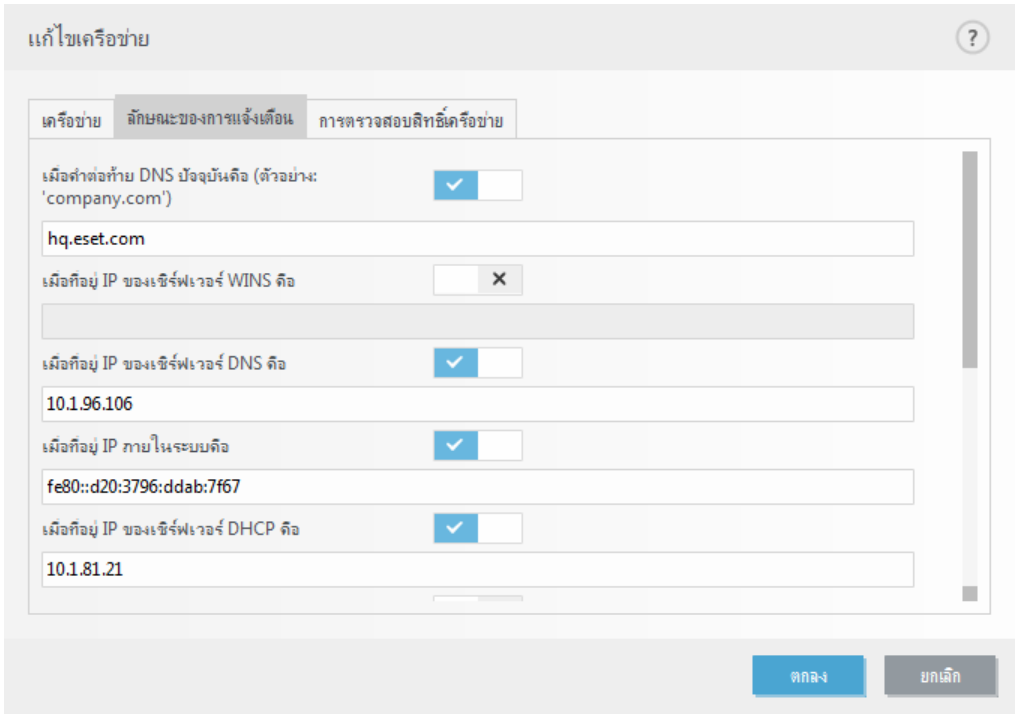
โปรไฟล์การอัพเดท – เลือกโปรไฟล์การอัพเดทที่จะใช้เมื่อเชื่อมต่อกับเครือข่ายนี้

เครือข่ายจะได้รับการทำเครื่องหมายเป็นเชื่อมต่อในรายการเครือข่ายที่เชื่อมต่อต่อเมื่อเป็นไปตามเงื่อนไขดังต่อไปนี้ :

- **การระบุรหัสประจำตัวเครือข่าย** – ข้อมูลที่ป้อนในพารามิเตอร์ทั้งหมดต้องตรงกับพารามิเตอร์ของการเชื่อมต่อที่ใช้งาน
- **การตรวจสอบสิทธิ์เครือข่าย** – ถ้าเลือกเซิร์ฟเวอร์การตรวจสอบสิทธิ์ ต้องผ่านการตรวจสอบสิทธิ์กับเซิร์ฟเวอร์การตรวจสอบสิทธิ์ของ ESET

การระบุรหัสประจำตัวเครือข่าย

ระบบจะใช้การระบุรหัสประจำตัวเครือข่ายตามพารามิเตอร์ของอะแดปเตอร์ของเครือข่ายภายในระบบ พารามิเตอร์ที่เลือกทั้งหมดจะถูกเปรียบเทียบกับพารามิเตอร์จริงของการเชื่อมต่อเครือข่ายที่ใช้งานอยู่ อนุญาตที่อยู่ IPv4 และ IPv6



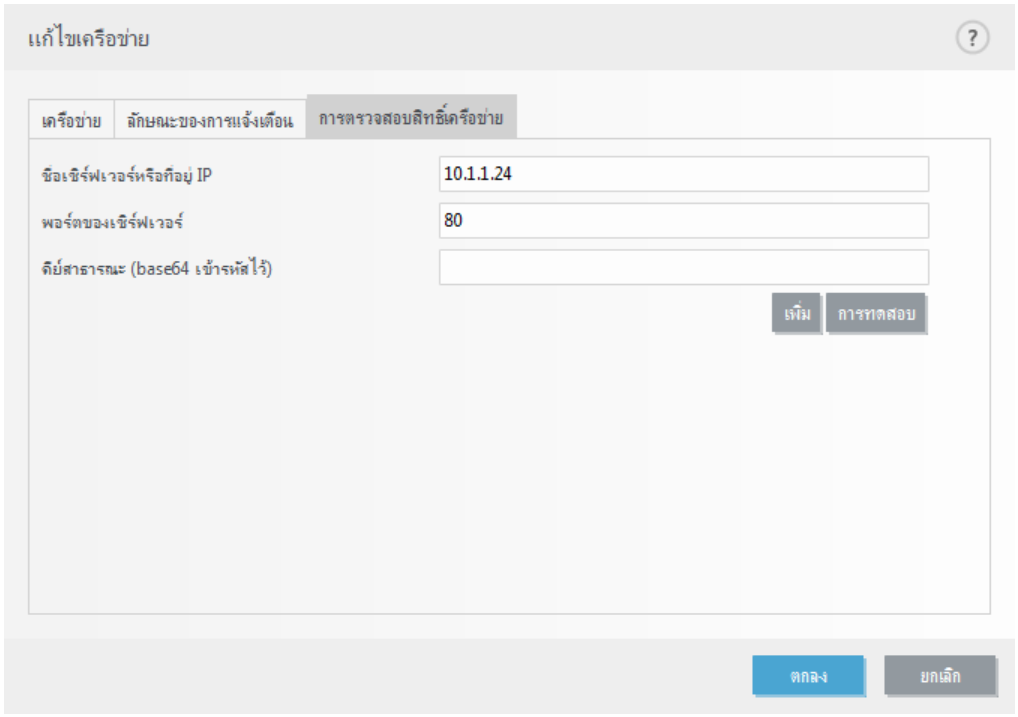
การตรวจสอบสิทธิ์เครือข่าย

การตรวจสอบสิทธิ์ของเครือข่ายจะค้นหาเซิร์ฟเวอร์ที่ต้องการในเครือข่าย และใช้การเข้ารหัสแบบไม่สมมาตร (RSA) เพื่อตรวจสอบสิทธิ์เซิร์ฟเวอร์นั้น ชื่อของเครือข่ายที่ถูกตรวจสอบสิทธิ์ต้องตรงกับชื่อโซนที่อยู่ในการตั้งค่าเซิร์ฟเวอร์การตรวจสอบสิทธิ์ ชื่อต้องตรงตามตัวพิมพ์เล็กและใหญ่ ระบุชื่อเซิร์ฟเวอร์ พอร์ตที่รับข้อมูลของเซิร์ฟเวอร์ และคีย์สาธารณะที่ตรงกับรหัสเซิร์ฟเวอร์ส่วนบุคคล (โปรดดู การตรวจสอบสิทธิ์เครือข่าย – การกำหนดค่าเซิร์ฟเวอร์) สามารถป้อนชื่อเซิร์ฟเวอร์ในรูปแบบที่อยู่ IP หรือ DNS หรือชื่อ NetBios และจะตามด้วยพาธที่ระบุตำแหน่งของรหัสในเซิร์ฟเวอร์ (ตัวอย่างเช่น server_name_/directory1/directory2/authentication) คุณสามารถระบุเซิร์ฟเวอร์สำรองเพื่อใช้เพิ่มไปยังพาธโดยคั่นด้วยเครื่องหมายเซมิโคลอน

ดาวน์โหลดเซิร์ฟเวอร์การตรวจสอบสิทธิ์ของ ESET.

สามารถนำเข้าคีย์สาธารณะโดยใช้ไฟล์ประเภทใดก็ได้ดังต่อไปนี้:

- รหัสสาธารณะที่เข้ารหัส PEM (.pem) คีย์นี้สามารถสร้างขึ้นได้โดยใช้เซิร์ฟเวอร์การตรวจสอบสิทธิ์ของ ESET (โปรดดู การตรวจสอบสิทธิ์เครือข่าย – การกำหนดค่าเซิร์ฟเวอร์)
- รหัสสาธารณะที่เข้ารหัส
- ใบรับรองรหัสสาธารณะ (.crt)



คลิก **ทดสอบ** เพื่อทดสอบการตั้งค่าของคุณ หากการตรวจสอบสิทธิ์เสร็จสมบูรณ์ ข้อความ การตรวจสอบสิทธิ์ของเซิร์ฟเวอร์เสร็จสมบูรณ์ จะปรากฏขึ้น ถ้าไม่กำหนดค่าการตรวจสอบสิทธิ์อย่างถูกต้อง ข้อความแสดงข้อผิดพลาดต่อไปนี้จะปรากฏ:

การตรวจสอบสิทธิ์ของเซิร์ฟเวอร์ล้มเหลว ลายเซ็นไม่ถูกต้องหรือไม่ตรงกัน
ลายเซ็นเซิร์ฟเวอร์ไม่ตรงกับคีย์สาธารณะที่ป้อน

การตรวจสอบสิทธิ์ของเซิร์ฟเวอร์ล้มเหลว ชื่อเครือข่ายไม่ตรงกัน
ชื่อเครือข่ายที่กำหนดค่าไว้ไม่ตรงกับชื่อโซนของเซิร์ฟเวอร์การตรวจสอบสิทธิ์ โปรดตรวจสอบชื่อทั้งสองเพื่อให้แน่ใจว่าเหมือนกัน

การตรวจสอบสิทธิ์ของเซิร์ฟเวอร์ล้มเหลว การตอบรับจากเซิร์ฟเวอร์ไม่ถูกต้องหรือไม่มีการตอบรับ
ไม่ได้รับการตอบกลับถ้าเซิร์ฟเวอร์ไม่ทำงานหรือไม่สามารถเข้าถึงได้ อาจได้รับการตอบกลับที่ไม่ถูกต้องถ้าชื่อเซิร์ฟเวอร์ HTTP อื่นทำงานในที่อยู่ที่ระบุ

ป้อนคีย์สาธารณะไม่ถูกต้อง
ยืนยันว่าไฟล์ของรหัสสาธารณะที่คุณป้อนไม่เสียหาย

การตรวจสอบสิทธิ์เครือข่าย - การกำหนดค่าเซิ

ร์ฟเวอร์

กระบวนการตรวจสอบสิทธิ์จะถูกเรียกใช้โดยคอมพิวเตอร์/เซิร์ฟเวอร์ที่เชื่อมต่อกับเครือข่ายที่จะต้องตรวจสอบสิทธิ์ ต้องมีการติดตั้งแอพพลิเคชันสำหรับเซิร์ฟเวอร์การตรวจสอบสิทธิ์ของ ESET ในคอมพิวเตอร์/เซิร์ฟเวอร์ที่สามารถเข้าถึงเพื่อตรวจสอบสิทธิ์ได้ตลอดเวลา ไม่ว่าไคลเอ็นต์จะพยายามเชื่อมต่อกับเครือข่ายเมื่อใดก็ตาม คุณสามารถดาวน์โหลดไฟล์การติดตั้งสำหรับแอพพลิเคชันเซิร์ฟเวอร์การตรวจสอบสิทธิ์ของ ESET ได้ที่เว็บไซต์ของ ESET

หลังจากติดตั้งแอพพลิเคชันสำหรับเซิร์ฟเวอร์การตรวจสอบสิทธิ์ของ ESET หน้าต่างข้อความจะปรากฏ (คุณสามารถเข้าถึงแอพพลิเคชันโดยคลิก **เริ่มต้น** > **โปรแกรม** > **ESET** > **เซิร์ฟเวอร์การตรวจสอบสิทธิ์ ESET**)

เมื่อต้องการกำหนดค่าเซิร์ฟเวอร์การตรวจสอบสิทธิ์ ให้ป้อนชื่อโซนการตรวจสอบสิทธิ์ พอร์ตที่รับข้อมูลของเซิร์ฟเวอร์ (ค่าเริ่มต้นคือ 80) และตำแหน่งที่เก็บคู่รหัสสาธารณะและส่วนบุคคล จากนั้น ให้สร้างรหัสสาธารณะและส่วนบุคคลที่จะใช้ในกระบวนการตรวจสอบสิทธิ์ รหัสส่วนบุคคลจะถูกตั้งค่าค้างไว้ในเซิร์ฟเวอร์ แต่รหัสสาธารณะต้องนำเข้าจากด้านไคลเอ็นต์ในส่วนการตรวจสอบสิทธิ์ของโซนเมื่อตั้งค่าโซนในการตั้งค่าไฟร์วอลล์

สำหรับข้อมูลที่มีรายละเอียดเพิ่มเติม ให้อ่าน บทความฐานความรู้ของ ESET ต่อไปนี้

การกำหนดค่าโซน

โซนคือชุดรวมของที่อยู่เครือข่ายที่สร้างกลุ่มลอจิคัลของที่อยู่ IP หนึ่งกลุ่ม มีประโยชน์เมื่อมีการใช้ชุดของที่อยู่ชุดเดียวกันอีกครั้งในกฎหลายกฎ ที่อยู่แต่ละแห่งในกลุ่มที่ให้นี้จะได้รับการกำหนดกฎที่คล้ายกัน ซึ่งกำหนดจากส่วนกลางสำหรับกลุ่มทั้งหมด ตัวอย่างหนึ่งของกลุ่มดังกล่าวคือ **โซนที่เชื่อถือ** โซนที่เชื่อถือแสดงถึงกลุ่มของที่อยู่เครือข่ายที่ไม่ถูกปิดกั้นโดยไฟร์วอลล์ไม่ว่าจะอย่างไรก็ตาม

หากต้องการเพิ่มโซนที่เชื่อถือได้ ให้:

1.เปิด **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **ขั้นพื้นฐาน** > **โซน**

2.คลิก **แก้ไข** ถัดจาก **โซน**

3.คลิก **เพิ่ม** พิมพ์ **ชื่อ** และ **คำอธิบาย** สำหรับโซน และพิมพ์ที่อยู่ IP ระยะไกลใน **ที่อยู่คอมพิวเตอร์ระยะไกล (IPv4/IPv6, ช่วง, มาสก์)**

4.คลิก**ตกลง**

สำหรับข้อมูลเพิ่มเติม โปรดดู โซนไฟร์วอลล์

โซนวอลล์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโซน ให้ดูที่ส่วน การกำหนดค่าโซน

คอลัมน์

ชื่อ – ชื่อกลุ่มของคอมพิวเตอร์ระยะไกล

ที่อยู่ IP - ที่อยู่ IP ระยะไกลที่อยู่ในโซน

องค์ประกอบการควบคุม

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

ชื่อ – ชื่อกลุ่มของคอมพิวเตอร์ระยะไกล

คำอธิบาย - คำอธิบายทั่วไปของกลุ่ม

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

ลบ - ลบโซนออกจากรายการ

> i โปรดทราบว่าคุณไม่สามารถลบโซนที่กำหนดค่าไว้ล่วงหน้าแล้วได้

ไฟร์วอลล์

ไฟร์วอลล์จะควบคุมการรับส่งของเครือข่ายทั้งหมดไปยังหรือจากระบบ ซึ่งจะทำงานด้วยการอนุญาตหรือปฏิเสธการเชื่อมต่อเครือข่ายแต่ละแห่งตามกฎการกรองที่กำหนดไว้ การทำเช่นนี้จะให้การป้องกันการโจมตีจากคอมพิวเตอร์ระยะไกลและสามารถปิดกั้นบริการบางอย่างที่เป็นภัยคุกคามได้

พื้นฐาน

เปิดใช้งานไฟร์วอลล์

เราขอแนะนำให้คุณเปิดคุณลักษณะนี้ไว้เพื่อให้แน่ใจว่าระบบของคุณจะปลอดภัยอยู่เสมอ ซึ่งเมื่อเปิดใช้งานไฟร์วอลล์ การรับส่งข้อมูลผ่านเครือข่ายจะถูกสแกนทั้งสองทาง

ประเมินกฎจาก Windows Firewall ด้วยเช่นกัน

ในโหมดอัตโนมัติ จะอนุญาตให้ใช้การรับส่งข้อมูลขาเข้าที่ได้รับการอนุญาตได้ตามกฎจาก Windows Firewall แล้ว เว้นแต่จะถูกปิดกั้นอย่างชัดเจนโดยกฎของ ESET

โหมดการกรอง

การทำงานของไฟร์วอลล์เปลี่ยนแปลงโดยขึ้นอยู่กับโหมดการกรอง โหมดการกรองจะมีผลกับระดับการโต้ตอบของผู้ใช้ที่ต้องการด้วย

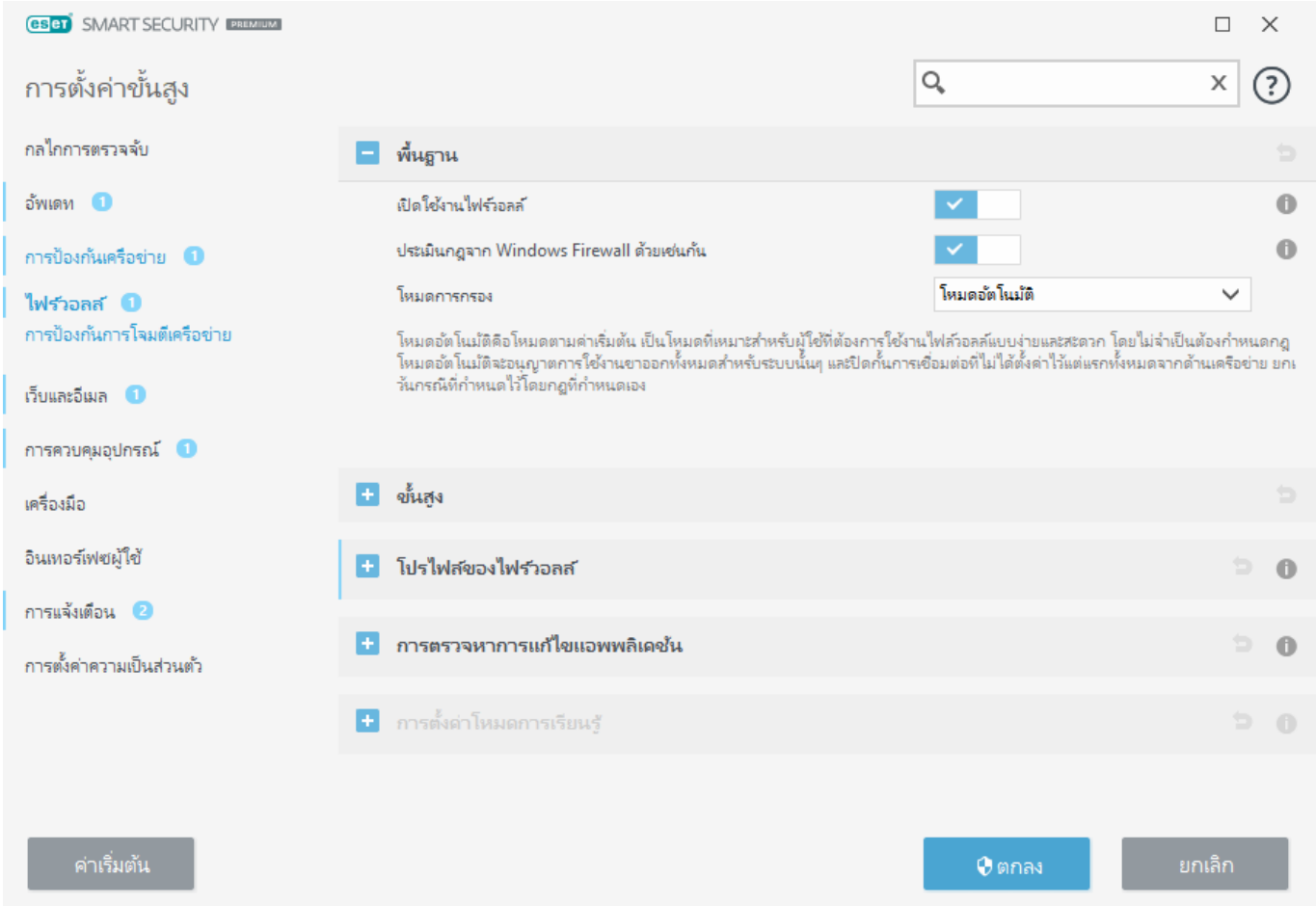
การทำงานของไฟร์วอลล์เปลี่ยนแปลงโดยขึ้นอยู่กับโหมดการกรอง โหมดการกรองจะมีผลกับระดับการโต้ตอบของผู้ใช้ที่ต้องการด้วย โหมดการกรองต่อไปนี้มีให้ใช้งานได้สำหรับไฟร์วอลล์ของ ESET Smart Security Premium:

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 Smart Security Premium จะบันทึกกฎตามพารามิเตอร์ที่กำหนดไว้ล่วงหน้า ควรใช้โหมดการเรียนรู้จนกว่ากฎทั้งหมดสำหรับการสื่อสารที่จำเป็นจะถูกสร้างขึ้นเพื่อป้องกันความเสี่ยงด้านความปลอดภัย

ขั้นสูง

กฎ

การตั้งค่ากฎจะอนุญาตให้คุณดูกฎทั้งหมดที่ใช้สำหรับการรับส่งข้อมูลที่สร้างโดยแอพพลิเคชันแต่ละรายการภายในโซนที่เชื่อถือและอินเทอร์เน็ต



คุณสามารถสร้างกฎ IDS เมื่อ บอทเน็ต โจมตีคอมพิวเตอร์ของคุณได้ โดยคุณสามารถแก้ไขกฎใน **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **การป้องกันการโจมตีเครือข่าย (IDS)** > **กฎ IDS** ได้ด้วยการคลิกที่ **แก้ไข**

บริการที่อนุญาต

กำหนดค่าการเข้าถึงบริการเครือข่ายทั่วไปที่ทำงานอยู่บนคอมพิวเตอร์ของคุณ โปรดตรวจสอบการให้บริการที่อนุญาตสำหรับข้อมูลเพิ่มเติม

โปรไฟล์ไฟร์วอลล์

โปรไฟล์ไฟร์วอลล์ สามารถนำมาใช้เพื่อปรับแต่งการทำงานของไฟร์วอลล์ ESET Smart Security Premium โดยระบุชุดกฎที่แตกต่างกันออกไปในสถานการณ์ที่แตกต่างกัน

การตรวจหาการแก้ไขแอพพลิเคชัน

คุณสมบัติการตรวจหาการแก้ไขแอพพลิเคชัน จะแสดงการแจ้งเตือนหากมีแอพพลิเคชันที่ถูกแก้ไขซึ่งมีกฎไฟร์วอลล์พยายามเริ่มต้นการเชื่อมต่อ

โปรไฟล์ไฟร์วอลล์

โปรไฟล์สามารถใช้เพื่อควบคุมการทำงานของไฟร์วอลล์ของ ESET Smart Security Premium เมื่อสร้างหรือแก้ไขกฎไฟร์วอลล์ คุณสามารถกำหนดกฎให้โปรไฟล์ที่ต้องการหรือใช้กฎกับทุกโปรไฟล์ได้ เมื่อมีโปรไฟล์ทำงานในส่วนติดต่อเครือข่าย โปรไฟล์จะใช้เฉพาะกฎร่วม (กฎที่ไม่ระบุโปรไฟล์) และกฎที่ระบุไปที่โปรไฟล์นั้นเท่านั้น คุณสามารถสร้างโปรไฟล์ได้หลายรายการซึ่งกำหนดกฎแตกต่างกันไปยังอะแดปเตอร์เครือข่ายหรือกำหนดไปยังเครือข่ายเพื่อแก้ไขการทำงานของไฟร์วอลล์ได้อย่างง่ายดาย

คลิก **แก้ไข** ที่อยู่ถัดจาก รายการของโปรไฟล์ เพื่อเปิดหน้าต่าง **โปรไฟล์ของไฟร์วอลล์** ที่ๆ คุณสามารถแก้ไขโปรไฟล์

อะแดปเตอร์เครือข่ายสามารถตั้งค่าให้ใช้โปรไฟล์ที่กำหนดค่าสำหรับเครือข่ายเฉพาะเมื่อเชื่อมต่อกับเครือข่ายนั้นได้ คุณยังสามารถกำหนดโปรไฟล์เฉพาะเพื่อใช้เมื่ออยู่บนเครือข่ายที่กำหนดใน **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **เครือข่ายที่รู้จัก** > **แก้ไข** เลือกเครือข่ายจากรายการ **เครือข่ายที่รู้จัก** และคลิก **แก้ไข** เพื่อกำหนดโปรไฟล์ไฟร์วอลล์ให้กับเครือข่ายเฉพาะจากเมนูแบบเลื่อนลง **โปรไฟล์ไฟร์วอลล์**

หากเครือข่ายนั้นไม่มีโปรไฟล์ที่กำหนด ระบบจะใช้โปรไฟล์เริ่มต้นของอะแดปเตอร์ หากอะแดปเตอร์ถูกตั้งค่าให้ไม่ใช้โปรไฟล์ของเครือข่าย ระบบจะใช้โปรไฟล์เริ่มต้นไม่ว่าจะเชื่อมต่อกับเครือข่ายใด หากไม่มีโปรไฟล์สำหรับเครือข่ายหรือการกำหนดค่าอะแดปเตอร์ ระบบจะใช้โปรไฟล์เริ่มต้นส่วนกลาง ในการกำหนดโปรไฟล์ให้กับอะแดปเตอร์เครือข่าย ให้เลือกอะแดปเตอร์เครือข่าย คลิก **แก้ไข** ถัดจาก **โปรไฟล์ที่กำหนดให้กับอะแดปเตอร์เครือข่าย** แก้ไขอะแดปเตอร์เครือข่ายที่เลือกและเลือกโปรไฟล์จากเมนูแบบเลื่อนลง **โปรไฟล์ไฟร์วอลล์เริ่มต้น**

เมื่อสลับไฟร์วอลล์ไปยังโปรไฟล์อื่น การแจ้งเตือนจะปรากฏที่มุมขวาล่างใกล้กับนาฬิการะบบ

หน้าต่างข้อความ - แก้ไขโปรไฟล์ไฟร์วอลล์

ที่ส่วนนี้ คุณสามารถ **เพิ่ม**, **แก้ไข** หรือ **ลบ** โปรไฟล์ได้ โปรดทราบว่าในการ **แก้ไข** หรือ **ลบ** โปรไฟล์ จะต้องไม่มีการเลือกจากรายการในหน้าต่าง **ไฟร์วอลล์โปรไฟล์**

สำหรับข้อมูลเพิ่มเติม ให้ดูที่หัวข้อ โปรไฟล์ไฟร์วอลล์

โปรไฟล์ที่มอบหมายให้อะแดปเตอร์เครือข่าย

ด้วยการสลับโปรไฟล์ คุณสามารถทำการเปลี่ยนแปลงหลายอย่างไปยังการทำงานของไฟร์วอลล์ได้อย่างรวดเร็ว สามารถตั้งค่ากฎที่กำหนดเองและใช้สำหรับโปรไฟล์เฉพาะ รายการอะแดปเตอร์เครือข่ายสำหรับอะแดปเตอร์ทั้งหมดที่อยู่ในเครื่องจะเพิ่มไปยังรายการ **อะแดปเตอร์เครือข่าย** โดยอัตโนมัติ

คอลัมน์

ชื่อ – ชื่อของอะแดปเตอร์เครือข่าย

โปรไฟล์ไฟร์วอลล์ตามค่าเริ่มต้น – ใช้โปรไฟล์ค่าเริ่มต้นเมื่อเครือข่ายที่คุณเชื่อมต่อไม่มีโปรไฟล์ที่กำหนดค่าหรืออะแดปเตอร์เครือข่ายของคุณตั้งค่าไว้ไม่ให้ใช้โปรไฟล์เครือข่าย

เลือกใช้โปรไฟล์ของเครือข่ายมากกว่า – เมื่อเปิดใช้งาน **เลือกใช้ไฟร์วอลล์ของเครือข่ายที่เชื่อมต่อมากกว่า** อะแดปเตอร์เครือข่ายจะใช้งานโปรไฟล์ไฟร์วอลล์ที่กำหนดไปยังเครือข่ายที่เชื่อมต่อในทุกครั้งที่สามารถทำได้

องค์ประกอบการควบคุม

เพิ่ม – เพิ่มอะแดปเตอร์เครือข่ายใหม่

แก้ไข – อนุญาตให้คุณแก้ไขอะแดปเตอร์เครือข่ายที่มีอยู่

ลบออก – เลือกอะแดปเตอร์เครือข่ายและคลิก **ลบออก**ถ้าคุณต้องการลบอะแดปเตอร์เครือข่ายออกจากรายการ

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

การกำหนดค่าและการใช้กฎ

กฎจะมีเงื่อนไขจำนวนหนึ่งที่ใช้เพื่อทดสอบการเชื่อมต่อเครือข่ายทั้งหมดอย่างสมเหตุสมผล และการทำงานทั้งหมดที่กำหนดไปยังเงื่อนไขเหล่านี้ เมื่อใช้ กฎไฟร์วอลล์ คุณสามารถกำหนดการกระทำที่จะดำเนินการเมื่อเริ่มต้นการเชื่อมต่อเครือข่ายประเภทต่างๆ ได้ ในการเข้าถึงการตั้งค่าการกรองกฎ ให้ไปที่ **การตั้งค่าขั้นสูง** (F5) > **ไฟร์วอลล์** > **ขั้นสูง** กฎที่กำหนดล่วงหน้าบางกฎเชื่อมโยงอยู่กับกล่องทำเครื่องหมายใน **บริการที่อนุญาต** (IDS และตัวเลือกขั้นสูง) และจะไม่สามารถปิดได้โดยตรง ซึ่งคุณสามารถใช้กล่องทำเครื่องหมายที่เชื่อมโยงกันดังกล่าวในการปิดแทนได้

ต่างจาก ESET Smart Security Premium เวอร์ชันที่ผ่านมา กฎจะถูกประเมินจากบนลงล่าง การทำงานของกฎการจับคู่แรกจะใช้กับแต่ละการเชื่อมต่อเครือข่ายที่ถูกประเมิน นี่เป็นการเปลี่ยนแปลงการทำงานที่สำคัญจากเวอร์ชันที่ผ่านมา ซึ่งลำดับความสำคัญของกฎจะถูกกำหนดโดยอัตโนมัติและกฎที่เจาะจงกว่ามีความสำคัญมากกว่ากฎทั่วไป

การเชื่อมต่อจะแบ่งออกเป็นการเชื่อมต่อขาเข้าและขาออก การเชื่อมต่อขาเข้าจะสร้างขึ้นโดยคอมพิวเตอร์ระยะไกลที่พยายามสร้างการเชื่อมต่อกับระบบภายใน การเชื่อมต่อขาออกจะทำงานในทางกลับกัน โดยระบบภายในจะติดต่อกับคอมพิวเตอร์ระยะไกล

ถ้าระบบตรวจพบการสื่อสารที่ไม่รู้จัก คุณต้องพิจารณาอย่างรอบคอบว่าจะอนุญาตหรือปฏิเสธการสื่อสารนี้ การเชื่อมต่อที่ไม่พึงประสงค์ ไม่ปลอดภัย หรือไม่รู้จักอาจทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบ หากมีการสร้างการเชื่อมต่อดังกล่าว เราขอแนะนำให้คุณให้ความสนใจเป็นพิเศษต่อคอมพิวเตอร์ระยะไกลและแอพพลิเคชันที่พยายามจะเชื่อมต่อกับคอมพิวเตอร์ของคุณ การแฝงตัวจำนวนมากพยายามที่จะหาและส่งข้อมูลส่วนบุคคล หรือดาวน์โหลดแอพพลิเคชันที่เป็นอันตรายต่อเวิร์กสเตชันของโฮสต์ ไฟร์วอลล์จะช่วยให้คุณสามารถตรวจหาและสิ้นสุดการเชื่อมต่อดังกล่าว

รายการกฎของไฟร์วอลล์

รายการกฎของไฟร์วอลล์สามารถพบได้ใน **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **ไฟร์วอลล์** > **ขั้นสูง** โดยคลิก **แก้ไข** ถัดจาก **กฎ**

คอลัมน์

ชื่อ – ชื่อของกฎ

เปิดใช้งาน – แสดงว่ากฎกำลังเปิดใช้งานหรือปิดใช้งานอยู่ โดยต้องเลือกช่องทำเครื่องหมายที่ตรงกันเพื่อเปิดใช้กฎ

โปรโตคอล – โปรโตคอลที่ถูกต้องสำหรับกฎนี้

โปรไฟล์ – แสดงโปรไฟล์ไฟร์วอลล์ที่ถูกต้องสำหรับกฎนี้

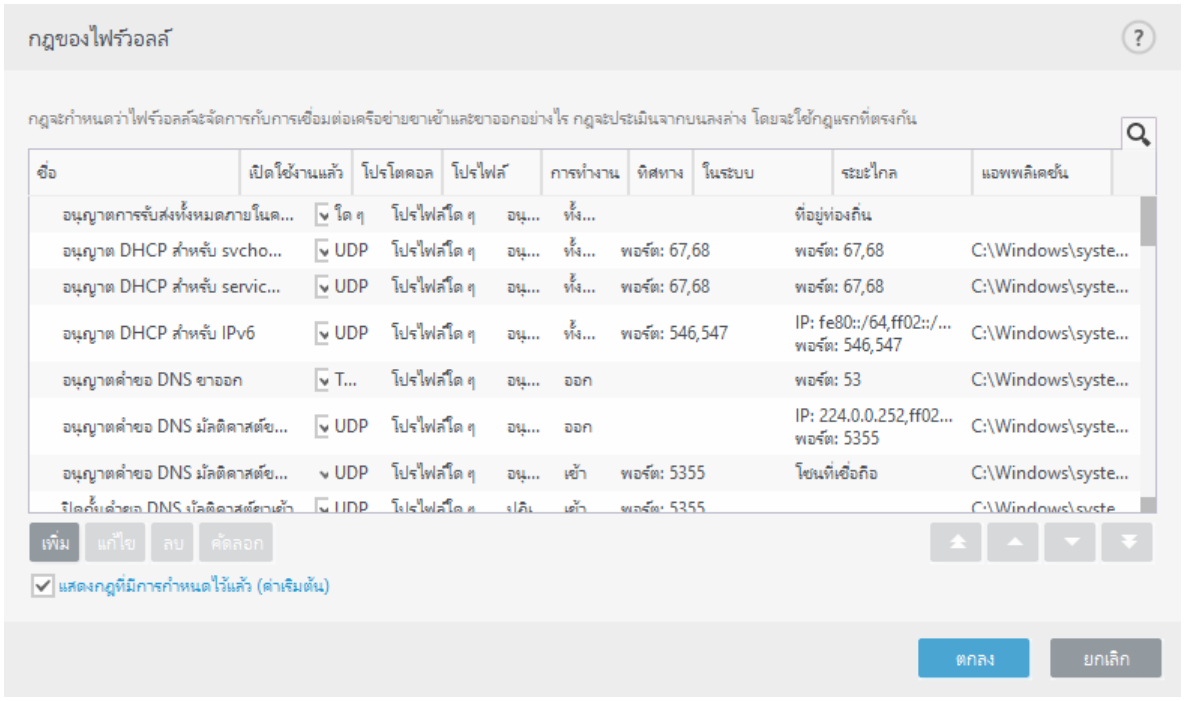
การทำงาน – แสดงสถานะของการสื่อสาร (ปิดกั้น/อนุญาต/ถาม)

ทิศทาง – ทิศทางของการสื่อสาร (ขาเข้า/ขาออก/สองทาง)

ในระบบ – ที่อยู่ / ช่วง / ซับเน็ต IPv4 หรือ IPv6 ระยะไกลและพอร์ตของคอมพิวเตอร์ในระบบ

ระยะไกล – ที่อยู่ / ช่วง / ซับเน็ต IPv4 หรือ IPv6 ระยะไกลและพอร์ตของคอมพิวเตอร์ระยะไกล

แอพพลิเคชัน – แอพพลิเคชันที่จะใช้กฎนี้



องค์ประกอบการควบคุม

เพิ่ม – สร้างกฎใหม่

แก้ไข – แก้ไขกฎที่มีอยู่

ลบออก – ลบกฎที่มีอยู่

คัดลอก - สร้างสำเนาของกฎที่เลือก

แสดงกฎที่มีในตัว (กำหนดไว้ก่อน) – กฎที่กำหนดไว้ล่วงหน้าโดย ESET Smart Security Premium ซึ่งอนุญาตหรือ

ปฏิเสธการสื่อสารที่ระบุ คุณสามารถปิดใช้งานกฎเหล่านี้ แต่คุณไม่สามารถลบกฎที่กำหนดไว้ล่วงหน้า

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

คลิกไอคอนการค้นหา ตรงมุมบนขวาเพื่อค้นหากฎโดยใช้ชื่อ โปรโตคอล หรือพอร์ต

การเพิ่มหรือแก้ไขกฎของไฟร์วอลล์

ต้องมีการแก้ไขในแต่ละครั้งที่เปลี่ยนแปลงพารามิเตอร์ที่ตรวจสอบ ถ้ามีการเปลี่ยนแปลงที่ทำให้กฎดังกล่าวไม่สามารถตอบสนองต่อเงื่อนไขและไม่สามารถใช้การทำงานที่ระบุได้ การเชื่อมต่อที่ใช้งานอยู่อาจถูกปฏิเสธ นี่อาจทำให้เกิดปัญหากับการทำงานของแอพพลิเคชันที่ได้รับผลจากกฎ ตัวอย่างคือการเปลี่ยนแปลงที่อยู่ของเครือข่ายหรือเลขที่พอร์ตสำหรับด้านระยะไกล

คำแนะนำพร้อมภาพประกอบ

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:

- เปิดหรือปิด (อนุญาตหรือปฏิเสธ) พอร์ตเฉพาะบน ESET ไฟร์วอลล์
- สร้างกฎของไฟร์วอลล์จากไฟล์บันทึกใน ESET Smart Security Premium

ด้านบนของหน้าต่างนี้จะประกอบด้วยแท็บสามแท็บ:

- **ทั่วไป** – ระบุชื่อกฎ ทิศทางของการเชื่อมต่อ การทำงาน (**อนุญาต ปฏิเสธ ถาม**) โปรโตคอล และโปรไฟล์ที่จะใช้กฎ
- **ในระบบ** – แสดงข้อมูลเกี่ยวกับด้านภายในระบบของการเชื่อมต่อ ได้แก่ จำนวนของพอร์ตในระบบหรือช่วงของพอร์ต และชื่อของแอพพลิเคชันการสื่อสาร และยังอนุญาตให้คุณเพิ่มโซนที่กำหนดไว้ล่วงหน้าหรือโซนที่สร้างขึ้นด้วยช่วงของที่อยู่ IP ที่นี่ด้วยการคลิก **เพิ่ม**
- **ระยะไกล** – แท็บนี้จะมีข้อมูลเกี่ยวกับพอร์ตระยะไกล (ช่วงพอร์ต) ซึ่งจะช่วยให้คุณกำหนดรายการของที่อยู่ IP หรือโซนระยะไกลสำหรับกฎที่มีให้ คุณยังสามารถเพิ่มโซนที่กำหนดไว้ล่วงหน้าหรือโซนที่สร้างขึ้นด้วยช่วงของที่อยู่ IP ที่นี่ด้วยการคลิก **เพิ่ม**

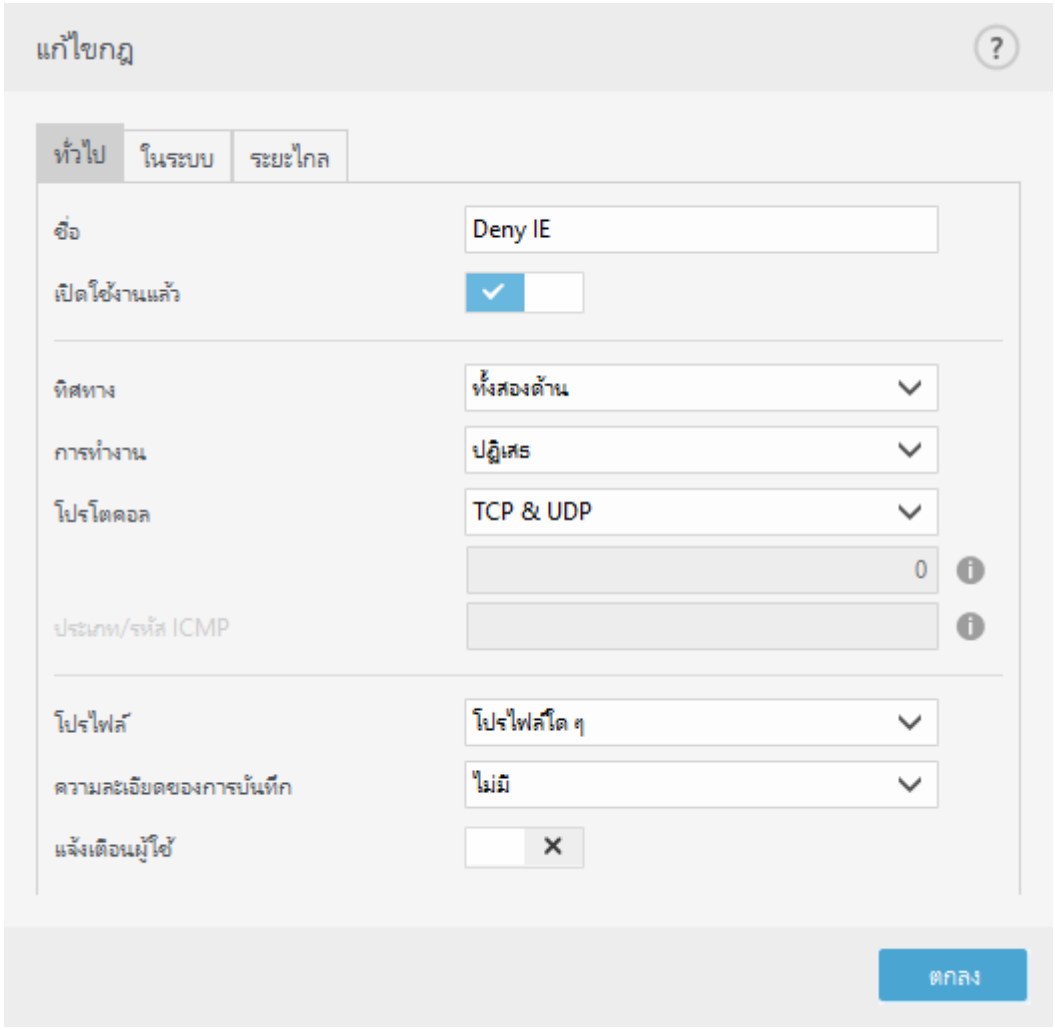
เมื่อสร้างกฎใหม่ คุณต้องพิมพ์ชื่อของกฎในช่อง **ชื่อ** เลือกทิศทางที่จะใช้กฎจากเมนูแบบเลื่อนลง **ทิศทาง** และการทำงานเมื่อการสื่อสารตรงตามกฎจากเมนูแบบเลื่อนลง **การทำงาน**

โปรโตคอล แสดง โปรโตคอลการรับส่งข้อมูลที่ใช้สำหรับกฎ เลือกโปรโตคอลที่ใช้สำหรับกฎที่มีให้จากเมนูแบบเลื่อนลง

ประเภท/รหัส ICMP แสดงถึงข้อความ ICMP ซึ่งระบุโดยตัวเลขหนึ่งหลัก (ตัวอย่างเช่น 0 แสดงถึง "ตอบกลับการสะท้อน")

กฎทั้งหมดจะเปิดใช้สำหรับ **โปรไฟล์ใดๆ** ตามค่าเริ่มต้น หรืออีกวิธีหนึ่ง ให้เลือกโปรไฟล์ของไฟร์วอลล์ที่กำหนดเองโดยใช้เมนูแบบเลื่อนลง **โปรไฟล์**

ถ้าคุณเปิดใช้งาน **ความรุนแรงของการบันทึก** การทำงานที่เชื่อมต่อกับกฎนั้นจะถูกบันทึกลงในบันทึก **แจ้งผู้ใช้** จะแสดงการแจ้งเตือนเมื่อมีการปรับใช้กฎ



เราสร้างกฎใหม่เพื่ออนุญาตให้แอพพลิเคชันเว็บเบราว์เซอร์ Firefox เข้าถึง Internet / เว็บไซต์เครือข่ายภายในระบบได้ ในตัวอย่างนี้ ต้องมีการกำหนดค่ารายการต่อไปนี้:
1.ในแท็บ **ทั่วไป** ให้เปิดใช้งานการสื่อสารขาออกผ่านโปรโตคอล TCP และ UDP
2.คลิกแท็บ**ในระบบ**
3.เลือกพาธไฟล์ของเว็บเบราว์เซอร์ที่คุณใช้โดยการคลิก **...** (ตัวอย่างเช่น *C:\Program Files\Firefox\Firefox.exe*) (ตัวอย่างเช่น C:\Program Files\Firefox\Firefox.exe) อย่าป้อนชื่อของแอพพลิเคชัน
4.ในแท็บ **ระยะไกล** ให้เปิดใช้งานหมายเลขพอร์ต 80 และ 443 เมื่อคุณต้องการอนุญาตอินเทอร์เน็ตแบบมาตรฐาน

โปรดทราบว่า กฎที่กำหนดไว้ล่วงหน้าสามารถแก้ไขได้จำกัด

กฎไฟร์วอลล์ - ในระบบ

ระบุชื่อของแอพพลิเคชันในระบบและพอร์ตหนึ่งพอร์ต/หลายพอร์ตในระบบที่ปรับใช้กฎ

พอร์ต – เลขที่พอร์ตระยะไกล หากไม่มีการระบุเลขที่ไว้ กฎจะมีผลใช้งานกับพอร์ตทั้งหมด เพิ่มพอร์ตการสื่อสารรายการเดียวหรือเพิ่มช่วงของพอร์ตการสื่อสาร

IP - อนุญาตให้คุณเพิ่มที่อยู่ระยะไกลหนึ่งที่อยู่/หลายที่อยู่ ช่วงของที่อยู่ หรือซับเน็ตที่กฎจะปรับใช้ หากไม่มีการระบุค่าไว้ กฎจะมีผลใช้งานกับการสื่อสารทั้งหมด

โซน – รายการโซนที่เพิ่ม

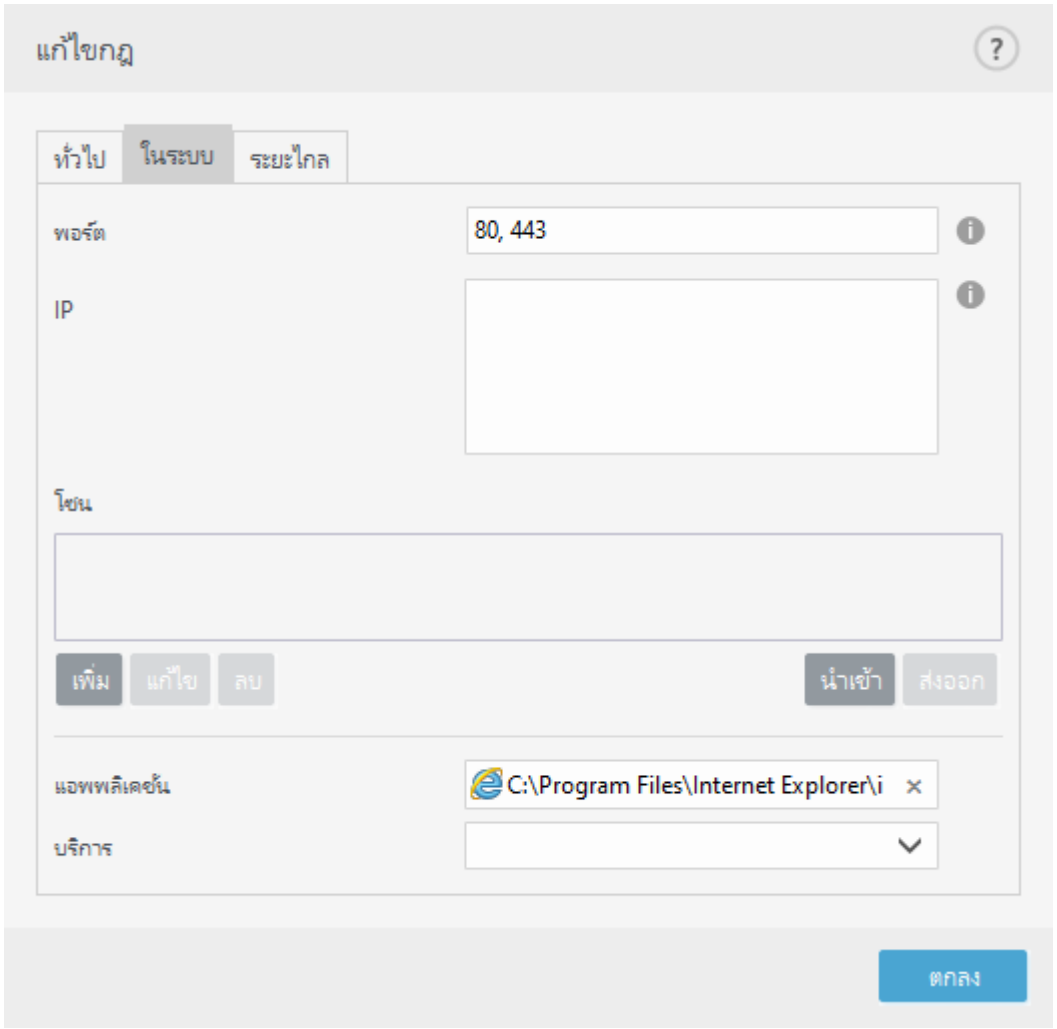
เพิ่ม – เพิ่มโซนที่สร้างจากเมนูแบบเลื่อนลง เมื่อต้องการสร้างโซน ให้ใช้แท็บ การตั้งค่าโซน

ลบออก – ลบโซนออกจากรายการ

แอพพลิเคชัน – ชื่อของแอพพลิเคชันที่จะใช้กฎ เพิ่มตำแหน่งของแอพพลิเคชันที่จะใช้กฎ

บริการ – เมนูแบบเลื่อนลงแสดงบริการของระบบ

> คุณอาจต้องการสร้างกฎสำหรับมิเรอร์ของคุณที่จะให้การอัพเดทผ่านพอร์ต 2221 โดยใช้บริการEHttpSrv เพื่อการสื่อสารในเมนูแบบเลื่อนลง



กฎไฟร์วอลล์ - ระยะไกล

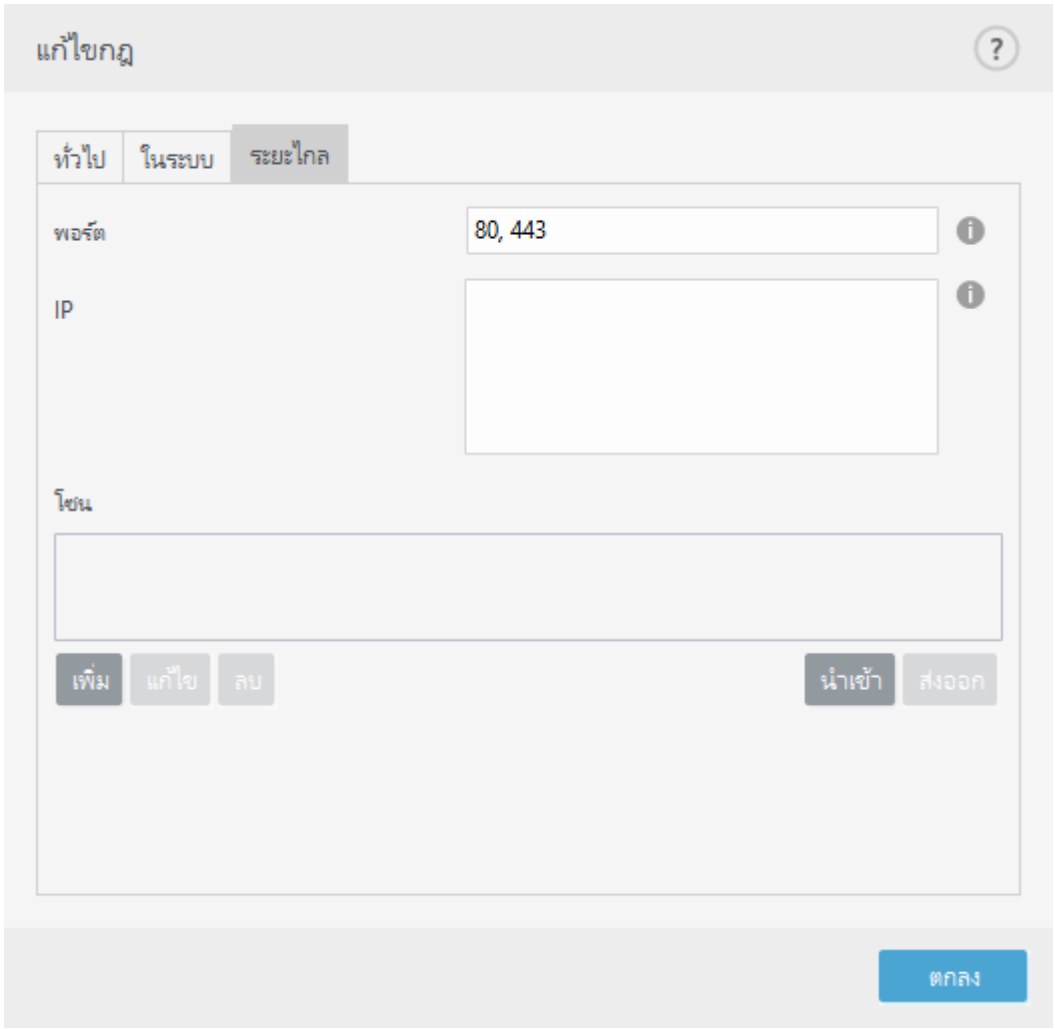
พอร์ต – เลขที่พอร์ตระยะไกล หากไม่มีการระบุเลขที่ไว้ กฎจะมีผลใช้งานกับพอร์ตทั้งหมด เพิ่มพอร์ตการสื่อสารรายการเดียวหรือเพิ่มช่วงของพอร์ตการสื่อสาร

IP - ช่วยให้คุณสามารถเพิ่มที่อยู่ระยะไกล ช่วงที่อยู่ หรือซับเน็ต ที่อยู่ ช่วง/ซับเน็ต หรือโซนระยะไกลซึ่งจะใช้กฎ หากไม่มีการระบุค่าไว้ กฎจะมีผลใช้งานกับการสื่อสารทั้งหมด

โซน – รายการโซนที่เพิ่ม

เพิ่ม - เพิ่มโซนด้วยการเลือกจากเมนูแบบเลื่อนลง เมื่อต้องการสร้างโซน ให้ใช้แท็บ การตั้งค่าโซน

ลบออก – ลบโซนออกจากรายการ



การตรวจหาการแก้ไขแอพพลิเคชัน

คุณสมบัติการตรวจหาการแก้ไขแอพพลิเคชัน จะแสดงการแจ้งเตือนหากมีแอพพลิเคชันที่ถูกแก้ไขซึ่งมีกฎไฟร์วอลล์พยายามเริ่มต้นการเชื่อมต่อ การแก้ไขแอพพลิเคชันคือกลไกของการแทนที่แอพพลิเคชันดั้งเดิมด้วยแอพพลิเคชันอื่นเป็นการชั่วคราวหรือโดยถาวรโดยไฟล์ที่เรียกใช้ได้ที่แตกต่างกัน (ป้องกันกฎไฟร์วอลล์ที่ไม่เหมาะสม)

โปรดทราบว่าคุณลักษณะนี้ไม่ได้สร้างขึ้นเพื่อตรวจหาการแก้ไขของแอพพลิเคชันใดๆ โดยทั่วไป เป้าหมายคือเพื่อหลีกเลี่ยงกฎของไฟร์วอลล์ที่ไม่เหมาะสม และจะตรวจสอบเฉพาะแอพพลิเคชันที่มีกฎของไฟร์วอลล์ที่ระบุเท่านั้น

เปิดใช้งานการตรวจหาการแก้ไขแอพพลิเคชัน – ถ้าเลือกตัวเลือกนี้ โปรแกรมจะตรวจสอบแอพพลิเคชันเพื่อหาการเปลี่ยนแปลง (การอัพเดท การติดไวรัส การแก้ไขอื่นๆ) เมื่อแอพพลิเคชันที่แก้ไขพยายามเริ่มต้นการเชื่อมต่อไฟร์วอลล์จะแจ้งให้คุณทราบ

อนุญาตให้มีการแก้ไขแอพพลิเคชันที่ลงชื่อ (เชื่อถือ) – ไม่ต้องแจ้งเตือนถ้าแอพพลิเคชันก่อนและหลังการแก้ไขมีลายเซ็นดิจิทัลที่ถูกต้องและเป็นลายเดียวกัน

รายชื่อแอพพลิเคชันที่ยกเว้นจากการตรวจหา – หน้าต่างนี้จะให้คุณเพิ่มหรือลบแอพพลิเคชันแต่ละรายการออกจากรายการที่อนุญาตให้แก้ไขโดยไม่ต้องแจ้งเตือน

รายการแอพพลิเคชันที่ยกเว้นจากการตรวจหา

ไฟร์วอลล์ใน ESET Smart Security Premium จะตรวจหาการเปลี่ยนแปลงของแอพพลิเคชันที่มีกฎ (โปรดดู การตรวจหาการแก้ไขแอพพลิเคชัน)

ในบางกรณี คุณอาจไม่ต้องการใช้ฟังก์ชันนี้สำหรับบางแอพพลิเคชัน ถ้าคุณต้องการยกเว้นจากการตรวจสอบโดยไฟร์วอลล์

เพิ่ม – เปิดหน้าต่างซึ่งคุณสามารถเลือกแอพพลิเคชันเพื่อเพิ่มไปยังรายการแอพพลิเคชันที่ยกเว้นจากการตรวจหาการแก้ไขได้ คุณสามารถเลือกจากรายการแอพพลิเคชันที่กำลังทำงานอยู่ได้ด้วยการสื่อสารบนเครือข่ายแบบเปิดซึ่งมีกฎไฟร์วอลล์อยู่ หรือเพิ่มแอพพลิเคชันเฉพาะ

แก้ไข – เปิดหน้าต่างซึ่งคุณสามารถเปลี่ยนตำแหน่งของแอพพลิเคชันที่อยู่ในรายการแอพพลิเคชันที่ยกเว้นจากการตรวจหาการแก้ไขได้ คุณสามารถเลือกจากรายการแอพพลิเคชันที่กำลังทำงานอยู่ได้ด้วยการสื่อสารบนเครือข่ายแบบเปิดซึ่งมีกฎไฟร์วอลล์อยู่ หรือเปลี่ยนตำแหน่งที่ตั้งด้วยตนเอง

ลบออก – ลบรายการออกจากรายการแอพพลิเคชันที่ยกเว้นจากการตรวจหาการแก้ไข

การตั้งค่าโหมดการเรียนรู้

โหมดเรียนรู้จะสร้างและบันทึกกฎของการสื่อสารแต่ละรายการที่สร้างขึ้นในระบบโดยอัตโนมัติ ผู้ใช้ไม่จำเป็นต้องดำเนินการใดๆ เนื่องจาก ESET Smart Security Premium จะบันทึกกฎตามพารามิเตอร์ที่กำหนดไว้ล่วงหน้า

โหมดนี้สามารถก่อให้เกิดความเสี่ยงต่อระบบของคุณได้ และโหมดนี้แนะนำให้ใช้เพื่อการกำหนดค่าเริ่มต้นของไฟร์วอลล์เท่านั้น

เลือก **โหมดเรียนรู้** จากเมนูแบบเลื่อนลงใน **การตั้งค่าขั้นสูง** (F5) > **ไฟล์วอลล์** > **พื้นฐาน** > **โหมดการกรอง** เพื่อเปิดใช้ **ตัวเลือกโหมดเรียนรู้** ในส่วนนี้จะมีรายการต่อไปนี้:

ขณะที่อยู่ในโหมดการเรียนรู้ ไฟร์วอลล์จะไม่กรองการสื่อสาร โดยจะอนุญาตการสื่อสารขาเข้าและขาออกทั้งหมด ในโหมดนี้ คอมพิวเตอร์ของคุณจะไม่ได้รับการป้องกันโดยไฟร์วอลล์

โหมดที่ได้รับการตั้งค่าหลังจากโหมดการเรียนรู้หมดอายุ – ระบุโหมดการกรองที่ไฟร์วอลล์ของ ESET Smart Security Premium จะแปลงไปยังช่วงเวลาหลังจากโหมดการเรียนรู้สิ้นสุด อ่านข้อมูลเพิ่มเติมเกี่ยวกับ โหมดการกรอง หลังจากหมดอายุ ตัวเลือก **ถามผู้ใช้** จะต้องใช้สิทธิ์อนุญาตของผู้ดูแลระบบเพื่อทำการเปลี่ยนแปลงโหมดการกรองไฟร์วอลล์

ประเภทการสื่อสาร – เลือกพารามิเตอร์การสร้างกฎที่ต้องการสำหรับการสื่อสารแต่ละประเภท การสื่อสารมีทั้งหมดสี่ประเภท:

- **การรับส่งขาเข้าจากโซนที่เชื่อถือ** – ตัวอย่างของการเชื่อมต่อขาเข้าภายในโซนที่เชื่อถือจะเป็นคอมพิวเตอร์ระยะไกลจากภายในโซนที่เชื่อถือ ซึ่งพยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันในระบบที่ทำงานบนคอมพิวเตอร์ของคุณ

- **การรับส่งขาออกไปยังโซนที่เชื่อถือ** – แอพพลิเคชันในระบบที่พยายามสร้างการเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่นภายในเครือข่ายในระบบ หรือภายในเครือข่ายในโซนที่เชื่อถือ

- **การรับส่งทางอินเทอร์เน็ตขาเข้า** – คอมพิวเตอร์ระยะไกลที่พยายามสื่อสารกับแอพพลิเคชันที่ทำงานบนคอมพิวเตอร์

- **การรับส่งทางอินเทอร์เน็ตขาออก** – แอพพลิเคชันในระบบที่พยายามสร้างการเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่น

แต่ละส่วนอนุญาตให้คุณระบุพารามิเตอร์ที่จะเพิ่มไปยังกฎสร้างใหม่:

เพิ่มพอร์ตในระบบ – รวมเลขที่พอร์ตในระบบของการสื่อสารในเครือข่าย สำหรับการสื่อสารขาออก โดยทั่วไประบบจะสร้างเลขที่แบบสุ่ม 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 ตัวเลือกนี้เหมาะสำหรับกรณีที่คุณต้องการกำหนดการดำเนินการสำหรับคอมพิวเตอร์บางเครื่องหรือกลุ่มของคอมพิวเตอร์ในเครือข่าย

จำนวนกฎสูงสุดสำหรับแอพพลิเคชัน – ถ้าแอพพลิเคชันสื่อสารผ่านหลายพอร์ตไปยังที่อยู่ IP ต่างๆ เป็นต้น ไฟร์วอลล์ในโหมดเรียนรู้จะสร้างจำนวนกฎที่เหมาะสมสำหรับแอพพลิเคชันนี้ ตัวเลือกนี้อนุญาตให้คุณจำกัดจำนวนกฎที่สามารถสร้างได้สำหรับแอพพลิเคชันหนึ่ง

เปิดใช้งานการป้องกันการโจมตีเครือข่าย (IDS)

การป้องกันการโจมตีเครือข่าย (IDS) จะปรับปรุงการตรวจหาช่องโหว่ของจุดอ่อนที่รู้จัก อ่านเพิ่มเติมเกี่ยวกับการป้องกันการโจมตีเครือข่ายใน ประมวลศัพท์

การป้องกันการโจมตีเครือข่าย (IDS) – วิเคราะห์เนื้อหาของการรับส่งของเครือข่ายและป้องกันการโจมตีเครือข่าย การรับส่งใด ๆ ที่ได้รับพิจารณาว่าเป็นอันตรายจะถูกปิดกั้น

เปิดใช้งานการป้องกันบอตเน็ต – ตรวจหาและปิดกั้นการสื่อสารกับคำสั่งที่เป็นอันตราย และควบคุมเซิร์ฟเวอร์ที่เกิดขึ้นตามรูปแบบปกติเมื่อคอมพิวเตอร์ติดไวรัสและบ็อตพยายามสื่อสาร อ่านเพิ่มเติมเกี่ยวกับการป้องกันบอตเน็ตในประมวลศัพท์

กฎ IDS – ตัวเลือกนี้อนุญาตให้คุณกำหนดค่าตัวเลือกการกรองขั้นสูงเพื่อตรวจหาการโจมตีและการใช้ช่องโหว่ประเภทต่างๆ ที่สามารถใช้เพื่อทำอันตรายคอมพิวเตอร์ของคุณได้

> **คำแนะนำพร้อมภาพประกอบ**
> บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
> - ยกเว้นที่อยู่ IP จาก IDS ใน ESET Smart Security Premium

เหตุการณ์สำคัญทั้งหมดที่ตรวจพบโดยการป้องกันเครือข่ายจะถูกบันทึกไว้ในไฟล์บันทึก ดูข้อมูลเพิ่มเติมได้จาก บันทึกการป้องกันเครือข่าย

การป้องกันการโจมตีแบบ Brute-Force

การป้องกันการโจมตีแบบ Brute-force จะบล็อกการโจมตีด้วยการคาดเดารหัสผ่านสำหรับบริการ RDP และ SMB การโจมตีแบบ Brute-force เป็นวิธีการค้นหารหัสผ่านเป้าหมายโดยลองใช้ชุดตัวอักษร ตัวเลข และสัญลักษณ์ทั้งหมดรวมกันอย่างเป็นระบบ ในการกำหนดค่าการป้องกันการโจมตีแบบ Brute-force ในหน้าต่างโปรแกรมหลัก ให้คลิก **ตั้งค่า** > **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **การป้องกันการโจมตีเครือข่าย** > **การป้องกันการโจมตีแบบ Brute-force**

เปิดใช้งานการป้องกันการโจมตีแบบ Brute-force – ESET Smart Security Premium ตรวจสอบเนื้อหาการรับส่ง

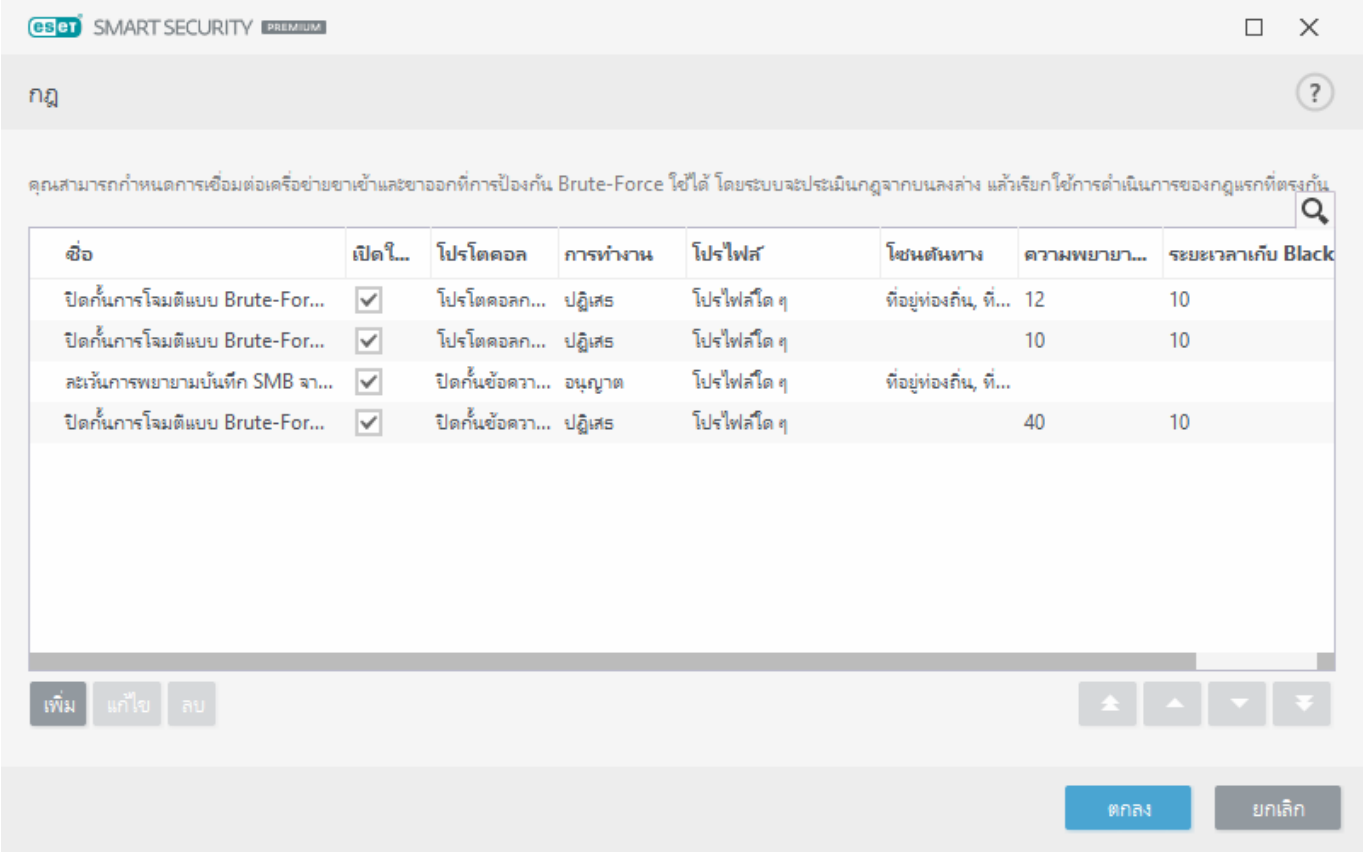
ข้อมูลเครือข่ายและบล็อกความพยายามในการโจมตีด้วยการคาดเดารหัสผ่าน

กฎ – ช่วยให้คุณสร้าง แก้ไข และดูกฎสำหรับการเชื่อมต่อเครือข่ายขาเข้าและขาออกได้ สำหรับข้อมูลเพิ่มเติม โปรดูส่วน กฎ

กฎ

กฎการป้องกันการโจมตีแบบ Brute-force จะช่วยให้คุณสร้าง แก้ไข และดูกฎสำหรับการเชื่อมต่อเครือข่ายขาเข้าและขาออกได้ กฎที่กำหนดไว้ล่วงหน้าไม่สามารถแก้ไขหรือลบได้

การจัดการกฎการป้องกันการโจมตีแบบ Brute-Force



เพิ่ม – สร้างกฎใหม่

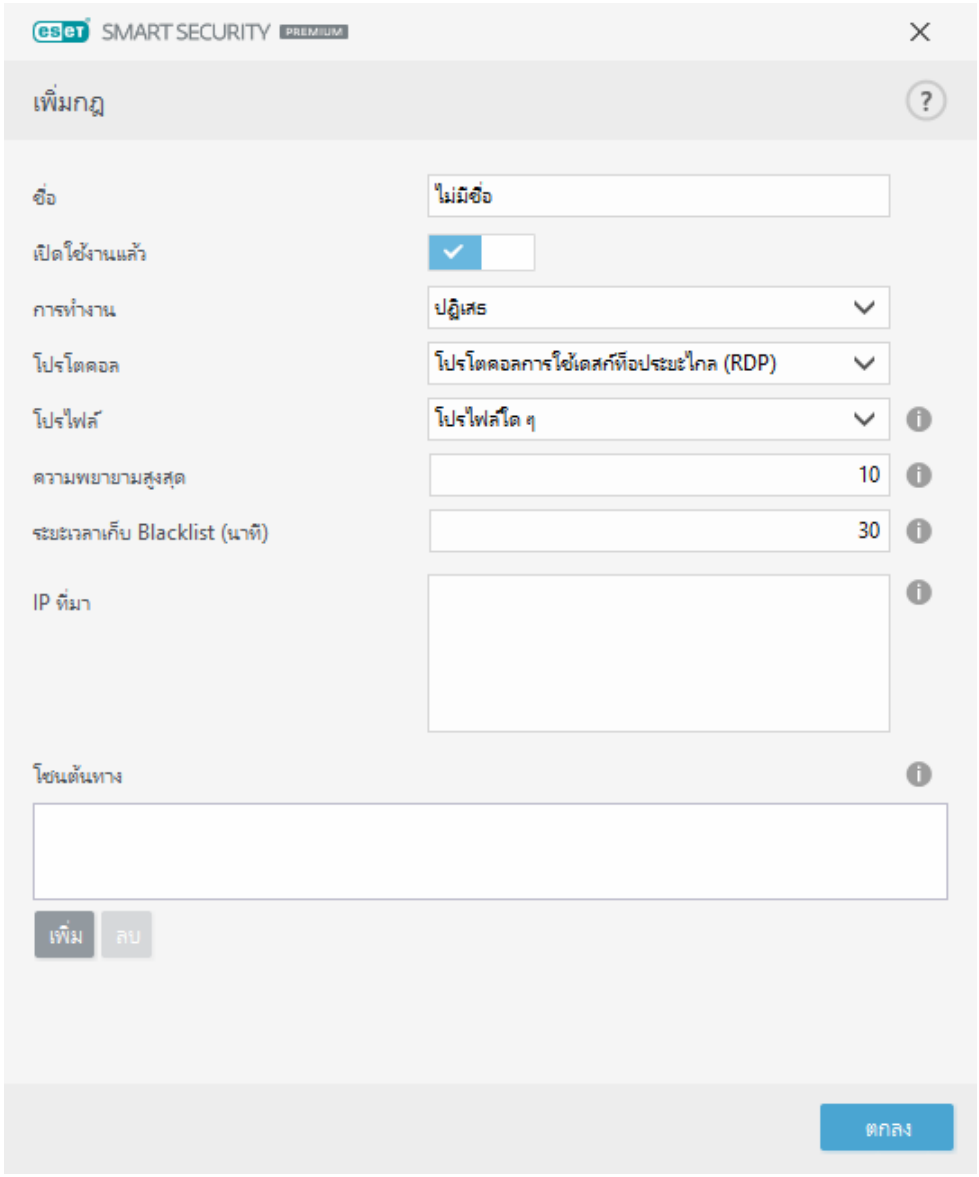
แก้ไข – แก้ไขกฎที่มีอยู่

ลบ – ลบกฎที่มีอยู่ออกจากรายการกฎ

บนสุด/ขึ้น/ลง/ล่างสุด – ปรับระดับความสำคัญของกฎ

เพื่อให้แน่ใจว่ามีการป้องกันสูงสุดที่เป็นไปได้ จะมีการใช้กฎการบล็อกที่มีค่า **ความพยายามสูงสุด** ต่ำสุดเมื่อกฎการบล็อกหลายกฎตรงกับเงื่อนไขการตรวจหา แม้ว่ากฎจะอยู่ในตำแหน่งรายการกฎที่ต่ำกว่าก็ตาม

ตัวแก้ไขกฎ



ชื่อ – ชื่อของกฎ

เปิดใช้งาน – ปิดใช้งานแถบเลื่อนนี้หากคุณต้องการคงกฎไว้ในรายการแต่ไม่ปรับใช้

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

โปรโตคอล – โปรโตคอลการสื่อสารที่กฎนี้จะตรวจสอบ

โปรไฟล์ – สามารถตั้งค่ากฎที่กำหนดเองและใช้สำหรับโปรไฟล์เฉพาะ

ความพยายามสูงสุด: จำนวนสูงสุดของความพยายามโจมตีซ้ำที่อนุญาตจนกว่าที่อยู่ IP จะถูกปิดกั้นและเพิ่มลงใน

ระยะเวลาการเก็บรักษา Blacklist (นาที) – ตั้งเวลาสำหรับให้ที่อยู่หมดอายุจาก Blacklist โดยช่วงเวลาตามค่าเริ่มต้นสำหรับการนับจำนวนครั้งที่พยายามคือ 30 นาที

IP ที่มา – รายการ / ช่วง / เครือข่ายย่อยของที่อยู่ IP โดยที่อยู่ที่มากกว่าหนึ่งแห่งจะต้องคั่นด้วยเครื่องหมายจุลภาค

โซนต้นทาง – ช่วยให้คุณเพิ่มโซนที่กำหนดไว้ล่วงหน้าหรือโซนที่สร้างด้วยช่วงของที่อยู่ IP ได้ที่นี่ด้วยการคลิก **เพิ่ม**

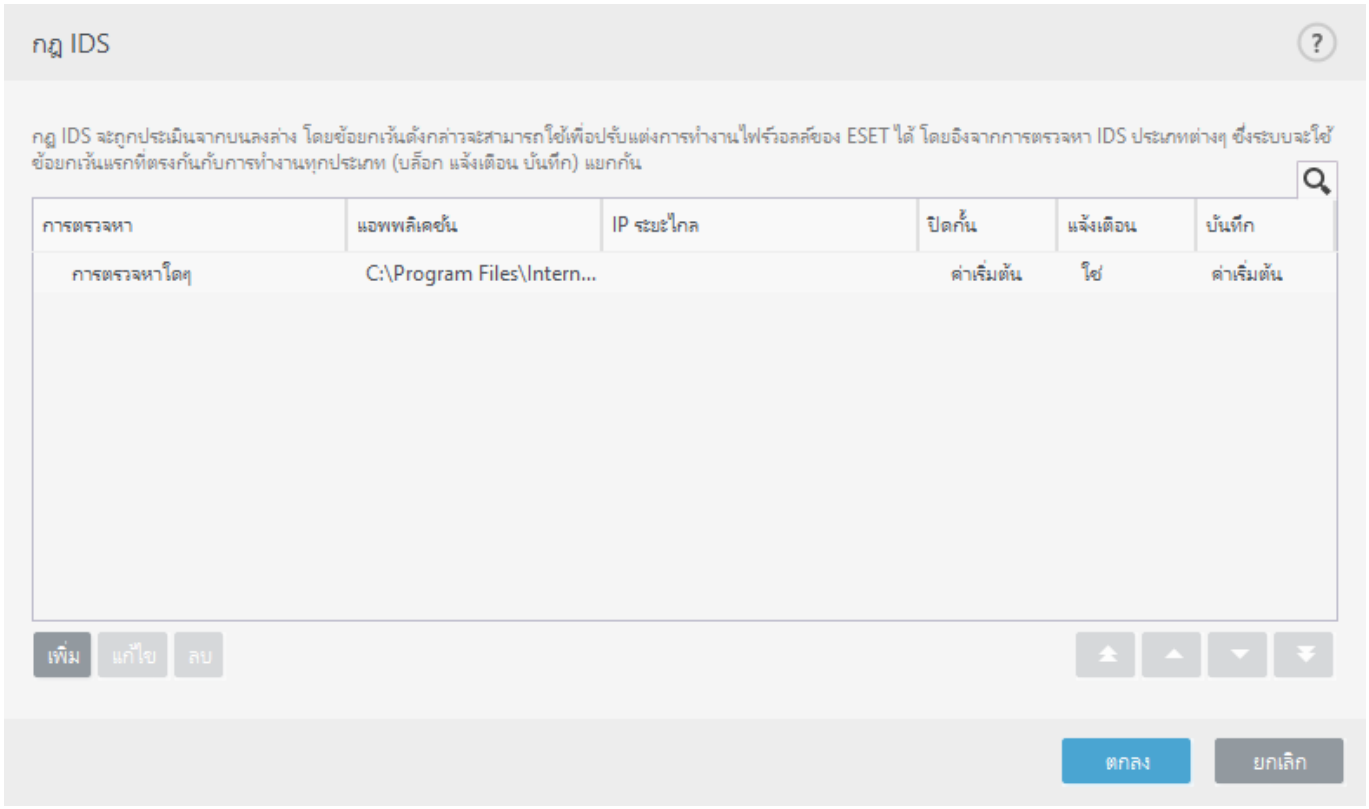
IDS กฎ

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

> **คำแนะนำพร้อมภาพประกอบ**
> บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
> - ยกเว้นที่อยู่ IP จาก IDS ใน ESET Smart Security Premium

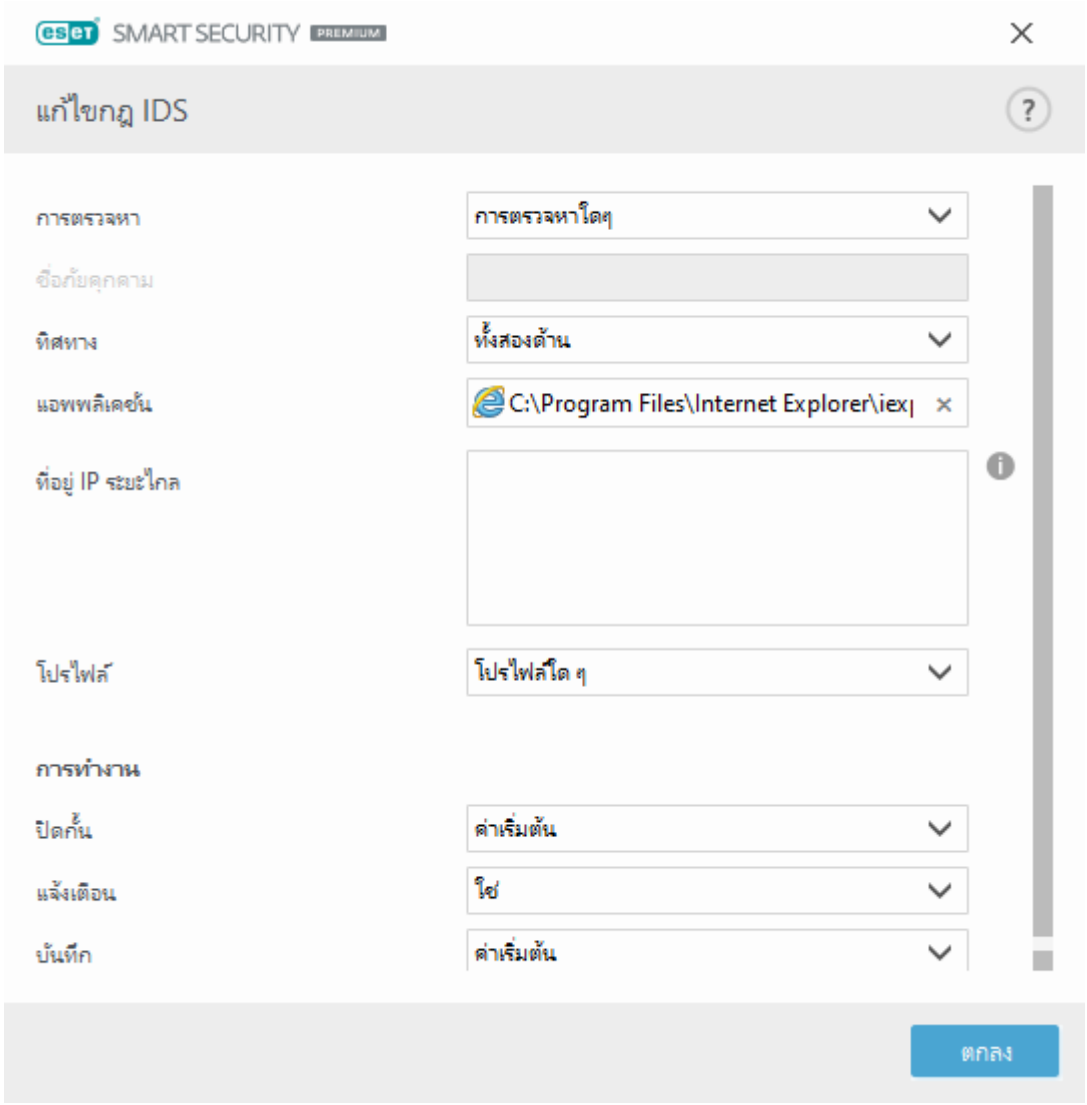
คอลัมน์

- **การตรวจหา** – ประเภทการยกเว้นการตรวจหา
- **แอพพลิเคชัน** – เลือกพาธไฟล์ของแอพพลิเคชันที่ได้รับการยกเว้นโดยการคลิก ... (ตัวอย่างเช่น C:\Program Files\Firefox\Firefox.exe) (ตัวอย่างเช่น C:\Program Files\Firefox\Firefox.exe) อย่าป้อนชื่อของแอพพลิเคชัน
- **IP ระยะไกล** – รายการที่อยู่ / ระยะ / ซับเน็ต IPv4 หรือ IPv6 ที่อยู่หลายแห่งต้องคั่นด้วยเครื่องหมายคอมมา
- **ปิดกั้น** – ทุกกระบวนการของระบบมีค่าเริ่มต้นของการทำงานและการทำงานที่กำหนดเป็นของตนเอง (ปิดกั้นและอนุญาต) เมื่อต้องการเขียนทับการทำงานที่เป็นค่าเริ่มต้นสำหรับ ESET Smart Security Premium คุณสามารถเลือกว่าจะปิดกั้นหรืออนุญาตค่าเริ่มต้นได้โดยใช้เมนูแบบเลื่อนลง
- **แจ้งเตือน** – เลือกว่าจะแสดง การแจ้งเตือนบนเดสก์ท็อป ในคอมพิวเตอร์ของคุณหรือไม่ เลือกค่า **ค่าเริ่มต้น/ใช่/ไม่ใช่**
- **บันทึก** – บันทึกเหตุการณ์ไปยัง ไฟล์บันทึกของ ESET Smart Security Premium เลือกค่า **ค่าเริ่มต้น/ใช่/ไม่ใช่**



การจัดการกฎ IDS

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



คุณต้องการแสดงการแจ้งเตือนและรวบรวมบันทึกในแต่ละครั้งที่กิจกรรมเกิดขึ้น:
1.คลิก **เพิ่ม** เพื่อเพิ่มกฎ IDS ใหม่
2.เลือกการตรวจหาเฉพาะจากเมนู **การตรวจหา** แบบเลื่อนลง
3.เลือกพาธแอพพลิเคชันโดยการคลิก **...** สำหรับพาธที่คุณต้องการใช้สำหรับการแจ้งเตือนนี้
4.ปล่อยให้เป็น **ค่าเริ่มต้น** ในเมนู **ปิดกั้น** แบบเลื่อนลง วิธีนี้จะสืบทอดการกระทำที่ใช้โดย ESET Smart Security Premium
5.ตั้งค่าทั้ง **การแจ้งเตือน** และเมนู **บันทึก** แบบเลื่อนลงเพื่อ **ใช่**
6.คลิก **ตกลง** เพื่อบันทึกการแจ้งเตือน

หากคุณไม่ต้องการแสดงการแจ้งเตือนซ้ำที่คุณพิจารณาว่าไม่เป็นภัยคุกคามประเภทจำเพาะของ **การตรวจหา**:
1.คลิก **เพิ่ม** เพื่อเพิ่มกฎ IDS ใหม่
2.เลือกการตรวจหาเฉพาะจากเมนู **การตรวจหา** แบบเลื่อนลง ตัวอย่างเช่น **ส่วน SMB ที่ไม่มีการขยายความปลอดภัย การโจมตีโดยการสแกนพอร์ต 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

ปิดกั้นภัยคุกคามที่น่าสงสัยแล้ว

สถานการณ์นี้อาจเกิดขึ้นได้เมื่อแอพพลิเคชันบนคอมพิวเตอร์ของคุณกำลังพยายามส่งการรับส่งข้อมูลที่เป็นอันตรายไปยังคอมพิวเตอร์อีกเครื่องในเครือข่าย การใช้ประโยชน์จากช่องโหว่ของการรักษาความปลอดภัยหรือตรวจพบความพยายามสแกนพอร์ตในระบบของคุณ

ภัยคุกคาม – ชื่อของภัยคุกคาม

ที่อยู่ระยะไกล - ที่อยู่ IP ระยะไกล

อนุญาต - สร้าง กฎบริการการตรวจหาผู้บุรุก (IDS) โดยมีการระบุข้อกำหนดไม่ให้ดำเนินการสำหรับการดำเนินการแต่ละประเภทไว้ล่วงหน้า (ปิดกั้น แจ้งเตือน บันทึก)

ปิดกั้นต่อไป - ปิดกั้นภัยคุกคามที่ตรวจพบ ในการสร้างข้อยกเว้น IDS สำหรับภัยคุกคามนี้ ให้เลือกกล่องกาเครื่องหมาย **ไม่ต้องแจ้งเตือนอีก** และกฎจะถูกเพิ่มโดยไม่มีการแจ้งและการบันทึกใดๆ

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

การแก้ไขปัญหาการป้องกันเครือข่าย

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

เมื่อคุณคลิก **ยกเลิกการปิดกั้น** การสื่อสารที่ถูกปิดกั้นไว้ก่อนหน้าจะได้รับอนุญาต หากคุณยังประสบปัญหากับแอพพลิเคชันของคุณ หรืออุปกรณ์ของคุณไม่ทำงานตามที่คาดไว้ ให้คลิก **แอพพลิเคชันยังไม่ทำงาน** และการสื่อสารทั้งหมดที่ถูกปิดกั้นไว้ก่อนหน้านี้ในอุปกรณ์ดังกล่าวจะได้รับอนุญาต หากปัญหายังคงอยู่ ให้เริ่มต้นระบบคอมพิวเตอร์ของคุณใหม่

คลิก **แสดงการเปลี่ยนแปลง** เพื่อดูกฎที่วิซาร์ดสร้างขึ้น นอกจากนี้ คุณสามารถดูกฎที่วิซาร์ดสร้างขึ้นได้ โดยไปที่

การตั้งค่าขั้นสูง > **การป้องกันเครือข่าย** > **ไฟร์วอลล์** > **ขั้นสูง** > **กฎ**

คลิก **ยกเลิกการปิดกั้นอื่นๆ** เพื่อแก้ไขปัญหาการเชื่อมต่อด้วยอุปกรณ์หรือแอพพลิเคชันอื่น

บริการที่อนุญาตและตัวเลือกขั้นสูง

ตัวเลือกขั้นสูงในส่วนการปกป้องการโจมตีเครือข่ายและไฟร์วอลล์ช่วยให้คุณสามารถกำหนดค่าการเข้าถึงการบริการบางอย่างที่ทำงานในคอมพิวเตอร์ของคุณจากโซนที่เชื่อถือ

คุณสามารถเปิดใช้งานหรือปิดใช้งานการตรวจหาการโจมตีและการใช้ช่องโหว่ประเภทต่างๆ ที่อาจทำอันตรายต่อคอมพิวเตอร์ของคุณได้

ในบางกรณี คุณจะไม่ได้รับการแจ้งเตือนภัยคุกคามเกี่ยวกับการสื่อสารที่ปิดกั้น โปรดศึกษาส่วน การบันทึกและการสร้างกฎหรือข้อยกเว้นการบันทึก สำหรับคำแนะนำในการดูการสื่อสารที่ปิดกั้นที่อยู่ในบันทึกไฟร์วอลล์

ความพร้อมในการใช้งานสำหรับตัวเลือกในหน้าต่างนี้อาจแตกต่างกันไป ทั้งนี้จะขึ้นอยู่กับประเภทหรือเวอร์ชันของผลิตภัณฑ์ของ ESET และโมดูลไฟร์วอลล์ รวมทั้งเวอร์ชันของระบบปฏิบัติการของคุณ

บริการที่อนุญาต

การตั้งค่าในกลุ่มนี้ตั้งขึ้นเพื่อทำให้การกำหนดค่าการเข้าถึงการบริการของคอมพิวเตอร์เครื่องนี้จากโซนที่เชื่อถือทำได้ง่ายดายมากขึ้น มีจำนวนมากที่เปิดใช้งาน/ปิดใช้งานกฎไฟร์วอลล์ที่กำหนดไว้ล่วงหน้า คุณสามารถแก้ไขบริการที่อนุญาตได้ใน **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **ไฟร์วอลล์** > **ขั้นสูง** > **บริการที่อนุญาต**

- **อนุญาตให้ใช้ไฟล์และเครื่องพิมพ์ร่วมกันในโซนที่เชื่อถือ** – อนุญาตให้คอมพิวเตอร์ระยะไกลในโซนที่เชื่อถือสามารถเข้าถึงไฟล์และเครื่องพิมพ์ที่ใช้ร่วมกันของคุณได้
- **อนุญาต UPNP สำหรับบริการของระบบในโซนที่เชื่อถือ** – อนุญาตคำขอขาเข้าและขาออกของโปรโตคอล UPnP สำหรับบริการของระบบ UPnP (Universal Plug and Play ซึ่งยังเป็นที่รู้จักในชื่อ Microsoft Network Discovery) ถูกใช้ใน Windows Vista และระบบปฏิบัติการเวอร์ชันใหม่กว่า
- **อนุญาตการสื่อสาร RPC ขาเข้าในโซนที่เชื่อถือ** – เปิดใช้งานการเชื่อมต่อ TCPTCP จากโซนที่เชื่อถือที่อนุญาตให้เข้าถึงบริการ MS RPC Portmapper และ RPC/DCOM
- **อนุญาตการใช้เดสก์ท็อประยะไกลในโซนที่เชื่อถือ** – เปิดใช้งานการเชื่อมต่อผ่าน Microsoft Remote Desktop Protocol (RDP) และอนุญาตคอมพิวเตอร์ในโซนที่เชื่อถือเพื่อเข้าถึงคอมพิวเตอร์ของคุณโดยใช้โปรแกรม

ที่ใช้ RDP (ตัวอย่างเช่น การเชื่อมต่อเดสก์ท็อประยะไกล)

- **เปิดใช้งานการเข้าสู่ระบบของกลุ่มมัลติคาสต์ผ่าน IGMP** – อนุญาตให้สตรีมมัลติคาสต์ IGMP ขาเข้า/ขาออกและ UDP ขาเข้า ตัวอย่างเช่น สตรีมวิดีโอที่สร้างโดยแอพพลิเคชันที่ใช้โปรโตคอล IGMP (Internet Group Management Protocol)

- **อนุญาตการสื่อสารสำหรับการเชื่อมต่อแบบบริดจ์** – เลือกตัวเลือกนี้เพื่อหลีกเลี่ยงการปิดการเชื่อมต่อแบบบริดจ์ การเชื่อมต่อแบบบริดจ์จะเชื่อมต่อเครื่องเสมือนเข้ากับเครือข่ายโดยใช้อะแดปเตอร์อีเธอร์เน็ตของคอมพิวเตอร์โฮสต์ หากคุณใช้การเชื่อมต่อแบบบริดจ์ เครื่องเสมือนจะสามารถเข้าถึงอุปกรณ์อื่นบนเครือข่ายได้ และในทางกลับกัน เช่นเดียวกับเมื่ออุปกรณ์ดังกล่าวเป็นคอมพิวเตอร์เครื่องจริงในเครือข่าย

- **อนุญาต Web Services Discovery (WSD) แบบอัตโนมัติสำหรับบริการของระบบในโซนที่เชื่อถือ** – อนุญาตคำขอของ Web Services Discovery ขาเข้าจากโซนที่เชื่อถือผ่านไฟร์วอลล์ WSD เป็นโปรโตคอลที่ใช้เพื่อระบุตำแหน่งของการบริการในเครือข่ายภายใน

- **อนุญาตการแปลค่าที่อยู่มัลติคาสต์ในโซนที่เชื่อถือ (LLMNR)** – LLMNR (Link-local Multicast Name Resolution) คือโปรโตคอลที่ใช้แพ็คเก็ต DNS ซึ่งอนุญาตทั้งโฮสต์ IPv4 และ IPv6 ให้แปลค่าชื่อสำหรับโฮสต์ในลิงค์ภายในเดียวกัน โดยไม่ต้องกำหนดค่าเซิร์ฟเวอร์ DNS หรือไคลเอ็นต์ DNS ตัวเลือกนี้จะอนุญาตให้ DNS มัลติคาสต์ขาเข้าส่งคำขอจากโซนที่เชื่อถือผ่านไฟร์วอลล์ได้

- **การสนับสนุน Windows HomeGroup** – เปิดใช้งานการสนับสนุน HomeGroup สำหรับ Windows 7 และระบบปฏิบัติการเวอร์ชันใหม่กว่า HomeGroup สามารถใช้ไฟล์และเครื่องพิมพ์ร่วมกันในเครือข่ายในบ้าน หากต้องการกำหนดค่า Homegroup ให้ไปที่ **Start** > **Control Panel** > **Network and Internet** > **HomeGroup**

การตรวจหาการบุกรุก

การตรวจจับการบุกรุกจะตรวจสอบการสื่อสารเครือข่ายของอุปกรณ์สำหรับกิจกรรมที่เป็นอันตราย คุณสามารถแก้ไขการตั้งค่าเหล่านี้ได้ใน **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **การป้องกันการโจมตีเครือข่าย** > **ตัวเลือกขั้นสูง** > **การตรวจหาการบุกรุก**

- **โปรโตคอล SMB** – ตรวจหาและปิดกั้นปัญหาด้านความปลอดภัยต่างๆ ในโปรโตคอล SMB

- **โปรโตคอล RPC** – ตรวจหาและปิดกั้น CVE ต่างๆ ในระบบการเรียกขั้นตอนระยะไกลที่พัฒนาสำหรับ Distributed Computing Environment (DCE)

- **โปรโตคอลRDP** – ตรวจหาและปิดกั้น CVE ที่หลากหลายในโปรโตคอล RDP (ดูด้านบน)

• **การตรวจหาการโจมตี ARP** Poisoning – การตรวจหาการโจมตี ARP Poisoning ที่เรียกใช้การโจมตีแบบคนกลางในการสื่อสารหรือการตรวจหาการดักจับที่สวิตช์เครือข่าย ARP (Address Resolution Protocol) ถูกใช้โดยแอพพลิเคชันหรืออุปกรณ์ของเครือข่ายเพื่อระบุที่อยู่อีเธอร์เน็ต

• การตรวจหาการโจมตี **TCP/UDP Port Scanning** – ตรวจหาการโจมตีซอฟต์แวร์การสแกนพอร์ต แอพพลิเคชันที่ออกแบบมาเพื่อโพรบโฮสต์สำหรับพอร์ตที่เปิดอยู่โดยการส่งคำขอของไคลเอ็นต์ไปยังช่วงของที่อยู่พอร์ต โดยมีเป้าหมายในการค้นหาพอร์ตที่เปิดใช้งานและการใช้ประโยชน์จากจุดอ่อนของบริการ อ่านเพิ่มเติมเกี่ยวกับการโจมตีประเภทนี้ได้ใน ประมวลศัพท์

• **ปิดกั้นที่อยู่ที่ไม่ปลอดภัยหลังการตรวจหาการโจมตี** – ที่อยู่ IP ที่ถูกตรวจพบว่าเป็นแหล่งที่มาของการโจมตีจะถูกเพิ่มไปยังบัญชีดำเพื่อป้องกันการเชื่อมต่อในช่วงเวลาหนึ่ง

• **แสดงการแจ้งเตือนหลังจากตรวจพบการโจมตี** – เปิดการแจ้งเตือนที่ถาดข้อมูลระบบที่มุมขวาล่างสุดของหน้าจอ

• **แสดงการแจ้งเตือนยังใช้เพื่อแจ้งเมื่อมีการโจมตีจุดอ่อนด้านการรักษาความปลอดภัย** – แจ้งให้คุณทราบถ้าตรวจพบการโจมตีจุดอ่อนด้านการรักษาความปลอดภัย หรือถ้าภัยคุกคามพยายามเข้าสู่ระบบด้วยวิธีนี้

การตรวจสอบแพ็คเก็ต

ประเภทของการวิเคราะห์แพคเก็ตที่กรองข้อมูลที่ถูกถ่ายโอนผ่านเครือข่าย คุณสามารถแก้ไขการตั้งค่าเหล่านี้ได้ใน **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **การป้องกันการโจมตีเครือข่าย** > **ตัวเลือกขั้นสูง** > **การตรวจสอบแพ็คเก็ต**

• **อนุญาตการเชื่อมต่อขาเข้าไปยังการใช้การดูแลระบบร่วมกันในโปรโตคอล SMB** - การใช้การดูแลระบบร่วมกัน (admin shares) คือเครือข่ายเริ่มต้นที่ให้ใช้พาร์ติชันฮาร์ดไดรฟ์ร่วมกัน (*C$, D$*, ...) ในระบบพร้อมกับโฟลเดอร์ระบบ (*ADMIN$*) การปิดใช้งานการเชื่อมต่อกับการใช้การดูแลระบบร่วมกันจะช่วยลดความเสี่ยงทางด้านความปลอดภัยหลาย 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) จากโฟลเดอร์ที่ใช้งานร่วมกันในเซิร์ฟเวอร์ที่ไม่ได้เป็นของโซนที่เชื่อถือในไฟร์วอลล์ โปรดทราบว่าการคัดลอกไฟล์ที่เรียกใช้ได้จากแหล่งข้อมูลที่เชื่อถืออาจทำได้อย่างถูกต้อง 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]

• **อนุญาตการสื่อสารกับบริการอื่น** – บริการMSRPC อื่นๆ

เครือข่ายที่เชื่อมต่อ

แสดงเครือข่ายที่อะแดปเตอร์เครือข่ายเชื่อมต่ออยู่ **เครือข่ายเชื่อมต่ออยู่** สามารถพบได้ในเมนูหลักภายใต้ **ตั้งค่า** > **การป้องกันเครือข่าย** หลังจากที่คลิกลิงก์ที่อยู่ด้านล่างของชื่อเครือข่าย คุณจะได้รับแจ้งให้เลือกประเภทการป้องกันสำหรับเครือข่ายที่คุณเชื่อมต่ออยู่

มีโหมดการป้องกันเครือข่ายสองโหมดที่คุณสามารถเลือกได้จากในหน้าต่างการกำหนดค่าการป้องกันเครือข่าย ดังนี้:

• **ใช่** – สำหรับเครือข่ายที่เชื่อถือ (เครือข่ายในบ้านหรือที่ทำงาน) ผู้ใช้เครือข่ายรายอื่นสามารถมองเห็นคอมพิวเตอร์และไฟล์ที่ใช้ร่วมกันที่เก็บไว้ในคอมพิวเตอร์ของคุณได้ และผู้ใช้รายอื่นบนเครือข่ายสามารถเข้าถึงทรัพยากรระบบได้ เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าถึงเครือข่ายภายในที่ปลอดภัย

• **ไม่** – สำหรับเครือข่ายที่ไม่เชื่อถือ (เครือข่ายสาธารณะ) ไฟล์และโฟลเดอร์ในระบบของคุณจะไม่ถูกใช้ร่วมกันหรือมองเห็นได้สำหรับผู้ใช้รายอื่นบนเครือข่าย และการแบ่งปันทรัพยากรระบบจะถูกปิดใช้งาน เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าสู่เครือข่ายไร้สาย

คลิกไอคอนรูปเฟือง ⚙ ที่อยู่ถัดจากเครือข่ายเพื่อเลือกจากตัวเลือกต่อไปนี้ (สำหรับเครือข่ายที่ไม่เชื่อถือ จะมีเฉพาะตัวเลือก **แก้ไขเครือข่าย** เท่านั้น):

• **แก้ไขเครือข่าย** – เปิด ตัวแก้ไขเครือข่าย

• **สแกนเครือข่ายด้วยตัวตรวจสอบเครือข่าย** – เปิด ตัวตรวจสอบเครือข่าย เพื่อเรียกใช้การสแกนเครือข่าย

• **ทำเครื่องหมายเป็น "เครือข่ายของฉัน"** – เพิ่มแท็กเครือข่ายของฉันไปยังเครือข่าย แท็กนี้จะแสดงถัดจากเครือข่ายทั่วทั้ง ESET Smart Security Premium เพื่อให้ได้การระบุตัวตนและภาพรวมการรักษาความปลอดภัยที่ดีขึ้น

• **ยกเลิกการทำเครื่องหมายเป็น "เครือข่ายของฉัน"** – ลบแท็กเครือข่ายของฉัน สามารถใช้งานได้เมื่อเครือข่ายถูกติดแท็กไว้แล้วเท่านั้น

เพื่อดูแต่ละอะแดปเตอร์เครือข่ายรวมถึงโปรไฟล์ไฟร์วอลล์และโซนที่เชื่อถือที่กำหนด ให้คลิกที่ **อะแดปเตอร์เครือข่าย** สำหรับข้อมูลเพิ่มเติมโปรดดูส่วน อะแดปเตอร์เครือข่าย

อะแดปเตอร์เครือข่าย

หน้าต่างอะแดปเตอร์เครือข่ายจะแสดงข้อมูลเกี่ยวกับอะแดปเตอร์เครือข่ายของคุณดังต่อไปนี้:

- ชื่ออะแดปเตอร์เครือข่ายและประเภทการเชื่อมต่อ (เป็นแบบใช้สาย เสมือน หรืออื่นๆ)
- ที่อยู่ IP พร้อมด้วยที่อยู่ MAC
- เครือข่ายที่เชื่อมต่อ (แสดงแท็กเครือข่ายของฉัน)
- ที่อยู่ IP ของโซนที่เชื่อถือพร้อมซับเน็ต
- โปรไฟล์ที่ทำงาน (โปรดดู โปรไฟล์ที่มอบหมายให้อะแดปเตอร์เครือข่าย)

บัญชีดำของที่อยู่ IP แบบชั่วคราว

หากต้องการดูที่อยู่ IP ที่ถูกตรวจพบว่าเป็นแหล่งที่มาของการโจมตีจะถูกเพิ่มเข้าไปยังบัญชีดำเพื่อปิดกั้นการเชื่อมต่อเป็นระยะเวลาหนึ่ง ESET Smart Security Premium สำรวจ **ตั้งค่า** > **การป้องกันเครือข่าย** > **ทำให้ที่อยู่ IP ขึ้นบัญชีดำชั่วคราว** ที่อยู่ IP ที่ถูกปิดกั้นชั่วคราวจะถูกปิดกั้นเป็นเวลา 1 ชั่วโมง

คอลัมน์

ที่อยู่ IP – แสดงที่อยู่ IP ที่ถูกปิดกั้น

เหตุผลในการปิดกั้น - แสดงการโจมตีประเภทต่างๆ ที่ถูกป้องกันจากที่อยู่ (ตัวอย่างเช่น การโจมตีการสแกนพอร์ต TCP)

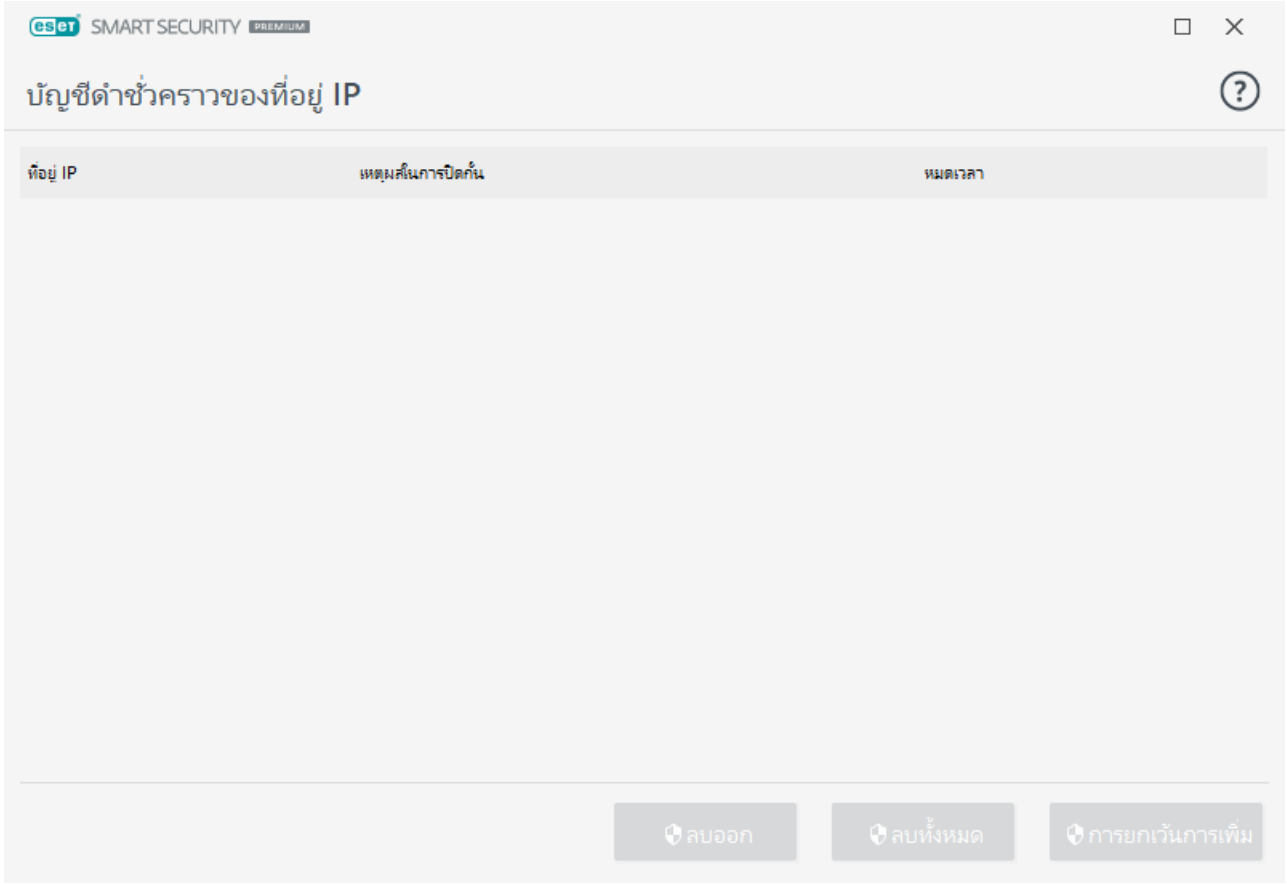
หมดเวลา – แสดงเวลาและวันที่ที่ที่อยู่จะหมดอายุจากบัญชีดำ

องค์ประกอบการควบคุม

ลบออก – คลิกเพื่อลบที่อยู่ออกจากบัญชีดำก่อนที่ที่อยู่จะหมดอายุจากบัญชีดำ

ลบทั้งหมด – คลิกเพื่อลบที่อยู่ทั้งหมดออกจากบัญชีดำในทันที

เพิ่มข้อยกเว้น – คลิกเพื่อเพิ่มข้อยกเว้นของไฟร์วอลล์ลงในการกรอง IDS



บันทึกการป้องกันเครือข่าย

การป้องกันเครือข่ายของ ESET Smart Security Premium จะบันทึกเหตุการณ์สำคัญทั้งหมดไว้ในไฟล์บันทึก ซึ่งจะสามารถดูได้โดยตรงจากเมนูหลัก คลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก** แล้วเลือก **การป้องกันเครือข่าย** จากเมนูแบบเลื่อนลง **บันทึก**

สามารถใช้ไฟล์บันทึกเพื่อตรวจหาข้อผิดพลาดและเปิดเผยการบุกรุกในระบบของคุณ บันทึกการป้องกันเครือข่ายของ ESET จะมีข้อมูลต่อไปนี้:

- วันที่และเวลาของเหตุการณ์
- ชื่อของเหตุการณ์
- ที่มา
- ที่อยู่เครือข่ายเป้าหมาย
- โปรโตคอลการสื่อสารของเครือข่าย
- กฎที่ใช้งาน หรือชื่อของเวิร์ม หากสามารถระบุได้

- แอพพลิเคชันที่เกี่ยวข้อง
- ผู้ใช้

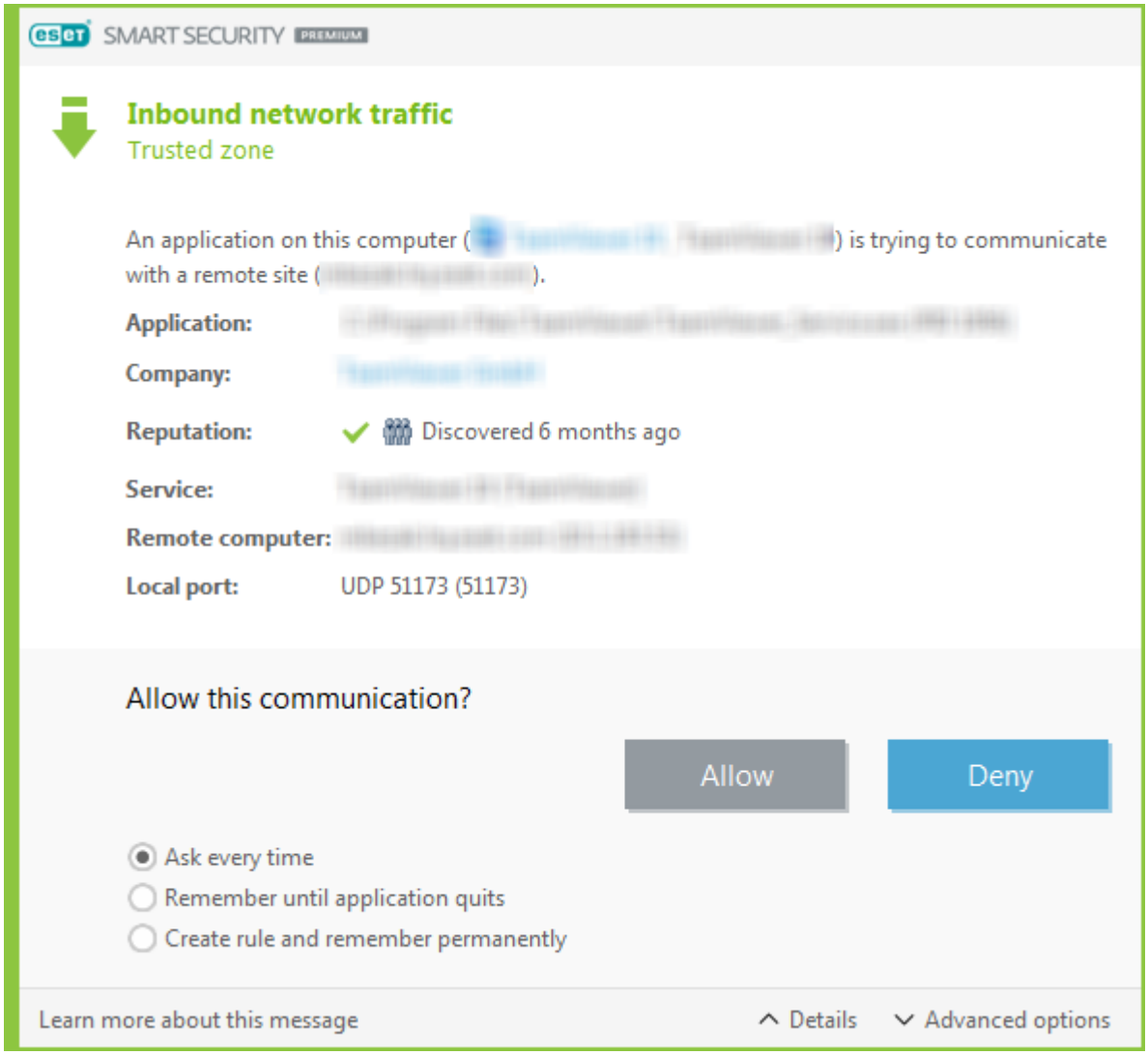
การวิเคราะห์ข้อมูลนี้โดยละเอียดช่วยให้สามารถตรวจหาความพยายามในการบุกรุกการรักษาความปลอดภัยของระบบ ปัจจัยอื่นๆ อีกมากมายสามารถระบุความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นนี้ได้และสามารถป้องกันได้โดยใช้ไฟร์วอลล์ เช่น: การเชื่อมต่อที่บ่อยจากตำแหน่งที่ไม่รู้จัก ความพยายามต่างๆ ที่จะสร้างการเชื่อมต่อ การสื่อสารของแอพพลิเคชันที่ไม่รู้จัก หรือเลขที่พอร์ตที่ผิดปกติที่ใช้งานอยู่

> **การใช้ประโยชน์จากจุดอ่อนของความปลอดภัย**
> ข้อความเกี่ยวกับการใช้ประโยชน์จากจุดอ่อนของความปลอดภัยจะถูกบันทึกไว้แม้จุดอ่อนดังกล่าวจะได้รับการแก้ไขแล้วนับตั้งแต่ตรวจพบและปิดกั้นความพยายามในการใช้ประโยชน์ดังกล่าวบนระดับเครือข่ายก่อนที่การใช้ประโยชน์จะเกิดขึ้นจริง

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

บริษัท – ชื่อผู้เผยแพร่แอพพลิเคชัน 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

การแก้ไขปัญหาเกี่ยวกับไฟร์วอลล์ของ ESET

หากคุณประสบปัญหาในการเชื่อมต่อกับ ESET Smart Security Premium ที่ติดตั้งไว้ มีหลายวิธีที่สามารถบอกได้ว่าไฟร์วอลล์ของ ESET เป็นเหตุให้เกิดปัญหานั้นๆ หรือไม่ นอกจากนี้ ไฟร์วอลล์ของ ESET ยังสามารถช่วยคุณสร้างกฎหรือข้อยกเว้นใหม่เพื่อแก้ไขปัญหาในการเชื่อมต่อได้

ดูหัวข้อต่อไปนี้เพื่อขอความช่วยเหลือในการแก้ไขปัญหาเกี่ยวกับไฟร์วอลล์ของ ESET:

- วิซาร์ดการแก้ไขปัญหา
- การบันทึกและการสร้างกฎหรือข้อยกเว้นการบันทึก
- การสร้างข้อยกเว้นการแจ้งเตือนไฟร์วอลล์
- การบันทึกขั้นสูงสำหรับการป้องกันเครือข่าย
- การแก้ไขปัญหาเกี่ยวกับการกรองโปรโตคอล

วิซาร์ดการแก้ไขปัญหา

วิซาร์ดการแก้ไขปัญหาจะตรวจสอบการเชื่อมต่อที่ปิดกั้นทั้งหมดโดยไม่ได้แจ้งให้ทราบ และจะนำคุณเข้าสู่กระบวนการแก้ไขปัญหาเพื่อแก้ไขปัญหาของไฟร์วอลล์ที่เกี่ยวกับแอพพลิเคชันหรืออุปกรณ์ที่ระบุเฉพาะ ขั้นตอนต่อไป วิซาร์ดจะแนะนำให้ปรับใช้ชุดกฎใหม่ถ้าคุณอนุมัติ พบ**วิซาร์ดการแก้ไขปัญหา**ได้ในเมนูหลักด้านใต้ **การตั้งค่า** > **เครือข่าย**

การบันทึกและการสร้างกฎหรือข้อยกเว้นการบันทึก

ตามค่าเริ่มต้น ไฟร์วอลล์ของ ESET ไม่ได้บันทึกการเชื่อมต่อที่ปิดกั้นทั้งหมด หากคุณต้องการดูรายการที่ถูกปิดกั้นโดยการป้องกันเครือข่าย ให้เปิดใช้งานการบันทึกใน **การตั้งค่าขั้นสูง** ภายใต้ **เครื่องมือ** > **การวินิจฉัย** > **การบันทึกขั้นสูง** > **เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันเครือข่าย** หากคุณเห็นบางอย่างในบันทึกที่คุณไม่ต้องการให้ไฟร์วอลล์ปิดกั้น คุณสามารถสร้างกฎหรือกฎ IDS สำหรับบันทึกนั้นโดยการคลิกขวาบนรายการนั้นแล้วเลือก **อย่าปิดกั้นเหตุการณ์คล้ายคลึงกันอีกในอนาคต** โปรดทราบว่าบันทึกของการเชื่อมต่อที่ถูกปิดกั้นทั้งหมดอาจมีรายการนับพันรายการและอาจจะยากต่อการค้นหาการเชื่อมต่อแบบเฉพาะในบันทึกนี้ คุณสามารถปิดการบันทึกได้หลังจากที่คุณแก้ไขปัญหาแล้ว

เมื่อต้องการข้อมูลเพิ่มเติมเกี่ยวกับบันทึก ให้ดูที่ ไฟล์บันทึก

ใช้การบันทึกเพื่อดูอันดับที่การป้องกันเครือข่ายปิดกั้นการเชื่อมต่อเฉพาะ ยิ่งกว่านั้น การสร้างกฎจากบันทึกยังทำให้คุณสามารถสร้างกฎที่ทำในสิ่งที่คุณต้องการเป็นพิเศษได้

สร้างกฎจากบันทึก

ESET Smart Security Premium เวอร์ชันใหม่ช่วยให้คุณสามารถสร้างกฎได้จากบันทึก จากเมนูหลัก ให้คลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก** เลือก **ไฟร์วอลล์** จากเมนูแบบเลื่อนลง คลิกขวาที่รายการบันทึกที่คุณต้องการ แล้วเลือก **อย่าปิดกั้นเหตุการณ์คล้ายคลึงกันอีกในอนาคต** จากเมนูบริบท หน้าต่างการแจ้งเตือนจะแสดงกฎใหม่ของคุณ

ถ้าต้องการให้อนุญาตให้สร้างกฎใหม่จากบันทึก ต้องกำหนดค่า ESET Smart Security Premium ด้วยการตั้งค่าต่อไปนี้:

1. ตั้งค่าความละเอียดการบันทึกต่ำสุดไปที่ **การวินิจฉัย** ใน **การตั้งค่าขั้นสูง** (F5) > **เครื่องมือ** > **ไฟล์บันทึก**
2. เปิดใช้งาน **แสดงการแจ้งเตือนยังใช้เพื่อแจ้งเมื่อมีการโจมตีจุดอ่อนด้านการรักษาความปลอดภัย** ใน **การตั้งค่าขั้นสูง** (F5) > **การป้องกันเครือข่าย** > **การป้องกันการโจมตีเครือข่าย** > **ตัวเลือกขั้นสูง** > **การตรวจหาการบุกรุก**

การสร้างข้อยกเว้นการแจ้งเตือนไฟร์วอลล์

เมื่อไฟร์วอลล์ของ ESET ตรวจพบกิจกรรมเครือข่ายที่เป็นอันตราย หน้าต่างการแจ้งเตือนที่อธิบายกิจกรรมนั้นจะปรากฏขึ้นมา การแจ้งเตือนนี้มีลิงก์ที่จะช่วยให้คุณสามารถเรียนรู้เพิ่มเติมเกี่ยวกับกิจกรรมและตั้งค่ากฎสำหรับกิจกรรมนี้ได้หากต้องการ

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*

การแก้ไขปัญหาเกี่ยวกับการกรองโปรโตคอล

ถ้าคุณประสบปัญหาเกี่ยวกับเบราว์เซอร์หรืออีเมลไคลเอ็นต์ของคุณ ขั้นตอนแรกคือการพิจารณาว่าการกรองโปรโตคอลมีการตอบสนองหรือไม่ ในการดำเนินการดังกล่าว ให้ลองปิดใช้งานการกรองโปรโตคอลแอพพลิเคชันชั่วคราวในการตั้งค่าขั้นสูง (อย่าลืมเปิดกลับอีกครั้งหลังจากทำเสร็จ ไม่เช่นนั้น เบราว์เซอร์หรืออีเมลไคลเอ็นต์ของคุณจะยังคงไม่ได้รับการป้องกัน) ถ้าปัญหาของคุณไม่ปรากฏขึ้นมาหลังจากปิดระบบ ต่อไปนี้คือรายการปัญหาที่พบบ่อยและวิธีการแก้ไขปัญหาเหล่านั้น:

อัพเดทหรือรักษาความปลอดภัยของปัญหาในการสื่อสาร

ถ้าแอพพลิเคชันของคุณแจ้งเกี่ยวกับการไม่สามารถอัพเดทหรือช่องทางการสื่อสารไม่ปลอดภัย:

- ถ้าคุณเปิดใช้งานการกรองโปรโตคอล SSL ให้ลองปิดชั่วคราว ถ้าการดำเนินการนั้นช่วยได้ คุณจะสามารถใช้การกรอง SSL ได้เสมอและจะดำเนินการอัพเดทได้โดยการยกเว้นการสื่อสารที่มีปัญหา:
  สลับโหมดการกรองโปรโตรคอล SSL เป็นแบบโต้ตอบ ดำเนินการอัพเดทใหม่ จะมีข้อความแจ้งคุณเกี่ยวกับการรับส่งข้อมูลทางเครือข่ายที่เข้ารหัส ตรวจสอบให้แน่ใจว่าแอพพลิเคชันนั้นตรงกับแอพพลิเคชันที่คุณกำลังแก้ไขปัญหาและใบรับรองดูเหมือนว่ามาจากเซิร์ฟเวอร์ที่อัพเดทมา จากนั้นเลือกจำการทำงานสำหรับใบรับรองนี้แล้วคลิกละเว้น ถ้าไม่ได้แสดงข้อความที่เกี่ยวข้องอีก คุณสามารถสลับโหมดการกรองกลับไปเป็นอัตโนมัติได้ และจะสามารถแก้ไขปัญหาได้

- ถ้าแอพพลิเคชันดังกล่าวไม่ใช่เบราว์เซอร์หรืออีเมลไคลเอ็นต์ คุณจะสามารถยกเว้นจากการกรองโปรโตคอลได้ทั้งหมด (การดำเนินการสิ่งนี้สำหรับเบราว์เซอร์หรืออีเมลไคลเอ็นต์อาจทำให้คุณเกิดความเสี่ยงได้) แอพพลิเคชันใดๆ ที่กรองการสื่อสารไว้ในอดีตจะอยู่ในรายการที่ให้คุณอยู่แล้วเมื่อเพิ่มข้อยกเว้น ดังนั้นจึงไม่จำเป็นต้องเพิ่มแอพพลิเคชันด้วยตัวเอง

ปัญหาในการเข้าถึงอุปกรณ์ในเครือข่ายของคุณ

ถ้าคุณไม่สามารถใช้ฟังก์ชันใดๆ ของอุปกรณ์ในเครือข่ายของคุณได้ (สิ่งนี้หมายถึงการเปิดหน้าเว็บของเว็บแคมของคุณหรือการเล่นวิดีโอในเครื่องเล่นสื่อในบ้าน) ให้ลองเพิ่มที่อยู่ IPv4 หรือ IPv6 ไปยังรายการที่อยู่ที่ยกเว้น

ปัญหาเกี่ยวกับเว็บไซต์ที่ระบุ

คุณสามารถยกเว้นเว็บไซต์ที่ระบุเฉพาะจากการกรองโปรโตคอลโดยใช้การจัดการที่อยู่ URL ได้ ตัวอย่างเช่น ถ้าคุณไม่สามารถเข้าไปที่ https://www.gmail.com/intl/en/mail/help/about.html ให้ลองเพิ่ม *gmail.com* ไปยังรายการที่อยู่ที่ยกเว้น

ข้อผิดพลาดแจ้งว่า "แอพพลิเคชันบางตัวที่สามารถนำเข้าใบรับรองหลักกำลังทำงานอยู่"

เมื่อคุณเปิดใช้งานการกรองโปรโตคอล SSL ESET Smart Security Premium จะตรวจสอบให้แน่ใจว่าแอพพลิเคชันที่ติดตั้งเชื่อถือวิธีการกรองโปรโตคอล SSL โดยการนำเข้าใบรับรองไปยังร้านใบรับรองของแอพพลิเคชัน สำหรับ

แอพพลิเคชันบางตัว การดำเนินการนี้จะไม่สามารถทำได้ในขณะทำงานอยู่ ซึ่งรวมถึง Firefox และ Opera ตรวจสอบว่าไม่ได้ใช้งานแอพพลิเคชันเหล่านั้นอยู่ (วิธีการตรวจสอบที่ดีที่สุดคือให้เปิดโปรแกรมจัดการงาน และตรวจสอบว่าไม่มี firefox.exe หรือ opera.exe ด้านใต้แท็บกระบวนการ) จากนั้นให้ลองใหม่

ข้อผิดพลาดเกี่ยวกับผู้ออกใบรับรองที่เชื่อถือหรือลายเซ็นที่ไม่ถูกต้อง

เป็นไปได้มากว่าข้อผิดพลาดนี้เกิดจากการนำเข้าที่อธิบายไว้ข้างต้นล้มเหลว ขั้นแรก ตรวจสอบให้แน่ใจว่าไม่ได้ใช้งานแอพพลิเคชันดังกล่าวอยู่ จากนั้นให้ปิดใช้งานการกรองโปรโตคอล SSL แล้วเปิดใช้งานอีกครั้ง ขั้นตอนนี้จะดำเนินการนำเข้าอีกครั้ง

> ดูบทความฐานความรู้เพื่อเรียนรู้ วิธีการจัดการการกรองโปรโตคอล/SSL/TLS ในผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้าน

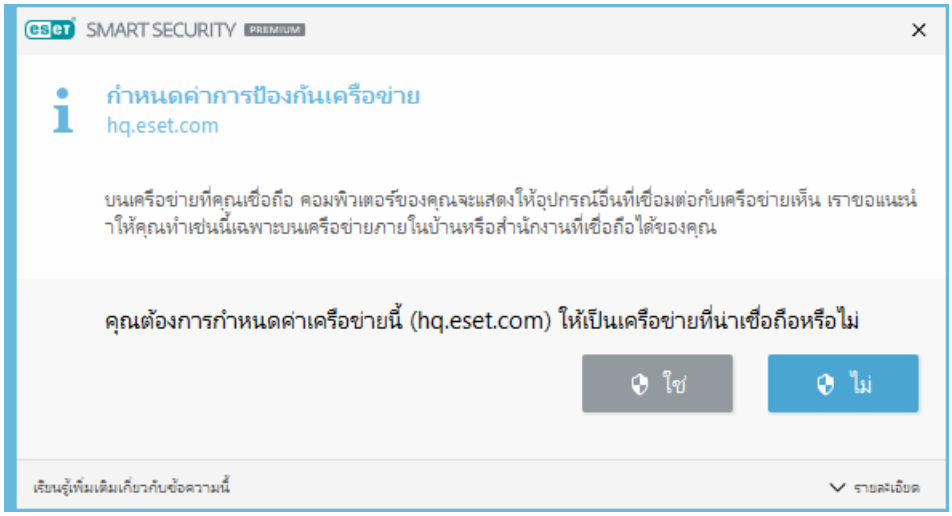
พบเครือข่ายใหม่

โดยค่าเริ่มต้น ESET Smart Security Premium จะใช้การตั้งค่า Windows เมื่อมีการตรวจพบเครือข่ายใหม่ หากต้องการให้แสดงหน้าต่างข้อความเมื่อตรวจพบเครือข่ายใหม่ ให้เปลี่ยนประเภทการป้องกันของเครือข่ายใหม่ใน เครือข่ายที่รู้จัก เป็นถามผู้ใช้ จากนั้นหากมีการตรวจพบการเชื่อมต่อกับเครือข่ายใหม่ ผู้ใช้สามารถเลือกระดับการป้องกันได้ การตั้งค่านี้จะใช้สำหรับการเชื่อมต่อกับคอมพิวเตอร์ระยะไกลทั้งหมดจากเครือข่ายที่กำหนด

มีโหมดการป้องกันเครือข่ายสองโหมดที่คุณสามารถเลือกได้จากในหน้าต่างการกำหนดค่าการป้องกันเครือข่าย ดังนี้:

- **ใช่** – สำหรับเครือข่ายที่เชื่อถือ (เครือข่ายในบ้านหรือที่ทำงาน) ผู้ใช้เครือข่ายรายอื่นสามารถมองเห็นคอมพิวเตอร์และไฟล์ที่ใช้ร่วมกันที่เก็บไว้ในคอมพิวเตอร์ของคุณได้ และผู้ใช้รายอื่นบนเครือข่ายสามารถเข้าถึงทรัพยากรระบบได้ เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าถึงเครือข่ายภายในที่ปลอดภัย

- **ไม่** – สำหรับเครือข่ายที่ไม่เชื่อถือ (เครือข่ายสาธารณะ) ไฟล์และโฟลเดอร์ในระบบของคุณจะไม่ถูกใช้ร่วมกันหรือมองเห็นได้สำหรับผู้ใช้รายอื่นบนเครือข่าย และการแบ่งปันทรัพยากรระบบจะถูกปิดใช้งาน เราขอแนะนำให้ใช้การตั้งค่านี้เมื่อเข้าสู่เครือข่ายไร้สาย



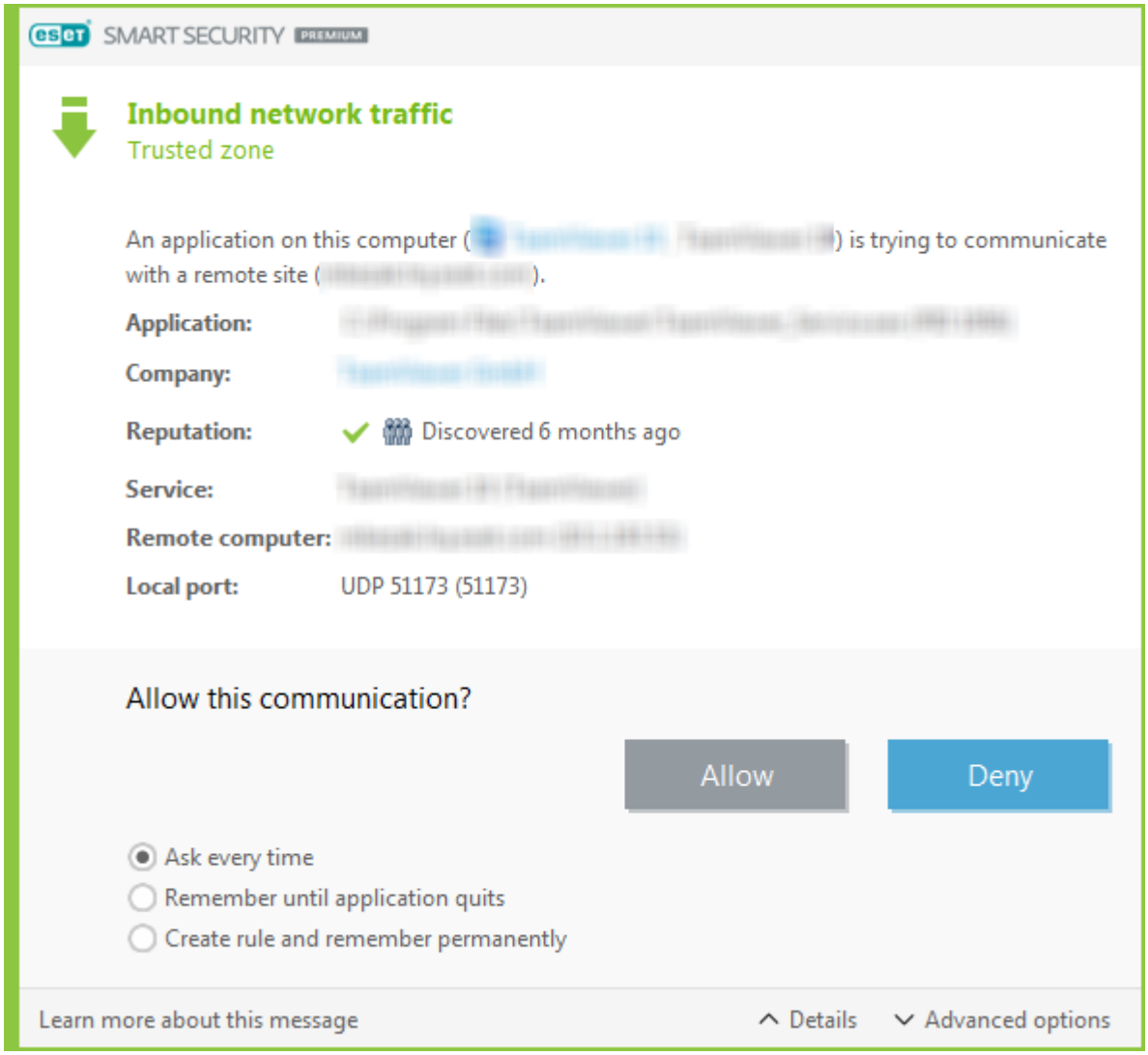
หากตั้งค่าเครือข่ายเป็นเชื่อถือได้ เครือข่ายย่อยที่เชื่อมต่อโดยตรงจะได้รับการพิจารณาเป็นเครือข่ายย่อยที่เชื่อถือโดยอัตโนมัติ

การเปลี่ยนแปลงแอพพลิเคชัน

ไฟล์วอลล์ส่วนบุคคลตรวจพบการแก้ไขในแอพพลิเคชัน ซึ่งใช้เพื่อสร้างการเชื่อมต่อขาออกจากคอมพิวเตอร์ของคุณ เป็นไปได้ว่า มีการอัพเดทแอพพลิเคชันเป็นเวอร์ชันใหม่ ในทางตรงกันข้าม การแก้ไขอาจเกิดจากแอพพลิเคชันที่เป็นอันตราย หากคุณไม่ทราบว่ามีการแก้ไขที่ถูกต้อง เราขอแนะนำให้คุณปฏิเสธการเชื่อมต่อ และ สแกนคอมพิวเตอร์ของคุณ โดยใช้ ฐานข้อมูลไวรัสล่าสุด

การสื่อสารขาเข้าที่เชื่อถือ

ตัวอย่างของการเชื่อมต่อขาเข้าภายในโซนที่เชื่อถือ:
คอมพิวเตอร์ระยะไกลจากโซนที่เชื่อถือ ซึ่งพยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันในระบบที่ทำงานบนคอมพิวเตอร์ของคุณ



แอพพลิเคชัน – แอพพลิเคชันที่ติดต่อโดยคอมพิวเตอร์ระยะไกล

บริษัท – ผู้เผยแพร่ของแอพพลิเคชัน

ความเชื่อถือ – ความเชื่อถือของแอพพลิเคชันที่ได้รับโดยเทคโนโลยี ESET LiveGrid®

บริการ - ชื่อของบริการที่ทำงานอยู่บนคอมพิวเตอร์ของคุณในขณะนี้

คอมพิวเตอร์ระยะไกล – คอมพิวเตอร์ระยะไกลที่พยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันบนคอมพิวเตอร์ของคุณ

พอร์ตในระบบ – พอร์ตที่ใช้สำหรับการสื่อสาร

ถามทุกครั้ง - หากการกระทำตามค่าเริ่มต้นสำหรับกฎถูกตั้งให้เป็น **ถาม** หน้าต่างข้อความจะปรากฏขึ้นในแต่ละครั้งที่กฎทำงาน

จดจำจนกว่าจะออกจากแอพพลิเคชัน - ESET Smart Security Premium จะจดจำการกระทำที่เลือกจนกว่าจะเริ่ม

ต้นระบบคอมพิวเตอร์ใหม่

สร้างกฎและจดจำอย่างถาวร - หากคุณเลือกตัวเลือกนี้ก่อนที่จะอนุญาตหรือปฏิเสธการติดต่อ ESET Smart Security Premium จะจดจำการกระทำและใช้การกระทำดังกล่าวหากแอพพลิเคชันเชื่อมต่อกับคอมพิวเตอร์ระยะไกลอีกครั้ง

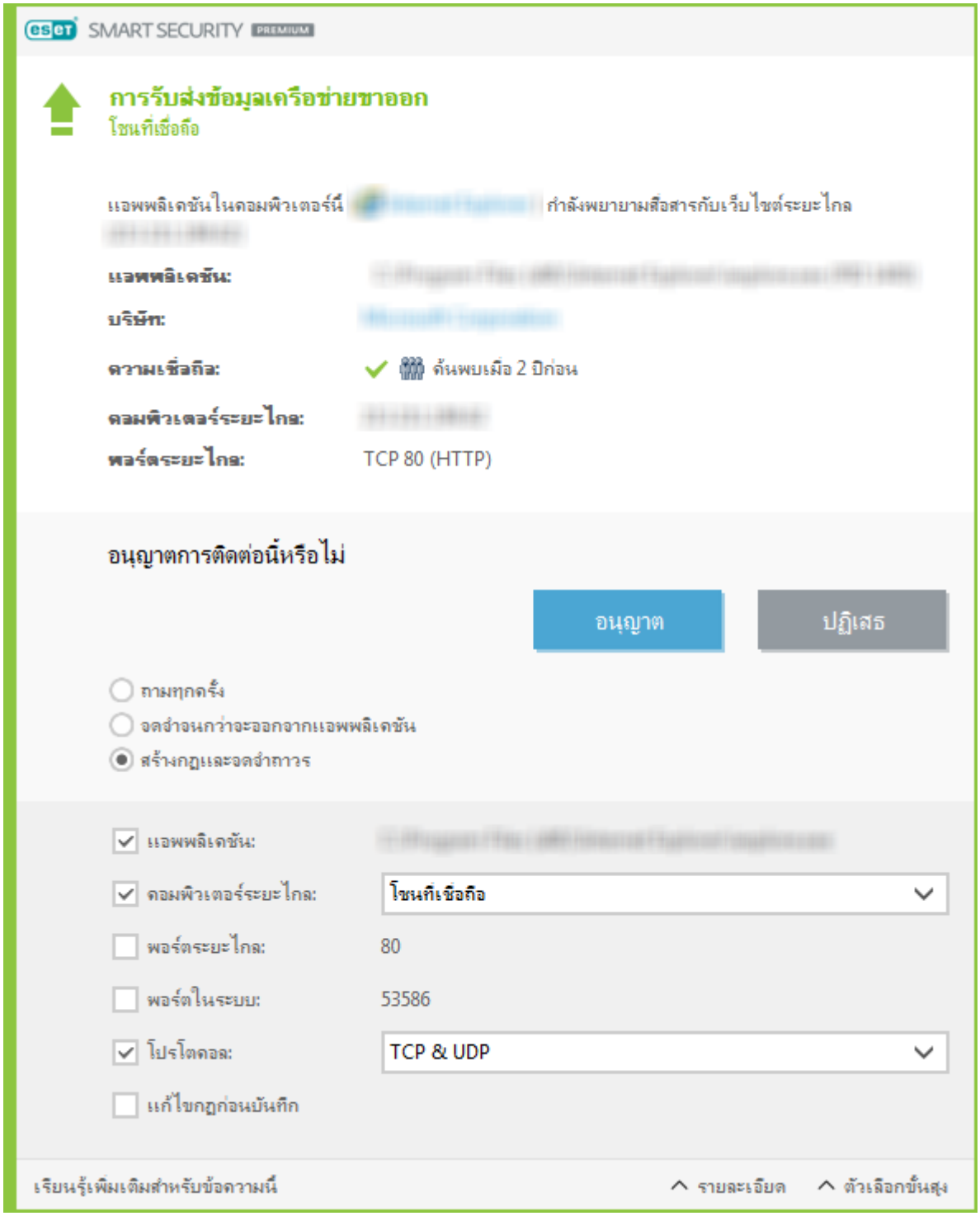
อนุญาต – อนุญาตการสื่อสารขาเข้า

ปฏิเสธ – ปฏิเสธการสื่อสารขาเข้า

ตัวเลือกขั้นสูง - อนุญาตให้คุณปรับคุณสมบัติของกฎ

การสื่อสารขาออกที่เชื่อถือ

ตัวอย่างของการเชื่อมต่อขาออกภายในโซนที่เชื่อถือ:
แอพพลิเคชันในระบบที่พยายามเริ่มต้นการเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่นภายในเครือข่ายของระบบ หรือภายในเครือข่ายในโซนที่เชื่อถือ



แอพพลิเคชัน – แอพพลิเคชันที่ติดต่อโดยคอมพิวเตอร์ระยะไกล

บริษัท – ผู้เผยแพร่ของแอพพลิเคชัน

ความเชื่อถือ – ความเชื่อถือของแอพพลิเคชันที่ได้รับโดยเทคโนโลยี ESET LiveGrid®

บริการ - ชื่อของบริการที่ทำงานอยู่บนคอมพิวเตอร์ของคุณในขณะนี้

คอมพิวเตอร์ระยะไกล – คอมพิวเตอร์ระยะไกลที่พยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันบนคอมพิวเตอร์ของ

คุณ

พอร์ตในระบบ – พอร์ตที่ใช้สำหรับการสื่อสาร

ถามทุกครั้ง - หากการกระทำตามค่าเริ่มต้นสำหรับกฎถูกตั้งให้เป็น **ถาม** หน้าต่างข้อความจะปรากฏขึ้นในแต่ละครั้งที่กฎทำงาน

จดจำจนกว่าจะออกจากแอพพลิเคชัน - ESET Smart Security Premium จะจดจำการกระทำที่เลือกจนกว่าจะเริ่มต้นระบบคอมพิวเตอร์ใหม่

สร้างกฎและจดจำอย่างถาวร - หากคุณเลือกตัวเลือกนี้ก่อนที่จะอนุญาตหรือปฏิเสธการติดต่อ ESET Smart Security Premium จะจดจำการกระทำและใช้การกระทำดังกล่าวหากแอพพลิเคชันเชื่อมต่อกับคอมพิวเตอร์ระยะไกลอีกครั้ง

อนุญาต – อนุญาตการสื่อสารขาเข้า

ปฏิเสธ – ปฏิเสธการสื่อสารขาเข้า

ตัวเลือกขั้นสูง - อนุญาตให้คุณปรับคุณสมบัติของกฎ

การสื่อสารขาเข้า

ตัวอย่างของการเชื่อมต่ออินเทอร์เน็ตขาเข้า:
คอมพิวเตอร์ระยะไกลที่พยายามสื่อสารกับแอพพลิเคชันที่ทำงานบนคอมพิวเตอร์

แอพพลิเคชัน – แอพพลิเคชันที่ติดต่อโดยคอมพิวเตอร์ระยะไกล

บริษัท – ผู้เผยแพร่ของแอพพลิเคชัน

ความเชื่อถือ – ความเชื่อถือของแอพพลิเคชันที่ได้รับโดยเทคโนโลยี ESET LiveGrid®

บริการ - ชื่อของบริการที่ทำงานอยู่บนคอมพิวเตอร์ของคุณในขณะนี้

คอมพิวเตอร์ระยะไกล – คอมพิวเตอร์ระยะไกลที่พยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันบนคอมพิวเตอร์ของคุณ

พอร์ตในระบบ – พอร์ตที่ใช้สำหรับการสื่อสาร

ถามทุกครั้ง - หากการกระทำตามค่าเริ่มต้นสำหรับกฎถูกตั้งให้เป็น **ถาม** หน้าต่างข้อความจะปรากฏขึ้นในแต่ละ

ครั้งที่กฎทำงาน

จดจำจนกว่าจะออกจากแอพพลิเคชัน - ESET Smart Security Premium จะจดจำการกระทำที่เลือกจนกว่าจะเริ่มต้นระบบคอมพิวเตอร์ใหม่

สร้างกฎและจดจำอย่างถาวร - หากคุณเลือกตัวเลือกนี้ก่อนที่จะอนุญาตหรือปฏิเสธการติดต่อ ESET Smart Security Premium จะจดจำการกระทำและใช้การกระทำดังกล่าวหากแอพพลิเคชันเชื่อมต่อกับคอมพิวเตอร์ระยะไกลอีกครั้ง

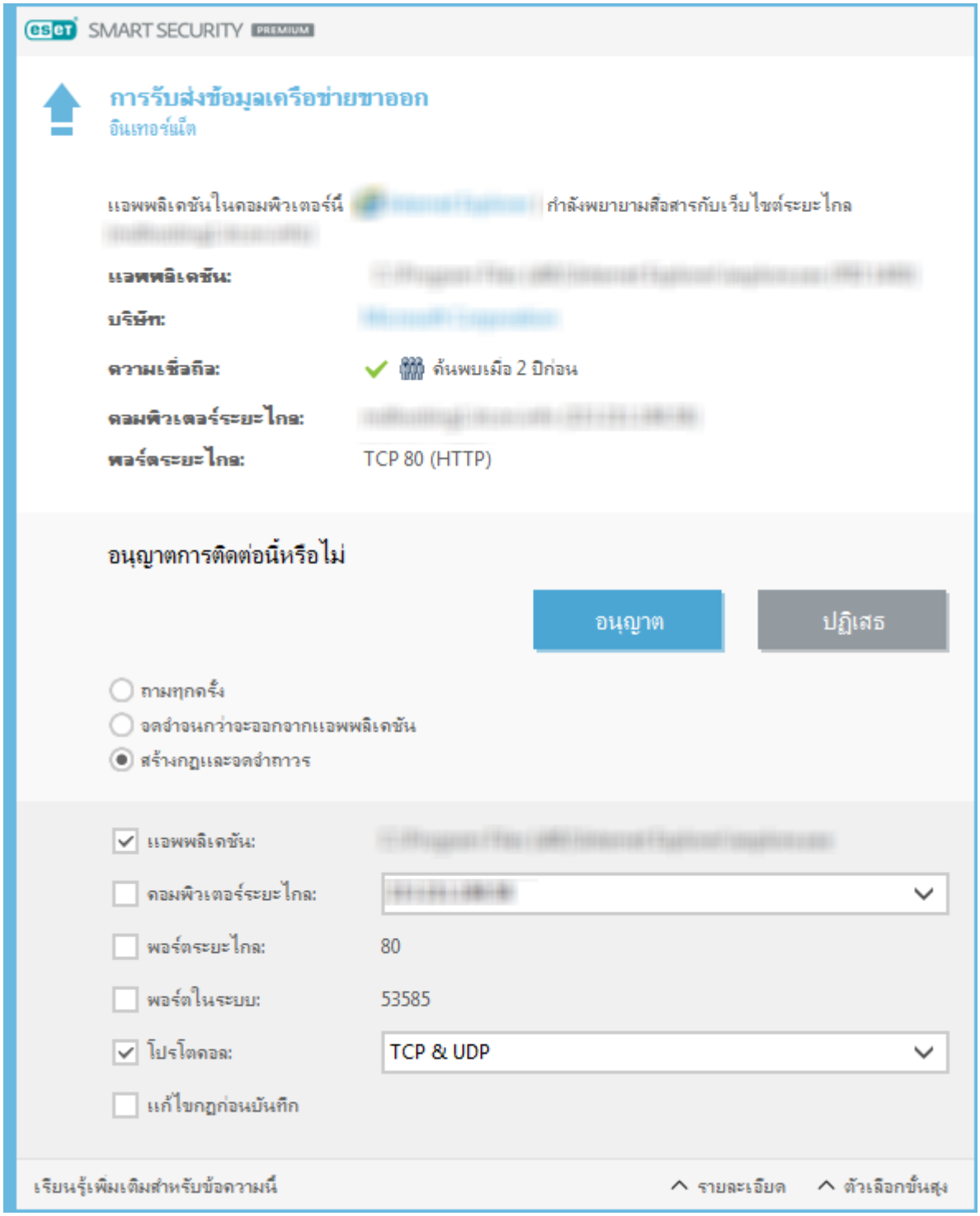
อนุญาต – อนุญาตการสื่อสารขาเข้า

ปฏิเสธ – ปฏิเสธการสื่อสารขาเข้า

ตัวเลือกขั้นสูง - อนุญาตให้คุณปรับคุณสมบัติของกฎ

การสื่อสารขาออก

ตัวอย่างของการเชื่อมต่ออินเทอร์เน็ตขาออก:
แอพพลิเคชันในระบบที่พยายามเริ่มต้นการเชื่อมต่ออินเทอร์เน็ต



แอพพลิเคชัน – แอพพลิเคชันที่ติดต่อโดยคอมพิวเตอร์ระยะไกล

บริษัท – ผู้เผยแพร่ของแอพพลิเคชัน

ความเชื่อถือ – ความเชื่อถือของแอพพลิเคชันที่ได้รับโดยเทคโนโลยี ESET LiveGrid®

บริการ - ชื่อของบริการที่ทำงานอยู่บนคอมพิวเตอร์ของคุณในขณะนี้

คอมพิวเตอร์ระยะไกล – คอมพิวเตอร์ระยะไกลที่พยายามเริ่มต้นการสื่อสารกับแอพพลิเคชันบนคอมพิวเตอร์ของ

คุณ

พอร์ตในระบบ – พอร์ตที่ใช้สำหรับการสื่อสาร

ถามทุกครั้ง - หากการกระทำตามค่าเริ่มต้นสำหรับกฎถูกตั้งให้เป็น **ถาม** หน้าต่างข้อความจะปรากฏขึ้นในแต่ละครั้งที่กฎทำงาน

จดจำจนกว่าจะออกจากแอพพลิเคชัน - ESET Smart Security Premium จะจดจำการกระทำที่เลือกจนกว่าจะเริ่มต้นระบบคอมพิวเตอร์ใหม่

สร้างกฎและจดจำอย่างถาวร - หากคุณเลือกตัวเลือกนี้ก่อนที่จะอนุญาตหรือปฏิเสธการติดต่อ ESET Smart Security Premium จะจดจำการกระทำและใช้การกระทำดังกล่าวหากแอพพลิเคชันเชื่อมต่อกับคอมพิวเตอร์ระยะไกลอีกครั้ง

อนุญาต – อนุญาตการสื่อสารขาเข้า

ปฏิเสธ – ปฏิเสธการสื่อสารขาเข้า

ตัวเลือกขั้นสูง - อนุญาตให้คุณปรับคุณสมบัติของกฎ

ตั้งค่ามุมมองการเชื่อมต่อ

คลิกขวาที่การเชื่อมต่อเพื่อดูตัวเลือกอื่นๆ ที่มีอยู่:

แปลค่าชื่อโฮสต์ – ถ้าเป็นไปได้ ที่อยู่เครือข่ายทั้งหมดจะแสดงในรูปแบบ DNS ไม่ใช่ในรูปแบบที่อยู่ IP ที่เป็นตัวเลข

แสดงเฉพาะการเชื่อมต่อ TCP – รายการจะแสดงเฉพาะการเชื่อมต่อที่อยู่ในชุดโปรโตคอล TCP

แสดงการเชื่อมต่อของรายชื่อ – เลือกตัวเลือกนี้เพื่อแสดงเฉพาะการเชื่อมต่อที่ยังไม่ได้เริ่มต้นการสื่อสาร แต่ระบบได้เปิดพอร์ตและกำลังรอการเชื่อมต่ออยู่

แสดงการเชื่อมต่อภายในคอมพิวเตอร์ – เลือกตัวเลือกนี้เพื่อแสดงเฉพาะการเชื่อมต่อที่คอมพิวเตอร์ระยะไกลเป็นระบบภายใน หรือเรียกว่าการเชื่อมต่อ localhost

ความเร็วในการรีเฟรช – เลือกความถี่ในการรีเฟรชการเชื่อมต่อที่ใช้งาน

รีเฟรชทันที – โหลดหน้าต่าง **การเชื่อมต่อในเครือข่าย** อีกครั้ง

เครื่องมือความปลอดภัย

การตั้งค่า **เครื่องมือรักษาความปลอดภัย** ช่วยให้คุณสามารถปรับโมดูลต่อไปนี้:

• **การป้องกันทางด้านธนาคารและการชำระเงิน** – จะเพิ่มระดับการป้องกันเบราว์เซอร์เพิ่มเติมซึ่งออกแบบมาเพื่อปกป้องข้อมูลทางการเงินของคุณระหว่างการทำธุรกรรมออนไลน์ เปิดใช้งาน **ป้องกันเบราว์เซอร์ทั้งหมด** เพื่อเริ่มใช้งาน เว็บเบราว์เซอร์ที่รองรับ ในโหมดปลอดภัย สำหรับข้อมูลเพิ่มเติมโปรดดู การป้องกันทางด้านธนาคารและการชำระเงิน

• **การควบคุมเนื้อหาเว็บไซต์** – โมดูล การควบคุมเนื้อหาเว็บไซต์ จะช่วยปกป้องบุตรหลานของคุณโดยบล็อกเนื้อหาที่ไม่เหมาะสมหรือเป็นอันตรายบนอินเทอร์เน็ต

• **Anti-Theft** – เปิดใช้งาน การป้องกันการโจรกรรม เพื่อป้องกันคอมพิวเตอร์ของคุณในกรณีที่เกิดการสูญหายหรือถูกโจรกรรม

• **Secure Data** — เมื่อเปิดใช้งาน ESET Secure Data คุณสามารถเข้ารหัสข้อมูลของคุณเพื่อป้องกันการใช้ข้อมูลส่วนตัวที่เป็นความลับในทางที่ผิด

• **Password Manager** – Password Manager จะปกป้องและจัดเก็บรหัสผ่านและข้อมูลส่วนบุคคลของคุณ

การป้องกันการธนาคารและการชำระเงิน

การป้องกันการธนาคารและการชำระเงินเป็นระดับการป้องกันเพิ่มเติมซึ่งออกแบบมาเพื่อปกป้องข้อมูลการเงินของคุณในระหว่างที่ทำธุรกรรมออนไลน์

ในกรณีส่วนใหญ่ เบราว์เซอร์ที่มีการป้องกันสำหรับการป้องกันทางด้านธนาคารและการชำระเงินจะเปิดในเบราว์เซอร์ที่คุณใช้งานอยู่ในขณะนี้หลังจากที่คุณเข้าไปที่เว็บไซต์บริการธนาคารที่รู้จัก

เลือกหนึ่งรายการจากตัวเลือกการกำหนดค่าพฤติกรรมของเบราว์เซอร์ที่มีการป้องกันต่อไปนี้:

• **ป้องกันเบราว์เซอร์ทั้งหมด** – หากเปิดใช้งาน เว็บเบราว์เซอร์ทั้งหมดที่รองรับจะเริ่มต้นในโหมดปลอดภัย ซึ่งช่วยให้คุณสามารถเรียกใช้อินเทอร์เน็ต เข้าถึงธนาคารบนอินเทอร์เน็ต และซื้อของออนไลน์ รวมถึงการทำธุรกรรมในหน้าต่างเบราว์เซอร์ที่มีการป้องกันโดยไม่ต้องเปลี่ยนเส้นทาง

• **การเปลี่ยนเส้นทางเว็บไซต์** (ค่าเริ่มต้น) – เว็บไซต์จากรายการเว็บไซต์ที่ได้รับการป้องกันและรายการ

ธนาคารบนอินเทอร์เน็ตภายในจะเปลี่ยนเส้นทางไปยังเบราว์เซอร์ที่มีการป้องกัน คุณสามารถเลือกได้ว่าจะเปิดเบราว์เซอร์ใด (มาตรฐานหรือมีการป้องกัน)

• ตัวเลือกทั้งสองตัวเลือกก่อนหน้านี้จะปิดใช้งานอยู่ – หากต้องการเข้าถึงเบราว์เซอร์ที่มีการป้องกันใน ESET Smart Security Premium ให้คลิก **เครื่องมือ** > **การป้องกันทางด้านธนาคารและการชำระเงิน** หรือคลิกไอคอนเดสก์ท็อป **การป้องกันทางด้านธนาคารและการชำระเงิน** เบราว์เซอร์ Windows จะเริ่มทำงานในโหมดปลอดภัยตามที่ตั้งไว้เป็นค่าเริ่มต้น

เมื่อต้องการกำหนดค่าลักษณะการทำงานของเบราว์เซอร์ที่มีการป้องกัน โปรดดู การตั้งค่าขั้นสูงของการป้องกันทางด้านธนาคารและการชำระเงิน เมื่อต้องการเปิดใช้งานคุณลักษณะป้องกันเบราว์เซอร์ทั้งหมดใน ESET Smart Security Premium ให้คลิก **การตั้งค่า** > **เครื่องมือความปลอดภัย** และเปิดใช้งานแถบตัวเลื่อน **ป้องกันเบราว์เซอร์ทั้งหมด**

การใช้การสื่อสารที่เข้ารหัส HTTPS นั้นเป็นสิ่งจำเป็นสำหรับการเรียกดูโดยได้รับการป้องกัน โดยเบราว์เซอร์ต่อไปนี้จะรองรับการป้องกันทางด้านธนาคารและการชำระเงิน:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับคุณสมบัติการป้องกันทางด้านธนาคารและการชำระเงิน ให้อ่านบทความฐานความรู้ ESET ต่อไปนี้ในภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษา:

- ฉันสามารถใช้ ESET การป้องกันการธนาคารและการชำระเงินได้อย่างไร
- เปิดหรือปิดใช้งาน ESETการป้องกันทางด้านธนาคารและการชำระเงินสำหรับเว็บไซต์เฉพาะ
- หยุดชั่วคราวหรือปิดใช้งานการป้องกันธนาคารและการชำระเงินในผลิตภัณฑ์ ESET Windows home
- การป้องกันทางด้านธนาคารและการชำระเงินของ ESET—ข้อผิดพลาดทั่วไป
- ประมวลศัพท์ ESET | การป้องกันการธนาคารและการชำระเงิน

การตั้งค่าขั้นสูงสำหรับการป้องกันทางด้านธนาคารและการชำระเงิน

การตั้งค่านี้มีให้ใช้งานใน **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล์** > **การป้องกันทางด้านธนาคารและการชำระเงิน**

พื้นฐาน

เปิดใช้การป้องกันการธนาคารและการชำระเงิน – เมื่อเปิดใช้งานการป้องกันการธนาคารและการชำระเงิน รายการของเว็บไซต์ที่มีการป้องกันจะทำงาน ซึ่งจะอนุญาตให้คุณแก้ไขรายการเว็บไซต์ที่มีการป้องกันได้

การป้องกันเบราว์เซอร์

ป้องกันเบราว์เซอร์ทั้งหมด – เปิดใช้งานตัวเลือกนี้เพื่อเริ่มเว็บเบราว์เซอร์ที่ได้รับการสนับสนุนในโหมดปลอดภัย

โหมดการติดตั้งส่วนขยาย – จากเมนูแบบเลื่อนลง คุณสามารถเลือกว่าจะอนุญาตส่วนขยายใดให้สามารถติดตั้งโดยเบราว์เซอร์ที่ ESET ป้องกันได้: การเปลี่ยนโหมดการติดตั้งส่วนขยายจะไม่มีผลกับส่วนขยายเบราว์เซอร์ที่ติดตั้งไว้ก่อนหน้านี้:

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

การเปลี่ยนเส้นทางเว็บไซต์

เปิดใช้งานการเปลี่ยนเส้นทางเว็บไซต์ที่ได้รับการป้องกัน – หากเปิดใช้งาน เว็บไซต์ต่างๆ ที่อยู่ในรายการเว็บไซต์ที่ได้รับการป้องกันและในรายการธนาคารอินเทอร์เน็ตภายในจะถูกเปลี่ยนเส้นทางไปยังเบราว์เซอร์ที่ปลอดภัย

เว็บไซต์ที่มีการป้องกัน - รายการของเว็บไซต์ที่คุณสามารถเลือกเบราว์เซอร์ (ทั่วไปหรือแบบปลอดภัย) ที่จะเปิดได้ โลโก้ ESET จะแสดงขึ้นในกรอบเบราว์เซอร์เพื่อยืนยันว่าเบราว์เซอร์ที่มีความปลอดภัยกำลังทำงานอยู่ หากต้องการแก้ไขรายการนี้โปรดดูเว็บไซต์ที่มีการป้องกัน

เบราว์เซอร์ที่มีการป้องกัน

เปิดใช้งานการป้องกันหน่วยความจำที่ได้รับการปรับปรุง – หากเปิดใช้งาน หน่วยความจำของเบราว์เซอร์ที่ปลอดภัยจะได้รับการป้องกันไม่ให้ถูกสอดส่องโดยกระบวนการอื่นๆ

เปิดใช้งานการป้องกันแป้นพิมพ์ – หากเปิดใช้งานแล้ว ข้อมูลที่คุณป้อนด้วยแป้นพิมพ์ลงในเบราว์เซอร์ที่มีการป้องกันจะถูกซ่อนจากแอพพลิเคชันอื่น การเปิดใช้งานจะเพิ่มการป้องกัน เครื่องมือบันทึกการกดแป้นพิมพ์

กรอบสีเขียวของเบราว์เซอร์ – หากปิดใช้งาน การแจ้งเตือนในเบราว์เซอร์ ที่ให้ข้อมูลและกรอบสีเขียวรอบๆ เบราว์เซอร์จะแสดงชั่วครู่ระหว่างการเริ่มต้นเบราว์เซอร์และจะหายไป

เว็บไซต์ที่มีการป้องกัน

ESET Smart Security Premium มีรายการเว็บไซต์ที่กำหนดไว้แล้วอยู่ภายในตัวซึ่งจะเรียกใช้เบราว์เซอร์ปลอดภัยในการเปิด คุณสามารถเพิ่มเว็บไซต์หรือแก้ไขรายการเว็บไซต์ในการกำหนดค่าผลิตภัณฑ์ได้

รายการ **เว็บไซต์ที่มีการป้องกัน** สามารถดูและแก้ไขได้ใน **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล์** > **การป้องกันทางด้านธนาคารและการชำระเงิน** > **พื้นฐาน** > **เว็บไซต์ที่มีการป้องกัน** > **แก้ไข** หน้าต่างจะประกอบด้วย:

คอลัมน์

เว็บไซต์ - เว็บไซต์ที่มีการป้องกัน

เบราว์เซอร์ที่มีการป้องกัน - โลโก้ของ ESET จะแสดงขึ้นรอบๆ ขอบของเบราว์เซอร์ของคุณระหว่างเลือกดูอินเทอร์เน็ตอย่างปลอดภัย

ถามฉัน - เมื่อเปิดใช้งาน ข้อความที่มีตัวเลือกการเลือกดูจะแสดงขึ้นในเวลาใดๆ ที่มีการเยี่ยมชมเว็บไซต์ที่มีการป้องกัน ESET Smart Security Premium สามารถจดจำการดำเนินการของคุณหรือคุณสามารถเลือกวิธีที่คุณจะดำเนินการด้วยตัวเองได้

เบราว์เซอร์ปกติ - การเลือกตัวเลือกนี้จะดำเนินการธุรกรรมทางธนาคารต่อโดยไม่มีความปลอดภัยเพิ่มเติม

องค์ประกอบการควบคุม

เพิ่ม - อนุญาตให้คุณเพิ่มเว็บไซต์ลงในรายการเว็บไซต์ที่รู้จัก

แก้ไข - อนุญาตให้คุณแก้ไขรายการที่เลือกได้

ลบออก – ลบรายการที่เลือกออก

นำเข้า/ส่งออก – อนุญาตให้คุณส่งออกเว็บไซต์ที่ได้รับการป้องกันและนำเข้าเว็บไซต์ดังกล่าวไปยังอุปกรณ์เครื่องใหม่

การแจ้งเตือนในเบราว์เซอร์

เบราว์เซอร์ที่มีการป้องกันจะแจ้งให้คุณทราบเกี่ยวกับสถานะปัจจุบันผ่านการแจ้งเตือนในเบราว์เซอร์และสีของกรอบเบราว์เซอร์

การแจ้งเตือนในเบราว์เซอร์จะแสดงในแท็บทางด้านขวา

หากต้องการขยายการแจ้งเตือนในเบราว์เซอร์ ให้คลิกไอคอน ESET หากต้องการย่อขนาดการแจ้งเตือน ให้คลิกข้อความการแจ้งเตือน หากต้องการปิดการแจ้งเตือน ให้คลิกไอคอนปิด

การแจ้งเตือนในเบราว์เซอร์

ประเภทการแจ้งเตือน	สถานะ
การแจ้งเตือนแบบมีข้อมูลและ กรอบเบราว์เซอร์สีเขียว	การป้องกันสูงสุดจะมั่นใจได้และการแจ้งเตือนในเบราว์เซอร์จะย่อขนาดลงตามค่าเริ่มต้น ขยายการแจ้งเตือนในเบราว์เซอร์เพื่อแสดงตัวเลือกการกำหนดค่า: • **ซ่อนกรอบสีเขียวของเบราว์เซอร์** – เลือกกล่องกาเครื่องหมายเพื่อซ่อนกรอบสีเขียวรอบเบราว์เซอร์เมื่อคุณปิดการแจ้งเตือน คุณสามารถปิดการแจ้งเตือนในเบราว์เซอร์ที่ให้ข้อมูลและกรอบสีเขียวรอบเบราว์เซอร์อย่างถาวรได้ในหน้าจอ การตั้งค่าขั้นสูงสำหรับการป้องกันทางด้านธนาคารและการชำระเงิน • **การตั้งค่า** – เปิดการตั้งค่า เครื่องมือความปลอดภัย
คำเตือนและกรอบเบราว์เซอร์สีส้ม	เบราว์เซอร์ที่มีการป้องกันต้องการความสนใจจากคุณหากมีปัญหาที่ไม่ร้ายแรง สำหรับข้อมูลเพิ่มเติมเกี่ยวกับปัญหาหรือวิธีแก้ไขปัญหา ให้ทำตามคำแนะนำของการแจ้งเตือนในเบราว์เซอร์

ประเภทการแจ้งเตือน	สถานะ
การเตือนความปลอดภัยและกรอบเบราว์เซอร์สีแดง	เบราว์เซอร์ไม่ได้รับการปกป้องโดยการป้องกันทางด้านธนาคารและการชำระเงินของ ESET ให้รีสตาร์ทเบราว์เซอร์เพื่อให้แน่ใจว่าการป้องกันทำงานอยู่ หากต้องการแก้ไขจุดที่ขัดแย้งกับไฟล์ที่โหลดในเบราว์เซอร์ โปรดติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET โดยทำตามคำแนะนำในบทความฐานความรู้ของเรา

การควบคุมเนื้อหา

โมดูลการควบคุมเนื้อหาจะช่วยให้คุณสามารถกำหนดค่าการตั้งค่าการควบคุมเนื้อหา ซึ่งจะให้เครื่องมืออัตโนมัติแก่ผู้ปกครองเพื่อช่วยป้องกันเด็กๆ ของพวกเขาและตั้งค่าข้อจำกัดสำหรับอุปกรณ์และบริการ เป้าหมายก็คือการป้องกันเด็กและวัยรุ่นเข้าถึงหน้าเว็บที่มีเนื้อหาที่ไม่เหมาะสมหรือเป็นอันตราย

การควบคุมเนื้อหาจะช่วยให้คุณปิดกั้นหน้าเว็บที่อาจมีเนื้อหาที่ไม่เหมาะสม นอกจากนี้ ผู้ปกครองสามารถห้ามการเข้าถึงเว็บไซต์ที่กำหนดไว้ล่วงหน้าได้มากกว่า 40 ประเภทและกว่า 140 ประเภทย่อย

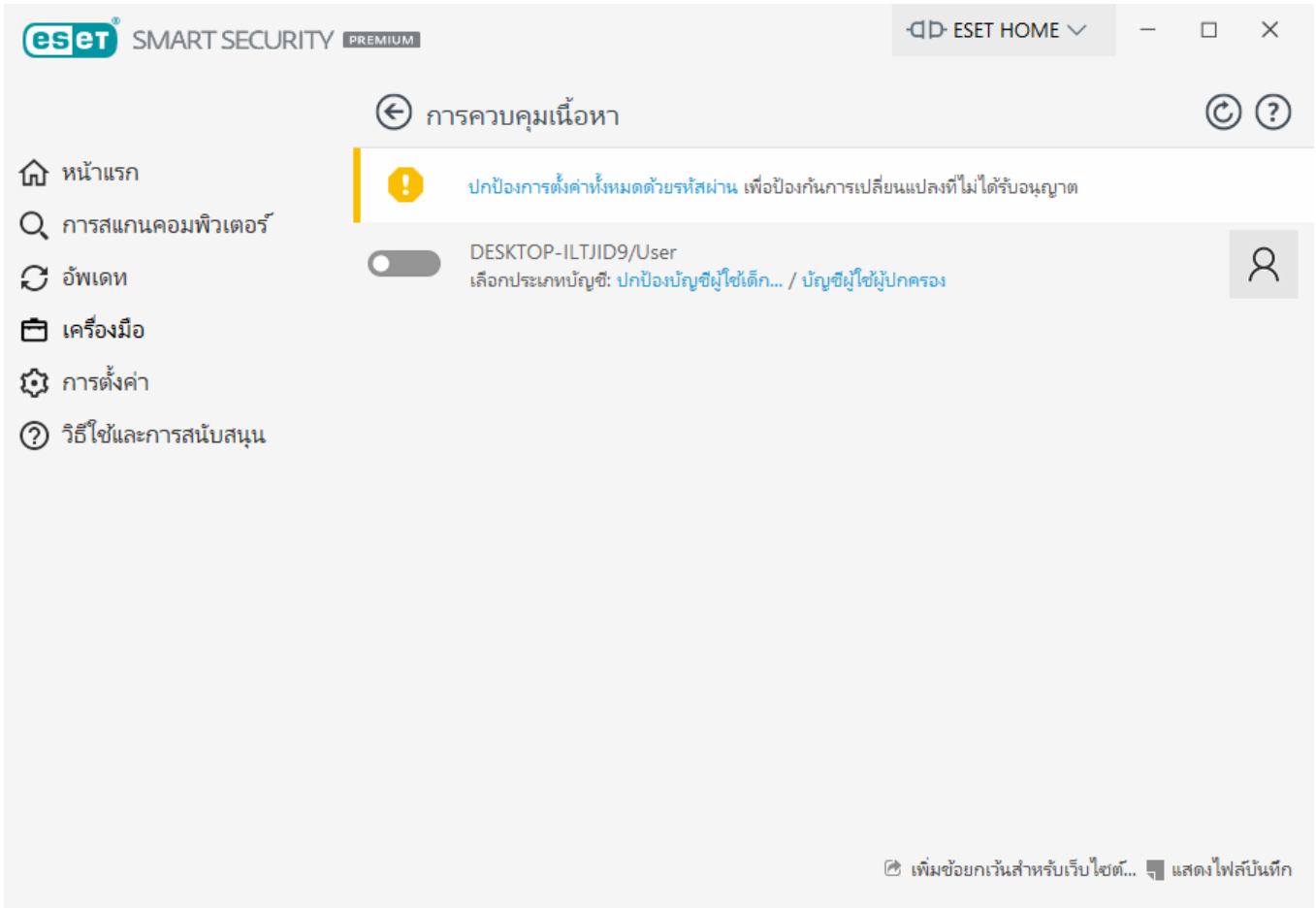
หากต้องการเปิดใช้งานการควบคุมเนื้อหาสำหรับบัญชีผู้ใช้ที่กำหนด โปรดดำเนินการตามขั้นตอนด้านล่างนี้:

1. ตามค่าเริ่มต้น การควบคุมเนื้อหาจะถูกปิดใช้งานใน ESET Smart Security Premium การเปิดใช้งานการควบคุมเนื้อหาสามารถทำได้สองวิธี:

   • คลิก ใน **การตั้งค่า** > **เครื่องมือความปลอดภัย** > **การควบคุมเนื้อหา** จากหน้าต่างโปรแกรมหลักและเปลี่ยนสถานะการควบคุมเนื้อหาเป็น เปิดใช้งาน

   • กด F5 เพื่อเข้าถึงโครงสร้าง **การตั้งค่าขั้นสูง** ไปที่ **เว็บและอีเมล** > **การควบคุมเนื้อหาเว็บไซต์** แล้วเปิดใช้งานแถบเลื่อนถัดจาก **เปิดใช้งานการควบคุมเนื้อหาเว็บไซต์**

2. คลิก **การตั้งค่า** > **เครื่องมือความปลอดภัย** > **การควบคุมเนื้อหาเว็บไซต์** จาก หน้าต่างโปรแกรมหลัก แม้ว่า **เปิดใช้งาน** จะปรากฏข้าง **การควบคุมเนื้อหาเว็บไซต์** คุณก็ต้องกำหนดค่าการควบคุมเนื้อหาเว็บไซต์สำหรับบัญชีที่ต้องการด้วยการคลิกสัญลักษณ์ลูกศร จากนั้นในหน้าต่างถัดไปให้เลือก **ป้องกันบัญชีผู้ใช้เด็ก** หรือ **บัญชีผู้ปกครอง** ในหน้าต่างถัดไป ให้เลือกวันเกิดเพื่อระบุระดับการเข้าถึงและแนะนำหน้าเว็บที่เหมาะสมกับอายุ ขณะนี้การควบคุมเนื้อหาเว็บไซต์จะเปิดใช้งานสำหรับบัญชีผู้ใช้ที่กำหนดแล้ว ให้คลิก **เนื้อหาและการตั้งค่าที่ปิดกั้น** ที่อยู่ใต้ชื่อบัญชีเพื่อปรับแต่งหมวดหมู่ที่คุณต้องการอนุญาตหรือปิดกั้นในแท็บ หมวดหมู่ ในการอนุญาตหรือปิดกั้นหน้าเว็บที่มีหมวดหมู่ไม่ตรงกัน ให้คลิกแท็บ ข้อยกเว้น



หากคุณคลิก **การตั้งค่า** > **เครื่องมือความปลอดภัย** > **การควบคุมเนื้อหา** จากหน้าต่างผลิตภัณฑ์หลักของ ESET Smart Security Premium คุณจะเห็นว่าหน้าต่างหลักมี:

บัญชีผู้ใช้ Windows

หากคุณสร้างบทบาทสำหรับบัญชีที่มีอยู่ บทบาทจะปรากฏที่นี่ คลิกตัวเลื่อน บทบาทจะแสดงเครื่องหมายถูกสีเขียว ถัดจากการควบคุมเนื้อหาสำหรับบัญชี ใต้บัญชีที่ใช้งาน ให้คลิก เนื้อหาและการตั้งค่าที่ปิดกั้น เพื่อดูรายการของหมวดหมู่ของหน้าเว็บที่อนุญาตสำหรับบัญชีนี้และหน้าเว็บที่ถูกปิดกั้นและที่ได้รับอนุญาต

หากต้องการสร้างบัญชีใหม่ (ตัวอย่างเช่น สำหรับเด็ก) ให้ใช้คำแนะนำแบบทีละขั้นตอนต่อไปนี้สำหรับ Windows 7 หรือ Windows Vista:
1.เปิด **บัญชีผู้ใช้** ด้วยการคลิกปุ่ม **Start** (อยู่ด้านซ้ายล่างของเดสก์ท็อป) แล้วคลิก **Control Panel** แล้วคลิก **User Accounts**
2.คลิก **จัดการบัญชีผู้ใช้** ถ้าคุณได้รับข้อความสำหรับรหัสผ่านของผู้ดูแลระบบหรือการยืนยัน ให้พิมพ์รหัสผ่านหรือยืนยันการดำเนินการ
3.คลิก **สร้างบัญชีใหม่**
4.พิมพ์ชื่อที่คุณต้องการสำหรับบัญชีผู้ใช้ คลิกประเภทบัญชี แล้วคลิก **สร้างบัญชี**
5.เปิดช่องการควบคุมเนื้อหาเว็บไซต์ใหม่อีกครั้งโดยคลิกอีกครั้งจาก หน้าต่างโปรแกรมหลัก ของ ESET Smart Security Premium ไปที่ **การตั้งค่า** > **เครื่องมือความปลอดภัย** > **การควบคุมเนื้อหาเว็บไซต์** แล้วคลิกที่สัญลักษณ์ลูกศร

ส่วนล่างของหน้าต่างมี

เพิ่มข้อยกเว้นสำหรับเว็บไซต์ - คุณสามารถอนุญาตหรือปิดกั้นเว็บไซต์บางเว็บไซต์ตามการตั้งค่าของคุณสำหรับบัญชีที่ควบคุมแต่ละบัญชีแยกต่างหากได้

แสดงบันทึก - ส่วนนี้จะแสดงบันทึกโดยละเอียดของกิจกรรมการควบคุมเนื้อหา (หน้าเว็บที่ปิดกั้น บัญชี เหตุผล หมวดหมู่ เป็นต้น) คุณยังสามารถกรองบันทึกนี้ตามเกณฑ์ที่คุณเลือกได้โดยคลิกที่ **การกรอง**

การควบคุมเนื้อหา

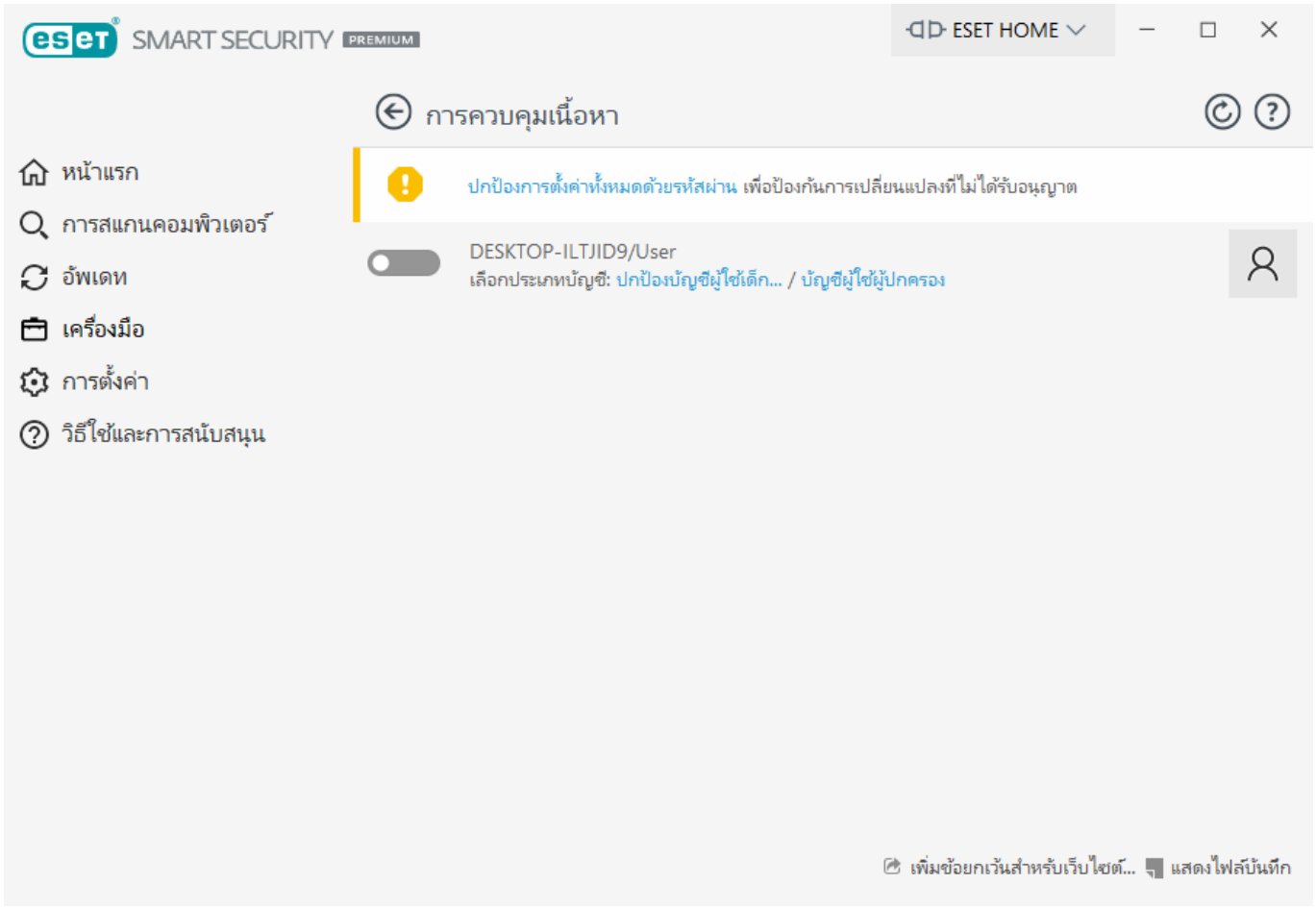
หลังจากที่ปิดใช้งานการควบคุมเนื้อหา หน้าต่าง **ปิดใช้งานการควบคุมเนื้อหา** จะปรากฏขึ้น จากส่วนนี้ คุณสามารถตั้งค่าช่วงเวลาที่จะปิดการป้องกัน ตัวเลือกจะเปลี่ยนเป็น **ที่หยุดชั่วคราว** หรือ **ที่ปิดใช้งานถาวร**

โปรดป้องกันการตั้งค่าใน ESET Smart Security Premium ด้วยรหัสผ่าน คุณสามารถตั้งค่ารหัสผ่านนี้ได้ในส่วน ตั้งค่าการเข้าถึง หากไม่ได้ตั้งรหัสผ่าน คำเตือนต่อไปนี้จะปรากฏขึ้น – **ป้องกันการตั้งค่าทั้งหมดด้วยรหัสผ่าน** เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต การจำกัดที่ตั้งค่าในการควบคุมเนื้อหาจะมีผลเฉพาะบัญชีผู้ใช้มาตรฐาน เนื่องจากผู้ดูแลระบบสามารถเขียนทับการจำกัดใดๆ ได้ จึงไม่มีผลแต่อย่างใด

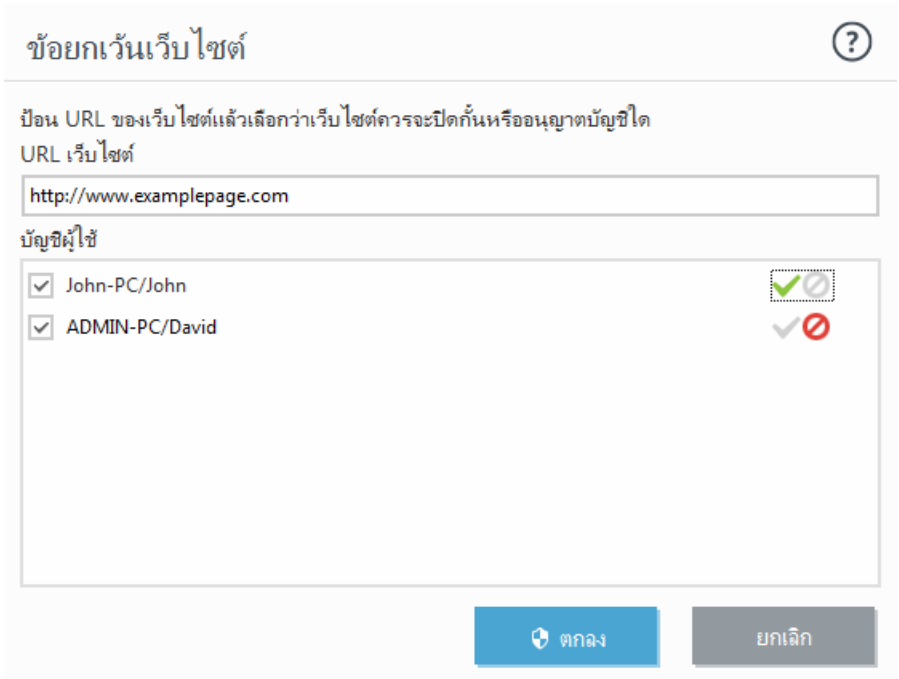
> i การควบคุมเนื้อหากำหนดให้มีการเปิดใช้งาน การกรองเนื้อหาของโปรโตคอลแอพพลิเคชัน, การตรวจสอบโปรโตคอล HTTP และ ไฟร์วอลล์ส่วนบุคคล เพื่อให้สามารถทำงานได้อย่างถูกต้อง ฟังก์ชันทั้งหมดนี้จะเปิดใช้งานเป็นค่าเริ่มต้น

ข้อยกเว้นเว็บไซต์

เพื่อเพิ่มข้อยกเว้นสำหรับเว็บไซต์ ให้คลิก **การตั้งค่า** > **เครื่องมือรักษาความปลอดภัย** > **การควบคุมเนื้อหา** จากนั้น คลิก **เพิ่มข้อยกเว้นสำหรับเว็บไซต์**

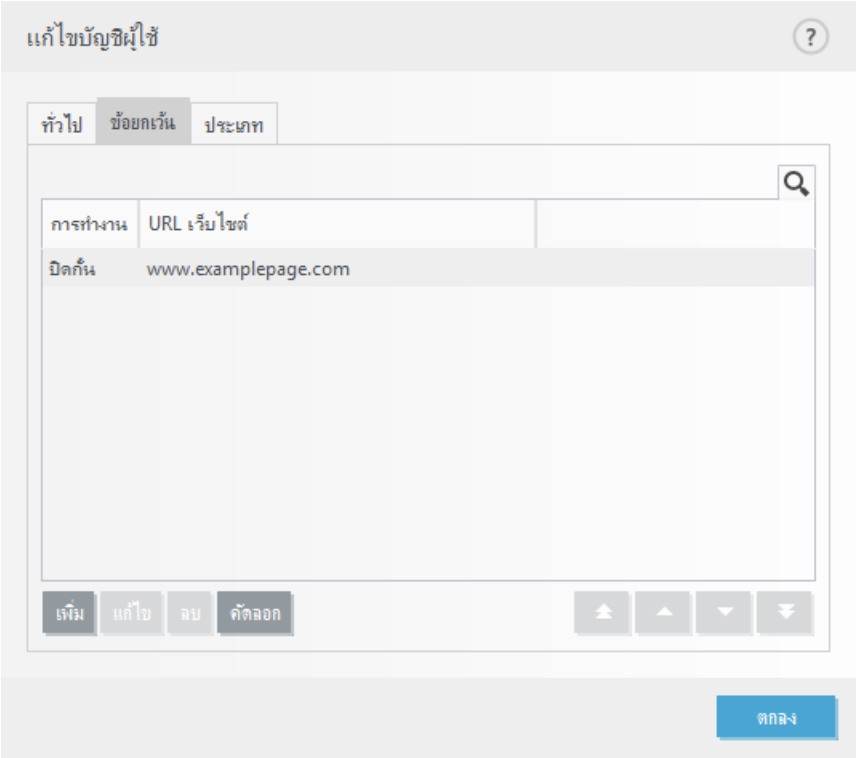


ป้อน URL ในช่อง **URL เว็บไซต์** แล้วเลือก ✔ (อนุญาต) หรือ ⊘ (ปิดกั้น) สำหรับบัญชีผู้ใช้รายใดรายหนึ่ง จากนั้นคลิก **ตกลง** เพื่อเพิ่มบัญชีนั้นไปยังรายการ



ในการลบที่อยู่ URL จากรายการ ให้คลิก **การตั้งค่า** > **เครื่องมือความปลอดภัย** > **การควบคุมเนื้อหา** > คลิก **เนื้อหาและการตั้งค่าที่ปิดกั้น** ด้านล่างบัญชีผู้ใช้ที่ต้องการ จากนั้นคลิกแท็บ**ข้อยกเว้น** เลือกข้อยกเว้นแล้วคลิก

ลบออก



ในรายการที่อยู่ URL จะไม่สามารถใช้สัญลักษณ์พิเศษ * (ดอกจัน) และ ? (เครื่องหมายคำถาม) ได้ ตัวอย่างเช่น จะต้องทำการป้อนที่อยู่หน้าเว็บที่มีหลาย TLD ด้วยตัวเอง (*examplepage.com*, *examplepage.sk*, ฯลฯ) เมื่อคุณเพิ่มโดเมนลงในรายการ เนื้อหาทั้งหมดที่อยู่บนโดเมนนี้และโดเมนย่อยทั้งหมด (ตัวอย่างเช่น sub.examplepage.com*sub.examplepage.com*) จะถูกปิดกั้นหรืออนุญาตตามการเลือกการทำงานตาม URL ของคุณ

i การปิดกั้นหรือการอนุญาตหน้าเว็บจะมีความแม่นยำมากกว่าการปิดกั้นหรือการอนุญาตหมวดหมู่ของหน้าเว็บ โปรดระมัดระวังเมื่อเปลี่ยนการตั้งค่าเหล่านี้ และเพิ่มประเภท/หน้าเว็บในรายการ

บัญชีผู้ใช้

การตั้งค่านี้มีให้ใช้งานใน **การตั้งค่าขั้นสูง** (F5) > **เว็บและอีเมล** > **การควบคุมเนื้อหาเว็บไซต์** > **บัญชีผู้ใช้** > **แก้ไข**

ในส่วนนี้ คุณจะสามารถเชื่อมโยงบัญชีผู้ใช้ Windows ที่ใช้งานโดยการควบคุมเนื้อหากับผู้ใช้บางรายเพื่อกำจัดความสามารถในการเข้าถึงเนื้อหาที่ไม่เหมาะสมหรือเป็นอันตรายในอินเทอร์เน็ตของพวกเขา

คอลัมน์

บัญชี Windows - ชื่อของผู้ใช้

เปิดใช้งานแล้ว - เมื่อเปิดใช้งาน การควบคุมเนื้อหาสำหรับผู้ใช้บางรายจะเปิดใช้งาน

โดเมน - ชื่อของโดเมนที่ผู้ใช้อยู่

วันเกิด - อายุของผู้ใช้ที่บัญชีนี้

องค์ประกอบการควบคุม

เพิ่ม - ข้อความ การทำงานกับบัญชีผู้ใช้ จะปรากฏขึ้น

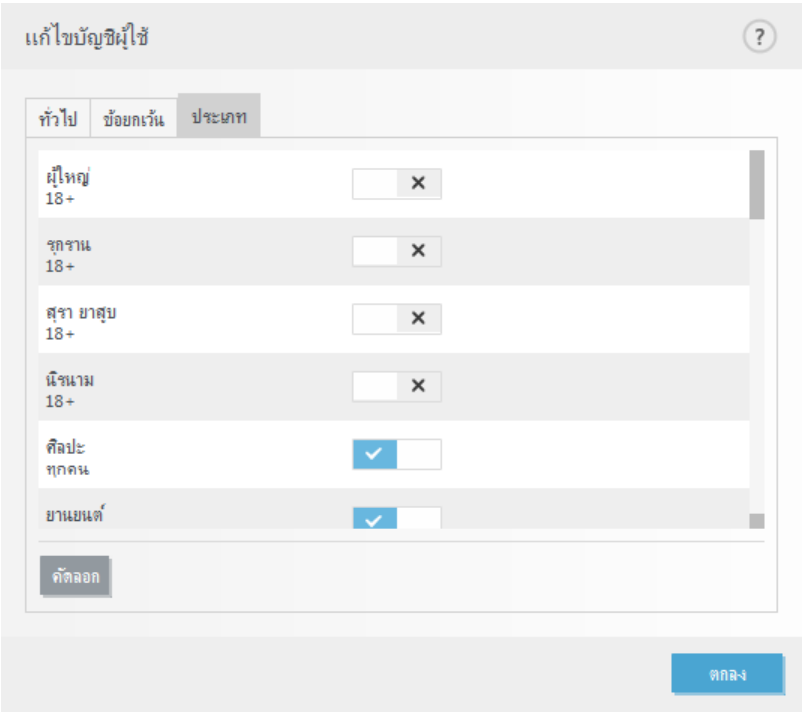
แก้ไข - ตัวเลือกนี้จะช่วยให้คุณแก้ไขบัญชีที่เลือก

ลบออก - ลบบัญชีที่เลือกออก

รีเฟรช - หากคุณเพิ่มบัญชีผู้ใช้ ESET Smart Security Premium สามารถรีเฟรชรายการของบัญชีผู้ใช้ได้โดยไม่จำเป็นต้องเปิดหน้าต่างนี้อีกครั้ง

ประเภท

ตรวจสอบช่องทำเครื่องหมายในคอลัมน์ **เปิดใช้งานแล้ว** ถัดจากประเภทเพื่ออนุญาตรายการดังกล่าว หากคุณไม่ทำเครื่องหมายช่อง ระบบจะไม่อนุญาตรายการประเภทสำหรับบัญชีนี้



ตัวอย่างของประเภท (กลุ่ม) ที่ผู้ใช้อาจไม่คุ้นเคยได้แก่:

• **เบ็ดเตล็ด** - มักเป็นที่อยู่ IP ส่วนบุคคล (ในระบบ) เช่น อินทราเน็ต, 127.0.0.0/8, 192.168.0.0/16 เป็นต้น เมื่อคุณได้รับรหัสข้อผิดพลาด 403 หรือ 404 เว็บไซต์จะจับคู่ประเภทนี้ด้วย

• **ไม่แปลค่า** - ประเภทนี้ประกอบด้วยหน้าเว็บที่ไม่มีการแปลค่า เนื่องจากเกิดข้อผิดพลาดในขณะเชื่อมต่อกับกลไกฐานข้อมูลการควบคุมเนื้อหา

• **ไม่ได้จัดประเภท** - หน้าเว็บที่ไม่รู้จักซึ่งยังไม่อยู่ในฐานข้อมูลการควบคุมเนื้อหา

• **ไดนามิค** – หน้าเว็บที่จะเปลี่ยนเส้นทางไปที่หน้าในเว็บอื่น

ทำงานกับบัญชีผู้ใช้

หน้าต่างนี้มีสามแท็บ ดังนี้:

ทั่วไป

คลิกแถบเลื่อนถัดจาก **เปิดใช้งาน** เพื่อเปิดการควบคุมเนื้อหาเว็บไซต์สำหรับบัญชี Windows ที่เลือกไว้ด้านล่าง

เลือก บัญชี Windows จากคอมพิวเตอร์ การจำกัดที่ตั้งค่าไว้ในการควบคุมเนื้อหาจะมีผลเฉพาะกับบัญชี Windows มาตรฐานเท่านั้น บัญชีผู้ดูแลระบบสามารถเขียนทับข้อจำกัดได้

หากบัญชีถูกใช้โดยผู้ปกครองเท่านั้น ให้เลือก **บัญชีผู้ปกครอง**

ตั้งค่า **วันเกิดของเด็ก** สำหรับบัญชีเพื่อกำหนดระดับการเข้าถึงและตั้งกฎการเข้าถึงสำหรับหน้าเว็บที่เหมาะสมกับวัย

ความละเอียดของการบันทึก

ESET Smart Security Premium จะบันทึกเหตุการณ์สำคัญทั้งหมดไว้ในไฟล์บันทึก ซึ่งจะสามารถดูได้โดยตรงจากเมนูหลัก คลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก** จากนั้นเลือก**การควบคุมเนื้อหาเว็บไซต์** จาก **บันทึก** ในเมนูแบบเลื่อนลง

• **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม

• **ข้อมูล** – บันทึกข้อความแจ้งข้อมูล รวมถึงข้อยกเว้นที่บล็อกแล้วและอนุญาตแล้ว รวมถึงบันทึกทั้งหมดข้างต้น

- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน
- **ไม่มี** – จะไม่มีการบันทึกใดๆ

ข้อยกเว้น

การสร้างข้อยกเว้นสามารถอนุญาตหรือปฏิเสธผู้ใช้ไม่ให้เข้าถึงเว็บไซต์ที่ไม่ได้อยู่ในรายการข้อยกเว้นได้ สิ่งนี้เป็นประโยชน์หากคุณต้องการควบคุมการเข้าถึงเว็บไซต์บางเว็บไซต์แทนการใช้หมวดหมู่ ข้อยกเว้นที่สร้างสำหรับบัญชีหนึ่งบัญชีสามารถคัดลอกและใช้กับบัญชีอื่นได้ สิ่งนี้อาจเป็นประโยชน์เมื่อคุณต้องการสร้างกฎที่เหมือนกันสำหรับเด็กที่มีอายุใกล้เคียงกัน

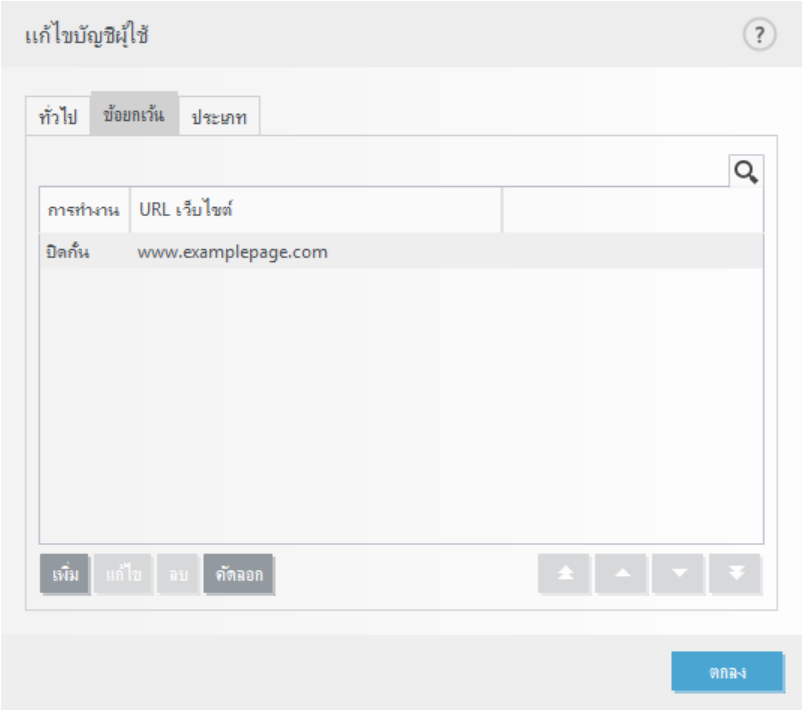
คลิกที่ **เพิ่ม** เพื่อสร้างข้อยกเว้นใหม่ ระบุ **การดำเนินการ** (ตัวอย่างเช่น **ปิดกั้น**) โดยใช้เมนูแบบเลื่อนลง ป้อน **URL เว็บไซต์** ที่ใช้ขอยกเว้นนี้ จากนั้นคลิก **ตกลง** ข้อยกเว้นจะถูกเพิ่มลงในรายการข้อยกเว้นที่มีอยู่พร้อมแสดงสถานะ

เพิ่ม - สร้างข้อยกเว้นใหม่

แก้ไข - คุณสามารถแก้ไข **URL เว็บไซต์** หรือ **การดำเนินการ** ของข้อยกเว้นที่เลือกได้

ลบ - ลบข้อยกเว้นที่เลือกออก

คัดลอก - เลือกผู้ใช้จากเมนูแบบเลื่อนลงจากรายการที่คุณต้องการคัดลอกข้อยกเว้นที่สร้างขึ้น



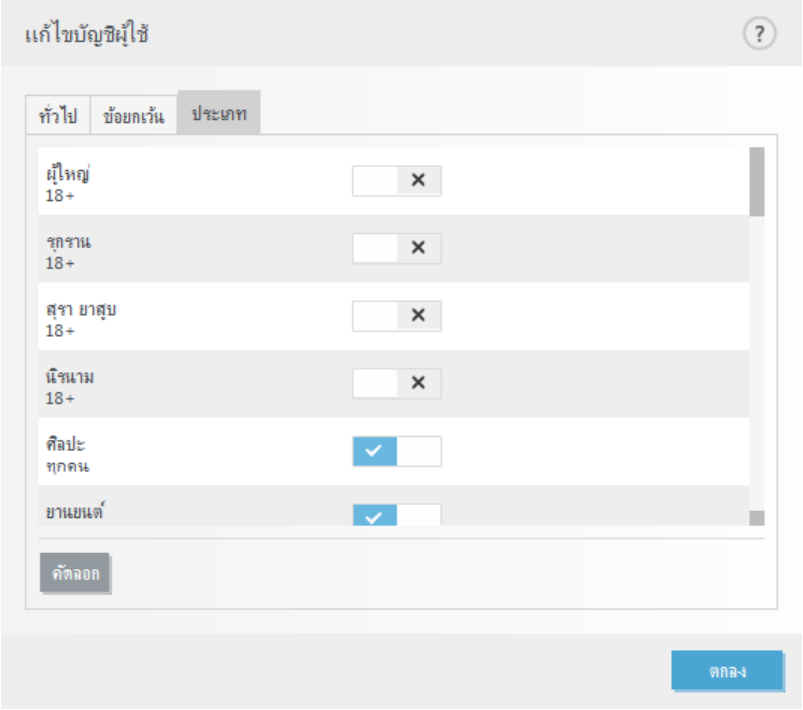
ข้อยกเว้นที่กำหนดจะเขียนทับหมวดหมู่ที่กำหนดไว้สำหรับบัญชีที่เลือก ตัวอย่างเช่น หากบัญชีปิดกั้นหมวดหมู่

ใหม่ แต่คุณได้กำหนดให้หน้าเว็บใหม่เป็นข้อยกเว้นที่ได้รับอนุญาต บัญชีจะสามารถเข้าถึงหน้าเว็บที่อนุญาตได้ คุณสามารถดูการเปลี่ยนแปลงใดๆ ที่ได้ทำไว้ในส่วน ข้อยกเว้น ได้

ประเภท

ในแท็บ **หมวดหมู่** คุณสามารถกำหนดหมวดหมู่ทั่วไปของเว็บไซต์ที่คุณต้องการปิดกั้นหรืออนุญาตสำหรับแต่ละบัญชีได้ เลือกกล่องทำเครื่องหมายที่อยู่ถัดจากหมวดหมู่เพื่ออนุญาตหมวดหมู่นั้น หากคุณไม่เลือกกล่องทำเครื่องหมาย หมวดหมู่จะไม่ได้รับอนุญาตสำหรับบัญชีดังกล่าว

คัดลอก - ให้คุณคัดลอกรายการของหมวดหมู่ที่ปิดกั้นหรืออนุญาตจากบัญชีที่แก้ไขที่มีอยู่



คัดลอกข้อยกเว้นจากผู้ใช้

เลือกผู้ใช้จากเมนูแบบเลื่อนลงจากอันที่คุณต้องการคัดลอกข้อยกเว้นที่สร้างขึ้น

คัดลอกประเภทจากบัญชี

ให้คุณคัดลอกรายการของหมวดหมู่ที่ปิดกั้นหรืออนุญาตจากบัญชีที่แก้ไขที่มีอยู่

เปิดใช้งานการควบคุมเนื้อหา

ตัวเลือก **เปิดใช้งานการควบคุมเนื้อหาเว็บไซต์** รวมการควบคุมเนื้อหาเว็บไซต์ไว้ใน ESET Smart Security Premium ส่วน การควบคุมเนื้อหาเว็บไซต์ ในหน้าต่างหลักภายใต้ **การตั้งค่า** > **เครื่องมือความปลอดภัย** > **การควบคุมเนื้อหาเว็บไซต์** จะแสดงขึ้น

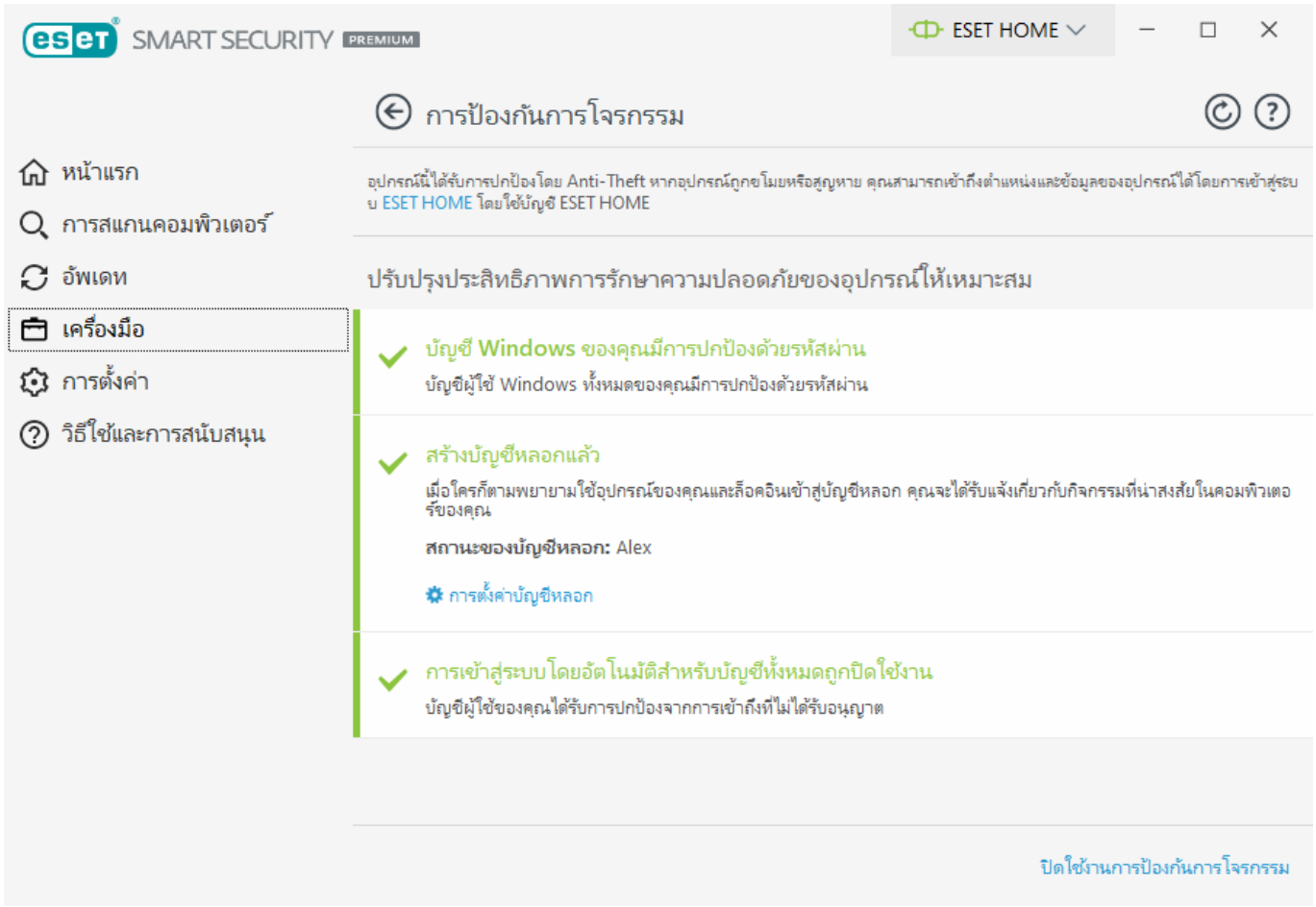
การป้องกันการโจรกรรม

ในระหว่างที่เราเดินทางในชีวิตประจำวันจากที่บ้านไปที่ทำงาน หรือไปยังสถานที่สาธารณะอื่นๆ อุปกรณ์ส่วนบุคคลของเราจะมีความเสี่ยงต่อการสูญหายหรือถูกขโมยอยู่ตลอดเวลา การป้องกันการโจรกรรม เป็นคุณลักษณะที่ขยายการรักษาความปลอดภัยในระดับผู้ใช้ที่ครอบคลุมถึงกรณีอุปกรณ์สูญหายหรือถูกขโมย โดย การป้องกันการโจรกรรม ช่วยให้คุณสามารถตรวจสอบการใช้อุปกรณ์และติดตามอุปกรณ์ที่สูญหายได้โดยใช้การบอกตำแหน่งตามที่อยู่ IP ใน ESET HOME ซึ่งวิธีนี้จะช่วยให้คุณได้อุปกรณ์กลับคืนมาและช่วยปกป้องข้อมูลส่วนบุคคลของคุณได้

การใช้เทคโนโลยีที่ทันสมัย เช่น การค้นหาที่อยู่ IP ตามตำแหน่งทางภูมิศาสตร์ การบันทึกภาพจากกล้องทางเว็บ การป้องกันบัญชีผู้ใช้ และการตรวจสอบอุปกรณ์ การป้องกันการโจรกรรม อาจช่วยเหลือคุณและหน่วยงานผู้รักษากฎหมายในการค้นหาคอมพิวเตอร์หรืออุปกรณ์ของคุณ หากเกิดการสูญหายหรือถูกโจรกรรม ใน ESET HOME คุณสามารถดูกิจกรรมที่เกิดขึ้นในคอมพิวเตอร์หรืออุปกรณ์ของคุณได้

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับ การป้องกันการโจรกรรม ใน ESET HOME โปรดดูวิธีใช้ออนไลน์ของ ESET HOME

หลังจากที่คุณเปิดใช้งาน การป้องกันการโจรกรรม คุณสามารถปรับปรุงประสิทธิภาพการรักษาความปลอดภัยของอุปกรณ์ให้เหมาะสมได้ในหน้าต่างโปรแกรมหลัก > **เครื่องมือ** > **การป้องกันการโจรกรรม**



ตัวเลือกการปรับให้เหมาะสม

ไม่มีบัญชีหลอกที่สร้าง

การสร้างบัญชีหลอกจะเพิ่มโอกาสในการค้นพบตำแหน่งของอุปกรณ์ที่สูญหายหรือถูกขโมย หากคุณทำเครื่องหมายอุปกรณ์ของคุณเป็นสูญหาย การป้องกันการโจรกรรม จะบล็อกการเข้าถึงบัญชีผู้ใช้ที่ใช้งานอยู่เพื่อปกป้องข้อมูลสำคัญของคุณ ใครก็ตามที่พยายามจะใช้อุปกรณ์เครื่องนั้นจะได้รับอนุญาตให้ใช้เฉพาะบัญชีหลอก บัญชีหลอกคือรูปแบบหนึ่งของบัญชีผู้เยี่ยมชมที่มีสิทธิ์จำกัด บัญชีดังกล่าวจะถูกใช้เป็นบัญชีระบบเริ่มต้นจนกว่าอุปกรณ์ของคุณจะถูกทำเครื่องหมายว่าได้คืนแล้ว เพื่อป้องกันไม่ให้บุคคลอื่นเข้าสู่ระบบบัญชีผู้ใช้อื่นๆ หรือเข้าถึงข้อมูลของผู้ใช้ได้

> เมื่อใดก็ตามที่มีคนล็อกอินเข้าสู่บัญชีหลอกเมื่อคอมพิวเตอร์ของคุณอยู่ในสภาวะปกติ คุณจะได้รับอีเมลแจ้งเตือนพร้อมข้อมูลเกี่ยวกับกิจกรรมที่น่าสงสัยในคอมพิวเตอร์ของคุณ หลังจากได้รับการแจ้งเตือนทางอีเมลแล้ว คุณสามารถตัดสินใจได้ว่าต้องการทำเครื่องหมายคอมพิวเตอร์เป็นสูญหายหรือไม่

หากต้องการสร้างบัญชีหลอก ให้คลิก **สร้างบัญชีหลอก** จากนั้นป้อน**ชื่อบัญชีหลอก**ลงในช่องข้อความแล้วคลิก **สร้าง**

เมื่อสร้างบัญชีหลอกไว้แล้ว คุณจะคลิก **การตั้งค่าบัญชีหลอก** เพื่อเปลี่ยนชื่อหรือลบบัญชีได้

การป้องกันบัญชี Windows ด้วยรหัสผ่าน

บัญชีผู้ใช้ของคุณไม่ได้รับการป้องกันด้วยรหัสผ่าน คุณจะได้รับคำเตือนการปรับให้เหมาะสมนี้หากบัญชีผู้ใช้อย่างน้อยหนึ่งบัญชีไม่ได้รับการป้องกันด้วยรหัสผ่าน การสร้างรหัสผ่านสำหรับผู้ใช้ทั้งหมด (ยกเว้น**บัญชีหลอก**) บนคอมพิวเตอร์จะแก้ปัญหานี้ได้

หากต้องการสร้างรหัสผ่านสำหรับบัญชีผู้ใช้ ให้คลิก **จัดการบัญชี Windows** แล้วเปลี่ยนรหัสผ่านหรือทำตามคำแนะนำด้านล่าง:

1. กด CTRL+Alt+Delete บนแป้นพิมพ์
2. คลิก **เปลี่ยนรหัสผ่าน**
3. เว้นช่อง **รหัสผ่านเดิม** ให้ว่างไว้
4. ป้อนรหัสผ่านลงในช่อง **รหัสผ่านใหม่** และช่อง **ยืนยันรหัสผ่าน** แล้วกด **Enter**

การเข้าสู่ระบบโดยอัตโนมัติสำหรับบัญชี Windows

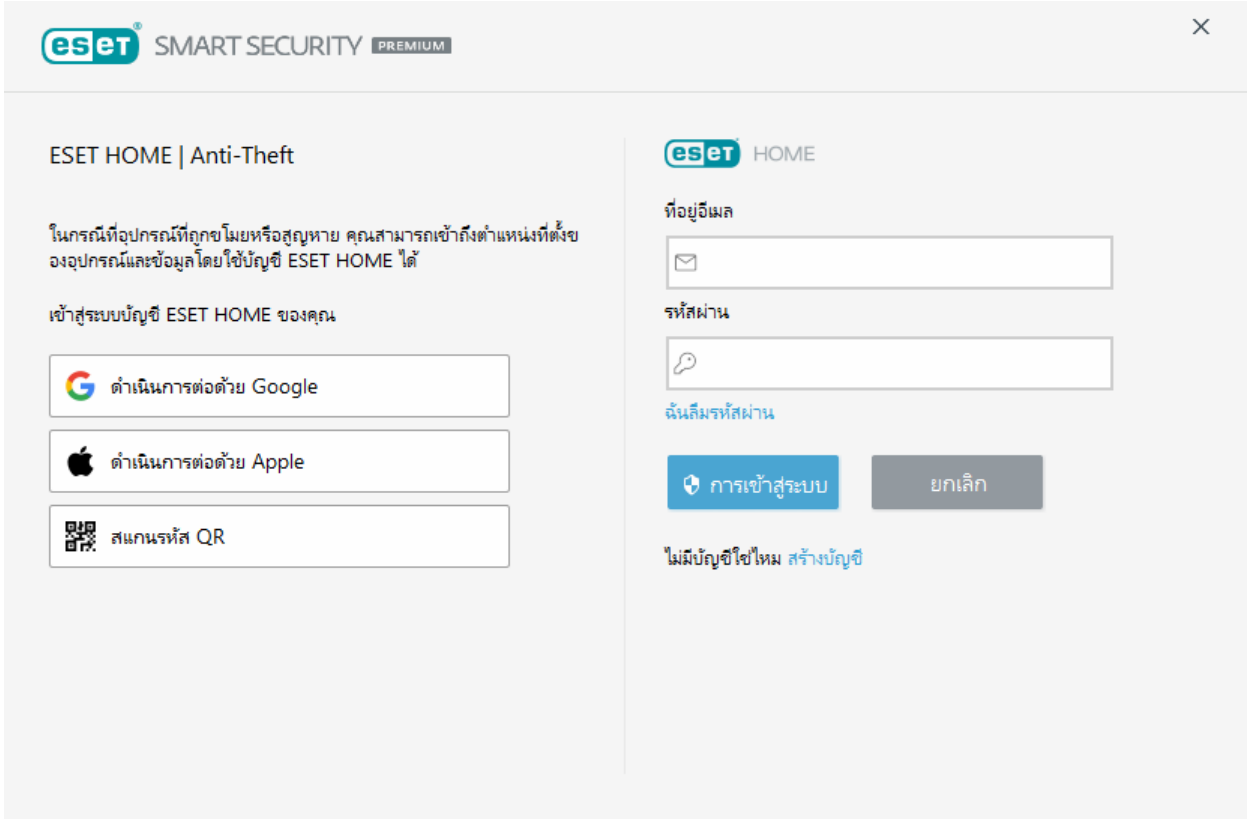
บัญชีผู้ใช้ของคุณเปิดใช้งานการเข้าสู่ระบบโดยอัตโนมัติอยู่ ดังนั้นจึงไม่ได้รับการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต คุณจะได้รับคำเตือนการปรับให้เหมาะสมนี้หากบัญชีผู้ใช้อย่างน้อยหนึ่งบัญชีเปิดใช้งานการเข้าสู่ระบบโดยอัตโนมัติอยู่ คลิก **ปิดใช้งานการเข้าสู่ระบบโดยอัตโนมัติ** เพื่อแก้ไขปัญหาการปรับให้เหมาะสมนี้

การเข้าสู่ระบบโดยอัตโนมัติสำหรับบัญชีหลอก

การเข้าสู่ระบบโดยอัตโนมัติสำหรับ**บัญชีหลอก**บนอุปกรณ์ของคุณเปิดใช้งานอยู่ เมื่ออุปกรณ์อยู่ในสถานะปกติ เราไม่แนะนำให้คุณใช้การเข้าสู่ระบบโดยอัตโนมัติ เพราะอาจทำให้เกิดปัญหาในการเข้าถึงบัญชีผู้ใช้จริง หรือมีการส่งการเตือนที่ผิดพลาดเกี่ยวกับสถานะสูญหายของคอมพิวเตอร์ของคุณ คลิก **ปิดใช้งานการเข้าสู่ระบบโดยอัตโนมัติ** เพื่อแก้ไขปัญหาการปรับให้เหมาะสมนี้

ล็อคอินเข้าสู่บัญชี ESET HOME ของคุณ

หากต้องการเปิดใช้งาน/ปิดใช้งาน การป้องกันการโจรกรรม และเข้าถึงตำแหน่งและข้อมูลของอุปกรณ์ใน ESET HOME ให้ล็อคอินเข้าสู่บัญชี ESET HOME ของคุณ



คุณสามารถล็อคอินเข้าสู่บัญชี ESET HOME ของคุณ ได้หลายวิธีดังนี้:

• **ใช้ที่อยู่อีเมล ESET HOME และรหัสผ่านของคุณ** – พิมพ์ **ที่อยู่อีเมล** และ **รหัสผ่าน** ที่คุณใช้สร้างบัญชี ESET HOME แล้วคลิก **ล็อคอิน**

• **ใช้บัญชี Google/AppleID** – คลิก **ดำเนินการต่อด้วย Google** หรือ **ดำเนินการต่อด้วย Apple** แล้วล็อคอินด้วยบัญชีที่ถูกต้อง หลังจากล็อคอินได้สำเร็จระบบจะเปลี่ยนเส้นทางคุณไปยังหน้าเว็บยืนยันของ ESET HOME หากต้องการดำเนินการต่อให้สลับกลับไปยังหน้าต่างผลิตภัณฑ์ ESET ของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการล็อคอินด้วยบัญชี Google /AppleID โปรดดูคำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME

• **สแกนรหัส QR** – คลิก **สแกนรหัส QR** เพื่อแสดงรหัส QR โปรดเปิดแอพโทรศัพท์มือถือ ESET HOME แล้วสแกนรหัส QR หรือหันกล้องบนอุปกรณ์ของคุณไปที่รหัส QR สำหรับข้อมูลเพิ่มเติม โปรดดูคำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME

⚠ ล็อคอินล้มเหลว - ข้อผิดพลาดทั่วไป

i หากคุณไม่มีบัญชี ESET HOME ให้คลิก **สร้างบัญชี** เพื่อลงทะเบียนหรือดูคำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME
หากคุณลืมรหัสผ่าน ให้คลิก **ฉันลืมรหัสผ่าน** และทำตามขั้นตอนบนหน้าจอหรือดู คำแนะนำใน ความช่วยเหลือออนไลน์ ESET HOME

i การป้องกันการโจรกรรม ไม่รองรับการทำงานของ Microsoft Windows Home Server

ตั้งค่าชื่ออุปกรณ์

ช่อง **ชื่ออุปกรณ์** คือช่องที่แสดงชื่อคอมพิวเตอร์ (อุปกรณ์) ของคุณที่จะแสดงเป็นตัวระบุในบริการ ESET HOME ทั้งหมด ชื่อคอมพิวเตอร์ของคอมพิวเตอร์ของคุณจะถูกใช้เป็นค่าเริ่มต้น ป้อนชื่ออุปกรณ์หรือใช้ชื่อเริ่มต้นแล้วคลิก **ดำเนินการต่อ**

การป้องกันการโจรกรรม เปิดใช้งานอยู่/ปิดใช้งานอยู่

หน้าต่างนี้มีข้อความการยืนยันเมื่อคุณเปิดใช้งาน/ปิดใช้งาน การป้องกันการโจรกรรม:

• เปิดใช้งานอยู่ – อุปกรณ์ของคุณได้รับการปกป้องโดย การป้องกันการโจรกรรม แล้ว และคุณสามารถจัดการความปลอดภัยของคุณลักษณะนี้จากระยะไกลได้ในพอร์ทัล ESET HOME โดยใช้บัญชีของคุณ

• ปิดใช้งานอยู่ – การป้องกันการโจรกรรม ปิดใช้งานอยู่บนอุปกรณ์นี้ และข้อมูลทั้งหมดที่เกี่ยวข้องกับ <%ESET_ANTTHEFT%> สำหรับอุปกรณ์นี้จะถูกลบออกจากพอร์ทัล ESET HOME

การเพิ่มอุปกรณ์ใหม่ล้มเหลว

คุณได้รับข้อผิดพลาดในขณะเปิดใช้งาน การป้องกันการโจรกรรม

สถานการณ์ที่พบมากที่สุดคือ:

• เกิดข้อผิดพลาดในการเข้าสู่ระบบ ESET HOME

• ไม่มีการเชื่อมต่ออินเทอร์เน็ต (หรืออินเทอร์เน็ตไม่ทำงานในขณะนี้)

หากคุณไม่สามารถแก้ไขปัญหาได้ โปรดติดต่อติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET

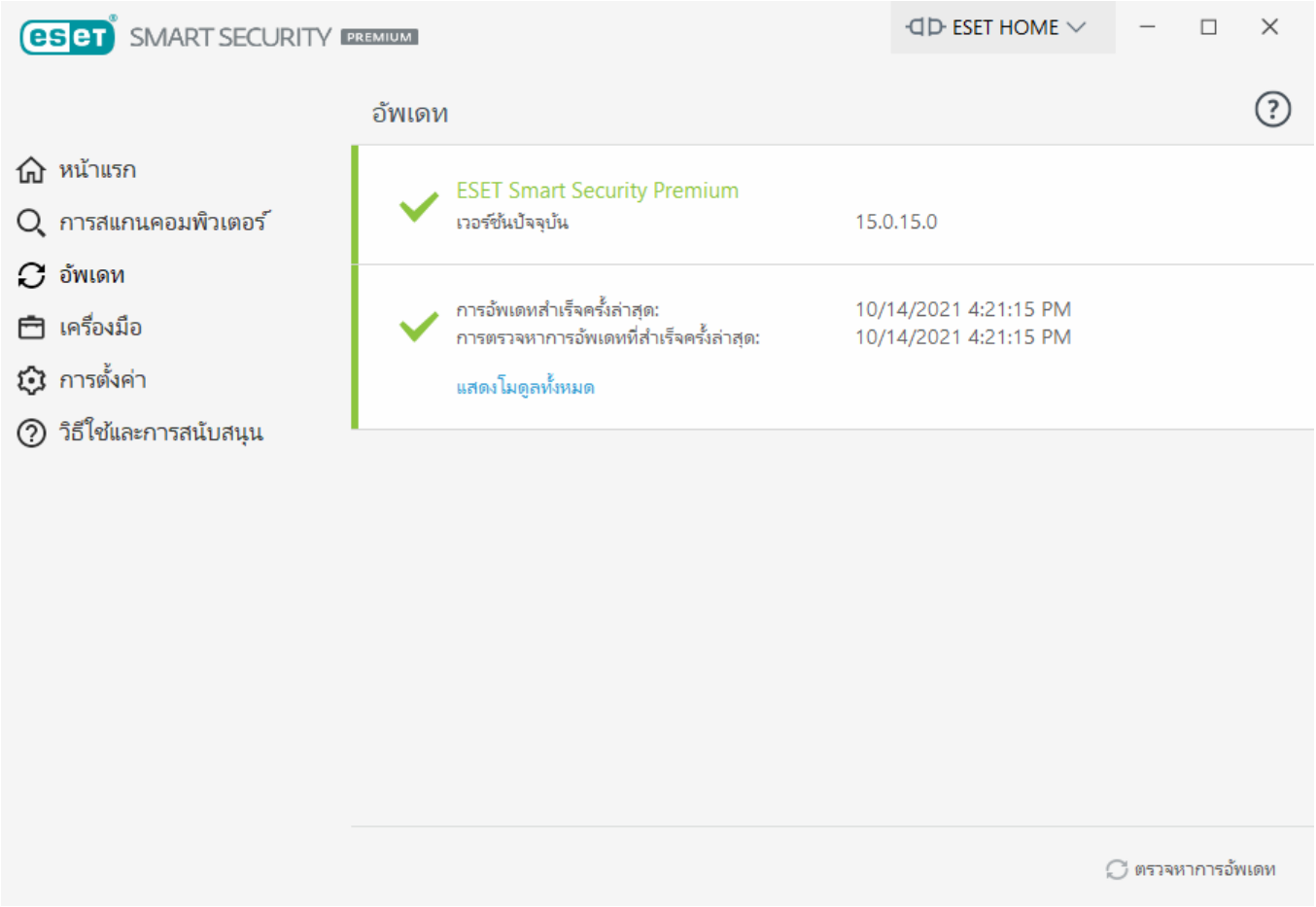
การอัพเดทโปรแกรม

การอัพเดท ESET Smart Security Premium เป็นประจำเป็นวิธีการที่ดีที่สุดเพื่อให้มั่นใจว่าคอมพิวเตอร์มีระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัพเดทจะช่วยให้มั่นใจได้ว่าทั้งโมดูลโปรแกรมและส่วนประกอบของระบบจะอัพเดทอยู่เสมอ

เมื่อคลิก **อัพเดท** ในหน้าต่างโปรแกรมหลัก คุณสามารถดูสถานะการอัพเดทในปัจจุบัน รวมถึงวันที่และเวลาของการอัพเดทที่สำเร็จครั้งล่าสุด และดูว่าจะต้องมีการอัพเดทหรือไม่ได้

นอกเหนือจากการอัพเดทอัตโนมัติแล้ว คุณยังสามารถคลิก **ตรวจหาการอัพเดท** เพื่อเรียกใช้การอัพเดทด้วยตนเองได้ การอัพเดทโมดูลและส่วนประกอบของโปรแกรมอย่างสม่ำเสมอเป็นสิ่งที่สำคัญในการรักษาการปกป้องอย่างแบบเต็มรูปแบบจากรหัสที่เป็นอันตราย โปรดให้ความสนใจในการกำหนดค่าและการทำงานของโปรแกรม คุณต้องเปิดใช้งานผลิตภัณฑ์ของคุณโดยใช้รหัสใบอนุญาตเพื่อรับการอัพเดท หากคุณไม่ได้อัพเดทในระหว่างการติดตั้ง คุณสามารถป้อนรหัสใบอนุญาตเพื่อเปิดใช้งานผลิตภัณฑ์ของคุณเมื่ออัพเดทเพื่อเข้าถึงเซิร์ฟเวอร์อัพเดทของ ESET ได้

รหัสใบอนุญาตจะถูกส่งเป็นอีเมลจาก ESET ไปหาคุณหลังทำการซื้อ ESET Smart Security Premium



เวอร์ชันปัจจุบัน – แสดงหมายเลขเวอร์ชันของผลิตภัณฑ์เวอร์ชันปัจจุบันที่คุณได้ติดตั้ง

การอัพเดทสำเร็จครั้งล่าสุด – แสดงวันที่อัพเดทสำเร็จครั้งล่าสุด หากคุณไม่พบวันที่ล่าสุด แสดงว่าโมดูลผลิตภัณฑ์ของคุณอาจไม่ใช่โมดูลปัจจุบัน

ตรวจหาการอัพเดทสำเร็จครั้งล่าสุด – แสดงวันที่ตรวจหาการอัพเดทสำเร็จครั้งล่าสุด

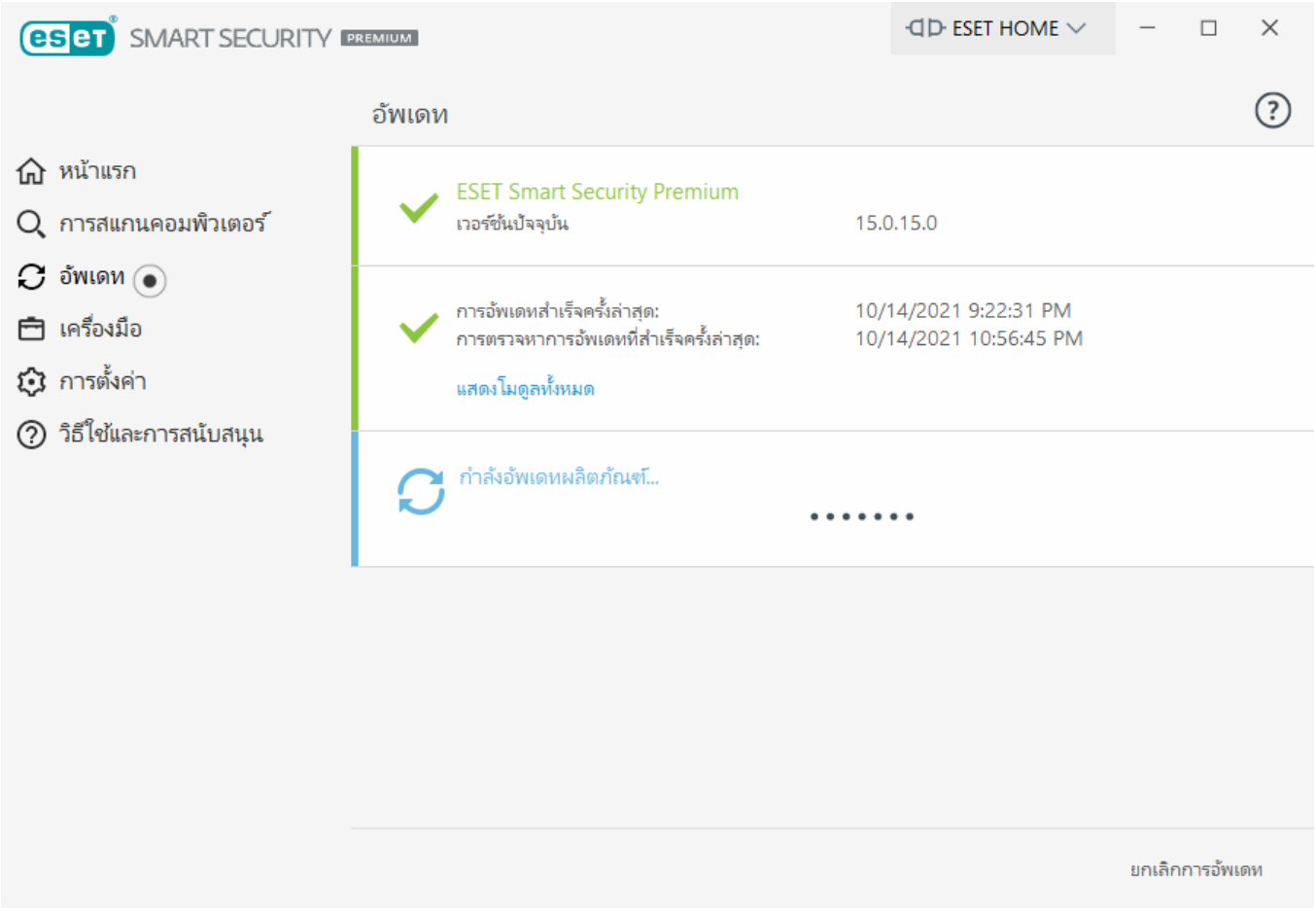
แสดงโมดูลทั้งหมด – แสดงรายการโมดูลโปรแกรมที่ติดตั้งแล้ว

คลิก **ตรวจสอบการอัพเดท** เพื่อตรวจหาเวอร์ชันล่าสุดที่ใช้ได้ของ ESET Smart Security Premium

---

กระบวนการอัพเดท

หลังจากคลิก **ตรวจหาการอัพเดท** การดาวน์โหลดจะเริ่มต้นทำงาน แถบแสดงความคืบหน้าการดาวน์โหลดและเวลาที่เหลือสำหรับการดาวน์โหลดจะปรากฏขึ้น เมื่อต้องการขัดจังหวะการอัพเดท ให้คลิก **ยกเลิกการอัพเดท**



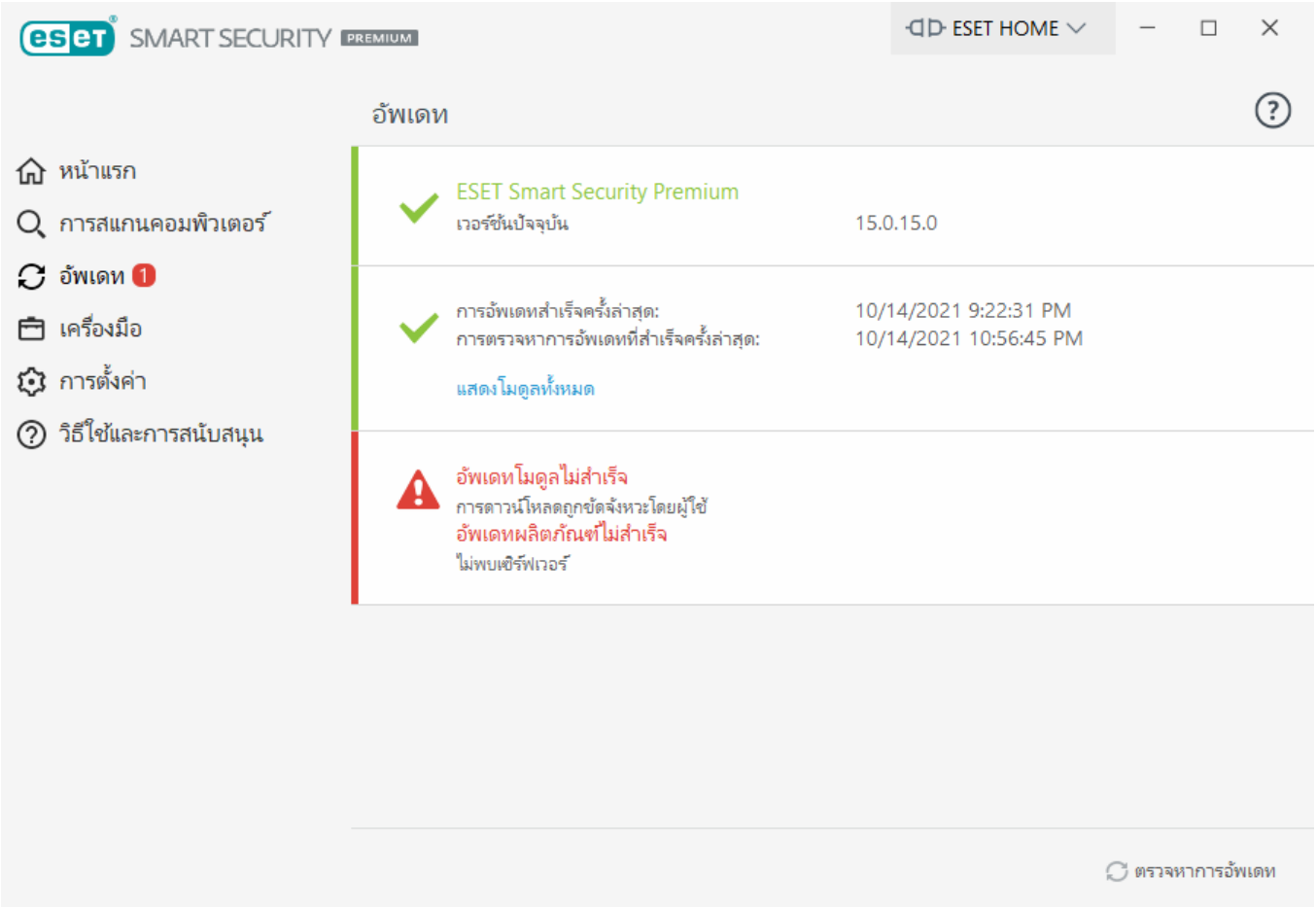
ในสถานการณ์ปกติ คุณจะเห็นเครื่องหมายถูกสีเขียวในหน้าต่าง **อัพเดท** ที่ระบุว่าโปรแกรมนั้นอัพเดทแล้ว หากไม่มีเครื่องหมายถูกสีเขียว แสดงว่าโปรแกรมไม่ได้อัพเดท และมีความเสี่ยงมากขึ้นในการติดไวรัส โปรดอัพเดทโมดูลเร็วที่สุดเท่าที่ทำได้

การอัพเดทที่ไม่สำเร็จ

หากคุณได้รับข้อความการอัพเดทโมดูลที่ไม่สำเร็จ ข้อความนี้อาจเกิดจากปัญหาต่อไปนี้:

1. **ใบอนุญาตไม่ถูกต้อง** – ใบอนุญาตที่ใช้สำหรับการเปิดใช้งานไม่ถูกต้องหรือหมดอายุแล้ว ใน หน้าต่างโปรแกรมหลัก ให้คลิก **วิธีใช้และสนับสนุน** > **เปลี่ยนใบอนุญาต** และป้อนรหัสใบอนุญาตใหม่

2. **เกิดข้อผิดพลาดขึ้นระหว่างดาวน์โหลดไฟล์การอัพเดท** - สาเหตุที่เป็นไปได้ของข้อผิดพลาดคือ การตั้งค่าการเชื่อมต่ออินเทอร์เน็ต ไม่ถูกต้อง เราขอแนะนำให้คุณตรวจสอบการเชื่อมต่ออินเทอร์เน็ตของคุณ (ด้วยการเปิดเว็บไซต์ในเว็บเบราว์เซอร์ของคุณ) ถ้าเว็บไซต์ไม่เปิด เป็นไปได้มากว่าไม่มีการเริ่มต้นการเชื่อมต่ออินเทอร์เน็ตหรือมีปัญหาในการเชื่อมต่อกับคอมพิวเตอร์ของคุณ โปรดตรวจสอบกับผู้ให้บริการอินเทอร์เน็ต (ISP) ถ้าคุณไม่มีการเชื่อมต่ออินเทอร์เน็ตที่ใช้ได้



เราแนะนำให้คุณเริ่มต้นคอมพิวเตอร์ใหม่หลังจากที่ทำการอัพเดท ESET Smart Security Premium เป็นเวอร์ชันผลิตภัณฑ์ที่ใหม่กว่าเป็นผลสำเร็จเพื่อให้แน่ใจว่าโมดูลโปรแกรมทั้งหมดจะได้รับการอัพเดทอย่างถูกต้อง ไม่จำเป็นต้องรีสตาร์ทคอมพิวเตอร์ของคุณหลังการอัพเดทโมเดลเป็นประจำ

สำหรับข้อมูลเพิ่มเติม โปรดไปที่ การแก้ไขปัญหาสำหรับข้อความ "อัพเดทโมดูลไม่สำเร็จ"

การตั้งค่าการอัพเดท

ตัวเลือกการตั้งค่าการอัพเดทจะมีอยู่ที่โครงสร้าง **การตั้งค่าขั้นสูง** (F5) ภายใต้ **อัพเดท** > **พื้นฐาน** ส่วนนี้จะระบุข้อมูลที่มาของการอัพเดทเหมือนกับการใช้เซิร์ฟเวอร์อัพเดทและข้อมูลการตรวจสอบสิทธิ์สำหรับเซิร์ฟเวอร์เหล่านี้

พื้นฐาน

โปรไฟล์การอัพเดทที่ใช้อยู่ (นอกจากบางโปรไฟล์ที่ถูกตั้งค่าใน **การตั้งค่าขั้นสูง** > **ไฟร์วอลล์** > **เครือข่ายที่รู้จัก**) จะแสดงในเมนูแบบเลื่อนลง **เลือกโปรไฟล์การอัพเดทตามค่าเริ่มต้น**

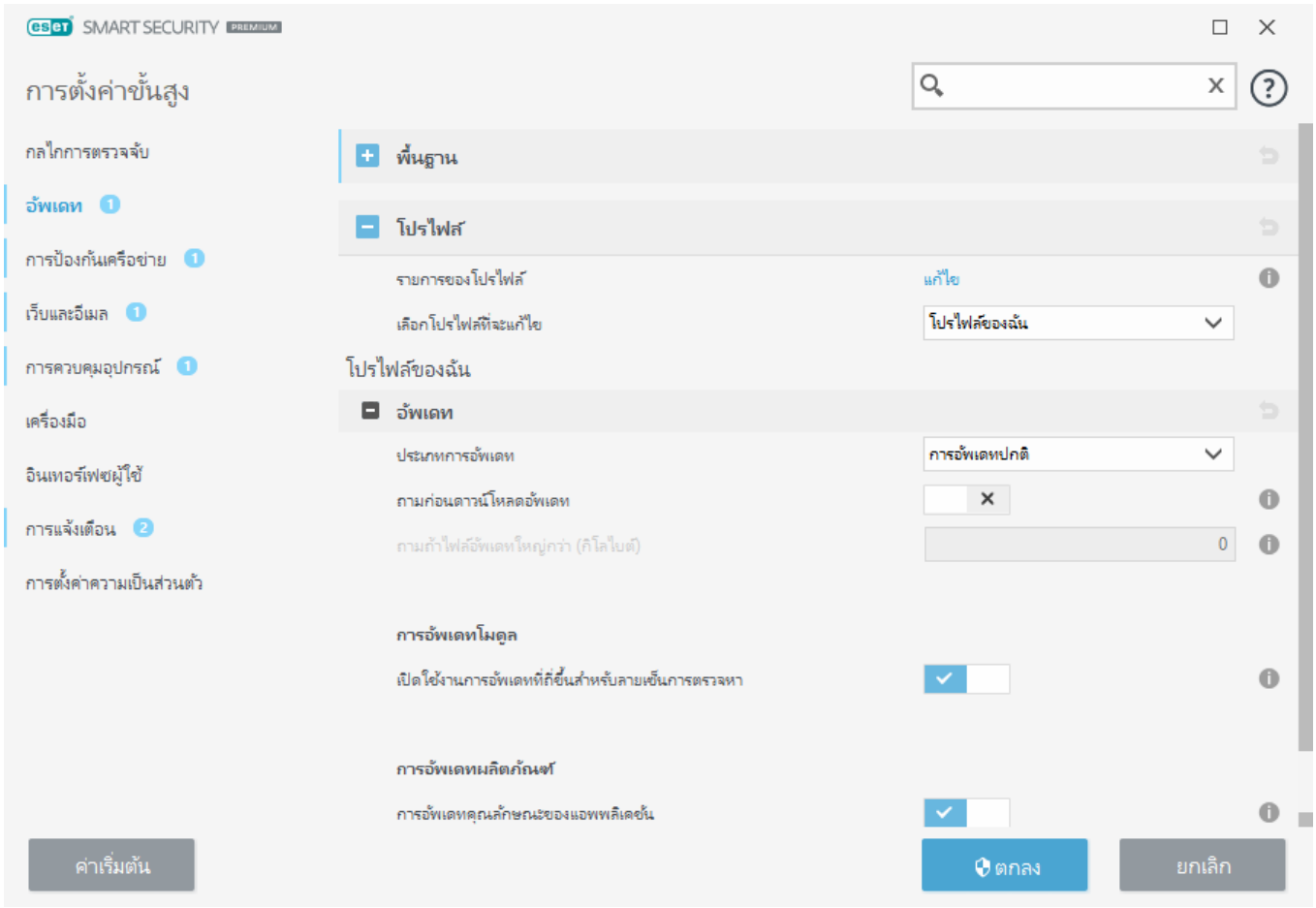
หากต้องการสร้างโปรไฟล์ใหม่ ให้ดูส่วน โปรไฟล์การอัพเดท

การสลับโปรไฟล์โดยอัตโนมัติ – จะทำให้คุณสามารถเปลี่ยนโปรไฟล์สำหรับเครือข่ายบางเครือข่ายได้

หากคุณประสบปัญหาขณะพยายามดาวน์โหลดการอัพเดทกลไกตรวจหา ให้คลิก **ล้าง** เพื่อล้างไฟล์อัพเดท/แคชชั่วคราว

การย้อนกลับโมดูล

หากคุณสงสัยว่าการอัพเดทใหม่ของกลไกตรวจหาและ/หรือโมดูลโปรแกรมอาจไม่เสถียรหรือเสียหาย คุณสามารถย้อนกลับไปเป็นเวอร์ชันก่อนหน้า ได้ แล้วปิดการใช้งานการอัพเดทสำหรับช่วงเวลาที่ตั้งค่าไว้



คุณต้องป้อนพารามิเตอร์ที่อัพเดททั้งหมดให้ถูกต้อง เพื่อให้ระบบดาวน์โหลดการอัพเดทอย่างถูกต้อง ถ้าคุณใช้ไฟร์วอลล์ โปรดตรวจสอบให้แน่ใจว่าโปรแกรม ESET ของคุณได้รับอนุญาตให้สื่อสารกับอินเทอร์เน็ต (ตัวอย่างเช่น การเชื่อมต่อ HTTPS)

โปรไฟล์

โปรไฟล์การอัพเดทสามารถสร้างขึ้นเพื่อการกำหนดค่าและงานการอัพเดทต่างๆ การสร้างโปรไฟล์การอัพเดทจะเป็นประโยชน์อย่างมากสำหรับผู้ใช้ที่ต้องเดินทางบ่อย ที่ต้องการโปรไฟล์สำรองสำหรับคุณสมบัติการเชื่อมต่ออินเทอร์เน็ตที่มีการเปลี่ยนแปลงเป็นประจำ

เมนู **เลือกโปรไฟล์ที่จะแก้ไข** แบบเลื่อนลงจะแสดงโปรไฟล์ที่เลือกในปัจจุบัน แล้วตั้งค่าเป็น **โปรไฟล์ของฉัน** ตามค่าเริ่มต้น ในการสร้างโปรไฟล์ใหม่ ให้คลิก **แก้ไข** ถัดจาก **รายการของโปรไฟล์** ป้อน **ของคุณเอง** แล้วคลิก **เพิ่ม**

การอัพเดท

ตามค่าเริ่มต้น **ประเภทการอัพเดท** จะถูกตั้งเป็น **การอัพเดทปกติ** เพื่อทำให้แน่ใจว่าไฟล์อัพเดทจะดาวน์โหลด

จากเซิร์ฟเวอร์ ESET โดยอัตโนมัติด้วยการรับส่งของเครือข่ายที่น้อยที่สุด การอัพเดทก่อนออก (ตัวเลือก **การอัพเดทก่อนออก**) เป็นการอัพเดทที่ผ่านการทดสอบภายในอย่างละเอียดและจะพร้อมใช้งานทั่วไปในเร็ว ๆ นี้ คุณสามารถใช้ประโยชน์จากการเปิดใช้งานการอัพเดทก่อนออกได้ ด้วยการเข้าถึงวิธีการตรวจหาและการแก้ไขล่าสุด อย่างไรก็ตาม การอัพเดทก่อนออกอาจไม่เสถียรตลอดเวลา และไม่ควรนำไปใช้บนเซิร์ฟเวอร์และเวิร์กสเตชันที่ใช้งานจริง ซึ่งต้องการความพร้อมในการใช้งานและเสถียรภาพสูงสุด

ถามก่อนที่จะดาวน์โหลดอัพเดท – โปรแกรมจะแสดงการแจ้งเตือนที่คุณสามารถเลือกที่จะยืนยันหรือปฏิเสธการดาวน์โหลดไฟล์อัพเดท

ถามหากไฟล์อัพเดทใหญ่กว่า (กิโลไบต์) – โปรแกรมจะแสดงข้อความยืนยันหากขนาดไฟล์อัพเดทใหญ่กว่าค่าที่กำหนด หากขนาดไฟล์อัพเดทถูกตั้งค่าเป็น 0 กิโลไบต์ โปรแกรมจะแสดงข้อความยืนยันเสมอ

ปิดใช้งานการแจ้งเตือนเกี่ยวกับรายการอัพเดทที่สำเร็จ – ปิดการแจ้งเตือนที่ถาดข้อมูลระบบที่มุมขวาล่างสุดของหน้าจอ การเลือกตัวเลือกนี้จะมีประโยชน์ ถ้ากำลังใช้แอพพลิเคชันหรือเกมแบบเต็มหน้าจออยู่ โปรดทราบว่าโหมดผู้เล่นเกมจะปิดการแจ้งเตือนทั้งหมด

การอัพเดทโมดูล

เปิดใช้งานการอัพเดทฐานข้อมูลการตรวจหาให้บ่อยขึ้น – ฐานข้อมูลการตรวจหาจะถูกอัพเดทในช่วงเวลาที่สั้นลง การปิดใช้งานการตั้งค่านี้อาจส่งผลกระทบทางลบต่ออัตราการตรวจจับ

การอัพเดทผลิตภัณฑ์

การอัพเดทคุณลักษณะของแอพพลิเคชัน – ติดตั้ง ESET Smart Security Premium เวอร์ชันใหม่โดยอัตโนมัติ

ตัวเลือกการเชื่อมต่อ

หากต้องการใช้พร็อกซีเซิร์ฟเวอร์เพื่อดาวน์โหลดการอัพเดท โปรดดูส่วนตัวเลือกการเชื่อมต่อ

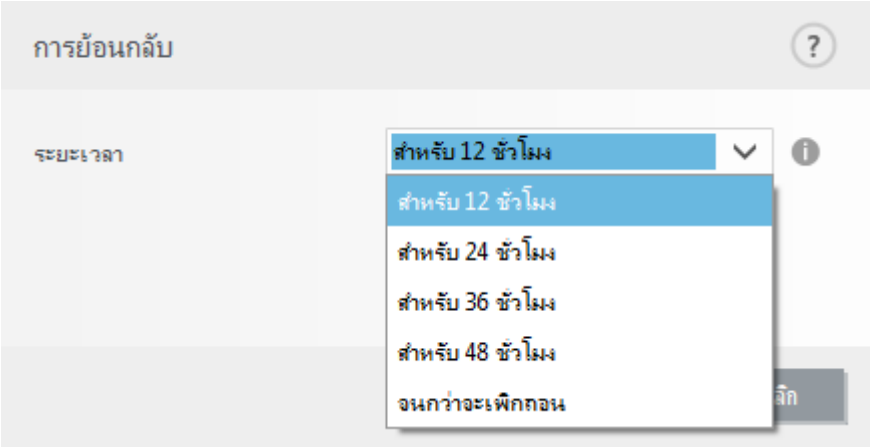
การอัพเดทย้อนหลัง

หากคุณสงสัยว่าการอัพเดทใหม่ของกลไกตรวจหาหรือโมดูลโปรแกรมอาจไม่เสถียรหรือเสียหาย คุณสามารถย้อนกลับเป็นเวอร์ชันก่อนหน้าและปิดใช้งานการอัพเดทชั่วคราว หรือมิฉะนั้น คุณสามารถเปิดใช้งานการอัพเดทที่ปิดใช้งานไว้ก่อนหน้านั้น ถ้าคุณได้เลื่อนการอัพเดทไว้อย่างไม่มีกำหนด

ESET Smart Security Premium จะบันทึกสแนปชอตของกลไกการตรวจหาและโมดูลโปรแกรมเพื่อใช้กับคุณลักษณะการย้อนกลับ หากต้องการสร้างสแนปชอตของฐานข้อมูลไวรัส ให้เปิดใช้งาน **สร้างสแนปชอตของโมดูล** ไว้ เมื่อ **สร้างสแนปชอตของโมดูล** เปิดใช้งาน สแนปชอตแรกจะถูกสร้างขึ้นในการอัพเดทครั้งแรก และสแนปชอตถัดไปจะถูกสร้างขึ้นหลังจากนั้น 48 ชั่วโมง ช่อง **จำนวนสแนปชอตที่เก็บในเครื่อง** จะระบุจำนวนของสแนปชอตกลไกการตรวจหาที่เก็บไว้

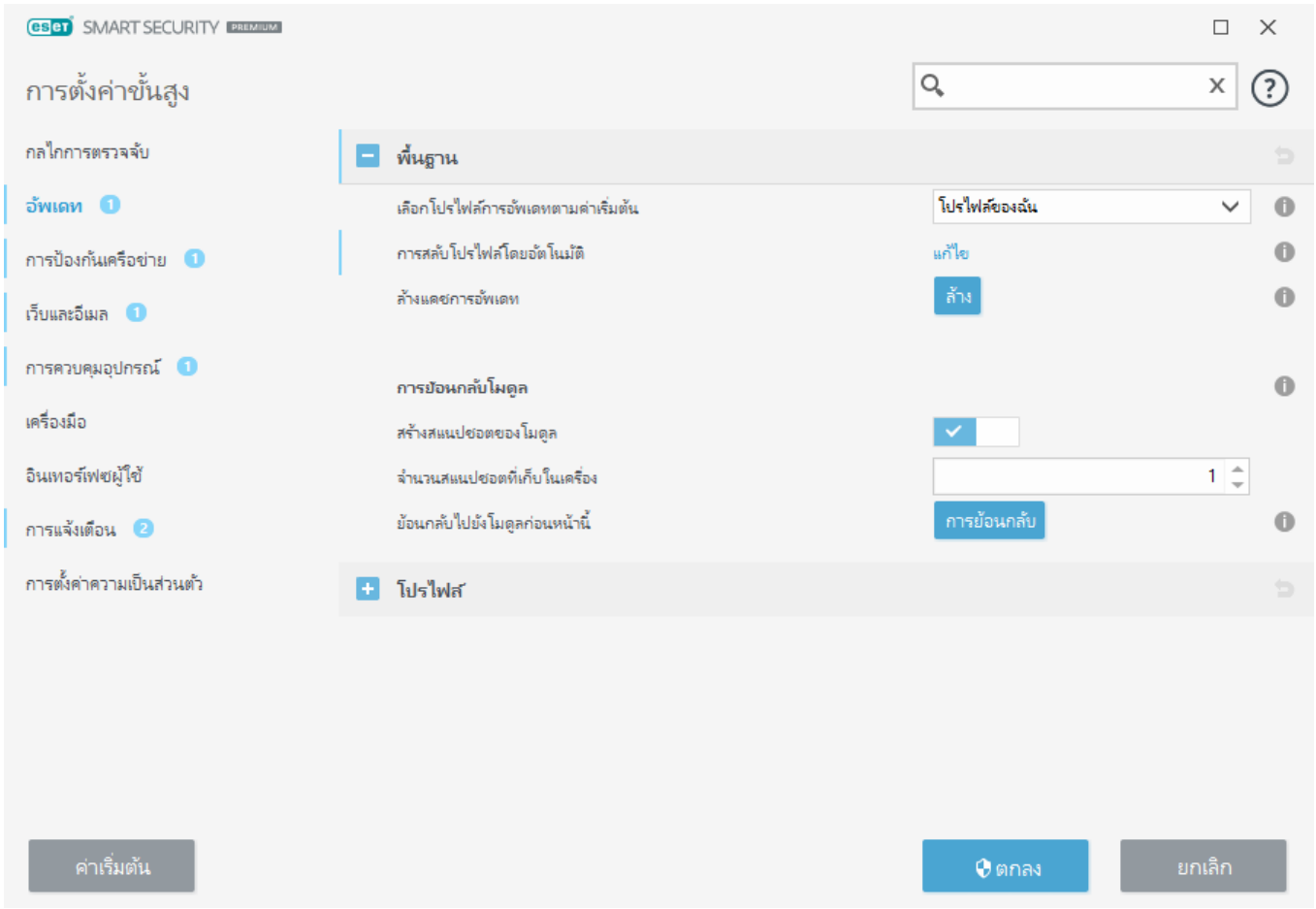
> เมื่อถึงจำนวนสูงสุดของสแนปชอต (เช่น สามภาพ) สแนปชอตที่เก่าที่สุดจะถูกแทนที่ด้วยสแนปชอตใหม่ทุก 48 ชั่วโมง ESET Smart Security Premium จะย้อนกลับกลไกการตรวจหาและรุ่นการปรับปรุงโมดูลโปรแกรมไปยังสแนปชอตที่เก่าที่สุด

หากคุณคลิก **ย้อนกลับ** (**การตั้งค่าขั้นสูง** (F5) > **อัพเดท** > **พื้นฐาน**) คุณต้องเลือกช่วงเวลาจากเมนูแบบเลื่อนลง **ระยะเวลา** ที่แสดงระยะเวลาที่จะมีการหยุดการอัพเดทกลไกตรวจหาและโมดูลโปรแกรมไว้ชั่วคราว



เลือก **จนกว่าจะยกเลิก** เพื่อเลื่อนการอัพเดทเป็นประจำออกไปโดยไม่มีกำหนดจนกว่าคุณจะเรียกการทำงานของการอัพเดทด้วยตนเอง เนื่องจากจะมีความเสี่ยงด้านความปลอดภัย ESET จึงไม่แนะนำให้เลือกตัวเลือกนี้

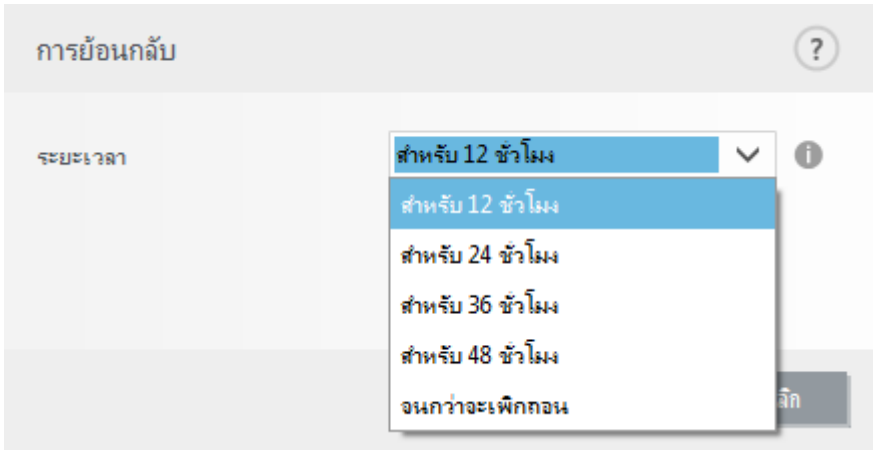
หากทำการย้อนกลับ ปุ่ม **การย้อนกลับ** จะเปลี่ยนเป็น **อนุญาตการอัพเดท** โดยจะไม่สามารถอัพเดทได้ในช่วงเวลาที่เลือกจากเมนู **ระงับการอัพเดท** แบบเลื่อนลง เวอร์ชันของกลไกตรวจหาจะถูกดาวน์เกรดมาเป็นรุ่นเก่าที่สุดที่มีและเก็บไว้เป็นสแนปชอตในระบบไฟล์ของเครื่องคอมพิวเตอร์



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

ช่วงเวลาย้อนกลับ

หากคุณคลิก **ย้อนกลับ** (**การตั้งค่าขั้นสูง** (F5) > **อัพเดท** > **พื้นฐาน**) คุณต้องเลือกช่วงเวลาจากเมนูแบบเลื่อนลง **ระยะเวลา** ที่แสดงระยะเวลาที่จะมีการหยุดการอัพเดทกลไกตรวจหาและโมดูลโปรแกรมไว้ชั่วคราว



เลือก **จนกว่าจะยกเลิก** เพื่อเลื่อนการอัพเดทเป็นประจำออกไปโดยไม่มีกำหนดจนกว่าคุณจะเรียกการทำงานของการอัพเดทด้วยตนเอง เนื่องจากจะมีความเสี่ยงด้านความปลอดภัย ESET จึงไม่แนะนำให้เลือกตัวเลือกนี้

การอัพเดทผลิตภัณฑ์

ส่วน **การอัพเดทผลิตภัณฑ์** ทำให้คุณสามารถติดตั้งการอัพเดทคุณลักษณะใหม่เมื่อพร้อมใช้งานได้โดยอัตโนมัติ

การอัพเดทคุณลักษณะของแอพพลิเคชันจะนำมาซึ่งคุณลักษณะใหม่ หรือการเปลี่ยนแปลงคุณลักษณะที่มีในอยู่เวอร์ชันก่อนหน้านี้ การอัพเกรดสามารถทำได้โดยอัตโนมัติโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ หรือคุณสามารถเลือกให้มีการแจ้งเตือนได้ หลังจากการติดตั้งการอัพเดทคุณลักษณะของแอพพลิเคชันแล้ว อาจจำเป็นต้องรีสตาร์ทคอมพิวเตอร์

การอัพเดทคุณลักษณะของแอพพลิเคชัน – เมื่อเปิดใช้งาน ระบบจะดำเนินการอัพเดทคุณลักษณะของแอพพลิเคชันโดยอัตโนมัติ

ตัวเลือกการเชื่อมต่อ

หากต้องการเข้าถึงตัวเลือกการตั้งค่าเซิร์ฟเวอร์พร็อกซีสำหรับโปรไฟล์การอัพเดทที่ระบุ ให้คลิก **อัพเดท** ในโครงสร้าง **การตั้งค่าขั้นสูง** (F5) จากนั้นคลิก **โปรไฟล์** > **อัพเดท** > **ตัวเลือกการเชื่อมต่อ** คลิกเมนูแบบเลื่อนลง **โหมดพร็อกซี** แล้วเลือกหนึ่งในสามตัวเลือกต่อไปนี้:

- ไม่ใช้พร็อกซีเซิร์ฟเวอร์
- การเชื่อมต่อผ่านพร็อกซีเซิร์ฟเวอร์
- ใช้การตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วม

เลือก **ใช้การตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วม** เพื่อใช้ตัวเลือกการกำหนดค่าพร็อกซีเซิร์ฟเวอร์ที่ระบุไว้แล้วในสาขาของ **เครื่องมือ** > **พร็อกซีเซิร์ฟเวอร์** ของโครงสร้างการตั้งค่าขั้นสูง

เลือก **ไม่ใช้เซิร์ฟเวอร์พร็อกซี** เพื่อระบุว่าจะไม่ใช้พร็อกซีเซิร์ฟเวอร์ในการอัพเดท ESET Smart Security Premium

ควรเลือกตัวเลือก **การเชื่อมต่อผ่านพร็อกซีเซิร์ฟเวอร์** ไว้ถ้า:

- พร็อกซีเซิร์ฟเวอร์อื่นนอกเหนือจากที่ระบุไว้ใน **เครื่องมือ** > **พร็อกซีเซิร์ฟเวอร์** ที่ใช้เพื่ออัพเดท ESET Smart

Security Premium ในการกำหนดค่านี้ ควรระบุข้อมูลสำหรับพร็อกซีใหม่ไว้ในที่อยู่ **พร็อกซีเซิร์ฟเวอร์**, **พอร์ต** การสื่อสาร (3128 ตามค่าเริ่มต้น) และ **ชื่อผู้ใช้** และ **รหัสผ่าน** สำหรับพร็อกซีเซิร์ฟเวอร์ หากต้องใช้

• การตั้งค่าพร็อกซีเซิร์ฟเวอร์ไม่ได้ถูกตั้งค่าให้ใช้ร่วมกัน แต่ ESET Smart Security Premium จะเชื่อมต่อกับพร็อกซีเซิร์ฟเวอร์เพื่อการอัพเดท

• คอมพิวเตอร์ของคุณจะเชื่อมต่อกับอินเทอร์เน็ตผ่านพร็อกซีเซิร์ฟเวอร์ การตั้งค่าจะมาจาก Internet Explorer ระหว่างการติดตั้งโปรแกรม แต่ถ้าการตั้งค่านี้มีการเปลี่ยนแปลง (เช่น หากคุณเปลี่ยน ISP) โปรดตรวจสอบให้แน่ใจว่าการตั้งค่าพร็อกซี ที่อยู่ในหน้าต่างนี้ถูกต้อง มิฉะนั้นโปรแกรมจะไม่สามารถเชื่อมต่อกับเซิร์ฟเวอร์การอัพเดท

การตั้งค่าเริ่มต้นสำหรับพร็อกซีเซิร์ฟเวอร์คือ **ใช้การตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วม**

ใช้การเชื่อมต่อโดยตรงหากพร็อกซีไม่สามารถใช้งานได้ – พร็อกซีจะถูกข้ามระหว่างการอัพเดทถ้าไม่สามารถเข้าถึงได้

ช่อง **ชื่อผู้ใช้** และ **รหัสผ่าน** ในส่วนนี้เป็นข้อมูลเจาะจงสำหรับพร็อกซีเซิร์ฟเวอร์โดยเฉพาะ กรอกช่องเหล่านี้เฉพาะเมื่อต้องใช้ชื่อผู้ใช้และรหัสผ่านเพื่อเข้าสู่พร็อกซีเซิร์ฟเวอร์เท่านั้น ช่องเหล่านี้ควรป้อนต่อเมื่อคุณทราบว่าคุณต้องใช้รหัสผ่านเพื่อเข้าถึงอินเทอร์เน็ตผ่านพร็อกซีเซิร์ฟเวอร์

วิธีสร้างงานการอัพเดท

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

การอัพเดทยังสามารถเรียกใช้งานเป็นงานตามกำหนดการ หากต้องการการกำหนดค่างานตามกำหนดการ ให้คลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **เครื่องมือวางกำหนดการณ์** ตามค่าเริ่มต้น เปิดใช้งานงานต่อไปนี้ในESET Smart Security Premium:

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

งานการอัพเดทแต่ละงานจะสามารถแก้ไขได้เพื่อให้เหมาะกับความต้องการของคุณ นอกเหนือจากงานการอัพเดทเริ่มต้นแล้ว คุณสามารถสร้างงานการอัพเดทใหม่ด้วยการกำหนดค่าที่ผู้ใช้กำหนดได้ สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการสร้างและการกำหนดค่างานการอัพเดท โปรดดูที่ เครื่องมือวางกำหนดการ

หน้าต่างข้อความ – ต้องเริ่มระบบใหม่

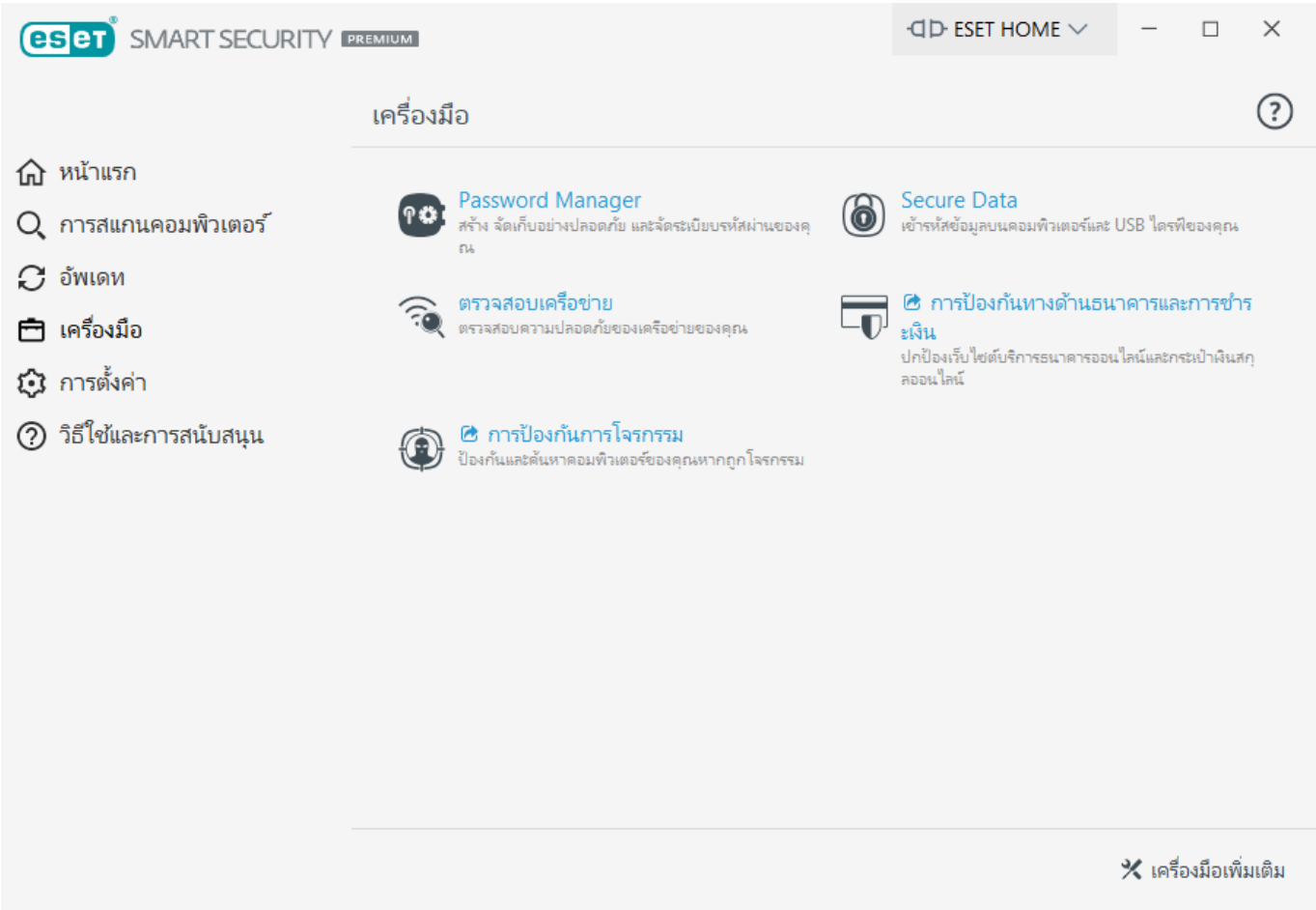
จำเป็นต้องรีสตาร์ทคอมพิวเตอร์หลังจากอัพเดท ESET Smart Security Premium เป็นเวอร์ชันใหม่ ESET Smart Security Premium เวอร์ชันใหม่ได้ออกมาเพื่อปรับปรุงประสิทธิภาพหรือแก้ไขปัญหาที่การอัพเดทอัตโนมัติของโมดูลโปรแกรมไม่สามารถแก้ไขได้

ESET Smart Security Premium เวอร์ชันใหม่สามารถติดตั้งอัตโนมัติได้ โดยขึ้นอยู่กับการตั้งค่าการอัพเดทโปรแกรมของคุณ หรือติดตั้งด้วยตนเองได้โดยดาวน์โหลดและติดตั้งเวอร์ชันใหม่ทับเวอร์ชันก่อนหน้า

คลิก **รีสตาร์ททันที** เพื่อรีสตาร์ทคอมพิวเตอร์ของคุณ หากคุณวางแผนจะรีสตาร์ทคอมพิวเตอร์ของคุณในภายหลัง ให้คลิก **เตือนฉันในภายหลัง** คุณสามารถรีสตาร์ทคอมพิวเตอร์ด้วยตนเองในภายหลังได้จากส่วน**หน้าแรก**ในหน้าต่างโปรแกรมหลัก

เครื่องมือ

เมนู **เครื่องมือ** ประกอบด้วยโมดูลที่ช่วยให้การจัดการโปรแกรมง่ายขึ้นและมีตัวเลือกเพิ่มเติมสำหรับผู้ใช้ขั้นสูง



 Password Manager – ดูแลรหัสผ่านของคุณให้ปลอดภัย

 **Secure Data** – ปกป้องไฟล์ส่วนตัวและไฟล์ลับของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับผลิตภัณฑ์ ให้ดู ESET Secure Data

 **ตัวตรวจสอบเครือข่าย** – ลดความเสี่ยงต่อการเกิดปัญหาด้านความปลอดภัยขณะเชื่อมต่อกับเครือข่าย สำหรับข้อมูลเพิ่มเติม ให้ดู ตัวตรวจสอบเครือข่าย

 **การป้องกันการธนาคารและการชำระเงิน** - ESET Smart Security Premium ป้องกันหมายเลขบัตรเครดิตและข้อมูลส่วนบุคคลอื่นๆ ที่เป็นความลับของคุณในขณะที่คุณใช้การธนาคารออนไลน์หรือเว็บไซต์ชำระเงิน เบราว์เซอร์ที่ปลอดภัยจะยังถูกเรียกใช้งานเพื่อทำให้คุณทำธุรกรรมทางธนาคารได้อย่างปลอดภัยมากขึ้น

 **การป้องกันการโจรกรรม** - ระบุตำแหน่งและช่วยค้นหาอุปกรณ์ที่หายไปของคุณในกรณีที่อุปกรณ์สูญหายหรือถูกขโมย

คลิก เครื่องมือเพิ่มเติม เพื่อแสดงเครื่องมืออื่นๆ สำหรับปกป้องคอมพิวเตอร์ของคุณ (เช่น การกักเก็บ)

Password Manager

Password Manager เป็นส่วนหนึ่งของแพ็คเกจ ESET Smart Security Premium

เป็น Password Manager ที่ป้องกันและจัดเก็บรหัสผ่านและข้อมูลส่วนบุคคลของคุณ ยังมีคุณสมบัติการกรอกแบบฟอร์มให้เสร็จสมบูรณ์ที่จะช่วยประหยัดเวลาโดยการกรอกแบบฟอร์มบนเว็บอย่างอัตโนมัติและแม่นยำ

สำหรับข้อมูลเพิ่มเติม โปรดดู วิธีใช้ออนไลน์ของ Password Manager

- Password Manager การติดตั้ง
- เริ่มใช้งาน Password Manager
- จัดการ Password Manager ที่จัดเก็บใน ESET HOME

Secure Data

Secure Data โดย ESET อนุญาตให้คุณเข้ารหัสข้อมูลบนคอมพิวเตอร์และ USB ไดรฟ์ของคุณเพื่อป้องกันการใช้งานข้อมูลส่วนตัวที่เป็นความลับในทางที่ผิดได้

- การติดตั้ง Secure Data
- สร้างไดรฟ์เสมือนที่เข้ารหัส
- ไดรฟ์ที่เข้ารหัสแบบถอดได้
- ดูบทความฐานความรู้ของเราสำหรับคำถามที่พบบ่อยเกี่ยวกับ ESET Secure Data

การติดตั้ง Secure Data

Secure Data เป็นส่วนหนึ่งของ ESET Smart Security Premium.

เมื่อปฏิบัติตามการติดตั้งและเปิดใช้งาน ESET Smart Security Premium แล้ว คุณจะมีตัวเลือกสำหรับเปิดใช้งาน Secure Data พร้อมทั้งคุณลักษณะอื่น โปรดคลิก **เปิดใช้งาน** ที่อยู่ถัดจาก **Secure Data** เพื่อเปิดใช้งาน Secure Data

หากคุณต้องการออกจากหน้าจอต้อนรับโดยไม่เปิดใช้งาน Secure Data คุณสามารถเปิดใช้งานคุณลักษณะการเข้ารหัสในส่วน **การตั้งค่า** > **เครื่องมือความปลอดภัย** ของ ESET Smart Security Premium ได้ โดยไปที่ **Secure Data**

คุณไม่สามารถติดตั้ง ESET Endpoint Encryption บนอุปกรณ์เครื่องเดียวกับที่ได้ติดตั้ง Secure Data ไว้ได้

การเริ่มต้นใช้งาน Secure Data

เมื่อคุณเปิดใช้งาน Secure Data ให้ไปที่ **เครื่องมือ** > **Secure Data** แล้วหน้าจอที่มีตัวเลือกการเข้ารหัสที่พร้อมใช้งานจะแสดงขึ้น

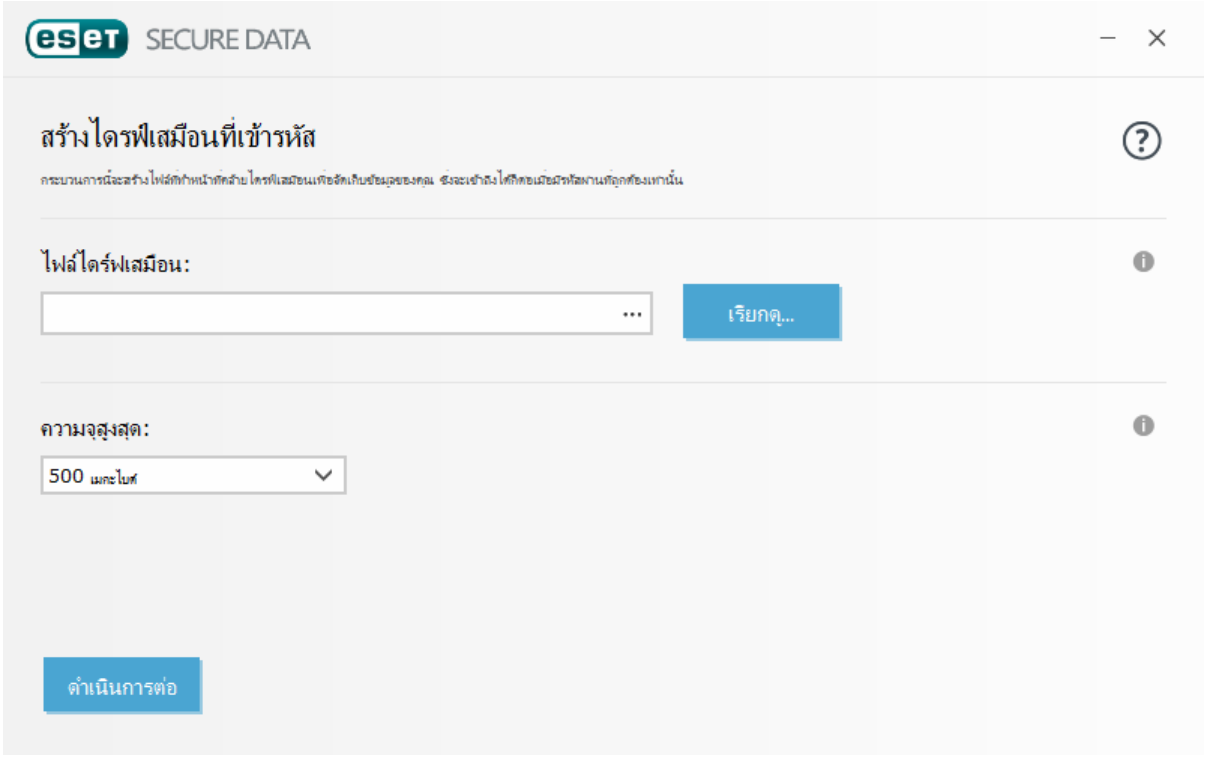
- สร้างไดรฟ์เสมือนที่เข้ารหัส
- ไดรฟ์ที่เข้ารหัสแบบถอดได้

ไดรฟ์เสมือนที่เข้ารหัส

คุณสามารถใช้ Secure Data เพื่อสร้างไดรฟ์เสมือนที่เข้ารหัสได้ จะไม่มีการจำกัดจำนวนของไดรฟ์ที่คุณสามารถสร้างได้ ตราบใดที่ยังคงมีพื้นที่ฮาร์ดไดรฟ์ที่สามารถใช้เพื่อการดำเนินการนี้ได้ โปรดปฏิบัติตามขั้นตอนด้านล่างเพื่อสร้างไดรฟ์เสมือนที่เข้ารหัส:

1.ในหน้าจอ **เข้ารหัสข้อมูลบนคอมพิวเตอร์นี้หรือไดรฟ์แบบถอดได้** ให้คลิก **ไดรฟ์เสมือน**

2.คลิก**เรียกดู** เลือกตำแหน่งสำหรับจัดเก็บไดรฟ์เสมือน



3.ป้อนชื่อสำหรับไดรฟ์เสมือนแล้วเลือก **บันทึก**

4.ใช้เมนูแบบเลื่อนลง **ความจุสูงสุด** เพื่อตั้งขนาดของไดรฟ์เสมือน จากนั้นคลิก**ดำเนินการต่อ**

5.ตั้งรหัสผ่านให้กับไดรฟ์เสมือน หากคุณไม่ต้องการให้ไดรฟ์เสมือนได้รับการถอดรหัสโดยอัตโนมัติเมื่อคุณล็อคอินเข้าสู่บัญชี Windows ให้เลิกเลือก **ถอดรหัสอัตโนมัติบนบัญชี Windows นี้** แล้วคลิก **ดำเนินการต่อ**

6.ไดรฟ์เสมือนที่เข้ารหัสของคุณได้รับการสร้างและพร้อมใช้งานแล้ว รายการนี้จะปรากฏเป็นดิสก์ภายใน

เครื่องถ้าคุณเปิด **พีซีเครื่องนี้** (**คอมพิวเตอร์** ใน Windows 7 และรุ่นก่อนหน้า)

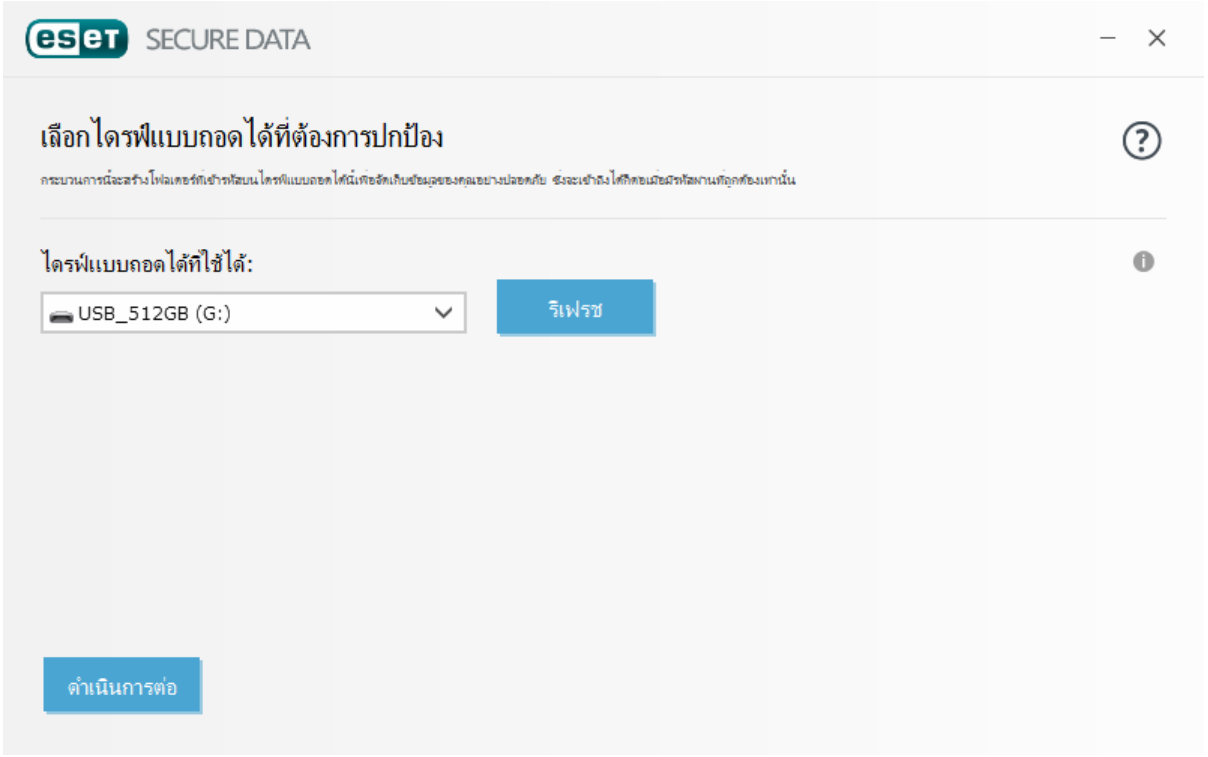
หากต้องการเข้าถึงไดรฟ์ที่เข้ารหัสหลังจากรีสตาร์ทเครื่องคอมพิวเตอร์ ให้ค้นหาไฟล์ของไดรฟ์ที่เข้ารหัส (ไฟล์ประเภท .eed) ที่คุณสร้างแล้วคลิกสองครั้งที่รายการดังกล่าว หากระบบขอ ให้ป้อนรหัสผ่านที่คุณตั้งค่าเมื่อสร้างไดรฟ์ที่เข้ารหัส ไดรฟ์ดังกล่าวจะถูกเมาต์และปรากฏเป็นดิสก์ภายในเครื่องภายใต้ **พีซีเครื่องนี้** (**คอมพิวเตอร์** ใน Windows 7 และรุ่นก่อนหน้า) เมื่อเมาต์ไดรฟ์ที่เข้ารหัสเป็นดิสก์ภายในเครื่องแล้ว ดิสก์ภายในเครื่องดังกล่าวและเนื้อหาที่ถอดรหัสดังกล่าวจะพร้อมใช้งานกับผู้ใช้รายอื่นบนเครื่อง Windows ยกเว้นว่าคุณจะออกจากระบบหรือรีสตาร์ทคอมพิวเตอร์

> **ฉันสามารถลบไดรฟ์เสมือนได้หรือไม่**
> ได้ หากต้องการลบไดรฟ์เสมือนที่เข้ารหัส ให้ ปฏิบัติตามคำแนะนำในบทความ ESET Secure Data FAQ ของเรา

ไดรฟ์ที่เข้ารหัสแบบถอดได้

Secure Data อนุญาตให้คุณสร้างไดเรกทอรีที่เข้ารหัสบนบนไดรฟ์แบบถอดได้ หากต้องการทำเช่นนั้น ให้ทำตามขั้นตอนด้านล่าง:

1. ใส่ไดรฟ์แบบถอดได้ (แฟลชไดรฟ์ USB, ฮาร์ดดิสก์ USB) เข้าไปในคอมพิวเตอร์
2. คลิก **ไดรฟ์แบบถอดได้** ใน หน้าจอ **เข้ารหัสข้อมูลบนคอมพิวเตอร์นี้หรือไดรฟ์แบบถอดได้**
3. เลือกเชื่อมต่อไดรฟ์แบบถอดได้เพื่อเข้ารหัสแล้วเลือก **ดำเนินการต่อ**
   คลิก **รีเฟรช** เพื่ออัพเดทรายการไดรฟ์ที่เข้ารหัสได้ ไดรฟ์ที่เข้ารหัสแล้วหรือไดรฟ์ที่ไม่รองรับจะไม่ปรากฏในรายการ
   ถ้าคุณต้องการเข้ารหัสโฟลเดอร์ที่ปลอดภัยในไดรฟ์แบบถอดได้ที่เลือกบนอุปกรณ์ Windows ใดๆ โดยไม่ต้องติดตั้ง ESET Smart Security Premium โปรดเลือก **ถอดรหัสโฟลเดอร์บนอุปกรณ์ Windows ใดๆ**



4. ตั้งรหัสผ่านที่ต้องการให้กับไดเรกทอรีที่เข้ารหัสบนรายการที่ถอดออกได้ หากคุณไม่ต้องการให้อุปกรณ์เสมือนได้รับการถอดรหัสโดยอัตโนมัติเมื่อคุณล็อคอินเข้าสู่บัญชี Windows ให้เลิกเลือก **ถอดรหัสอัตโนมัติบนบัญชี Windows นี้** แล้วคลิก **ดำเนินการต่อ**

5. ไดรฟ์แบบถอดได้ของคุณได้รับการป้องกันและไดเรกทอรีที่เข้ารหัสไว้พร้อมใช้งานแล้ว

นับจากตอนนี้ หากคุณเชื่อมต่อไดรฟ์แบบถอดได้ของคุณเข้ากับคอมพิวเตอร์โดยยังไม่ได้ติดตั้ง Secure Data

โฟลเดอร์ที่เข้ารหัสจะไม่สามารถมองเห็นได้ หากไดรฟ์แบบถอดได้ไม่ได้เชื่อมต่ออยู่กับคอมพิวเตอร์ที่ติดตั้ง Secure Data ระบบจะขอให้คุณป้อนรหัสผ่านเพื่อถอดรหัสไดรฟ์แบบถอดได้ หากคุณไม่ได้ป้อนรหัสผ่าน โฟลเดอร์ที่เข้ารหัสจะมองเห็นได้แต่ยังคงเข้าถึงไม่ได้

ตัวตรวจสอบเครือข่าย

ตัวตรวจสอบเครือข่ายสามารถช่วยระบุจุดอ่อน (เช่น พอร์ตที่เปิดอยู่หรือรหัสผ่านเราเตอร์ที่คาดเดาได้ง่าย) ในเครือข่ายที่เชื่อถือของคุณ (เครือข่ายบ้านหรือที่ทำงาน) คุณลักษณะนี้ยังมาพร้อมกับรายชื่ออุปกรณ์ที่เชื่อมต่ออยู่ พร้อมจัดเรียงตามประเภทอุปกรณ์ (เช่น เครื่องพิมพ์ เราเตอร์ อุปกรณ์เคลื่อนที่ ฯลฯ) เพื่อแสดงให้คุณเห็นว่าอะไรบ้างที่กำลังเชื่อมต่อกับเครือข่ายของคุณอยู่ (เช่น เครื่องเล่นเกม, IoT หรืออุปกรณ์อัจฉริยะภายในบ้านชนิดอื่นๆ)

ตัวตรวจสอบเครือข่ายจะช่วยให้คุณระบุจุดอ่อนของเราเตอร์และเพิ่มระดับการป้องกันเมื่อเชื่อมต่อกับเครือข่ายได้

ตัวตรวจสอบเครือข่ายจะไม่กำหนดค่าเราเตอร์ใหม่ให้คุณ คุณจะต้องทำการเปลี่ยนค่าด้วยตัวเองโดยใช้ส่วนติดต่อเฉพาะของเราเตอร์ มีความเสี่ยงสูงมากที่มัลแวร์จะใช้เราเตอร์บ้านเพื่อการโจมตีการปฏิเสธบริการ (DDoS) เป็นวงกว้าง หากรหัสผ่านเราเตอร์ไม่ได้ถูกเปลี่ยนจากค่าเริ่มต้นโดยผู้ใช้ แฮคเกอร์จะสามารถเดาและล็อคอินเราเตอร์ของคุณแล้วกำหนดค่าใหม่ หรือทำให้เครือข่ายของคุณมีความเสี่ยงได้อย่างง่ายดาย

เราแนะนำเป็นอย่างยิ่งให้คุณสร้างรหัสผ่านที่คาดเดาได้ยากซึ่งยาวเพียงพอและมีตัวเลข สัญลักษณ์ หรืออักษรตัวพิมพ์ใหญ่อยู่ด้วย หากต้องการทำให้รหัสผ่านเจาะได้ยากขึ้น ให้ใช้อักขระประเภทต่างๆ ผสมกัน

หากเครือข่ายที่คุณเชื่อมต่อได้รับการกำหนดค่าเป็นเครือข่ายที่เชื่อถือ คุณสามารถทำเครื่องหมายเครือข่ายนั้นเป็น "เครือข่ายของฉัน" ได้ คลิก **ทำเครื่องหมายเป็น "เครือข่ายของฉัน"** เพื่อเพิ่มแท็กเครือข่ายของฉันไปยังเครือข่ายดังกล่าว แท็กนี้จะแสดงถัดจากเครือข่ายทั่วทั้ง ESET Smart Security Premium เพื่อให้ได้การระบุตัวตนและภาพรวมการรักษาความปลอดภัยที่ดีขึ้น คลิก **ยกเลิกการทำเครื่องหมายเป็น "เครือข่ายของฉัน"** เพื่อลบแท็กออก

อุปกรณ์แต่ละเครื่องที่เชื่อมต่อกับเครือข่ายของคุณจะแสดงโดยมีข้อมูลพื้นฐานในมุมมองรายการ คลิกอุปกรณ์ที่ต้องการเพื่อ แก้ไขอุปกรณ์หรือดูข้อมูลโดยละเอียดเกี่ยวกับอุปกรณ์

เมนู **เครือข่าย** แบบเลื่อนลงจะช่วยให้คุณสามารถกรองอุปกรณ์ตามเกณฑ์ต่อไปนี้ได้:

- อุปกรณ์ที่เชื่อมต่อกับเครือข่ายเฉพาะ
- อุปกรณ์ที่เชื่อมต่ออยู่กับ **ทุกเครือข่าย**
- อุปกรณ์ที่ไม่จัดหมวดหมู่

หากต้องการให้แสดงอุปกรณ์ที่เชื่อมต่อทั้งหมดในมุมมอง Sonar ให้คลิกไอคอน Sonar เลื่อนเคอร์เซอร์ไปที่ไอคอนอุปกรณ์เพื่อดูข้อมูลพื้นฐาน เช่น ชื่อเครือข่ายและวันที่เห็นล่าสุด

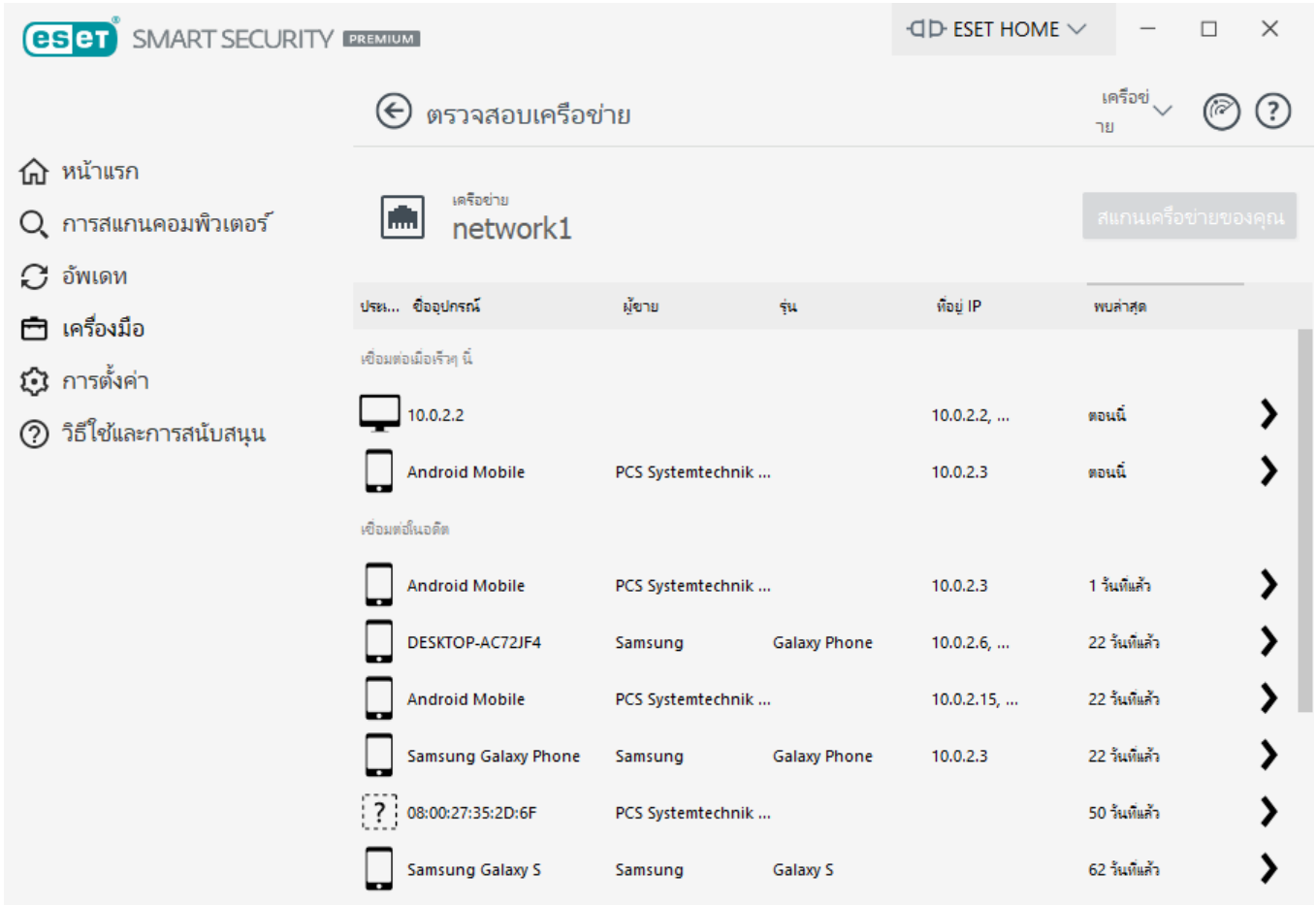
คลิกไอคอนอุปกรณ์เพื่อ แก้ไขอุปกรณ์หรือดูข้อมูลโดยละเอียดเกี่ยวกับอุปกรณ์ อุปกรณ์ที่เชื่อมต่อล่าสุดจะแสดงใกล้กับเราเตอร์เพื่อให้คุณมองเห็นได้ง่าย

คลิก **สแกนเครือข่ายของคุณ** เพื่อสแกนเครือข่ายที่คุณกำลังเชื่อมต่ออยู่ด้วยตัวคุณเอง **สแกนเครือข่ายของคุณ** สามารถใช้งานได้เฉพาะกับเครือข่ายที่เชื่อถือเท่านั้น ดู เครือข่ายที่รู้จัก เพื่อตรวจสอบหรือแก้ไขการตั้งค่าเครือข่ายของคุณ

คุณสามารถเลือกได้จากตัวเลือกการสแกนต่อไปนี้:

- สแกนทุกอย่าง
- สแกนเราเตอร์เท่านั้น
- สแกนอุปกรณ์เท่านั้น

ดำเนินการสแกนเครือข่ายกับเครือข่ายที่เชื่อถือเท่านั้น! หากคุณสแกนเครือข่ายที่ไม่เชื่อถือ โปรดระวังอันตรายที่อาจเกิดขึ้น



เมื่อการสแกนเสร็จสิ้น การแจ้งเตือนที่มีลิงก์ไปยังข้อมูลพื้นฐานเกี่ยวกับอุปกรณ์จะปรากฏขึ้น หรือคุณสามารถคลิกสองครั้งที่อุปกรณ์ที่น่าสงสัยนั้นในมุมมองรายการหรือมุมมอง Sonar ได้ คลิก **การแก้ไขปัญหา** เพื่อดูการสื่อสารที่ถูกปิดกั้นล่าสุด ข้อมูลเพิ่มเติมเกี่ยวกับการแก้ไขปัญหาไฟร์วอลล์

มีการแจ้งเตือนสองประเภทที่จะแสดงโดยโมดูลตัวตรวจสอบเครือข่ายที่เชื่อมต่ออยู่:

- **อุปกรณ์ใหม่เชื่อมต่อกับเครือข่ายแล้ว** – หากอุปกรณ์ที่ไม่พบก่อนหน้านี้ได้เชื่อมต่อกับเครือข่ายในขณะที่ผู้ใช้เชื่อมต่ออยู่ การแจ้งเตือนนี้จะปรากฏขึ้น
- **พบอุปกรณ์เครือข่ายใหม่** – การแจ้งเตือนนี้จะปรากฏขึ้นเมื่อคุณเชื่อมต่อกับเครือข่ายที่เชื่อถือของคุณอีกครั้ง และอุปกรณ์ที่ไม่พบก่อนหน้านี้ได้ปรากฏขึ้น

การแจ้งเตือนทั้งสองประเภทจะแจ้งให้คุณทราบหากมีอุปกรณ์ที่ไม่ได้รับอนุญาตพยายามจะเชื่อมต่อกับเครือข่ายของคุณ คลิก **ดูรายละเอียดอุปกรณ์** เพื่อแสดงรายละเอียด

ไอคอนอุปกรณ์ในตัวตรวจสอบเครือข่ายหมายความว่าอย่างไร

	ไอคอนดาวสีเหลืองจะระบุถึงอุปกรณ์ใหม่ในเครือข่ายที่เพิ่งถูกตรวจพบโดย ESET เป็นครั้งแรก
	ไอคอนข้อควรระวังสีเหลืองจะระบุว่าเราเตอร์ของคุณอาจมีจุดอ่อน คลิกที่ไอคอนในผลิตภัณฑ์ของคุณสำหรับข้อมูลอย่างละเอียดเกี่ยวกับปัญหา
	ไอคอนคำเตือนสีแดงจะระบุว่าอุปกรณ์ที่อยู่ภายในเราเตอร์ของคุณมีจุดอ่อนและอาจติดไวรัส คลิกที่ไอคอนในผลิตภัณฑ์ของคุณสำหรับข้อมูลอย่างละเอียดเกี่ยวกับปัญหา
	ไอคอนสีน้ำเงินอาจปรากฏขึ้นเมื่อผลิตภัณฑ์ ESET ของคุณมีข้อมูลเพิ่มเติมสำหรับเราเตอร์แต่ไม่ต้องการการดำเนินการใดๆ โดยทันทีเนื่องจากไม่ใช่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงด้านความปลอดภัย คลิกที่ไอคอนในผลิตภัณฑ์ของคุณสำหรับข้อมูลอย่างละเอียดเกี่ยวกับปัญหา

อุปกรณ์เครือข่ายในตัวตรวจสอบเครือข่าย

ข้อมูลโดยละเอียดเกี่ยวกับอุปกรณ์สามารถพบได้ที่นี่ รวมถึงข้อมูลต่อไปนี้:

- ชื่ออุปกรณ์:
- ประเภทอุปกรณ์
- พบล่าสุด
- ชื่อเครือข่าย
- ที่อยู่ IP

- ที่อยู่ MAC
- ระบบปฏิบัติการ

ไอคอนดินสอแสดงให้ทราบว่าคุณสามารถแก้ไขชื่ออุปกรณ์หรือเปลี่ยนประเภทของอุปกรณ์ได้

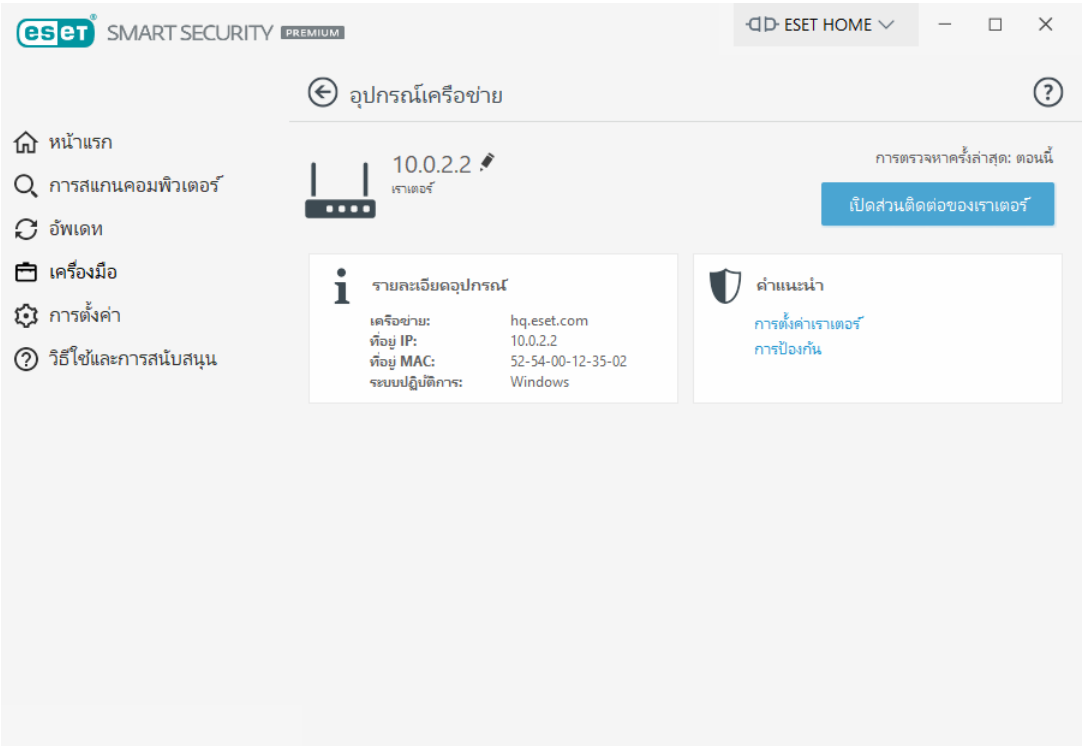
ลบออกจากประวัติ – ลบอุปกรณ์ออกจากรายการอุปกรณ์ ตัวเลือกนี้จะใช้ได้เฉพาะกับอุปกรณ์ที่ไม่ได้เชื่อมต่อกับเครือข่ายของคุณในขณะนี้

การทำงานที่ใช้ได้สำหรับอุปกรณ์แต่ละประเภท มีดังนี้:

เราเตอร์

การตั้งค่าเราเตอร์ – คุณสามารถเข้าถึงการตั้งค่าเราเตอร์จากส่วนติดต่อทางเว็บหรือแอพพลิเคชันโทรศัพท์มือถือ หรือคลิก **เปิดส่วนติดต่อของเราเตอร์** หากคุณมีเราเตอร์ซึ่งให้บริการโดยผู้ให้บริการอินเทอร์เน็ตของคุณ อาจจำเป็นที่จะต้องติดต่อกับฝ่ายทรัพยากรสนับสนุนของผู้ให้บริการอินเทอร์เน็ตหรือผู้ผลิตเราเตอร์ของคุณเพื่อแก้ไขปัญหาด้านความปลอดภัยที่ตรวจพบ โปรดปฏิบัติตามข้อควรระวังด้านความปลอดภัยที่ระบุในคู่มือผู้ใช้เราเตอร์ของคุณเสมอ

การป้องกัน – หากต้องการป้องกันเราเตอร์และเครือข่ายของคุณจากการโจมตีการรักษาความปลอดภัยทางไซเบอร์ให้ทำตามคำแนะนำพื้นฐานต่อไปนี้

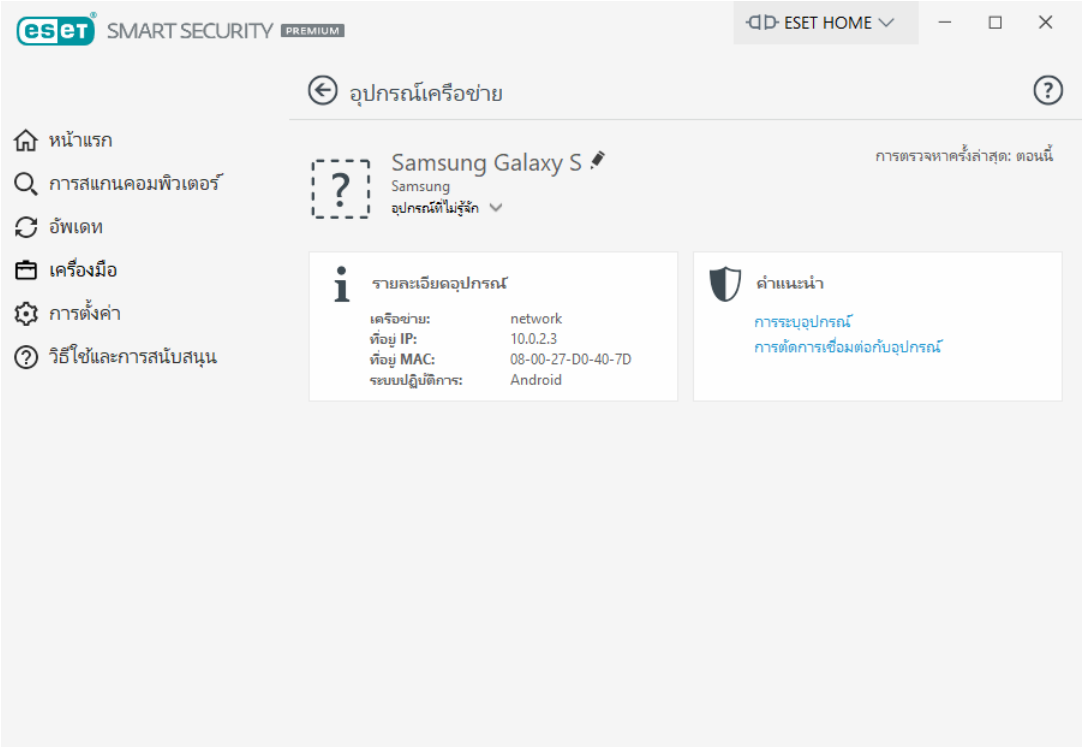


อุปกรณ์เครือข่าย

การระบุอุปกรณ์ – หากคุณไม่แน่ใจเรื่องอุปกรณ์ที่เชื่อมต่ออยู่กับเครือข่ายของคุณ ให้ตรวจสอบชื่อผู้ขายหรือผู้ผลิตด้านล่างชื่ออุปกรณ์ ซึ่งสามารถช่วยคุณในการระบุว่าอุปกรณ์ดังกล่าวเป็นอุปกรณ์ชนิดใด คุณสามารถเปลี่ยนชื่ออุปกรณ์เพื่อการอ้างอิงในอนาคตได้

การตัดการเชื่อมต่อกับอุปกรณ์ –หากคุณแน่ใจว่าอุปกรณ์ที่เชื่อมต่ออยู่นั้นปลอดภัยกับเครือข่ายหรืออุปกรณ์ของคุณหรือไม่ ให้จัดการการเข้าถึงเครือข่ายสำหรับอุปกรณ์นี้ในการตั้งค่าเราเตอร์หรือเปลี่ยนรหัสผ่านเครือข่ายของคุณ

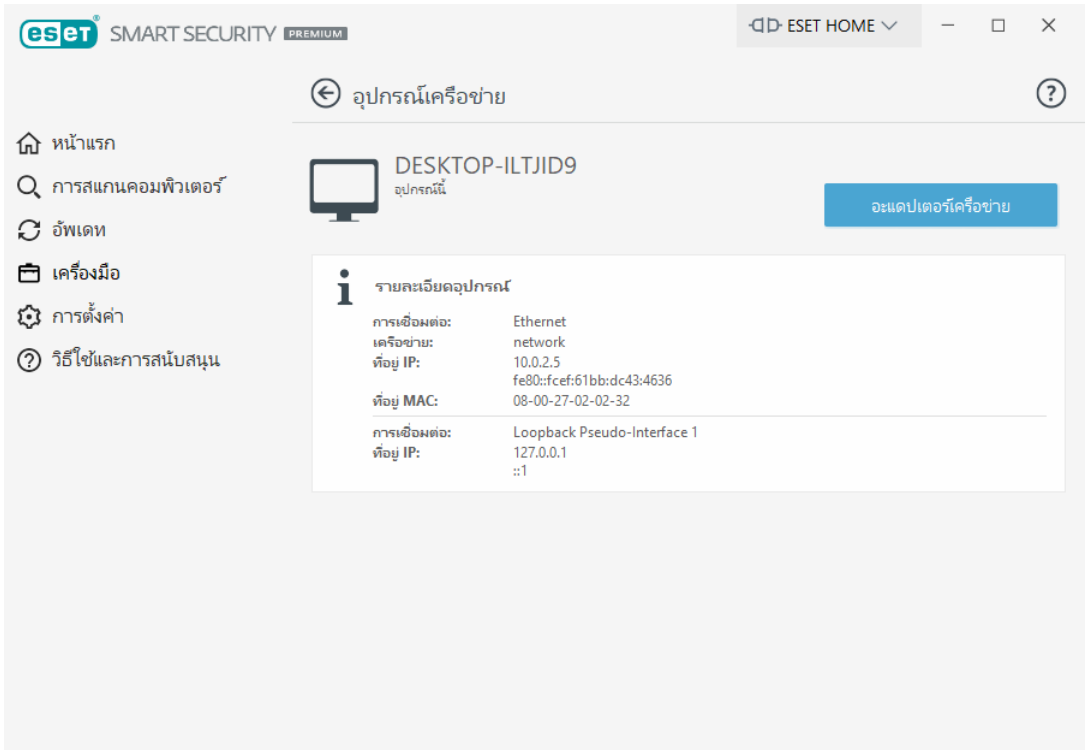
การป้องกัน – หากต้องการป้องกันอุปกรณ์ของคุณจากการโจมตีของซอฟต์แวร์ที่เป็นอันตราย โปรดติดตั้งการป้องกันการรักษาความปลอดภัยทางไซเบอร์บนอุปกรณ์ของคุณ และอัพเดทให้ระบบปฏิบัติการและซอฟต์แวร์ที่ติดตั้งทันสมัยอยู่เสมอ หากต้องการให้ได้รับการป้องกันต่อไป โปรดอย่าเชื่อมต่อกับเครือข่าย Wi-Fi ที่ไม่ปลอดภัย



อุปกรณ์นี้

อุปกรณ์นี้จะเป็นตัวแทนเครื่องคอมพิวเตอร์ของคุณบนเครือข่าย

อะแดปเตอร์เครือข่าย– แสดงข้อมูล อะแดปเตอร์เครือข่าย ของคุณ



การแจ้งเตือน | ตัวตรวจสอบเครือข่าย

ด้านล่างคือการแจ้งเตือนหลายรูปแบบที่อาจปรากฏเมื่อ ESET Smart Security Premium ตรวจพบปัญหาจุดอ่อนบนเราเตอร์ของคุณ การแจ้งเตือนแต่ละรายการจะมีคำอธิบายสั้นๆ และระบุวิธีการแก้ไขปัญหาหรือขั้นตอนที่ควรกระทำเพื่อลดความเสี่ยงด้านจุดอ่อนของเราเตอร์ของคุณ หากคุณไม่รู้จักการเปลี่ยนแปลงดังกล่าวของเราเตอร์ เราขอแนะนำให้ติดต่อผู้ผลิตเราเตอร์หรือผู้ให้บริการอินเทอร์เน็ตของคุณ

พบสิ่งที่อาจเป็นจุดอ่อน
เราเตอร์ของคุณอาจมีจุดอ่อนที่รู้จักซึ่งอาจง่ายต่อการถูกโจมตีและมุ่งใช้ประโยชน์ อัพเดทเฟิร์มแวร์ของเราเตอร์ของคุณ

พบจุดอ่อน
เราเตอร์ของคุณมีจุดอ่อนที่รู้จักซึ่งง่ายต่อการถูกโจมตีและมุ่งใช้ประโยชน์ อัพเดทเฟิร์มแวร์ของเราเตอร์ของคุณ

พบภัยคุกคาม
เราเตอร์ของคุณติดไวรัสจากมัลแวร์ รีสตาร์ทเราเตอร์ของคุณและทำการสแกนซ้ำ

รหัสผ่านเราเตอร์ที่มีความปลอดภัยต่ำ
รหัสผ่านบนเราเตอร์ของคุณมีความปลอดภัยต่ำ และบุคคลอื่นอาจคาดเดาได้ง่าย เปลี่ยนรหัสผ่านในเราเตอร์ของคุณ

การเปลี่ยนเส้นทางเครือข่ายที่เป็นอันตราย
การรับส่งของอินเทอร์เน็ตของคุณดูเหมือนจะเปลี่ยนเส้นทางไปยังเว็บไซต์ที่เป็นอันตราย ซึ่งอาจหมายความได้ว่าเราเตอร์ของคุณเกิดความหละหลวม เปลี่ยนการตั้งค่าเซิร์ฟเวอร์ DNS ในเราเตอร์ของคุณ

บริการเครือข่ายแบบเปิด
เราเตอร์ของคุณใช้งานบริการเครือข่ายโดยผู้อื่นที่อาจใช้งานอย่างไม่ถูกต้อง ซึ่งอาจเนื่องมาจากการกำหนดค่าที่ไม่ดีหรือเราเตอร์ไม่ปลอดภัย ตรวจสอบการกำหนดค่าของเราเตอร์ของคุณ

บริการเครือข่ายแบบเปิดที่ละเอียดอ่อน
เราเตอร์ของคุณใช้งานบริการเครือข่ายที่ละเอียดอ่อนซึ่งอาจถูกบุคคลอื่นมุ่งใช้ประโยชน์ ซึ่งอาจเนื่องมาจากการกำหนดค่าที่ไม่ดีหรือเราเตอร์ไม่ปลอดภัย ตรวจสอบการกำหนดค่าของเราเตอร์ของคุณ

เฟิร์มแวร์ล้าสมัย
เฟิร์มแวร์บนเราเตอร์ของคุณล้าสมัยและอาจมีจุดอ่อน อัพเดทเฟิร์มแวร์บนเราเตอร์ของคุณ

การตั้งค่าเราเตอร์ที่เป็นอันตราย
เซิร์ฟเวอร์ DNS ที่คุณใช้เป็นอันตรายและอาจส่งคุณไปยังเว็บไซต์ที่อันตราย ซึ่งอาจหมายความได้ว่าเราเตอร์ของคุณเกิดความหละหลวม เปลี่ยนการตั้งค่าเซิร์ฟเวอร์ DNS ในเราเตอร์ของคุณ

บริการเครือข่าย
เราเตอร์ของคุณใช้งานบริการเครือข่ายทั่วไป ซึ่งจำเป็นต่อเครือข่ายและอาจปลอดภัย ตรวจสอบการกำหนดค่าของเราเตอร์ของคุณ

เครื่องมือใน ESET Smart Security Premium

เมนู **เครื่องมือ** ประกอบด้วยโมดูลที่ช่วยให้การจัดการโปรแกรมง่ายขึ้นและมีตัวเลือกเพิ่มเติมสำหรับผู้ใช้ขั้นสูง เครื่องมือเหล่านี้จะปรากฏเมื่อคุณคลิก **เครื่องมือเพิ่มเติม** ตรงด้านขวาล่างเท่านั้น

เมนูนี้จะมีเครื่องมือต่อไปนี้:

ไฟล์บันทึก

รายงานด้านความปลอดภัย

กระบวนการที่ทำงานอยู่ (หาก ESET LiveGrid® ได้เปิดใช้อยู่ใน ESET Smart Security Premium)

การเชื่อมต่อเครือข่าย (หาก ไฟร์วอลล์ เปิดใช้งานอยู่ใน ESET Smart Security Premium)

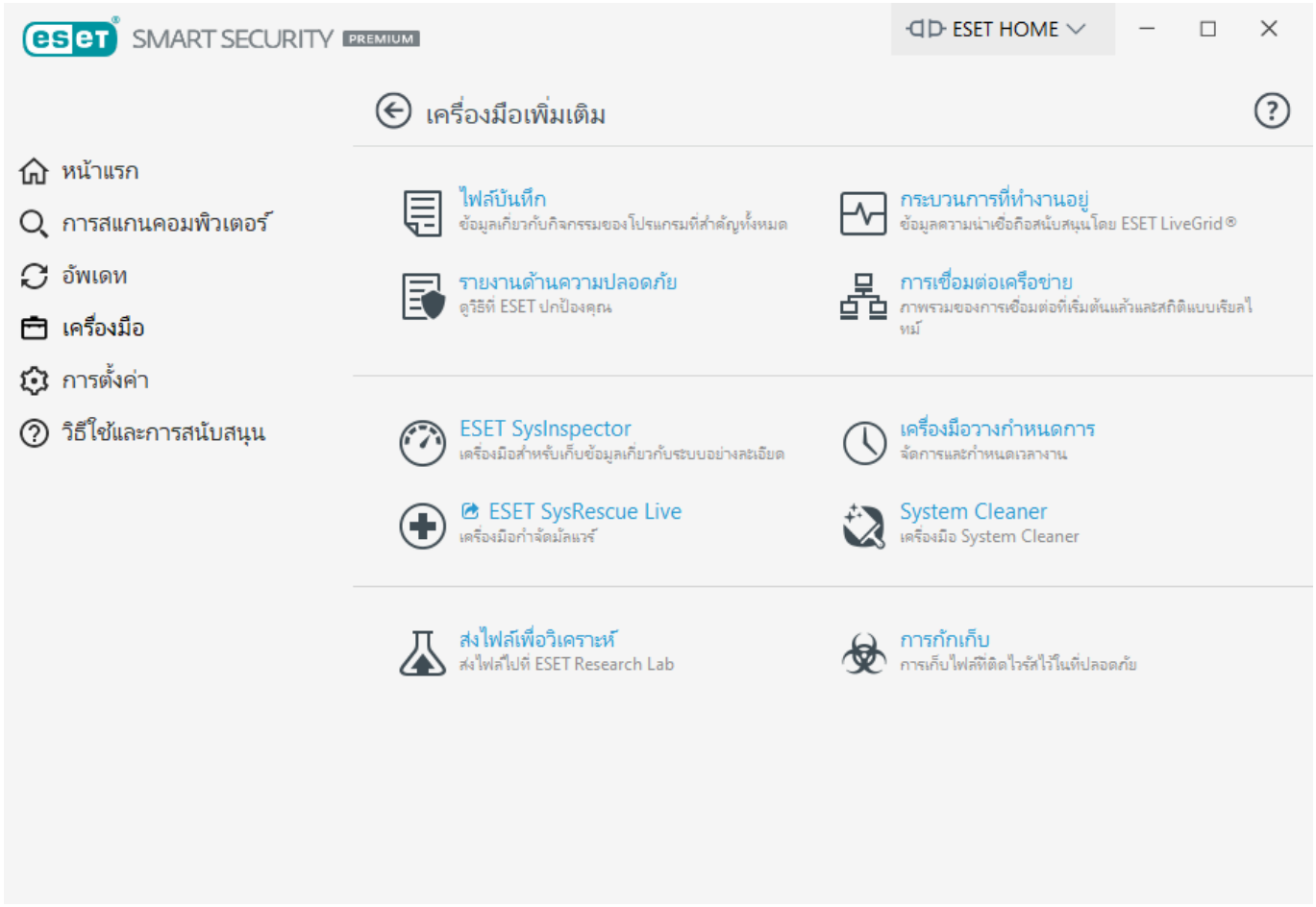
ESET SysInspector

ESET SysRescue Live – เปลี่ยนเส้นทางคุณไปยังเว็บไซต์ของ ESET SysRescue Live ที่คุณสามารถดาวน์โหลด ESET SysRescue Live .iso ผู้สร้างซีดี/ดีวีดี

เครื่องมือวางกำหนดการ

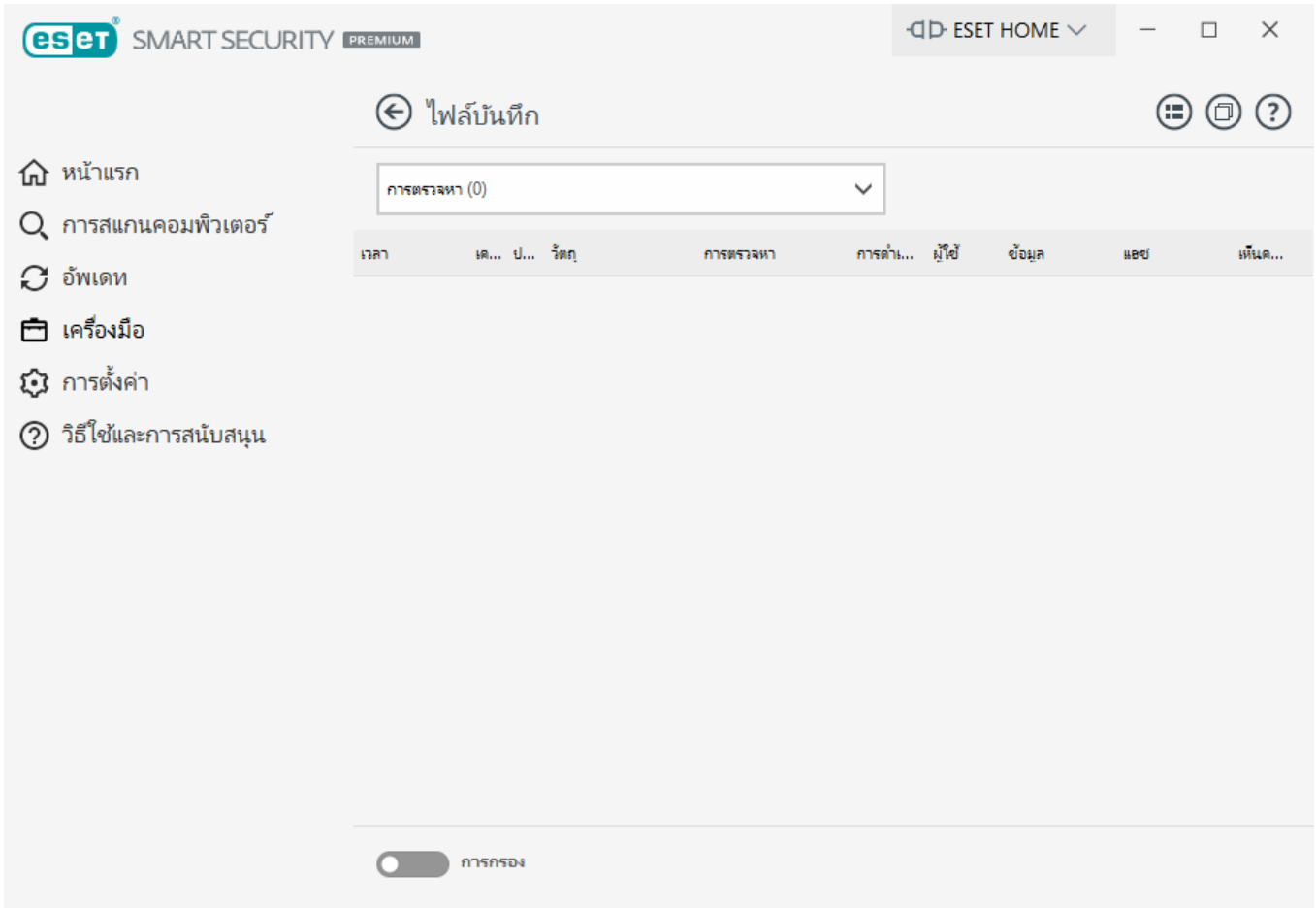
System Cleaner - ช่วยให้คุณเรียกคืนคอมพิวเตอร์ให้มีสถานะที่ใช้งานได้หลังจากกำจัดภัยคุกคาม

ส่งตัวอย่างเพื่อวิเคราะห์ – อนุญาตให้คุณส่งไฟล์ที่น่าสงสัยไปยังห้องปฏิบัติการวิจัยของ ESET เพื่อวิเคราะห์ (อาจไม่สามารถใช้งานได้ขึ้นอยู่กับการกำหนดค่าของ ESET LiveGrid®)



ไฟล์บันทึก

ไฟล์บันทึกประกอบด้วยข้อมูลเกี่ยวกับเหตุการณ์ของโปรแกรมที่สำคัญที่เกิดขึ้น และให้ภาพรวมของภัยคุกคามที่พบ การบันทึกเป็นส่วนที่จำเป็นในการวิเคราะห์ระบบ การตรวจหาภัยคุกคาม และการแก้ไขปัญหา การบันทึกนั้นดำเนินการในพื้นหลังโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ข้อมูลจะถูกบันทึกตามการตั้งค่าความละเอียดของการบันทึกปัจจุบัน ผู้ใช้สามารถดูข้อความและบันทึกได้โดยตรงจากระบบ ESET Smart Security Premium และสามารถอาร์ไคฟ์การบันทึกได้



ไฟล์บันทึกนั้นสามารถเข้าถึงได้จาก หน้าต่างโปรแกรมหลัก โดยคลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ไฟล์บันทึก**. เลือกประเภทการบันทึกที่ต้องการโดยใช้เมนูแบบเลื่อนลง **บันทึก** มีบันทึกที่ใช้ได้ดังต่อไปนี้:

• **การตรวจหา** บันทึกนี้จะให้ข้อมูลเกี่ยวกับการตรวจหาและการแฝงตัวที่ตรวจพบโดย ESET Smart Security Premium ข้อมูลบันทึกจะประกอบด้วยเวลาที่ตรวจพบ ประเภทเครื่องมือสแกน ประเภทวัตถุ ตำแหน่งของวัตถุ ชื่อของการตรวจหา การดำเนินการ และชื่อของผู้ใช้ที่เข้าสู่ระบบเมื่อการแฝงตัวถูกตรวจพบ แฮช และการปรากฏครั้งแรก การแฝงตัวที่ยังไม่ถูกกำจัดจะถูกทำเครื่องหมายด้วยข้อความสีแดงบนพื้นหลังสีแดงอ่อนเสมอ การแฝงตัวที่ถูกกำจัดแล้วจะถูกทำเครื่องหมายด้วยข้อความสีเหลืองบนพื้นหลังสีขาว PUA ที่ไม่ถูกกำจัดหรือแอปพลิเคชั่นที่อาจไม่ปลอดภัยถูกทำเครื่องหมายด้วยข้อความสีเหลืองบนพื้นหลังสีขาว

• **เหตุการณ์** – การทำงานที่สำคัญทั้งหมดซึ่งดำเนินการโดย ESET Smart Security Premium จะบันทึกไว้ในบันทึกเหตุการณ์ บันทึกเหตุการณ์จะมีข้อมูลเกี่ยวกับเหตุการณ์และข้อผิดพลาดที่เกิดขึ้นในโปรแกรม ตัวเลือกนี้ได้รับการออกแบบมาสำหรับผู้ดูแลระบบและผู้ใช้เพื่อแก้ไขปัญหา ข้อมูลที่พบในส่วนนี้มักจะช่วยให้คุณพบทางแก้ปัญหาที่เกิดขึ้นในโปรแกรม

• **การสแกนคอมพิวเตอร์** – ผลลัพธ์ของการสแกนครั้งก่อนหน้าทั้งหมดจะแสดงในหน้าต่างนี้ แต่ละบรรทัดจะแสดงถึงการควบคุมคอมพิวเตอร์หนึ่งรายการ คลิกสองครั้งที่รายการใดก็ได้เพื่อดูรายละเอียดของการสแกนที่เลือก

• **ไฟล์ที่ส่ง** - มีบันทึกของตัวอย่างที่ส่งไปยัง ESET LiveGuard

• **HIPS** - ประกอบไปด้วยบันทึกของกฎ HIPS เฉพาะซึ่งทำเครื่องหมายสำหรับการบันทึก โปรโตคอลแสดงแอพพลิเคชันที่เรียกใช้การทำงาน ผลลัพธ์ (ไม่ว่ากฎจะได้รับอนุญาตหรือถูกห้าม) และชื่อของกฎ

• **การป้องกันเครือข่าย** – บันทึกการป้องกันเครือข่าย จะแสดงการโจมตีระยะไกลทั้งหมดที่ตรวจพบโดยไฟร์วอลล์ การป้องกันการโจมตีเครือข่าย(IDS) และการป้องกันบอทเน็ต ในส่วนนี้คุณจะสามารถดูข้อมูลเกี่ยวกับการโจมตีทั้งหมดในคอมพิวเตอร์ของคุณ คอลัมน์ เหตุการณ์ แสดงการโจมตีที่ตรวจพบ คอลัมน์ ที่มา จะแจ้งให้คุณทราบเพิ่มเติมเกี่ยวกับผู้โจมตี คอลัมน์ โปรโตคอล จะเปิดเผยโปรโตคอลการสื่อสารที่ใช้สำหรับการโจมตี การวิเคราะห์ของการบันทึกการป้องกันเครือข่ายอาจช่วยคุณตรวจหาความพยายามในการแฝงตัวในระบบได้ทันเวลา สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการโจมตีทางเครือข่าย โปรดดูที่ IDS และตัวเลือกขั้นสูง

• **เว็บไซต์ที่กรอง** – รายการนี้จะมีประโยชน์ในกรณีที่คุณต้องการดูรายการเว็บไซต์ที่ถูกปิดกั้นโดย การป้องกันการเข้าถึงเว็บ หรือ การควบคุมเนื้อหา ในแต่ละบันทึกจะมีดูข้อมูลเวลา ที่อยู่ URL ผู้ใช้และแอพพลิเคชันที่สร้างการเชื่อมต่อกับเว็บไซต์หนึ่ง

• **การป้องกันสแปม** – มีบันทึกที่เกี่ยวข้องกับข้อความอีเมลที่ทำเครื่องหมายเป็นสแปม

• **การควบคุมเนื้อหา** - แสดงหน้าเว็บที่ถูกปิดกั้นหรืออนุญาตโดยการควบคุมเนื้อหา คอลัมน์ ประเภทการจับคู่ และ ค่าการจับคู่ จะบอกคุณว่ากฎการกรองนั้นใช้งานอย่างไร

• **การควบคุมอุปกรณ์** – มีบันทึกของสื่อหรืออุปกรณ์ที่ถอดเข้าออกได้ที่เชื่อมต่ออยู่กับคอมพิวเตอร์ เฉพาะอุปกรณ์ที่มีกฎการควบคุมอุปกรณ์ต่อไปนี้เท่านั้นที่จะถูกบันทึกลงในไฟล์บันทึก หากกฎไม่ตรงกับอุปกรณ์ที่เชื่อมต่อ จะไม่มีการสร้างรายการบันทึกสำหรับอุปกรณ์ที่เชื่อมต่อ และคุณยังสามารถดูรายละเอียดต่างๆ เช่น ประเภทอุปกรณ์ หมายเลขซีเรียล ชื่อผู้ขาย และขนาดของสื่อ (หากมี)

• **การป้องกัน Webcam** - ประกอบไปด้วยบันทึกเกี่ยวกับแอพพลิเคชั่นที่ถูกปิดกั้นโดยการป้องกัน Webcam

เลือกเนื้อหาของบันทึกใดก็ได้ แล้วกด **CTRL + C** เพื่อคัดลอกเนื้อหานั้นไปยังคลิปบอร์ด กด **CTRL** หรือ **SHIFT** ค้างไว้เพื่อเลือกหลายรายการ

คลิก **การกรอง** เพื่อเปิดหน้าต่าง การกรองบันทึก ที่ซึ่งคุณสามารถกำหนดเกณฑ์การกรองได้

คลิกขวาบนบันทึกใดบันทึกหนึ่งเพื่อเปิดเมนูบริบท ตัวเลือกต่อไปนี้จะสามารถใช้ได้ในเมนูบริบท:

• **แสดง** – แสดงข้อมูลโดยละเอียดยิ่งขึ้นเกี่ยวกับบันทึกที่เลือกในหน้าต่างใหม่

• **กรองบันทึกเดียวกัน** – หลังจากเปิดใช้งานตัวกรองนี้ คุณจะเห็นเฉพาะบันทึกประเภทเดียวกันเท่านั้น (การวินิจฉัย การเตือน เป็นต้น)

• **กรอง** – หลังจากคลิกตัวเลือกนี้ หน้าต่าง การกรองบันทึก จะอนุญาตให้คุณกำหนดเกณฑ์การกรองสำหรับรายการบันทึกที่ระบุ

• **เปิดใช้งานตัวกรอง** – เปิดใช้งานการตั้งค่าตัวกรอง

• **ปิดใช้งานการกรอง** - ล้างการตั้งค่าตัวกรองทั้งหมด (ดังที่อธิบายไว้ที่ด้านบน)

• **คัดลอก/คัดลอกทั้งหมด** – คัดลอกข้อมูลเกี่ยวกับบันทึกที่เลือกบนหน้าต่าง

• **ลบ/ลบทั้งหมด** – ลบบันทึกที่เลือกหรือบันทึกทั้งหมดที่ปรากฏ การดำเนินการนี้ต้องใช้สิทธิ์ของผู้ดูแลระบบ

• **ส่งออก/ส่งออกทั้งหมด** – ส่งออกข้อมูลเกี่ยวกับบันทึกที่เลือกหรือบันทึกทั้งหมดในรูปแบบ XML

• **ค้นหา/ค้นหาถัดไป/ค้นหาก่อนหน้า** – หลังจากคลิกตัวเลือกนี้ คุณสามารถกำหนดเกณฑ์การกรองโดยใช้หน้าต่างการกรองบันทึกเพื่อทำไฮไลต์รายการเฉพาะได้

• **คำอธิบายการตรวจหา** – เปิดสารานุกรมภัยคุกคามของ ESET ซึ่งมีข้อมูลโดยละเอียดเกี่ยวกับอันตรายและอาการของการแฝงตัวที่บันทึกไว้

• **สร้างการยกเว้น** – สร้าง การยกเว้นการตรวจหาโดยใช้วิซาร์ด (ไม่สามารถใช้งานได้กับการตรวจหามัลแวร์)

การกรองบันทึก

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

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

พิมพ์คำหลักที่คุณกำลังค้นหาในช่อง **ค้นหาข้อความ** ใช้เมนู **ค้นหาในคอลัมน์** แบบเลื่อนลงเพื่อค้นหาอย่างละเอียด เลือกหนึ่งในบันทึกจากเมนู **บันทึกประเภทของการบันทึก** แบบเลื่อนลง ระบุ**ช่วงเวลา** จากผลลัพธ์ที่คุณ

ต้องการแสดง 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

เปิดใช้งานตัวเลือกนี้ หากเป็นสำคัญสำหรับคุณเพื่อใช้ตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ในขณะที่กรองอยู่ เมื่อคุณกำหนดค่าตัวเลือกการกรอง/การค้นหาแล้ว ให้คลิก**ตกลง** เพื่อแสดงบันทึกการกรองหรือ**ค้นหา** เพื่อเริ่มการค้นหา ไฟล์บันทึกจะถูกค้นหาจากบนลงล่าง เริ่มจากตำแหน่งปัจจุบันของคุณ (บันทึกที่ถูกไฮไลท์) การค้นหาจะหยุดเมื่อค้นหาบันทึกที่ตรงกันอย่างแรก กด**F3** เพื่อค้นหาบันทึกถัดไปหรือคลิกขวา แล้วเลือก**ค้นหา** เพื่อระบุตัวเลือกการค้นหาของคุณอีกครั้ง

การกำหนดค่าการบันทึก

การกำหนดค่าการบันทึกของ ESET Smart Security Premium สามารถเข้าถึงได้จากหน้าต่างหลักของโปรแกรม คลิก **การตั้งค่า** > **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 (ข้อผิดพลาดในการเริ่มต้นการป้องกันไวรัสไฟร์วอลล์เป็นต้น)

การเชื่อมต่อที่ปิดกั้นจะบันทึกไว้เมื่อคุณเลือกระดับค่าความละเอียดของ การวินิจฉัย

รายการบันทึกที่เก่ากว่าจำนวนวันที่ระบุในช่อง **ลบอัตโนมัติสำหรับบันทึกที่เก่ากว่า (วัน)** จะถูกลบโดยอัตโนมัติ

ปรับปรุงประสิทธิภาพไฟล์บันทึกโดยอัตโนมัติ - หากทำเครื่องหมาย ไฟล์บันทึกจะถูกจัดระเบียบใหม่โดยอัตโนมัติ หากจำนวนเปอร์เซ็นต์สูงกว่าค่าที่ระบุในช่อง **ถ้าจำนวนบันทึกที่ไม่ได้ใช้งานเกิน (%)**

คลิก **ปรับปรุงประสิทธิภาพ** เพิ่มเริ่มต้นการจัดระเบียบบันทึกไฟล์ใหม่ รายการบันทึกที่ว่างเปล่าทั้งหมดจะถูกลบออกระหว่างกระบวนการนี้ ซึ่งช่วยปรับปรุงประสิทธิภาพและบันทึกความเร็วของการประมวลผล การปรับปรุงนี้จะเห็นได้ชัดโดยเฉพาะถ้าบันทึกมีรายการจำนวนมาก

เปิดใช้งานโปรโตคอลข้อความ เปิดใช้งานการบันทึกในรูปแบบอื่นแยกจาก ไฟล์บันทึก:

• **ไดเรกทอรีเป้าหมาย** - ไดเรกทอรีที่จะจัดเก็บไฟล์บันทึก (ใช้เฉพาะกับ Text/CSV) แต่ละส่วนบันทึกมีไฟล์และชื่อไฟล์ที่กำหนดไว้ล่วงหน้าเป็นของตัวเอง (ตัวอย่างเช่น virlog.txt สำหรับส่วน **การตรวจหา** ของไฟล์บันทึก ถ้าคุณใช้ไฟล์รูปแบบข้อความธรรมดาในการจัดเก็บบันทึก)

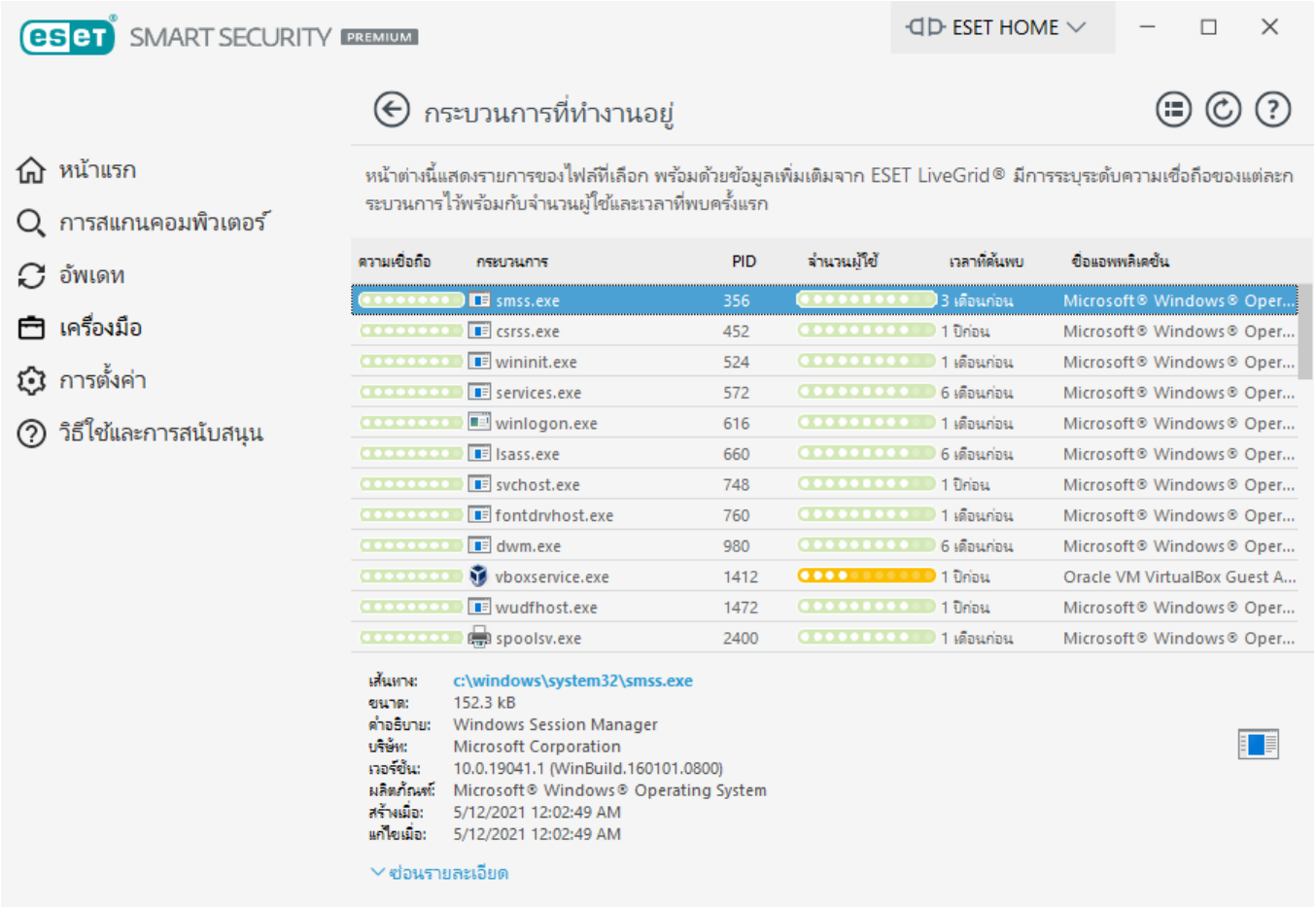
• **ประเภท** – ถ้าคุณเลือกรูปแบบไฟล์เป็น **ข้อความ** บันทึกจะจัดเก็บเป็นไฟล์ข้อความและข้อมูลจะคั่นด้วยแท็บต่างๆ การดำเนินการเดียวกันนี้ใช้เครื่องหมายจุลภาคเพื่อคั่นรูปแบบไฟล์ประเภท **CSV** ถ้าคุณเลือก **เหตุการณ์** การบันทึกจะจัดเก็บในบันทึก Windows Event (สามารถดูผ่าน Event Viewer ใน Control panel ได้) แทนที่จะเก็บไปยังไฟล์

• **ลบไฟล์บันทึกทั้งหมด** – ลบบันทึกที่เก็บไว้ทั้งหมดที่เลือกในปัจจุบันในเมนูแบบเลื่อนลง **ประเภท** การแจ้งเตือนเกี่ยวกับการลบบันทึกได้สำเร็จจะปรากฏขึ้น

i เพื่อให้สามารถแก้ไขปัญหาได้เร็วยิ่งขึ้น ESET อาจขอให้คุณมอบบันทึกจากคอมพิวเตอร์ของคุณ ESET Log Collector ช่วยให้คุณสามารถเก็บข้อมูลที่จำเป็นได้ง่ายยิ่งขึ้น สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ESET Log Collector โปรดไปที่ บทความฐานความรู้ ESET ของเรา

กระบวนการที่ทำงานอยู่

กระบวนการที่ทำงานอยู่จะแสดง โปรแกรมหรือกระบวนการ ที่ทำงานอยู่ในคอมพิวเตอร์ของคุณ และทำให้ ESET ได้รับรู้ข้อมูลเกี่ยวกับการบุกรุกใหม่ได้ทันทีและต่อเนื่อง ESET Smart Security Premium จะแสดงข้อมูลโดยละเอียดเกี่ยวกับกระบวนการที่ทำงานอยู่เพื่อคุ้มครองผู้ใช้ด้วยเทคโนโลยี ESET LiveGrid®



ความเชื่อถือ – ในกรณีส่วนใหญ่ ESET Smart Security Premium และเทคโนโลยี ESET LiveGrid® จะกำหนดระดับความเสี่ยงให้กับวัตถุ (ไฟล์ กระบวนการ รหัสรีจิสตรี เป็นต้น) โดยใช้ชุดกฎการวิเคราะห์พฤติกรรมที่ตรวจสอบลักษณะของวัตถุแต่ละรายการ จากนั้นจะชั่งน้ำหนักโอกาสที่จะเป็นกิจกรรมที่เป็นอันตราย จากการวิเคราะห์พฤติกรรมเหล่านี้ วัตถุจะได้รับการกำหนดระดับความเสี่ยงตั้งแต่ 1 – ดี (สีเขียว) จนถึง 9 – มีความเสี่ยง (สีแดง)

กระบวนการ – ชื่ออิมเมจของโปรแกรมหรือกระบวนการที่เรียกใช้อยู่บนคอมพิวเตอร์ของคุณในขณะนี้ คุณสามารถใช้โปรแกรมจัดการงาน Windows เมื่อต้องการดูกระบวนการทั้งหมดที่ทำงานอยู่บนคอมพิวเตอร์ เพื่อเปิดโปรแกรมจัดการงาน ให้คลิกขวาที่พื้นที่ว่างบนแถบงาน แล้วคลิก **โปรแกรมจัดการงาน** หรือกด **Ctrl+Shift+Esc** บนแป้นพิมพ์

i แอพพลิเคชันที่รู้จักและถูกทำเครื่องหมายเป็น ดี (สีเขียว) เพื่อแสดงว่ามีความปลอดภัย (อยู่ในรายการที่ปลอดภัย) และจะไม่รวมในการสแกนเพื่อปรับปรุงประสิทธิภาพ

PID - หมายเลขตัวบ่งชี้กระบวนการอาจถูกใช้เป็นพารามิเตอร์ในการเรียกฟังก์ชันต่างๆ เช่น การปรับลำดับความสำคัญของกระบวนการ

จำนวนผู้ใช้ – จำนวนผู้ใช้ที่ใช้แอพพลิเคชันที่ระบุ ข้อมูลนี้ได้รับการรวบรวมโดยเทคโนโลยี ESET LiveGrid®

เวลาที่ค้นพบ – ระยะเวลาตั้งแต่เทคโนโลยี ESET LiveGrid® ค้นพบแอพพลิเคชัน

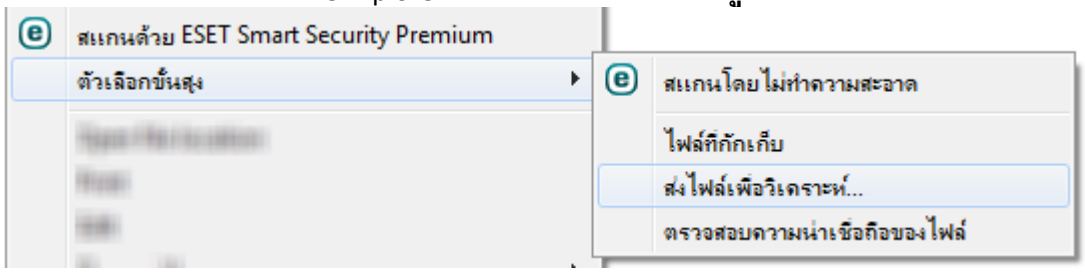
แอพพลิเคชันที่ถูกทำเครื่องหมายเป็น ไม่ทราบ (สีส้ม) ไม่ได้หมายความว่าจะเป็นซอฟต์แวร์ที่เป็นอันตรายเสมอไป โดยปกติแล้วจะเป็นแอพพลิเคชันใหม่ หากคุณไม่แน่ใจเกี่ยวกับไฟล์ คุณสามารถ ส่งไฟล์สำหรับการวิเคราะห์ ไปที่ ESET Research Lab หากตรวจพบว่าไฟล์เป็นแอพพลิเคชันที่เป็นอันตราย ข้อมูลการตรวจพบไฟล์นี้จะถูกเพิ่มในการอัพเดทที่กำลังจะมีขึ้น

ชื่อแอพพลิเคชัน – ชื่อที่กำหนดของโปรแกรมหรือกระบวนการ

คลิกที่แอพพลิเคชันหนึ่งเพื่อแสดงรายละเอียดต่อไปนี้ของแอพพลิเคชันดังกล่าว:

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

อีกทั้งคุณยังสามารถตรวจสอบความเชื่อถือในไฟล์ที่ไม่ได้เป็นโปรแกรม/กระบวนการที่ทำงานอยู่ หากต้องการทำเช่นนั้น ให้คลิกขวาใน File Explorer แล้วเลือก **ตัวเลือกขั้นสูง** > **ตรวจสอบความน่าเชื่อถือของไฟล์**



รายงานด้านความปลอดภัย

คุณลักษณะนี้จะให้ภาพรวมสถิติสำหรับประเภทต่อไปนี้:

- **หน้าเว็บที่ถูกปิดกั้น** – แสดงจำนวนหน้าเว็บที่ถูกปิดกั้น (URL ของ PUA ที่อยู่ในบัญชีดำ, ฟิชชิ่ง, เราเตอร์ที่ถูกเจาะระบบ, IP หรือใบรับรอง)
- **ตรวจพบวัตถุอีเมลติดไวรัส** – แสดงจำนวนวัตถุอีเมลติดไวรัสที่ตรวจพบ

• **หน้าเว็บในการควบคุมเนื้อหาเว็บไซต์ถูกบล็อก** – แสดงจำนวนหน้าเว็บที่ถูกบล็อกใน การควบคุมเนื้อหาเว็บไซต์

• **ตรวจพบ PUA** – แสดงจำนวนแอพพลิเคชันที่อาจไม่พึงประสงค์ (PUA)

• **ตรวจพบอีเมลสแปม** – แสดงจำนวนอีเมลสแปมที่ตรวจพบ

• **การเข้าถึงเว็บแคมถูกปิดกั้น** – แสดงจำนวนการเข้าถึงเว็บแคมที่ถูกปิดกั้น

• **การเชื่อมต่อบริการธนาคารผ่านอินเทอร์เน็ตที่ได้รับการปกป้อง** – แสดงจำนวนการเข้าถึงบริการธนาคารผ่านอินเทอร์เน็ตที่ถูกปิดกั้นผ่านคุณสมบัติการป้องกันการธนาคารและการชำระเงิน

• **ตรวจสอบเอกสารต่างๆ แล้ว** – แสดงจำนวนวัตถุเอกสารที่สแกนแล้ว

• **สแกนแอพพลิเคชันแล้ว** – แสดงจำนวนวัตถุที่สามารถเรียกใช้ที่สแกนแล้วได้

• **ตรวจวัตถุต่างๆ แล้ว** – แสดงจำนวนวัตถุอื่นๆ ที่สแกนแล้ว

• **สแกนวัตถุหน้าเว็บแล้ว** – แสดงจำนวนวัตถุหน้าเว็บที่สแกนแล้ว

• **สแกนวัตถุอีเมลแล้ว** – แสดงจำนวนวัตถุอีเมลที่สแกนแล้ว

• **ไฟล์ที่วิเคราะห์โดย ESET LiveGuard** – แสดงจำนวนตัวอย่างที่วิเคราะห์โดย ESET LiveGuard

ลำดับของประเภทเหล่านี้จะเป็นไปตามค่าตัวเลขจากสูงสุดไปต่ำสุด ประเภทที่มีค่าเป็นศูนย์จะไม่ถูกแสดง คลิก **แสดงเพิ่มขึ้น** เพื่อขยายและแสดงประเภทที่ซ่อนอยู่

คุณสามารถเปิดใช้งานคุณลักษณะต่อไปนี้ในส่วนสุดท้ายของรายงานด้านความปลอดภัยได้:

• ESET LiveGuard

• Secure Data

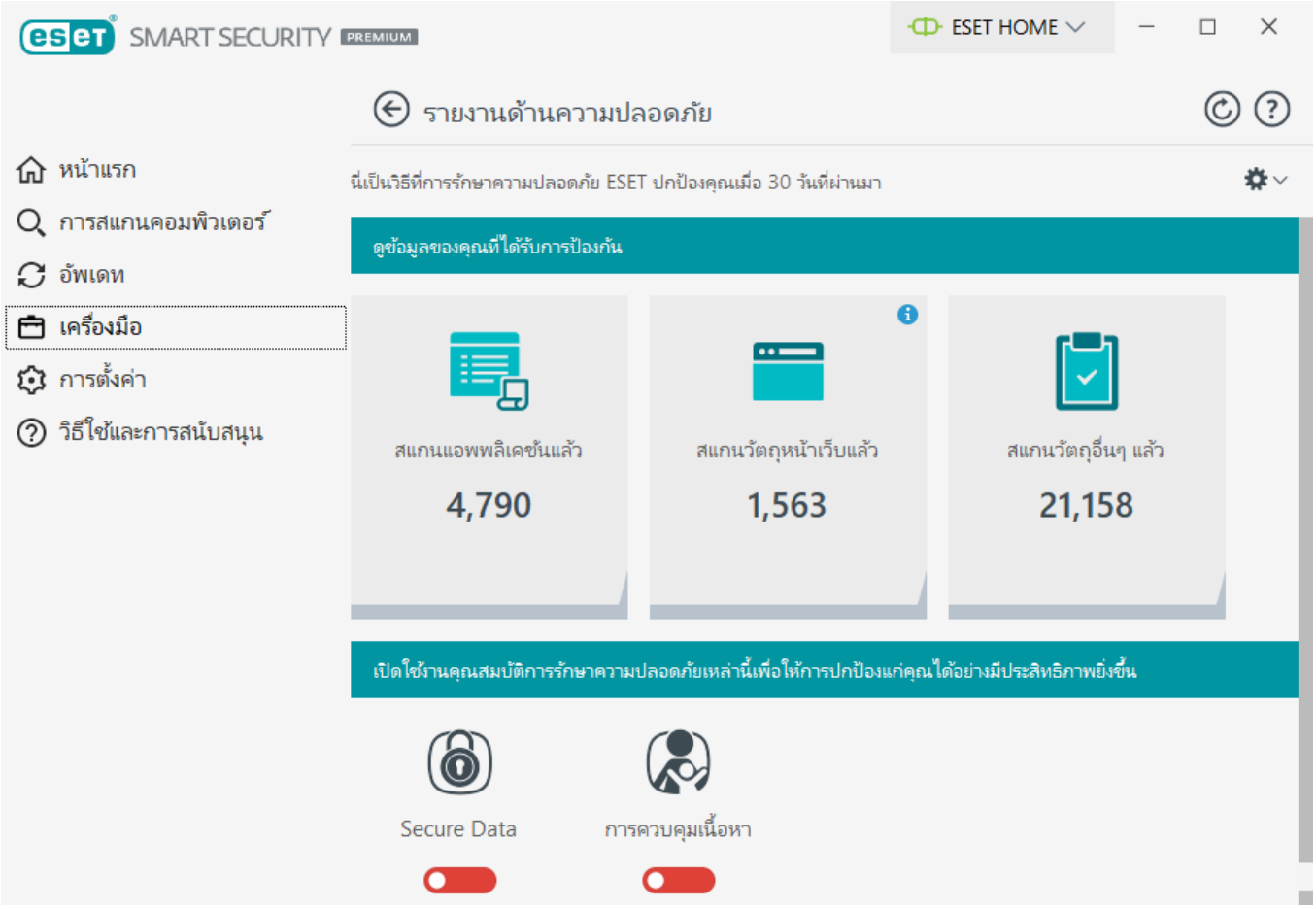
• การควบคุมเนื้อหา

• การป้องกันการโจรกรรม

เมื่อคุณลักษณะนี้ถูกเปิดใช้งาน คุณลักษณะดังกล่าวจะไม่แสดงเป็นไม่ทำงานในรายงานด้านความปลอดภัยอีกต่อไป

เมื่อคลิกที่ล้อเฟือง⚙ ที่มุมขวาบน คุณจะสามารถ **เปิด/ปิดใช้งานการแจ้งเตือนรายงานด้านความปลอดภัย** หรือเลือกว่าจะให้โปรแกรมแสดงข้อมูลจาก 30 วันที่ผ่านมาหรือนับจากที่คุณเริ่มเปิดใช้งานผลิตภัณฑ์ได้ หากคุณติด

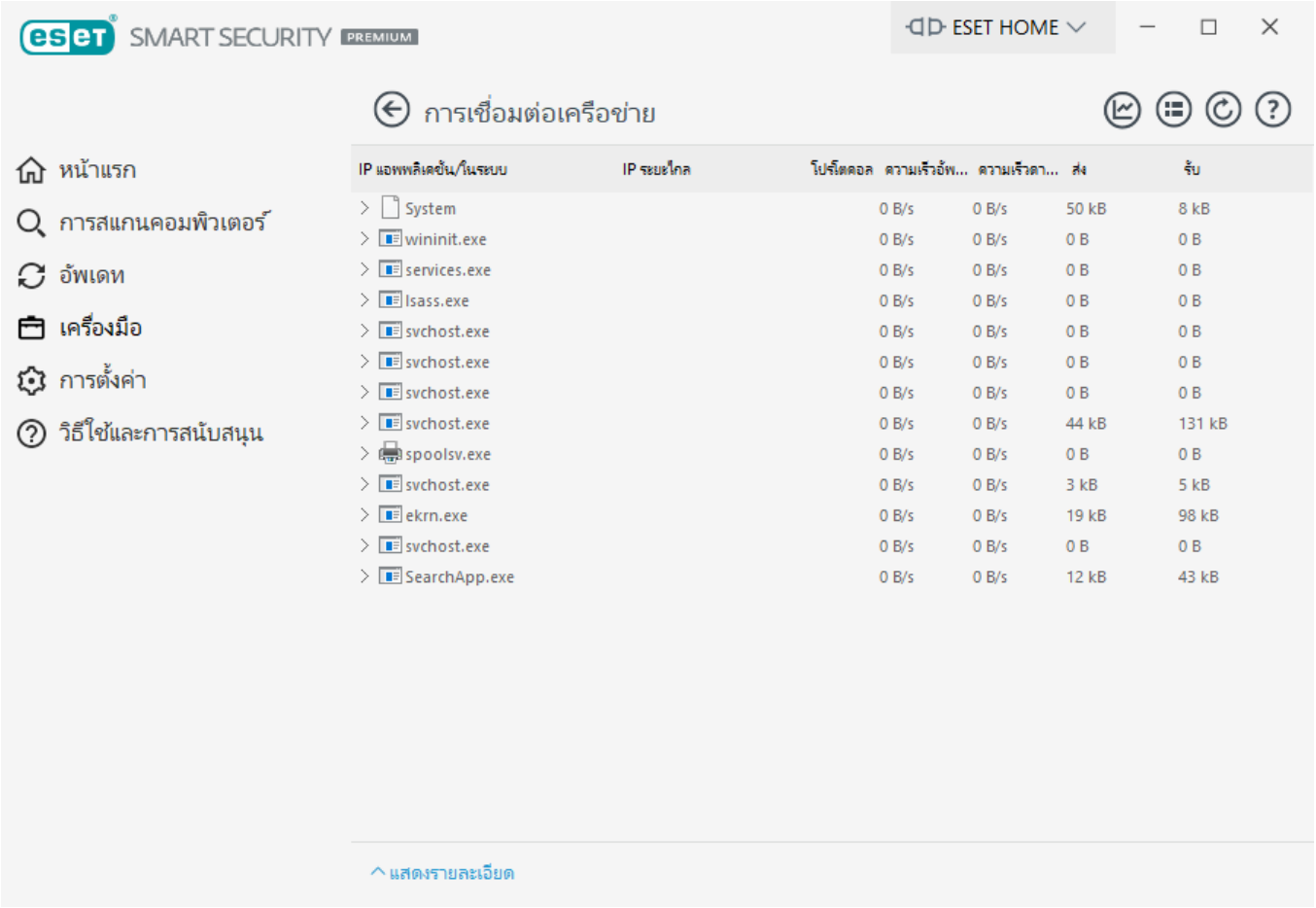
ตั้ง ESET Smart Security Premium เป็นเวลาน้อยกว่า 30 วัน คุณจะสามารถเลือกจำนวนวันนับจากที่คุณเริ่มติดตั้งผลิตภัณฑ์ได้เท่านั้น ช่วงเวลา 30 วันจะถูกเลือกตามค่าเริ่มต้น



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

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

คลิกขวาที่การเชื่อมต่อเพื่อดูตัวเลือกอื่นๆ ที่มีอยู่:

แปลค่าชื่อโฮสต์ – ถ้าเป็นไปได้ ที่อยู่เครือข่ายทั้งหมดจะแสดงในรูปแบบ DNS ไม่ใช่ในรูปแบบที่อยู่ IP ที่เป็นตัวเลข

แสดงเฉพาะการเชื่อมต่อ TCP – รายการจะแสดงเฉพาะการเชื่อมต่อที่อยู่ในชุดโปรโตคอล TCP

แสดงการเชื่อมต่อของรายชื่อ – เลือกตัวเลือกนี้เพื่อแสดงเฉพาะการเชื่อมต่อที่ยังไม่ได้เริ่มต้นการสื่อสาร แต่ระบบได้เปิดพอร์ตและกำลังรอการเชื่อมต่ออยู่

แสดงการเชื่อมต่อภายในคอมพิวเตอร์ – เลือกตัวเลือกนี้เพื่อแสดงเฉพาะการเชื่อมต่อที่คอมพิวเตอร์ระยะไกลเป็นระบบภายใน หรือเรียกว่าการเชื่อมต่อ localhost

ความเร็วในการรีเฟรช – เลือกความถี่ในการรีเฟรชการเชื่อมต่อที่ใช้งาน

รีเฟรชทันที – โหลดหน้าต่าง **การเชื่อมต่อในเครือข่าย** อีกครั้ง

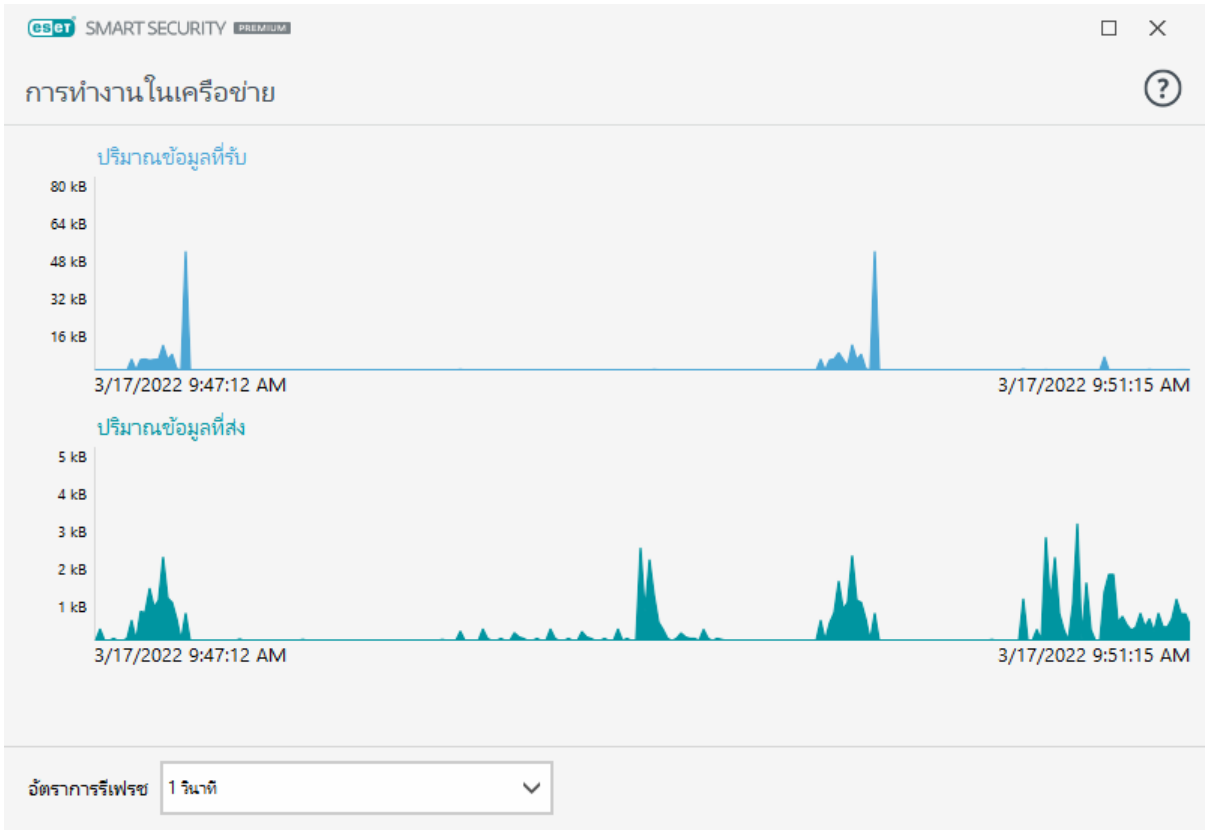
ตัวเลือกต่อไปนี้จะสามารถใช้ได้หลังจากคลิกแอพพลิเคชันหรือกระบวนการเท่านั้น ไม่ใช่คลิกที่การเชื่อมต่อที่ใช้งาน:

ปฏิเสธการสื่อสารสำหรับกระบวนการชั่วคราว – ปฏิเสธการเชื่อมต่อปัจจุบันสำหรับแอพพลิเคชันที่ระบุ ถ้าเริ่มต้นการเชื่อมต่อใหม่แล้ว ไฟร์วอลล์จะใช้กฎที่กำหนดไว้ล่วงหน้า คุณสามารถดูคำอธิบายของการตั้งค่าในส่วน การกำหนดค่าและการใช้กฎ ได้

อนุญาตการสื่อสารสำหรับกระบวนการชั่วคราว – อนุญาตการเชื่อมต่อปัจจุบันสำหรับแอพพลิเคชันที่ระบุ ถ้าเริ่มต้นการเชื่อมต่อใหม่แล้ว ไฟร์วอลล์จะใช้กฎที่กำหนดไว้ล่วงหน้า คุณสามารถดูคำอธิบายของการตั้งค่าในส่วน การกำหนดค่าและการใช้กฎ ได้

การทำงานในเครือข่าย

หากต้องการดู **กิจกรรมเครือข่าย** ปัจจุบันในรูปแบบกราฟ ให้คลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **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

• **เปรียบเทียบ** – เปรียบเทียบบันทึกสองรายการที่มีอยู่

• **สร้าง** – สร้างบันทึกใหม่ รอจนกระทั่ง ESET SysInspector ถูกสร้างขึ้น (สถานะ **สร้างแล้ว**) ก่อนพยายามเข้าถึงบันทึก

• **ลบ** – ลบบันทึกที่เลือกออกจากรายการ

รายการต่อไปนี้จะนำมาใช้ได้จากเมนูบริบทเมื่อเลือกไฟล์บันทึกหนึ่งไฟล์หรือหลายไฟล์:

• **แสดง** – เปิดบันทึกที่เลือกใน ESET SysInspector (ทำงานเช่นเดียวกับการคลิกสองครั้งที่บันทึก)

• **เปรียบเทียบ** – เปรียบเทียบบันทึกสองรายการที่มีอยู่

• **สร้าง** – สร้างบันทึกใหม่ รอจนกระทั่ง ESET SysInspector ถูกสร้างขึ้น (สถานะ **สร้างแล้ว**) ก่อนพยายามเข้าถึงบันทึก

• **ลบ** – ลบบันทึกที่เลือกออกจากรายการ

• **ลบทั้งหมด** – ลบบันทึกทั้งหมด

• **ส่งออก** – ส่งออกบันทึกไปยังไฟล์ .xml หรือ .xml ที่บีบอัด บันทึกจะถูกส่งออกไปยัง C:\ProgramData\ESET\ESET Security\SysInspector

เครื่องมือวางกำหนดการ

เครื่องมือวางกำหนดการจะจัดการและเรียกใช้งานตามกำหนดการโดยใช้การกำหนดค่าและคุณสมบัติที่กำหนดไว้ล่วงหน้า

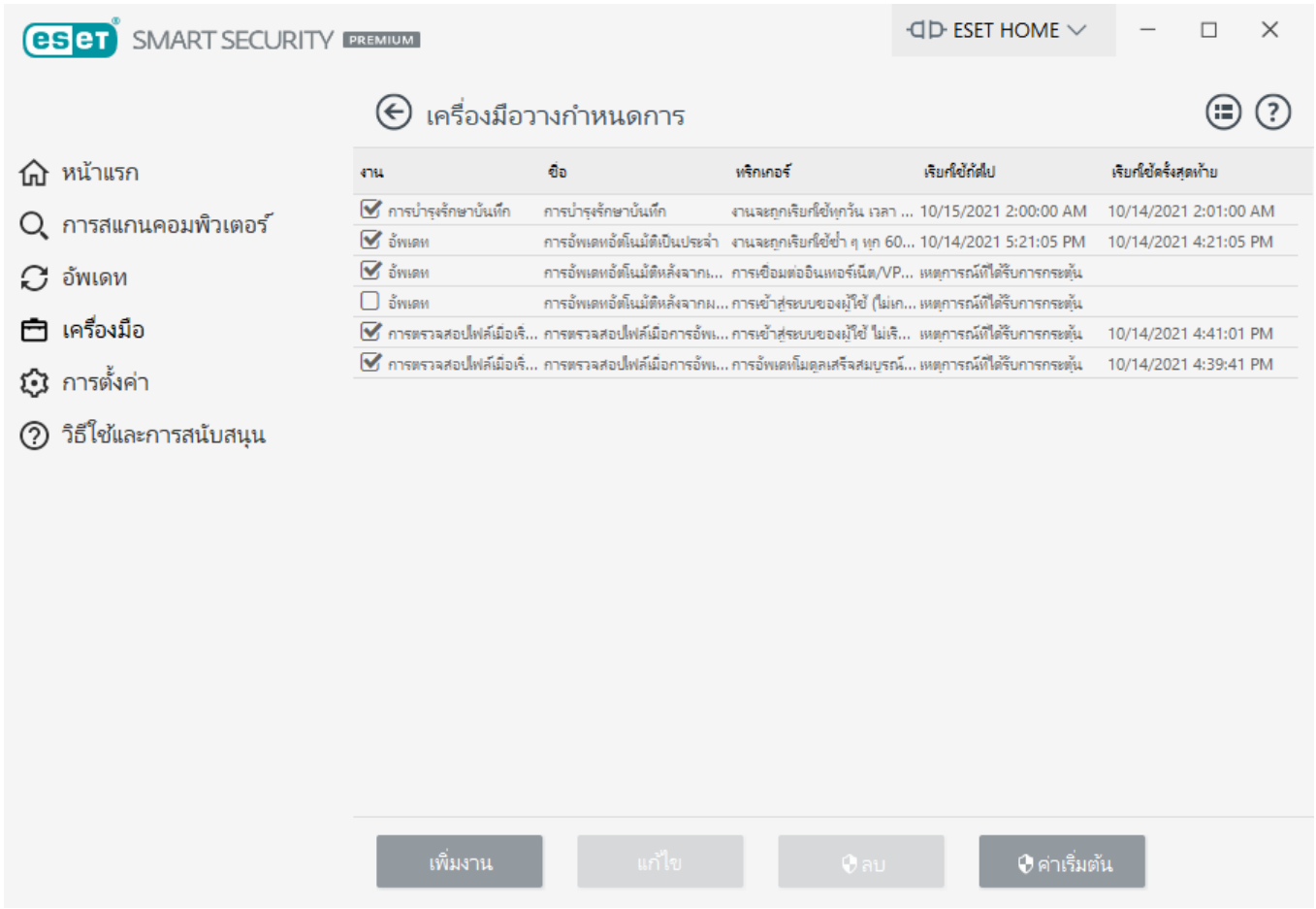
เครื่องมือวางกำหนดการณ์นั้นสามารถเข้าถึงได้จาก หน้าต่างโปรแกรมหลัก ของ ESET Smart Security Premium โดยคลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **เครื่องมือวางกำหนดการณ์ เครื่องมือวางกำหนดการณ์** มีรายการงานตามกำหนดการทั้งหมด และคุณสมบัติของการกำหนดค่า เช่น วันที่ที่กำหนดไว้ล่วงหน้า เวลา และโปรไฟล์การสแกนที่ใช้

เครื่องมือวางกำหนดการจะทำหน้าที่ในการวางกำหนดการงานต่อไปนี้: การอัพเดทโมดูล การสแกนงาน การตรวจสอบไฟล์การเริ่มต้นของระบบ และการบำรุงรักษาบันทึก คุณสามารถเพิ่มหรือลบงานได้โดยตรงจากหน้าต่างของเครื่องมือวางกำหนดการหลัก (คลิก **เพิ่มงาน** หรือ **ลบ** ที่ส่วนล่างของหน้าต่าง) คุณสามารถคืนค่ารายการงานตามกำหนดการเป็นค่าเริ่มต้นและลบการเปลี่ยนแปลงทั้งหมดโดยคลิก **ค่าเริ่มต้น** คลิกขวาที่ใดก็ได้ในหน้าต่างของเครื่องมือวางกำหนดการเพื่อดำเนินการดังต่อไปนี้: แสดงข้อมูลเป็นรายละเอียด ทำงานทันที เพิ่มงานใหม่ และลบงานที่มีอยู่ ใช้ช่องทำเครื่องหมายที่ด้านหน้าของแต่ละรายการเพื่อเปิด/ปิดการทำงาน

ตามค่าเริ่มต้น งานตามกำหนดการต่อไปนี้จะปรากฏใน **เครื่องมือวางกำหนดการ**:

- **การบำรุงรักษาการบันทึก**
- **การอัพเดทอัตโนมัติเป็นประจำ**
- **การอัพเดทอัตโนมัติหลังจากเชื่อมต่อผ่านหมายเลขโทรศัพท์**
- **การอัพเดทอัตโนมัติหลังจากผู้ใช้เข้าสู่ระบบ**
- **การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้น** (หลังจากการเข้าสู่ระบบของผู้ใช้)
- **การตรวจสอบไฟล์เมื่อเริ่มต้น** (หลังจากการอัพเดทกลไกตรวจหาเสร็จสมบูรณ์)

หากต้องการแก้ไขการกำหนดค่าของงานตามกำหนดการที่มีอยู่ (ทั้งค่าเริ่มต้นและที่ผู้ใช้กำหนด) ให้คลิกขวาที่งานแล้วคลิก **แก้ไข** หรือเลือกงานที่คุณต้องการแก้ไขแล้วคลิก **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** – วางกำหนดการงานการอัพเดทโดยการอัพเดทโมดูลเหล่านี้

4. เปิดแถบเลื่อนถัดจาก **เปิดใช้งาน** เพื่อเปิดใช้งานนี้ (คุณสามารถดำเนินการในภายหลังได้ด้วยการเลือก /ยกเลิกการเลือกกล่องทำเครื่องมือวางกำหนดการณ์) ให้คลิก **ถัดไป** และเลือกหนึ่งในตัวเลือกเวลา:

• **หนึ่งครั้ง** – งานจะดำเนินการตามวันและเวลาที่กำหนดไว้ล่วงหน้า

• **ซ้ำ** – งานจะดำเนินการตามระยะเวลาที่กำหนด

• **รายวัน** – งานจะเรียกใช้ซ้ำทุกวันตามเวลาที่กำหนด

• **รายสัปดาห์** – งานจะเรียกใช้ตามวันที่และเวลาที่เลือก

• **ตามเหตุการณ์** – งานจะดำเนินการตามเหตุการณ์ที่กำหนด

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

• **เมื่อเวลาที่กำหนดไว้ครั้งต่อไป**

• **เร็วที่สุดเท่าที่ทำได้**

• **ทันที หากระยะเวลาตั้งแต่เรียกใช้ครั้งล่าสุดเกิน (ชั่วโมง)** – หมายถึงเวลาที่ผ่านไปนับตั้งแต่ข้ามการเรียกใช้งานนี้เป็นครั้งแรก หากเกินเวลานี้ งานจะดำเนินการทันที ตั้งเวลาโดยใช้ตัวหมุนด้านล่าง

คุณสามารถดูงานตามกำหนดการด้วยการคลิกขวาแล้วคลิก **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) และประเมิน

ระดับความเสี่ยงขององค์ประกอบแต่ละรายการ

• **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.

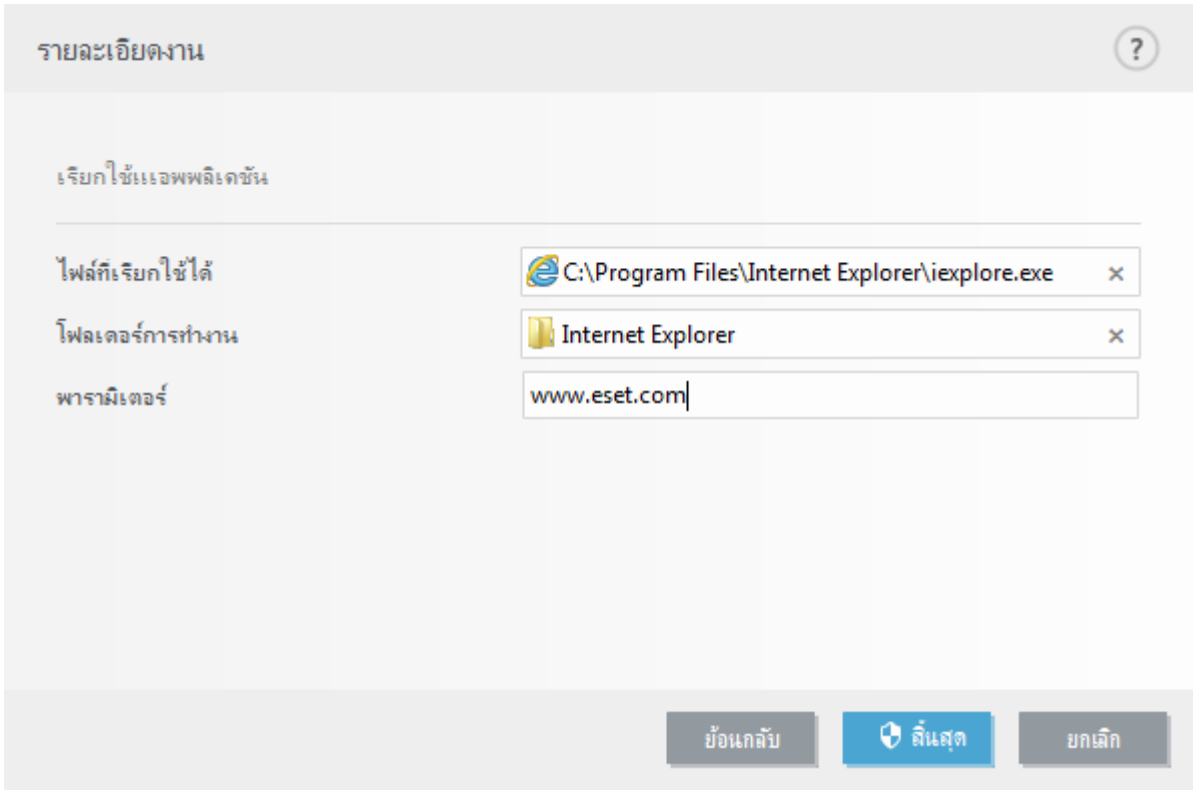
• คอมพิวเตอร์จะตื่นขึ้นในเวลา 16:30 น. การข้ามการเรียกใช้ครั้งแรกเกิดขึ้นเมื่อเวลา 14:00 น. เวลาผ่านไปสองชั่วโมงครึ่งนับตั้งแต่ 14:00 น. ดังนั้นงานจะดำเนินการทันที

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 **ไฟล์ที่เรียกใช้ได้** ที่เลือกไว้จะสร้างขึ้นภายในไดเรกทอรีนี้

พารามิเตอร์ – พารามิเตอร์ของบรรทัดคำสั่งสำหรับแอพพลิเคชัน (ไม่จำเป็น)

คลิก **สิ้นสุด** เพื่อใช้งาน

เครื่องมือทำความสะอาดระบบ

เครื่องมือทำความสะอาดระบบเป็นเครื่องมือที่จะช่วยให้คุณกู้คืนคอมพิวเตอร์ให้อยู่ในสภาพที่ใช้งานได้หลังจากกำจัดภัยคุกคามแล้ว มัลแวร์สามารถปิดใช้งานโปรแกรมอรรถประโยชน์ของระบบได้ เช่น Registry Editor, โปรแกรมจัดการงาน หรือการอัพเดท Windows เครื่องมือทำความสะอาดระบบจะกู้คืนค่าและการตั้งค่าเริ่มต้นของระบบดังกล่าวด้วยการคลิกเพียงครั้งเดียว

เครื่องมือทำความสะอาดระบบจะรายงานปัญหาจากประเภทการตั้งค่าห้าประเภท:

- **การตั้งค่าการรักษาความปลอดภัย**: การเปลี่ยนแปลงการตั้งค่าซึ่งอาจเพิ่มจุดอ่อนให้กับคอมพิวเตอร์ของคุณ เช่น Windows Update

- **การตั้งค่าระบบ**: การเปลี่ยนแปลงการตั้งค่าระบบซึ่งสามารถเปลี่ยนแปลงการทำงานของคอมพิวเตอร์ของคุณได้ เช่น การเชื่อมโยงไฟล์
- **ลักษณะที่ปรากฏของระบบ**: การตั้งค่าที่เปลี่ยนรูปลักษณ์ของระบบของคุณ เช่น ภาพพื้นหลังเดสก์ท็อป
- **คุณลักษณะที่ถูกปิดใช้งาน**: คุณลักษณะและแอพพลิเคชันที่สำคัญที่อาจถูกปิดใช้งาน
- **Windows System Restore**: การตั้งค่าสำหรับคุณลักษณะ Windows System Restore ซึ่งอนุญาตให้คุณคืนค่าระบบของคุณเป็นสถานะก่อนหน้านี้

สามารถเรียกใช้เครื่องมือกำจัดไวรัสในระบบได้เมื่อ:

- พบภัยคุกคาม
- ผู้ใช้คลิก **รีเซ็ต**

คุณสามารถตรวจสอบการเปลี่ยนแปลงและรีเซ็ตการตั้งค่าได้หากเหมาะสม

เฉพาะผู้ใช้ที่มีสิทธิ์ของผู้ดูแลระบบที่สามารถดำเนินการในเครื่องมือทำความสะอาดระบบได้

ESET SysRescue Live

ESET SysRescue Live คือยูทิลีตีแบบฟรีที่ช่วยให้คุณสามารถสร้างซีดี/ดีวีดีกู้คืนที่สามารถบูตได้หรือไดรฟ์ USB โดยคุณสามารถบูตคอมพิวเตอร์ที่ติดไวรัสได้จากสื่อกู้คืนเพื่อสแกนหามัลแวร์และกำจัดไฟล์ที่ติดไวรัสได้

ประโยชน์หลักของ ESET SysRescue Live คือข้อเท็จจริงที่ว่าสามารถทำงานเป็นอิสระจากระบบปฏิบัติการโฮสต์ แต่มีสิทธิ์เข้าถึงดิสก์และระบบไฟล์ได้โดยตรง ซึ่งทำให้สามารถลบภัยคุกคามที่ภายใต้เงื่อนไขการปฏิบัติการปกติไม่สามารถทำได้ (ตัวอย่างเช่น เมื่อระบบปฏิบัติการกำลังทำงานอยู่ เป็นต้น)

- ความช่วยเหลือออนไลน์สำหรับ ESET SysRescue Live

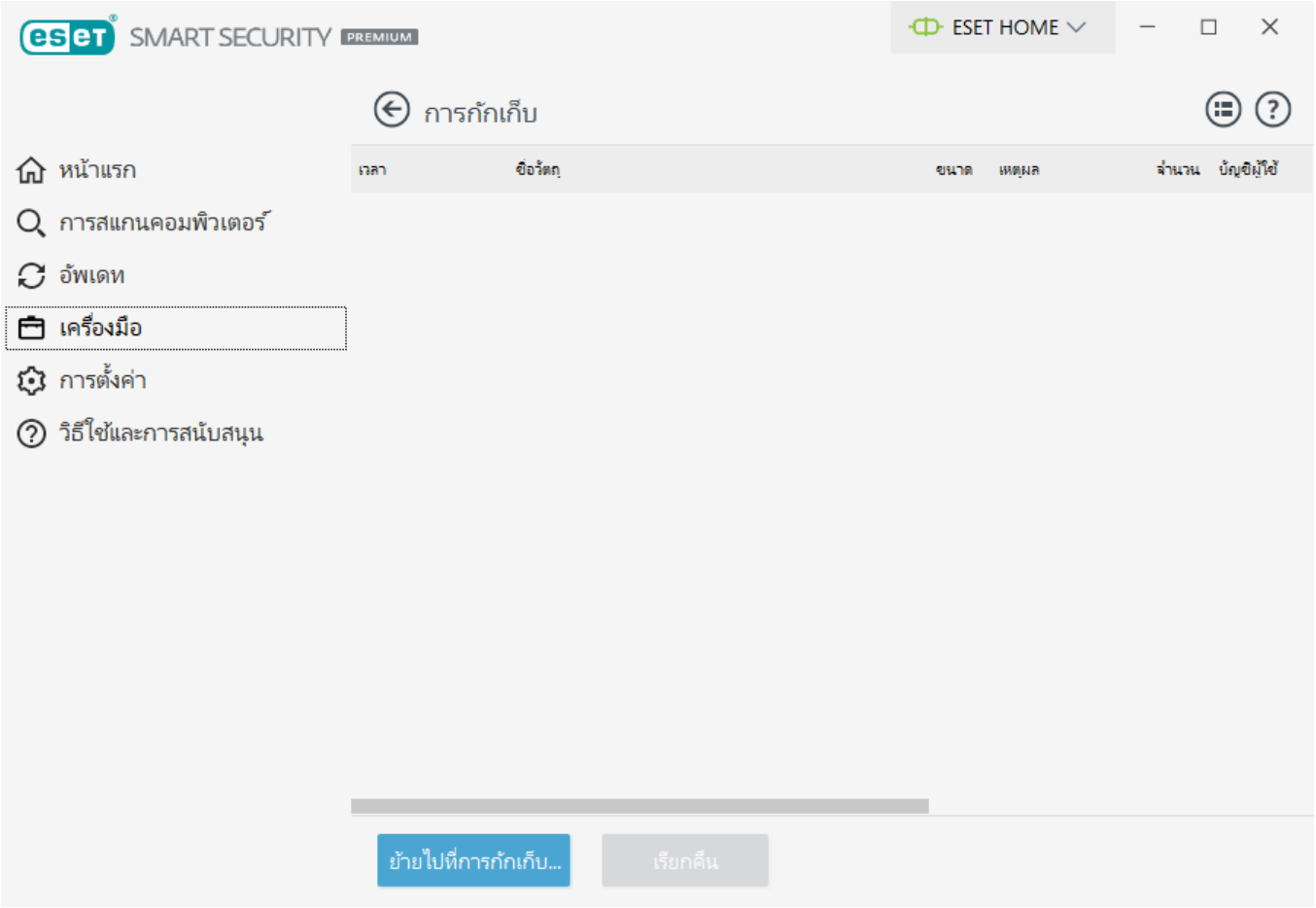
กักเก็บ

ฟังก์ชันหลักของการกักเก็บคือการจัดเก็บวัตถุที่มีการรายงานไว้อย่างปลอดภัย (เช่น มัลแวร์ ไฟล์ที่ติดไวรัสหรือแอปพลิเคชั่นที่อาจไม่พึงประสงค์)

การกักเก็บนั้นสามารถเข้าถึงได้จากหน้าต่างโปรแกรมหลัก ESET Smart Security Premium โดยการคลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **การกักเก็บ**

ไฟล์ที่เก็บไว้ในโฟลเดอร์กักเก็บนั้นสามารถดูได้ในตารางที่แสดง:

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



การกักเก็บไฟล์

ESET Smart Security Premium จะกักเก็บไฟล์ที่ลบโดยอัตโนมัติ (หากคุณไม่ได้ยกเลิกตัวเลือกนี้ใน หน้าต่างเตือนภัย)

ไฟล์เพิ่มเติมที่ควรถูกกักเก็บหาก:

a.ไม่สามารถกำจัดได้

b.หากเป็นไฟล์ที่ไม่ปลอดภัยหรือระบบแนะนำให้ลบ

c.หากมีการตรวจพบด้วยความผิดพลาดโดย ESET Smart Security Premium

d.หากไฟล์ทำงานน่าสงสัยแต่ไม่มีการตรวจพบโดย เครื่องมือสแกน

คุณมีตัวเลือกหลายประการในการกักเก็บไฟล์:

a.คุณสามารถใช้คุณสมบัติลากและวางเพื่อกักเก็บไฟล์ด้วยตัวเองได้ โดยให้คลิกที่ไฟล์หรือโฟลเดอร์ แล้วเลื่อนตัวชี้เมาส์ไปยังบริเวณที่ทำเครื่องหมายขณะที่กดปุ่มเมาส์ค้างไว้ จากนั้นจึงปล่อยนิ้ว หลังจากนั้น

แอพพลิเคชันจะเลื่อนมาที่เบื้องหน้า

b.คลิกขวาที่ไฟล์ > คลิก **ตัวเลือกขั้นสูง** > **ไฟล์การกักเก็บ**

c.คลิก **ย้ายเพื่อกักเก็บ** จากหน้าต่าง **การกักเก็บ**

d.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

คำอธิบายการตรวจหา

คลิกขวาที่รายการและคลิก **คำอธิบายการตรวจหา** เพื่อเปิดสารานุกรมภัยคุกคามของ ESET ซึ่งมีข้อมูลโดยละเอียดเกี่ยวกับอันตรายและอาการของการแฝงตัวที่บันทึกไว้

> **คำแนะนำพร้อมภาพประกอบ**
> บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
> - เรียกคืนไฟล์ที่กักเก็บใน ESET Smart Security Premium
> - ลบไฟล์ที่กักเก็บใน ESET Smart Security Premium
> - ผลิตภัณฑ์ My ESET แจ้งเตือนการตรวจหาให้ฉันทราบ—ฉันควรทำอย่างไร

การกักเก็บล้มเหลว

เหตุผลที่ไฟล์บางไฟล์ไม่สามารถย้ายไปยังการกักเก็บมีดังต่อไปนี้:

- **คุณไม่มีสิทธิ์ในการอ่าน** – หมายความว่าคุณไม่สามารถดูเนื้อหาของไฟล์ได้
- **คุณไม่ได้มีสิทธิ์ในการเขียน** – หมายความว่าคุณไม่สามารถปรับเปลี่ยนเนื้อหาของไฟล์ เช่น ทั้งเพิ่มเนื้อหาใหม่หรือลบเนื้อหาที่มีอยู่
- **ไฟล์ที่คุณพยายามการกักเก็บมีขนาดใหญ่เกินไป** – คุณจำเป็นต้องลดขนาดไฟล์

เมื่อคุณได้รับข้อความแสดงข้อผิดพลาด “การกักเก็บล้มเหลว” ให้คลิก **ข้อมูลเพิ่มเติม** หน้าต่างรายการข้อผิดพลาดในการกักเก็บปรากฏขึ้นและคุณจะเห็นชื่อของไฟล์และเหตุผล ว่าทำไมไฟล์ไม่สามารถกักเก็บได้

พร็อกซีเซิร์ฟเวอร์

ในเครือข่าย LAN ขนาดใหญ่ การสื่อสารระหว่างคอมพิวเตอร์ของคุณกับอินเทอร์เน็ตสามารถกระทำผ่านพร็อกซีเซิร์ฟเวอร์ ต้องมีการกำหนดการตั้งค่าต่อไปนี้เมื่อใช้การกำหนดค่านี้ มิฉะนั้น โปรแกรมจะไม่สามารถอัพเดทโดยอัตโนมัติ ใน ESET Smart Security Premium การตั้งค่าพร็อกซีเซิร์ฟเวอร์สามารถใช้ได้จากสองส่วนที่แตกต่างกันของโครงสร้างการตั้งค่าขั้นสูง

ส่วนแรก สามารถกำหนดค่าการตั้งค่าพร็อกซีเซิร์ฟเวอร์ได้ใน **การตั้งค่าขั้นสูง** ภายใต้ **เครื่องมือ** > **พร็อกซีเซิร์ฟเวอร์** การระบุพร็อกซีเซิร์ฟเวอร์ที่ระดับนี้จะกำหนดการตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วมสำหรับ ESET Smart Security Premium ทั้งหมด พารามิเตอร์ในที่นี้จะถูกนำมาใช้โดยโมดูลทั้งหมดที่ต้องการการเชื่อมต่ออินเทอร์เน็ต

เมื่อต้องการระบุการตั้งค่าพร็อกซีเซิร์ฟเวอร์สำหรับระดับนี้ ให้เลือก **ใช้พร็อกซีเซิร์ฟเวอร์** แล้วป้อนที่อยู่ของพร็อก

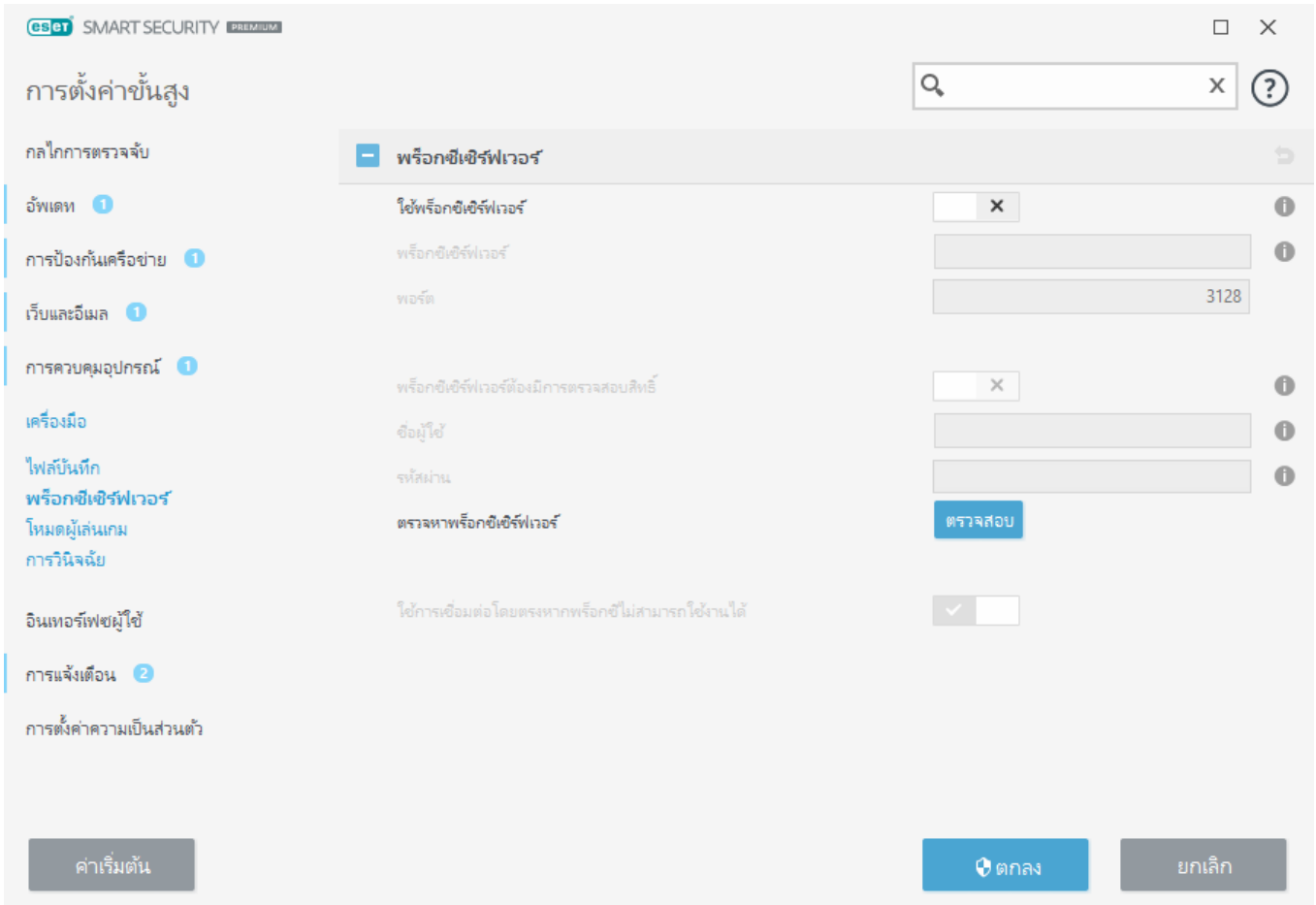
ซีเซิร์ฟเวอร์ในช่อง **พร็อกซีเซิร์ฟเวอร์** พร้อมด้วยหมายเลข **พอร์ต** ของพร็อกซีเซิร์ฟเวอร์

หากการสื่อสารกับพร็อกซี่เซิร์ฟเวอร์ที่จำเป็นต้องมีการตรวจสอบสิทธิ์ ให้เลือก**พร็อกซี่เซิร์ฟเวอร์ต้องมีการตรวจสอบสิทธิ์** แล้วป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** ที่ถูกต้องลงในช่องที่สอดคล้องกัน คลิก **ตรวจหาพร็อกซีเซิร์ฟเวอร์** เพื่อตรวจหาและเติมการตั้งค่าพร็อกซีเซิร์ฟเวอร์โดยอัตโนมัติ พารามิเตอร์ที่ระบุในตัวเลือกอินเทอร์เน็ตสำหรับ Internet Explorer หรือ Google Chrome จะถูกคัดลอกไว้

คุณต้องป้อนชื่อผู้ใช้และรหัสผ่านของคุณลงในการตั้งค่า **พร็อกซีเซิร์ฟเวอร์** ด้วยตัวเอง

ใช้การเชื่อมต่อโดยตรงหากพร็อกซีไม่สามารถใช้งานได้ – หาก ESET Smart Security Premium ถูกกำหนดค่าผ่านพร็อกซี่และไม่สามารถเข้าถึงพร็อกซี่ได้ESET Smart Security Premium จะข้ามพร็อกซี่และสื่อสารกับเซิร์ฟเวอร์ ESET โดยตรง

นอกจากนี้ การตั้งค่าพร็อกซีเซิร์ฟเวอร์ยังสามารถเริ่มต้นได้จากการตั้งค่าการอัพเดทขั้นสูง (**การตั้งค่าขั้นสูง** > **อัพเดท** > **โปรไฟล์** > **อัพเดท** > **ตัวเลือกการเชื่อมต่อ** ด้วยการเลือก **เชื่อมต่อผ่านพร็อกซีเซิร์ฟเวอร์** จากเมนูแบบเลื่อนลง **โหมดพร็อกซี**) การตั้งค่านี้ใช้สำหรับโปรไฟล์การอัพเดทที่มีให้และแนะนำให้ใช้กับแล็ปท็อป เนื่องจากเป็นอุปกรณ์ที่มักได้รับการอัพเดทกลไกตรวจหาจากตำแหน่งระยะไกล สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่านี้ โปรดดู การตั้งค่าการอัพเดทขั้นสูง



เลือกตัวอย่างเพื่อวิเคราะห์

หากคุณพบไฟล์ที่มีพฤติกรรมน่าสงสัยในคอมพิวเตอร์ของคุณหรือเว็บไซต์ที่น่าสงสัยในอินเทอร์เน็ต คุณสามารถส่งไปยังห้องปฏิบัติการวิจัย ESET เพื่อรับการวิเคราะห์ได้ (อาจไม่สามารถใช้งานได้ขึ้นอยู่กับการตั้งค่า ESET LiveGrid® ของคุณ)

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

คุณสามารถส่งตัวอย่าง (ไฟล์หรือเว็บไซต์) ไปยัง ESET เพื่อวิเคราะห์โดยใช้หนึ่งในวิธีดังต่อไปนี้:

1. ใช้รูปแบบการส่งตัวอย่างในผลิตภัณฑ์ของคุณ โดยรูปแบบดังกล่าวจะอยู่ใน **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **ส่งตัวอย่างเพื่อการวิเคราะห์** ขนาดสูงสุดของตัวอย่างที่ส่งคือ 256MB

2. อีกวิธีหนึ่งคือ คุณสามารถส่งไฟล์ทางอีเมล ถ้าคุณเลือกตัวเลือกนี้ ให้บรรจุไฟล์เป็นแพ็คโดยใช้ WinRAR/WinZIP ป้องกันอาร์ไคฟ์ด้วยรหัสผ่าน "infected" และส่งไปยัง samples@eset.com

3. สำหรับการรายงานสแปม สแปมการตรวจพบที่ผิดพลาดหรือเว็บไซต์ที่กำหนดประเภทอย่างไม่ถูกต้องโดยโมดูลการควบคุมเนื้อหา โปรดดูบทความฐานความรู้ของ ESET ของเรา

ในรูปแบบ **เลือกตัวอย่างเพื่อวิเคราะห์** เลือกคำอธิบายจากเมนูแบบเลื่อนลง **เหตุผลสำหรับการส่งตัวอย่าง** ที่เหมาะกับข้อความของคุณที่สุด:

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

ไฟล์/ไซต์ – พาธไปยังไฟล์หรือเว็บไซต์ที่คุณต้องการส่ง

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

> **คุณอาจไม่ได้รับการตอบสนองจาก ESET**
> คุณอาจไม่ได้รับการตอบสนองจาก ESET ยกเว้นในกรณีที่ต้องการข้อมูลเพิ่มเติมจากคุณ เนื่องจากเซิร์ฟเวอร์ของเราได้รับไฟล์หลายหมื่นไฟล์ในแต่ละวัน เราจึงไม่สามารถตอบกลับได้ทั้งหมด
> หากตรวจพบว่าตัวอย่างเป็นแอพพลิเคชันหรือเว็บไซต์ที่เป็นอันตราย การตรวจพบไฟล์นี้จะถูกเพิ่มในการอัพเดทที่กำลังจะมีขึ้นของ ESET

เลือกตัวอย่างเพื่อวิเคราะห์ – ไฟล์ที่น่าสงสัย

สัญญาณและอาการที่พบของการติดไวรัสจากมัลแวร์ – ป้อนคำอธิบายเกี่ยวกับการทำงานของไฟล์ที่น่าสงสัยที่พบในคอมพิวเตอร์ของคุณ

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

หมายเหตุและข้อมูลเพิ่มเติม - คุณสามารถป้อนข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยในการระบุไฟล์ที่น่าสงสัยได้ที่นี้

> พารามิเตอร์แรก – จำเป็นต้องมี **สัญญาณและอาการที่พบของการติดไวรัสจากมัลแวร์** แต่การให้ข้อมูลเพิ่มเติมจะช่วยห้องปฏิบัติการของเราในการระบุกระบวนการและประมวลผลตัวอย่างได้เป็นอย่างมาก

เลือกตัวอย่างเพื่อวิเคราะห์–เว็บไซต์ที่น่าสงสัย

โปรดเลือกตัวเลือกใดตัวเลือกหนึ่งต่อไปนี้จากเมนูแบบเลื่อนลง **เกิดอะไรขึ้นกับไซต์นี้**:

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

หมายเหตุและข้อมูลเพิ่มเติม – คุณสามารถป้อนข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยในการวิเคราะห์เว็บไซต์ที่

น่าสงสัยได้ที่นี่

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

รายการอัพเดทของ Microsoft Windows

คุณลักษณะการอัพเดท Windows เป็นองค์ประกอบสำคัญสำหรับการป้องกันผู้ใช้ให้พ้นจากซอฟต์แวร์ที่เป็นอันตราย ด้วยเหตุผลนี้ การติดตั้งการอัพเดทของ Microsoft Windows ให้เร็วที่สุดเมื่อมีการเผยแพร่จึงเป็นสิ่งที่สำคัญ ESET Smart Security Premium จะแจ้งคุณเกี่ยวกับการอัพเดทที่ขาดหายไป ตามระดับที่คุณระบุ ระดับที่ใช้ได้มีดังนี้:

- **ไม่มีการอัพเดท** – ไม่มีการเสนอการอัพเดทเพื่อให้ดาวน์โหลด
- **การอัพเดทที่เป็นตัวเลือก** – ระบบจะเสนอการอัพเดทที่ทำเครื่องหมายว่าเป็นอัพเดทมีความสำคัญต่ำและสูงกว่าให้ดาวน์โหลด
- **การอัพเดทที่แนะนำ** – ระบบจะเสนอการอัพเดทที่ทำเครื่องหมายว่าเป็นอัพเดททั่วไปและสูงกว่าให้ดาวน์โหลด
- **การอัพเดทสำคัญ** – ระบบจะเสนอการอัพเดทที่ทำเครื่องหมายว่าเป็นอัพเดทสำคัญและสูงกว่าให้ดาวน์โหลด
- **การอัพเดทที่สำคัญมาก** – ระบบจะเสนอเฉพาะการอัพเดทที่สำคัญมากให้ดาวน์โหลด

คลิกที่ **ตกลง** เพื่อบันทึกการเปลี่ยนแปลง หน้าต่างการอัพเดทระบบจะปรากฏหลังการตรวจสอบสถานะกับเซิร์ฟเวอร์การอัพเดท ดังนั้น ข้อมูลการอัพเดทระบบอาจไม่ปรากฏทันทีหลังจากบันทึกการเปลี่ยนแปลง

หน้าต่างข้อความ – การอัพเดทระบบ

หากมีรายการอัพเดทสำหรับระบบปฏิบัติการของคุณ หน้าต่างหน้าแรกของ ESET Smart Security Premium จะแสดงการแจ้งเตือน คลิก **ข้อมูลเพิ่มเติม** เพื่อเปิดหน้าต่างการอัพเดทระบบ

หน้าต่างการอัพเดทระบบจะแสดงรายการอัพเดทที่พร้อมสำหรับการดาวน์โหลดและติดตั้ง ประเภทการอัพเดทจะ

ปรากฏถัดจากชื่อของการอัพเดทนั้น

คลิกสองครั้งที่แถวของการอัพเดทแถวใดก็ได้เพื่อแสดงหน้าต่างข้อมูลการอัพเดทที่มีข้อมูลเพิ่มเติม

คลิกที่ **เรียกใช้การอัพเดทระบบ** เพื่อเริ่มต้นดาวน์โหลดและติดตั้งการอัพเดทระบบปฏิบัติการ

ข้อมูลการอัพเดท

ข้อมูลเกี่ยวกับการอัพเดท Windows ชื่อและจำนวนการอัพเดทจะปรากฏที่ด้านบนของหน้าต่าง ตามด้วยลำดับความสำคัญ และคำอธิบายปัญหาที่แก้ไขด้วยการอัพเดท

ส่วนติดต่อผู้ใช้

เมื่อต้องการกำหนดค่าลักษณะการทำงานของส่วนติดต่อกับผู้ใช้ (GUI) ของโปรแกรม ในหน้าต่างโปรแกรมหลัก ให้คลิก **ตั้งค่า** > **การตั้งค่าขั้นสูง** (F5) > **ส่วนติดต่อกับผู้ใช้**

คุณสามารถปรับรูปลักษณ์และเอฟเฟ็กต์ของโปรแกรมได้ใน องค์ประกอบส่วนติดต่อกับผู้ใช้ ของหน้าจอการตั้งค่าขั้นสูง

เพื่อให้มีการรักษาความปลอดภัยสูงสุดจากซอฟต์แวร์การรักษาความปลอดภัย คุณสามารถป้องกันการถอนการติดตั้งหรือการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตได้โดยปกป้องการตั้งค่าด้วยรหัสผ่านโดยใช้เครื่องมือ ตั้งค่าการเข้าถึง

> หากต้องการกำหนดค่าลักษณะการทำงานของการแจ้งเตือนระบบ การเตือนการตรวจหา และสถานะแอพพลิเคชัน ให้ดูที่ส่วน การแจ้งเตือน

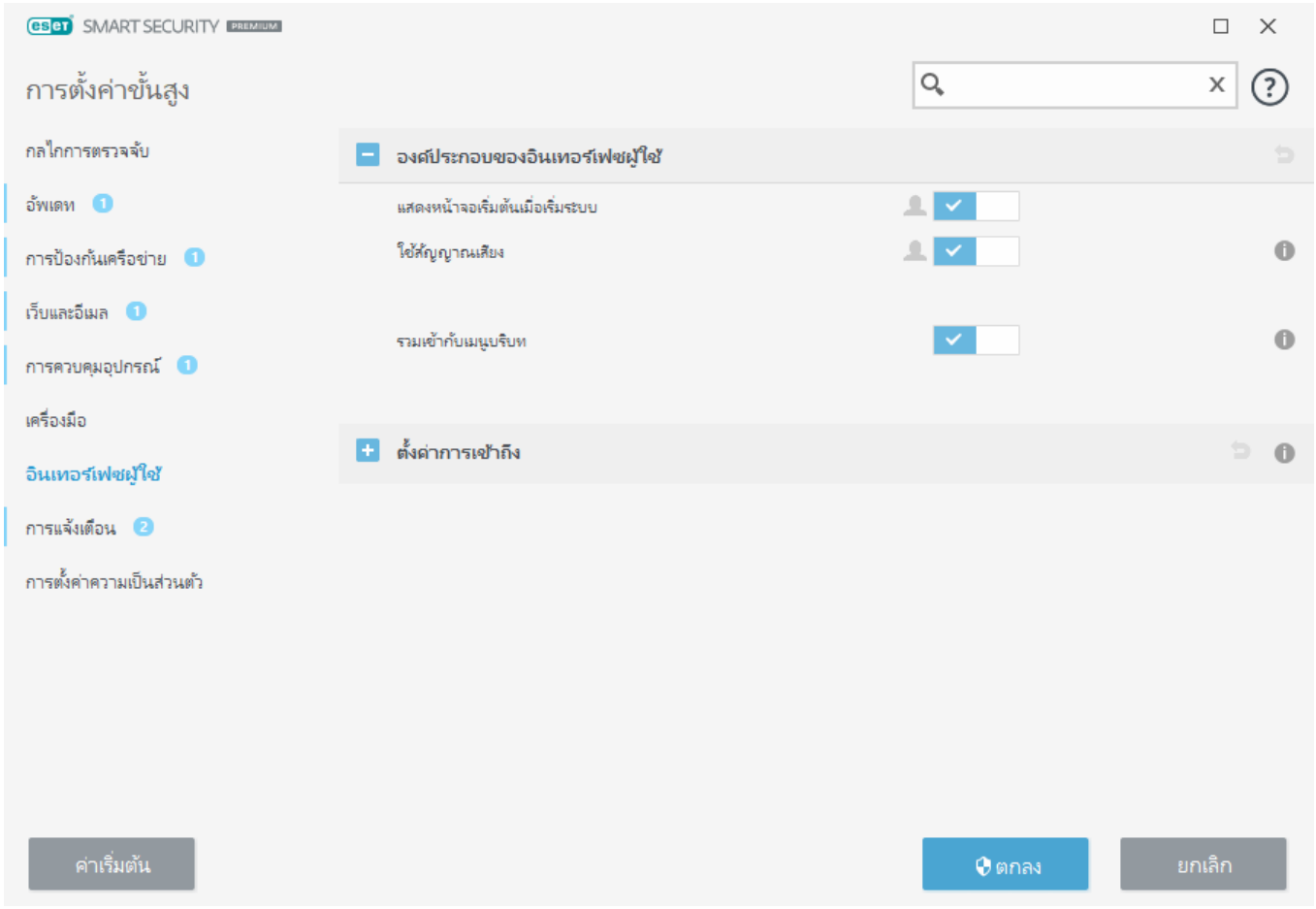
องค์ประกอบของส่วนติดต่อผู้ใช้

ตัวเลือกการกำหนดค่าส่วนติดต่อผู้ใช้ใน ESET Smart Security Premium จะช่วยให้คุณสามารถปรับระบบการทำงานเพื่อให้เหมาะกับความต้องการของคุณ ตัวเลือกการกำหนดค่าเหล่านี้สามารถเข้าถึงได้ใน **การตั้งค่าขั้นสูง** (F5) > **ส่วนติดต่อผู้ใช้** > **องค์ประกอบของส่วนติดต่อผู้ใช้**

ถ้าคุณต้องการปิดใช้งานหน้าจอเริ่มต้นของ ESET Smart Security Premium ให้ยกเลิกการเลือก **แสดงหน้าจอเริ่มต้น**

ใช้สัญญาณเสียง – ESET Smart Security Premium เล่นเสียงเมื่อมีเหตุการณ์สำคัญเกิดขึ้นระหว่างการสแกน ตัวอย่างเช่น เมื่อพบภัยคุกคามหรือเมื่อการสแกนเสร็จสิ้น

รวมเข้ากับเมนูบริบท – รวมองค์ประกอบการควบคุม ESET Smart Security Premium ไว้ในเมนูบริบท



ตั้งค่าการเข้าถึง

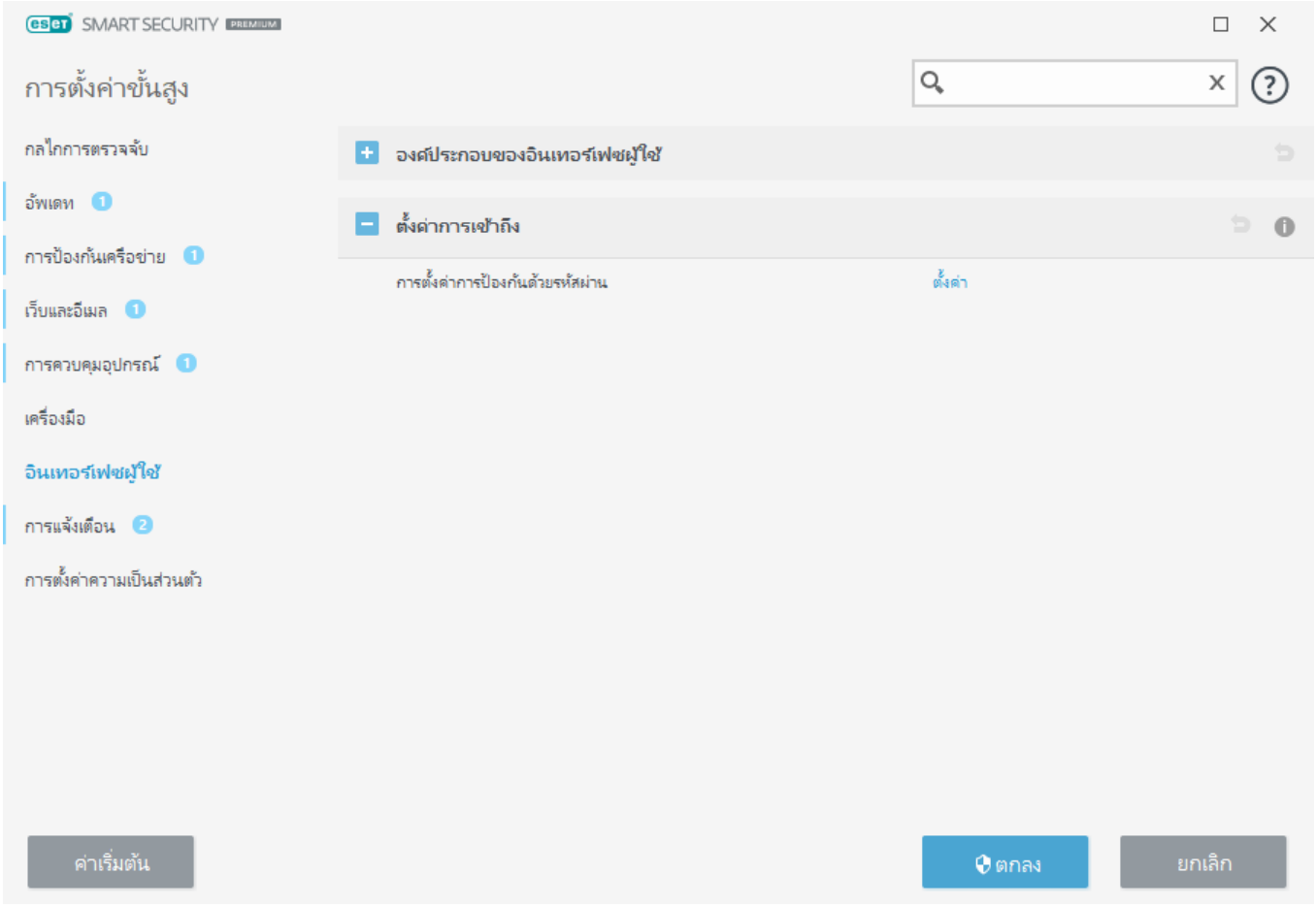
การตั้งค่า ESET Smart Security Premium เป็นส่วนสำคัญของนโยบายรักษาความปลอดภัย การแก้ไขโดยไม่ได้รับอนุญาตอาจเป็นอันตรายต่อเสถียรภาพและการป้องกันระบบของคุณ เมื่อต้องการหลีกเลี่ยงการแก้ไขที่ไม่ได้รับอนุญาต คุณสามารถป้องกันพารามิเตอร์การตั้งค่าและการลบการติดตั้ง ESET Smart Security Premium ด้วยรหัสผ่านได้

หากต้องการตั้งรหัสผ่านเพื่อป้องกันพารามิเตอร์การตั้งค่าและการลบการติดตั้ง ESET Smart Security Premium ให้คลิก **ตั้งค่า** ถัดจาก **การตั้งค่าการป้องกันด้วยรหัสผ่าน**

เมื่อคุณเข้าใช้การตั้งค่าขั้นสูงที่มีการป้องกัน หน้าต่างสำหรับป้อนรหัสผ่านจะแสดงขึ้น หากคุณลืมหรือทำรหัสผ่านหาย ให้คลิกตัวเลือก **เรียกคืนรหัสผ่าน** ด้านล่างแล้วใส่ที่อยู่อีเมลที่คุณใช้ในการลงทะเบียนใบอนุญาต ESET จะส่งอีเมลที่มีรหัสยืนยันความถูกต้องและคำแนะนำเกี่ยวกับวิธีรีเซ็ตรหัสผ่านของคุณ
- วิธีปลดล็อคการตั้งค่าขั้นสูง

หากต้องการเปลี่ยนรหัสผ่าน ให้คลิก **เปลี่ยนรหัสผ่าน** ถัดจาก **การตั้งค่าการป้องกันด้วยรหัสผ่าน**

หากต้องการลบรหัสผ่าน ให้คลิก **ลบออก** ถัดจาก **การตั้งค่าการป้องกันด้วยรหัสผ่าน**



รหัสผ่านสำหรับการตั้งค่าขั้นสูง

หากต้องการป้องกันการตั้งค่าขั้นสูงของ ESET Smart Security Premium เพื่อหลีกเลี่ยงการแก้ไขที่ไม่ได้รับอนุญาต คุณต้องตั้งค่ารหัสผ่านใหม่

เมื่อคุณต้องการเปลี่ยนแปลงรหัสผ่านที่มีอยู่แล้ว:

1. พิมพ์รหัสผ่านเดิมของคุณในช่อง **รหัสผ่านเดิม**
2. ป้อนรหัสผ่านใหม่ของคุณในช่อง **รหัสผ่านใหม่** และ **ยืนยันรหัสผ่าน**
3. คลิก**ตกลง**

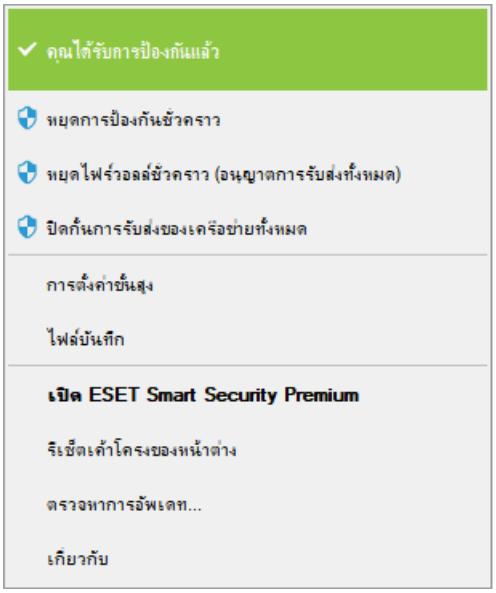
รหัสผ่านนี้จำเป็นต้องใช้ในการแก้ไขใดๆ ในอนาคตสำหรับ ESET Smart Security Premium

หากคุณลืมรหัสผ่าน การเข้าถึงการตั้งค่าขั้นสูงสามารถช่วยให้คุณ กู้คืนรหัสผ่านได้ด้วยการใช้วิธี "กู้คืนรหัสผ่าน"

หากต้องการเรียกคืนรหัสใบอนุญาต ESET, วันหมดอายุของใบอนุญาตของคุณ หรือข้อมูลอื่นๆ ของใบอนุญาตสำหรับ ESET Smart Security Premium โปรดดู บทความฐานความรู้ของเรา

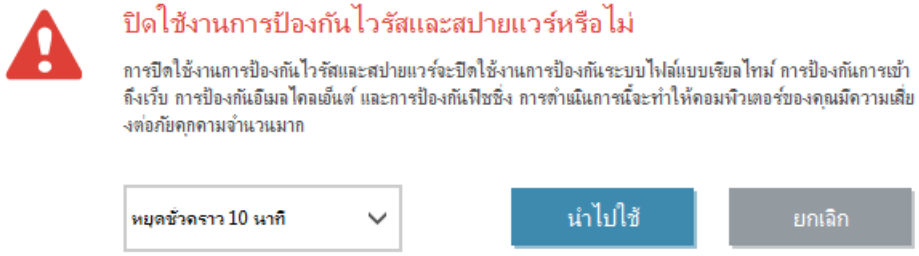
ไอคอนในถาดข้อมูลระบบ

มีตัวเลือกและคุณลักษณะของการตั้งค่าที่สำคัญที่สุดบางรายการสามารถใช้ได้ด้วยการคลิกขวาที่ไอคอนในถาดข้อมูลระบบ



หยุดการป้องกันชั่วคราว – แสดงกล่องข้อความยืนยันที่ปิดใช้งาน กลไกการตรวจจับ ที่ป้องกันระบบที่เป็นอันตรายโดยการควบคุมไฟล์ การสื่อสารทางเว็บและอีเมล

เมนู**ช่วงเวลา** แบบเลื่อนลงที่จะปิดการใช้งานการป้องกันทั้งหมด



ปิดไฟร์วอลล์ชั่วขณะ (อนุญาตการรับส่งทั้งหมด) – สลับไฟร์วอลล์เป็นสถานะไม่ใช้งาน โปรดดู เครือข่าย สำหรับข้อมูลเพิ่มเติม

ปิดกั้นการรับส่งของเครือข่ายทั้งหมด – ปิดกั้นการรับส่งของเครือข่ายทั้งหมด คุณสามารถเปิดใช้งานอีกครั้งได้โดยการคลิกที่**หยุดปิดกั้นการรับส่งข้อมูลเครือข่ายทั้งหมด**

การตั้งค่าขั้นสูง – เลือกตัวเลือกนี้เพื่อไปยังโครงสร้าง **การตั้งค่าขั้นสูง** นอกจากนี้ ยังมีวิธีอื่นในการเปิดการตั้งค่าขั้นสูง เช่น กดแป้น F5 หรือไปที่ **การตั้งค่า** > **การตั้งค่าขั้นสูง**

ไฟล์บันทึก – ไฟล์บันทึก ประกอบไปด้วยข้อมูลเกี่ยวกับเหตุการณ์ของโปรแกรมสำคัญที่เกิดขึ้น และให้ภาพรวมของการตรวจพบ

เปิดESET Smart Security Premium – เปิดหน้าต่างโปรแกรมหลักของESET Smart Security Premium จากไอคอนถาด

รีเซ็ตเค้าโครงหน้าต่าง - รีเซ็ตหน้าต่างของ ESET Smart Security Premium เป็นขนาดและตำแหน่งเริ่มต้นบนหน้าจอ

ตรวจสอบการอัพเดท – เริ่มอัพเดทกลไกตรวจหา (ก่อนหน้านี้เรียกว่า "ฐานข้อมูลไวรัส") เพื่อให้มั่นใจในระดับการป้องกันรหัสที่เป็นอันตรายของคุณ

เกี่ยวกับ - แสดงข้อมูลระบบ รายละเอียดเกี่ยวกับเวอร์ชันของ ESET Smart Security Premium ที่ติดตั้งและโมดูลของโปรแกรมที่ติดตั้ง นอกจากนี้ คุณยังสามารถดูวันที่หมดอายุของใบอนุญาตและข้อมูลเกี่ยวกับระบบปฏิบัติการและทรัพยากรระบบได้จากส่วนนี้

การสนับสนุนโปรแกรมอ่านหน้าจอ

ESET Smart Security Premium สามารถใช้งานร่วมกับโปรแกรมอ่านหน้าจอเพื่อให้ผู้ใช้ ESET ที่มีความบกพร่องทางสายตาสามารถนำทางผลิตภัณฑ์หรือตั้งค่าการตั้งค่าได้ โปรแกรมอ่านหน้าจอต่อไปนี้รองรับใน (JAWS, NVDA, Narrator)

เพื่อให้แน่ใจว่าซอฟต์แวร์โปรแกรมอ่านหน้าจอสามารถเข้าถึง GUI ของ ESET Smart Security Premium ได้อย่างถูกต้อง ให้ดำเนินการตามคำแนะนำในบทความฐานความรู้ของเรา

วิธีใช้และการสนับสนุน

ESET Smart Security Premium ประกอบไปด้วยเครื่องมือสำหรับการแก้ไขปัญหาและข้อมูลการสนับสนุนซึ่งจะช่วยคุณในการแก้ไขปัญหาต่างๆ ที่คุณอาจพบ

ใบอนุญาต

• **การแก้ไขปัญหาใบอนุญาต** – คลิกลิงก์นี้เพื่อค้นหาวิธีแก้ไขปัญหาเกี่ยวกับการเปิดใช้งานหรือการเปลี่ยนแปลงใบอนุญาต

• **เปลี่ยนใบอนุญาต** - คลิกเพื่อเรียกใช้หน้าต่างการเปิดใช้งานและเปิดใช้งานผลิตภัณฑ์ของคุณ หากอุปกรณ์ของคุณ เชื่อมต่ออยู่กับ ESET HOME ให้เลือกใบอนุญาตจากบัญชี ESET HOME ของคุณหรือเพิ่มใหม่

ผลิตภัณฑ์ที่ติดตั้ง

• **มีอะไรใหม่**–โปรดคลิกรายการนี้เพื่อเปิดหน้าต่างเกี่ยวกับคุณสมบัติใหม่ที่ได้รับการปรับปรุง

• **เกี่ยวกับESET Smart Security Premium** – แสดงข้อมูลเกี่ยวกับสำเนา ESET Smart Security Premium ของคุณ

• **การแก้ไขปัญหาผลิตภัณฑ์** – คลิกลิงก์นี้เพื่อค้นหาวิธีแก้ไขสำหรับปัญหาที่พบบ่อยที่สุด

• **เปลี่ยนผลิตภัณฑ์** – คลิกเพื่อดูว่า ESET Smart Security Premium สามารถเปลี่ยนเป็น ผลิตภัณฑ์รุ่นอื่น ที่มีใบอนุญาตปัจจุบันได้หรือไม่

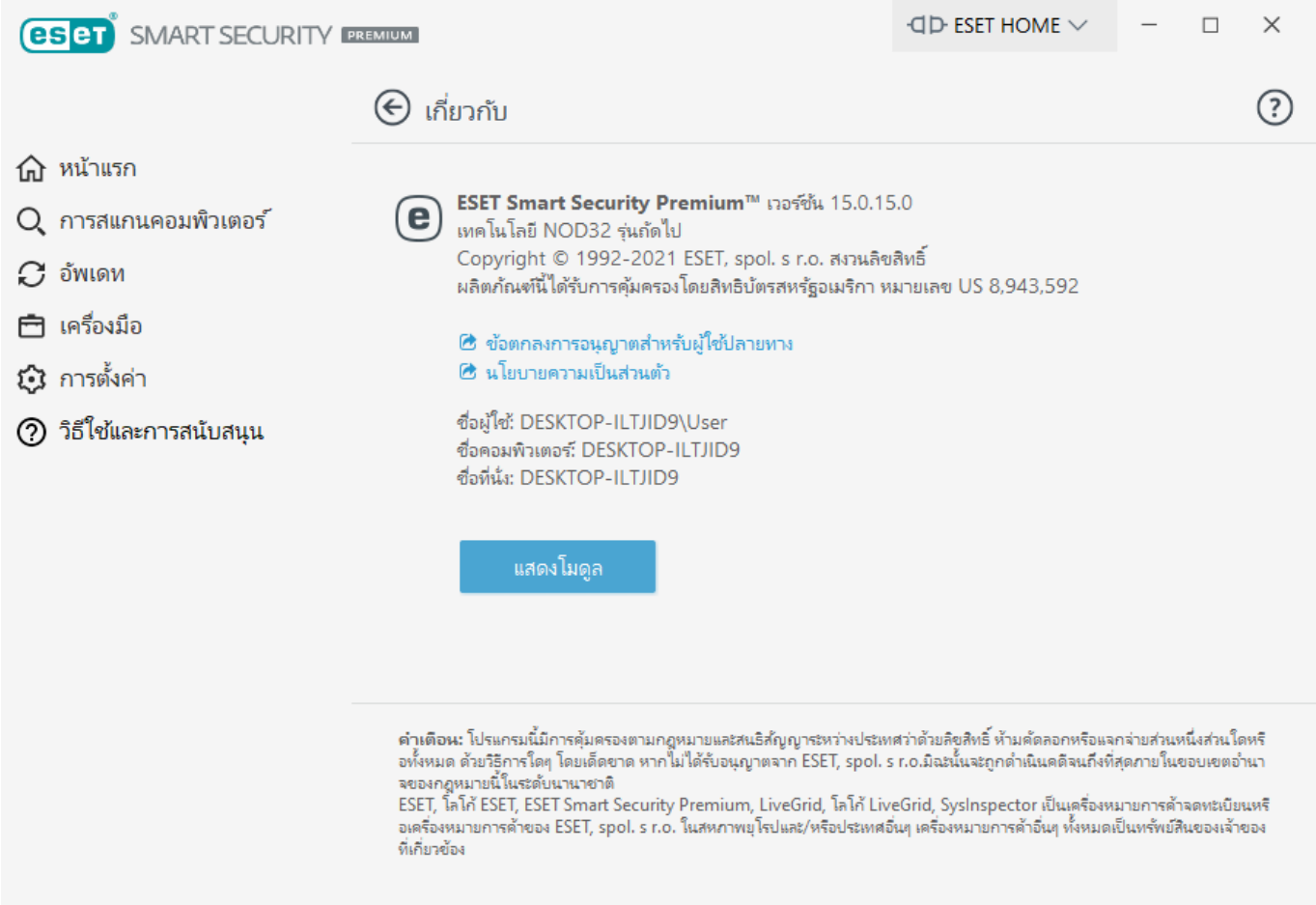
หน้าวิธีใช้ – คลิกลิงค์นี้เพื่อเริ่มต้นหน้าวิธีใช้ ESET Smart Security Premium

ฝ่ายสนับสนุนด้านเทคนิค

ฐานความรู้ – ฐานความรู้ของ ESET มีคำตอบสำหรับคำถามที่พบบ่อยที่สุด รวมถึงทางแก้ไขที่แนะนำสำหรับปัญหาต่างๆ ผู้เชี่ยวชาญด้านเทคนิคของ ESET จะอัพเดทข้อมูลนี้เป็นประจำ เพื่อให้ฐานความรู้เป็นเครื่องมือที่มีประสิทธิภาพสูงสุดสำหรับการแก้ไขปัญหาประเภทต่างๆ

เกี่ยวกับ ESET Smart Security Premium

หน้าต่างนี้จะแสดงรายละเอียดเกี่ยวกับ ESET Smart Security Premium เวอร์ชันที่ติดตั้งและคอมพิวเตอร์ของคุณ



คลิก **แสดงโมดูล** เพื่อดูข้อมูลเกี่ยวกับรายชื่อโมดูลโปรแกรมที่โหลด

• คุณสามารถคัดลอกข้อมูลเกี่ยวกับโมดูลไปไว้ที่คลิปบอร์ดได้ด้วยการคลิก **คัดลอก** การดำเนินการนี้อาจมีประโยชน์เมื่อแก้ไขปัญหา หรือเมื่อติดต่อกับฝ่ายสนับสนุนด้านเทคนิค

• คลิก **กลไกการตรวจจับ** ในหน้าต่างโมดูลเพื่อเปิดเรดาร์ไวรัสของ ESET ซึ่งบรรจุข้อมูลเกี่ยวกับกลไกการตรวจจับของ ESET แต่ละเวอร์ชัน

ข่าวสารของ ESET

ในหน้าต่างนี้ ESET Smart Security Premium จะแจ้งให้คุณทราบเกี่ยวกับข่าวของ ESET เป็นประจำ

การส่งข้อความในผลิตภัณฑ์ไม่ได้ออกแบบมาเพื่อแจ้งข่าวสารและการติดต่อสื่อสารอื่นๆ ของ ESET ให้ผู้ใช้ทราบ การส่งข้อความการตลาดจะต้องได้รับการยินยอมจากผู้ใช้ ดังนั้นการส่งข้อความการตลาดจะไม่ถูกส่งให้ผู้ใช้โดยค่าเริ่มต้น (แสดงในเครื่องหมายคำถาม) โดยการเปิดใช้งานตัวเลือกนี้ คุณยอมที่จะรับข้อความการตลาดของ ESET หากคุณไม่สนใจที่จะรับข้อมูลทางการตลาดของ ESET ให้ปิดใช้งานตัวเลือก **แสดงข้อความด้านการตลาด**

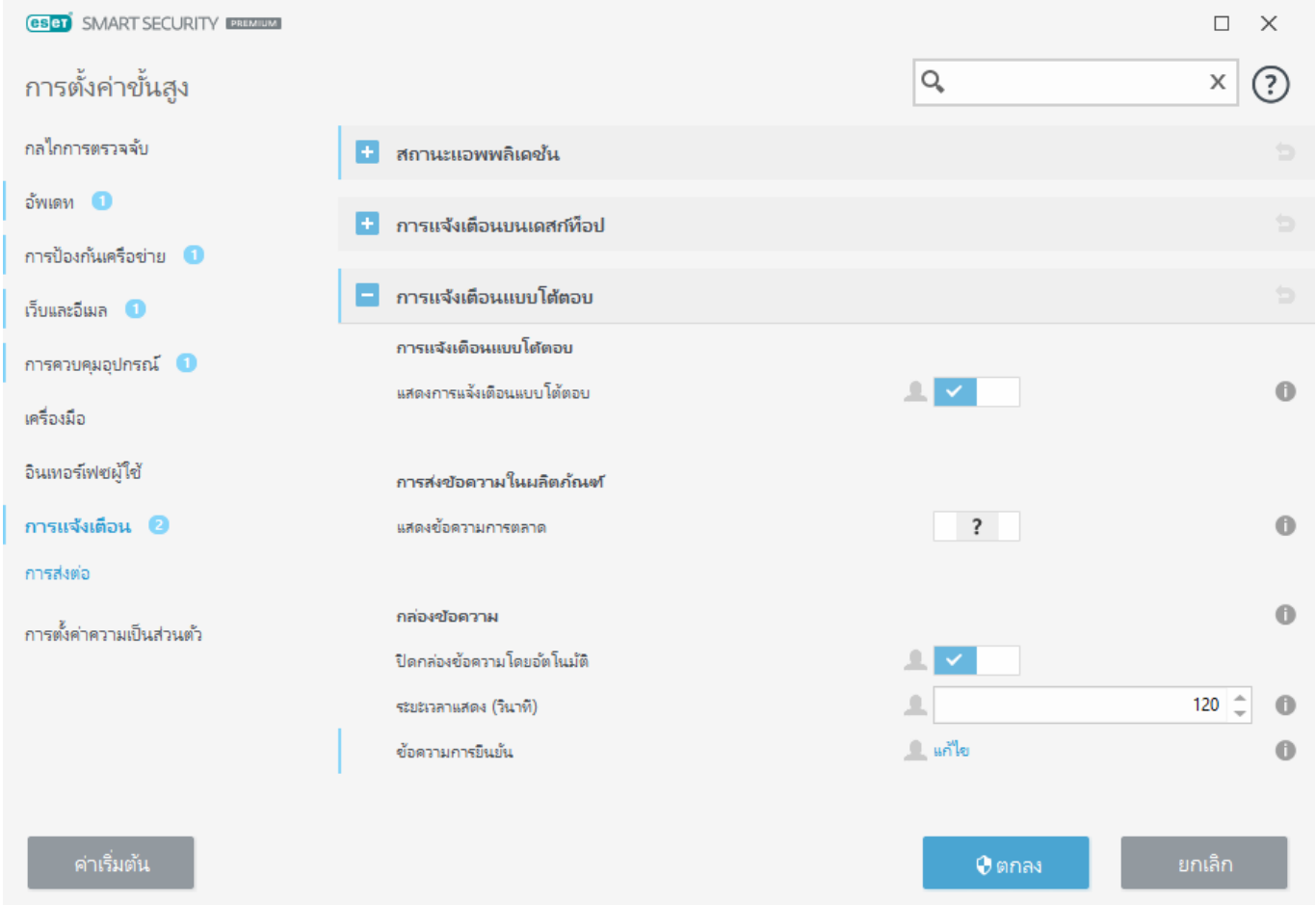
หากต้องการเปิดหรือปิดการรับข้อความด้านการตลาดผ่านหน้าต่างป๊อปอัพ ให้ทำตามคำแนะนำด้านล่างนี้

1. เปิดหน้าต่างโปรแกรมหลักของผลิตภัณฑ์ ESET ของคุณ

2. กดแป้น **F5** เพื่อเข้าถึง **การตั้งค่าขั้นสูง**

3. คลิก **การแจ้งเตือน** > **การแจ้งเตือนแบบโต้ตอบ**

4. ปรับเปลี่ยนตัวเลือก **แสดงข้อความด้านการตลาด**



ส่งข้อมูลการกำหนดค่าระบบ

ESET จำเป็นต้องขอข้อมูลเกี่ยวกับการกำหนดค่า ESET Smart Security Premium ข้อมูลระบบโดยละเอียดและกระบวนการที่ทำงานอยู่ (ไฟล์บันทึก ESET SysInspector) และข้อมูลรีจิสตรีเพื่อการช่วยเหลืออย่างรวดเร็วและถูกต้องที่สุดเท่าที่จะทำได้ ESET จะใช้ข้อมูลนี้เพื่อให้ความช่วยเหลือด้านเทคนิคแก่ลูกค้าเพียงอย่างเดียว

เมื่อส่ง แบบฟอร์มเว็บ ข้อมูลการกำหนดค่าระบบของคุณจะถูกส่งให้กับ ESET เลือก **ส่งข้อมูลนี้เสมอ** หากคุณต้องการจำการดำเนินการนี้สำหรับกระบวนการนี้ ในการส่งแบบฟอร์มโดยไม่ส่งข้อมูลใด ให้คลิก **อย่าส่งข้อมูล** และคุณสามารถติดต่อฝ่ายสนับสนุนด้านเทคนิค ESET โดยใช้แบบฟอร์มขอรับการสนับสนุนออนไลน์ได้

ยังสามารถกำหนดค่าการตั้งค่านี้ใน **การตั้งค่าขั้นสูง** > **เครื่องมือ** > **การวินิจฉัย** > ฝ่ายดูแลลูกค้า

หากคุณตัดสินใจส่งข้อมูลระบบ คุณจำเป็นต้องกรอกรายละเอียดลงในฟอร์มทางเว็บและส่ง ไม่เช่นนั้น ระบบจะไม่สร้างตั๋วให้กับคุณ และข้อมูลระบบของคุณจะหายไป

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

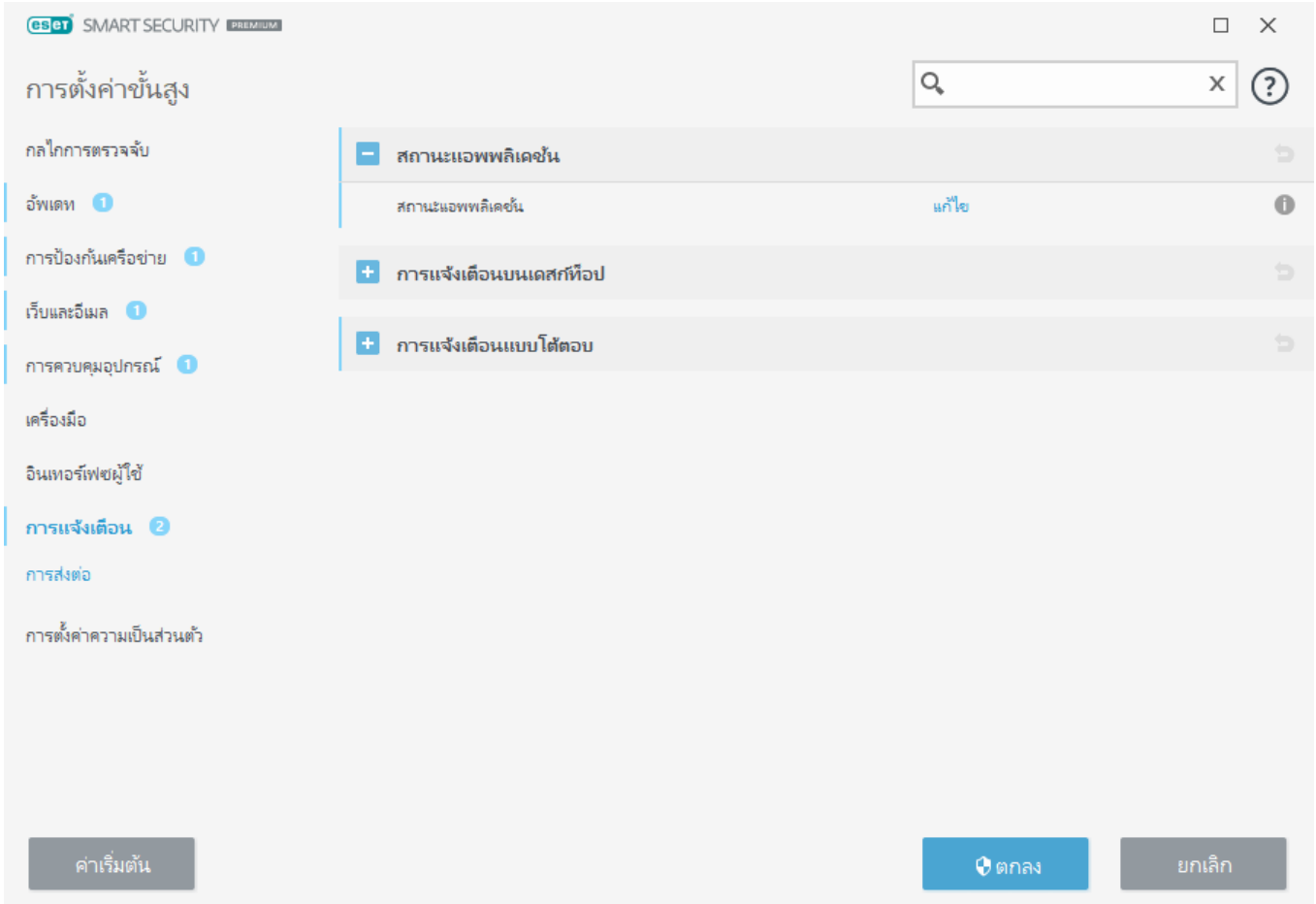
ESET Log Collector - ลิงก์ไปยังบทความฐานความรู้ของ ESET ที่คุณสามารถดาวน์โหลด ESET Log Collector ซึ่งเป็นแอพพลิเคชันที่รวบรวมข้อมูลโดยอัตโนมัติและบันทึกจากคอมพิวเตอร์เพื่อช่วยให้แก้ไขปัญหาได้รวดเร็วยิ่งขึ้น สำหรับข้อมูลเพิ่มเติมเกี่ยวกับผลิตภัณฑ์ ดูที่ คู่มือผู้ใช้แบบออนไลน์ของ ESET Log Collector

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

การแจ้งเตือน

หากต้องการจัดการการแจ้งเตือน ESET Smart Security Premium ให้เปิด **การตั้งค่าขั้นสูง** (F5) > **การแจ้งเตือน** คุณสามารถกำหนดค่าการแจ้งเตือนประเภทต่อไปนี้ได้:

- สถานะแอพพลิเคชัน – การแจ้งเตือนที่แสดงในส่วนหน้าแรกของหน้าต่างโปรแกรมหลัก
- การแจ้งเตือนบนเดสก์ท็อป – หน้าต่างป๊อปอัปขนาดเล็กถัดจากแถบงานของระบบ
- การแจ้งเตือนแบบโต้ตอบ – หน้าต่างการเตือนและกล่องข้อความที่ต้องการการโต้ตอบของผู้ใช้
- การส่งต่อ การแจ้งเตือนทางอีเมล – การแจ้งเตือนทางอีเมลจะถูกส่งไปยังที่อยู่อีเมลที่ระบุ



สถานะแอพพลิเคชัน

สถานะแอพพลิเคชัน – คลิก **แก้ไข** เพื่อเลือกสถานะแอพพลิเคชันที่จะแสดงในส่วนหน้าแรกของหน้าต่างโปรแก

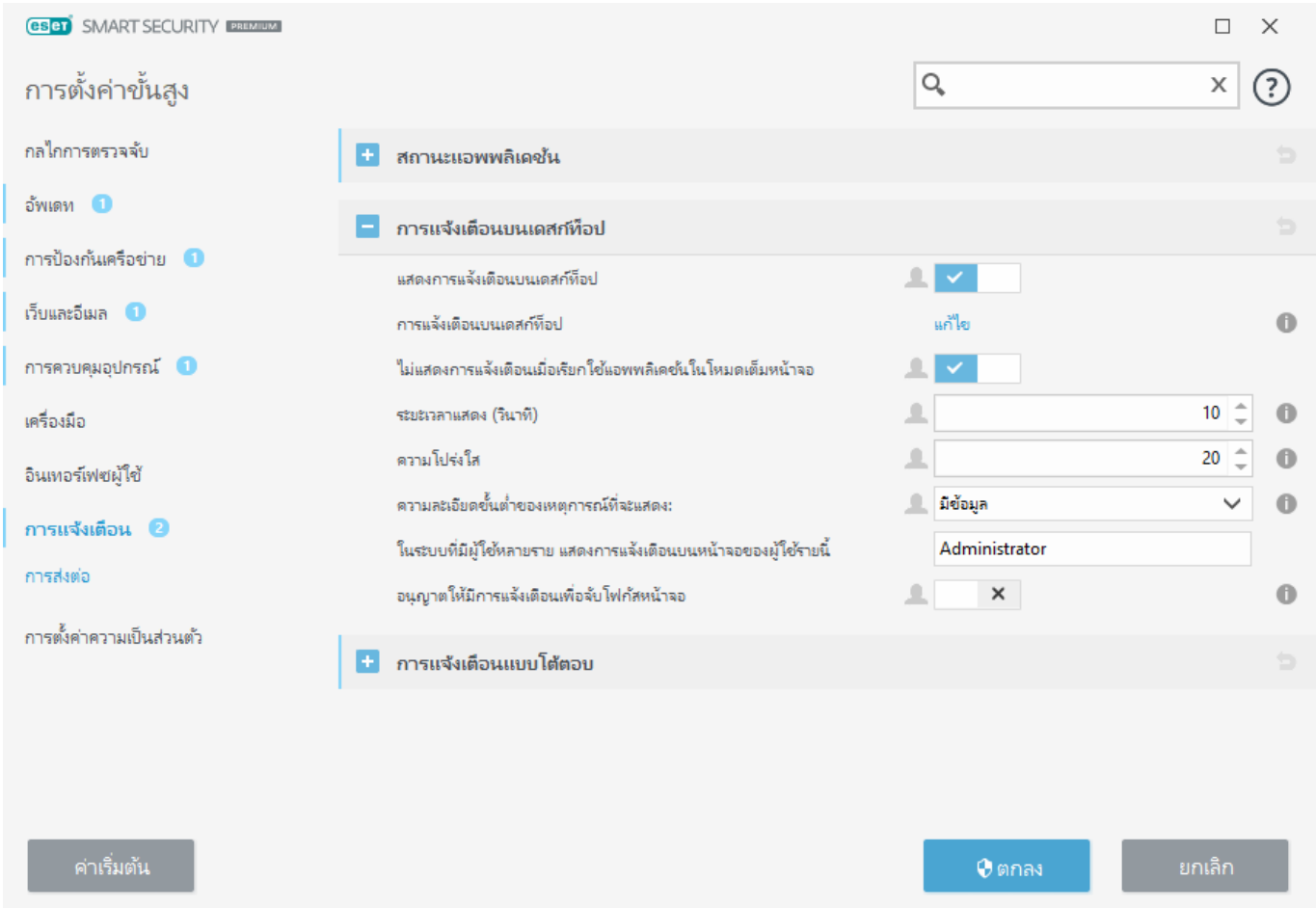
หน้าต่างข้อความ – สถานะแอพพลิเคชัน

ในหน้าต่างข้อความนี้ คุณสามารถเลือกสถานะแอพพลิเคชันที่จะแสดงได้ ตัวอย่างเช่น เมื่อคุณหยุดการป้องกันไวรัสและสปายแวร์ชั่วคราว หรือเปิดใช้งานโหมดผู้เล่นเกมส์

สถานะแอพพลิเคชันจะแสดงขึ้นเช่นกันหากผลิตภัณฑ์ของคุณไม่ได้เปิดใช้งานหรือใบอนุญาตของคุณหมดอายุ

การแจ้งเตือนบนเดสก์ท็อป

การแจ้งเตือนบนเดสก์ท็อปจะแสดงด้วยหน้าต่างป๊อปอัพซึ่งอยู่ถัดจากแถบงานระบบ ซึ่งถูกตั้งค่าให้แสดงเป็นเวลา 10 วินาทีโดยค่าเริ่มต้น ก่อนจะค่อยๆ หายไปอย่างช้าๆ การแจ้งเตือนจะประกอบด้วยการอัพเดทผลิตภัณฑ์ที่เสร็จสิ้น อุปกรณ์ใหม่ที่เชื่อมต่อ งานด้านการสแกนไวรัสที่เสร็จสมบูรณ์ หรือการค้นพบภัยคุกคามใหม่



แสดงการแจ้งเตือนบนเดสก์ท็อป – เราขอแนะนำให้เปิดใช้งานตัวเลือกนี้เพื่อให้ผลิตภัณฑ์สามารถแจ้งให้คุณ

ทราบเมื่อมีเหตุการณ์ใหม่เกิดขึ้น

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:

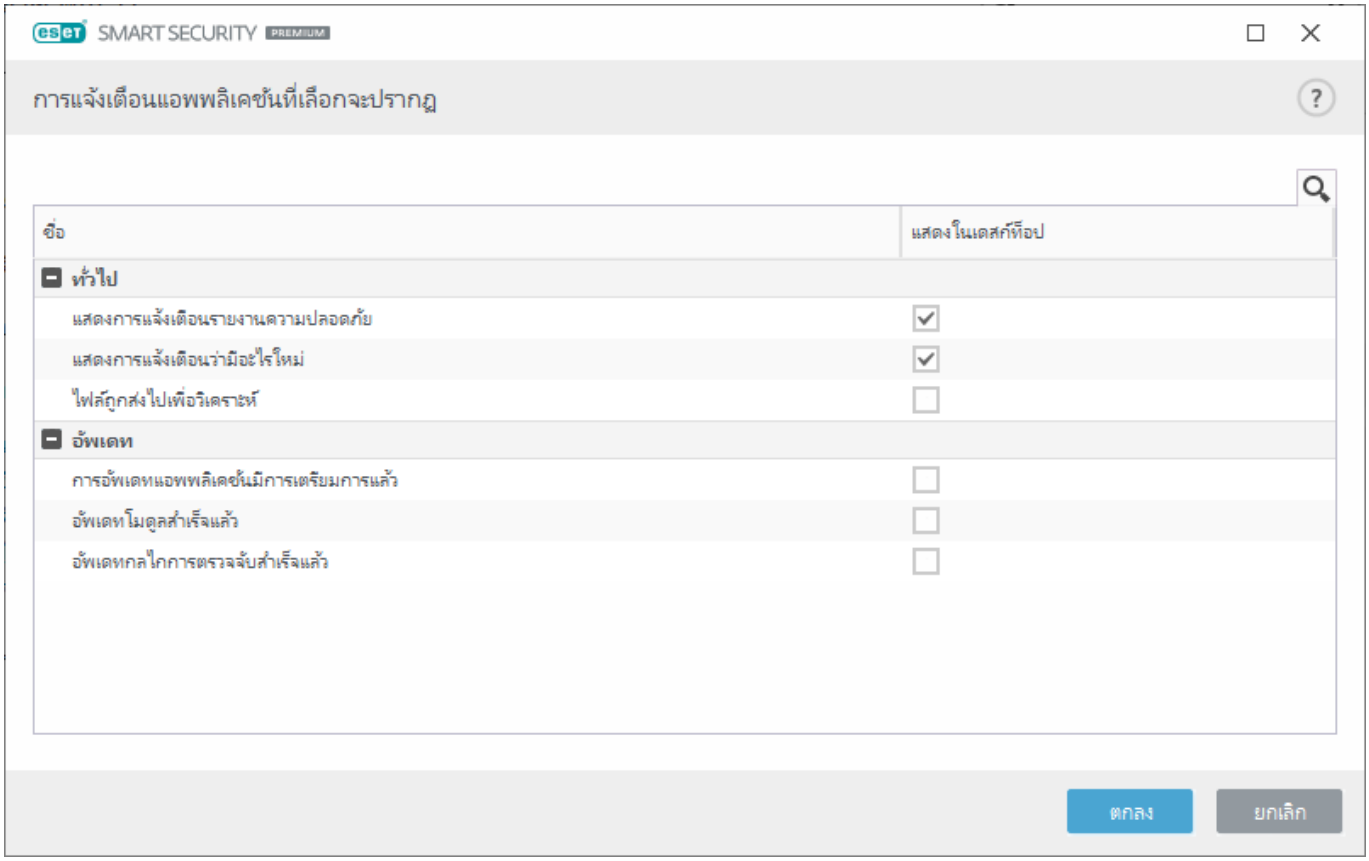
- o**การวินิจฉัย** – แสดงข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- o**แจ้งข้อมูล** – แสดงข้อความแจ้งข้อมูล เช่น กิจกรรมเครือข่ายที่ไม่ปกติ รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น
- o**คำเตือน** – แสดงข้อความเตือนและข้อผิดพลาดร้ายแรง (เช่น Antistealth ทำงานผิดปกติหรือการอัพเดทล้มเหลว)
- o**ข้อผิดพลาด** – แสดงข้อผิดพลาด (เช่น การป้องกันไฟล์เอกสารไม่เริ่มต้นทำงาน) และข้อผิดพลาดร้ายแรง
- o**ร้ายแรง** – แสดงเฉพาะข้อผิดพลาดร้ายแรง (พบข้อผิดพลาดในการเริ่มต้นการป้องกันไวรัสหรือระบบที่ติดไวรัส และอื่นๆ)

ในระบบที่มีผู้ใช้หลายราย แสดงการแจ้งเตือนบนหน้าจอของผู้ใช้รายนี้ – อนุญาตให้บัญชีที่เลือกสามารถรับการแจ้งเตือนบนเดสก์ท็อปได้ ตัวอย่างเช่น หากคุณไม่ได้ใช้บัญชีผู้ดูแลระบบ ให้พิมพ์ชื่อเต็มของบัญชี จากนั้นระบบจะแสดงการแจ้งเตือนบนเดสก์ท็อปสำหรับบัญชีที่ระบุ โดยจะมีเพียงบัญชีเดียวเท่านั้นที่สามารถรับการแจ้งเตือนบนเดสก์ท็อปได้

อนุญาตให้การแจ้งเตือนจับโฟกัสหน้าจอได้ – อนุญาตให้การแจ้งเตือนจับโฟกัสหน้าจอและเข้าถึงได้ด้วยเมนู **ALT + Tab**

รายการการแจ้งเตือนบนเดสก์ท็อป

หากต้องการปรับการมองเห็นการแจ้งเตือนบนเดสก์ท็อป (แสดงอยู่ที่ด้านล่างขวาของหน้าจอ) ให้เปิด **การตั้งค่าขั้นสูง** (F5) > **การแจ้งเตือน** > **การแจ้งเตือนบนเดสก์ท็อป** คลิก **แก้ไข** ถัดจาก **การแจ้งเตือนบนเดสก์ท็อป** แล้วเลือกช่องทำเครื่องหมาย **แสดง** ที่เหมาะสม



ทั่วไป

แสดงการแจ้งเตือนรายงานความปลอดภัย – รับการแจ้งเตือนเมื่อมีการสร้าง รายงานความปลอดภัย ใหม่

แสดงการแจ้งเตือนว่ามีอะไรใหม่ – การแจ้งเตือนเกี่ยวกับคุณลักษณะของเวอร์ชันผลิตภัณฑ์ล่าสุดที่ได้รับการปรับปรุงใหม่ทั้งหมด

ไฟล์ถูกส่งไปเพื่อการวิเคราะห์ - รับการแจ้งเตือนทุกครั้งที่ ESET Smart Security Premium ส่งไฟล์สำหรับการวิเคราะห์

อัพเดท

เตรียมอัปเดตแอพพลิเคชันแล้ว – รับการแจ้งเตือนเมื่อมีการอัปเดตเป็นเวอร์ชันใหม่ ESET Smart Security Premium ที่เตรียมไว้แล้ว

กลไกการตรวจหาได้รับการปรับปรุงเรียบร้อยแล้ว – รับการแจ้งเตือนเมื่อผลิตภัณฑ์การอัพเดทโมดูลกลไกการตรวจจับ

โมดูลได้รับการปรับปรุงเรียบร้อยแล้ว - รับการแจ้งเตือนเมื่อผลิตภัณฑ์อัพเดทส่วนประกอบของโปรแกรม

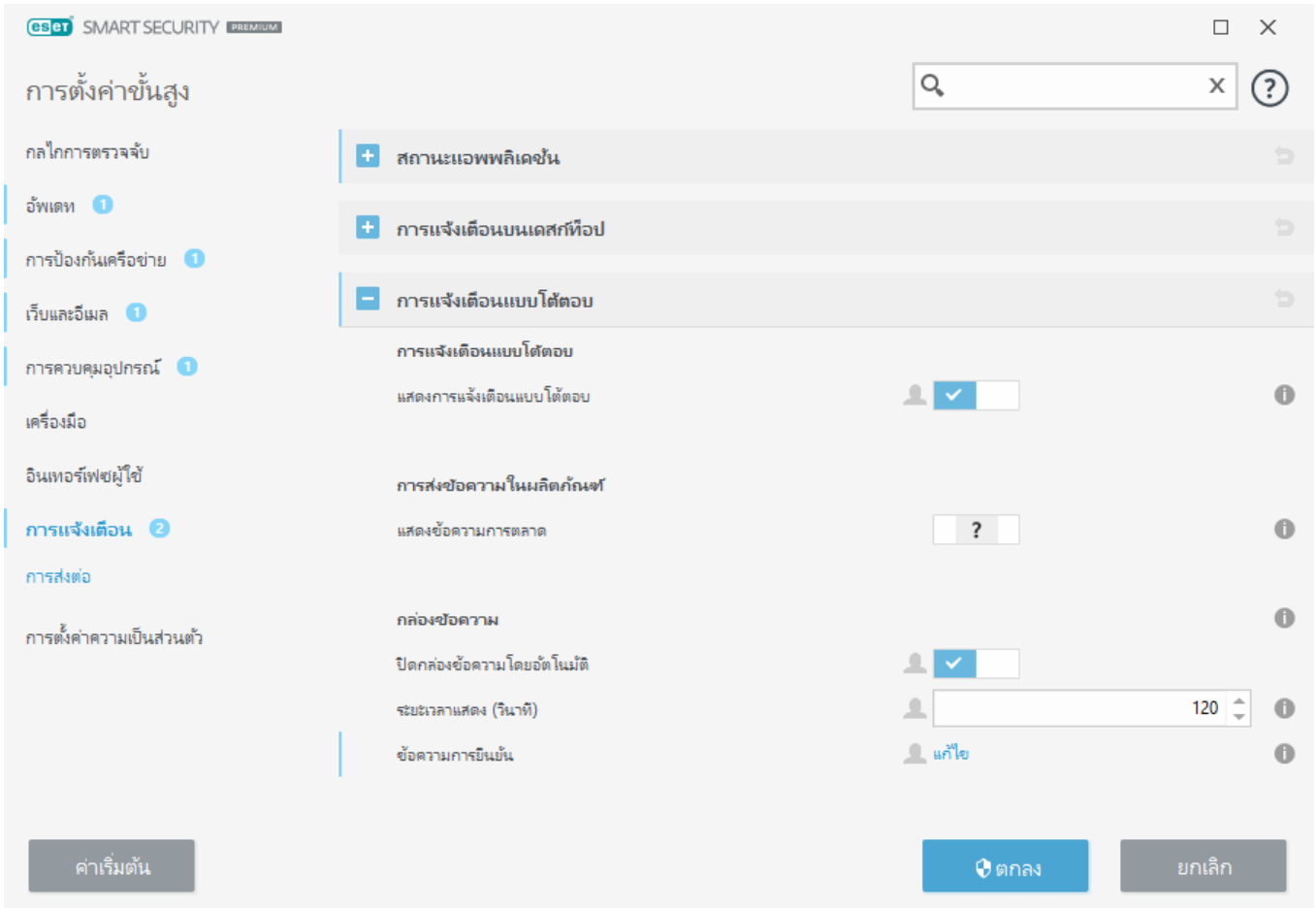
หากต้องการตั้งค่าทั่วไปสำหรับการแจ้งเตือนบนเดสก์ท็อป ตัวอย่างเช่น ข้อความจะปรากฏขึ้นนานเพียงใดหรือความละเอียดขั้นต่ำของเหตุการณ์ที่จะแสดง ดูที่ การแจ้งเตือนบนเดสก์ท็อป ใน **การตั้งค่าขั้นสูง** (F5) > **การแจ้งเตือน**

การแจ้งเตือนแบบโต้ตอบ

มองหาข้อมูลเกี่ยวกับการเตือนและการแจ้งเตือนทั่วไปอยู่ใช่ไหม

- พบภัยคุกคาม
- ที่อยู่ถูกปิดกั้นแล้ว
- ยังไม่ได้เปิดใช้งานผลิตภัณฑ์
- เปลี่ยนเป็นผลิตภัณฑ์ที่มีคุณลักษณะมากขึ้น
- เปลี่ยนเป็นผลิตภัณฑ์รุ่นรอง
- มีรายการอัปเดตให้ใช้งานได้
- ข้อมูลการอัพเดทไม่ตรงกัน
- การแก้ไขปัญหาสำหรับข้อความ "อัพเดทโมดูลไม่สำเร็จ"
- แก้ไขข้อผิดพลาดในการอัพเดทโมดูล
- ปิดกั้นภัยคุกคามเครือข่ายแล้ว
- ใบรับรองเว็บไซต์ที่ยกเลิก

ส่วน **การแจ้งเตือนแบบโต้ตอบ** ใน **การตั้งค่าขั้นสูง** (F5) > **การแจ้งเตือน** ช่วยให้คุณสามารถกำหนดค่าวิธีการที่กล่องข้อความและการแจ้งเตือนแบบโต้ตอบสำหรับการตรวจจับ ซึ่งจำเป็นต้องมีการตัดสินใจโดยผู้ใช้ (ตัวอย่างเช่น เว็บไซต์ที่อาจเป็นการฟิชชิ่ง) จะได้รับการจัดการโดย ESET Smart Security Premium



การแจ้งเตือนแบบโต้ตอบ

การปิดใช้งาน **แสดงการแจ้งเตือนแบบโต้ตอบ** จะซ่อนหน้าต่างการเตือนและข้อความในเบราว์เซอร์ทั้งหมด และจะเหมาะสำหรับสถานการณ์เฉพาะที่มีจำนวนจำกัดเท่านั้น ESET ขอแนะนำให้เปิดใช้งานตัวเลือกนี้ไว้

การส่งข้อความในผลิตภัณฑ์

การส่งข้อความในผลิตภัณฑ์ไม่ได้ออกแบบมาเพื่อแจ้งข่าวสารและการติดต่อสื่อสารอื่นๆ ของ ESET ให้ผู้ใช้ทราบ การส่งข้อความการตลาดจะต้องได้รับการยินยอมจากผู้ใช้ ดังนั้นการส่งข้อความการตลาดจะไม่ถูกส่งให้ผู้ใช้โดยค่าเริ่มต้น (แสดงในเครื่องหมายคำถาม) โดยการเปิดใช้งานตัวเลือกนี้ คุณยอมที่จะรับข้อความการตลาดของ ESET หากคุณไม่สนใจที่จะรับข้อมูลทางการตลาดของ ESET ให้ปิดใช้งานตัวเลือก **แสดงข้อความด้านการตลาด**

กล่องข้อความ

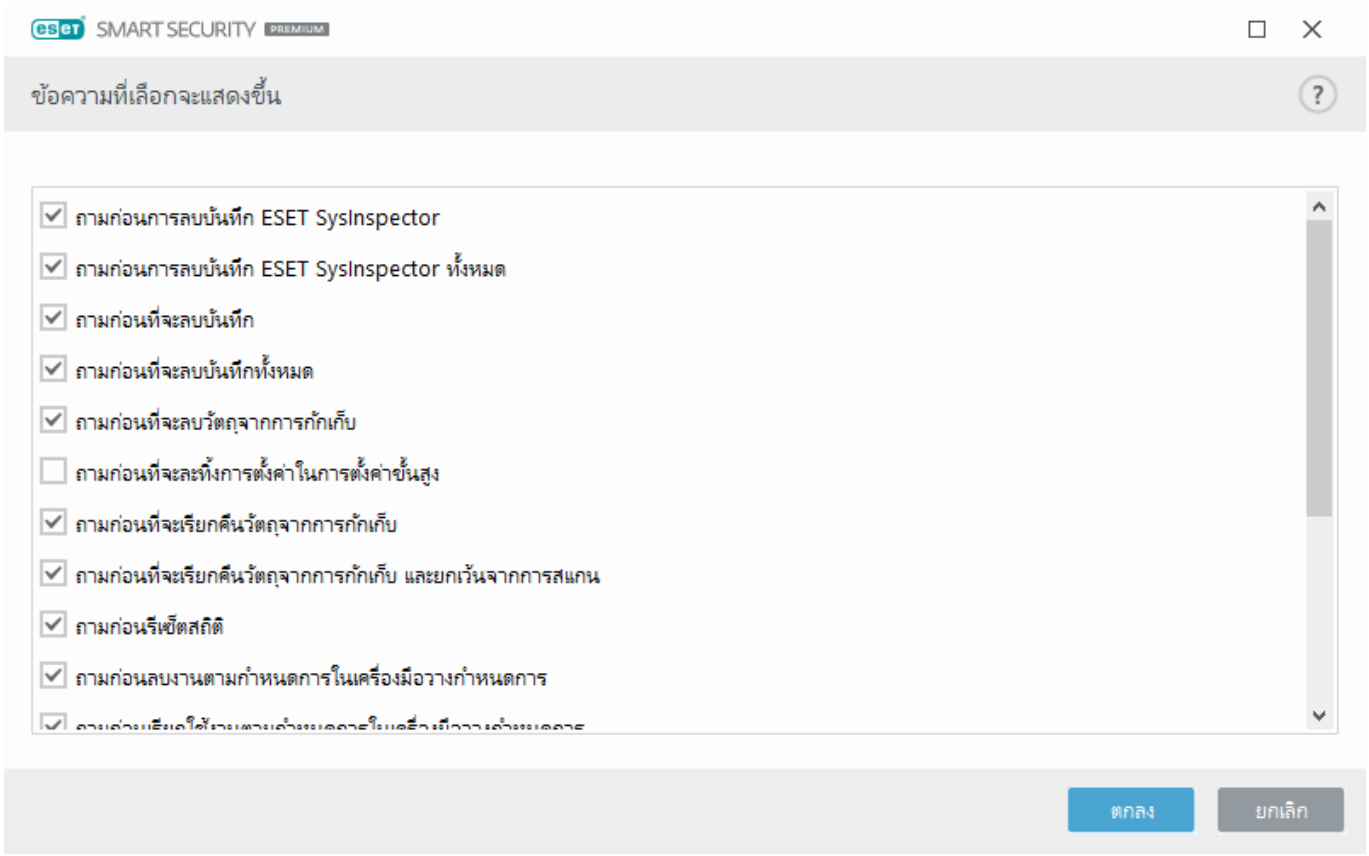
หากต้องการปิดกล่องข้อความโดยอัตโนมัติหลังจากปรากฏมาเป็นระยะเวลาหนึ่ง ให้เลือก **ปิดกล่องข้อความโดยอัตโนมัติ** หากไม่ปิดหน้าต่างดังกล่าวด้วยตนเอง หน้าต่างการเตือนจะปิดโดยอัตโนมัติหลังจากหมดเวลาตามที่กำหนด

หมดเวลาเป็นวินาที – ตั้งค่าระยะเวลาที่สามารถมองเห็นการเตือนได้ โดยค่านี้จะต้องอยู่ระหว่าง 10-999 วินาที

ข้อความการยืนยัน – คลิก **แก้ไข** เพื่อแสดง รายการของข้อความการยืนยัน ซึ่งคุณสามารถเลือกให้แสดงหรือไม่แสดงก็ได้

ข้อความการยืนยัน

ในการปรับข้อความการยืนยัน ให้ไปที่ **การตั้งค่าขั้นสูง** (F5) > **การแจ้งเตือน** > **การแจ้งเตือนแบบโต้ตอบ** และคลิก **แก้ไข** ถัดจาก **ข้อความการยืนยัน**



หน้าต่างข้อความนี้แสดงข้อความการยืนยันที่ ESET Smart Security Premium จะแสดงขึ้นมาก่อนที่จะดำเนินการทำงานใดๆ เลือกหรือยกเลิกการเลือกกล่องทำเครื่องหมายที่อยู่ถัดจากแต่ละข้อความการยืนยันเพื่ออนุญาตหรือปิดใช้งานข้อความเหล่านั้น

เรียนรู้เพิ่มเติมเกี่ยวกับคุณลักษณะเฉพาะที่เกี่ยวข้องกับข้อความการยืนยัน:

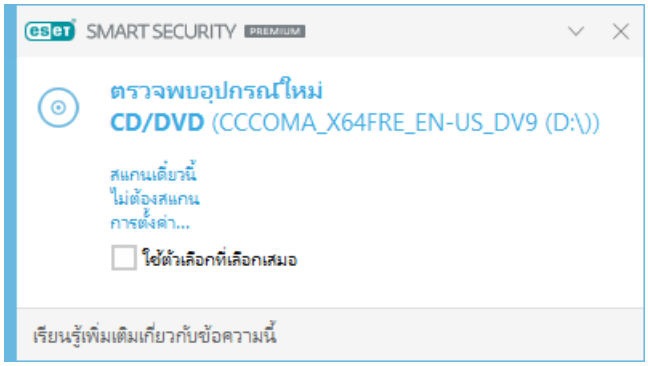
- ถามก่อนการลบบันทึก ESET SysInspector
- ถามก่อนการลบบันทึก ESET SysInspector ทั้งหมด
- ถามก่อนที่จะลบวัตถุจากการกักเก็บ

- ถามก่อนที่จะละทิ้งการตั้งค่าในการตั้งค่าขั้นสูง
- ถามก่อนเว้นภัยคุกคามที่ตรวจพบทิ้งไว้จากหน้าต่างการเตือน
- ถามก่อนที่จะลบบันทึก
- ถามก่อนลบงานตามกำหนดการในเครื่องมือวางกำหนดการ
- ถามก่อนที่จะลบบันทึกทั้งหมด
- ถามก่อนรีเซ็ตสถิติ
- ถามก่อนที่จะเรียกคืนวัตถุจากการกักเก็บ
- ถามก่อนที่จะเรียกคืนวัตถุจากการกักเก็บ และยกเว้นจากการสแกน
- ถามก่อนเรียกใช้งานตามกำหนดการในเครื่องมือวางกำหนดการ
- แสดงการแจ้งเตือนผลลัพธ์ของกระบวนการป้องกันสแปม
- แสดงการแจ้งเตือนผลลัพธ์ของกระบวนการป้องกันสแปมของไคลเอ็นต์อีเมล
- แสดงข้อความยืนยันผลิตภัณฑ์สำหรับอีเมลไคลเอ็นต์ Outlook Express และ Windows Mail
- แสดงข้อความยืนยันผลิตภัณฑ์สำหรับ Windows Live Mail
- แสดงข้อความยืนยันผลิตภัณฑ์สำหรับอีเมลไคลเอ็นต์ Outlook

สื่อที่ถอดเข้าออกได้

ESET Smart Security Premium จะทำการสแกนสื่อที่ถอดเข้าออกได้ (ซีดี/ดีวีดี/USB/...) โดยอัตโนมัติขณะใส่เข้าไปในคอมพิวเตอร์ ซึ่งอาจเป็นประโยชน์ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์ต้องการป้องกันไม่ให้ผู้ใช้ใช้งานสื่อที่ถอดเข้าออกได้ที่มีเนื้อหาที่ไม่พึงประสงค์

เมื่อใส่อุปกรณ์สื่อที่ถอดเข้าออกได้ และมีการตั้งค่า **แสดงตัวเลือกการสแกน** ใน ESET Smart Security Premium ข้อความต่อไปนี้จะปรากฏขึ้น:



ตัวเลือกสำหรับกล่องโต้ตอบนี้:

- **สแกนเดี๋ยวนี้** – ตัวเลือกนี้จะเรียกใช้การสแกนอุปกรณ์สื่อที่ถอดเข้าออกได้
- **ไม่ต้องสแกน** – สื่อที่ถอดเข้าออกได้จะไม่ถูกสแกน
- **ตั้งค่า** – เปิดส่วน**การตั้งค่าขั้นสูง**
- **ใช้ตัวเลือกที่เลือกเสมอ** – เมื่อเลือกตัวเลือกนี้ การดำเนินการแบบเดิมจะเกิดขึ้นเมื่อใส่อุปกรณ์สื่อที่ถอดเข้าออกได้ในเวลาอื่น

นอกจากนี้ ESET Smart Security Premium จะมีคุณลักษณะของฟังก์ชันการควบคุมอุปกรณ์ ซึ่งช่วยให้คุณสามารถกำหนดกฎในการใช้งานอุปกรณ์ภายนอกบนเครื่องคอมพิวเตอร์ที่ระบุได้ สามารถดูรายละเอียดเพิ่มเติมเกี่ยวกับการควบคุมอุปกรณ์ได้ในส่วน สื่อที่ถอดเข้าออกได้

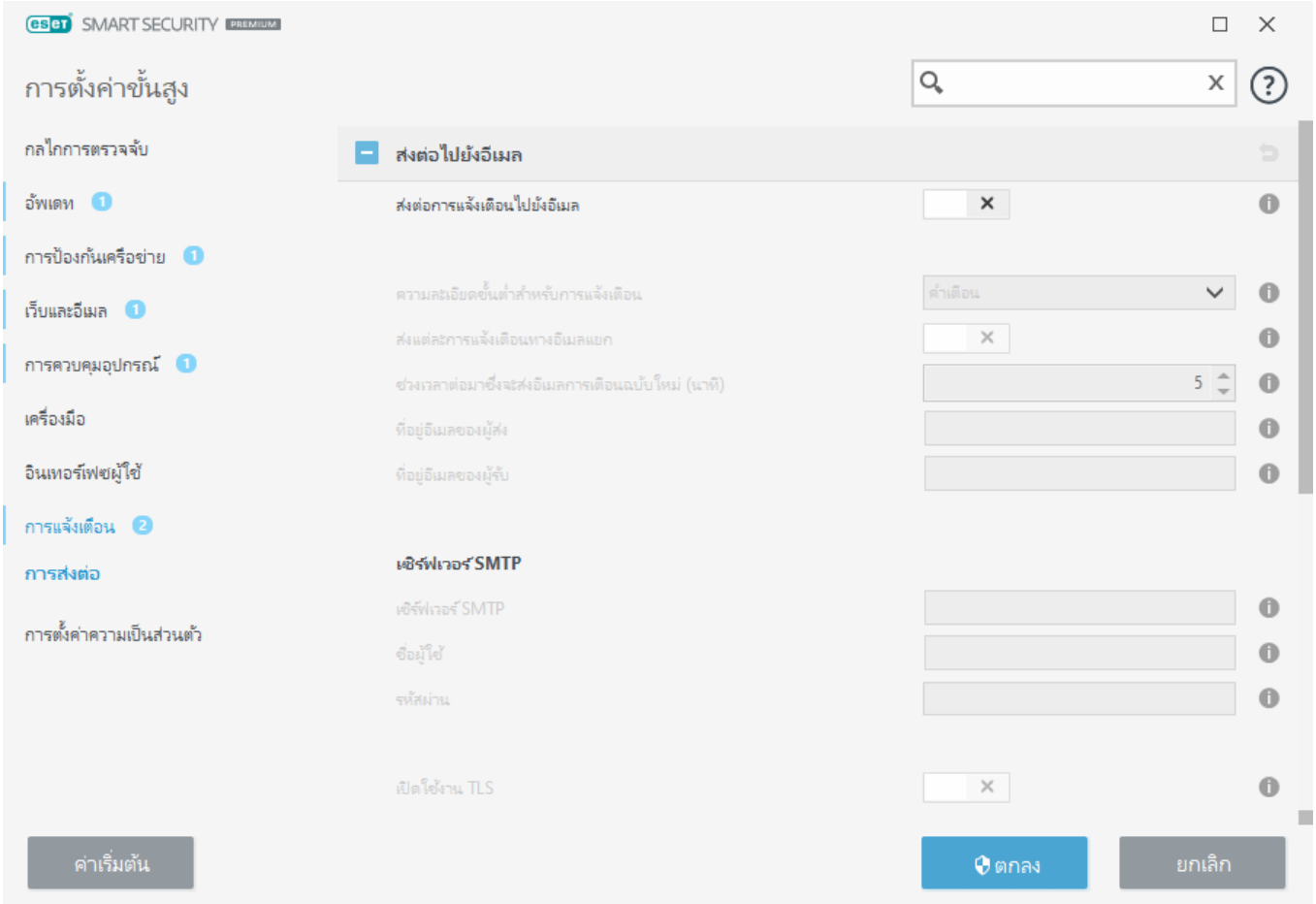
ในการเข้าถึงการตั้งค่าสำหรับการสแกนสื่อที่ถอดเข้าออกได้ ให้เปิด การตั้งค่าขั้นสูง (**F5**) > **กลไกการตรวจจับ** > **การสแกนมัลแวร์** > **สื่อที่ถอดเข้าออกได้**

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

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

การส่งต่อ

ESET Smart Security Premium สามารถส่งอีเมลแจ้งเตือนได้โดยอัตโนมัติหากมีเหตุการณ์ที่มีระดับความละเอียดที่เลือกไว้เกิดขึ้น เปิด **การตั้งค่าขั้นสูง** (F5) > **การแจ้งเตือน** > **การส่งต่อ** และเปิดใช้งาน **ส่งต่อการแจ้งเตือนไปยังอีเมล** เพื่อเปิดใช้งานการแจ้งเตือนทางอีเมล



จากเมนูแบบเลื่อนลง **ความละเอียดขั้นต่ำสำหรับการแจ้งเตือน** คุณสามารถเลือกระดับความรุนแรงเริ่มต้นของการแจ้งเตือนที่จะส่ง

- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- **มีข้อมูล** – บันทึกข้อความแจ้งข้อมูล เช่น กิจกรรมเครือข่ายที่ไม่ได้มาตรฐาน รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน (Antistealth ทำงานผิดปกติหรือการอัพเดทล้มเหลว)
- **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

SMTP เซิร์ฟเวอร์

SMTP เซิร์ฟเวอร์ – เซิร์ฟเวอร์SMTP ที่ใช้สำหรับการส่งการแจ้งเตือน (ตัวอย่างเช่น smtp.provider.com:587 พอร์ตที่ระบุไว้ล่วงหน้าคือ 25)

> เซิร์ฟเวอร์ SMTP ที่มีการเข้ารหัส TLS นั้น ได้รับการสนับสนุนโดย ESET Smart Security Premium

ชื่อผู้ใช้ และ **รหัสผ่าน** – ถ้าเซิร์ฟเวอร์ SMTP ต้องมีการตรวจสอบสิทธิ์ ผู้ใช้ควรป้อนชื่อผู้ใช้และรหัสผ่านที่ถูกต้องในช่องเหล่านี้เพื่อเข้าถึงเซิร์ฟเวอร์ SMTP

เปิดใช้งาน TLS – Secure Alert และข้อความการแจ้งเตือนโดยไม่ใช้การเข้ารหัส TLS

ทดสอบการเชื่อมต่อ SMTP – อีเมลทดสอบจะถูกส่งไปยังที่อยู่อีเมลของผู้รับ จะต้องเติมเซิร์ฟเวอร์ SMTP ชื่อผู้ใช้ รหัสผ่าน ที่อยู่ของผู้ส่ง และที่อยู่ของผู้รับ

รูปแบบข้อความ

การสื่อสารระหว่างโปรแกรมและผู้ใช้หรือผู้ดูแลระบบระยะไกลจะกระทำผ่านอีเมลหรือข้อความ LAN (โดยใช้บริการส่งข้อความของ Windows) **ใช้รูปแบบข้อความเริ่มต้น** สำหรับข้อความการเตือนและการแจ้งเตือนจะเหมาะสมที่สุดสำหรับสถานการณ์ส่วนใหญ่ แต่ในบางกรณี คุณอาจต้องการเปลี่ยนรูปแบบข้อความของข้อความเหตุการณ์

รูปแบบของข้อความเหตุการณ์ – รูปแบบข้อความของเหตุการณ์ที่แสดงบนคอมพิวเตอร์ระยะไกล

รูปแบบของข้อความเตือนภัยคุกคาม – ข้อความการเตือนและข้อความการแจ้งเตือนภัยคุกคามจะมีรูปแบบเริ่มต้นที่กำหนดไว้ล่วงหน้า ESET แนะนำให้เก็บรูปแบบที่กำหนดไว้ล่วงหน้านี้ไว้ 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 "?"

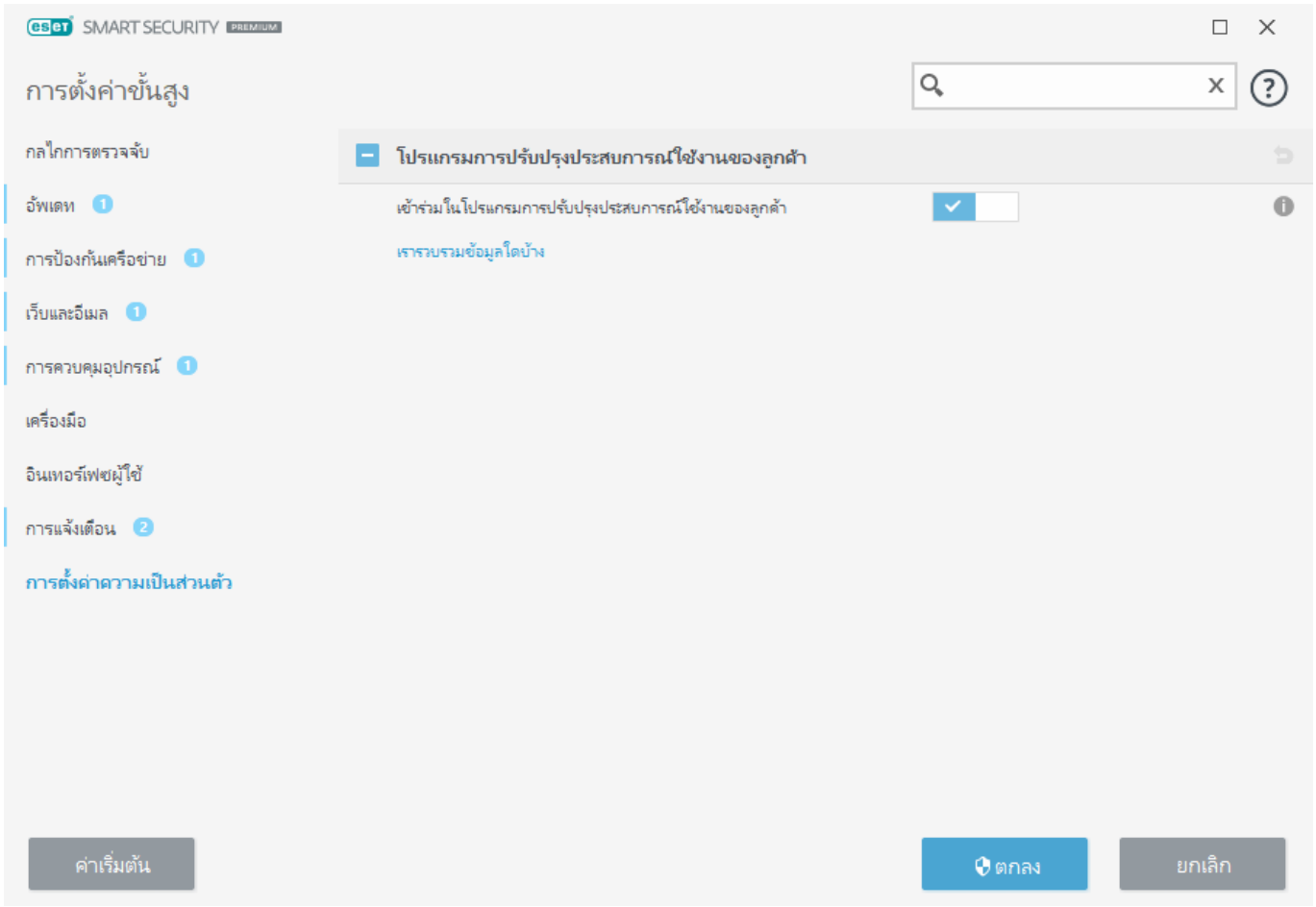
ใช้การเข้ารหัสในรูปแบบ Quoted-printable - ที่มาของข้อความอีเมลจะถูกเข้ารหัสในรูปแบบ Quoted-printable (QP) ซึ่งใช้อักขระ ASCII และสามารถส่งอักขระพิเศษของภาษาทางอีเมลได้อย่างถูกต้องในรูปแบบ 8 บิต (áéíóú)

- **%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

การตั้งค่าความเป็นส่วนตัว

ในหน้าต่างโปรแกรมหลัก คลิก **การตั้งค่า** > **การตั้งค่าขั้นสูง** (F5) > **การตั้งค่าความเป็นส่วนตัว**



โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า

เปิดใช้งานแถบเลื่อนที่อยู่ถัดจาก **เข้าร่วมในโปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า** เพื่อเข้าร่วมโปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า เมื่อเข้าร่วมแล้ว คุณจะต้องให้ข้อมูลที่ไม่ระบุตัวตนเกี่ยวกับการใช้ผลิตภัณฑ์ ESET แก่ ESET ข้อมูลที่รวบรวมจะช่วยให้เราปรับปรุงประสบการณ์ของคุณได้ และข้อมูลดังกล่าวจะไม่ถูกแบ่งปันกับบุคคลที่สาม เรารวบรวมข้อมูลใดบ้าง

โปรไฟล์

ตัวจัดการโปรไฟล์ถูกใช้อยู่สองส่วนภายใน ESET Smart Security Premium ในส่วน **การสแกนคอมพิวเตอร์ตามต้องการ** และในส่วน **อัพเดท**

การสแกนคอมพิวเตอร์

โปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าใน ESET Smart Security Premium จะมีอยู่ด้วยกันทั้งหมด 4 รายการ:

- **การสแกนแบบสมาร์ท** - เป็นการสแกนขั้นสูงตามค่าเริ่มต้น โดยโปรไฟล์การสแกนแบบสมาร์ทใช้เทคโน

โลยี Smart Optimization ซึ่งไม่รวมไฟล์ที่พบว่าปลอดภัยในการสแกนก่อนหน้านี้และไม่ได้ถูกแก้ไขตั้งแต่การสแกนครั้งก่อนหน้า วิธีนี้ช่วยให้เวลาในการสแกนลดลงโดยมีผลกระทบต่อความปลอดภัยของระบบน้อยที่สุด

• **การสแกนเมนูบริบท** - คุณสามารถเริ่มสแกนไฟล์ใดก็ได้จากเมนูบริบทได้ตามต้องการ โปรไฟล์การสแกนเมนูบริบทจะช่วยให้คุณกำหนดการกำหนดค่าการสแกนซึ่งจะใช้เมื่อคุณเปิดการสแกนวิธีนี้

• **สแกนเชิงลึก** - โปรไฟล์การสแกนเชิงลึกไม่ได้ใช้ Smart Optimization โดยค่าเริ่มต้น ดังนั้นจะไม่มีไฟล์ใดที่ไม่รวมอยู่ในการสแกนเมื่อใช้โปรไฟล์นี้

• **การสแกนคอมพิวเตอร์** - เป็นโปรไฟล์ตามค่าเริ่มต้นที่ใช้ในการสแกนคอมพิวเตอร์มาตรฐาน

คุณสามารถบันทึกพารามิเตอร์การสแกนที่ต้องการได้เพื่อการสแกนในอนาคต ขอแนะนำให้คุณสร้างโปรไฟล์อีกโปรไฟล์หนึ่ง (ที่มีเป้าหมายการสแกน วิธีการสแกน และพารามิเตอร์อื่นๆ) สำหรับแต่ละการสแกนที่ใช้เป็นประจำ

หากต้องการสร้างโปรไฟล์ใหม่ ให้เปิดหน้าต่างการตั้งค่าขั้นสูง (F5) และคลิก **กลไกตรวจหา** > **การสแกนมัลแวร์** > **การสแกนตามต้องการ** > **รายการของโปรไฟล์** หน้าต่าง **ตัวจัดการโปรไฟล์** มีเมนูแบบเลื่อนลง **โปรไฟล์ที่เลือก** ซึ่งแสดงโปรไฟล์การสแกนที่มีอยู่และตัวเลือกสำหรับสร้างโปรไฟล์ใหม่ เพื่อช่วยให้คุณสร้างโปรไฟล์การสแกนให้เหมาะสมกับความต้องการ โปรดไปที่ส่วน ThreatSenseการตั้งค่าพารามิเตอร์กลไก เพื่อดูคำอธิบายของพารามิเตอร์แต่ละรายการของการตั้งค่าการสแกน

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

อัพเดท

เครื่องมือแก้ไขโปรไฟล์ในส่วนการตั้งค่าการอัพเดทจะช่วยให้ผู้ใช้สร้างโปรไฟล์การอัพเดทใหม่ สร้างและใช้โปรไฟล์แบบกำหนดเองของคุณ (นอกเหนือจาก **โปรไฟล์ของฉัน** ที่เป็นค่าเริ่มต้น) ต่อเมื่อคอมพิวเตอร์ของคุณใช้วิธีการเชื่อมต่อหลายวิธีในการอัพเดทเซิร์ฟเวอร์

ตัวอย่างเช่น แล็ปท็อปที่โดยปกติแล้วจะเชื่อมต่อกับเซิร์ฟเวอร์ในระบบ (มิเรอร์) ในเครือข่ายในระบบ แต่จะดาวน์โหลดการอัพเดทโดยตรงจากเซิร์ฟเวอร์การอัพเดทของ ESET เมื่อตัดการเชื่อมต่อจากเครือข่ายในระบบ (การเดินทางเพื่อธุรกิจ) อาจใช้โปรไฟล์สองโปรไฟล์: โปรไฟล์แรกใช้เพื่อเชื่อมต่อกับเซิร์ฟเวอร์ในระบบ และอีกโปรไฟล์หนึ่งใช้เพื่อเชื่อมต่อกับเซิร์ฟเวอร์ของ ESET หลังจากโปรไฟล์เหล่านี้ได้รับการกำหนดค่าแล้ว ให้นำทางไปยัง **เครื่องมือ** > **เครื่องมือวางกำหนดการ** และแก้ไขพารามิเตอร์งานการอัพเดท กำหนดโปรไฟล์หนึ่งเป็นโปรไฟล์หลักและ

อีกแบบหนึ่งเป็นโปรไฟล์สำรอง

โปรไฟล์การอัพเดท – โปรไฟล์การอัพเดทที่ใช้อยู่ในขณะนี้ เมื่อต้องการเปลี่ยนแปลง ให้เลือกโปรไฟล์จากเมนูแบบเลื่อนลง

รายการของโปรไฟล์ – สร้างโปรไฟล์อัพเดทใหม่หรือลบโปรไฟล์อัพเดทที่มีอยู่

แป้นพิมพ์ลัด

เพื่อให้การนำทางใน ESET Smart Security Premium ดียิ่งขึ้น คุณสามารถใช้แป้นพิมพ์ลัดต่อไปนี้ได้:

แป้นพิมพ์ลัด	การทำงาน
F1	เปิดหน้าวิธีใช้
F5	เปิดการตั้งค่าขั้นสูง
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

การวินิจฉัย

การวินิจฉัยจะให้บันทึกข้อมูลความล้มเหลวของแอพพลิเคชันของกระบวนการ ESET (ekrn เป็นต้น) หากแอพพลิเคชันล่ม บันทึกข้อมูลความล้มเหลวจะถูกสร้างขึ้น สิ่งนี้สามารถช่วยให้นักพัฒนาแก้ไขปัญหาและปรับแก้ปัญหาต่างๆ ของ ESET Smart Security Premium 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

เปิดใช้งานการบันทึกขั้นสูงในข้อความทางการตลาด – บันทึกเหตุการณ์ทั้งหมดที่เกี่ยวข้องกับข้อความทางการตลาดภายในผลิตภัณฑ์

เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันสแปม – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นระหว่างการสแกนสแปม ซึ่งจะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับกลไก ESET Antispam

เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันการโจรกรรม – บันทึกเหตุการณ์ทั้งหมดในการป้องกันโจรกรรมเพื่อให้สามารถดำเนินการวินิฉัยและแก้ปัญหาได้

เปิดใช้งานการบันทึกขั้นสูงการป้องกันทางด้านธนาคารและการชำระเงิน – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการป้องกันการธนาคารและการชำระเงิน

เปิดใช้งานการบันทึกขั้นสูงสำหรับเครื่องมือสแกน – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นระหว่างการสแกนไฟล์และโฟลเดอร์โดยการสแกนคอมพิวเตอร์

เปิดใช้งานการบันทึกขั้นสูงสำหรับการควบคุมเนื้อหา – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการควบคุมอุปกรณ์ ซึ่งจะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับการควบคุมอุปกรณ์ได้

เปิดใช้งานการบันทึกขั้นสูงสำหรับ Direct Cloud – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นใน ESET LiveGrid® ซึ่งจะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับ ESET LiveGrid® ได้

เปิดใช้งานการบันทึกขั้นสูงของการป้องกันเอกสาร – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการป้องกันเอกสาร

เพื่ออนุญาตการวินิจฉัยและการแก้ไขปัญหา

เปิดใช้งานการบันทึกขั้นสูงของการป้องกันอีเมลไคลเอ็นต์ - บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการป้องกันอีเมลไคลเอ็นต์และปลั๊กอินอีเมลไคลเอ็นต์เพื่อให้สามารถดำเนินการวินิจฉัยและแก้ปัญหาได้

เปิดใช้งานการบันทึกขั้นสูงสำหรับเคอร์เนล – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในเคอร์เนล ESET (ekrn)

เปิดใช้งานการอนุญาตการบันทึกขั้นสูง – บันทึกการสื่อสารทั้งหมดของผลิตภัณฑ์ด้วยการเปิดใช้งาน ESET หรือเซิร์ฟเวอร์ ESET License Manager

เปิดใช้งานการบันทึกขั้นสูงสำหรับ ESET LiveGuard – บันทึกเหตุการณ์ทั้งหมดใน ESET LiveGuard เพื่อให้สามารถดำเนินการวินิฉัยและแก้ปัญหาได้

เปิดใช้งานการติดตามหน่วยความจำ - บันทึกเหตุการณ์ทั้งหมดที่จะช่วยนักพัฒนาในการวินิจฉัยปัญหาหน่วยความจำรั่ว

เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันเครือข่าย - บันทึกข้อมูลทั้งหมดในเครือข่ายที่ส่งผ่านไฟร์วอลล์ในรูปแบบ PCAP เพื่อช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวข้องกับไฟร์วอลล์ได้

เปิดใช้งานการบันทึกขั้นสูงสำหรับระบบปฏิบัติการ – บันทึกข้อมูลเพิ่มเติมเกี่ยวกับระบบปฏิบัติการ เช่น กระบวนการที่ทำงานอยู่ กิจกรรม CPU และการทำงานของดิสก์ ซึ่งสามารถช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับผลิตภัณฑ์ ESET ที่ทำงานอยู่ในระบบปฏิบัติการของคุณได้

เปิดใช้งานการบันทึกขั้นสูงสำหรับการควบคุมเนื้อหา – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการควบคุมเนื้อหา ซึ่งจะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับการควบคุมเนื้อหาได้

เปิดใช้งานการบันทึกขั้นสูงสำหรับการกรองโปรโตคอล – บันทึกข้อมูลทั้งหมดที่ส่งผ่านกลไกการกรองโปรโตคอลในรูปแบบ PCAP เพื่อช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับการกรองโปรโตคอลได้

เปิดใช้งานการบันทึกขั้นสูงสำหรับการส่งข้อความแบบพุช – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในระหว่างการส่งข้อความแบบพุช

เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันระบบไฟล์แบบเรียลไทม์ – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นระหว่างการสแกนไฟล์และโฟลเดอร์โดยการป้องกันระบบไฟล์แบบเรียลไทม์

เปิดใช้งานการบันทึกขั้นสูงสำหรับกลไกอัพเดท – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในกระบวนการอัพเดท ซึ่งการทำเช่นนี้จะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวข้องกับกลไกการอัพเดทได้

แฟ้มบันทึกจะอยู่ใน *C:\ProgramData\ESET\ESET Security\Diagnostics*

ฝ่ายสนับสนุนด้านเทคนิค

เมื่อ ติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET จาก ESET Smart Security Premium แล้ว คุณสามารถส่งข้อมูลการกำหนดค่าระบบได้ เลือก **ส่งเสมอ** จากเมนูแบบเลื่อนลง **ส่งข้อมูลการกำหนดค่าระบบ** เพื่อส่งข้อมูลโดยอัตโนมัติ หรือเลือก **ถามก่อนส่ง** เพื่อให้ได้รับข้อความเตือนก่อนจะส่งข้อมูล

นำเข้าและส่งออกการตั้งค่า

คุณสามารถนำเข้าหรือส่งออกไฟล์การกำหนดค่า .xml ของ ESET Smart Security Premium ที่กำหนดเองของคุณจากเมนู **การตั้งค่า**

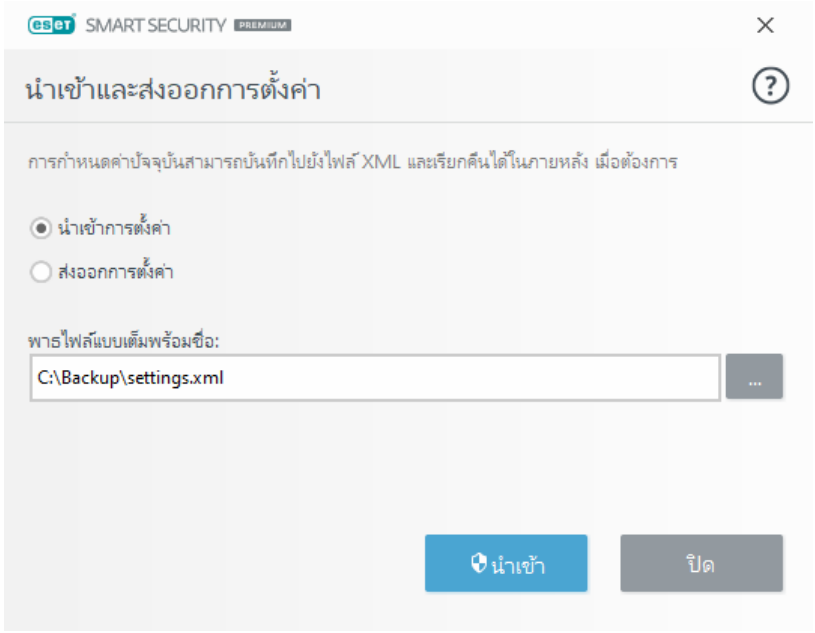
> **คำแนะนำพร้อมภาพประกอบ**
> ดู นำเข้าหรือส่งออกการตั้งค่าการกำหนดค่า ESET โดยใช้ไฟล์ .xml สำหรับคำแนะนำพร้อมภาพประกอบที่แสดงในภาษาอังกฤษและภาษาอื่นๆ

การนำเข้าและการส่งออกไฟล์การกำหนดค่าจะมีประโยชน์ในกรณีที่คุณต้องสำรองการกำหนดค่าปัจจุบันของ ESET Smart Security Premium 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



แปลงกลับการตั้งค่าทุกอย่างในส่วนปัจจุบัน

คลิกลูกศรโค้ง เพื่อแปลงกลับการตั้งค่าทุกอย่างในส่วนปัจจุบันไปเป็นการตั้งค่าเริ่มต้นที่กำหนดโดย ESET

โปรดทราบว่า การเปลี่ยนแปลงใดๆ ที่ดำเนินการไว้จะสูญหายหลังจากที่คุณคลิก **แปลงกลับเป็นค่าเริ่มต้น**

แปลงกลับสารบัญ – เมื่อเปิดใช้งานตัวเลือกนี้ กฎ งานหรือโปรไฟล์ที่ได้เพิ่มด้วยตนเองหรือโดยอัตโนมัติจะสูญหาย

โปรดดู การตั้งค่าการนำเข้าและส่งออก

แปลงกลับเป็นการตั้งค่าเริ่มต้น

คลิก **ค่าเริ่มต้น การตั้งค่าขั้นสูง** (F5) เพื่อแปลงการตั้งค่าโปรแกรมทั้งหมดสำหรับโมดูลทั้งหมดกลับ สิ่งนี้จะถูกรีเซ็ตกลับเป็นสถานะที่เคยมีหลังการติดตั้งใหม่

โปรดดู การตั้งค่าการนำเข้าและส่งออก

เกิดข้อผิดพลาดขณะบันทึกการกำหนดค่า

ข้อความแสดงข้อผิดพลาดนี้ระบุว่าระบบไม่ได้บันทึกการตั้งค่าอย่างถูกต้อง เนื่องจากเกิดข้อผิดพลาด

ซึ่งมักหมายความว่าผู้ใช้ที่พยายามจะปรับแต่งพารามิเตอร์โปรแกรมจะ:

• มีสิทธิ์การเข้าถึงไม่เพียงพอหรือไม่มีสิทธิ์พิเศษของระบบปฏิบัติการที่จำเป็นต้องใช้ในการปรับแต่งไฟล์การกำหนดค่าและรีจิสทรีระบบ
> ในการดำเนินการแก้ไขตามต้องการ ผู้ดูแลระบบต้องลงชื่อเข้า

• ได้เปิดใช้งานโหมดการเรียนรู้ใน HIPS หรือไฟร์วอลล์ และพยายามจะเปลี่ยนแปลงการตั้งค่าขั้นสูง
> ในการบันทึกการกำหนดค่าและหลีกเลี่ยงข้อขัดแย้งในการกำหนดค่า ให้ปิดการตั้งค่าขั้นสูงโดยไม่บันทึกและพยายามเปลี่ยนแปลงตามต้องการอีกครั้ง

สาเหตุทั่วไปลำดับที่สองอาจเป็นการที่โปรแกรมไม่สามารถทำงานได้อย่างถูกต้อง เกิดความเสียหาย และต้องติดตั้งใหม่

เครื่องมือสแกนของบรรทัดคำสั่ง

โมดูลป้องกันไวรัสของ ESET Smart Security Premium นั้นสามารถเรียกใช้ผ่านบรรทัดคำสั่ง ทั้งด้วยตนเอง (โดยใช้คำสั่ง "ecls") หรือใช้ไฟล์แบทช์ ("bat")

การใช้เครื่องสแกนบรรทัดคำสั่งของ ESET:

```
ecls [OPTIONS..] FILES..
```

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

ESET CMD

นี่เป็นคุณลักษณะที่ทำให้สามารถใช้คำสั่ง ecmd แบบขั้นสูงได้ ซึ่งจะช่วยให้คุณสามารถส่งออกและนำเข้าการตั้งค่าได้โดยใช้บรรทัดคำสั่ง (ecmd.exe) ตอนนี้ คุณจะสามารถส่งออกการตั้งค่าได้โดยใช้ GUI เท่านั้น ส่วนการกำหนดค่า ESET Smart Security Premium 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 Smart Security Premium 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

คำสั่งส่งออกการตั้งค่า:
```
ecmd /getcfg c:\config\settings.xml
```
คำสั่งนำเข้าการตั้งค่า:
```
ecmd /setcfg c:\config\settings.xml
```

คำสั่ง ecmd ขั้นสูงสามารถเรียกใช้ในระบบได้เท่านั้น

การลงชื่อไฟล์การกำหนดค่า *.xml*:

1. ดาวน์โหลดไฟล์ที่เรียกใช้ XmlSignTool

2. เปิด Windows Command Prompt (cmd) โดยใช้ **เรียกใช้ในฐานะผู้ดูแล**

3. ไปที่ตำแหน่งที่บันทึก `xmlsigntool.exe`

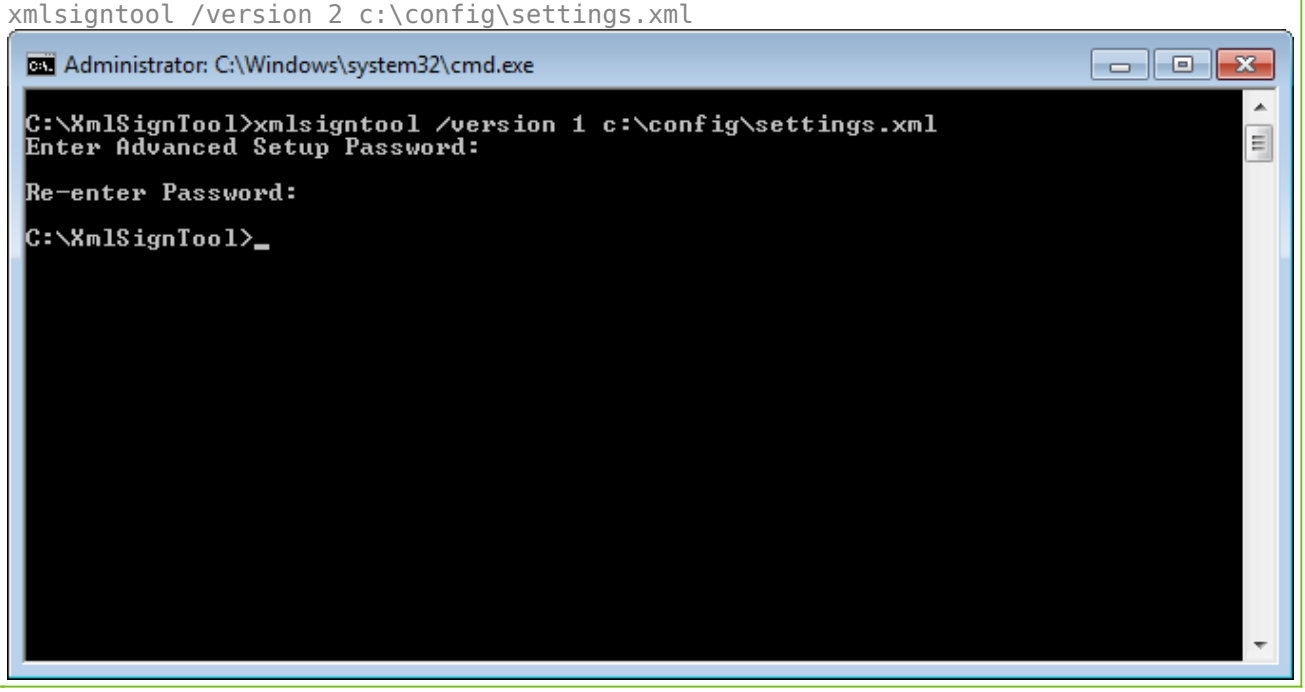
4. ดำเนินการคำสั่งเพื่อลงชื่อไฟล์การกำหนดค่า *.xml* การใช้งาน: `xmlsigntool /version 1|2 <xml_file_path>`

ค่าพารามิเตอร์ของ `/version` จะขึ้นอยู่กับเวอร์ชันของ ESET Smart Security Premium ใช้ `/version 1` กับ ESET Smart Security Premium เวอร์ชันเก่ากว่า 11.1 ใช้ `/version 2` สำหรับ ESET Smart Security Premium เวอร์ชันปัจจุบัน

5. ป้อนแล้วป้อนรหัสผ่านของ การตั้งค่าขั้นสูง อีกครั้งตามที่ได้รับแจ้งจาก XmlSignTool ไฟล์การกำหนดค่า *.xml* ของคุณได้รับการลงชื่อแล้วตอนนี้ และสามารถใช้นำเข้าในอีกอินสแตนซ์หนึ่งของ ESET Smart Security Premium ด้วย ESET CMD ได้โดยใช้วิธีการให้สิทธิ์รหัสผ่าน

คำสั่งลงชื่อไฟล์การกำหนดค่าที่ส่งออก:

```
xmlsigntool /version 2 c:\config\settings.xml
```



หากรหัสผ่าน ตั้งค่าการเข้าถึง ของคุณเปลี่ยนและคุณต้องการนำเข้าการกำหนดค่าที่ลงชื่อไว้ก่อนหน้าด้วยรหัสเก่า คุณจะต้องลงชื่อไฟล์การตั้งค่า *.xml* อีกครั้งโดยใช้รหัสผ่านปัจจุบันของคุณ การดำเนินการนี้จะทำให้คุณสามารถใช้ไฟล์การกำหนดค่าเก่าโดยไม่ต้องส่งออกไปอีกเครื่องที่กำลังเรียกใช้ ESET Smart Security Premium ก่อนที่จะนำเข้า

ไม่แนะนำให้เปิดใช้งาน ESET CMD โดยไม่ใช้วิธีการให้สิทธิ์ เนื่องจากวิธีนี้จะอนุญาตการนำเข้าการกำหนดค่าใดๆ ที่ไม่ได้ลงชื่อ ตั้งรหัสผ่านใน **การตั้งค่าขั้นสูง** > **ส่วนติดต่อผู้ใช้** > **ตั้งค่าการเข้าถึง** เพื่อป้องกันไม่ให้มีการแก้ไขโดยไม่ได้รับอนุญาตจากผู้ใช้

การตรวจหาสภาวะไม่ใช้งาน

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

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

ใช้แถบเลื่อนสำหรับแต่ละสถานะที่สอดคล้องกันเพื่อเปิดหรือปิดใช้งานการเรียกใช้การตรวจหาสถานะไม่ใช้งานต่างๆ

คำถามทั่วไป

คุณสามารถดูคำถามที่พบบ่อยและปัญหาที่พบได้ที่ด้านล่างนี้ คลิกที่ชื่อหัวข้อเพื่อค้นหาวิธีแก้ไขปัญหา:

- วิธีอัพเดท ESET Smart Security Premium
- วิธีลบไวรัสออกจากคอมพิวเตอร์
- วิธีอนุญาตการสื่อสารสำหรับแอพพลิเคชัน
- วิธีเปิดใช้งานการควบคุมเนื้อหาสำหรับบัญชี
- วิธีสร้างงานใหม่ในเครื่องมือวางกำหนดการ
- วิธีวางกำหนดการงานสแกน (รายสัปดาห์)
- วิธีแก้ไข "การป้องกันทางด้านธนาคารและการชำระเงินไม่สามารถเปลี่ยนเส้นทางไปยังหน้าเว็บที่ร้องขอได้"
- วิธีปลดล็อคการตั้งค่าขั้นสูง
- วิธีแก้ปัญหาการปิดใช้งานผลิตภัณฑ์จาก ESET HOME

หากปัญหาของคุณไม่ได้รวมอยู่ในรายการด้านบนนี้ ให้ลองค้นหาในวิธีใช้ออนไลน์ของ ESET Smart Security Premium

หากคุณไม่พบทางแก้ไขสำหรับปัญหา/คำถามในวิธีใช้ออนไลน์ของ ESET Smart Security Premium คุณสามารถไปที่ฐานความรู้ของ ESET แบบออนไลน์ที่มีการอัพเดทเป็นประจำของพวกเราได้ ลิงก์ไปยังบทความฐานความรู้ที่ได้รับความนิยมของพวกเราอยู่ที่ด้านล่างนี้:

- จะต่ออายุใบอนุญาตของฉันได้อย่างไร
- ฉันได้รับข้อผิดพลาดของการเปิดใช้งานขณะติดตั้งผลิตภัณฑ์ ESET หมายความว่าอย่างไร
- เปิดใช้งานผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้านของฉันโดยใช้ชื่อผู้ใช้ รหัสผ่าน หรือรหัสใบอนุญาตของฉัน
- ถอนการติดตั้งหรือติดตั้งผลิตภัณฑ์ ESET Windows สำหรับใช้ที่บ้านของฉันใหม่อีกครั้ง
- ฉันได้รับข้อความว่าการติดตั้ง ESET ของฉันเสร็จสิ้นอย่างไม่สมบูรณ์

- ฉันต้องทำอย่างไรหลังจากที่ต่ออายุใบอนุญาตของฉันแล้ว (ผู้ใช้เริ่มต้น)
- จะเกิดอะไรขึ้นหากฉันเปลี่ยนที่อยู่อีเมลของฉัน
- ย้ายผลิตภัณฑ์ ESET ของฉันไปยังคอมพิวเตอร์หรืออุปกรณ์เครื่องใหม่
- จะเริ่ม Windows ในโหมดปลอดภัยหรือโหมดปลอดภัยที่มีเครือข่ายได้อย่างไร
- ยกเว้นเว็บไซต์ที่ปลอดภัยไม่ให้ถูกบล็อก
- อนุญาตการเข้าถึงสำหรับซอฟต์แวร์ตัวอ่านหน้าจอไปยัง ESET GUI

หากจำเป็น คุณสามารถติดต่อฝ่ายสนับสนุนด้านเทคนิคของเรา ได้หากคุณมีคำถามหรือปัญหา

วิธีอัพเดท ESET Smart Security Premium

การอัพเดท ESET Smart Security Premium สามารถดำเนินการได้ทั้งด้วยตนเองหรือโดยอัตโนมัติ ในการเรียกการอัพเดท ให้คลิก **อัพเดท** ในหน้าต่างโปรแกรมหลักแล้วคลิก **ตรวจหาการอัพเดท**

การตั้งค่าการติดตั้งเริ่มต้นจะสร้างงานการอัพเดทอัตโนมัติ ซึ่งสามารถทำงานเป็นประจำในแต่ละชั่วโมง ถ้าคุณต้องการเปลี่ยนระยะเวลา ให้ไปที่ **เครื่องมือ** > **เครื่องมือวางกำหนดการ**

วิธีลบไวรัสออกจากคอมพิวเตอร์

ถ้าคอมพิวเตอร์ของคุณแสดงอาการการติดไวรัสจากมัลแวร์ เช่น ทำงานช้า ค้างบ่อยๆ เราขอแนะนำให้คุณดำเนินการดังนี้:

1.ใน หน้าต่างโปรแกรมหลัก ให้คลิก **การสแกนคอมพิวเตอร์**

2.คลิก **การสแกนคอมพิวเตอร์ของคุณ** เพื่อเริ่มต้นการสแกนระบบของคุณ

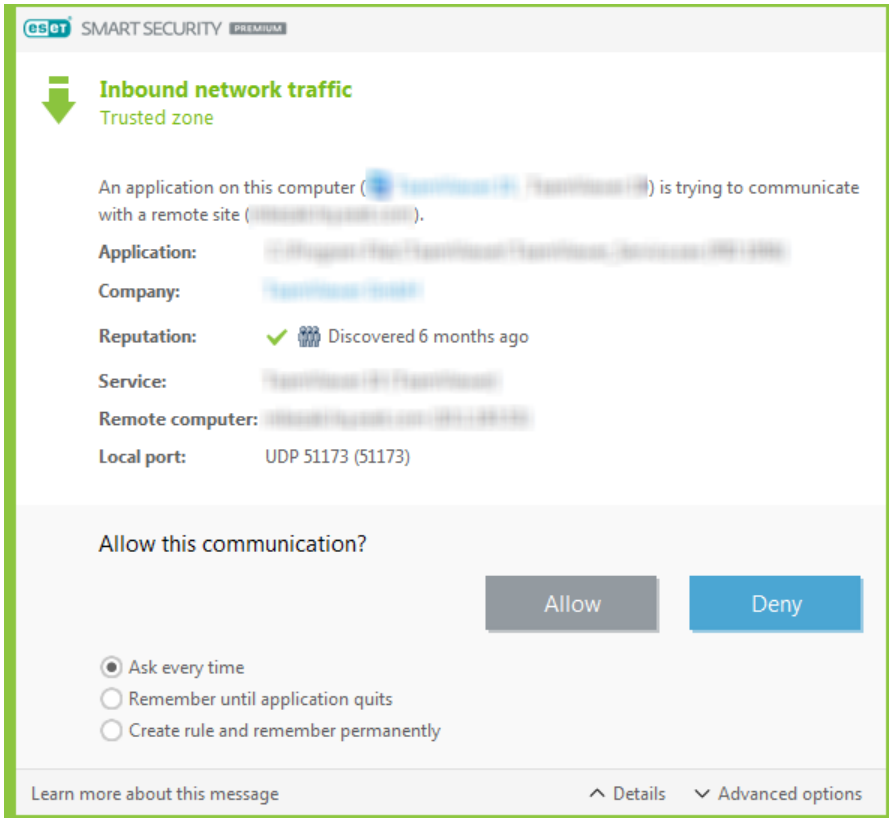
3.หลังจากสแกนเสร็จสิ้นแล้ว ให้ตรวจดูบันทึกสำหรับจำนวนไฟล์ที่สแกน ไฟล์ที่ติดไวรัส และไฟล์ที่กำจัด

4.หากคุณต้องการสแกนเฉพาะบางส่วนของดิสก์ ให้คลิก **การสแกนที่กำหนดเอง** และเลือกเป้าหมายที่จะสแกนไวรัส

สำหรับข้อมูลเพิ่มเติม โปรดดู บทความฐานความรู้ของ ESET ของเราที่มีการอัพเดทเป็นประจำ

วิธีอนุญาตการสื่อสารสำหรับแอพพลิเคชัน

ถ้าตรวจพบการเชื่อมต่อใหม่ในโหมดตอบสนอง และไม่มีกฎการจับคู่ คุณจะได้รับข้อความเพื่อให้อนุญาตหรือปฏิเสธการเชื่อมต่อ ถ้าคุณต้องการให้ ESET Smart Security Premium ทำงานเหมือนกันทุกครั้งที่แอพพลิเคชันพยายามเริ่มต้นการเชื่อมต่อ ให้เลือกช่องทำเครื่องหมาย **สร้างกฎและจดจำถาวร**



คุณสามารถสร้างกฎไฟร์วอลล์ใหม่สำหรับแอพพลิเคชันก่อนที่ ESET Smart Security Premium จะตรวจพบในการตั้งค่าของไฟร์วอลล์ โดยเปิด หน้าต่างโปรแกรมหลัก > **การตั้งค่า** > **การป้องกันเครือข่าย** > คลิก ⚙ ถัดจาก **ไฟร์วอลล์** > **กำหนดค่า** > **ขั้นสูง** > **กฎ** > **แก้ไข**

คลิกปุ่ม **เพิ่ม** และในแท็บ **ทั่วไป** ให้ป้อนชื่อ คำสั่ง และโปรโตคอลการสื่อสารสำหรับกฎ หน้าต่างนี้ช่วยให้คุณสามารถกำหนดการกระทำที่จะดำเนินการเมื่อใช้กฎ

ป้อนพาธไปยังไฟล์ที่เรียกใช้ของแอพพลิเคชันและพอร์ตการสื่อสารในระบบในแท็บ **ในระบบ** คลิกแท็บ **ระยะไกล** เพื่อป้อนที่อยู่และพอร์ตระยะไกล (ถ้ามี) กฎที่สร้างใหม่จะถูกนำไปใช้เมื่อแอพพลิเคชันพยายามสื่อสารอีกครั้ง

วิธีเปิดใช้งานการควบคุมเนื้อหาสำหรับบัญชี

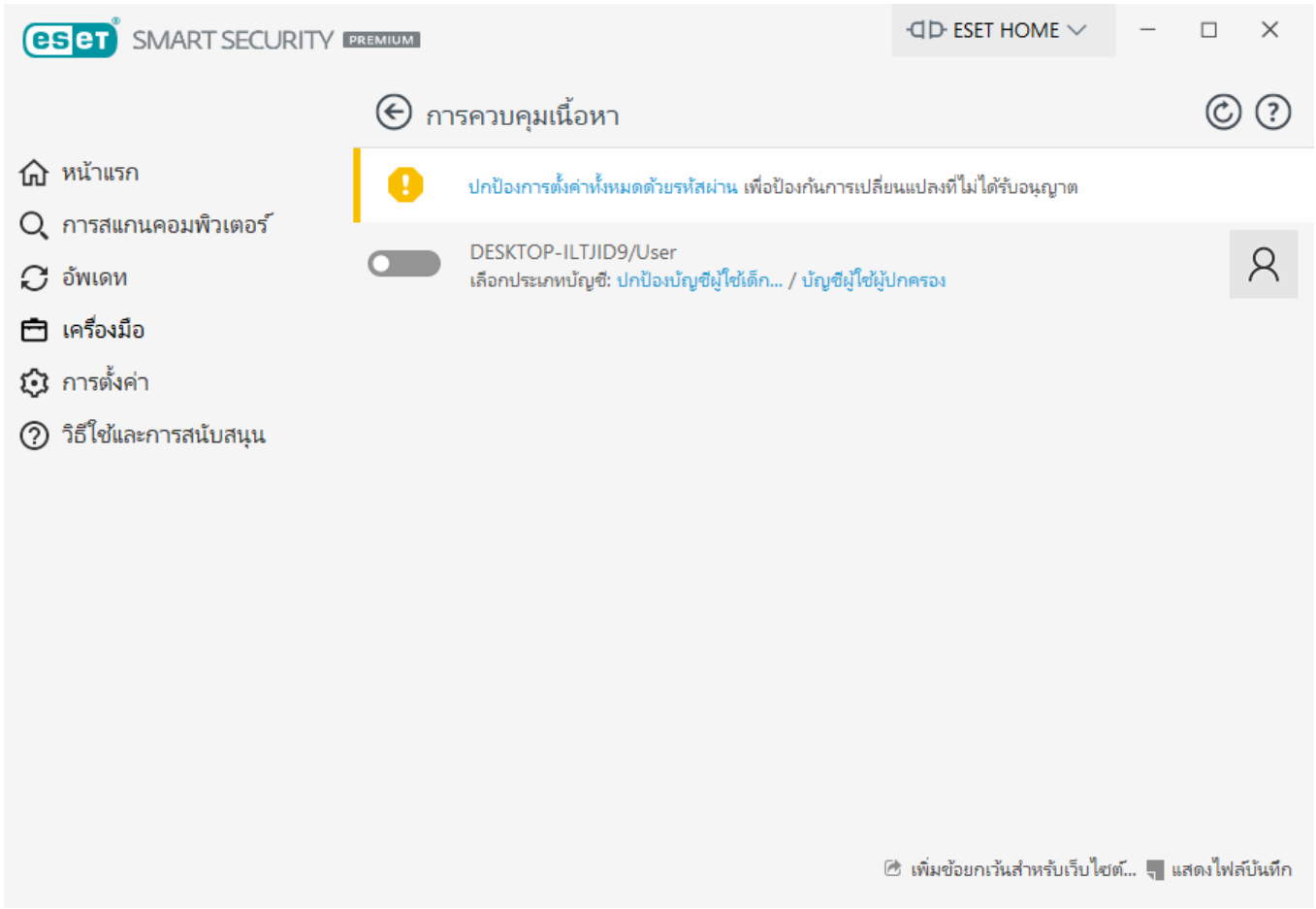
หากต้องการเปิดใช้งานการควบคุมเนื้อหาสำหรับบัญชีผู้ใช้ที่กำหนด โปรดดำเนินการตามขั้นตอนด้านล่างนี้:

1. ตามค่าเริ่มต้น การควบคุมเนื้อหาจะถูกปิดใช้งานใน ESET Smart Security Premium การเปิดใช้งานการควบคุมเนื้อหาสามารถทำได้สองวิธี:

   • คลิก  ใน **การตั้งค่า** > **เครื่องมือความปลอดภัย** > **การควบคุมเนื้อหา** จากหน้าต่างโปรแกรมหลักและเปลี่ยนสถานะการควบคุมเนื้อหาเป็น เปิดใช้งาน

   • กด F5 เพื่อเข้าถึงโครงสร้าง **การตั้งค่าขั้นสูง** ไปที่ **เว็บและอีเมล** > **การควบคุมเนื้อหาเว็บไซต์** แล้วเปิดใช้งานแถบเลื่อนถัดจาก **เปิดใช้งานการควบคุมเนื้อหาเว็บไซต์**

2. คลิก **การตั้งค่า** > **เครื่องมือความปลอดภัย** > **การควบคุมเนื้อหาเว็บไซต์** จาก หน้าต่างโปรแกรมหลัก แม้ว่า **เปิดใช้งาน** จะปรากฏข้าง **การควบคุมเนื้อหาเว็บไซต์** คุณก็ต้องกำหนดค่าการควบคุมเนื้อหาเว็บไซต์สำหรับบัญชีที่ต้องการด้วยการคลิกสัญลักษณ์ลูกศร จากนั้นในหน้าต่างถัดไปให้เลือก **ป้องกันบัญชีผู้ใช้เด็ก** หรือ **บัญชีผู้ปกครอง** ในหน้าต่างถัดไป ให้เลือกวันเกิดเพื่อระบุระดับการเข้าถึงและแนะนำหน้าเว็บที่เหมาะสมกับอายุ ขณะนี้การควบคุมเนื้อหาเว็บไซต์จะเปิดใช้งานสำหรับบัญชีผู้ใช้ที่กำหนดแล้ว ให้คลิก **เนื้อหาและการตั้งค่าที่ปิดกั้น** ที่อยู่ใต้ชื่อบัญชีเพื่อปรับแต่งหมวดหมู่ที่คุณต้องการอนุญาตหรือปิดกั้นในแท็บ หมวดหมู่ ในการอนุญาตหรือปิดกั้นหน้าเว็บที่มีหมวดหมู่ไม่ตรงกัน ให้คลิกแท็บ ข้อยกเว้น



วิธีสร้างงานใหม่ในเครื่องมือวางกำหนดการ

หากต้องการสร้างงานใหม่ใน **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **เครื่องมือวางกำหนดการ** ให้คลิก **เพิ่ม** หรือคลิกขวาแล้วเลือก **เพิ่ม** มีงานตามกำหนดการห้าประเภท:

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

• **อัพเดท** – วางกำหนดการงานการอัพเดทโดยการอัพเดทโมดูลเหล่านี้

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 หากเวลานับตั้งแต่การเรียกใช้งานครั้งสุดท้ายเกินค่าที่ระบุไว้** (สามารถกำหนดช่วงเวลาได้โดยใช้กล่องเลื่อน **เวลานับตั้งแต่การเรียกใช้งานครั้งสุดท้าย (ชั่วโมง)**)

ในขั้นถัดไป โปรแกรมจะแสดงข้อมูลสรุปพร้อมด้วยข้อมูลเกี่ยวกับงานตามกำหนดการปัจจุบัน คลิก **สิ้นสุด** เมื่อคุณแก้ไขจนเสร็จสิ้นแล้ว

หน้าต่างข้อความจะปรากฏ เพื่อให้คุณเลือกโปรไฟล์ที่จะใช้สำหรับงานตามกำหนดการ ในที่นี้คุณจะสามารถตั้งค่าโปรไฟล์หลักและโปรไฟล์รอง โปรไฟล์รองจะใช้ในกรณีที่ไม่สามารถทำงานให้เสร็จสมบูรณ์โดยใช้โปรไฟล์หลัก ยืนยันด้วยการคลิก **สิ้นสุด** และงานตามกำหนดการใหม่จะถูกเพิ่มในรายการของงานตามกำหนดการปัจจุบัน

วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์

หากต้องการวางกำหนดการงานทั่วไป ให้เปิด หน้าต่างโปรแกรมหลัก และคลิก **เครื่องมือ** > **เครื่องมือเพิ่มเติม** > **เครื่องมือวางกำหนดการณ์** ที่ด้านล่างคือคู่มือสั้นๆ เกี่ยวกับวิธีการวางกำหนดงานที่จะสแกนไดรฟ์ในระบบของคุณในทุกสัปดาห์ ให้ดู บทความฐานความรู้ สำหรับคำแนะนำอย่างละเอียดเพิ่มเติม

เมื่อต้องการวางกำหนดการงานสแกน:

1. คลิก **เพิ่ม** ในหน้าจอเครื่องมือวางกำหนดการหลัก

2. ป้อนชื่อสำหรับงานแล้วเลือก **สแกนคอมพิวเตอร์ตามความต้องการ** จากเมนูแบบเลื่อนลง **ประเภทงาน**

3. เลือก **รายสัปดาห์** เป็นความถี่ของงาน

4. ตั้งวันและเวลาที่จะทำงาน

5. เลือก **เรียกใช้งานให้เร็วที่สุดเท่าที่ทำได้** เพื่อทำงานในภายหลังในกรณีที่การเรียกใช้งานตามกำหนดการไม่ทำงานด้วยสาเหตุใดก็ตาม (ตัวอย่างเช่น หากคอมพิวเตอร์ถูกปิดในเวลานั้น)

6. ดูข้อมูลสรุปของงานตามกำหนดการ และคลิกที่ **สิ้นสุด**

7. จากเมนูแบบเลื่อนลง **เป้าหมาย** ให้เลือก **ไดรฟ์ในระบบ**

8. คลิก **สิ้นสุด** เพื่อใช้งาน

วิธีแก้ไข "การป้องกันทางด้านธนาคารและการชำระเงินไม่สามารถเปลี่ยนเส้นทางไปยังหน้าเว็บที่ร้องขอได้"

ใช้ตัวเลือกป้องกันเบราว์เซอร์ทั้งหมดแทนการเปลี่ยนเส้นทางเว็บไซต์
ตามค่าเริ่มต้น เบราว์เซอร์ที่มีการป้องกันสำหรับการป้องกันทางด้านธนาคารและการชำระเงินจะเปิดในเบราว์เซอร์ที่คุณใช้งานอยู่ในขณะนี้ หลังจากที่คุณเข้าไปที่เว็บไซต์บริการธนาคารที่รู้จัก คุณสามารถใช้ตัวเลือกป้องกันเบราว์เซอร์ทั้งหมดเพื่อเริ่มต้นเบราว์เซอร์ที่รองรับทั้งหมดในโหมดปลอดภัยแทนการเปลี่ยนเส้นทางเว็บไซต์ได้ ซึ่งจะช่วยให้คุณสามารถเรียกใช้อินเทอร์เน็ต เข้าถึงธนาคารบนอินเทอร์เน็ต และทำธุรกรรมออนไลน์โดยไม่ต้องเปลี่ยนเส้นทางได้ในหน้าต่างเบราว์เซอร์ที่ปลอดภัยเพียงหนึ่งเดียว
หากต้องการใช้ตัวเลือกป้องกันเบราว์เซอร์ทั้งหมด ให้เปิด หน้าต่างโปรแกรมหลัก ไปยัง **การตั้งค่า** > **เครื่องมือความปลอดภัย** และเปิดใช้งานแถบเลื่อนถัดจาก **ป้องกันเบราว์เซอร์ทั้งหมด**

หากต้องการแก้ไขข้อผิดพลาดในการเปลี่ยนเส้นทางเว็บไซต์ ให้ดำเนินการตามคำแนะนำด้านล่าง:

หลังทำขั้นตอนต่างๆ เสร็จสิ้น ให้ตรวจสอบว่าการป้องกันการชำระเงินผ่านธนาคารกำลังดำเนินการอยู่
หากหน้าต่างเบราว์เซอร์ยังคงไม่ทำงาน ให้ทำตามขั้นตอนต่อไปนี้ให้เสร็จสิ้นจนกว่าหน้าต่างจะกลับมาทำงานอีกครั้ง

1. รีสตาร์ทคอมพิวเตอร์ของคุณ

2. ตรวจสอบให้แน่ใจว่าคุณกำลังใช้งานระบบปฏิบัติการ Windows และ ESET Smart Security Premium เวอร์ชันล่าสุด: อัพเกรดผลิตภัณฑ์ ESET Windows สำหรับใช้ภายในบ้านให้เป็นเวอร์ชันล่าสุด

3. คุณอาจพบข้อขัดแย้งกับซอฟต์แวร์รักษาความปลอดภัย, VPN หรือไฟร์วอลล์ของบริษัทอื่น โปรดปิดการใช้งานหรือถอนการติดตั้งซอฟต์แวร์นี้ชั่วคราว

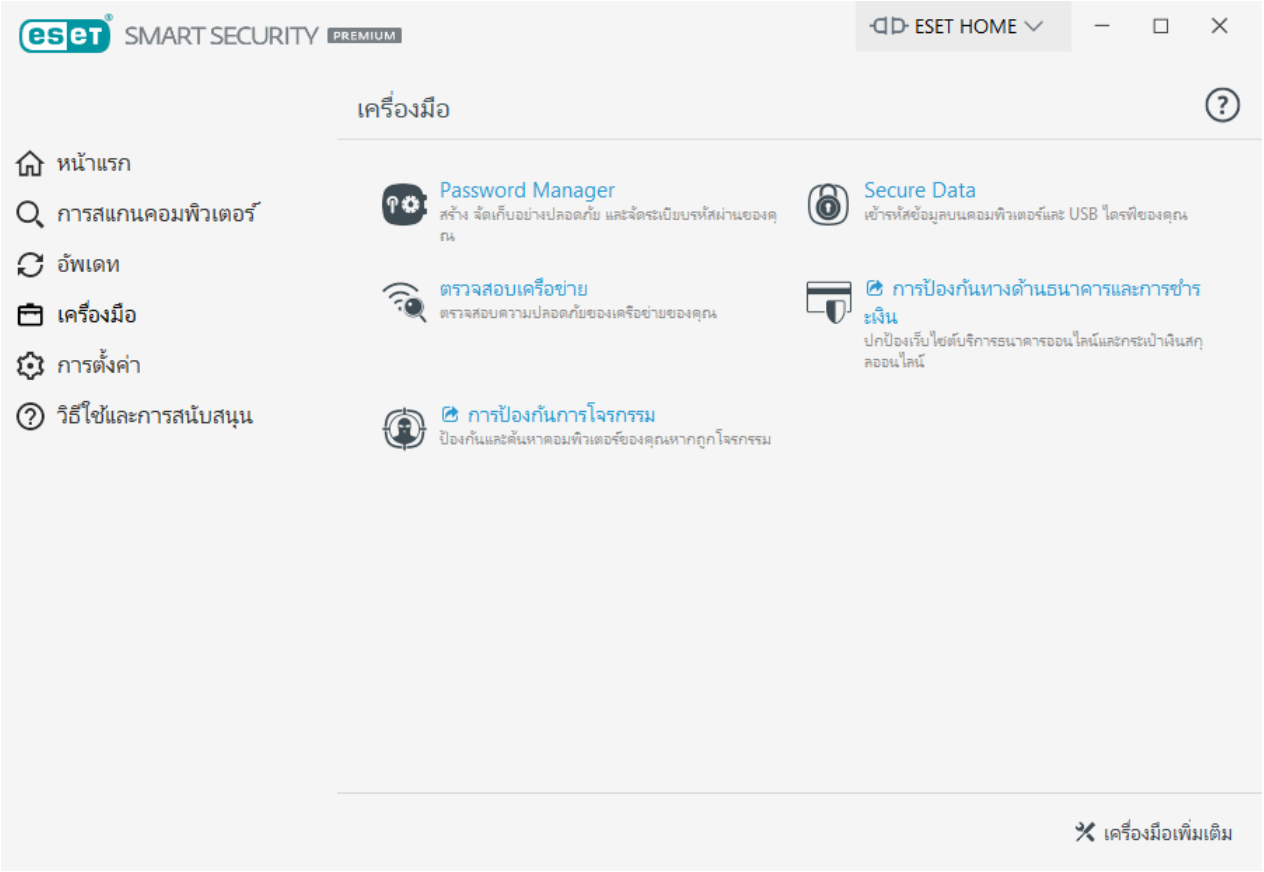
4. ปิดใช้งานส่วนขยายเบราว์เซอร์ของบุคคลที่สามทั้งหมด

5. ล้างแคชในเบราว์เซอร์ ต้องใช้วิธีใดในการ ล้าง แคช ของ Firefox หรือ ล้าง แคช ของ Google Chrome ในเบราว์เซอร์ของฉัน

6. ตรวจสอบให้แน่ใจว่าเบราว์เซอร์เริ่มต้นของคุณไม่ได้ถูกยกเว้นใน **การตั้งค่าขั้นสูง** > **เว็บและอีเมล** > **การกรองโปรโตคอล** > **แอพพลิเคชันที่ยกเว้น** เข้าถึงการตั้งค่าขั้นสูง

7. หากคุณไม่ได้อัพเกรดผลิตภัณฑ์ ESET ในขั้นตอนก่อนหน้านี้ ให้ ถอนการติดตั้งและติดตั้งผลิตภัณฑ์ ESET ของคุณอีกครั้ง แล้วรีสตาร์ทคอมพิวเตอร์ของคุณหลังจากติดตั้ง

8. หากปัญหายังคงอยู่ คุณสามารถ เปิดใช้งานตัวเลือกป้องกันเบราว์เซอร์ทั้งหมด หรือเข้าถึงเบราว์เซอร์ที่มีการป้องกันจาก หน้าต่างโปรแกรมหลัก > **เครื่องมือ** > **การป้องกันทางด้านธนาคารและการชำระเงิน**



การป้องกันการธนาคารและการชำระเงินเป็นระดับการป้องกันเพิ่มเติมซึ่งออกแบบมาเพื่อปกป้องข้อมูลการเงินของคุณในระหว่างที่ทำธุรกรรมออนไลน์

ในกรณีส่วนใหญ่ เบราว์เซอร์ที่มีการป้องกันสำหรับการป้องกันทางด้านธนาคารและการชำระเงินจะเปิดในเบราว์เซอร์ที่คุณใช้งานอยู่ในขณะนี้หลังจากที่คุณเข้าไปที่เว็บไซต์บริการธนาคารที่รู้จัก

เลือกหนึ่งรายการจากตัวเลือกการกำหนดค่าพฤติกรรมของเบราว์เซอร์ที่มีการป้องกันต่อไปนี้:

• **ป้องกันเบราว์เซอร์ทั้งหมด** – หากเปิดใช้งาน เว็บเบราว์เซอร์ทั้งหมดที่รองรับจะเริ่มต้นในโหมดปลอดภัย ซึ่งช่วยให้คุณสามารถเรียกใช้อินเทอร์เน็ต เข้าถึงธนาคารบนอินเทอร์เน็ต และซื้อของออนไลน์ รวมถึงการทำธุรกรรมในหน้าต่างเบราว์เซอร์ที่มีการป้องกันโดยไม่ต้องเปลี่ยนเส้นทาง

• **การเปลี่ยนเส้นทางเว็บไซต์** (ค่าเริ่มต้น) – เว็บไซต์จากรายการเว็บไซต์ที่ได้รับการป้องกันและรายการธนาคารบนอินเทอร์เน็ตภายในจะเปลี่ยนเส้นทางไปยังเบราว์เซอร์ที่มีการป้องกัน คุณสามารถเลือกได้ว่าจะเปิดเบราว์เซอร์ใด (มาตรฐานหรือมีการป้องกัน)

• ตัวเลือกทั้งสองตัวเลือกก่อนหน้านี้จะปิดใช้งานอยู่ – หากต้องการเข้าถึงเบราว์เซอร์ที่มีการป้องกันใน ESET Smart Security Premium ให้คลิก **เครื่องมือ** > **การป้องกันทางด้านธนาคารและการชำระเงิน** หรือคลิกไอคอนเดสก์ท็อป **การป้องกันทางด้านธนาคารและการชำระเงิน** เบราว์เซอร์ Windows จะเริ่มทำงานในโหมดปลอดภัยตามที่ตั้งไว้เป็นค่าเริ่มต้น

เมื่อต้องการกำหนดค่าลักษณะการทำงานของเบราว์เซอร์ที่มีการป้องกัน โปรดดู การตั้งค่าขั้นสูงของการป้องกันทางด้านธนาคารและการชำระเงิน เมื่อต้องการเปิดใช้งานคุณลักษณะป้องกันเบราว์เซอร์ทั้งหมดใน ESET Smart Security Premium ให้คลิก **การตั้งค่า** > **เครื่องมือความปลอดภัย** และเปิดใช้งานแถบตัวเลื่อน **ป้องกันเบราว์เซอร์ทั้งหมด**

การใช้การสื่อสารที่เข้ารหัส HTTPS นั้นเป็นสิ่งจำเป็นสำหรับการเรียกดูโดยได้รับการป้องกัน โดยเบราว์เซอร์ต่อไปนี้จะรองรับการป้องกันทางด้านธนาคารและการชำระเงิน:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับคุณสมบัติการป้องกันทางด้านธนาคารและการชำระเงิน ให้อ่านบทความฐานความรู้ ESET ต่อไปนี้ในภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษา:

- ฉันสามารถใช้ ESET การป้องกันการธนาคารและการชำระเงินได้อย่างไร

- เปิดหรือปิดใช้งาน ESETการป้องกันทางด้านธนาคารและการชำระเงินสำหรับเว็บไซต์เฉพาะ
- หยุดชั่วคราวหรือปิดใช้งานการป้องกันธนาคารและการชำระเงินในผลิตภัณฑ์ ESET Windows home
- การป้องกันทางด้านธนาคารและการชำระเงินของ ESET—ข้อผิดพลาดทั่วไป
- ประมวลศัพท์ ESET | การป้องกันการธนาคารและการชำระเงิน

หากคุณไม่สามารถแก้ไขปัญหาของคุณได้ โปรดติดต่อ ฝ่ายดูแลลูกค้าของ ESET

วิธีปลดล็อคการตั้งค่าขั้นสูงที่มีการป้องกันด้วยรหัสผ่าน

เมื่อคุณต้องการเข้าใช้การตั้งค่าขั้นสูงที่มีการป้องกัน หน้าต่างสำหรับป้อนรหัสผ่านจะแสดงขึ้น หากคุณลืมหรือทำรหัสผ่านหาย ให้คลิก **เรียกคืนรหัสผ่าน** แล้วพิมพ์ที่อยู่อีเมลที่คุณใช้ในการลงทะเบียนใบอนุญาต ทาง ESET จะส่งอีเมลที่มีรหัสการตรวจสอบให้กับคุณ พิมพ์รหัสการตรวจสอบดังกล่าว จากนั้นเขียนและยืนยันรหัสผ่านใหม่ รหัสการตรวจสอบนี้จะใช้งานได้เป็นเวลา 7 วัน

เรียกคืนรหัสผ่านผ่านบัญชี ESET HOME – ใช้ตัวเลือกนี้หากใบอนุญาตที่ใช้สำหรับเปิดใช้งานเชื่อมโยงอยู่กับบัญชี ESET HOME ของคุณ โปรดพิมพ์อีเมลที่คุณใช้ล็อคอินบัญชี ESET HOME ของคุณ

หากคุณจำที่อยู่อีเมลไม่ได้หรือพบความยากลำบากในการเรียกคืนรหัสผ่าน ให้คลิก **ติดต่อฝ่ายสนับสนุนด้านเทคนิค** ระบบจะเปลี่ยนเส้นทางคุณไปยังเว็บไซต์ ESET เพื่อติดต่อฝ่ายสนับสนุนด้านเทคนิค

สร้างรหัสสำหรับฝ่ายสนับสนุนด้านเทคนิค – ตัวเลือกนี้จะสร้างรหัสสำหรับฝ่ายสนับสนุนด้านเทคนิค ให้คัดลอกรหัสที่ฝ่ายสนับสนุนด้านเทคนิคให้แล้วคลิก **ฉันมีรหัสการตรวจสอบ** พิมพ์รหัสการตรวจสอบดังกล่าว จากนั้นเขียนและยืนยันรหัสผ่านใหม่ รหัสการตรวจสอบนี้จะใช้งานได้เป็นเวลา 7 วัน

สำหรับข้อมูลเพิ่มเติม โปรดดู ปลดล็อกการตั้งค่ารหัสผ่านผลิตภัณฑ์ ESET สำหรับ Windows สำหรับใช้งานในบ้าน

วิธีแก้ปัญหาการปิดใช้งานผลิตภัณฑ์จาก ESET HOME

ยังไม่ได้เปิดใช้งานผลิตภัณฑ์

ข้อความแสดงข้อผิดพลาดนี้จะปรากฏขึ้นเมื่อเจ้าของใบอนุญาตปิดการใช้งาน ESET Smart Security Premium ของคุณจากพอร์ทัล ESET HOME หรือเมื่อไม่มีการแชร์ใบอนุญาตที่ใช้ร่วมกับบัญชี ESET HOME ของคุณอีกต่อไป หากต้องการแก้ไขปัญหานี้ ให้:

- คลิก **เปิดใช้งาน** และใช้หนึ่งใน วิธีการเปิดใช้งาน เพื่อเปิดใช้งาน ESET Smart Security Premium
- ติดต่อเจ้าของใบอนุญาตเพื่อแจ้งข้อมูลว่า ESET Smart Security Premium ของคุณถูกปิดใช้งานโดยเจ้าของใบอนุญาต หรือแจ้งว่าไม่มีการแชร์ใบอนุญาตกับคุณอีกต่อไป เจ้าของสามารถแก้ปัญหาใน ESET HOME ได้

ปิดใช้งานผลิตภัณฑ์แล้ว ยกเลิกการเชื่อมต่ออุปกรณ์แล้ว

ข้อความแสดงข้อผิดพลาดนี้จะปรากฏขึ้นหลังจาก นำอุปกรณ์ออกจากบัญชี ESET HOME หากต้องการแก้ไขปัญหานี้ ให้:

- คลิก **เปิดใช้งาน** และใช้หนึ่งใน วิธีการเปิดใช้งาน เพื่อเปิดใช้งาน ESET Smart Security Premium
- ติดต่อเจ้าของใบอนุญาตเพื่อแจ้งข้อมูลว่า ESET Smart Security Premium ของคุณถูกปิดใช้งาน และอุปกรณ์ถูกตัดการเชื่อมต่อจาก ESET HOME
- หากคุณเป็นเจ้าของใบอนุญาตและไม่ทราบถึงการเปลี่ยนแปลงเหล่านี้ ให้ตรวจสอบ ฟีดกิจกรรมของ ESET HOME หากคุณพบกิจกรรมที่น่าสงสัย ให้ เปลี่ยนรหัสผ่านบัญชี ESET HOME ของคุณ และ ติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET

ปิดใช้งานผลิตภัณฑ์แล้วยกเลิกการเชื่อมต่ออุปกรณ์แล้ว

ข้อความแสดงข้อผิดพลาดนี้จะปรากฏขึ้นหลังจาก นำอุปกรณ์ออกจากบัญชี ESET HOME หากต้องการแก้ไขปัญหานี้ ให้:

• คลิก **เปิดใช้งาน** และใช้หนึ่งใน วิธีการเปิดใช้งาน เพื่อเปิดใช้งาน ESET Smart Security Premium

• ติดต่อเจ้าของใบอนุญาตเพื่อแจ้งข้อมูลว่า ESET Smart Security Premium ของคุณถูกปิดใช้งาน และอุปกรณ์ถูกตัดการเชื่อมต่อจาก ESET HOME

• หากคุณเป็นเจ้าของใบอนุญาตและไม่ทราบถึงการเปลี่ยนแปลงเหล่านี้ ให้ตรวจสอบ ฟีดกิจกรรมของ ESET HOME หากคุณพบกิจกรรมที่น่าสงสัย ให้ เปลี่ยนรหัสผ่านบัญชี ESET HOME ของคุณ และ ติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET

ยังไม่ได้เปิดใช้งานผลิตภัณฑ์

ข้อความแสดงข้อผิดพลาดนี้จะปรากฏขึ้นเมื่อเจ้าของใบอนุญาตปิดการใช้งาน ESET Smart Security Premium ของคุณจากพอร์ทัล ESET HOME หรือเมื่อไม่มีการแชร์ใบอนุญาตที่ใช้ร่วมกับบัญชี ESET HOME ของคุณอีกต่อไป หากต้องการแก้ไขปัญหานี้ ให้:

• คลิก **เปิดใช้งาน** และใช้หนึ่งใน วิธีการเปิดใช้งาน เพื่อเปิดใช้งาน ESET Smart Security Premium

• ติดต่อเจ้าของใบอนุญาตเพื่อแจ้งข้อมูลว่า ESET Smart Security Premium ของคุณถูกปิดใช้งานโดยเจ้าของใบอนุญาต หรือแจ้งว่าไม่มีการแชร์ใบอนุญาตกับคุณอีกต่อไป เจ้าของสามารถแก้ปัญหาใน ESET HOME ได้

โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า

เมื่อเข้าร่วมโปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า คุณจะมอบข้อมูลแบบไม่ระบุตัวตนเกี่ยวกับวิธีใช้ผลิตภัณฑ์ของเราให้แก่ ESET สามารถดูข้อมูลเพิ่มเติมเกี่ยวกับการประมวลผลข้อมูลได้ใน นโยบายความเป็นส่วนตัว

คำยินยอมของคุณ

โปรแกรมนี้เปิดให้เข้าร่วมโดยสมัครใจและขึ้นอยู่กับความยินยอมของคุณ หลังจากที่เข้าร่วมแล้ว การมีส่วนร่วมทั้งหมดจะเป็นแบบไม่ต้องโต้ตอบ ซึ่งหมายความว่าคุณไม่จำเป็นต้องดำเนินการเพิ่มเติมใดๆ คุณสามารถถอนความยินยอมของคุณได้ทุกเมื่อด้วยการเปลี่ยนการตั้งค่าผลิตภัณฑ์ ซึ่งจะเป็นการยุติไม่ให้เราประมวลผลข้อมูลแบบไม่ระบุตัวตนของคุณอีกต่อไป

คุณสามารถถอนความยินยอมของคุณได้ทุกเมื่อด้วยการเปลี่ยนการตั้งค่าผลิตภัณฑ์

- เปลี่ยนแปลงการตั้งค่าโปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้าในผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้าน

เรารวบรวมข้อมูลประเภทใดบ้าง

ข้อมูลเกี่ยวกับการโต้ตอบกับผลิตภัณฑ์

ข้อมูลนี้จะช่วยให้เราทราบเพิ่มเติมว่าผลิตภัณฑ์ของเราถูกใช้งานอย่างไร ข้อมูลนี้ทำให้เราทราบสิ่งต่างๆ เช่น มักใช้การทำงานแบบใด ผู้ใช้แก้ไขการตั้งค่าใดบ้าง หรือผู้ใช้ใช้งานผลิตภัณฑ์เป็นเวลาเท่าใด

ข้อมูลเกี่ยวกับอุปกรณ์

เราเก็บรวบรวมข้อมูลนี้เพื่อทำความเข้าใจว่าอุปกรณ์ใดและที่ใดบ้างที่ผลิตภัณฑ์ของเราได้รับการใช้งาน ตัวอย่างทั่วไปคือ รุ่นของอุปกรณ์ ประเทศ เวอร์ชัน และชื่อของระบบปฏิบัติการ

การวินิจฉัยข้อมูลข้อผิดพลาด

เราเก็บรวบรวมข้อมูลเกี่ยวกับข้อผิดพลาดและสถานการณ์ความล้มเหลวต่างๆ เช่น เกิดข้อผิดพลาดใดบ้างและการกระทำใดที่ส่งผลให้เกิดข้อผิดพลาดนั้น

เหตุใดเราจึงรวบรวมข้อมูลนี้

ข้อมูลแบบไม่ระบุตัวตนนี้ช่วยให้เราสามารถปรับปรุงผลิตภัณฑ์ให้คุณซึ่งเป็นผู้ใช้ของเรา ทำให้มีความเกี่ยวข้อง ใช้งานง่าย และไร้ข้อผิดพลาดมากขึ้นเท่าที่จะทำได้

ใครควบคุมข้อมูลนี้

ESET, spol. s r.o. คือผู้ควบคุมการเก็บรวบรวมข้อมูลในโปรแกรมนี้แต่เพียงผู้เดียว ซึ่งข้อมูลนี้จะไม่เปิดเผยให้บุคคลที่สาม

ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง

มีผลตั้งแต่วันที่ 19 ตุลาคม 2021

ข้อมูลสำคัญ: โปรดอ่านข้อกำหนดและเงื่อนไขของการใช้งานผลิตภัณฑ์ที่กำหนดไว้ด้านล่างนี้อย่างถี่ถ้วนก่อนที่จะ

ดาวน์โหลด 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 ดาวน์โหลดจากเซิร์ฟเวอร์ของผู้ให้บริการหรือได้รับจากแหล่งอื่นๆ 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 ตามที่ผู้ให้

บริการให้อนุญาตแก่คุณตามข้อ 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 คุณต้องไม่แบ่งปันใบอนุญาตกับบุคคลที่สามหรืออนุญาติให้บุคคลที่สามใช้รหัสใบอนุญาตเว้นแต่

จะได้รับอนุญาตจากข้อตกลงนี้หรือจากผู้ให้บริการ 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 ยกเว้นผู้ใช้ปลายทางจะปิดใช้งานการติดตั้งการอัพเดทโดยอัตโนมัติ สำหรับการจัดหาการอัพเดท จะต้องใช้การตรวจสอบความถูกต้องของใบอนุญาต ซึ่งรวมถึงข้อมูลเกี่ยวกับคอมพิวเตอร์และ/หรือแพลตฟอร์มที่ติดตั้งซอฟต์แวร์นั้นตามนโยบายความเป็นส่วนตัว

การจัดหาการอัพเดทใดๆ อาจอยู่ภายใต้นโยบายการสิ้นสุดอายุการใช้งาน ("นโยบาย EOL") ซึ่งมีอยู่ใน https://go.eset.com/eol_home จะไม่มีการอัพเดทใดๆ หลังจากซอฟต์แวร์หรือคุณลักษณะใดๆ ของซอฟต์แวร์ถึงวัน

สิ้นสุดอายุการใช้งานที่กำหนดไว้ในนโยบาย EOL

ข) **การส่งต่อการแฝงตัวและข้อมูลแก่ผู้ให้บริการ** ซอฟต์แวร์นี้มีฟังก์ชันที่ทำหน้าที่เก็บตัวอย่างของไวรัส คอมพิวเตอร์ 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 หรือกับหุ้นส่วนธุรกิจที่เป็นส่วนหนึ่งของภาคการจัดจำหน่ายของผู้ให้บริการตลอดจนเครือข่ายที่รองรับ ทั้งนี้เพื่อตรวจสอบถึงฟังก์ชันการใช้งานและการได้รับอนุญาตให้ใช้ซอฟต์แวร์และเพื่อคุ้มครองสิทธิ์ของผู้ให้บริการ

ตามข้อสรุปของข้อตกลงนี้ ผู้ให้บริการหรือหุ้นส่วนธุรกิจที่เป็นส่วนหนึ่งของภาคการจัดจำหน่ายของผู้ให้บริการและเครือข่ายที่รองรับจะได้รับสิทธิ์ให้โอน ประมวลผล และจัดเก็บข้อมูลสำคัญที่จะระบุตัวคุณ เพื่อการเรียกเก็บเงินและ

การปฏิบัติตามข้อตกลงนี้ รวมถึงการส่งการแจ้งเตือนในคอมพิวเตอร์ของคุณ

สามารถดูรายละเอียดเกี่ยวกับการป้องกันความเป็นส่วนตัว ข้อมูลส่วนบุคคล และสิทธิ์ของคุณในแง่ของข้อมูลได้ในนโยบายความเป็นส่วนตัวซึ่งอยู่ในเว็บไซต์ของผู้ให้บริการและสามารถเข้าถึงได้โดยตรงจากกระบวนการติดตั้ง คุณสามารถดูจากส่วนวิธีใช้ของซอฟต์แวร์ได้เช่นกัน

5. **การใช้สิทธิ์ของผู้ใช้ปลายทาง** คุณต้องใช้สิทธิ์ของผู้ใช้ปลายทางในนามบุคคลหรือผ่านพนักงาน คุณได้รับสิทธิ์ให้ใช้ซอฟต์แวร์เฉพาะเพื่อปกป้องการทำงานของคุณและคุ้มครองคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่คุณได้รับใบอนุญาตเท่านั้น

6. **ข้อจำกัดเกี่ยวกับสิทธิ์** คุณไม่สามารถคัดลอก แจกจ่าย ดึงข้อมูลจากองค์ประกอบ หรือทำผลงานที่ต่อเนื่องของซอฟต์แวร์นี้ เมื่อใช้ซอฟต์แวร์ จะถือว่าคุณต้องปฏิบัติตามข้อจำกัดต่อไปนี้:

ก) คุณสามารถสร้างสำเนาของซอฟต์แวร์เก็บไว้หนึ่งฉบับในสื่อสำหรับการจัดเก็บข้อมูลถาวร เพื่อเป็นสำเนาสำรองข้อมูลแบบถาวร ซึ่งจะทำให้ไม่มีการติดตั้งหรือใช้สำเนาสำรองข้อมูลอาร์ไคฟ์ในคอมพิวเตอร์เครื่องอื่น สำเนาอื่นๆ ที่คุณดำเนินการจากซอฟต์แวร์จะถือว่าเป็นการละเมิดข้อตกลงนี้

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 นับจากที่ได้รับข้อมูลดังกล่าวเป็นต้นไป 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 ตลอดจนเอกสารที่เกี่ยวข้องทั้งหมดที่คุณได้รับจากผู้ให้บริการหรือจากหุ้นส่วนธุรกิจของผู้ให้บริการโดยเป็นผู้ออกค่าใช้จ่ายเอง สิทธิ์ในการใช้ซอฟต์แวร์และคุณลักษณะใดๆ ของซอฟต์แวร์อาจอยู่ภายใต้นโยบาย EOL สิทธิ์ในการใช้ซอฟต์แวร์ของคุณจะสิ้นสุดลงหลังจากซอฟต์แวร์หรือคุณลักษณะใดๆ ของซอฟต์แวร์ถึงวันสิ้นสุดอายุการใช้งานที่กำหนดไว้ในนโยบาย EOL ไม่ว่าการยุติข้อตกลงนี้จะเกิดขึ้นด้วยสาเหตุใด บทบัญญัติของข้อ 7, 8, 11, 13, 19 และ 21 จะยังคงมีผลบังคับโดยไม่จำกัดเวลา

11. **ประกาศของผู้ใช้ปลายทาง** ในฐานะที่เป็นผู้ใช้ปลายทาง คุณรับทราบว่าซอฟต์แวร์นี้มีให้แก่คุณแบบ "ตามสภาพ" โดยไม่มีการรับประกันทั้งโดยชัดแจ้งหรือโดยนัย ไม่ว่าในประเภทใดภายในขอบเขตสูงสุดที่กฎหมาย

อนุญาต 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 การสูญเสียข้อมูลธุรกิจหรือความเสียหายเป็นกรณีพิเศษ 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 อาจจำเป็นต้องใช้ข้อมูลใบ

อนุญาต 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) ผ่านการส่งอีเมลที่ส่งไปยังผู้ให้บริการซึ่งมีรายละเอียดของการอนุญาต (ชื่อผู้ใช้และรหัสผ่าน) อาจจำเป็นต้องใช้ข้อมูลใบอนุญาตและข้อมูลอัตลักษณ์ผู้ใช้ปลายทางตามที่ระบุไว้ในนโยบายความเป็นส่วนตัว เพื่อวัตถุประสงค์ในการตรวจสอบความเป็นของแท้ของซอฟต์แวร์

18. **การอนุญาตสำหรับหน่วยงานของรัฐที่มีอำนาจและรัฐบาลของสหรัฐอเมริกา** หน่วยงานของรัฐที่มีอำนาจรวมถึงรัฐบาลของสหรัฐอเมริกา 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

ส่วนเพิ่มเติมสำหรับข้อตกลง

การประเมินความปลอดภัยของอุปกรณ์ที่เชื่อมต่อกับเครือข่าย บทบัญญัติเพิ่มเติมจะนำไปใช้กับการประเมินความปลอดภัยของอุปกรณ์ที่เชื่อมต่อกับเครือข่ายดังต่อไปนี้:

ซอฟต์แวร์มีฟังก์ชันสำหรับตรวจสอบความปลอดภัยของเครือข่ายภายในระบบของผู้ใช้ปลายทางและความปลอดภัยของอุปกรณ์ ซึ่งจำเป็นต้องใช้ชื่อของเครือข่ายภายในระบบและข้อมูลเกี่ยวกับอุปกรณ์ในเครือข่ายภายในระบบ เช่น การมีอยู่, ประเภท, ชื่อ, ที่อยู่ IP และที่อยู่ MAC ของอุปกรณ์ในเครือข่ายภายในระบบที่เชื่อมต่อโดยมีข้อมูลใบอนุญาต ข้อมูลดังกล่าวยังรวมถึงประเภทความปลอดภัยไร้สายและประเภทการเข้ารหัสไร้สายของอุปกรณ์เราเตอร์ด้วย ฟังก์ชันนี้ยังอาจให้ข้อมูลเกี่ยวกับความพร้อมใช้งานของโซลูชันซอฟต์แวร์ความปลอดภัยเพื่อช่วยให้อุปกรณ์ในเครือข่ายภายในระบบปลอดภัย

การป้องกันการใช้ข้อมูลในทางที่ผิด บทบัญญัติเพิ่มเติมจะนำไปใช้กับการป้องกันการใช้ข้อมูลในทางที่ผิดดังต่อไปนี้:

ซอฟต์แวร์ประกอบด้วยฟังก์ชันที่ป้องกันการสูญหายหรือการใช้ข้อมูลสำคัญผิดวัตถุประสงค์ ซึ่งเชื่อมโยงโดยตรงกับการโจรกรรมคอมพิวเตอร์ ฟังก์ชันนี้จะถูกปิดไว้ในการตั้งค่าเริ่มต้นของซอฟต์แวร์ คุณจำเป็นต้องสร้างบัญชี ESET

HOME ขึ้นเพื่อเปิดใช้งาน ซึ่งฟังก์ชั่นนี้จะเปิดใช้งานการเก็บข้อมูลในกรณีที่คอมพิวเตอร์ถูกโจรกรรม ถ้าคุณเลือกที่จะเปิดใช้งานฟังก์ชันนี้ของซอฟต์แวร์ ข้อมูลเกี่ยวกับคอมพิวเตอร์ที่ถูกโจรกรรมจะถูกส่งให้แก่ผู้ให้บริการซึ่งอาจรวมถึงข้อมูลเกี่ยวกับตำแหน่งเครือข่ายของคอมพิวเตอร์ ข้อมูลเกี่ยวกับเนื้อหาที่แสดงบนหน้าจอคอมพิวเตอร์ ข้อมูลเกี่ยวกับการกำหนดค่าคอมพิวเตอร์และ/หรือข้อมูลที่บันทึกโดยกล้องที่เชื่อมต่อกับคอมพิวเตอร์ (ในที่นี้จะเรียกว่า "ข้อมูล") ผู้ใช้ปลายทางมีสิทธิ์ที่จะใช้ข้อมูลที่ได้รับจากฟังก์ชันนี้และที่มีการส่งมอบผ่านทางบัญชี ESET HOME เพื่อการแก้ไขสถานการณ์ที่เกิดจากการโจรกรรมคอมพิวเตอร์ สำหรับวัตถุประสงค์ของฟังก์ชันนี้เพียงอย่างเดียว ผู้ให้บริการจะดำเนินการข้อมูลตามที่ระบุไว้ในนโยบายความเป็นส่วนตัวและตามระเบียบข้อบังคับตามกฎหมายที่เกี่ยวข้อง ผู้ให้บริการจะอนุญาตให้ผู้ใช้ปลายทางเข้าถึงข้อมูลเป็นระยะเวลาที่จำเป็นสำหรับวัตถุประสงค์ของการรับข้อมูลนั้นๆ ซึ่งต้องไม่เกินระยะเวลาตามที่ระบุไว้ในนโยบายความเป็นส่วนตัว การป้องกันการใช้ข้อมูลในทางที่ผิดจะใช้เฉพาะกับคอมพิวเตอร์และบัญชีที่ผู้ใช้ปลายทางมีสิทธิ์เข้าถึงที่ถูกต้อง การใช้งานโดยผิดกฎหมายจะถูกรายงานแก่หน่วยงานผู้มีอำนาจ ผู้ให้บริการจะปฏิบัติตามกฎหมายที่เกี่ยวข้อง และช่วยเหลือหน่วยงานผู้รักษากฎหมายในกรณีของการใช้งานผิดวัตถุประสงค์ คุณยอมรับและรับทราบว่าคุณต้องรับผิดชอบต่อการรักษารหัสผ่านในการเข้าถึงบัญชี ESET HOME และคุณยอมรับว่าคุณจะไม่เปิดเผยรหัสผ่านแก่บุคคลที่สาม ผู้ใช้ปลายทางต้องรับผิดชอบต่อกิจกรรมใดๆ ที่ใช้ฟังก์ชันการป้องกันการใช้ข้อมูลในทางที่ผิด และบัญชี ESET HOME ไม่ว่าจะได้รับอนุญาตหรือไม่ ถ้าบัญชี ESET HOME ถูกบุกรุก โปรดแจ้งผู้ให้บริการโดยทันที บทบัญญัติเพิ่มเติมสำหรับการป้องกันการใช้ข้อมูลในทางที่ผิดจะบังคับใช้เฉพาะสำหรับผู้ใช้ปลายทางของ ESET Internet Security และ ESET Smart Security Premium เท่านั้น

ESET Secure Data บทบัญญัติเพิ่มเติมจะนำไปใช้กับ ESET Secure Data ดังต่อไปนี้:

1. คำนิยาม ในบทบัญญัติเพิ่มเติมสำหรับ ESET Secure Data นี้ คำต่างๆ จะมีความหมายที่ตรงกัน ดังนี้:

ก) "ข้อมูล"ข้อมูลหรือข้อมูลใดๆ ที่เข้ารหัสหรือถอดรหัสโดยใช้ซอฟต์แวร์;

ข) "ผลิตภัณฑ์" ซอฟต์แวร์ ESET Secure Data และเอกสารประกอบ;

ค) "ESET Secure Data"ซอฟต์แวร์หนึ่งหรือหลายซอฟต์แวร์ที่ใช้เพื่อเข้ารหัสหรือถอดรหัสข้อมูลอิเล็กทรอนิกส์;

การอ้างอิงข้อความที่เป็นพหูพจน์ทั้งหมดต้องมีเอกพจน์รวมอยู่ด้วย และการอ้างอิงข้อความที่หมายถึงเพศชายทั้งหมดต้องมีเพศหญิงและความไม่มีเพศรวมอยู่ด้วย หรือในทางกลับกัน คำต่างๆ ที่ไม่มีคำนิยามเฉพาะจะถูกใช้ตามคำนิยามที่ระบุไว้ในข้อตกลงนี้

2. คำประกาศของผู้ใช้ปลายทางเพิ่มเติม คุณรับทราบและยอมรับ ดังนี้

ก) เป็นหน้าที่ของคุณที่ต้องปกป้อง รักษา และสำรองข้อมูล;

ข) คุณควรสำรองข้อมูลทั้งหมดอย่างเต็มรูปแบบ รวมถึงข้อมูล (รวมถึงและไม่จำกัดเพียงข้อมูลที่สำคัญและข้อมูลต่างๆ) ในคอมพิวเตอร์ของคุณก่อนที่จะติดตั้ง ESET Secure Data;

ค) คุณต้องเก็บรหัสผ่านหรือข้อมูลอื่นๆ ที่ใช้ในการตั้งค่าและใช้งาน ESET Secure Data ให้ปลอดภัยอยู่เสมอ อีกทั้งคุณต้องสำรองข้อมูลสำเนาของรหัสการเข้ารหัส รหัสใบอนุญาต ไฟล์รหัส และข้อมูลอื่นๆ ที่สร้างเพื่อแยกสื่อเก็บข้อมูล;

ง) คุณต้องรับผิดชอบต่อการใช้งานผลิตภัณฑ์ ผู้ให้บริการจะไม่มีส่วนรับผิดต่อการสูญเสีย การกล่าวอ้าง หรือความเสียหายที่เป็นผลมาจากการเข้ารหัสหรือถอดรหัสข้อมูลหรือข้อมูลอื่นๆ อย่างผิดพลาดหรือไม่ได้รับอนุญาต ไม่ว่าข้อมูลดังกล่าวจะเก็บไว้ที่ใดหรือเก็บไว้อย่างไรก็ตาม;

จ) ขณะที่ผู้ให้บริการได้ดำเนินขั้นตอนที่สมเหตุสมผลทั้งหมดเพื่อให้แน่ใจว่า ESET Secure Data จะสมบูรณ์แบบและมีความปลอดภัย ผู้ใช้จะต้องไม่นำผลิตภัณฑ์นี้ (หรือผลิตภัณฑ์ใดๆ) ไปใช้ในพื้นที่ซึ่งมีระดับความปลอดภัยแบบที่ต้องใช้อุปกรณ์ป้องกันภัย หรือเสี่ยงต่ออันตรายหรือไม่ปลอดภัย ซึ่งรวมถึงแต่ไม่จำกัดเพียงสถานประกอบการด้านนิวเคลียร์ ระบบนำร่องเครื่องบิน ระบบควบคุมหรือสื่อสาร อาวุธและระบบป้องกันการโจมตี รวมถึงระบบกู้ชีพหรือระบบเฝ้าสังเกตการณ์ชีวิต;

ฉ) เป็นหน้าที่ของผู้ใช้ปลายทางที่ต้องตรวจสอบให้แน่ใจว่าระดับความปลอดภัยและการเข้ารหัสที่ผลิตภัณฑ์มีให้นั้นเหมาะสมกับความต้องการของคุณเอง;

ช) คุณต้องรับผิดชอบต่อการใช้งานผลิตภัณฑ์นี้หรือผลิตภัณฑ์ใดๆ ของคุณ ซึ่งรวมถึงแต่ไม่จำกัดเพียงการตรวจสอบให้แน่ใจว่าการใช้งานดังกล่าวตรงตามกฎหมายและข้อบังคับที่มีผลบังคับใช้ของสาธารณรัฐสโลวักหรือประเทศภูมิภาค หรือรัฐอื่นใดที่นำผลิตภัณฑ์นี้ไปใช้งาน คุณจำเป็นต้องตรวจสอบให้แน่ใจว่าก่อนลงมือใช้ผลิตภัณฑ์ใดๆ นั้น คุณได้ตรวจสอบให้แน่ใจแล้วว่าจะไม่เป็นการฝ่าฝืนต่อคำสั่งห้ามตามกฎหมายของรัฐบาลใดๆ (ในสาธารณรัฐสโลวักหรือที่อื่นใด);

ซ) ESET Secure Data อาจติดต่อกับเซิร์ฟเวอร์ของผู้ให้บริการเป็นระยะๆ เพื่อตรวจสอบหาข้อมูลใบอนุญาต การแก้ไขข้อผิดพลาดที่มีให้บริการ Service Pack และรายการอัพเดทอื่นๆ ที่สามารถช่วยปรับปรุง ดูแล แก้ไข หรือเพิ่มประสิทธิภาพให้แก่การดำเนินการของ ESET Secure Data และอาจส่งข้อมูลระบบทั่วไปที่เกี่ยวข้องกับการทำงานของโปรแกรมตามที่ระบุในนโยบายความเป็นส่วนตัว

ผม)ผู้ให้บริการจะไม่รับผิดชอบแต่การสูญหาย ความเสียหาย ค่าใช้จ่าย หรือการกล่าวอ้างที่เกิดขึ้นจากการสูญหาย โจรกรรม การใช้งานอย่างผิดวัตถุประสงค์ การชำรุด ความเสียหายหรือการทำลายรหัสผ่าน ข้อมูลการตั้งค่า รหัสการเข้ารหัส รหัสการเปิดใช้งานใบอนุญาต และข้อมูลอื่นๆ ซึ่งสร้างหรือจัดเก็บในระหว่างที่ใช้งานซอฟต์แวร์นี้

บทบัญญัติเพิ่มเติมสำหรับ ESET Secure Data จะบังคับใช้เฉพาะสำหรับผู้ใช้ปลายทางของ ESET Smart Security Premium เท่านั้น

Password Managerซอฟต์แวร์. บทบัญญัติเพิ่มเติมจะนำไปใช้กับซอฟต์แวร์ Password Manager ดังต่อไปนี้:

1. คำประกาศของผู้ใช้ปลายทางเพิ่มเติม คุณรับทราบและยอมรับว่าคุณจะไม่สามารถทำสิ่งต่างๆ ดังนี้

ก) ใช้ Password Manager Software เพื่อดำเนินการในภารกิจร้ายแรงที่ซึ่งมีผลต่อชีวิตของมนุษย์หรือทรัพย์สิน คุณเข้าใจเป็นอย่างดีว่า Password Manager Software ไม่ได้ออกแบบมาเพื่อวัตถุประสงค์ดังกล่าวและผู้ให้บริการจะไม่มีส่วนรับผิดชอบต่อการที่ซอฟต์แวร์ไม่อาจปฏิบัติภารกิจที่ผิดวัตถุประสงค์นั้นให้ลุล่วงได้ ซึ่งนำไปสู่การเสียชีวิต การบาดเจ็บของบุคคล หรือความเสียหายร้ายแรงต่อทรัพย์สินหรือสภาพแวดล้อม

PASSWORD MANAGER SOFTWARE ไม่ได้ออกแบบ มีวัตถุประสงค์ หรือรับสิทธิอนุญาตให้ใช้ในสภาพแวดล้อมที่เป็นอันตรายที่ซึ่งต้องควบคุมให้ใช้อุปกรณ์ป้องกันภัย ซึ่งรวมถึงแต่ไม่จำกัดเพียงการออกแบบ การก่อสร้าง การบำรุงรักษา หรือลงมือปฏิบัติการในสถานประกอบการด้านนิวเคลียร์ ระบบนำร่องเครื่องบินหรือระบบสื่อสาร ระบบควบคุมเส้นทางบิน และระบบกู้ชีพหรือระบบอาวุธ ผู้ให้บริการขอปฏิเสธอย่างเจาะจงว่าจะไม่ให้การรับประกันทั้งโดยชัดแจ้งหรือโดยนัยต่อความเหมาะสมกับวัตถุประสงค์ดังกล่าว

ข) นำ Password Manager Software ไปใช้ในลักษณะที่ละเมิดต่อข้อตกลงฉบับนี้หรือละเมิดกฎหมายของสาธารณรัฐสโลวักหรือเขตอำนาจศาลในพื้นที่ของคุณ โดยเฉพาะอย่างยิ่ง คุณต้องไม่ใช้ Password Manager Software เพื่อลงมือหรือดำเนินกิจกรรมใดๆ ที่ผิดกฎหมาย อันรวมถึงการอัพโหลดข้อมูลซึ่งมีเนื้อหาที่เป็นอันตราย หรือเนื้อที่อาจนำไปใช้ในกิจกรรรมผิดกฎหมายใดๆ หรือวิธีการใดๆ ก็ตามซึ่งอาจผิดกฎหมายหรือละเมิดสิทธิ์ของบุคคลที่สาม (รวมถึงสิทธิ์ในทรัพย์สินทางปัญญา) รวมถึงแต่ไม่จำกัดเพียง การพยายามเข้าสู่บัญชีต่างๆ ใน พื้นที่เก็บข้อมูล (ตามวัตถุประสงค์ของข้อกำหนดเพิ่มเติมไปยังซอฟต์แวร์ Password Manager นี้ “พื้นที่เก็บข้อมูล“ หมายถึงพื้นที่สำหรับจัดเก็บข้อมูลซึ่งบริหารจัดการโดยผู้ให้บริการหรือบุคคลที่สามนอกเหนือจากผู้ให้บริการและผู้ใช้ โดยมีวัตถุประสงค์เพื่อเปิดใช้งานการซิงโครไนซ์และสำรองข้อมูลผู้ใช้) หรือในบัญชีและข้อมูลใดๆ ของผู้ใช้ Password Manager Software หรือพื้นที่เก็บข้อมูลรายอื่น หากคุณละเมิดบทบัญญัติข้อใดเหล่านี้ ผู้ให้บริการจะมีสิทธิ์ยุติข้อตกลงฉบับนี้ในทันที และส่งค่าใช้จ่ายในการเยียวยาที่จำเป็นไปให้คุณ รวมถึงดำเนินขั้นตอนที่จำเป็นเพื่อป้องกันไม่ให้คุณใช้งาน Password Manager Software ต่อไปโดยที่คุณไม่มีสิทธิ์ขอรับเงินคืนแต่อย่างใด

2. ข้อจำกัดความรับผิด PASSWORD MANAGER SOFTWARE นี้ได้จัดหาให้แก่คุณแบบ "ตามสภาพ" โดยไม่มีการรับประกันทั้งโดยชัดแจ้งหรือโดยนัย คุณใช้งานซอฟต์แวร์นี้โดยรับความเสี่ยงด้วยตัวคุณเอง ผู้ให้บริการจะไม่มีความรับผิดต่อการสูญเสียข้อมูล ความเสียหาย การจำกัดการเปิดให้บริการ ซึ่งรวมถึงข้อมูลใดๆ ที่ส่งโดย PASSWORD MANAGER SOFTWARE ไปยังพื้นที่เก็บข้อมูลภายนอกโดยมีวัตถุประสงค์เพื่อซิงโครไนซ์และสำรองข้อมูล การเข้า

รหัสข้อมูลโดยใช้ PASSWORD MANAGER SOFTWARE ไม่ได้หมายความว่าผู้ให้บริการต้องรับผิดชอบต่อความปลอดภัยของข้อมูลดังกล่าว คุณยอมรับโดยตรงว่าข้อมูลที่ได้รับ ใช้ เข้ารหัส จัดเก็บ ซิงโครไนซ์ หรือส่งโดยใช้ PASSWORD MANAGER SOFTWARE นั้นสามารถจัดเก็บลงในเซิร์ฟเวอร์ของบุคคลที่สามได้ (มีผลเฉพาะกับการใช้งาน PASSWORD MANAGER SOFTWARE ที่เปิดใช้งานบริการซิงโครไนซ์และสำรองข้อมูลเท่านั้น) หากผู้ให้บริการใช้ดุลยพินิจและตัดสินใจเลือกที่จะใช้งานพื้นที่จัดเก็บ เว็บไซต์ เว็บพอร์ทัล เซิร์ฟเวอร์หรือบริการของบุคคลที่สาม ผู้ให้บริการจะไม่มีส่วนรับผิดชอบในคุณภาพ ความปลอดภัย หรือความพร้อมให้บริการของบริการของบุคคลที่สามดังกล่าว และไม่ว่าด้วยขอบเขตใดก็ตาม ผู้ให้บริการจะไม่มีส่วนรับผิดชอบต่อคุณในกรณีที่บุคคลที่สามทำผิดข้อมูลผูกมัดในสัญญาหรือข้อกฎหมาย และผู้ให้บริการไม่มีส่วนรับผิดชอบต่อความเสียหาย การสูญเสียรายได้ ความเสียหายทางการเงินหรือไม่ใช่ทางการเงิน หรือความสูญเสียอื่นๆ ในระหว่างที่ใช้งานซอฟต์แวร์ ผู้ให้บริการไม่มีส่วนรับผิดชอบต่อเนื้อหาหรือข้อมูลใดๆ ที่ได้รับ ใช้ เข้ารหัส จัดเก็บ ซิงโครไนซ์ หรือส่งโดยใช้ PASSWORD MANAGER SOFTWARE หรือในพื้นที่จัดเก็บ คุณรับทราบว่าผู้ให้บริการไม่สามารถเข้าถึงเนื้อหาของข้อมูลที่จัดเก็บอยู่ได้ รวมถึงไม่สามารถตรวจสอบเนื้อหานั้นหรือลบเนื้อหาที่เป็นอันตรายต่อกฎหมายได้

ผู้ให้บริการมีสิทธิ์ทุกประการในการปรับปรุง อัพเกรด และแก้ไขสิ่งต่างๆ ที่เกี่ยวข้องกับ Password MANAGER Software ("การปรับปรุง") ซึ่งหมายรวมถึงในสถานการณ์ที่การปรับปรุงดังกล่าวเกิดขึ้นจากคำติชม ความคิดเห็นหรือคำแนะนำที่คุณส่งเข้ามาไม่ว่าในรูปแบบใดก็ตาม คุณจะไม่มีสิทธิ์ในค่าตอบแทนใดๆ รวมถึงไม่มีสิทธิ์ในเงินค่าลิขสิทธิ์ใดๆ ที่เกี่ยวข้องกับการปรับปรุงดังกล่าว

บุคลากรและผู้ให้การอนุญาตของผู้ให้บริการจะไม่มีส่วนรับผิดชอบใดๆ ต่อการกล่าวอ้าง และไม่มีส่วนรับผิดชอบต่อผลอันเกิดจาก หรือมีส่วนเกี่ยวข้องใดๆ กับการใช้งาน PASSWORD MANAGER SOFTWARE ของคุณหรือของบุคคลที่สาม ต่อการใช้หรือการไม่ใช้บริษัทนายหน้าหรือตัวแทนจำหน่าย หรือการขายหรือการซื้อความปลอดภัยใดๆ ไม่ว่าการกล่าวอ้างและส่วนรับผิดชอบดังกล่าวจะตั้งอยู่บนทฤษฎีทางกฎหมายหรือความเที่ยงตรงยุติธรรมใดก็ตาม

บุคลากรและผู้ให้การอนุญาตของผู้ให้บริการจะไม่มีส่วนรับผิดชอบต่อความเสียหายทั้งหมดหรือความเสียหายทางตรง เกิดขึ้นโดยอุบัติเหตุ เป็นกรณีพิเศษ ทางอ้อม หรือเป็นผลต่อเนื่อง ซึ่งเกิดขึ้นจากหรือมีส่วนเกี่ยวข้องกับซอฟต์แวร์ใดๆ ของบุคคลที่สาม ข้อมูลใดๆ ที่เข้าถึงผ่าน PASSWORD MANAGER SOFTWARE การใช้หรือไม่สามารถใช้หรือเข้าถึง PASSWORD MANAGER SOFTWARE ของคุณ หรือข้อมูลใดๆ ที่จัดหาให้ผ่าน PASSWORD MANAGER SOFTWARE ไม่ว่าการกล่าวอ้างเรื่องความเสียหายดังกล่าวจะหยิบยกขึ้นมาจากข้อเท็จจริงทางกฎหมายหรือความยุติธรรมก็ตาม ความเสียหายต่างๆ ที่ไม่อยู่ในข้อกำหนดนี้ ซึ่งรวมถึงแต่ไม่จำกัดเพียงการสูญเสียรายได้ทางธุรกิจ การบาดเจ็บเสียหายที่เกิดกับบุคคลหรือทรัพย์สิน การหยุดชะงักของธุรกิจ การสูญเสียข้อมูลธุรกิจหรือส่วนบุคคล บางเขตอำนาจศาลไม่อนุญาตให้มีการจำกัดความเสียหายทางอุบัติเหตุหรือความเสียหายที่เกิดขึ้นในภายหลัง ดังนั้นข้อจำกัดนี้อาจไม่ได้บังคับใช้กับคุณ ในกรณีดังกล่าว ความรับผิดชอบของผู้ให้บริการจะมีขอบเขตเท่ากับขอบเขตขั้นต่ำที่กฎหมายอนุญาต

ข้อมูลที่มอบให้ผ่านทาง PASSWORD MANAGER SOFTWARE ซึ่งรวมถึงราคาเสนอหุ้น บทวิเคราะห์ ข้อมูลตลาด ข่าวสาร และข้อมูลทางการเงินอาจมีความล่าช้า ไม่แม่นยำ หรือมีข้อผิดพลาดหรือส่วนที่ขาดหาย และบุคลากรและผู้ให้การอนุญาตของผู้ให้บริการจะไม่มีส่วนรับผิดชอบต่อสิ่งต่างๆ ดังกล่าว ผู้ให้บริการอาจเปลี่ยนหรือหยุดพัฒนาส่วนหรือคุณลักษณะใดๆ ของ PASSWORD MANAGER SOFTWARE หรือการใช้งานของคุณลักษณะหรือเทคโนโลยีใดๆ ใน PASSWORD MANAGER SOFTWARE ได้ทุกเมื่อโดยไม่ต้องแจ้งให้คุณทราบล่วงหน้า

หากเงื่อนไขในบทความนี้เป็นโมฆะไม่ว่าด้วยเหตุผลใดก็ตาม หรือมีการถือให้ผู้ให้บริการมีหน้าที่รับผิดชอบต่อความสูญเสีย ความเสียหาย ฯลฯ ภายใต้กฎหมายที่บังคับใช้ ทุกฝ่ายจะยอมรับว่าความรับผิดชอบที่ผู้ให้บริการมีต่อคุณจะจำกัดอยู่เพียงเท่ากับยอดรวมค่าใบอนุญาตทั้งหมดที่คุณได้ชำระเท่านั้น

คุณยอมรับที่จะชดใช้ค่าเสียหาย ปกป้อง และไม่แสดงความมุ่งร้ายต่อผู้ให้บริการรวมถึงลูกค้า สำนักงานสาขา กิจการในเครือ แบรนด์ปรับโฉมใหม่และคู่ค้าอื่นๆ ของผู้ให้บริการจากการกล่าวอ้าง ความรับผิดชอบ ความเสียหาย ความสูญเสีย ต้นทุน ค่าใช้จ่าย ค่าธรรมเนียมทั้งหมดของบุคคลที่สาม (รวมถึงเจ้าของอุปกรณ์หรือฝ่ายที่สิทธิ์ได้รับผลกระทบจากข้อมูลที่ใช้ใน PASSWORD MANAGER SOFTWARE หรือในพื้นที่จัดเก็บ) ที่ฝ่ายดังกล่าวอาจประสบอันเป็นผลมาจากการใช้งาน PASSWORD MANAGER SOFTWARE ของคุณ

3. ข้อมูลใน Password Manager Software เว้นแต่คุณจะเลือกไว้อย่างชัดเจน ข้อมูลทั้งหมดที่คุณป้อนซึ่งบันทึกไว้ในฐานข้อมูล Password Manager Software จะถูกจับเก็บในรูปแบบเข้ารหัสไว้ในคอมพิวเตอร์ของคุณ หรืออุปกรณ์จัดเก็บอื่นๆ ที่คุณกำหนด คุณเข้าใจเป็นอย่างดีว่าในกรณีที่มีการลบหรือเกิดความเสียหายขึ้นกับฐานข้อมูลใดของ Password Manager Software หรือไฟล์อื่นๆ ข้อมูลทั้งหมดที่อยู่ในนั้นจะสูญหายไปโดยไม่อาจนำกลับมาได้อีก และคุณเข้าใจและยอมรับความเสี่ยงของความสูญเสียดังกล่าว ความจริงที่ว่าข้อมูลส่วนตัวของคุณจัดเก็บอยู่ในรูปแบบเข้ารหัสไว้ในคอมพิวเตอร์นั้นไม่ได้หมายความว่าข้อมูลดังกล่าวไม่อาจถูกขโมยหรือถูกนำไปใช้ในทางที่ผิดโดยน้ำมือของผู้ที่ค้นพบรหัสผ่านหลักหรือสามารถเข้าสู่อุปกรณ์เปิดใช้งานที่ลูกค้ากำหนดไว้เพื่อเปิดฐานข้อมูล คุณมีหน้าที่รับผิดชอบในการดูแลความปลอดภัยของทุกช่องทางการเข้าถึง

4. การรับส่งข้อมูลส่วนบุคคลไปยังผู้ให้บริการหรือพื้นที่เก็บข้อมูล หากคุณได้เลือกไว้และมีวัตถุประสงค์เพียงเพื่อที่จะให้แน่ใจว่าการซิงโครไนซ์และสำรองข้อมูลจะเป็นไปตามเวลาที่กำหนด Password Manager Software จะรับส่งหรือส่งข้อมูลส่วนบุคคลจากฐานข้อมูล Password Manager Software ซึ่งได้แก่รหัสผ่าน ข้อมูลการเข้าสู่ระบบ บัญชีและข้อมูลประจำตัว ผ่านทางอินเทอร์เน็ตไปยังพื้นที่จัดเก็บ ข้อมูลจะรับส่งในรูปแบบเข้ารหัสเท่านั้น การใช้งาน Password Manager Software เพื่อกรอกแบบฟอร์มออนไลน์ด้วยรหัสผ่าน ข้อมูลเข้าสู่ระบบ หรือข้อมูลอื่นๆ อาจต้องอาศัยการส่งข้อมูลดังกล่าวผ่านทางอินเทอร์เน็ตไปยังเว็บไซต์ที่คุณกำหนด การรับส่งข้อมูลดังกล่าวนี้ไม่ได้เริ่มดำเนินการโดย Password Manager Software และจะไม่ถือว่าผู้ให้บริการต้องรับผิดชอบใดๆ ต่อความปลอดภัยของการโต้ตอบกับเว็บไซต์ใดๆ ที่สนับสนุนโดยผู้ให้บริการรายต่างๆ ดังกล่าว การรับส่งข้อมูลผ่านอินเทอร์เน็ตใดก็ตาม

ไม่ว่าจะเกิดขึ้นร่วมกับ Password Manager Software หรือไม่ล้วนกระทำโดยตั้งอยู่บนดุลพินิจและความเสี่ยงของคุณเอง และคุณจะเป็นผู้รับผิดชอบแต่เพียงผู้เดียวต่อความเสียหายใดๆ ที่เกิดขึ้นกับระบบคอมพิวเตอร์ของคุณหรือการสูญเสียข้อมูลอันเป็นผลมาจากการดาว์นโหลดและ/หรือใช้งานเนื้อหาหรือบริการดังกล่าว เพื่อเป็นการลดความเสี่ยงต่อการสูญเสียข้อมูลที่สำคัญ ผู้ให้บริการขอแนะนำให้ลูกค้าทำการสำรองข้อมูลในฐานข้อมูลและไฟล์ที่ละเอียดอ่อนอื่นๆ ไปยังไดรฟ์ภายนอกเป็นระยะๆ ผู้ให้บริการไม่สามารถมอบความช่วยเหลือในการกู้คืนข้อมูลที่สูญหายหรือเสียหายใดๆ ได้ หากผู้ให้บริการมอบบริการสำรองข้อมูลสำหรับไฟล์ฐานข้อมูลผู้ใช้ในกรณีที่เกิดความเสียต่อหรือการลบไฟล์ในพีซีของผู้ใช้ บริการสำรองข้อมูลดังกล่าวจะไม่มีการรับประกันใดๆ และไม่ได้มีนัยว่าผู้ให้บริการต้องมีความรับผิดชอบใดๆ ต่อคุณแต่อย่างใด

เมื่อใช้งาน Password Manager Software จะถือว่าคุณยอมรับว่าซอฟต์แวร์นี้อาจติดต่อกับเซิร์ฟเวอร์ของผู้ให้บริการเป็นระยะๆ เพื่อตรวจสอบหาข้อมูลใบอนุญาต การแก้ไขข้อผิดพลาดที่มีให้บริการ Service Pack และรายการอัพเดทอื่นๆ ที่สามารถช่วยปรับปรุง ดูแล แก้ไข หรือเพิ่มประสิทธิภาพให้แก่การดำเนินการของ Password Manager Software ซอฟต์แวร์นี้อาจส่งข้อมูลระบบทั่วไปที่เกี่ยวข้องกับการทำงานของ Password Manager Software ตามที่ระบุในนโยบายความเป็นส่วนตัว

5. ข้อมูลและคำแนะนำเกี่ยวกับการถอนการติดตั้ง คุณต้องส่งออกข้อมูลใดๆ ที่คุณต้องการเก็บจากฐานข้อมูลก่อนที่จะถอนการติดตั้ง Password Manager Software

บทบัญญัติเพิ่มเติมสำหรับซอฟต์แวร์ Password Manager จะบังคับใช้เฉพาะสำหรับผู้ใช้ปลายทางของ ESET Smart Security Premium เท่านั้น

ESET LiveGuard. บทบัญญัติเพิ่มเติมจะนำไปใช้กับ ESET LiveGuard ดังต่อไปนี้:

ซอฟต์แวร์มีฟังก์ชั่นการวิเคราะห์ไฟล์ที่ส่งโดยผู้ใช้ปลายทางเพิ่มเติม ผู้ให้บริการจะใช้เฉพาะไฟล์ที่ส่งโดยผู้ใช้ปลายทางและผลการวิเคราะห์ที่สอดคล้องกับนโยบายความเป็นส่วนตัวและสอดคล้องกับข้อบังคับทางกฎหมายที่เกี่ยวข้องเท่านั้น

บทบัญญัติเพิ่มเติมสำหรับ ESET LiveGuard จะบังคับใช้เฉพาะสำหรับผู้ใช้ปลายทางของ ESET Smart Security Premium เท่านั้น

EULAID: EULA-PRODUCT-LG-EHSW; 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 ให้ความสำคัญต่อการปกป้องข้อมูลส่วนบุคคลเป็นพิเศษ ในฐานะผู้ควบคุมข้อมูล ("ESET" หรือ "เรา") เราต้องการปฏิบัติตามข้อกำหนดด้านความโปร่งใสตามมาตรฐานทางกฎหมาย ภายใต้ระเบียบการคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป ("GDPR") เพื่อให้บรรลุเป้าหมายนี้ เราเผยแพร่นโยบายความเป็นส่วนตัวนี้โดยมีวัตถุประสงค์เพื่อแจ้งข้อมูลลูกค้าของเราเท่านั้น ("ผู้ใช้ปลายทาง" หรือ "คุณ") ในฐานะเจ้าของข้อมูล เกี่ยวกับหัวข้อการปกป้องข้อมูลส่วนบุคคลต่อไปนี้:

- พื้นฐานทางกฎหมายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
- การแชร์ข้อมูลและการรักษาความลับ
- การรักษาความปลอดภัยของข้อมูล
- สิทธิของคุณในฐานะเจ้าของข้อมูล
- การประมวลผลข้อมูลส่วนบุคคลของคุณ
- ข้อมูลติดต่อ

พื้นฐานทางกฎหมายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

พื้นฐานทางกฎหมายสำหรับการประมวลผลข้อมูลที่เราใช้ตามกรอบกฎหมายที่บังคับใช้ซึ่งเกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคลนั้นมีจำนวนไม่มากนัก โดยหลักแล้วการประมวลผลข้อมูลส่วนบุคคลที่ ESET นั้นจำเป็นต่อการปฏิบัติงานของ ผู้ใช้ปลายทางข้อตกลงการอนุญาตใช้งาน (“EULA”) ที่มีผู้ใช้ปลายทาง (มาตรา 6 (1) (b) GDPR) ซึ่งมีผลบังคับใช้สำหรับการจัดหาผลิตภัณฑ์หรือบริการของ ESET เว้นแต่จะมีการระบุไว้อย่างชัดเจนเป็นอย่างอื่น เช่น

- พื้นฐานทางกฎหมายด้านผลประโยชน์ที่ชอบด้วยกฎหมาย (มาตรา 6 (1) (f) GDPR) ซึ่งช่วยให้เราสามารถประมวลผลข้อมูลเกี่ยวกับวิธีที่ลูกค้าของเราใช้บริการและความพึงพอใจของลูกค้า เพื่อให้ผู้ใช้ของเราได้รับการคุ้มครอง การสนับสนุน และประสบการณ์ที่ดีที่สุดที่เราสามารถนำเสนอได้ แม้แต่การตลาดก็ได้รับการยอมรับจากกฎหมายที่เกี่ยวข้องว่าเป็นประโยชน์โดยชอบด้วยกฎหมาย ด้วยเหตุนี้เราจึงมักพึ่งพาคุกกี้นี้เพื่อสื่อสารด้านการตลาดกับลูกค้าของเรา

- เราอาจร้องขอความยินยอม (มาตรา 6 (1) (a) GDPR) จากคุณในสถานการณ์ที่เฉพาะเจาะจง เมื่อเราเล็งเห็นว่าพื้นฐานทางกฎหมายนี้เป็นพื้นฐานที่เหมาะสมที่สุด หรือหากกฎหมายกำหนดไว้

- ความสอดคล้องกับข้อผูกมัดทางกฎหมาย (มาตรา 6 (1) (c) GDPR) เช่น ความต้องการด้านการกำหนดเงื่อนไขสำหรับการติดต่อสื่อสารทางอิเล็กทรอนิกส์ การเก็บรักษาเอกสารใบแจ้งหนี้หรือใบเรียกเก็บเงิน

การแชร์ข้อมูลและการรักษาความลับ

เราจะไม่แบ่งปันข้อมูลของคุณกับบริษัทอื่น อย่างไรก็ตาม ESET เป็นบริษัทที่ดำเนินธุรกิจทั่วโลกผ่านบริษัทในเครือหรือคู่ค้าเป็นส่วนหนึ่งของเครือข่ายการขาย การให้บริการ และการสนับสนุนของเรา ข้อมูลการอนุญาต การเรียกเก็บเงิน และการสนับสนุนด้านเทคนิคที่ ESET เป็นผู้ประมวลผลอาจสามารถถ่ายโอนไปยังและจากเครือหรือคู่ค้าเพื่อจุดประสงค์ในการปฏิบัติตาม EULA เช่น การให้บริการหรือการสนับสนุน

ESET จะประมวลผลข้อมูลในสหภาพยุโรป (EU) ถ้าเป็นไปได้ อย่างไรก็ตาม เราอาจจำเป็นต้องถ่ายโอนข้อมูลของคุณไปยังประเทศที่อยู่นอกสหภาพยุโรปโดยขึ้นอยู่กับตำแหน่งที่ตั้งของคุณ (การใช้ผลิตภัณฑ์และ/หรือบริการของเราที่อยู่นอกสหภาพยุโรป) และ/หรือบริการที่คุณเลือก ตัวอย่างเช่น เราใช้บริการของบริษัทอื่นในการเชื่อมต่อกับการประมวลผลแบบคลาวด์ ในกรณีเหล่านี้ เราจะเลือกผู้ให้บริการของเราอย่างรอบคอบ และรับรองว่ามีการป้องกันข้อมูลในระดับที่เหมาะสมผ่านมาตรการทางสัญญา เช่นเดียวกับมาตรการทางเทคนิคและองค์กร ตามกฎแล้ว เรายอมรับข้อสัญญามาตรฐานของสหภาพยุโรป โดยมีข้อบังคับเพิ่มเติมทางสัญญาหากจำเป็น

สำหรับบางประเทศนอกสหภาพยุโรป เช่น สหราชอาณาจักรและสวิตเซอร์แลนด์ สหภาพยุโรปได้กำหนดระดับการคุ้มครองข้อมูลไว้ในระดับที่เทียบเคียงกันได้แล้ว เนื่องจากมีการป้องกันข้อมูลในระดับที่เทียบเคียงกันได้ การถ่ายโอนข้อมูลไปยังประเทศเหล่านี้จึงไม่จำเป็นต้องมีการอนุญาตหรือข้อตกลงพิเศษใดๆ

การรักษาความปลอดภัยของข้อมูล

ESET ใช้มาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมเพื่อให้แน่ใจว่ามีระดับความปลอดภัยที่เหมาะสมกับความเสี่ยงที่อาจเกิดขึ้น เรากำลังพยายามอย่างเต็มที่เพื่อให้มั่นใจได้ถึงการรักษาความลับที่ต่อเนื่อง ความสมบูรณ์ ความพร้อมใช้งาน และความยืดหยุ่นของระบบและบริการด้านการประมวลผล อย่างไรก็ตาม ในกรณีที่ข้อมูลถูกละเมิดจนเป็นผลทำให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของคุณ เราพร้อมที่จะแจ้งให้หน่วยงานกำกับดูแลที่เกี่ยวข้องทราบรวมถึงผู้ใช้ปลายทางที่เป็นเจ้าของข้อมูลด้วย

สิทธิของเจ้าของข้อมูล

สิทธิของผู้ใช้ปลายทางทุกคนมีความสำคัญ และเราขอแจ้งให้คุณทราบว่าผู้ใช้ปลายทางทั้งหมด (จากประเทศในสหภาพยุโรปหรือไม่ใช่สหภาพยุโรป) จะได้รับการรับประกันสิทธิดังต่อไปนี้ที่ ESET หากต้องการใช้สิทธิ์ในการเป็นเจ้าของข้อมูลของคุณ คุณสามารถติดต่อเราผ่านแบบฟอร์มการสนับสนุนหรือทางอีเมลได้ที่ dpo@eset.sk เราจะขอข้อมูลต่อไปนี้จากคุณเพื่อวัตถุประสงค์ในการระบุตัวตน ชื่อ ที่อยู่อีเมล และรหัสใบอนุญาตหรือหมายเลขลูกค้าและบริษัทที่เป็นเครือข่าย หากมี โปรดอย่าส่งข้อมูลส่วนบุคคลอื่นๆ เช่น วันเดือนปีเกิด ให้แก่เรา เราขอชี้ว่า เราจะประมวลผลข้อมูลส่วนบุคคลของคุณเพื่อให้สามารถดำเนินการตามคำขอของคุณได้ รวมถึงเพื่อวัตถุประสงค์ในการระบุตัวตน

สิทธิในการเพิกถอนความยินยอม สิทธิในการเพิกถอนความยินยอมจะใช้ได้ในกรณีที่มีการประมวลผลตามความยินยอมเท่านั้น หากเราประมวลผลข้อมูลส่วนบุคคลตามความยินยอมของคุณ คุณมีสิทธิที่จะเพิกถอนความยินยอมได้ทุกเมื่อโดยไม่ต้องให้เหตุผล การเพิกถอนความยินยอมของคุณจะมีผลเฉพาะในอนาคต และไม่มีผลต่อความชอบด้วยกฎหมายของข้อมูลที่ประมวลผลก่อนการเพิกถอนดังกล่าว

สิทธิในการคัดค้าน สิทธิในการคัดค้านการประมวลผลจะใช้ได้ในกรณีที่มีการประมวลผลตามผลประโยชน์ที่ชอบด้วยกฎหมายของ ESET หรือบริษัทอื่นเท่านั้น หากเราประมวลผลข้อมูลส่วนบุคคลของคุณเพื่อปกป้องผลประโยชน์ที่ชอบด้วยกฎหมาย คุณในฐานะเจ้าของข้อมูลมีสิทธิคัดค้านผลประโยชน์ที่ชอบด้วยกฎหมายที่เรากำหนดให้ และคัดค้านการประมวลผลข้อมูลส่วนบุคคลของคุณได้ตลอดเวลา การคัดค้านของคุณจะมีผลเฉพาะในอนาคต และไม่มีผลต่อความถูกต้องตามกฎหมายของข้อมูลที่ประมวลผลก่อนการคัดค้านดังกล่าว หากเราประมวลผลข้อมูลส่วนบุคคลของคุณเพื่อวัตถุประสงค์ทางการตลาดทางตรง คุณไม่จำเป็นต้องให้เหตุผลในการคัดค้านของคุณ ความนี้ยังใช้กับการสร้างโปรไฟล์ ตราบเท่าที่มีการเชื่อมต่อกับการตลาดทางตรงดังกล่าวอีกด้วย ในกรณีอื่นๆ เราขอให้คุณแจ้งให้เราทราบสั้นๆ เกี่ยวกับข้อร้องเรียนว่าด้วยผลประโยชน์ที่ชอบด้วยกฎหมายของ ESET ในการประมวลผลข้อมูลส่วนบุคคลของคุณ

โปรดทราบว่าในบางกรณี เรามีสิทธิประมวลผลข้อมูลส่วนบุคคลของคุณต่อไปบนพื้นฐานของพื้นฐานทางกฎหมายอื่นๆ ตัวอย่างเช่น เพื่อการปฏิบัติตามสัญญา แม้จะมีการเพิกถอนความยินยอมจากคุณก็ตาม

สิทธิในการเข้าถึง ในฐานะเจ้าของข้อมูล คุณมีสิทธิที่จะได้รับข้อมูลเกี่ยวกับข้อมูลของคุณที่ ESET จัดเก็บโดยไม่เสียค่าใช้จ่ายได้ตลอดเวลา

สิทธิในการแก้ให้ถูกต้อง หากเราประมวลผลข้อมูลส่วนบุคคลที่ไม่ถูกต้องเกี่ยวกับคุณโดยไม่ได้ตั้งใจ คุณมีสิทธิที่จะแก้ไขข้อมูลดังกล่าว

สิทธิในการลบและสิทธิในการจำกัดการประมวลผล ในฐานะเจ้าของข้อมูล คุณมีสิทธิร้องขอให้ลบหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลของคุณ หากเราประมวลผลข้อมูลส่วนบุคคลของคุณ ตัวอย่างเช่น ด้วยความยินยอมของคุณ และคุณเพิกถอนความยินยอมนั้นโดยไม่มีพื้นฐานทางกฎหมายอื่นๆ ตัวอย่างเช่น สัญญา เราจะลบข้อมูลส่วนบุคคลของคุณทันที ข้อมูลส่วนบุคคลของคุณจะถูกลบทันทีที่ไม่จำเป็นต้องใช้ตามวัตถุประสงค์ที่ระบุไว้ เมื่อสิ้นสุดระยะเวลาการเก็บรักษาข้อมูล

หากเราใช้ข้อมูลส่วนบุคคลของคุณเพื่อวัตถุประสงค์ในการตลาดทางตรง และคุณได้เพิกถอนความยินยอมของคุณหรือคัดค้านผลประโยชน์ที่ชอบด้วยกฎหมายของ ESET เราจะจำกัดการประมวลผลข้อมูลส่วนบุคคลของคุณเท่าที่เรารวบรวมข้อมูลติดต่อของคุณไว้ได้ในบัญชีดำภายในของเรา ทั้งนี้เพื่อหลีกเลี่ยงการติดต่อที่ไม่พึงประสงค์ มิฉะนั้น ข้อมูลส่วนบุคคลของคุณจะถูกลบ

โปรดทราบว่าเราอาจจำเป็นต้องเก็บข้อมูลของคุณไว้จนกว่าภาระผูกพันในการเก็บรักษาและระยะเวลา ซึ่งออกโดยสมาชิกสภานิติบัญญัติหรือหน่วยงานกำกับดูแล จะหมดอายุ ภาระผูกพันในการเก็บรักษาและระยะเวลานี้อาจเป็นผลมาจากกฎหมายของสโลวะเกีย หลังจากนั้น ข้อมูลที่เกี่ยวข้องจะถูกลบเป็นประจำ

สิทธิ์ในการเคลื่อนย้ายข้อมูล เรายินดีที่จะมอบข้อมูลส่วนบุคคลที่ประมวลผลโดย ESET ในรูปแบบ xls ให้แก่คุณซึ่งเป็นเจ้าของข้อมูล

สิทธิในการยื่นเรื่องร้องเรียน ในฐานะเจ้าของข้อมูล คุณมีสิทธิที่จะยื่นเรื่องร้องเรียนต่อหน่วยงานกำกับดูแลได้ตลอดเวลา ESET มีหน้าที่ต้องปฏิบัติตามกฎหมายของประเทศสโลวาเกียและเราต้องปฏิบัติตามกฎหมายว่าด้วยการปกป้องข้อมูลในฐานะส่วนหนึ่งของสหภาพยุโรป หน่วยงานกำกับดูแลข้อมูลที่เกี่ยวข้องคือสำนักงานคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสโลวัก ซึ่งตั้งอยู่ที่ Hraničná 12, 82007 Bratislava 27, Slovak Republic

การประมวลผลข้อมูลส่วนบุคคลของคุณ

บริการที่ ESET นำเสนอในผลิตภัณฑ์ของเรามีให้ภายใต้ข้อกำหนดของ EULAแต่อาจต้องให้ความสนใจบางผลิตภัณฑ์เป็นพิเศษ ราต้องการให้รายละเอียดเพิ่มเติมเกี่ยวกับการรวบรวมข้อมูลที่เกี่ยวข้องกับการให้บริการของเรา เราให้บริการต่างๆ ตามที่ได้อธิบายไว้ใน EULA และผลิตภัณฑ์ เอกสารประกอบ. เพื่อให้การทำงานทั้งหมด เราจำเป็นต้องรวบรวมข้อมูลต่อไปนี้:

ข้อมูลการออกใบอนุญาตและการเรียกเก็บเงิน ESET จะเก็บรวบรวมและประมวลผลชื่อ ที่อยู่อีเมล รหัสใบอนุญาตและที่อยู่ (หากมี) บริษัทในเครือและข้อมูลการชำระเงิน เพื่ออำนวยความสะดวกในการเปิดใช้งานใบอนุญาต การส่งมอบรหัสใบอนุญาต การแจ้งเตือนเกี่ยวกับการหมดอายุ คำขอสนับสนุน การตรวจสอบความถูกต้องของใบอนุญาต การให้บริการของเรา และการแจ้งเตือนอื่นๆ รวมถึงข้อความทางการตลาดที่สอดคล้องกับกฎหมายที่บังคับ

ใช้ หรือความยินยอมของคุณ ESET มีหน้าที่ตามกฎหมายในการเก็บรักษาข้อมูลการเรียกเก็บเงินเป็นระยะเวลา 10 ปี อย่างไรก็ตาม ข้อมูลการออกใบอนุญาตจะไม่ระบุตัวตนภายใน 12 เดือนหลังจากใบอนุญาตหมดอายุ

รายการอัพเดทและสถิติอื่นๆ ข้อมูลที่ประมวลผลได้แก่ข้อมูลเกี่ยวกับกระบวนการติดตั้งและคอมพิวเตอร์ของคุณ รวมทั้งแพลตฟอร์มที่ติดตั้งผลิตภัณฑ์ของเราและข้อมูลเกี่ยวกับการดำเนินงานและฟังก์ชันการทำงานของผลิตภัณฑ์ของเรา เช่น ระบบปฏิบัติการ, ข้อมูลฮาร์ดแวร์, ไอดีการติดตั้ง, ไอดีใบอนุญาต, ที่อยู่ IP, ที่อยู่ MAC, การตั้งค่าของผลิตภัณฑ์ ซึ่งจะถูกประมวลผลเพื่อวัตถุประสงค์ในการให้บริการอัพเดทและอัพเกรด และเพื่อวัตถุประสงค์ในการบำรุงรักษา การรักษาความปลอดภัย และการปรับปรุงโครงสร้างพื้นฐานแบ็กเอนด์ของเรา

ข้อมูลนี้จะถูกเก็บไว้โดยแยกจากข้อมูลประจำตัวที่จำเป็นสำหรับวัตถุประสงค์ในการออกใบอนุญาตและการเรียกเก็บเงิน เนื่องจากไม่จำเป็นต้องระบุตัวตนของผู้ใช้ปลายทาง โดยมีระยะเวลาการเก็บรักษาไม่เกิน 4 ปี

ระบบตรวจสอบความเชื่อถือ ESET LiveGrid® แฮชแบบวันเวย์ที่เกี่ยวกับการแทรกซึมเพื่อวัตถุประสงค์ในการใช้งานระบบตรวจสอบความเชื่อถือ ESET LiveGrid® ซึ่งปรับปรุงประสิทธิภาพของโซลูชันการป้องกันมัลแวร์ของเราโดยการเปรียบเทียบไฟล์ที่สแกนกับฐานข้อมูลของรายการที่อยู่ใน Whitelist และ Blacklist ในคลาวด์ ผู้ใช้ปลายทางจะไม่ถูกระบุตัวตนในระหว่างกระบวนการนี้

ระบบคำติชม ESET LiveGrid® ตัวอย่างและเมตาดาต้าที่น่าสงสัยจากภายนอกที่เป็นส่วนหนึ่งของ ESET LiveGrid® Feedback System ซึ่งช่วยให้ ESET สามารถตอบสนองต่อความต้องการของผู้ใช้ปลายทางของเราได้ทันที และช่วยให้เราสามารถตอบสนองต่อภัยคุกคามล่าสุดได้ เราจำเป็นต้องพึ่งพาข้อมูลที่คุณส่งให้เรา

- การแทรกซึมต่างๆ เช่น ตัวอย่างของไวรัสและโปรแกรมที่เป็นอันตรายอื่นๆ และที่น่าสงสัย ปัญหา วัตถุที่อาจไม่เป็นที่ต้องการหรืออาจไม่ปลอดภัย เช่น ไฟล์ที่สามารถเปิดใช้งานได้ ข้อความอีเมลที่คุณเป็นผู้รายงานว่าเป็นสแปมหรือที่ผลิตภัณฑ์ของเราปักธงเตือน
- ข้อมูลที่เกี่ยวกับการใช้อินเทอร์เน็ต เช่น ที่อยู่ IP และข้อมูลเกี่ยวกับภูมิศาสตร์, แพ็คเกจ IP, URL และเฟรมอีเธอร์เน็ต
- ไฟล์แครชดัมป์และข้อมูลต่างๆ ที่มีอยู่

ไม่ไม่ได้ประสงค์ที่จะรวบรวมข้อมูลของคุณนอกเหนือจากขอบเขตที่ระบุนี้ แต่ในบางเวลาเราก็ไม่สามารถที่จะป้องกันได้ ข้อมูลที่เก็บรวบรวมโดยไม่ได้ตั้งใจอาจรวมอยู่ในตัวของมัลแวร์เอง (เก็บรวบรวมโดยไม่ได้แจ้งให้คุณทราบหรือคุณไม่ได้อนุมัติ) หรือที่ถูกเก็บรวบรวมโดยเป็นส่วนหนึ่งของชื่อไฟล์หรือ URL และเรามิได้ต้องการข้อมูลเหล่านั้นมาเป็นส่วนหนึ่งของระบบของเราหรือประมวลผลข้อมูลเหล่านั้นตามวัตถุประสงค์ที่แจ้งไว้ในนโยบายความเป็นส่วนตัวนี้

ข้อมูลทั้งหมดที่ได้รับและประมวลผลผ่านระบบคำติชม ESET LiveGrid® จะถูกนำมาใช้โดยไม่มีการระบุตัวตนของผู้ใช้ปลายทาง

การประเมินความปลอดภัยของอุปกรณ์ที่เชื่อมต่อกับเครือข่าย เพื่อมอบฟังก์ชันในการประเมินความปลอดภัย เราจะประมวลผลชื่อของเครือข่ายภายในระบบและข้อมูลเกี่ยวกับอุปกรณ์ในเครือข่ายภายในระบบ เช่น การมีอยู่, ประเภท, ชื่อ, ที่อยู่ IP และที่อยู่ MAC ของอุปกรณ์ในเครือข่ายภายในระบบที่เชื่อมต่อโดยมีข้อมูลใบอนุญาต ข้อมูลดังกล่าวยังรวมถึงประเภทความปลอดภัยไร้สายและประเภทการเข้ารหัสไร้สายของอุปกรณ์เราเตอร์ด้วย ข้อมูลใบอนุญาตที่ระบุตัวตนของผู้ใช้ปลายทางจะไม่ระบุตัวตนภายใน 12 เดือนหลังจากใบอนุญาตหมดอายุ

การสนับสนุนด้านเทคนิค ข้อมูลติดต่อ ข้อมูลการอนุญาต และข้อมูลที่อยู่ในคำขอการสนับสนุนของคุณอาจจำเป็นสำหรับการให้บริการสนับสนุน โดยขึ้นอยู่กับช่องทางที่คุณเลือกในการติดต่อเรา เราอาจเก็บรวบรวมข้อมูลที่อยู่อีเมล หมายเลขโทรศัพท์ ข้อมูลใบอนุญาต รายละเอียดผลิตภัณฑ์ และคำอธิบายของกรณีการสนับสนุนของคุณ คุณอาจถูกขอให้ระบุข้อมูลอื่นๆ เพื่อให้บริการสนับสนุนรวดเร็วมากยิ่งขึ้น ข้อมูลที่ใช้ประมวลผลสำหรับการสนับสนุนด้านเทคนิคจะถูกเก็บไว้เป็นเวลา 4 ปี

การป้องกันการใช้ข้อมูลในทางที่ผิด หากมีการสร้างบัญชี ESET HOME ใน https://home.eset.com และเปิดใช้งานฟังก์ชันโดยผู้ใช้ปลายทางซึ่งเกี่ยวข้องกับการโจรกรรมคอมพิวเตอร์ จะมีการรวบรวมและประมวลผลข้อมูลดังต่อไปนี้: ข้อมูลเกี่ยวกับตำแหน่งที่ตั้ง ภาพหน้าจอ ข้อมูลเกี่ยวกับการกำหนดค่าคอมพิวเตอร์ และข้อมูลที่บันทึกโดยกล้องของคอมพิวเตอร์ ข้อมูลที่ถูกเก็บรวบรวมจะจัดเก็บไว้ในเซิร์ฟเวอร์ของเราหรือในเซิร์ฟเวอร์ของผู้ให้บริการของเราโดยมีระยะเวลาการเก็บรักษาเป็นเวลา 3 เดือน

Password Manager. หากคุณเลือกเปิดใช้งานฟังก์ชันของ Password Manager ข้อมูลที่เกี่ยวข้องกับรายละเอียดการเข้าสู่ระบบของคุณจะถูกจัดเก็บในรูปแบบที่เข้ารหัสเฉพาะในคอมพิวเตอร์ของคุณหรืออุปกรณ์ที่กำหนดเท่านั้น หากคุณเปิดใช้งานบริการซิงโครไนซ์ ข้อมูลที่เข้ารหัสจะถูกจัดเก็บในเซิร์ฟเวอร์ของเราหรือในเซิร์ฟเวอร์ของผู้ให้บริการของเราเพื่อรับประกันบริการดังกล่าว ทั้ง ESET และผู้ให้บริการจะไม่สามารถเข้าถึงข้อมูลที่เข้ารหัสได้ มีเพียงคุณเท่านั้นที่มีกุญแจในการไขรหัสข้อมูลนั้น ข้อมูลจะถูกลบออกเมื่อปิดใช้งานฟังก์ชัน

ESET LiveGuard. หากคุณเลือกเปิดใช้งานฟังก์ชัน ESET LiveGuard จะต้องส่งตัวอย่าง เช่น ไฟล์ที่กำหนดไว้ล่วงหน้าและเลือกโดยผู้ใช้ปลายทาง ตัวอย่างที่คุณเลือกสำหรับการวิเคราะห์ระยะไกลจะอัพโหลดไปยังบริการ ESET และผลการวิเคราะห์จะถูกส่งกลับไปยังคอมพิวเตอร์ของคุณ ตัวอย่างที่น่าสงสัยใดๆ จะประมวลผลในลักษณะของข้อมูลที่เก็บรวบรวมโดยระบบคำติชม ESET LiveGrid®

โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า หากคุณเลือกที่จะเปิดใช้งาน โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า เราจะเก็บรวบรวมและใช้ข้อมูลทางไกลแบบไม่ระบุตัวตนที่เกี่ยวกับการใช้งานของ

ผลิตภัณฑ์ของเราที่อิงจากการยินยอมของคุณ

โปรดทราบว่าหากบุคคลที่ใช้ผลิตภัณฑ์และบริการของเราไม่ใช่ผู้ใช้ปลายทางที่ซื้อผลิตภัณฑ์หรือบริการและได้เข้าร่วม EULA กับเรา (เช่น พนักงานของผู้ใช้ปลายทาง สมาชิกในครอบครัว หรือบุคคลที่ได้รับอนุญาตให้ใช้ผลิตภัณฑ์หรือบริการโดยผู้ใช้ปลายทางตาม EULA การประมวลผลข้อมูลจะดำเนินการตามผลประโยชน์ที่ชอบด้วยกฎหมายของ ESET ภายใต้นิยามของมาตรา 6 (1) f) GDPR เพื่อให้ผู้ใช้ที่ได้รับอนุญาตจากผู้ใช้ปลายทางสามารถใช้ผลิตภัณฑ์และบริการที่เราจัดหาให้ได้ตาม EULA

ข้อมูลติดต่อ

หากคุณประสงค์ที่จะใช้สิทธิ์ของคุณในฐานะที่เป็นเจ้าของข้อมูล หรือหากคุณมีข้อสงสัยหรือข้อกังวล โปรดส่งข้อความมาที่:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk