ESET Cyber Security

คู่มือผู้ใช้

คลิกที่นี่เพื่อแสดงเวอร์ชันออนไลน์ของเอกสารนี้

Digital Security
Progress. Protected.

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

สำหรับข้อมูลเพิ่มเติม โปรดไปที่ https://www.eset.com

ฝ่ายสนับสนุนด้านเทคนิค: https://support.eset.com

REV. 12/4/2024

ESET Cyber Security

ESET Cyber Security เป็นวิธีการใหม่ในการรักษาความปลอดภัยคอมพิวเตอร์แบบผสานรวมอย่างแท้จริง เวอร์ชันล่าสุดของกลไกการสแกนของ ThreatSense® ใช้ความรวดเร็วและความแม่นยำเพื่อช่วยรักษาคอมพิวเตอร์ของคุณให้ปลอดภัย ผลลัพธ์คือระบบอัจฉริยะที่จะแจ้งเตือนอยู่เสมอเกี่ยวกับการคุ้มครองคอมพิวเตอร์ของคุณจากการโจมตีและซอฟต์แวร์ที่เป็นอันตราย

ESET Cyber Security คือโซลูชันรักษาความปลอดภัยที่สมบูรณ์แบบ ซึ่งสร้างขึ้นจากการทำงานที่ยาวนานเพื่อรวมการป้องกันสูงสุดกับการใช้ทรัพยากรของระบบน้อยที่สุด เทคโนโลยีขั้นสูงที่ใช้ระบบอัจฉริยะที่มี ESET Cyber Security สามารถกำจัดการแฝงตัวของไวรัส เวิร์ม ม้าโทรจัน สปายแวร์ แอดแวร์ รูทคิต และการโจมตีจากอินเทอร์เน็ตในรูปแบบอื่นๆ ได้ในเชิงรุก โดยไม่ขัดขวางการทำงานของระบบ

มีอะไรใหม่ในเวอร์ชัน 6

ESET Cyber Security เวอร์ชัน 6 แนะนำการอัพเดทและการปรับปรุงต่อไปนี้:

- **การรองรับสถาปัตยกรรมแบบ 64 บิต**
- **การป้องกันฟิชชิ่ง** – ป้องกันเว็บไซต์หลอกลวงที่ปลอมแปลงเป็นเว็บไซต์ที่น่าเชื่อถือจากการล้วงข้อมูลส่วนบุคคลของคุณ
- **การอัพเดทระบบ** – ESET Cyber Security เวอร์ชัน 6 มาพร้อมกับการแก้ไขจุดบกพร่องและการปรับปรุงที่หลากหลาย ซึ่งรวมถึงการแจ้งเตือนสำหรับการอัพเดทระบบปฏิบัติการ ในการเรียนรู้เพิ่มเติมเกี่ยวกับสิ่งนี้ ให้ดูที่ส่วน การอัพเดทระบบ
- **สถานะการป้องกัน** – ซ่อนการแจ้งเตือนจากหน้าจอสถานะการป้องกัน (เช่น การป้องกันอีเมลถูกปิดใช้งาน หรือ ต้องเริ่มต้นระบบคอมพิวเตอร์ใหม่)
- **สื่อที่จะสแกน** – คุณสามารถยกเว้นสื่อบางประเภทจากเครื่องมือสแกนแบบเรียลไทม์ได้ (ไดรฟ์ในเครื่อง สื่อที่ถอดเข้าออกได้ สื่อเครือข่าย)
- **การเชื่อมต่อเครือข่าย** - แสดงการเชื่อมต่อเครือข่ายบนคอมพิวเตอร์ของคุณ และช่วยให้คุณสร้างกฎสำหรับการเชื่อมต่อเหล่านี้ได้

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับคุณลักษณะใหม่ใน ESET Cyber Security โปรดอ่าน บทความฐานความรู้ของ ESET ต่อไปนี้

ความต้องการของระบบ

เพื่อให้ ESET Cyber Security มีประสิทธิภาพสูงสุด ระบบของคุณควรตรงตามข้อกำหนดด้านฮาร์ดแวร์และซอฟต์แวร์ต่อไปนี้:

	ความต้องการของระบบ:
สถาปัตยกรรมของตัวประมวลผล	Intel 64-bit, M1, M2
ระบบปฏิบัติการ	macOS 10.12 และใหม่กว่า
หน่วยความจำ	300 MB
พื้นที่ว่างในดิสก์	200 MB

นอกเหนือจากการรองรับ Intel ที่มีอยู่ ESET Cyber Security เวอร์ชัน 6.10.900.0 และรุ่นที่ใหม่กว่าจะรองรับชิป Apple M1 และ M2 ที่ใช้ Rosetta 2 ด้วย

การติดตั้ง

ก่อนที่คุณจะเริ่มต้นกระบวนการติดตั้ง โปรดปิดโปรแกรมที่เปิดไว้ทั้งหมดในคอมพิวเตอร์ ESET Cyber Security มีองค์ประกอบที่อาจขัดแย้งกับโปรแกรมป้องกันไวรัสอื่นๆ ที่อาจมีการติดตั้งไว้ในคอมพิวเตอร์ของคุณแล้ว ESET ขอแนะนำให้คุณลบโปรแกรมป้องกันไวรัสอื่น ๆ ออกเพื่อป้องกันปัญหาที่อาจเกิดขึ้น

ในการเปิดทำงานตัวช่วยเหลือการติดตั้ง ให้ปฏิบัติตามวิธีใดวิธีหนึ่งต่อไปนี้:

- หากคุณติดตั้งจากไฟล์ที่ดาวน์โหลดจากเว็บไซต์ ESET ให้เปิดไฟล์แล้วคลิกสองครั้งที่ไอคอน **ติดตั้ง**
- หากคุณติดตั้งจากซีดี/ดีวีดีสำหรับติดตั้ง ให้ใส่ซีดี/ดีวีดีลงในคอมพิวเตอร์ของคุณ แล้วเปิดจากเดสก์ท็อปของคุณหรือหน้าต่าง **Finder** แล้วคลิกสองครั้งที่ไอคอน **ติดตั้ง**

ตัวช่วยเหลือการติดตั้งจะแนะนำคุณผ่านการตั้งค่าพื้นฐาน ในระหว่างช่วงเริ่มต้นของการติดตั้ง ตัวติดตั้งจะตรวจสอบสำหรับเวอร์ชั่นล่าสุดของผลิตภัณฑ์ผ่านทางออนไลน์โดยอัตโนมัติ หากพบเวอร์ชั่นใหม่ คุณจะได้รับตัวเลือกในการดาวน์โหลดเวอร์ชั่นล่าสุดก่อนดำเนินการกระบวนการติดตั้งต่อ

หลังจากยอมรับข้อตกลงใบอนุญาตของผู้ใช้ คุณจะถูกถามให้เลือกหนึ่งในโหมดการติดตั้งต่อไปนี้:

- การติดตั้งปกติ
- การติดตั้งแบบกำหนดเอง

การติดตั้งปกติ

โหมดการติดตั้งปกติจะมีตัวเลือกการกำหนดค่าที่เหมาะสมสำหรับผู้ใช้งานส่วนใหญ่ การตั้งค่าเหล่านี้จะมีการรักษาความปลอดภัยสูงสุดรวมกับประสิทธิภาพการทำงานของระบบที่ยอดเยี่ยม การติดตั้งปกติเป็นตัวเลือกเริ่มต้นและแนะนำให้ใช้หากคุณไม่มีความต้องการเป็นพิเศษสำหรับการตั้งค่าแบบเจาะจง

1.ในหน้าต่าง **ESET LiveGrid** ให้เลือกตัวเลือกที่คุณต้องการแล้วคลิก **ดำเนินการต่อ** หากคุณตัดสินใจว่าต้องการเปลี่ยนการตั้งค่านี้ในภายหลัง คุณจะสามารถดำเนินการได้โดยใช้ **การตั้งค่า LiveGrid** ได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ESET Live Grid โปรดเยี่ยมชมประมวลศัพท์ของเรา

2.ในหน้าต่าง **แอพพลิเคชันที่อาจไม่พึงประสงค์** ให้เลือกตัวเลือกที่คุณต้องการ (ดู แอพพลิเคชันที่อาจไม่พึงประสงค์คืออะไร) แล้วคลิก **ดำเนินการต่อ** หากคุณตัดสินใจว่าต้องการเปลี่ยนการตั้งค่านี้ในภายหลัง โปรดใช้ **การตั้งค่าขั้นสูง**

3.คลิก **ติดตั้ง** หากระบบขอให้คุณป้อนรหัสผ่าน macOS ให้ป้อนรหัสดังกล่าวแล้วคลิก **ติดตั้งซอฟต์แวร์**

หลังจากติดตั้ง ESET Cyber Security แล้ว:

macOS Big Sur (11)

1.อนุญาตส่วนขยายระบบ

2.อนุญาตการเข้าถึงทั้งดิสก์

3.อนุญาต ESET ไปยังเพิ่มการกำหนดค่าพร็อกซี่ แล้วคุณจะได้รับการแจ้งเตือนต่อไปนี้: "ESET Cyber Security" **ต้องการที่จะเพิ่มการกำหนดค่าพร็อกซี่** เมื่อคุณได้รับการแจ้งเตือนนี้ ให้คลิก **อนุญาต** หากคุณคลิก **ไม่อนุญาต** การป้องกันการเข้าถึงเว็บไซต์จะไม่ทำงาน

macOS 10.15 และเก่ากว่า

1.บน macOS 10.13 ขึ้นไป คุณจะได้รับการแจ้งเตือน **การปิดกั้นส่วนขยายระบบ** จากระบบของคุณและการแจ้งเตือน **คอมพิวเตอร์ของคุณไม่ได้รับการป้องกัน** จาก ESET Cyber Security หากต้องการเข้าถึงฟังก์ชัน ESET Cyber Security ทั้งหมด คุณต้องอนุญาตส่วนขยายเคอร์เนลบนอุปกรณ์ของคุณ ในการอนุญาตส่วนขยายเคอร์เนลบนอุปกรณ์ของคุณ ให้ไปที่ **การตั้งค่าระบบ** > **ความปลอดภัยและความเป็นส่วนตัว** แล้วคลิก **อนุญาต** เพื่ออนุญาตซอฟต์แวร์ระบบจากนักพัฒนา **ESET, spol. s.r.o.** สำหรับข้อมูลอย่างละเอียดเพิ่มเติม โปรดไปที่ บทความฐานความรู้ของเรา

2.บน macOS 10.14 และใหม่กว่า คุณจะได้รับการแจ้งเตือน**คอมพิวเตอร์ของคุณได้รับการป้องกันบางส่วน** จาก ESET Cyber Security หากต้องการเข้าถึงฟังก์ชัน ESET Cyber Security ทั้งหมด คุณต้องให้การอนุญาต **เข้าถึงดิสก์เต็มรูปแบบ** แก่ ESET Cyber Security คลิก **เปิดการตั้งค่าระบบ** > **ความปลอดภัยและความเป็นส่วนตัว** ไปที่แท็บ **ความเป็นส่วนตัว** แล้วเลือกตัวเลือก **เข้าถึงดิสก์เต็มรูปแบบ** คลิกไอคอนแม่กุญแจเพื่อเปิดใช้งานการแก้ไข คลิกไอคอนบวก แล้วเลือกแอพพลิเคชันESET Cyber Security คอมพิวเตอร์ของคุณจะแสดงการแจ้งเตือนเพื่อรีสตาร์ทคอมพิวเตอร์ ให้คลิก **ภายหลัง** อย่ารีสตาร์ทคอมพิวเตอร์ในตอนนี้ ให้คลิก **เริ่มต้นอีกครั้ง** ในหน้าต่างการแจ้งเตือน ESET Cyber Security หรือรีสตาร์ทคอมพิวเตอร์ของคุณ สำหรับข้อมูลอย่างละเอียดเพิ่มเติม ให้ไปที่ บทความฐานความรู้

หลังจากติดตั้ง ESET Cyber Security คุณควรดำเนินการสแกนคอมพิวเตอร์เพื่อหารหัสที่เป็นอันตราย จากหน้าต่างหลักของโปรแกรม ให้คลิก **การสแกนคอมพิวเตอร์** > **การสแกนแบบสมาร์ท** สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการสแกนคอมพิวเตอร์ตามต้องการ ให้ดูที่ส่วน การสแกนคอมพิวเตอร์ตามต้องการ

การติดตั้งแบบกำหนดเอง

โหมดการติดตั้งแบบกำหนดเองได้รับการออกแบบมาเพื่อผู้ใช้ที่มีประสบการณ์ ซึ่งต้องการแก้ไขการตั้งค่าขั้นสูงในระหว่างกระบวนการติดตั้ง

- **พร็อกซีเซิร์ฟเวอร์**

หากคุณใช้พร็อกซีเซิร์ฟเวอร์ ให้กำหนดพารามิเตอร์โดยเลือก **ฉันใช้พร็อกซีเซิร์ฟเวอร์** ในหน้าต่างถัดไป ให้ป้อนที่อยู่ IP หรือ URL ของพร็อกซีเซิร์ฟเวอร์ของคุณในช่อง**ที่อยู่** ในฟิลด์ **พอร์ต** ให้ระบุพอร์ตที่พร็อกซีเซิร์ฟเวอร์ยอมรับการเชื่อมต่อ (3128 ตามค่าเริ่มต้น) ในกรณีที่พร็อกซีเซิร์ฟเวอร์ต้องการการตรวจสอบสิทธิ์ ให้ป้อน**ชื่อผู้ใช้**และ**รหัสผ่าน**ที่ถูกต้อง เพื่อให้สิทธิ์ในการเข้าถึงพร็อกซีเซิร์ฟเวอร์ หากคุณไม่ใช้พร็อกซีเซิร์ฟเวอร์ ให้เลือก **ฉันไม่ใช้พร็อกซีเซิร์ฟเวอร์** หากคุณไม่แน่ใจว่าคุณใช้พร็อกซีเซิร์ฟเวอร์อยู่หรือไม่ ให้เลือก **ใช้การตั้งค่าระบบ (แนะนำ)** เพื่อใช้การตั้งค่าระบบปัจจุบันของคุณ

- **สิทธิ์**

คุณจะมีตัวเลือกในการกำหนดผู้ใช้หรือกลุ่มที่มีสิทธิ์ที่จะสามารถแก้ไขการกำหนดค่าโปรแกรมได้ จากรายการผู้ใช้ที่ด้านซ้าย ให้เลือกผู้ใช้และ **เพิ่ม** ผู้ใช้ไปยังรายการ **ผู้ใช้ที่มีสิทธิ์** ในการแสดงผู้ใช้ระบบทั้งหมด ให้เลือก **แสดงผู้ใช้ทั้งหมด** ถ้าคุณปล่อยให้รายการผู้ใช้ที่มีสิทธิ์ว่างไว้ ระบบจะถือว่าผู้ใช้ทั้งหมดคือผู้ใช้ที่มีสิทธิ์

- **ESET LiveGrid®**

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ESET Live Grid โปรดเยี่ยมชมประมวลศัพท์ของเรา

- **แอพพลิเคชันที่อาจไม่พึงประสงค์**

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับแอพพลิเคชันที่อาจไม่พึงประสงค์ โปรดเยี่ยมชมประมวลศัพท์ของเรา

หลังจากติดตั้ง ESET Cyber Security แล้ว:

macOS Big Sur (11)

1. อนุญาตส่วนขยายระบบ
2. อนุญาตการเข้าถึงทั้งดิสก์
3. อนุญาต ESET ไปยังเพิ่มการกำหนดค่าพร็อกซี่ แล้วคุณจะได้รับการแจ้งเตือนต่อไปนี้: "ESET Cyber Security'' **ต้องการที่จะเพิ่มการกำหนดค่าพร็อกซี่** เมื่อคุณได้รับการแจ้งเตือนนี้ ให้คลิก **อนุญาต** หากคุณคลิก **ไม่อนุญาต** การป้องกันการเข้าถึงเว็บไซต์จะไม่ทำงาน

macOS 10.15 และเก่ากว่า

1.บน macOS 10.13 ขึ้นไป คุณจะได้รับการแจ้งเตือน **การปิดกั้นส่วนขยายระบบ** จากระบบของคุณและการแจ้งเตือน **คอมพิวเตอร์ของคุณไม่ได้รับการป้องกัน** จาก ESET Cyber Security หากต้องการเข้าถึงฟังก์ชัน ESET Cyber Security ทั้งหมด คุณต้องอนุญาตส่วนขยายเคอร์เนลบนอุปกรณ์ของคุณ ในการอนุญาตส่วนขยายเคอร์เนลบนอุปกรณ์ของคุณ ให้ไปที่ **การตั้งค่าระบบ** > **ความปลอดภัยและความเป็นส่วนตัว** แล้วคลิก **อนุญาต** เพื่ออนุญาตซอฟต์แวร์ระบบจากนักพัฒนา **ESET, spol. s.r.o.** สำหรับข้อมูลอย่างละเอียดเพิ่มเติม โปรดไปที่ บทความฐานความรู้ของเรา

2.บน macOS 10.14 และใหม่กว่า คุณจะได้รับการแจ้งเตือน**คอมพิวเตอร์ของคุณได้รับการป้องกันบางส่วน** จาก ESET Cyber Security หากต้องการเข้าถึงฟังก์ชัน ESET Cyber Security ทั้งหมด คุณต้องให้การอนุญาต **เข้าถึงดิสก์เต็มรูปแบบ** แก่ ESET Cyber Security คลิก **เปิดการตั้งค่าระบบ** > **ความปลอดภัยและความเป็นส่วนตัว** ไปที่แท็บ **ความเป็นส่วนตัว** แล้วเลือกตัวเลือก **เข้าถึงดิสก์เต็มรูปแบบ** คลิกไอคอนแม่กุญแจเพื่อเปิดใช้งานการแก้ไข คลิกไอคอนบวก แล้วเลือกแอพพลิเคชันESET Cyber Security คอมพิวเตอร์ของคุณจะแสดงการแจ้งเตือนเพื่อรีสตาร์ทคอมพิวเตอร์ ให้คลิก **ภายหลัง** อย่ารีสตาร์ทคอมพิวเตอร์ในตอนนี้ ให้คลิก **เริ่มต้นอีกครั้ง** ในหน้าต่างการแจ้งเตือน ESET Cyber Security หรือรีสตาร์ทคอมพิวเตอร์ของคุณ สำหรับข้อมูลอย่างละเอียดเพิ่มเติม ให้ไปที่ บทความฐานความรู้

หลังจากติดตั้ง ESET Cyber Security คุณควรดำเนินการสแกนคอมพิวเตอร์เพื่อหารหัสที่เป็นอันตราย จากหน้าต่างหลักของโปรแกรม ให้คลิก **การสแกนคอมพิวเตอร์** > **การสแกนแบบสมาร์ท** สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการสแกนคอมพิวเตอร์ตามต้องการ ให้ดูที่ส่วน การสแกนคอมพิวเตอร์ตามต้องการ

อนุญาตส่วนขยายระบบ

ใน macOS 11 (Big Sur) ส่วนขยายเคอร์เนลจะถูกแทนที่ด้วยส่วนขยายระบบ ซึ่งจำเป็นต้องได้รับการอนุญาตจากผู้ใช้ก่อนที่จะทำการโหลดส่วนขยายระบบของบริษัทอื่น

หลังการติดตั้ง ESET Cyber Security บน macOS Big Sur (11) ขึ้นไป คุณจะได้รับการแจ้งเตือนส่วนขยายระบบถูกปิดกั้นจากระบบของคุณและการแจ้งเตือน คอมพิวเตอร์ของคุณไม่ได้รับการป้องกันจาก ESET Cyber Security หากต้องการเข้าถึงฟังก์ชัน ESET Cyber Security ทั้งหมด คุณต้องอนุญาตส่วนขยายระบบบนอุปกรณ์ของคุณ

อัพเกรดจาก macOS รุ่นก่อนหน้าเป็น Big Sur

หากคุณมี ESET Cyber Security ติดตั้งไว้อยู่แล้ว และคุณกำลังจะอัพเกรดเป็น macOS Big Sur คุณจะต้องอนุญาตส่วนขยายเคอร์เนล ESET ด้วยตัวเองหลังจากที่ทำการอัพเกรดแล้ว โดยจำเป็นต้องใช้การเข้าถึงเครื่องไคลเอ็นต์แบบจริง ซึ่งในระหว่างการเข้าถึงจากระยะไกล ปุ่มอนุญาตจะถูกปิดใช้งาน

หากคุณมีผลิตภัณฑ์ ESET ติดตั้งไว้อยู่แล้วบน macOS Big Sur ขึ้นไป คุณจะต้องอนุญาตส่วนขยายระบบ ESET ด้วยตัวเอง โดยจำเป็นต้องใช้การเข้าถึงเครื่องไคลเอ็นต์แบบจริง ซึ่งในระหว่างการเข้าถึงจากระยะไกล ตัวเลือกนี้จะถูกปิดใช้งาน

อนุญาตส่วนขยายระบบด้วยตัวเอง

1.คลิก **เปิดการตั้งค่าระบบ** หรือ **เปิดการตั้งค่าความปลอดภัย** ในหน้าต่างข้อความการเตือน

2.คลิกไอคอนล็อคที่ส่วนล่างซ้ายเพื่อเปลี่ยนหน้าต่างการตั้งค่า

3.ใช้ Touch ID หรือคลิก **ใช้รหัสผ่าน** แล้วพิมพ์ชื่อผู้ใช้และรหัสผ่านของคุณ จากนั้นคลิก **ปลดล็อค**

4.คลิก **รายละเอียด**

5.เลือกตัวเลือก ESET Cyber Security**.app** ทั้งสองตัวเลือก

6.คลิก**ตกลง**

สำหรับคู่มือแบบละเอียดทีละขั้นตอน โปรดเยี่ยมชม บทความฐานความรู้ของเรา (บทความฐานความรู้ไม่มีให้บริการในทุกภาษา)

อนุญาตการเข้าถึงทั้งดิสก์

บน macOS 10.14 คุณจะได้รับการแจ้งเตือน **คอมพิวเตอร์ของคุณได้รับการป้องกันบางส่วน** จาก ESET Cyber Security หากต้องการเข้าถึงฟังก์ชัน ESET Cyber Security ทั้งหมด คุณจำเป็นต้องอนุญาต **การเข้าถึงดิสก์แบบเต็ม** แก่ ESET Cyber Security

1.คลิก **เปิดการตั้งค่าระบบ** ในหน้าต่างข้อความ

2.คลิกไอคอนล็อคที่ส่วนล่างซ้ายเพื่อเปลี่ยนหน้าต่างการตั้งค่า

3.ใช้ Touch ID หรือคลิก **ใช้รหัสผ่าน** แล้วพิมพ์ชื่อผู้ใช้และรหัสผ่านของคุณ จากนั้นคลิก **ปลดล็อค**

4.เลือก ESET Cyber Security**.app** จากรายการ

5.การแจ้งเตือนรีสตาร์ท ESET Cyber Security จะแสดงขึ้น คลิกภายหลัง

6.เลือก **การป้องกันระบบไฟล์แบบเรียลไทม์ของ ESET** จากรายการ

ไม่มีการป้องกันระบบไฟล์แบบเรียลไทม์ของ ESET
หากไม่มีตัวเลือก **การป้องกันระบบไฟล์แบบเรียลไทม์** ในรายการ คุณจำเป็นต้อง อนุญาตส่วนขยายระบบสำหรับผลิตภัณฑ์ ESET

7.คลิกเริ่มต้นอีกครั้งในหน้าต่างข้อความการเตือนของ ESET Cyber Security หรือรีสตาร์ทคอมพิวเตอร์ของคุณ สำหรับข้อมูลเพิ่มเติมแบบละเอียด โปรดเยี่ยมชม บทความฐานความรู้ ของเรา

การเปิดใช้งานผลิตภัณฑ์

หลังจากการติดตั้ง หน้าต่างการเปิดใช้งานผลิตภัณฑ์จะปรากฏขึ้นโดยอัตโนมัติ หากต้องการเข้าถึงหน้าต่างโต้ตอบการเปิดใช้งานผลิตภัณฑ์เมื่อใดก็ตาม ให้คลิกไอคอน ESET Cyber Security ที่อยู่ในแถบเมนู macOS (ด้านบนสุดของหน้าจอ) แล้วคลิก **การเปิดใช้งานผลิตภัณฑ์...**

• **รหัสใบอนุญาต** – สตริงที่ไม่ซ้ำกันในรูปแบบ XXXX-XXXX-XXXX-XXXX-XXXX หรือ XXXX-XXXXXXXX ที่ใช้เพื่อระบุเจ้าของใบอนุญาตและเพื่อเปิดใช้งานใบอนุญาต หากคุณซื้อผลิตภัณฑ์เวอร์ชันขายปลีกในบรรจุภัณฑ์แบบกล่อง ให้เปิดใช้งานผลิตภัณฑ์ของคุณโดยใช้รหัสใบอนุญาต รหัสการเปิดใช้งานมักจะอยู่ด้านในหรือบนด้านหลังบรรจุภัณฑ์ของผลิตภัณฑ์

• **ชื่อผู้ใช้และรหัสผ่าน** – หากคุณมีชื่อผู้ใช้และรหัสผ่าน แต่ไม่ทราบวิธีการเปิดใช้งาน ESET Cyber Security ให้คลิก **ฉันมีชื่อผู้ใช้และรหัสผ่าน ฉันควรทำอย่างไร** ระบบจะนำคุณไปที่ my.eset.com ซึ่งคุณสามารถแปลงข้อมูลประจำตัวของคุณเป็นรหัสใบอนุญาตได้

• **ใบอนุญาตเวอร์ชันทดลองใช้ฟรี** - เลือกตัวเลือกนี้หากคุณต้องการประเมิน ESET Cyber Security ก่อนซื้อ ป้อนที่อยู่อีเมลและประเทศของคุณเพื่อเปิดใช้งาน ESET Cyber Security ในระยะเวลาที่จำกัด ใบอนุญาตทดสอบของคุณจะถูกส่งอีเมลไปถึงคุณ ใบอนุญาตทดสอบจะสามารถเปิดใช้งานได้หนึ่งครั้งต่อลูกค้าหนึ่งรายเท่านั้น

• **ซื้อใบอนุญาต** – หากคุณไม่มีใบอนุญาตและต้องการซื้อ ให้คลิก ซื้อใบอนุญาต การดำเนินการนี้จะเปลี่ยนเส้นทางคุณไปยังเว็บไซต์ของตัวแทนจำหน่าย ESET ในพื้นที่ของคุณ

• **เปิดใช้งานในภายหลัง** – คลิกตัวเลือกนี้หากคุณไม่ต้องการเปิดใช้งานในขณะนี้

การลบการติดตั้ง

หากต้องการลบการติดตั้ง ESET Cyber Security ให้ดำเนินการอย่างใดอย่างหนึ่งต่อไปนี้:

• ใส่ซีดี/ดีวีดีการติดตั้ง ESET Cyber Security ลงในคอมพิวเตอร์ของคุณ เปิดแผ่นจากเดสก์ท็อปหรือหน้าต่าง **Finder** แล้วดับเบิลคลิก **ลบการติดตั้ง**

• เปิดไฟล์การติดตั้งของ ESET Cyber Security (*.dmg*) แล้วดับเบิลคลิก **ลบการติดตั้ง**

• เริ่มต้น **Finder** โดยเปิดโฟลเดอร์ **แอพพลิเคชัน** ในฮาร์ดไดรฟ์ของคุณ แล้วกด ctrl และคลิกที่ไอคอน **ESET Cyber Security** แล้วเลือก **แสดงเนื้อหาแพ็คเกจ** เปิด **Contents** > โฟลเดอร์ **Helpers** แล้วดับเบิลคลิกไอคอน **Uninstaller**

ภาพรวมพื้นฐาน

หน้าต่างหลักของโปรแกรม ESET Cyber Security จะถูกแบ่งออกเป็นสองส่วนหลัก หน้าต่างหลักที่ด้านขวาจะแสดงข้อมูลที่เกี่ยวข้องกับตัวเลือกที่เลือกจากเมนูหลักทางด้านซ้าย

ส่วนต่อไปนี้จะสามารถเข้าถึงได้จากเมนูหลัก:

• **หน้าแรก** – ให้ข้อมูลเกี่ยวกับสถานะของการป้องกันของคอมพิวเตอร์ การป้องกันเว็บและอีเมล

• **การสแกนคอมพิวเตอร์** – ส่วนนี้จะช่วยให้คุณสามารถกำหนดค่าและเริ่มต้น การสแกนคอมพิวเตอร์ตามต้องการ

• **อัพเดท** - แสดงข้อมูลเกี่ยวกับการอัพเดทของโมดูลการตรวจหา

• **ตั้งค่า** – เลือกส่วนนี้เพื่อปรับระดับการรักษาความปลอดภัยของคอมพิวเตอร์

• **เครื่องมือ** – ให้การเข้าถึง ไฟล์บันทึก เครื่องมือวางกำหนดการ การกักเก็บ กระบวนการที่ทำงานอยู่ และคุณลักษณะอื่นๆ ของโปรแกรม

• **วิธีใช้** – แสดงการเข้าถึงไฟล์วิธีใช้ ฐานความรู้ทางอินเทอร์เน็ต ฟอร์มคำขอการสนับสนุน และข้อมูลโปรแกรมเพิ่มเติม

แป้นพิมพ์ลัด

คีย์ลัดแป้นพิมพ์ที่สามารถใช้ได้เมื่อทำงานร่วมกับ ESET Cyber Security:

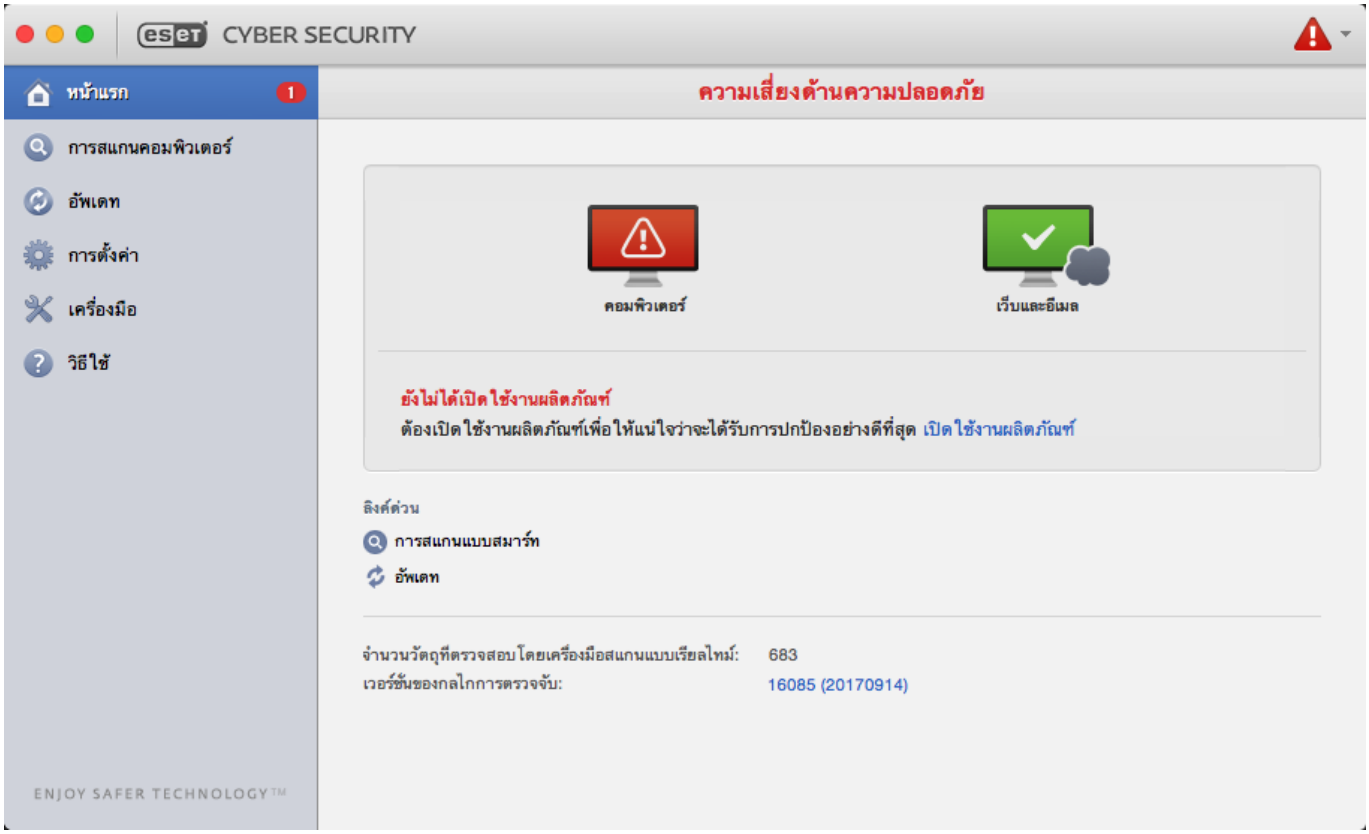
- cmd+, - แสดงการตั้งค่า ESET Cyber Security,
- cmd+O - ปรับขนาดหน้าต่าง GUI หลักของ ESET Cyber Security ให้เป็นขนาดเริ่มต้นแล้วเคลื่อนย้ายไปยังกึ่งกลางของหน้าจอ,
- cmd+Q - ซ่อนหน้าต่าง GUI หลักของ ESET Cyber Security คุณสามารถเปิดได้โดยคลิกไอคอน ESET Cyber Security ในแถบเมนูของ macOS (ด้านบนสุดของหน้าจอ),
- cmd+W - ปิดหน้าต่าง GUI หลักของ ESET Cyber Security

คีย์ลัดแป้นพิมพ์ต่อไปนี้จะทำงานเฉพาะหาก **ใช้เมนูมาตรฐาน** เปิดอยู่ใน **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** > **ส่วนติดต่อ**:

- cmd+alt+L - เปิดส่วน ไฟล์บันทึก,
- cmd+alt+S - เปิดส่วน เครื่องมือวางกำหนดการ,
- cmd+alt+Q - เปิดส่วน การกักเก็บ,

การตรวจสอบสถานะของการป้องกัน

หากต้องการดูสถานะการป้องกันของคุณ ให้คลิก **หน้าแรก** จากเมนูหลัก ข้อมูลสรุปของสถานะเกี่ยวกับการทำงานของโมดูล ESET Cyber Security จะปรากฏในหน้าต่างหลัก



ควรทำอย่างไรเมื่อโปรแกรมทำงานไม่ถูกต้อง

หากโมดูลทำงานอย่างถูกต้อง ไอคอนสีเขียวจะปรากฏขึ้น หากโมดูลทำงานไม่ถูกต้อง เครื่องหมายอัศเจรีย์สีแดงหรือไอคอนการแจ้งสีส้มจะปรากฏขึ้น ข้อมูลเพิ่มเติมเกี่ยวกับโมดูลและทางแก้ไขที่แนะนำสำหรับการแก้ไขปัญหาจะปรากฏขึ้น เมื่อต้องการเปลี่ยนสถานะของแต่ละโมดูล ให้คลิกลิงก์สีน้ำเงินด้านล่างข้อความการแจ้งเตือนแต่ละข้อความ

หากคุณไม่สามารถแก้ไขปัญหาโดยใช้การแก้ไขที่แนะนำได้ คุณสามารถค้นหาการแก้ไขได้ที่ ฐานความรู้ของ ESET หรือติดต่อ ฝ่ายดูแลลูกค้าของ ESET ฝ่ายดูแลลูกค้าจะตอบคำถามของคุณอย่างรวดเร็วและช่วยแก้ไขปัญหาใดๆ ด้วย ESET Cyber Security

การป้องกันคอมพิวเตอร์

สามารถดูการกำหนดค่าคอมพิวเตอร์ได้ใน **ตั้งค่า** > **คอมพิวเตอร์** การกำหนดค่าจะแสดงสถานะของ **การป้องกันระบบไฟล์แบบเรียลไทม์** และ **การปิดกั้นสื่อที่ถอดเข้าออกได้** หากต้องการปิดแต่ละโมดูล ให้เปลี่ยนปุ่มของโมดูลที่ต้องการเป็น **ปิดใช้งาน** โปรดทราบว่าการดำเนินการนี้อาจลดระดับการป้องกันคอมพิวเตอร์ของคุณ หากต้องการเข้าถึงการตั้งค่าโดยละเอียดสำหรับแต่ละโมดูล ให้คลิก **ตั้งค่า...**

การป้องกันไวรัสและสปายแวร์

การป้องกันไวรัสจะช่วยป้องกันการโจมตีจากระบบที่เป็นอันตรายโดยการแก้ไขไฟล์ที่อาจเป็นภัยคุกคาม หากตรวจพบภัยคุกคามที่มีรหัสที่เป็นอันตราย โมดูลป้องกันไวรัสสามารถกำจัดรหัสดังกล่าวด้วยการปิดกั้น จากนั้นจึงกำจัด ลบ หรือย้ายไปยังที่กักเก็บ

ทั่วไป

ในส่วน **ทั่วไป** (**การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน...** > **ทั่วไป**) คุณสามารถเปิดใช้งานการตรวจหาแอพพลิเคชันประเภทต่อไปนี้:

• **แอพพลิเคชันที่อาจไม่พึงประสงค์** - เกรย์แวร์หรือแอพพลิเคชันที่อาจไม่พึงประสงค์ (PUA) เป็นซอฟต์แวร์ประเภทกว้างๆ ที่ไม่ได้มีเจตนาที่เป็นอันตรายอย่างชัดแจ้งเมื่อเทียบกับมัลแวร์ประเภทอื่น เช่น ไวรัสหรือม้าโทรจัน อย่างไรก็ตาม ซอฟต์แวร์นี้อาจติดตั้งซอฟต์แวร์อื่นที่ไม่ต้องการเพิ่มเติม เปลี่ยนลักษณะการทำงานของอุปกรณ์ดิจิทัล หรือดำเนินการกิจกรรมที่ผู้ใช้ไม่อนุญาตหรือไม่คาดหมาย อ่านเพิ่มเติมเกี่ยวกับแอพพลิเคชันประเภทนี้ได้ใน ประมวลศัพท์

• **แอพพลิเคชันที่อาจไม่ปลอดภัย** - แอพพลิเคชันเหล่านี้คือซอฟต์แวร์เชิงพาณิชย์ที่ถูกต้อง ซึ่งอาจถูกนำไปใช้ในทางมิชอบโดยผู้โจมตี หากมีการติดตั้งโดยไม่ได้รับความยินยอมจากผู้ใช้ การจำแนกประเภทนี้จะรวมถึงโปรแกรมต่างๆ เช่น เครื่องมือการเข้าถึงระยะไกล ซึ่งสาเหตุนี้ทำให้มีการปิดใช้งานตัวเลือกนี้เป็นค่าเริ่มต้น

• **แอพพลิเคชันที่น่าสงสัย** - แอพพลิเคชันเหล่านี้จะรวมถึงโปรแกรมที่บีบอัดด้วยแพ็คเกอร์หรือตัวป้องกัน ตัวป้องกันประเภทเหล่านี้มักจะถูกใช้ประโยชน์โดยผู้เขียนมัลแวร์เพื่อหลบเลี่ยงการตรวจหา แพ็คเกอร์คือรันไทม์ที่ขยายในตัวและเรียกใช้ได้ที่รวมมัลแวร์หลายชนิดเป็นแพ็คเกจเดียว แพ็คเกอร์ที่พบได้บ่อยที่สุดคือ UPX, PE_Compact, PKLite และ ASPack มัลแวร์ที่เหมือนกันอาจถูกตรวจพบแตกต่างกันเมื่อถูกบีบอัดโดยใช้แพ็คเกอร์ที่ต่างกัน แพ็คเกอร์ยังมีความสามารถที่จะทำให้ "ลายเซ็น" ของตัวมันเปลี่ยนแปลงไปตามช่วงเวลา ทำให้ตรวจหาและลบมัลแวร์ได้ยากมากขึ้น

ในการตั้งค่า ข้อยกเว้นของระบบไฟล์หรือเว็บและจดหมาย คลิกปุ่ม **การตั้งค่า...**

การยกเว้น

ในส่วน **การยกเว้น** คุณสามารถยกเว้นไฟล์/โฟลเดอร์ แอพพลิเคชัน หรือที่อยู่แบบ IP/IPv6 บางรายการจากการสแกนได้

ไฟล์และโฟลเดอร์ที่อยู่ในรายการในแถบ **ระบบไฟล์** จะได้รับการยกเว้นจากการสแกน: เริ่มต้น เรียลไทม์ และเมื่อต้องการ (การสแกนคอมพิวเตอร์)

- **พาธ** – พาธไปยังไฟล์และโฟลเดอร์ที่ยกเว้น
- **ภัยคุกคาม** – หากมีชื่อของภัยคุกคามถัดจากไฟล์ที่ยกเว้น หมายความว่า ไฟล์ดังกล่าวจะถูกยกเว้นสำหรับภัยคุกคามที่กำหนดเท่านั้น แต่ไม่ใช่ทั้งหมด หากไฟล์นั้นติดไวรัสมัลแวร์อื่น ๆ ในภายหลัง ไฟล์ที่ถูกตรวจพบด้วยโมดูลการป้องกันไวรัส
- [+] – สร้างการยกเว้นใหม่ ป้อนพาธไปยังวัตถุ (คุณยังสามารถใช้สัญลักษณ์ * และ ?) หรือเลือกโฟลเดอร์หรือไฟล์จากลำดับโครงสร้าง
- [−] – ลบรายการที่เลือกออก
- **ค่าเริ่มต้น** – ยกเลิกการยกเว้นทั้งหมด

ในแถบ **เว็บและอีเมล** คุณสามารถยกเว้น **แอพพลิเคชัน** หรือ **ที่อยู่แบบ IP/IPv6** บางรายการจากการสแกนโปรโตคอลได้

การป้องกันเมื่อเริ่มต้นระบบ

การตรวจสอบไฟล์เมื่อเริ่มต้นระบบจะสแกนไฟล์เมื่อเริ่มต้นระบบโดยอัตโนมัติ โดยค่าเริ่มต้น การสแกนนี้จะทำงานอย่างสม่ำเสมอในฐานะที่เป็นงานตามกำหนดการหลังจากที่ผู้ใช้เข้าสู่ระบบหรือหลังจากการอัพเดทโมดูลการตรวจหาสำเร็จ ในการแก้ไขการตั้งค่าพารามิเตอร์กลไก ThreatSense ที่ใช้ได้กับการสแกนขณะเริ่มต้นระบบ ให้คลิกที่ปุ่ม **การตั้งค่า** คุณสามารถเรียนรู้เพิ่มเติมเกี่ยวกับการตั้งค่าโปรแกรม ThreatSense ได้โดยอ่านที่ ส่วนนี้

การป้องกันระบบไฟล์แบบเรียลไทม์

การป้องกันระบบไฟล์แบบเรียบไทม์จะตรวจสอบสื่อทุกประเภทและเริ่มการสแกนโดยขึ้นอยู่กับกิจกรรมต่าง ๆ ในการใช้เทคโนโลยี ThreatSense (ที่อธิบายอยู่ใน การตั้งค่าพารามิเตอร์กลไก ThreatSense) การป้องกันระบบไฟล์แบบเรียลไทม์อาจแตกต่างกันสำหรับไฟล์ที่เพิ่งสร้างใหม่และไฟล์ที่มีอยู่แล้ว ไฟล์ที่เพิ่งสร้างใหม่จะสามารถควบคุมได้แม่นยำมากกว่า

ตามค่าเริ่มต้น ไฟล์ทั้งหมดจะถูกสแกนเมื่อมีการ **เปิดไฟล์ สร้างไฟล์** หรือ **เรียกใช้ไฟล์** ขอแนะนำให้คุณคงการตั้งค่าเริ่มต้นเหล่านี้ไว้ เนื่องจากการตั้งค่าเหล่านี้จะให้การป้องกันแบบเรียลไทม์ในระดับสูงสุดสำหรับคอมพิวเตอร์ของคุณ การป้องกันแบบเรียลไทม์จะทำงานเมื่อเริ่มต้นระบบและทำการสแกนอย่างต่อเนื่องไม่ติดขัด ในกรณีพิเศษ (ตัวอย่างเช่น หากมีความขัดแย้งกับตัวสแกนแบบเรียลไทม์อีกเครื่อง) การปกป้องแบบเรียลไทม์สามารถถูกผิดลงได้โดยคลิกไอคอน ESET Cyber Security ◉ ที่อยู่ในแถบเมนูของคุณ (ด้านบนสุดของหน้าจอ) แล้วเลือก **ปิดใช้งานการปกป้องระบบไฟล์แบบเรียลไทม์** การป้องกันระบบไฟล์แบบเรียบไทม์ยังสามารถปิดใช้งานได้จากหน้าต่างโปรแกรมหลัก (คลิก **การตั้งค่า** > **คอมพิวเตอร์** แล้วสลับ **การป้องกันระบบไฟล์แบบเรียบไทม์** ให้เป็น **ปิดใช้งาน**)

ประเภทของสื่อต่อไปนี้สามารถยกเว้นจากเครื่องมือสแกนแบบ Real-time ได้:

- **ไดรฟ์ในเครื่อง** - ฮาร์ดไดรฟ์ของระบบ
- **สื่อที่ถอดเข้าออกได้** - ซีดี/ดีวีดี, สื่อ USB, อุปกรณ์ Bluetooth และอื่นๆ
- **เครือข่าย** - ไดรฟ์ที่แมปทั้งหมด

เราขอแนะนำให้คุณใช้การตั้งค่าเริ่มต้น และแก้ไขรายการยกเว้นการสแกนเฉพาะบางกรณีเท่านั้น เช่น เมื่อการสแกนสื่อบางชนิดทำให้การรับส่งข้อมูลช้าลงอย่างมาก

ในการแก้ไขการตั้งค่าขั้นสูงสำหรับการป้องกันระบบไฟล์แบบเรียบไทม์ ให้ไปที่ **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** (หรือกด *cmd+,*) > **การป้องกันแบบเรียลไทม์** และคลิก **การตั้งค่า...** ที่อยู่ข้าง **ตัวเลือกขั้นสูง** (ดังที่อธิบายไว้ใน ตัวเลือกการสแกนขั้นสูง)

ตัวเลือกขั้นสูง

ในหน้าต่างนี้คุณสามารถกำหนดประเภทของวัตถุที่ต้องการสแกนโดยกลไก ThreatSense ได้ ถ้าต้องการเรียนรู้เพิ่มเติมเกี่ยวกับ **อาร์ไคฟ์แบบคลายตัวเอง รันไทม์แพ็คเกอร์** และ**การวิเคราะห์พฤติกรรมขั้นสูง** โปรดดู การตั้งค่าพารามิเตอร์กลไก ThreatSense

เราไม่แนะนำให้ทำการเปลี่ยนแปลงในส่วน **การตั้งค่าอาร์ไคฟ์เริ่มต้น** ยกเว้นถ้าจำเป็นสำหรับการแก้ไขปัญหาเนื่องจากค่าการซ้อนของอาร์ไคฟ์ที่สูงขึ้นอาจทำให้ประสิทธิภาพการทำงานของระบบลดลง

พารามิเตอร์ ThreatSense เพิ่มเติมสำหรับไฟล์ที่เรียกใช้ - ตามค่าเริ่มต้น จะใช้ **การวิเคราะห์พฤติกรรมขั้นสูง** เมื่อเรียกใช้ไฟล์ เราขอแนะนำให้เปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ทและ ESET Live Grid ต่อไปเพื่อลดผลกระทบต่อประสิทธิภาพของระบบ

เพิ่มการทำงานร่วมกันของไดรฟ์ข้อมูลเครือข่าย - ตัวเลือกนี้จะเพิ่มประสิทธิภาพเมื่อเข้าถึงไฟล์บนเครือข่าย คุณควรเปิดใช้งานคุณสมบัตินี้ไว้ถ้าคุณพบว่าระบบช้าลงขณะเข้าถึงไดรฟ์เครือข่าย คุณสมบัตินี้ใช้ตัวเชื่อมต่อไฟล์ระบบบน macOS 10.10 ขึ้นไป โปรดทราบว่าไม่ใช่ทุกแอพพลิเคชันที่สนับสนุนตัวประสานงานไฟล์ ตัวอย่างเช่น Microsoft Word 2011 ไม่สนับสนุนตัวประสานงานไฟล์ ขณะที่ Word 2016 สนับสนุน เป็นต้น

เมื่อใดควรแก้ไขการกำหนดค่าการป้องกันแบบเรียลไทม์

การป้องกันแบบเรียลไทม์เป็นองค์ประกอบที่สำคัญที่สุดในการรักษาระบบที่ปลอดภัยด้วย ESET Cyber Security โปรดใช้ความระมัดระวังเมื่อแก้ไขพารามิเตอร์ของการป้องกันแบบเรียลไทม์ เราขอแนะนำให้คุณแก้ไขพารามิเตอร์เหล่านี้ในกรณีพิเศษเท่านั้น ตัวอย่างเช่น ในกรณีที่มีข้อขัดแย้งกับบางแอพพลิเคชัน

หลังจากการติดตั้ง ESET Cyber Security การตั้งค่าทั้งหมดจะได้รับการเพิ่มประสิทธิภาพเพื่อให้การรักษาความปลอดภัยให้กับระบบในระดับสูงสุดสำหรับผู้ใช้ หากต้องการเรียกคืนการตั้งค่าเริ่มต้น ให้คลิก **ค่าเริ่มต้น** ที่อยู่บริเวณด้านซ้ายล่างของหน้าต่าง **การป้องกันแบบเรียลไทม์ (ตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > การป้องกันแบบเรียลไทม์)**

การตรวจสอบการป้องกันแบบเรียลไทม์

หากต้องการตรวจสอบว่าการป้องกันแบบเรียลไทม์กำลังทำงานและตรวจหาไวรัสอยู่ ให้ดาวน์โหลดไฟล์ทดสอบจาก eicar.com และตรวจสอบเพื่อดูว่า ESET Cyber Security ระบุไฟล์เป็นภัยคุกคามหรือไม่ ไฟล์ทดสอบนี้เป็นไฟล์พิเศษที่ไม่มีอันตราย ซึ่งจะตรวจพบได้โดยโปรแกรมป้องกันไวรัสทุกโปรแกรม ไฟล์นี้สร้างขึ้นโดยสถาบัน EICAR (European Institute for Computer Antivirus Research) เพื่อทดสอบการทำงานของโปรแกรมป้องกันไวรัส

ควรทำอย่างไรเมื่อการป้องกันแบบเรียลไทม์ไม่ทำงาน

ในบทนี้ เราจะอธิบายสถานการณ์ของปัญหาที่อาจเกิดขึ้นเมื่อใช้การป้องกันแบบเรียลไทม์ รวมถึงการแก้ปัญหาดังกล่าวด้วย

การป้องกันแบบเรียลไทม์ถูกปิดใช้งาน

หากผู้ใช้ปิดการป้องกันแบบเรียลไทม์โดยไม่ได้ตั้งใจ ผู้ใช้จะต้องเปิดการใช้งานใหม่อีกครั้ง หากต้องการเปิดใช้งานการป้องกันแบบเรียลไทม์อีกครั้ง ให้คลิก **ตั้งค่า** > **คอมพิวเตอร์** จากเมนูหลัก และเปลี่ยน **การป้องกันระบบไฟล์แบบเรียลไทม์** เป็น **เปิดใช้งาน** หรือคุณสามารถเปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์ได้ในหน้าต่างการตั้งค่าแอพพลิเคชันใน **การป้องกันแบบเรียลไทม์** ด้วยการเลือกตัวเลือก **เปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์**

การป้องกันแบบเรียลไทม์ไม่พบและไม่กำจัดการแฝงตัว

ตรวจสอบว่าไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอื่นในคอมพิวเตอร์ของคุณ หากมีการใช้การป้องกันแบบเรียลไทม์สองชนิดในเวลาเดียวกัน อาจมีข้อขัดแย้งเกิดขึ้นระหว่างกัน ขอแนะนำให้คุณถอนการติดตั้งโปรแกรมป้องกันไวรัสอื่นที่อาจมีอยู่ในระบบของคุณ

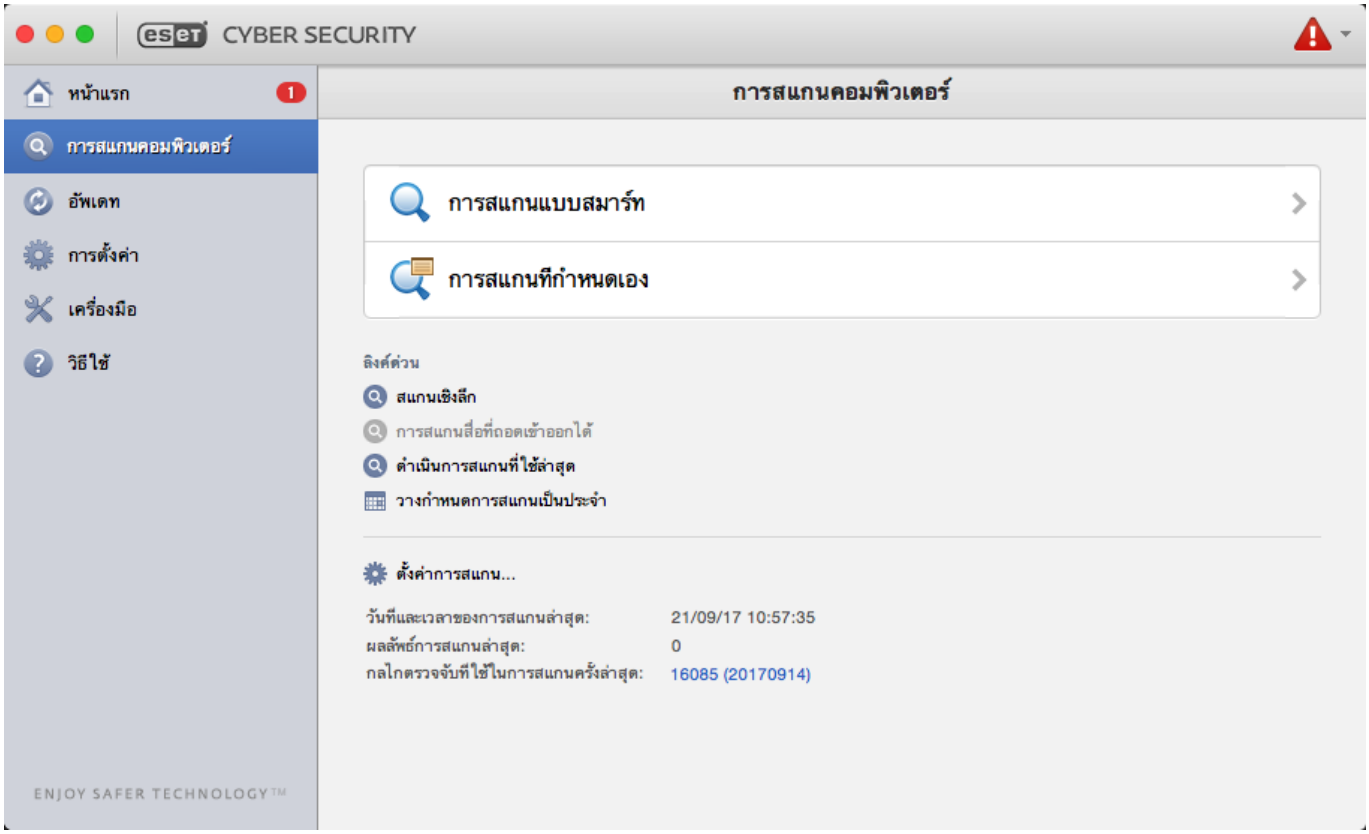
การป้องกันแบบเรียลไทม์ไม่เริ่มต้นทำงาน

ถ้าการป้องกันแบบเรียลไทม์ไม่เริ่มต้นทำงานเมื่อเริ่มต้นระบบ โปรแกรมอาจเกิดข้อขัดแย้งกับโปรแกรมอื่น หากเป็นกรณีนี้ โปรดติดต่อฝ่ายดูแลลูกค้าของ ESET

การสแกนคอมพิวเตอร์ตามต้องการ

หากคุณสงสัยว่าคอมพิวเตอร์ของคุณติดไวรัส (คอมพิวเตอร์ทำงานผิดปกติ) ให้เรียกใช้ **การสแกนแบบสมาร์ท** เพื่อตรวจหาการแฝงตัวในคอมพิวเตอร์ของคุณ เพื่อให้มีการป้องกันสูงสุด ควรเรียกใช้การสแกนคอมพิวเตอร์สม่ำเสมอในฐานะเป็นส่วนหนึ่งของมาตรการรักษาความปลอดภัย ไม่ใช่เรียกใช้เมื่อสงสัยว่ามีการติดไวรัส การสแกนเป็นประจำสามารถตรวจหาการแฝงตัวที่เครื่องมือสแกนแบบเรียลไทม์ตรวจไม่พบเมื่อมีการบันทึกไปยังดิสก์ ซึ่งอาจเกิดขึ้นในกรณีที่เครื่องมือสแกนแบบเรียลไทม์ถูกปิดการใช้งานในขณะที่มีการติดไวรัส หรือโมดูลการตรวจหาไม่ได้อัพเดท

ขอแนะนำให้คุณเรียกใช้การสแกนคอมพิวเตอร์ตามต้องการอย่างน้อยเดือนละหนึ่งครั้ง คุณสามารถกำหนดค่าการสแกนเป็นงานตามกำหนดการได้จาก **เครื่องมือ** > **เครื่องมือวางกำหนดการ**



ประเภทการสแกน

มีการสแกนคอมพิวเตอร์ตามต้องการสองประเภท **สแกนแบบสมาร์ท** จะสแกนระบบอย่างรวดเร็ว โดยไม่ต้องมีการกำหนดค่าพารามิเตอร์การสแกนเพิ่มเติม **การสแกนที่กำหนดเอง** จะช่วยให้คุณสามารถเลือกโปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าได้ และเลือกเป้าหมายการสแกนได้อย่างเจาะจง

สแกนแบบสมาร์ท

การสแกนแบบสมาร์ทจะช่วยให้คุณเริ่มต้นการสแกนคอมพิวเตอร์และกำจัดไฟล์ที่ติดไวรัสได้อย่างรวดเร็ว โดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ประโยชน์สำคัญคือการดำเนินการที่ง่ายโดยไม่ต้องกำหนดค่าการสแกนโดยละเอียด การสแกนแบบสมาร์ทจะตรวจสอบทุกไฟล์ในโฟลเดอร์ทั้งหมด รวมทั้งกำจัดหรือลบการแฝงตัวที่ตรวจพบโดยอัตโนมัติ โปรแกรมจะตั้งค่าระดับการกำจัดเป็นค่าเริ่มต้นโดยอัตโนมัติ สำหรับข้อมูลโดยละเอียดเกี่ยวกับประเภทการกำจัด โปรดดูที่ส่วน การกำจัด

การสแกนที่กำหนดเอง

การสแกนที่กำหนดเอง เป็นการสแกนที่เหมาะสมถ้าคุณต้องการระบุพารามิเตอร์การสแกน เช่น เป้าหมายการสแกน และวิธีการสแกน ประโยชน์ของการเรียกใช้การสแกนที่กำหนดเองคือ คุณสามารถกำหนดค่ารายละเอียดของพารามิเตอร์ได้ คุณสามารถบันทึกการกำหนดค่าอื่นๆ ไว้เป็นโปรไฟล์การสแกนที่ผู้ใช้กำหนด ซึ่งจะเป็นประโยชน์ถ้ามีการสแกนซ้ำโดยใช้พารามิเตอร์เดียวกัน

เมื่อต้องการเลือกเป้าหมายการสแกน ให้เลือก **การสแกนคอมพิวเตอร์** > **การสแกนที่กำหนดเอง** จากนั้น เลือก **เป้าหมายการสแกน** ที่เจาะจงจากลำดับโครงสร้าง นอกจากนี้ คุณสามารถระบุเป้าหมายการสแกนได้อย่างแม่นยำมากขึ้นโดยป้อนพาธไปยังโฟลเดอร์หรือไฟล์ที่คุณต้องการให้รวมไว้ หากคุณต้องการเพียงสแกนระบบโดยไม่ต้องมีการกำจัด ให้เลือก **สแกนโดยไม่กำจัด** นอกจากนี้ คุณยังสามารถเลือกระดับการกำจัดได้สามระดับโดยคลิกที่ **ตั้งค่า...** > **การกำจัด**

> **การสแกนที่กำหนดเอง**
> ขอแนะนำให้ดำเนินการสแกนคอมพิวเตอร์โดยใช้การสแกนที่กำหนดเองสำหรับผู้ใช้ขั้นสูงที่มีประสบการณ์การใช้โปรแกรมป้องกันไวรัสมาก่อนหน้านี้

เป้าหมายการสแกน

ลำดับโครงสร้างของเป้าหมายการสแกนจะช่วยให้คุณสามารถเลือกไฟล์และโฟลเดอร์ที่จะสแกนหาไวรัส โฟลเดอร์อาจถูกเลือกตามการตั้งค่าโปรไฟล์

คุณสามารถกำหนดเป้าหมายการสแกนได้อย่างแม่นยำมากขึ้นโดยป้อนพาธไปยังโฟลเดอร์หรือไฟล์ที่คุณต้องการให้รวมไว้ในการสแกน เลือกเป้าหมายจากลำดับโครงสร้างที่แสดงโฟลเดอร์ที่ใช้ได้ทั้งหมดในคอมพิวเตอร์ด้วยการเลือก

กล่องกาเครื่องหมายที่เกี่ยวข้องกับไฟล์หรือโฟลเดอร์ที่กำหนด

โปรไฟล์การสแกน

การตั้งค่าการสแกนที่ต้องการของคุณจะถูกบันทึกไว้สำหรับการสแกนในอนาคต เราขอแนะนำให้คุณสร้างโปรไฟล์ที่แตกต่าง (ที่มีเป้าหมายการแสกน วิธีการสแกนและพารามิเตอร์อื่น ๆ ที่ต่างกัน) สำหรับการสแกนที่ใช้เป็นประจำแต่ละการสแกน

หากต้องการสร้างโปรไฟล์ใหม่ จากเมนูหลัก ให้คลิก **ตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน...** (หรือกด *cmd+,*) > **สแกนคอมพิวเตอร์** แล้วคลิก **แก้ไข...** ที่อยู่ถัดจากรายการของโปรไฟล์ปัจจุบัน

ในการช่วยให้คุณสร้างโปรไฟล์การสแกนที่ตรงกับความต้องการของคุณ ให้ดูที่ส่วน การตั้งค่าพารามิเตอร์โปรแกรม ThreatSense สำหรับคำอธิบายของแต่ละพารามิเตอร์ของการตั้งค่าการสแกน

ตัวอย่างเช่น: สมมติว่าคุณต้องการสร้างโปรไฟล์การสแกนของคุณเองและการกำหนดค่าของการสแกนแบบสมาร์ทนั้นตรงกับความต้องการของคุณบางส่วน แต่คุณไม่ต้องการที่จะสแกนรันไทม์แพ็คเกอร์หรือแอพพลิเคชันที่ไม่ปลอดภัยและคุณยังต้องการที่จะปรับใช้การทำความสะอาดอย่างเข้มงวด ในหน้าต่าง **รายการโปรไฟล์ตัวแสกนเมื่อต้องการ** ให้พิมพ์ชื่อโปรไฟล์ คลิกปุ่ม **เพิ่ม** แล้วยืนยันโดยการคลิก **ตกลง** จากนั้นปรับพารามิเตอร์ให้ตรงกับความต้องการของคุณโดยตั้งค่า **โปรแกรม ThreatSense** และ **เป้าหมายสแกน**

หากคุณต้องการปิดระบบปฏิบัติการและปิดระบบคอมพิวเตอร์หลังจากเสร็จสิ้นการสแกนตามต้องการ ให้ใช้ตัวเลือก **ปิดระบบคอมพิวเตอร์หลังจากสแกน**

การตั้งค่าพารามิเตอร์กลไก ThreatSense

ThreatSense เป็นเทคโนโลยีกรรมสิทธิ์ของ ESET ที่ประกอบไปด้วยวิธีการตรวจหาภัยคุกคามที่ซับซ้อนหลายรูปแบบ เทคโนโลยีนี้เป็นการป้องกันในเชิงรุก ซึ่งหมายความว่าจะมีการป้องกันตั้งแต่ช่วงต้นที่มีการแพร่กระจายของภัยคุกคามใหม่ เทคโนโลยีนี้จะใช้หลายวิธีร่วมกัน (การวิเคราะห์รหัส การจำลองรหัส ฐานข้อมูลทั่วไป เป็นต้น) ซึ่งทำงานร่วมกันอย่างสอดคล้อง เพื่อเพิ่มประสิทธิภาพของการรักษาความปลอดภัยให้กับระบบได้อย่างมาก กลไกการสแกนสามารถควบคุมสตรีมข้อมูลต่างๆ ได้พร้อมกัน ซึ่งเพิ่มประสิทธิภาพและอัตราการตรวจพบสูงสุด นอกจากนี้ เทคโนโลยี ThreatSense ยังช่วยล้างรูทคิทด้วย

ตัวเลือกการตั้งค่าของเทคโนโลยี ThreatSense ช่วยให้ผู้ใช้สามารถระบุพารามิเตอร์การสแกนต่างๆ ได้:

- ประเภทไฟล์และนามสกุลที่จะสแกน
- การใช้วิธีการตรวจหาต่างๆ ร่วมกัน
- ระดับการล้าง เป็นต้น

ในการเปิดหน้าต่างการตั้งค่า ให้คลิก **การตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน** (หรือกด *cmd+,*) แล้วคลิกกลไก ThreatSense ปุ่ม **การตั้งค่า** ที่อยู่ในโมดูล **การป้องกันขั้นสูงสุด** โมดูล **การป้องกันแบบเรียลไทม์** และโมดูล **การสแกนคอมพิวเตอร์** ซึ่งใช้เทคโนโลยี ThreatSense ทั้งหมด (ดูที่ด้านล่าง) สถานการณ์ด้านความปลอดภัยที่ต่างกันอาจต้องใช้การกำหนดค่าที่ต่างกัน โปรดทราบว่า ThreatSense สามารถกำหนดค่าแยกกันได้สำหรับโมดูลการป้องกันต่อไปนี้:

- **การป้องกันเมื่อเริ่มต้นระบบ** - การตรวจสอบไฟล์เมื่อเริ่มต้นระบบโดยอัตโนมัติ
- **การป้องกันแบบเรียลไทม์** - การป้องกันระบบไฟล์แบบเรียลไทม์
- **การสแกนคอมพิวเตอร์** - การสแกนคอมพิวเตอร์ตามต้องการ
- **การป้องกันการเข้าถึงเว็บ**
- **การป้องกันอีเมล**

พารามิเตอร์ ThreatSense มีการปรับให้เหมาะสำหรับแต่ละโมดูลโดยเฉพาะ และการแก้ไขเหล่านี้จะมีผลกับการทำงานของระบบมากด้วยเช่นกัน ตัวอย่างเช่น การเปลี่ยนการตั้งค่าเพื่อให้สแกนรันไทม์แพ็คเกอร์อยู่ตลอดเวลาหรือการเปิดใช้งานการวิเคราะห์พฤติกรรมขั้นสูงในโมดูลการป้องกันระบบไฟล์แบบเรียลไทม์อาจทำให้ระบบทำงานช้าลง ดังนั้น เราขอแนะนำให้คุณคงพารามิเตอร์ ThreatSense เริ่มต้นไว้สำหรับโมดูลทั้งหมด ยกเว้นการสแกนคอมพิวเตอร์

วัตถุ

ส่วน **วัตถุ** จะช่วยให้คุณสามารถกำหนดว่าจะสแกนหาการแฝงตัวจากไฟล์ใด

• **ลิงค์สัญลักษณ์** - (การสแกนคอมพิวเตอร์เท่านั้น) สแกนไฟล์ประเภทพิเศษที่มีสตริงข้อความที่ได้รับการตีความและตามด้วยระบบปฏิบัติการในฐานะที่เป็นพาธไปยังไฟล์หรือไดเรกทอรีอื่น

• **ไฟล์อีเมล** - (ไม่สามารถใช้ได้ในการป้องกันแบบเรียลไทม์) สแกนไฟล์อีเมล

• **กล่องจดหมาย** - (ไม่สามารถใช้ได้ในการป้องกันแบบเรียลไทม์) สแกนกล่องจดหมายของผู้ใช้ในระบบ การใช้งานตัวเลือกนี้อย่างไม่ถูกต้องอาจทำให้เกิดข้อขัดแย้งกับอีเมลไคลเอ็นต์ของคุณ เมื่อต้องการเรียนรู้เพิ่มเติมเกี่ยวกับข้อดีและข้อเสียของตัวเลือกนี้ โปรดอ่าน บทความฐานความรู้ ต่อไปนี้

• **อาร์ไคฟ์** - (ไม่สามารถใช้ได้ในการป้องกันแบบเรียลไทม์) สแกนไฟล์ที่บีบอัดในอาร์ไคฟ์ (.rar, .zip, .arj, .tar เป็นต้น)

• **อาร์ไคฟ์ที่ขยายในตัว** - (ไม่สามารถใช้ได้ในการป้องกันแบบเรียลไทม์) สแกนไฟล์ที่อยู่ในไฟล์อาร์ไคฟ์ที่ขยายในตัว

• **รันไทม์แพ็คเกอร์** - แตกต่างจากอาร์ไคฟ์ประเภทมาตรฐาน รันไทม์แพ็คเกอร์จะขยายในหน่วยความจำ เมื่อสิ่งนี้ถูกเลือก แพ็คเกอร์คงที่แบบมาตรฐาน (UPX, yoda, ASPack, FGS เป็นต้น) จะถูกสแกนด้วย

ตัวเลือก

ในส่วน **ตัวเลือก** คุณสามารถเลือกวิธีที่ใช้ระหว่างการสแกนระบบได้ ตัวเลือกที่ใช้ได้มีดังนี้:

• **การวิเคราะห์พฤติกรรม** – การวิเคราะห์พฤติกรรมใช้อัลกอริทึมที่วิเคราะห์การทำงาน (ที่เป็นอันตราย) ของโปรแกรม ประโยชน์สำคัญของการตรวจหาการวิเคราะห์พฤติกรรมคือความสามารถในการตรวจหาซอฟต์แวร์ที่เป็นอันตรายใหม่ที่ไม่เคยมีมาก่อน

• **การวิเคราะห์พฤติกรรมขั้นสูง** – การวิเคราะห์พฤติกรรมขั้นสูงประกอบด้วยอัลกอริทึมการวิเคราะห์พฤติกรรมที่ไม่ซ้ำกัน ที่พัฒนาโดย ESET มีการปรับปรุงประสิทธิภาพสำหรับการตรวจหาเวิร์มของคอมพิวเตอร์และม้าโทรจัน ซึ่งเขียนในภาษาที่ใช้เขียนโปรแกรมระดับสูง ความสามารถในการตรวจหาของโปรแกรมจะสูงขึ้นอย่างเห็นได้ชัดอันเนื่องมาจากการวิเคราะห์พฤติกรรมขั้นสูง

การกำจัด

การตั้งค่าการกำจัดจะเป็นตัวกำหนดรูปแบบที่เครื่องมือสแกนกำจัดไฟล์ที่ติดไวรัส การกำจัดมี 3 ระดับ:

• **ไม่มีการกำจัด** - โปรแกรมจะไม่กำจัดไฟล์ที่ติดไวรัสโดยอัตโนมัติ โปรแกรมจะแสดงหน้าต่างคำเตือน และช่วยให้คุณเลือกการดำเนินการ

• **การกำจัดมาตรฐาน** - โปรแกรมจะพยายามกำจัดหรือลบไฟล์ที่ติดไวรัสโดยอัตโนมัติ ถ้าไม่สามารถเลือกการดำเนินการที่ถูกต้องโดยอัตโนมัติ โปรแกรมจะเสนอตัวเลือกของการดำเนินการ ตัวเลือกของการดำเนินการจะปรากฏในกรณีที่ไม่สามารถดำเนินการตามที่กำหนดไว้ล่วงหน้าด้วย

• **การกำจัดอย่างเข้มงวด** – โปรแกรมจะกำจัดหรือลบไฟล์ที่ติดไวรัสทั้งหมด (รวมถึงอาร์ไคฟ์ด้วย) แต่จะยกเว้นไฟล์ของระบบ หากไม่สามารถกำจัดไฟล์ได้ คุณจะได้รับการแจ้งเตือนและระบบจะให้คุณเลือกประเภทการดำเนินการที่ต้องการ

ไฟล์อาร์ไคฟ์
ในโหมดการกำจัดมาตรฐานที่เป็นค่าเริ่มต้น ไฟล์อาร์ไคฟ์ทั้งหมดจะถูกลบต่อเมื่อไฟล์ทั้งหมดในอาร์ไคฟ์ติดไวรัส หากอาร์ไคฟ์มีไฟล์ที่ถูกต้องและไฟล์ที่ติดไวรัส อาร์ไคฟ์จะไม่ถูกลบ หากตรวจพบไฟล์อาร์ไคฟที่ติดไวรัสในโหมดการกำจัดอย่างเข้มงวด โปรแกรมจะลบทั้งอาร์ไคฟ์ แม้ว่าจะมีไฟล์ที่ไม่ติดไวรัสอยู่ก็ตาม

การสแกนอาร์ไคฟ์
ในโหมดการกำจัดมาตรฐานที่เป็นค่าเริ่มต้น ไฟล์อาร์ไคฟ์ทั้งหมดจะถูกลบต่อเมื่อไฟล์ทั้งหมดในอาร์ไคฟ์ติดไวรัส หากอาร์ไคฟ์มีไฟล์ที่ถูกต้องและไฟล์ที่ติดไวรัส อาร์ไคฟ์จะไม่ถูกลบ หากตรวจพบไฟล์อาร์ไคฟที่ติดไวรัสในโหมดการกำจัดอย่างเข้มงวด โปรแกรมจะลบทั้งอาร์ไคฟ์ แม้ว่าจะมีไฟล์ที่ไม่ติดไวรัสอยู่ก็ตาม

การยกเว้น

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่าพารามิเตอร์ ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะยกเว้นจากการสแกน

โดยปกติแล้ว โปรแกรมจะสแกนไฟล์ทั้งหมดโดยไม่คำนึงถึงนามสกุลไฟล์ คุณสามารถเพิ่มนามสกุลในรายการไฟล์ที่จะยกเว้นจากการสแกน เมื่อใช้ปุ่ม + และ − คุณสามารถเปิดใช้งานหรือยกเว้นการสแกนนามสกุลที่เจาะจงได้

ในบางครั้ง การยกเว้นไฟล์จากการสแกนจะเป็นสิ่งจำเป็น ถ้าประเภทไฟล์บางประเภทของการสแกนป้องกันโปรแกรมเพื่อไม่ให้ทำงานอย่างถูกต้อง ตัวอย่างเช่น ควรยกเว้นไฟล์ *log*, *cfg* และ *tmp* รูปแบบที่ถูกต้องสำหรับการ

ป้อนนามสกุลไฟล์คือ:

log

cfg

tmp

ขีดจำกัด

ส่วน **ขีดจำกัด** ช่วยให้คุณสามารถระบุขนาดสูงสุดของวัตถุ และระดับของอาร์ไคฟ์ที่ซ้อนที่จะสแกน:

• **ขนาดสูงสุด:** กำหนดขนาดสูงสุดของวัตถุที่จะสแกน เมื่อขนาดสูงสุดถูกกำหนด โมดูลป้องกันไวรัสจะสแกนเฉพาะวัตถุที่เล็กกว่าขนาดที่ระบุเท่านั้น ผู้ที่สามารถแก้ไขตัวเลือกนี้ควรเป็นผู้ใช้ขั้นสูง ซึ่งมีเหตุผลบางอย่างสำหรับการยกเว้นวัตถุขนาดใหญ่จากการสแกน

• **เวลาสแกนสูงสุด:** กำหนดค่าเวลาสูงสุดสำหรับการสแกนวัตถุ หากมีการป้อนค่าที่ผู้ใช้กำหนดไว้ โมดูลป้องกันไวรัสจะหยุดสแกนวัตถุเมื่อพ้นระยะเวลาดังกล่าว ไม่ว่าการสแกนจะเสร็จสิ้นแล้วหรือไม่

• **ระดับการซ้อนสูงสุด:** ระบุความลึกสูงสุดของการสแกนอาร์ไคฟ์ เราไม่แนะนำให้แก้ไขค่า 10 ซึ่งเป็นค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดที่จะต้องแก้ไขค่านี้ในสถานการณ์ปกติ หากการสแกนสิ้นสุดลงก่อนกำหนด เนื่องจากจำนวนอาร์ไคฟ์ที่ซ้อนกัน อาร์ไคฟ์จะไม่ได้รับการตรวจสอบ

• **ขนาดไฟล์สูงสุด:** ตัวเลือกนี้ช่วยให้คุณสามารถระบุขนาดไฟล์สูงสุดสำหรับไฟล์ที่อยู่ในอาร์ไคฟ์ (เมื่อดึงข้อมูล) ที่จะสแกน ถ้าการสแกนสิ้นสุดก่อนกำหนดด้วยผลของขีดจำกัดนี้ อาร์ไคฟ์จะไม่ได้รับการตรวจสอบ

อื่นๆ

เปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท

เมื่อเปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท การตั้งค่าจะได้รับการปรับให้เหมาะสมเพื่อให้มีการสแกนที่มีประสิทธิภาพและไม่ทำให้ความเร็วของการสแกนลดลง โมดูลการป้องกันต่างๆ จะสแกนอย่างชาญฉลาด โดยใช้วิธีการสแกนที่แตกต่างกัน การเพิ่มประสิทธิภาพแบบสมาร์ทจะไม่ได้กำหนดไว้อย่างแน่ชัดภายในผลิตภัณฑ์ ทีมพัฒนา ESET จะคงใช้งานการเปลี่ยนแปลงใหม่ๆ อย่างต่อเนื่อง ซึ่งจะนำมารวมกับ ESET Cyber Security ผ่านการอัพเดทเป็นประจำ ถ้าปิดใช้การเพิ่มประสิทธิภาพแบบสมาร์ท ระบบจะใช้เฉพาะการตั้งค่าที่ผู้ใช้กำหนดในกลไก ThreatSense ของโมดูลเมื่อดำเนินการสแกน

สแกนสตรีมข้อมูลสำรอง (เฉพาะเครื่องสแกนตามต้องการเท่านั้น)

สตรีมข้อมูลสำรอง ที่ใช้งานโดยระบบไฟล์เป็นการเชื่อมโยงไฟล์และโฟลเดอร์ซึ่งจะไม่ปรากฏกับเทคนิคการสแกนทั่วไป การแฝงตัวจำนวนมากพยายามหลีกเลี่ยงการตรวจสอบนี้ โดยปลอมแปลงตัวเองเป็นสตรีมข้อมูลสำรอง

ตรวจพบการแฝงตัว

การแฝงตัวสามารถเข้าสู่ระบบได้จากจุดเข้าใช้ต่างๆ เช่น หน้าเว็บ โฟลเดอร์ที่ใช้ร่วมกัน อีเมล หรือจากอุปกรณ์คอมพิวเตอร์ที่ถอดเข้าออกได้ (USB, ดิสก์ภายนอก, ซีดี, ดีวีดี เป็นต้น)

ถ้าคอมพิวเตอร์ของคุณแสดงสัญญาณการติดไวรัสจากมัลแวร์ เช่น ทำงานช้า ค้างบ่อย ๆ เป็นต้น เราขอแนะนำให้ดำเนินการตามขั้นตอนต่อไปนี้:

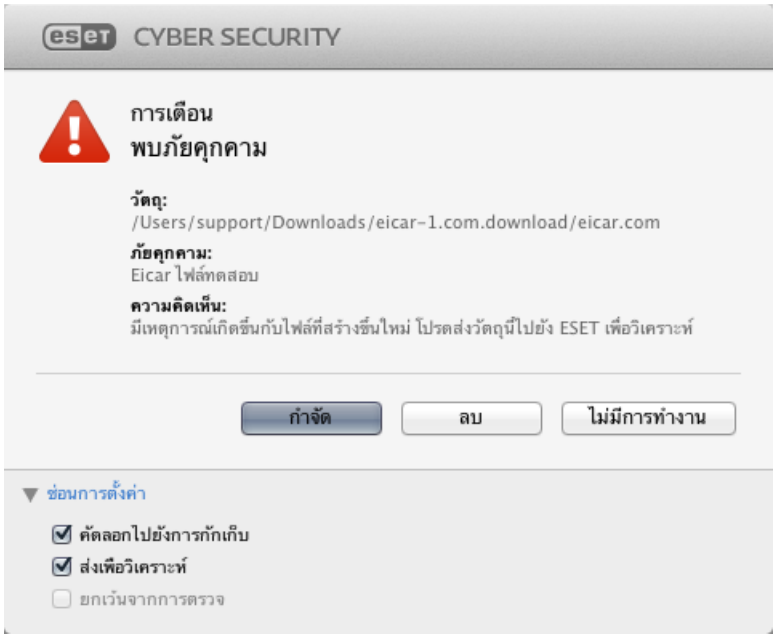
1. คลิก **การสแกนคอมพิวเตอร์**
2. คลิก **การสแกนแบบสมาร์ท** (สำหรับข้อมูลเพิ่มเติม โปรดดูส่วน การสแกนแบบสมาร์ท)
3. หลังจากสแกนเสร็จสิ้นแล้ว ให้ตรวจดูบันทึกสำหรับจำนวนไฟล์ที่สแกน ไฟล์ที่ติดไวรัส และไฟล์ที่มีการกำจัดไวรัส

หากคุณต้องการสแกนเฉพาะบางส่วนของดิสก์ของคุณ ให้คลิก **การสแกนที่กำหนดเอง** และเลือกเป้าหมายที่จะสแกนหาไวรัส

ต่อไปนี้เป็นตัวอย่างทั่วไปสำหรับวิธีจัดการกับการแฝงตัวโดย ESET Cyber Security สมมติว่าการแฝงตัวถูกตรวจพบโดยการตรวจสอบระบบไฟล์แบบเรียลไทม์ ซึ่งใช้ระดับการกำจัดเริ่มต้น การป้องกันแบบเรียลไทม์จะพยายามทำความสะอาดหรือลบไฟล์ หากไม่มีการดำเนินการที่กำหนดไว้ล่วงหน้าสำหรับโมดูลการป้องกันแบบเรียลไทม์ ระบบจะให้คุณเลือกตัวเลือกในหน้าต่างการเตือน โดยทั่วไปแล้วจะมีตัวเลือก **กำจัด**, **ลบ** และ **ไม่มีการทำงาน** ไม่แนะนำให้เลือก **ไม่มีการทำงาน** เนื่องจากไฟล์ที่ติดไวรัสจะถูกทิ้งในสถานะที่ติดไวรัสอยู่ ตัวเลือกนี้ใช้กับสถานการณ์ที่เมื่อคุณแน่ใจว่าไฟล์ดังกล่าวไม่มีอันตราย และตรวจพบผิดพลาดว่ามีไวรัส

การกำจัดและการลบ

ใช้การกำจัดถ้าไฟล์ถูกโจมตีโดยไวรัสที่มีการแนบรหัสที่เป็นอันตรายกับไฟล์นั้น ในกรณีนี้ ขั้นแรกให้พยายามกำจัดไวรัสออกจากไฟล์ที่ติดเชื้อเพื่อคืนค่าไฟล์สู่สภาวะเดิม ถ้าไฟล์มีเฉพาะรหัสที่เป็นอันตราย ไฟล์ดังกล่าวจะถูกลบ



การลบไฟล์ในอาร์ไคฟ์

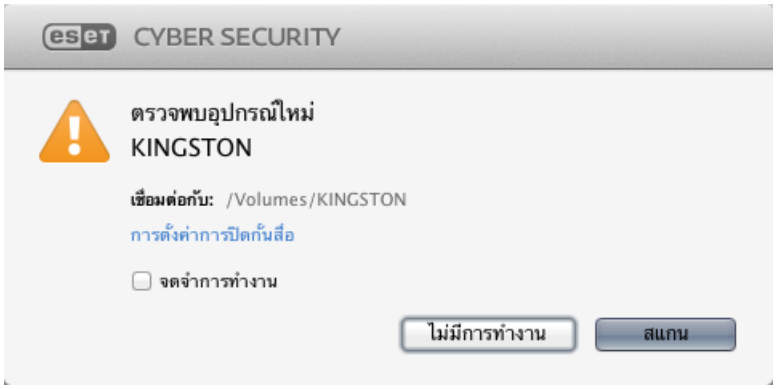
ในโหมดการกำจัดเริ่มต้น ระบบจะลบทั้งอาร์ไคฟ์ต่อเมื่อมีไฟล์ที่ติดไวรัส และไม่มีไฟล์ที่ปลอดไวรัสเลย กล่าวอีกนัยหนึ่งก็คือ โปรแกรมจะไม่ลบอาร์ไคฟ์ ถ้ายังมีไฟล์ที่ไม่เป็นอันตรายรวมอยู่ด้วย อย่างไรก็ตาม โปรดใช้ความระมัดระวังเมื่อสแกน **การกำจัดอย่างเข้มงวด** เนื่องจากเมื่อใช้การกำจัดอย่างเข้มงวด โปรแกรมจะลบอาร์ไคฟ์แม้ว่าจะมีไฟล์ที่ติดไวรัสเพียงไฟล์เดียวก็ตาม โดยไม่คำนึงถึงสถานะของไฟล์อื่นๆ ในอาร์ไคฟ์

การสแกนและการปิดกั้นสื่อที่ถอดเข้าออกได้

ESET Cyber Security สามารถเรียกใช้การสแกนตามต้องการของอุปกรณ์หน่วยความจำที่ถอดเข้าออกได้ที่ใส่ไว้ (ซีดี, ดีวีดี, USB ฯลฯ) บน macOS 10.15 ESET Cyber Security จะยังสามารถสแกนอุปกรณ์สื่อภายนอกอื่นๆ ได้อีกด้วย

การสแกนสื่อที่ถอดเข้าออกได้บน macOS 11 และใหม่กว่า

ESET Cyber Security ที่ติดตั้งบน macOS 11 และใหม่กว่า จะสแกนเฉพาะอุปกรณ์หน่วยความจำเท่านั้น



สื่อที่ถอดเข้าออกได้อาจมีรหัสที่เป็นอันตรายและทำให้คอมพิวเตอร์ของคุณได้รับความเสี่ยง เมื่อต้องการปิดกั้นสื่อที่ถอดเข้าออกได้ ให้คลิกปุ่ม **การตั้งค่าการปิดกั้นสื่อ** (ดูภาพด้านบน) หรือจากเมนูหลัก คลิก **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** > **สื่อ** จากหน้าต่างโปรแกรมหลักและเลือก **เปิดใช้งานการปิดกั้นสื่อที่ถอดเข้าออกได้** เมื่อต้องการอนุญาตการเข้าถึงสื่อบางประเภท ให้ยกเลิกการเลือกไดรฟ์ข้อมูลของสื่อที่ต้องการของคุณ

การเข้าถึงซีดีรอม
เมื่อต้องการอนุญาตการเข้าถึงไดรฟ์ซีดีรอมภายนอกที่เชื่อมต่อไปยังคอมพิวเตอร์ของคุณผ่านสาย USB ให้ยกเลิกการเลือกที่ตัวเลือก **ซีดีรอม**

การป้องกันฟิชชิ่ง

คำว่า ฟิชชิ่ง หมายถึงกิจกรรมทางอาชญากรรมที่ใช้วิศวกรรมสังคม (การดำเนินการของผู้ใช้เพื่อให้ได้มาซึ่งข้อมูลลับเฉพาะ) การฟิชชิ่งมักใช้เพื่อให้ได้เข้าถึงข้อมูลที่ละเอียดอ่อน เช่น หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต หมายเลขพินหรือชื่อผู้ใช้และรหัสผ่าน

เราขอแนะนำให้คุณเปิดใช้งานการป้องกันฟิชชิ่ง (**การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** > **การป้องกันฟิชชิ่ง**) การโจมตีทั้งหมดที่อาจเป็นการโจมตีแบบฟิชชิ่งซึ่งมาจากเว็บไซต์หรือโดเมนที่เป็นอันตรายจะถูกปิดกั้น และการแจ้งเตือนจะปรากฏขึ้นเพื่อแจ้งให้คุณทราบถึงการโจมตีนั้น

การป้องกันเว็บและอีเมล

หากต้องการเข้าถึงการป้องกันเว็บและเมลจากเมนูหลัก ให้คลิก **ตั้งค่า** > **เว็บและอีเมล** จากจุดนี้ คุณยังสามารถเข้าถึงการตั้งค่าอย่างละเอียดสำหรับโมดูลแต่ละโมดูลโดยคลิก **การตั้งค่า...**

- **การป้องกันการเข้าถึงเว็บ** - ตรวจสอบการเชื่อมต่อ HTTP ระหว่างเว็บเบราว์เซอร์และเซิร์ฟเวอร์ระยะไกล
- **การป้องกันอีเมลไคลเอ็นต์** - ให้การควบคุมการสื่อสารอีเมลที่ได้รับผ่านโปรโตคอล POP3 และ IMAP
- **การป้องกันฟิชชิ่ง** - ปิดกั้นการโจมตีที่อาจเป็นการโจมตีแบบฟิชชิ่งซึ่งมาจากเว็บไซต์หรือโดเมน

ข้อยกเว้นการสแกน
ESET Cyber Security จะไม่สแกนโปรโตคอลที่เข้ารหัส HTTPS, POP3S และ IMAPS

การป้องกันเว็บ

การป้องกันการเข้าถึงเว็บจะตรวจสอบการสื่อสารระหว่างเว็บเบราว์เซอร์และเซิร์ฟเวอร์ระยะไกลสำหรับทำตามกฎ HTTP (Hypertext Transfer Protocol)

การกรองเว็บสามารถทำได้โดยกำหนด หมายเลขพอร์ตสำหรับการเชื่อมต่อ HTTP และ/หรือ ที่อยู่ URL

พอร์ต

ในแท็บ **พอร์ต** คุณสามารถกำหนดเลขที่พอร์ตที่ใช้สำหรับการสื่อสารของ HTTP ตามค่าเริ่มต้น เลขที่พอร์ต 80, 8080 และ 3128 จะถูกกำหนดไว้ล่วงหน้า

รายการ URL

ส่วน **รายการ URL** จะช่วยให้คุณสามารถระบุที่อยู่ HTTP เพื่อปิดกั้น อนุญาต หรือยกเว้นจากการตรวจสอบ เว็บไซต์ในรายการของที่อยู่ที่ปิดกั้นจะไม่สามารถเข้าถึงได้ เว็บไซต์ในรายการของที่อยู่ที่ยกเว้นจะสามารถเข้าถึงได้ โดยไม่ต้องสแกนหารหัสที่เป็นอันตราย

หากต้องการอนุญาตการเข้าถึงเฉพาะที่อยู่ URL ที่ระบุไว้ใน **URL ที่อนุญาต** ให้เลือกตัวเลือก **จำกัดที่อยู่ URL**

หากต้องการเปิดใช้งานรายการ ให้เลือก **เปิดใช้งาน** ข้างชื่อรายการ หากคุณต้องการได้รับการแจ้งเตือนเมื่อป้อนที่อยู่จากรายการปัจจุบัน ให้เลือก **แจ้งเตือน**

ในรายการใดๆ สัญลักษณ์พิเศษ *(เครื่องหมายดอกจัน) และ ?(เครื่องหมายคำถาม) สามารถใช้ได้ เครื่องหมายดอกจันจะแทนอักขระ และเครื่องหมายคำถามจะแทนสัญลักษณ์ ควรพิจารณาอย่างรอบคอบเมื่อระบุที่อยู่ที่ยกเว้น เนื่องจากรายการดังกล่าวควรมีเฉพาะที่อยู่ที่เชื่อถือและปลอดภัยเท่านั้น ในทำนองเดียวกัน ควรตรวจสอบว่ามีการใช้สัญลักษณ์ * และ ? อย่างถูกต้องในรายการนี้

การป้องกันอีเมล

การป้องกันอีเมลจะมีการควบคุมการสื่อสารทางอีเมลที่ได้รับผ่านโปรโตคอล POP3 และ IMAP เมื่อตรวจสอบข้อความขาเข้า ESET Cyber Security จะใช้วิธีการสแกนขั้นสูงทั้งหมดที่มีอยู่ในกลไกการสแกนของ ThreatSense การสแกน

การสื่อสารของโปรโตคอล POP3 และ IMAP จะไม่ขึ้นอยู่กับอีเมลไคลเอ็นต์ที่ใช้

กลไก ThreatSense: การตั้งค่า – การตั้งค่าเครื่องมือสแกนขั้นสูงจะช่วยให้คุณสามารถกำหนดค่าเป้าหมายการสแกน วิธีการตรวจหา และอื่นๆ ได้ คลิก **การตั้งค่า** เพื่อแสดงหน้าต่างการตั้งค่าเครื่องมือสแกนอย่างละเอียด

ต่อท้ายข้อความแท็กกับส่วนท้ายของอีเมล – หลังจากสแกนอีเมลแล้ว การแจ้งเตือนที่มีผลลัพธ์การสแกนจะสามารถนำไปต่อท้ายข้อความได้ ข้อความแท็กเป็นเครื่องมือที่มีประโยชน์ แต่ไม่ควรใช้เป็นปัจจัยที่ตัดสินความปลอดภัยของข้อความ เนื่องจากข้อความแท็กอาจไม่ปรากฏในข้อความ HTML ที่เป็นปัญหา และอาจถูกปลอมแปลงโดยภัยคุกคามบางตัวได้ ตัวเลือกที่ใช้ได้มีดังนี้:

- **ไม่** – จะไม่มีข้อความแท็กจะถูกเพิ่มลงในอีเมลใดๆ
- **ไปยังอีเมลที่ติดไวรัสเท่านั้น** – เฉพาะอีเมลที่มีมัลแวร์เท่านั้นที่จะถูกแท็กเป็นตรวจสอบแล้ว
- **ไปยังอีเมลทุกฉบับที่สแกน** – อีเมลที่สแกนทั้งหมดจะถูกต่อท้ายด้วยข้อความแท็ก

เพิ่มบันทึกต่อท้ายหัวเรื่องของอีเมลที่ติดไวรัสที่ได้รับและอ่าน – เลือกช่องทำเครื่องหมายนี้หากคุณต้องการให้การป้องกันอีเมลครอบคลุมถึงการเตือนภัยคุกคามในอีเมลที่ติดไวรัสด้วย คุณลักษณะนี้จะช่วยให้สามารถใช้การกรองแบบง่ายสำหรับอีเมลที่ติดไวรัส นอกจากนี้ยังช่วยเพิ่มระดับความน่าเชื่อถือสำหรับผู้รับ และถ้ามีการตรวจพบการแฝงตัว การดำเนินการนี้จะให้ข้อมูลที่เป็นประโยชน์เกี่ยวกับระดับภัยคุกคามของอีเมลหรือผู้ส่งที่ระบุ

เพิ่มแม่แบบไปยังหัวเรื่องของอีเมลที่ติดไวรัส – แก้ไขแม่แบบนี้เพื่อแก้ไขรูปแบบคำนำหน้าของหัวเรื่องของอีเมลที่ติดไวรัส

- %avstatus% เพิ่มสถานะของอีเมลที่ติดไวรัส (ตัวอย่างเช่น: สะอาด ติดไวรัส...)
- %virus% - เพิ่มชื่อของภัยคุกคาม
- %aspmstatus% - เปลี่ยนหัวข้อโดยขึ้นอยู่กับผลลัพธ์ของการสแกนป้องกันสแปม
- %product% - เพิ่มชื่อผลิตภัณฑ์ ESETของคุณ (ในกรณีนี้คือ - ESET Cyber Security)
- %product_url% - เพิ่มลิงก์เว็บไซต์ของ ESET (www.eset.com)

ที่ด้านล่างของหน้าต่างนี้ คุณยังสามารถเปิด/ปิดใช้งานการตรวจสอบการสื่อสารทางอีเมลที่ได้รับผ่านโปรโตคอล POP3 และ IMAP ได้อีกด้วย ถ้าต้องการเรียนรู้เพิ่มเติมในเรื่องนี้ โปรดดูหัวข้อต่อไปนี้:

- การตรวจสอบโปรโตคอล POP3
- การตรวจสอบโปรโตคอล IMAP

การตรวจสอบโปรโตคอล POP3

โปรโตคอล POP3 เป็นโปรโตคอลที่มีการใช้งานอย่างแพร่หลายมากที่สุด โดยใช้เพื่อรับการสื่อสารทางอีเมลในแอพพลิเคชันของอีเมลไคลเอ็นต์ ESET Cyber Security มีการป้องกันสำหรับโปรโตคอลนี้ โดยไม่คำนึงถึงอีเมลไคลเอ็นต์ที่ใช้งาน

โมดูลการป้องกันที่ให้การควบคุมนี้จะเริ่มต้นโดยอัตโนมัติเมื่อเริ่มต้นระบบ แล้วมีการใช้งานในหน่วยความจำ ตรวจสอบให้แน่ใจว่าเปิดใช้งานโมดูลอยู่เพื่อให้การกรองโปรโตคอลทำงานได้อย่างถูกต้อง การตรวจสอบโปรโตคอล POP3 จะดำเนินการโดยอัตโนมัติโดยไม่จำเป็นต้องกำหนดค่าอีเมลไคลเอ็นต์ของคุณใหม่ ตามค่าเริ่มต้น การสื่อสารทั้งหมดในพอร์ต 110 จะถูกสแกน แต่สามารถเพิ่มพอร์ตการสื่อสารอื่นๆ ได้ตามจำเป็น ต้องคั่นเลขที่พอร์ตด้วยเครื่องหมายจุลภาค

หากเลือกตัวเลือก **เปิดใช้งานการตรวจสอบโปรโตคอล POP3** ระบบจะตรวจสอบการรับส่งข้อมูลผ่าน POP3 ทั้งหมดเพื่อตรวจหาซอฟต์แวร์ที่เป็นอันตราย

การตรวจสอบโปรโตคอล IMAP

Internet Message Access Protocol (IMAP) คือโปรโตคอลอินเทอร์เน็ตอื่นสำหรับการเรียกอีเมล IMAP มีคุณประโยชน์บางอย่างเหนือ POP3 ตัวอย่างเช่น ไคลเอ็นต์หลายรายการสามารถเชื่อมต่อกับกล่องขาเข้าเดียวกันได้พร้อมกันและรักษาข้อมูลสถานะของข้อความ เช่น อ่าน ตอบกลับ หรือลบข้อความแล้วหรือไม่ ESET Cyber Security มีการป้องกันสำหรับโปรโตคอลนี้ โดยไม่คำนึงถึงอีเมลไคลเอ็นต์ที่ใช้งาน

โมดูลการป้องกันที่ให้การควบคุมนี้จะเริ่มต้นโดยอัตโนมัติเมื่อเริ่มต้นระบบ แล้วมีการใช้งานในหน่วยความจำ ตรวจสอบให้แน่ใจว่าการตรวจสอบโปรโตคอล IMAP เปิดใช้งานอยู่เพื่อให้โมดูลทำงานได้อย่างถูกต้อง การควบคุมโปรโตคอล IMAP จะดำเนินการโดยอัตโนมัติโดยไม่จำเป็นต้องกำหนดค่าอีเมลไคลเอ็นต์ของคุณใหม่ ตามค่าเริ่มต้น การสื่อสารทั้งหมดในพอร์ต 143 จะถูกสแกน แต่สามารถเพิ่มพอร์ตการสื่อสารอื่นๆ ได้ตามจำเป็น ต้องคั่นเลขที่พอร์ตด้วยเครื่องหมายจุลภาค

หากเลือก **เปิดใช้งานการตรวจสอบโปรโตคอล IMAP** ระบบจะตรวจสอบการรับส่งข้อมูลผ่าน IMAP ทั้งหมดเพื่อตรวจหาซอฟต์แวร์ที่เป็นอันตราย

อัพเดท

การอัพเดท ESET Cyber Security เป็นประจำเป็นสิ่งจำเป็นเพื่อรักษาระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัพเดทจะดำเนินการให้มั่นใจว่าโปรแกรมนั้นอัพเดทอยู่เสมอโดยการดาวน์โหลดโมดูลการตรวจหาล่าสุด

คลิก **อัพเดท** จากเมนูหลักเพื่อดูสถานะการอัพเดทในปัจจุบันของ ESET Cyber Security รวมไปถึงวันและเวลาของการอัพเดทล่าสุดที่สำเร็จและหากต้องการการอัพเดท หากต้องการเริ่มต้นกระบวนการอัพเดทด้วยตนเอง ให้คลิก **อัพเดทโมดูล**

ในสถานการณ์ปกติ เมื่อดาวน์โหลดรายการอัพเดทอย่างถูกต้องแล้ว ข้อความ **ไม่จำเป็นต้องอัพเดท โมดูลที่ติดตั้งอยู่เป็นข้อมูลปัจจุบัน** จะปรากฏในหน้าต่างการอัพเดท หากไม่สามารถอัพเดทโมดูลได้ เราขอแนะนำให้คุณตรวจสอบ การตั้งค่าการอัพเดท - สาเหตุทั่วไปส่วนใหญ่สำหรับข้อผิดพลาดนี้คือข้อมูลการตรวจสอบสิทธิ์ที่ป้อนไม่ถูกต้อง (ชื่อผู้ใช้และรหัสผ่าน) หรือกำหนดค่าไม่ถูกต้อง การตั้งค่าการเชื่อมต่อ

หน้าต่างอัพเดทจะมีหมายเลขเวอร์ชันกลไกตรวจหาด้วย หมายเลขเวอร์ชันจะเชื่อมโยงไปยังหน้าเว็บ ESET ที่แสดงรายการข้อมูลของการอัพเดทกลไกตรวจหา

การตั้งค่าการอัพเดท

เมื่อต้องการลบข้อมูลการอัพเดทที่เก็บไว้ชั่วคราวทั้งหมด ให้คลิกปุ่ม **ล้าง** ที่อยู่ถัดจาก **ล้างแคชการอัพเดท** ใช้ตัวเลือกนี้ถ้าคุณพบปัญหาในระหว่างการอัพเดท

ตัวเลือกขั้นสูง

ในการปิดใช้งานการแจ้งเตือนที่แสดงหลังจากการอัพเดทสำเร็จแต่ละครั้ง ให้เลือก **ไม่แสดงการแจ้งเตือนเกี่ยวกับอัพเดทที่สำเร็จ**

เปิดใช้งาน **การอัพเดทก่อนออก** เพื่อดาวน์โหลดโมดูลการพัฒนาที่อยู่ในช่วงการทดสอบขั้นสุดท้าย การอัพเดทก่อนออกมักจะมีการแก้ไขปัญหาผลิตภัณฑ์หลายรายการ **การอัพเดทที่ล่าช้า** จะดาวน์โหลดการอัพเดทหลังจากที่มีการเผยแพร่การอัพเดทแล้วสองสามชั่วโมง เพื่อให้แน่ใจว่าลูกค้าจะไม่ได้รับการอัพเดทจนกว่าจะยืนยันว่าไม่มีปัญหาที่เกี่ยวกับไวรัสที่ยังไม่ถูกตรวจสอบ

ESET Cyber Security จะบันทึกสแนปช็อตของกลไกตรวจหาและโมดูลโปรแกรมเพื่อใช้กับคุณลักษณะ **การย้อนกลับ**

การอัพเดท ปล่อยให้ **สร้างสแนปช็อตของไฟล์อัพเดท** เปิดใช้งานไว้เพื่อให้ ESET Cyber Security บันทึกสแนปช็อตเหล่านี้โดยอัตโนมัติ หากคุณสงสัยว่าโมดูลการตรวจหาตัวใหม่และ/หรือการอัพเดทโมดูลโปรแกรมอาจไม่เสถียรหรือเสียหาย คุณสามารถใช้คุณลักษณะการย้อนกลับเพื่อย้อนเป็นเวอร์ชันก่อนหน้าและปิดใช้งานการอัพเดทสำหรับช่วงเวลาที่ตั้งค่าไว้ได้ หากต้องการคืนค่าอัพเดทให้เป็นเวอร์ชั่นที่เก่าสุดในประวัติ ให้คลิก **การย้อนกลับ** หรืออีกวิธีหนึ่ง คุณสามารถเปิดใช้งานการอัพเดทที่ปิดใช้งานไว้ก่อนหน้านั้นในกรณีที่คุณได้เลื่อนการอัพเดทไว้อย่างไม่มีกำหนด เมื่อใช้ใช้คุณลักษณะการย้อนกลับการอัพเดทเพื่อย้อนเป็นเวอร์ชันก่อนหน้า ให้ใช้เมนูแบบเลื่อนลง **ตั้งช่วงเวลาระงับเป็น** เพื่อระบุช่วงเวลาสำหรับรายการที่คุณต้องการระงับการอัพเดท หากคุณเลือก **จนกว่าจะยกเลิก** การอัพเดทปกติจะไม่ทำงานต่อจนกว่าคุณจะเรียกคืนการอัพเดทด้วยตนเอง คลิก **อนุญาต** โปรดใช้ความระมัดระวังเมื่อตั้งค่าช่วงเวลาเพื่อระงับการอัพเดท

ตั้งค่าอายุสูงสุดของกลไกการตรวจจับโดยอัตโนมัติ – อนุญาตให้คุณกำหนดระยะเวลาสูงสุด (เป็นวัน) ก่อนที่โมดูลการตรวจจับจะถูกรายงานว่าไม่อัพเดท ค่าเริ่มต้นคือ 7 วัน

วิธีสร้างงานการอัพเดท

คุณสามารถเรียกการอัพเดทได้ด้วยตนเองโดยคลิก **อัพเดท** จากเมนูหลัก จากนั้นคลิก **อัพเดทโมดูล**

การอัพเดทสามารถเรียกใช้เป็นงานตามกำหนดการ เมื่อต้องการกำหนดค่างานตามกำหนดการ ให้คลิก **เครื่องมือ** > **เครื่องมือวางกำหนดการ** ตามค่าเริ่มต้น งานต่อไปนี้จะเปิดใช้ใน ESET Cyber Security:

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

งานการอัพเดทแต่ละงานจะสามารถแก้ไขได้เพื่อให้เหมาะกับความต้องการของคุณ นอกเหนือจากงานการอัพเดทเริ่มต้นแล้ว คุณสามารถสร้างงานการอัพเดทใหม่ด้วยการกำหนดค่าที่ผู้ใช้กำหนดได้ สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการสร้างและการกำหนดค่างานการอัพเดท โปรดดูที่ส่วน เครื่องมือวางกำหนดการ

การอัพเกรด ESET Cyber Security เป็นเวอร์ชันใหม่

เพื่อให้มีการป้องกันสูงสุด สิ่งสำคัญคือจะต้องใช้ ESET Cyber Security รุ่นล่าสุด หากต้องการตรวจสอบเวอร์ชันใหม่ให้คลิก **หน้าแรก** จากเมนูหลัก ถ้ามีรุ่นใหม่ที่ใช้ได้ ระบบจะแสดงข้อความ คลิก **เรียนรู้เพิ่มเติม...** เพื่อแสดงหน้าต่างใหม่ที่มีหมายเลขเวอร์ชันของรุ่นใหม่และบันทึกการเปลี่ยนแปลง

คลิก **ใช่** เพื่อดาวน์โหลดรุ่นล่าสุด หรือคลิก **ข้ามไปก่อน** เพื่อปิดหน้าต่าง และดาวน์โหลดการอัพเกรดในภายหลัง

หากคุณคลิก **ใช่** ไฟล์จะถูกดาวน์โหลดไปยังโฟลเดอร์การดาวน์โหลดของคุณ (หรือโฟลเดอร์เริ่มต้นที่ตั้งขึ้นโดยเบราว์เซอร์ของคุณ) เมื่อเสร็จสิ้นการดาวน์โหลดไฟล์ ให้เริ่มต้นไฟล์และดำเนินการตามคำแนะนำการติดตั้ง ชื่อผู้ใช้และรหัสผ่านของคุณจะถูกโอนไปยังการติดตั้งใหม่โดยอัตโนมัติ ขอแนะนำให้คุณตรวจสอบการอัพเกรดเป็นประจำ โดยเฉพาะเมื่อติดตั้ง ESET Cyber Security จากซีดี/ดีวีดี

อัพเดทระบบ

คุณสมบัติรายการอัพเดทระบบ macOS คือส่วนประกอบที่สำคัญที่ออกแบบมาเพื่อปกป้องผู้ใช้จากซอฟต์แวร์ที่เป็นอันตราย สำหรับความปลอดภัยสูงสุด เราขอแนะนำให้คุณติดตั้งการอัพเดทเหล่านี้ทันทีเมื่อตัวอัพเดทสามารถใช้งานได้ ESET Cyber Security จะแจ้งให้คุณทราบเกี่ยวกับการอัพเดทที่ขาดหายไปโดยขึ้นอยู่กับระดับที่คุณระบุ คุณสามารถปรับความพร้อมใช้งานของการแจ้งเตือนการอัพเดทใน **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** (หรือกด *cmd+,*) > **การเตือนและการแจ้งเตือน > การตั้งค่า...** โดยการเปลี่ยนตัวเลือก **แสดงเงื่อนไข** ที่อยู่ถัดจาก **อัพเดทระบบปฏิบัติการ**

- **แสดงตัวอีพเดททั้งหมด** - การแจ้งเตือนจะถูกแสดงในเวลาใดก็ตามที่ตัวอัพเดทระบบขาดหายไป
- **แสดงเฉพาะที่แนะนำ** - คุณจะได้รับแจ้งเกี่ยวกับการอัพเดทที่แนะนำเท่านั้น

หากคุณไม่ต้องการได้รับการแจ้งเตือนเกี่ยวกับตัวอัพเดทที่ขาดหายไป ให้ยกเลิกการเลือกที่กล่องกาเครื่องหมายที่อยู่ถัดจาก **อัพเดทระบบปฏิบัติการ**

หน้าต่างการแจ้งเตือนจะช่วยให้คุณมีภาพรวมของรายการอัพเดทที่มีให้ใช้งานได้ของระบบปฏิบัติการและแอปพลิเคชันที่อัพเดทผ่านเครื่องมือที่ให้มาพร้อม macOS อย่างรายการอัพเดทซอฟต์แวร์ คุณสามารถใช้งานการอัพเดทได้โดยตรงจากหน้าต่างการแจ้งเตือนหรือจาก **หน้าแรก** ของ ESET Cyber Security โดยคลิก **ติดตั้งตัวอัพเดทที่ขาดหายไป**

หน้าต่างการแจ้งเตือนประกอบด้วยชื่อแอพพลิเคชัน เวอร์ชัน ขนาด คุณสมบัติ (ติดธง) และข้อมูลเพิ่มเติมเกี่ยวกับตัวอัพเดทที่สามารถใช้งานได้ คอลัมน์ติดธงประกอบด้วยข้อมูลต่อไปนี้:

- [**ที่แนะนำ**] - ผู้ผลิตระบบปฏิบัติการแนะนำให้คุณติดตั้งตัวอัพเดทนี้เพื่อเพิ่มความปลอดภัยและความเสถียรของระบบ
- [**รีสตาร์ท**] - ต้องการการรีสตาร์ทคอมพิวเตอร์ในการติดตั้งต่อไปนี้

• [**ปิดระบบ**] - ต้องคอมพิวเตอร์จากนั้นเปิดอีกครั้งในการติดตั้งต่อไปนี้

หน้าต่างการแจ้งเตือนจะแสดงตัวอัพเดทที่ได้รับโดยเครื่องมือบรรทัดคำสั่งที่เรียกว่า 'การอัพเดทซอฟต์แวร์' ตัวอัพเดทที่ได้รับโดยเครื่องมือนี้สามารถเป็นได้หลากหลายจากตัวอัพเดทที่แสดงโดยแอพพลิเคชัน 'การอัพเดทซอฟต์แวร์' หากคุณต้องการติดตั้งตัวอัพเดทที่สามรถใช้งานได้ที่แสดงในหน้าต่าง 'การอัพเดทระบบที่ขาดหายไป' และการอัพเดทที่ไม่แสดงโดยแอพพลิเคชัน 'การอัพเดทซอฟต์แวร์' คุณต้องใช้เครื่องมือบรรทัดคำสั่ง 'การอัพเดทซอฟต์แวร์' หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับเครื่องมือนี้ ให้อ่านคู่มือ 'การอัพเดทซอฟต์แวร์' โดยพิมพ์ man softwareupdate ลงในหน้าต่างปลายทาง เราขอแนะนำสิ่งนี้สำหรับผู้ใช้ขั้นสูงเท่านั้น

เครื่องมือ

เมนู **เครื่องมือ** รวมถึงโมดูลที่ช่วยทำให้การดูแลโปรแกรมง่ายขึ้นและเสนอตัวเลือกเพิ่มเติมสำหรับผู้ใช้ขั้นสูง

ไฟล์บันทึก

ไฟล์บันทึกมีข้อมูลเกี่ยวกับกิจกรรมโปรแกรมที่สำคัญที่ได้เกิดขึ้นและให้ภาพรวมของภัยคุกคามที่ตรวจพบ การบันทึกจะทำหน้าที่เป็นเครื่องมือที่จำเป็นในการวิเคราะห์ระบบ การตรวจจับภันคุกคามและการแก้ไขปัญหา การบันทึกจะดำเนินการอย่างแข็งขันในพื้นหลังโดยปราศจากการโต้ตอบของผู้ใช้ ข้อมูลจะถูกบันทึกโดยขึ้นอยู่กับการตั้งค่าการใช้บันทึกฟุ่มเฟือยในปัจจุบัน อาจเป็นไปได้ในการดูข้อความตัวอักษรและบันทึกโดยตรงจากสภาพแวดล้อมของ ESET Cyber Security รวมถึงบันทึกถาวร

คุณสามารถเข้าถึงไฟล์บันทึกได้จากเมนูหลักของ ESET Cyber Security โดยคลิก **เครื่องมือ** > **บันทึก** เลือกประเภทของบันทึกที่ต้องการโดยใช้เมนูแบบหล่นลง **บันทึก** ที่ด้านบนของหน้าต่าง บันทึกต่อไปนี้สามารถใช้ได้:

1. **ตรวจพบภัยคุกคาม** - ใช้ตัวเลือกนี้เพื่อดูข้อมูลเกี่ยวกับกิจกรรมทั้งหมดที่เกี่ยวข้องกับการตรวจจับการแทรกซึม
2. **เหตุการณ์** - ตัวเลือกนี้ออกแบบมาเพื่อช่วยให้ผู้ดูแลและผู้ใช้แก้ไขปัญหาได้ การทำงานที่สำคัญที่ดำเนินการโดย ESET Cyber Security จะถูกบันทึกไว้ในบันทึกกิจกรรม
3. **สแกนคอมพิวเตอร์** - ผลลัพธ์ของการสแกนที่เสร็จสิ้นทั้งหมดจะถูกแสดงในบันทึกนี้ คลิกสองครั้งที่รายการใด ๆ เพื่อดูรายละเอียดของการสแกนคอมพิวเตอร์ตามต้องการตามลำดับ
4. **เว็บไซต์ที่กรอง** - รายการนี้มีประโยชน์เมื่อคุณต้องการดูรายการเว็บไซต์ที่ถูกปิดกั้นโดยการป้องกันการเข้าถึง

เว็บ ในบันทึกเหล่านี้ คุณจะเห็นเวลา, URL, สถานะ, IP address, ผู้ใช้ และแอพพลิเคชันที่เปิดการเชื่อมต่อกับเว็บไซต์หนึ่ง

ในแต่ละส่วน คุณสามารถคัดลอกข้อมูลที่แสดงไปยังคลิปบอร์ดได้โดยการเลือกที่รายการแล้วคลิกที่ปุ่ม **Copy**

การบำรุงรักษาการบันทึก

การกำหนดค่าการบันทึกสำหรับ ESET Cyber Security สามารถเข้าถึงได้จากหน้าต่างโปรแกรมหลัก คลิก **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน** (หรือกด *cmd+,*) > **ไฟล์บันทึก** คุณสามารถระบุตัวเลือกต่อไปนี้สำหรับไฟล์บันทึก:

- **ลบการบันทึกเก่าโดยอัตโนมัติ** - รายการบันทึกที่เก่ากว่าจำนวนวันที่ระบุไว้จะถูกลบโดยอัตโนมัติ (90 วัน เป็นค่าเริ่มต้น)
- **ปรับปรุงประสิทธิภาพไฟล์บันทึกโดยอัตโนมัติ** - เปิดใช้งานการจัดระเบียบไฟล์บันทึกอัตโนมัติหากเกินจำนวนร้อยละของการบันทึกที่ไม่ได้ใช้ที่ระบุไว้ (25% เป็นค่าเริ่มต้น)

ข้อมูลที่เกี่ยวข้องทั้งหมดที่แสดงในส่วนติดต่อผู้ใช้ ข้อความภัยคุกคามและเหตุการณ์สามารถเก็บไว้ในรูปแบบข้อความที่คนอ่านได้ เช่น ข้อความธรรมดา หรือ CSV (Comma-separated values) หากคุณต้องการทำให้ไฟล์เหล่านี้สามารถประมวลผลได้โดยใช้เครื่องมือของบริษัทอื่น ให้คลิกเลือกช่องทำเครื่องหมายถัดจาก **เปิดใช้งานการบันทึกไฟล์ข้อความ**

ในการกำหนดโฟลเดอร์เป้าหมายที่จะบันทึกไฟล์บันทึก ให้คลิก **การตั้งค่า** ถัดจาก **ตัวเลือกขั้นสูง**

ขึ้นอยู่กับตัวเลือกที่เลือกใต้ **ไฟล์บันทึกข้อความ: แก้ไข** คุณสามารถบันทึกรายการบันทึกด้วยข้อมูลที่เขียนไว้ต่อไปนี้:

- เหตุการณ์ต่างๆ เช่น ชื่อผู้ใช้และรหัสผ่านไม่ถูกต้อง, ไม่สามารถอัพเดทโมดูลได้ เป็นต้น จะถูกเขียนลงในไฟล์ eventslog.txt
- ภัยคุกคามที่ตรวจพบโดยเครื่องมือสแกนเมื่อเริ่มต้น การป้องกันแบบเรียลไทม์ หรือการสแกนคอมพิวเตอร์ จะถูกเก็บไว้ในไฟล์ชื่อ threatslog.txt
- ผลลัพธ์ของการสแกนที่เสร็จสมบูรณ์แล้วทั้งหมดจะถูกบันทึกไว้ในรูปแบบ scanlog.ตัวเลข.txt

ในการกำหนดค่าตัวกรองสำหรับ **รายการบันทึกการสแกนคอมพิวเตอร์เริ่มต้น** ให้คลิก **แก้ไข** แล้วเลือก/ยกเลิกการเลือกประเภทรายการบันทึกตามต้องการ คำอธิบายเพิ่มเติมเรื่องประเภทรายการบันทึกเหล่านี้สามารถพบได้ใน การกรองบันทึก

การกรองบันทึก

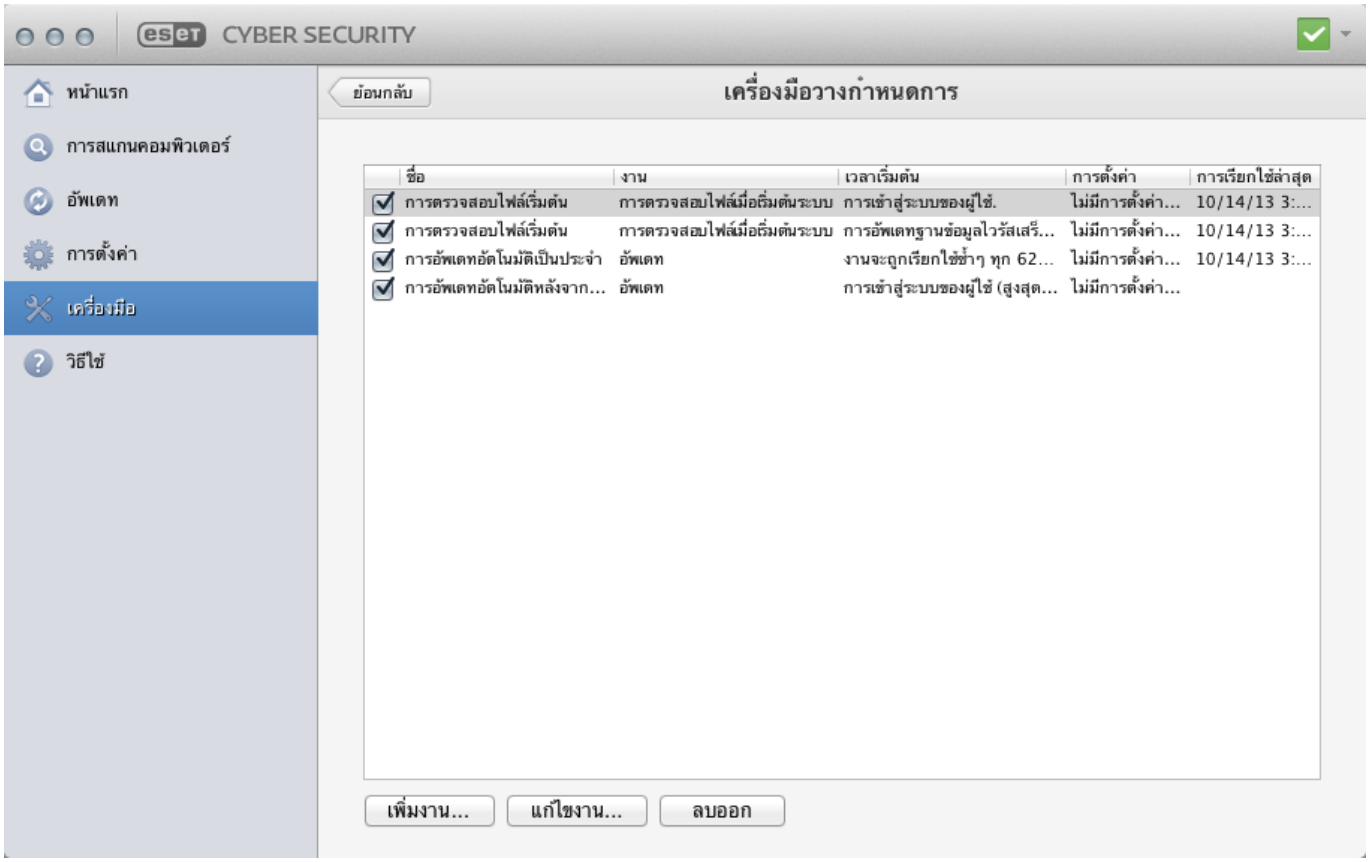
บันทึกจะเก็บข้อมูลเกี่ยวกับเหตุการณ์ของระบบที่มีความสำคัญ คุณลักษณะการกรองบันทึกช่วยให้คุณแสดงบันทึกเกี่ยวกับเหตุการณ์ประเภทที่ระบุ

ประเภทของบันทึกที่ใช้บ่อยมีดังนี้

- **คำเตือนที่ร้ายแรง** - ข้อผิดพลาดของระบบที่ร้ายแรง (เช่น การป้องกันไวรัสไม่เริ่มต้นทำงาน)
- **ข้อผิดพลาด** - ข้อความแสดงข้อผิดพลาด เช่น "เกิดข้อผิดพลาดขณะดาวน์โหลดไฟล์" และข้อผิดพลาดร้ายแรง
- **คำเตือน** - ข้อความแสดงคำเตือน
- **บันทึกเพื่อแจ้งข้อมูล**- ข้อความแจ้งข้อมูล รวมถึงการอัพเดทที่เสร็จสมบูรณ์ การเตือน เป็นต้น
- **บันทึกเพื่อการวินิจฉัย** - ข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรมและการบันทึกทั้งหมดที่อธิบายไว้ที่ด้านบน

เครื่องมือวางกำหนดการ

เครื่องมือวางกำหนดการ สามารถพบได้ในเมนูหลักของ ESET Cyber Security ภายใต้ **เครื่องมือ เครื่องมือวางกำหนดการ** มีรายการงานตามกำหนดการทั้งหมด และคุณสมบัติของการกำหนดค่า เช่น วันที่ที่กำหนดไว้ล่วงหน้า เวลา และโปรไฟล์การสแกนที่ใช้



เครื่องมือวางกำหนดการจะจัดการและเรียกใช้งานตามกำหนดการโดยใช้การกำหนดค่าและคุณสมบัติที่กำหนดไว้ล่วงหน้า การกำหนดค่าและคุณสมบัติจะมีข้อมูลต่างๆ เช่น วันที่และเวลา ตลอดจนโปรไฟล์ที่ระบุให้ใช้ระหว่างการเรียกใช้งาน

ตามค่าเริ่มต้น งานตามกำหนดการต่อไปนี้จะปรากฏในเครื่องมือวางกำหนดการ:

- การบำรุงรักษาบันทึก (หลังจากเปิดใช้งานตัวเลือก **แสดงงานของระบบ** ในการตั้งค่าเครื่องมือวางกำหนดการ)
- การตรวจสอบไฟล์เมื่อเริ่มต้นหลังจากการเข้าสู่ระบบของผู้ใช้
- การตรวจสอบไฟล์เมื่อเริ่มต้นระบบหลังจากการอัพเดทโมดูลการตรวจหาเสร็จสมบูรณ์
- การอัพเดทอัตโนมัติเป็นประจำ
- การอัพเดทอัตโนมัติหลังจากผู้ใช้เข้าสู่ระบบ

เมื่อต้องการแก้ไขการกำหนดค่าของงานตามกำหนดการที่มีอยู่ (ทั้งค่าเริ่มต้นและที่ผู้ใช้กำหนด) ให้กด CTRL และคลิกที่งานที่คุณต้องการแก้ไขแล้วเลือก **แก้ไข** หรือเลือกงานนั้นและคลิก **แก้ไขงาน**

การสร้างงานใหม่

ในการสร้างงานใหม่ในเครื่องมือวางกำหนดการ ให้คลิก **เพิ่มงาน...** หรือ CTRL+click ในช่วงว่างแล้วเลือก **เพิ่ม...** จากเมนูบริบท งานตามกำหนดการที่ใช้ได้มีห้าประเภท:

- **เรียกใช้แอพพลิเคชัน**
- **อัพเดท**
- **การบำรุงรักษาการบันทึก**
- **การสแกนคอมพิวเตอร์ตามต้องการ**
- **การตรวจสอบไฟล์เมื่อเริ่มต้น**

เรียกใช้แอพพลิเคชัน

คุณสามารถเปิดทำงานโปรแกรมเป็นผู้ใช้ระบบที่เรียกว่า "nobody" โดยการเลือก **เปิดทำงานแอพพลิเคชัน** สิทธิ์อนุญาตสำหรับการเรียกใช้งานแอปพลิเคชันผ่านตัวกำหนดเวลาได้ถูกกำหนดโดย macOS เมื่อต้องการเปลี่ยนผู้ใช้จากค่าเริ่มต้น ให้พิมพ์ชื่อผู้ใช้ตามด้วยเครื่องหมายโคลอน (:) ที่ด้านหน้าของคำสั่ง คุณยังสามารถใช้ผู้ใช้ **รูท** ในคุณลักษณะนี้ได้อีกด้วย

ตัวอย่าง: เรียกใช้งานในฐานะผู้ใช้

ในตัวอย่างนี้ เราจะวางกำหนดการให้แอพเครื่องคิดเลขเริ่มต้นในเวลาที่เลือกในฐานะผู้ใช้ที่มีชื่อว่า **UserOne**:

1. ใน **เครื่องมือวางกำหนดการ** ให้เลือก **เพิ่มงาน**
2. พิมพ์ข้อมูลลงในชื่องาน เลือก **เรียกใช้แอพพลิเคชัน** เป็น **งานตามกำหนดการ** ในหน้าต่าง **เรียกใช้งาน** ให้เลือก **หนึ่งครั้ง** เพื่อเรียกใช้งานนี้เพียงครั้งเดียว คลิก **ถัดไป**
3. คลิกเรียกดู แล้วเลือกแอพเครื่องคิดเลข
4. พิมพ์ **UserOne:** ที่หน้าพาธของแอพพลิเคชัน (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') แล้วคลิก **ถัดไป**
5. เลือกเวลาที่จะเรียกใช้งานนี้ แล้วคลิก **ถัดไป**
6. เลือกตัวเลือกอื่นหากไม่สามารถเรียกใช้งานได้ แล้วคลิก **ถัดไป**
7. คลิก **เสร็จสิ้น**
8. เครื่องมือวางกำหนดการของ ESET จะเริ่มต้นแอพเครื่องคิดเลขในเวลาที่คุณเลือก

ตัวอย่าง: งานการอัพเดท

คุณสามารถสแกนไดเรกทอรีต่างๆ ในฐานะเจ้าของไดเรกทอรีได้:

1. จากเมนูแบบหล่นลง **งานที่มีกำหนดการ** เลือก **อัพเดท**
2. ป้อนชื่องานลงในช่อง **ชื่องาน**
3. เลือกความถี่ของงานจากเมนูแบบเลื่อนลง **เรียกใช้งาน** คุณจะได้รับแจ้งให้ระบุพารามิเตอร์การอัพเดทอื่น โดยอ้างอิงจากความถี่ที่เลือก หากคุณเลือก **ผู้ใช้กำหนด** คุณจะได้รับแจ้งให้ระบุวันที่/เวลาในรูปแบบครอน (ดูที่ส่วน การสร้างงานแบบผู้ใช้กำหนด สำหรับรายละเอียดเพิ่มเติม)
4. ในขั้นตอนต่อไป ให้ระบุการกระทำที่จะใช้หากไม่สามารถดำเนินงานหรือไม่สามารถทำให้เสร็จตามเวลาที่กำหนดไว้ได้
5. ในขั้นตอนสุดท้าย หน้าต่างเนื้อหาสรุปที่มีข้อมูลเกี่ยวกับงานที่มีกำหนดการปัจจุบันจะแสดงขึ้น คลิก **เสร็จสิ้น** งานตามกำหนดการใหม่จะถูกเพิ่มในรายการของงานตามกำหนดการปัจจุบัน

โดยค่าเริ่มต้นแล้ว ESET Cyber Security จะมีงานที่มีกำหนดการล่วงหน้าเพื่อทำให้แน่ใจในความสามารถในการทำงานของผลิตภัณฑ์ที่ถูกต้อง งานเหล่านี้ไม่ควรมีการแก้ไขและจะถูกซ่อนตามค่าเริ่มต้น ในการทำให้งานเหล่านี้สามารถมองเห็นได้ จากเมนูหลัก ให้คลิก **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** (หรือกด *cmd+,*) > **เครื่องมือวางกำหนดการ** แล้วเลือก **แสดงงานระบบ**

การสแกนในฐานะเจ้าของไดเรกทอรี

คุณสามารถสแกนไดเรกทอรีต่างๆ ในฐานะเจ้าของไดเรกทอรีได้:

```
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -
f %u "$VOLUME"` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan' -
f /tmp/scan_log "$VOLUME"; done
```

คุณยังสามารถสแกนโฟลเดอร์ `/tmp` ในฐานะผู้ใช้ที่ล็อกอินในปัจจุบันได้อีกด้วย:

```
root:sudo -u \#`stat -f %u /dev/console` '/แอพพลิ
เคชัน/ESET Cyber Security.app/Contents/MacOS/esets_scan' /tmp
```

การสร้างงานที่ผู้ใช้กำหนด

วันที่และเวลาของงานที่ **ผู้ใช้กำหนด** ต้องป้อนในรูปแบบ cron แบบขยายปี (สตริงที่ประกอบด้วยฟิลด์ 6 ฟิลด์ คั่นด้วยช่องว่าง):

```
นาที(0-59) ชั่วโมง(0-23) วันที่ของเดือน(1-31) เดือน(1-12) ปี(1970-2099) วันที่ของสัปดาห์(0-7)(วันอาทิตย์ = 0 หรือ 7)
```

ตัวอย่าง:

```
30 6 22 3 2012 4
```

อักขระพิเศษมีการสนับสนุนในนิพจน์ของ cron:

- เครื่องหมายดอกจัน (`*`) - นิพจน์จะตรงกับค่าทั้งหมดของฟิลด์ เช่น เครื่องหมายดอกจันในฟิลด์ที่ 3 (วันที่ของเดือน) หมายถึงทุกวัน
- เครื่องหมายขีดกลาง (`-`) - กำหนดช่วง เช่น `3-9`

• เครื่องหมายคอมมา (,) - แบ่งตัวเลขของรายการ เช่น 1,3,7,8

• เครื่องหมายสแลช (/) - กำหนดการเพิ่มของช่วง เช่น 3-28/5 ในฟิลด์ที่ 3 (วันที่ของเดือน) หมายถึงวันที่ 3 ของเดือน หลังจากนั้นจะเป็นทุก 5 วัน

ไม่สนับสนุนชื่อวัน (Monday-Sunday) และชื่อเดือน (January-December)

การเรียกใช้คำสั่ง
ถ้าคุณกำหนดทั้งวันที่ของเดือนและวันที่ของสัปดาห์คำสั่งจะถูกเรียกใช้ต่อเมื่อค่าตรงกับทั้งสองฟิลด์นี้

กักเก็บ

หน้าที่หลักของการกักเก็บก็คือการเก็บไฟล์ที่ติดไวรัสไว้ในที่ปลอดภัย ไฟล์ควรมีการกักเก็บถ้าไม่สามารถล้างไวรัสได้ ถ้าไม่ปลอดภัยหรือไม่ควรลบไฟล์เหล่านี้ หรือถ้ามีการตรวจพบด้วยความผิดพลาดโดย ESET Cyber Security

คุณสามารถเลือกที่จะกักเก็บไฟล์ได้ ซึ่งเป็นตัวเลือกที่แนะนำ ถ้าไฟล์ทำงานน่าสงสัยแต่ไม่มีการตรวจพบโดยเครื่องมือสแกนป้องกันไวรัส ไฟล์ที่ถูกกักเก็บจะสามารถส่งเพื่อรับการวิเคราะห์ที่แล็บภัยคุกคามของ ESET

ไฟล์ที่เก็บไว้ในโฟลเดอร์การกักเก็บนั้นสามารถดูได้ในตารางที่แสดงวันที่และเวลาของการกักเก็บ พาธไปยังตำแหน่งดั้งเดิมของไฟล์ที่ติดไวรัส ขนาดเป็นไบต์ สาเหตุ (เช่น เพิ่มโดยผู้ใช้...) และจำนวนภัยคุกคาม (เช่น ถ้าเป็นอาร์ไคฟ์ที่มีการแฝงตัวหลายรายการ) โฟลเดอร์การกักเก็บที่มีไฟล์ที่กักเก็บ () จะอยู่ในระบบแม้ว่าจะถอนการติดตั้ง ESET Cyber Security แล้ว ไฟล์ที่กักเก็บจะถูกเก็บไว้ในรูปแบบที่เข้ารหัสที่ปลอดภัย และสามารถเรียกคืนได้อีกครั้งหลังจากติดตั้ง ESET Cyber Security

การกักเก็บไฟล์

ESET Cyber Security จะกักเก็บไฟล์ที่ถูกลบให้โดยอัตโนมัติ (หากคุณไม่ได้ยกเลิกการเลือกตัวเลือกนี้ในหน้าต่างการเตือน) คุณสามารถกักเก็บไฟล์ใดๆ ที่น่าสงสัยด้วยตนเองได้โดยคลิก **กักเก็บ...** . เมนูบริบทสามารถใช้สำหรับวัตถุประสงค์นี้ได้เช่นกัน กด ctrl และคลิกช่องว่าง เลือก **กักเก็บ** แล้วเลือกไฟล์ที่คุณต้องการกักเก็บ จากนั้นคลิก **เปิด**

การเรียกคืนจากการกักเก็บ

ไฟล์ที่กักเก็บยังสามารถเรียกคืนไปยังตำแหน่งเดิมของไฟล์ได้ หากต้องการดำเนินการเช่นนั้น ให้เลือกไฟล์ที่กักเก็บ แล้วคลิก **เรียกคืน** การเรียกคืนจะยังมีให้ใช้งานจากเมนูบริบท กด CTRL และคลิกไฟล์ที่มีให้ในหน้าต่างกักเก็บ แล้วคลิก **เรียกคืน** นอกจากนี้เมนูบริบทยังมีตัวเลือก **เรียกคืนไปที่...** ซึ่งช่วยให้คุณสามารถเรียกคืนไฟล์ไปยังตำแหน่งอื่นนอกเหนือจากตำแหน่งที่ถูกลบได้

การส่งไฟล์จากการกักเก็บ

หากคุณได้กักเก็บไฟล์ที่น่าสงสัยที่ไม่ได้ตรวจพบโดยโปรแกรม หรือหากไฟล์ถูกประเมินว่าติดไวรัสโดยไม่ถูกต้อง (เช่น โดยการวิเคราะห์พฤติกรรมของรหัส) และมีการกักเก็บหลังจากนั้น โปรดส่งไฟล์ไปยังแล็บภัยคุกคามของ ESET หากต้องการส่งไฟล์จากการกักเก็บ ให้กด CTRL และคลิกที่ไฟล์ แล้วเลือก **ส่งไฟล์เพื่อวิเคราะห์** จากเมนูบริบท

กระบวนการที่ทำงานอยู่

รายการ **กระบวนการที่ทำงานอยู่** จะแสดงกระบวนการที่ทำงานอยู่ในคอมพิวเตอร์ของคุณ ซึ่ง ESET Cyber Security จะให้ข้อมูลอย่างละเอียดเกี่ยวกับกระบวนการที่ทำงานอยู่ เพื่อคุ้มครองผู้ใช้ด้วยเทคโนโลยี ESET Live Grid

- **กระบวนการ** - ชื่ออิมเมจของกระบวนการที่ทำงานอยู่บนคอมพิวเตอร์ในขณะนี้ ในการดูกระบวนการที่ทำงานอยู่ทั้งหมด คุณสามารถใช้ Activity Monitor (อยู่ใน */Applications/Utilities*)
- **ระดับความเสี่ยง** - ในกรณีส่วนใหญ่ ESET Cyber Security และเทคโนโลยี ESET Live Grid จะกำหนดระดับความเสี่ยงให้กับวัตถุ (ไฟล์ กระบวนการ เป็นต้น) โดยใช้ชุดกฎการวิเคราะห์พฤติกรรมที่ตรวจสอบลักษณะของวัตถุแต่ละรายการ จากนั้นจะชั่งน้ำหนักของโอกาสที่จะเป็นกิจกรรมที่เป็นอันตราย จากการวิเคราะห์พฤติกรรมเหล่านี้จะมีการกำหนดระดับความเสี่ยงให้กับวัตถุ แอพพลิเคชันที่รู้จักและมีเครื่องหมายสีเขียวแสดงว่ามีความปลอดภัย (อยู่ในรายการที่ปลอดภัย) และจะไม่รวมในการสแกน ซึ่งจะช่วยเพิ่มความเร็วของการสแกนตามความต้องการและการสแกนแบบเรียลไทม์ เมื่อทำเครื่องหมายแอพพลิเคชันว่า ไม่ทราบ (สีเหลือง) ไม่ได้หมายความว่าจะเป็นซอฟต์แวร์ที่เป็นอันตรายเสมอไป โดยปกติแล้วจะเป็นแอพพลิเคชันใหม่ หากคุณไม่แน่ใจเกี่ยวกับไฟล์ คุณสามารถส่งไฟล์ไปยังแล็บภัยคุกคาม ESET เพื่อวิเคราะห์ได้ หากตรวจพบว่าไฟล์เป็นแอพพลิเคชันที่เป็นอันตราย สัญลักษณ์ของไฟล์นี้จะถูกเพิ่มในการอัพเดทหนึ่งที่กำลังจะมีขึ้น

- **จำนวนผู้ใช้** - จำนวนผู้ใช้ที่ใช้แอพพลิเคชันที่มีให้ ข้อมูลนี้จะถูกรวบรวมโดยเทคโนโลยี ESET Live Grid
- **เวลาที่พบ** - ระยะเวลานับจากเทคโนโลยี ESET LiveGrid® พบแอพพลิเคชัน
- **ID ของชุดแอพพลิเคชัน** - ชื่อของผู้ขายหรือกระบวนการแอพพลิเคชัน

เมื่อคลิกที่กระบวนการ ข้อมูลต่อไปนี้จะปรากฏที่ด้านล่างของหน้าต่าง:

- **ไฟล์** - ตำแหน่งของแอพพลิเคชันในคอมพิวเตอร์ของคุณ
- **ขนาดไฟล์** - ขนาดทางกายภาพของไฟล์บนดิสก์
- **คำอธิบายไฟล์** - ลักษณะของไฟล์ตามคำอธิบายของระบบปฏิบัติการ
- **ID ของชุดแอพพลิเคชัน** - ชื่อของผู้ขายหรือกระบวนการแอพพลิเคชัน
- **เวอร์ชันของไฟล์** - ข้อมูลจากผู้เผยแพร่แอพพลิเคชัน
- **ชื่อผลิตภัณฑ์** - ชื่อแอพพลิเคชันและ/หรือชื่อทางธุรกิจ

การเชื่อมต่อเครือข่าย

การเชื่อมต่อเครือข่ายเป็นรายการการเชื่อมต่อเครือข่ายที่ใช้งานอยู่ภายในคอมพิวเตอร์ของคุณ ESET Cyber Security ให้ข้อมูลอย่างละเอียดเกี่ยวกับการเชื่อมต่อแต่ละรายการและอนุญาตให้คุณสร้างกฎในการปิดกั้นการเชื่อมต่อเหล่านี้ได้

สร้างกฎการปิดกั้นสำหรับการเชื่อมต่อนี้

ESET Cyber Security อนุญาตให้คุณสร้างกฎการปิดกั้นสำหรับการเชื่อมต่อแต่ละรายการในโปรแกรมจัดการ**การเชื่อมต่อเครือข่าย** คุณสามารถสร้างกฎการปิดกั้นได้โดยคลิกขวาบนการเชื่อมต่อ แล้วเลือก **สร้างกฎการปิดกั้นสำหรับการเชื่อมต่อนี้**

1.เลือก **โปรไฟล์** การเชื่อมต่อที่คุณต้องการสร้างกฎ แล้วป้อนชื่อของกฎนั้น เลือกแอปพลิเคชั่นที่จะใช้กฎ หรือเลือกช่องทำเครื่องหมายเพื่อใช้กฎนั้นกับทุกแอปพลิเคชั่น

2.เลือกการดำเนินการสำหรับการเชื่อมต่อเพื่อปฏิเสธ (ปิดกั้น) หรืออนุญาตการเชื่อมต่อ เลือกทิศทางของการสื่อสารที่จะนำกฎไปใช้ คุณสามารถสร้างไฟล์บันทึกสำหรับกฎได้โดยคลิก **กฎการบันทึก**

3.เลือกโปรโตคอลการเชื่อมต่อและพอร์ตประเภทต่างๆ เลือกพอร์ตสำหรับบริการหรือระบุช่วงของพอร์ตโดยใช้รูปแบบ: จาก-ถึง

4.เลือกปลายทางแล้วป้อนข้อมูลลงในช่องที่จำเป็นตามปลายทางที่คุณเลือก

Live Grid

ระบบการเตือนภัยล่วงหน้า Live Grid จะให้ ESET แจ้งคุณเกี่ยวกับการแทรกซึมใหม่ ๆ โดยทันทีและต่อเนื่องอยู่เสมอ ระบบการเตือนภัยล่วงหน้า Live Grid แบบสองทิศทางมีวัตถุประสงค์เพียงหนึ่งเดียว - เพื่อปรับปรุงการป้องกันที่เราสามารถนำเสนอให้กับคุณได้ วิธีที่ดีที่สุดที่จะทำให้แน่ใจได้ว่าเราจะเห็นภัยคุกคามใหม่ๆ ได้ทันทีเมื่อภัยคุกคามปรากฏคือการ “เชื่อมต่อ“ กับลูกค้าของเราให้มากที่สุดเท่าที่จะทำได้ และให้ลูกค้าสอดแนมภัยคุกคามให้กับเรา คุณลักษณะนี้มีสองตัวเลือก:

1.คุณสามารถเลือกที่จะไม่เปิดใช้งานระบบการเตือนภัยล่วงหน้า Live Grid คุณจะไม่สูญเสียความสามารถในการทำงานใด ๆ จากซอฟต์แวร์ของคุณ และคุณจะยังได้รับการป้องกันที่ดีที่สุดที่พวกเรานำเสนอ

2.คุณสามารถกำหนดค่าระบบการเตือนภัยล่วงหน้า Live Grid เพื่อส่งข้อมูลที่ไม่ระบุชื่อเกี่ยวกับภัยคุกคามใหม่และตำแหน่งที่มีรหัสที่เป็นภัยคุกคามอยู่ คุณสามารถส่งข้อมูลนี้ไปยัง ESET สำหรับการวิเคราะห์อย่างละเอียดได้ การศึกษาภัยคุกคามเหล่านี้จะช่วย ESET อัพเดทกลไกตรวจหาและปรับปรุงความสามารถของโปรแกรมในการตรวจจับภัยคุกคาม

ระบบการเตือนภัยล่วงหน้า Live Grid จะเก็บรวบรวมข้อมูลเกี่ยวกับคอมพิวเตอร์ของคุณที่เกี่ยวกับภัยคุกคามที่เพิ่งตวจพบ ข้อมูลนี้อาจรวมถึงตัวอย่างหรือสำเนาของไฟล์ที่ภัยคุกคามนั้นปรากฏ พาธไปยังไฟล์นั้น ชื่อไฟล์ วันที่และเวลา กระบวนการที่ภัยคุกคามปรากฏบนคอมพิวเตอร์ของคุณ และข้อมูลเกี่ยวกับระบบปฏิบัติการของคอมพิวเตอร์ของคุณ

ในขณะที่มีโอกาสที่สิ่งนี้อาจเปิดเผยข้อมูลบางอย่างเกี่ยวกับคุณหรือคอมพิวเตอร์ของคุณในบางครั้ง (ชื่อผู้ใช้ในเส้นทางไดเร็กเทอรี่อื่น ๆ) ไปยังห้องทดลองภัยคุกคามของ ESET ข้อมูลนี้จะไม่ถูกใช้เพื่อวัตถุประสงค์ใด ๆ นอกจากเพื่อช่วยให้พวกเราตอบสนองต่อภัยคุกคามใหม่ ๆ ได้ทันท่วงที

ในการเข้าถึงการตั้งค่า Live Grid จากเมนูหลัก ให้คลิก **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** (หรือกด *cmd+,*) > **Live Grid** เลือก **เปิดใช้งานระบบการเตือนภัยล่วงหน้า Live Grid** เพื่อเปิดใช้งาน Live Grid จากนั้นคลิก **การตั้งค่า...** ที่อยู่ถัดจาก **ตัวเลือกขั้นสูง**

การตั้งค่า Live Grid

ตามค่าเริ่มต้น ESET Cyber Security จะได้รับการกำหนดค่าเพื่อส่งไฟล์ที่น่าสงสัยไปยังแล็บภัยคุกคามของ ESETเพื่อรับการวิเคราะห์โดยละเอียด หากคุณไม่ต้องการส่งไฟล์เหล่านี้โดยอัตโนมัติ ให้ยกเลิกการเลือก **ส่งไฟล์**

ถ้าคุณพบไฟล์ที่น่าสงสัย คุณสามารถส่งไปยังแล็บภัยคุกคามของเราเพื่อวิเคราะห์ได้ เพื่อทำเช่นนั้น ให้คลิก **เครื่องมือ** > **ส่งตัวอย่างเพื่อวิเคราะห์** จากหน้าต่างหลักของโปรแกรม หากเป็นแอพพลิเคชันที่เป็นอันตราย การตรวจหาแอพพลิเคชันตัวนี้จะถูกเพิ่มในการอัพเดทที่กำลังจะมีขึ้น

ส่งสถิติที่ไม่ระบุชื่อ – ระบบการเตือนล่วงหน้า Live Grid ของ ESET จะเก็บข้อมูลที่ไม่ระบุตัวบุคคลเกี่ยวกับคอมพิวเตอร์ของคุณ ซึ่งเกี่ยวข้องกับภัยคุกคามที่ตรวจพบใหม่ ข้อมูลนี้อาจรวมชื่อของการแฝงตัว วันที่และเวลาที่ตรวจพบ เวอร์ชันของผลิตภัณฑ์การรักษาความปลอดภัยของ ESET เวอร์ชันของระบบปฏิบัติการของคุณ และการตั้งค่าตำแหน่ง โดยทั่วไปแล้ว โปรแกรมจะส่งข้อมูลสถิติไปยังเซิร์ฟเวอร์ของ ESET วันละหนึ่งหรือสองครั้ง

ตัวกรองการยกเว้น – ตัวเลือกนี้จะช่วยให้คุณสามารถยกเว้นไฟล์บางประเภทจากการส่งได้ ตัวอย่างเช่น ตัวเลือกนี้อาจมีประโยชน์สำหรับการยกเว้นไฟล์ที่อาจมีข้อมูลลับเฉพาะ เช่น เอกสารหรือสเปรดชีท ประเภทไฟล์ที่ใช้งานทั่วไปจะถูกยกเว้นตามค่าเริ่มต้น (.doc .rtf เป็นต้น) คุณสามารถเพิ่มประเภทไฟล์ไปยังรายการไฟล์ที่ยกเว้นได้

อีเมลที่ติดต่อได้ (ไม่จำเป็น) – ระบบอาจใช้ที่อยู่อีเมลของคุณในกรณีต้องการข้อมูลเพิ่มเติมเพื่อการวิเคราะห์ โปรดทราบว่าคุณจะไม่ได้รับการตอบกลับจาก ESET ยกเว้นกรณีที่ต้องการข้อมูลเพิ่มเติม

ส่งตัวอย่างเพื่อวิเคราะห์

หากคุณพบไฟล์ที่มีพฤติกรรมน่าสงสัยในคอมพิวเตอร์ คุณสามารถส่งไฟล์ดังกล่าวไปยัง ESET Research Lab เพื่อรับการวิเคราะห์ได้

ก่อนการส่งตัวอย่างไปยัง ESET

อย่าส่งตัวอย่างจนกว่าจะพบว่าตัวอย่างเป็นไปตามเกณฑ์ดังต่อไปนี้:

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

หากต้องการส่งตัวอย่าง ให้ใช้แบบฟอร์มการส่งตัวอย่างในผลิตภัณฑ์ของคุณ โดยแบบฟอร์มดังกล่าวจะอยู่ใน

เครื่องมือ > **ส่งตัวอย่างเพื่อการวิเคราะห์**

ในแบบฟอร์ม **ส่งตัวอย่างเพื่อวิเคราะห์** ให้กรอกข้อมูลต่อไปนี้:

ไฟล์ – พาธไปยังไฟล์ที่คุณต้องการส่ง

ความคิดเห็น – อธิบายสาเหตุที่คุณส่งไฟล์

อีเมลที่ติดต่อ – โปรแกรมจะส่งอีเมลที่ติดต่อนี้ไปยัง ESET พร้อมกับไฟล์ที่น่าสงสัย และอาจใช้เพื่อติดต่อคุณ ถ้าต้องการข้อมูลเพิ่มเติมสำหรับการวิเคราะห์ คุณจะป้อนอีเมลที่ติดต่อหรือไม่ก็ได้

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

ส่วนติดต่อผู้ใช้

ตัวเลือกการกำหนดค่าส่วนติดต่อผู้ใช้อนุญาตให้คุณปรับสภาพแวดล้อมการทำงานเพื่อให้ตรงกับความต้องการของคุณ ตัวเลือกเหล่านี้สามารถเข้าถึงได้จากเมนูหลักโดยคลิกที่ **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** (หรือกด *cmd+,*) > **ส่วนติดต่อผู้ใช้**

• ในการแสดงหน้าจอเริ่มต้นของ ESET Cyber Security เมื่อเริ่มต้นระบบ ให้เลือก **แสดงหน้าจอเริ่มต้นเมื่อเริ่มต้นระบบ**

• **แอปพลิเคชันที่อยู่ใน Dock** จะช่วยให้คุณแสดงไอคอน ESET Cyber Security ใน Dock ของ macOS และสลับระหว่าง ESET Cyber Security และแอปพลิเคชันอื่นๆ ที่ใช้งานอยู่โดยกด *cmd+tab* การเปลี่ยนแปลงจะเกิดผลหลังจากที่คุณรีสตาร์ท ESET Cyber Security (โดยปกติแล้วจะทำงานโดยการรีสตาร์ทคอมพิวเตอร์)

• ตัวเลือก **ใช้เมนูมาตรฐาน**จะช่วยให้คุณใช้ปุ่มลัดแป้นพิมพ์บางรายการ (ดูปุ่มลัดแป้นพิมพ์) และดูรายการเมนูมาตรฐาน (ใช้อินเทอร์เฟซ การตั้งค่าและเครื่องมือ) บนแถบเมนู macOS (ด้านบนสุดของหน้าจอ)

• ในการเปิดใช้งานคำแนะนำเครื่องมือสำหรับตัวเลือกบางอย่างของ ESET Cyber Security ให้เลือก **แสดงคำแนะนำเครื่องมือ**

• **แสดงไฟล์ที่ซ่อน** อนุญาตให้คุณดูและเลือกไฟล์ที่ซ่อนอยู่ในการตั้งค่า **เป้าหมายแสกน** ของ **การสแกนคอมพิวเตอร์**

• โดยค่าเริ่มต้น ไอคอน ESET Cyber Security จะแสดงในแถบเมนูเพิ่มเติมที่ปรากฏที่ด้านขวาของแถบเมนู macOS (ด้านบนสุดของหน้าจอ) หากต้องการปิดใช้งานสิ่งนี้ ให้เลิกเลือก **แสดงไอคอนในแถบเมนูเพิ่มเติม** การเปลี่ยนแปลงนี้จะเกิดผลหลังจากคุณเริ่มการทำงาน ESET Cyber Security ของคุณใหม่ (โดยปกติแล้วจะได้รับการกระตุ้นเมื่อคอมพิวเตอร์เริ่มการทำงานใหม่)

การเตือนและการแจ้งเตือน

ส่วน **การเตือนและการแจ้งเตือน** จะช่วยให้คุณสามารถกำหนดค่าวิธีจัดการการเตือนภัยคุกคามและการแจ้งเตือนของระบบที่จัดการโดย ESET Cyber Security

การปิดใช้งาน **แสดงการเตือน** จะปิดใช้งานหน้าต่างการเตือนทั้งหมด และเหมาะสำหรับในบางสถานการณ์เท่านั้น สำหรับผู้ใช้ส่วนใหญ่ เราขอแนะนำให้ใช้การตั้งค่าเริ่มต้นของตัวเลือกนี้ (เปิดใช้งานไว้แล้ว) ตัวเลือกขั้นสูงมีการอธิบายอยู่ ในบทนี้

การเลือก **แสดงการแจ้งเตือนบนเดสก์ท็อป** จะช่วยให้หน้าต่างการเตือนที่ไม่จำเป็นต้องมีการดำเนินการจากผู้ใช้สามารถปรากฏบนเดสก์ท็อปได้ (ตามค่าเริ่มต้นแล้ว จะปรากฏที่มุมขวาบนของหน้าจอ) คุณสามารถกำหนดระยะเวลาแสดงการแจ้งเตือนได้โดยปรับค่า **ปิดการแจ้งเตือนโดยอัตโนมัติหลังจาก** X **วินาที** (ค่าเริ่มต้นคือ 5 วินาที)

ตั้งแต่ ESET Cyber Security เวอร์ชัน 6.2 เป็นต้นไป คุณยังสามารถป้องกันไม่ให้ **สถานะการป้องกัน** แสดงหน้าจอหลักของโปรแกรมได้อีกด้วย (หน้าต่าง **สถานะการป้องกัน**) ถ้าต้องการเรียนรู้เพิ่มเติมในเรื่องนี้ โปรดดู สถานะการป้องกัน

แสดงการเตือน

ESET Cyber Security แสดงหน้าต่างข้อความการเตือนที่แจ้งให้คุณทราบเกี่ยวกับเวอร์ชันใหม่ของโปรแกรม การอัพเดทระบบปฏิบัติการ การปิดใช้งานองค์ประกอบบางอย่างของโปรแกรม การลบบันทึก เป็นต้น คุณสามารถปิดการแจ้งเตือนแต่ละรายการได้ด้วยการเลือก **ไม่ต้องแสดงข้อความนี้อีก**

รายการข้อความ (**ตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** > **การเตือนและการแจ้งเตือน** > **ตั้งค่า...**) แสดงรายการของข้อความการเตือนทั้งหมดที่เรียกโดย ESET Cyber Security หากต้องการเปิดใช้งานหรือปิดการแจ้งเตือนแต่ละรายการ ให้เลือกกล่องกาเครื่องหมายของ **ชื่อข้อความ** นอกจากนี้ คุณสามารถกำหนด **แสดงเงื่อนไข** ซึ่งจะแสดงการแจ้งเตือนเกี่ยวกับเวอร์ชันใหม่ของโปรแกรมและการอัพเดทระบบปฏิบัติการจะปรากฏขึ้น

สถานะการป้องกัน

สถานะการป้องกันในปัจจุบันของ ESET Cyber Security สามารถเปลี่ยนแปลงได้โดยการเปิดใช้งานและปิดการใช้งานสถานะใน **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน...** > **การเตือนและการแจ้งเตือน** > **แสดงในหน้าจอสถานะการป้องกัน: การตั้งค่า** สถานะของคุณลักษณะของโปรแกรมจะถูกแสดงหรือซ่อนจากหน้าจอหลักของ ESET Cyber Security (หน้าต่าง **สถานะการป้องกัน**)

คุณสามารถซ่อนสถานะของคุณลักษณะของโปรแกรมต่อไปนี้ได้:

- การป้องกันฟิชชิ่ง
- การป้องกันการเข้าถึงเว็บ
- การป้องกันอีเมล์ไคลเอนต์
- การอัพเดทระบบปฏิบัติการ
- ใบอนุญาตหมดอายุ
- ต้องการการเริ่มต้นระบบคอมพิวเตอร์ใหม่

สิทธิ์

การตั้งค่า ESET Cyber Security เป็นส่วนสำคัญอย่างมากต่อนโยบายความปลอดภัยขององค์กรของคุณ การแก้ไขโดยไม่ได้รับอนุญาตอาจเป็นอันตรายต่อเสถียรภาพและการป้องกันระบบของคุณ ด้วยเหตุผลนี้ คุณสามารถระบุว่าผู้ใช้ใดที่มีสิทธิ์ในการแก้ไขการกำหนดค่าโปรแกรม

ในการระบุผู้ใช้ที่มีสิทธิพิเศษ ให้คลิก **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** (หรือกด *cmd+,*) > **สิทธิพิเศษ** เลือกผู้ใช้หรือกลุ่มจากรายการด้านซ้ายและคลิก **เพิ่ม** หากต้องการแสดงผู้ใช้ระบบ/กลุ่มทั้งหมด ให้เลือก **แสดงผู้ใช้ระบบ/กลุ่มทั้งหมด** หากต้องการเอาผู้ใช้ออก ให้เลือกชื่อจากรายการ**ผู้ใช้ที่เลือก** ที่อยู่ด้านขวาแล้วคลิก **เอาออก**

เกี่ยวกับการอัพเกรด
หากคุณปล่อยให้รายการผู้ใช้ที่เลือกว่างเปล่า จะถือว่าผู้ใช้ทุกคนมีสิทธิ์

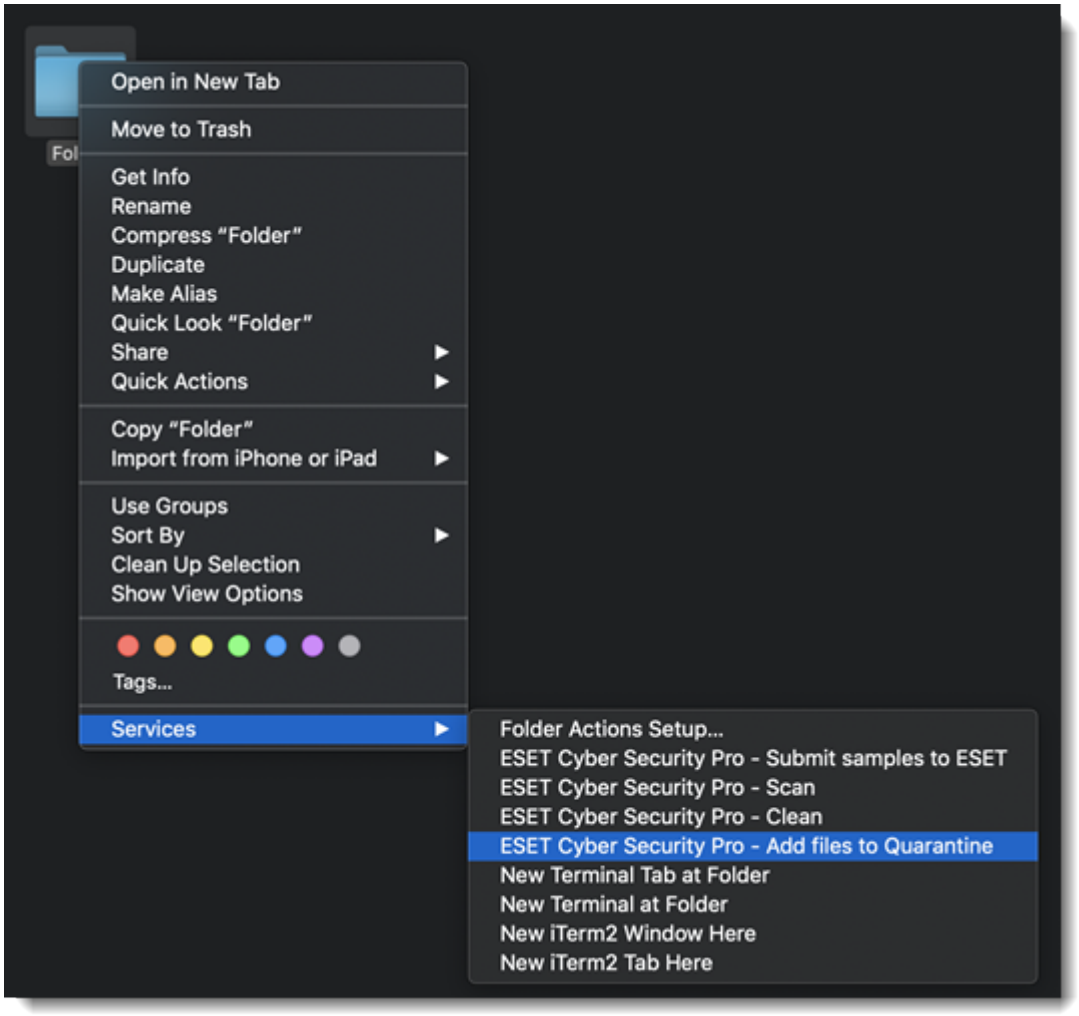
เมนูบริบท

คุณสามารถเปิดใช้งานการรวมเมนูบริบทได้โดยคลิก **การตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** (หรือกดส่วน *cmd+,*) > **เมนูบริบท** โดยเลือกตัวเลือก **รวมเป็นเมนูบริบท** ต้องการการออกจากระบบหรือการรีสตาร์ทคอมพิวเตอร์เพื่อให้การเปลี่ยนแปลงมีผล ตัวเลือกเมนูบริบทสามารถใช้งานได้ในหน้าต่าง **Finder** เมื่อคุณ CTRL+click ในไฟล์ใด ๆ

คุณสามารถเลือกตัวเลือกที่แสดงอยู่ในเมนูบริบทได้ โดยคุณสามารถแสดงตัวเลือก **สแกนเท่านั้น** ซึ่งจะช่วยคุณในการสแกนไฟล์ที่เลือก ตัวเลือก **ทำความสะอาดเท่านั้น** จะช่วยคุณในการทำความสะอาดไฟล์ที่เลือกจากเมนูบริบท ใช้การทำความสะอาดถ้าไฟล์ถูกโจมตีโดยไวรัสที่มีการแนบรหัสที่เป็นอันตรายกับไฟล์นั้น ในกรณีนี้ ขั้นแรกให้พยายามทำความสะอาดไวรัสออกจากไฟล์ที่ติดเชื้อเพื่อคืนค่าไฟล์สู่สภาวะเดิม ถ้าไฟล์มีเฉพาะรหัสที่เป็นอันตรายไฟล์ดังกล่าวจะถูกลบ

ถ้าคุณเลือกตัวเลือก **ทั้งหมด** คุณสามารถดำเนินการดังต่อไปนี้จากเมนูบริบทได้:

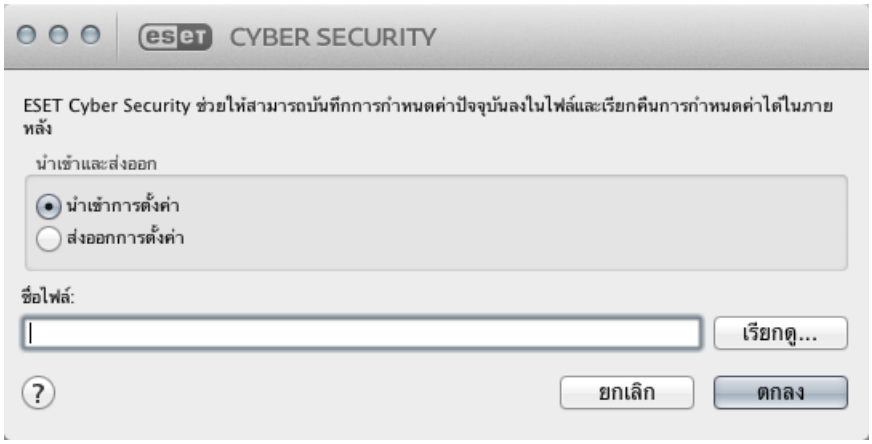
- ส่งตัวอย่างเพื่อวิเคราะห์
- สแกน
- กำจัด
- เพิ่มไฟล์ไปยังการกักเก็บ



นำเข้าและส่งออกการตั้งค่า

หากต้องการนำเข้าการกำหนดค่าที่มีอยู่แล้วหรือส่งออกการกำหนดค่า ESET Cyber Security ของคุณ ให้คลิก **การตั้งค่า** > **นำเข้าหรือส่งออกการตั้งค่า**

การนำเข้าและส่งออกจะมีประโยชน์ในกรณีที่คุณต้องสำรองการกำหนดค่าปัจจุบันของ ESET Cyber Security ของคุณสำหรับการใช้ในภายหลัง ส่งออกการตั้งค่า ยังสะดวกสำหรับผู้ใช้ที่ต้องการใช้การกำหนดค่าที่ต้องการของ ESET Cyber Security ในหลายระบบ คุณสามารถนำเข้าไฟล์การกำหนดค่าเพื่อโอนการตั้งค่าที่ต้องการได้อย่างง่ายดาย



ถ้าต้องการนำเข้าการกำหนดค่า ให้เลือก **นำเข้าการตั้งค่า** และคลิก **เรียกดู** เพื่อไปยังไฟล์การกำหนดค่าที่คุณต้องการนำเข้า ถ้าการส่งออก ให้เลือก **ส่งออกการตั้งค่า** และใช้เบราว์เซอร์เพื่อเลือกตำแหน่งบนคอมพิวเตอร์ของคุณที่ต้องการบันทึกไฟล์การกำหนดค่า

การตั้งค่าพร็อกซีเซิร์ฟเวอร์

การตั้งค่าพร็อกซีเซิร์ฟเวอร์สามารถกำหนดค่าได้ใน **ตั้งค่า** > **ป้อนการตั้งค่าแอพพลิเคชัน ...** (หรือกด *cmd+,*) > **พร็อกซีเซิร์ฟเวอร์** การระบุพร็อกซีเซิร์ฟเวอร์ที่ระดับนี้จะกำหนดการตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วมสำหรับฟังก์ชันทั้งหมดของ ESET Cyber Security พารามิเตอร์ที่กำหนดในที่นี้จะถูกนำมาใช้โดยโมดูลทั้งหมดที่ต้องการการเชื่อมต่ออินเทอร์เน็ต ESET Cyber Security สนับสนุนประเภทการตรวจสอบสิทธิ์แบบ Basic Access (การเข้าถึงพื้นฐาน) และ NTLM (ตัวจัดการ NT LAN)

เมื่อต้องการระบุการตั้งค่าพร็อกซีเซิร์ฟเวอร์สำหรับระดับนี้ ให้เลือก **ใช้พร็อกซีเซิร์ฟเวอร์** และป้อนที่อยู่ IP หรือ URL ของพร็อกซีเซิร์ฟเวอร์ของคุณในช่อง **พร็อกซีเซิร์ฟเวอร์** ในฟิลด์พอร์ต ให้ระบุพอร์ตที่พร็อกซีเซิร์ฟเวอร์ยอมรับการเชื่อมต่อ (3128 ตามค่าเริ่มต้น) คุณสามารถคลิก **ตรวจหา** เพื่อให้โปรแกรมกรอกข้อมูลทั้งสองฟิลด์ได้เช่นกัน

หากจำเป็นต้องสื่อสารด้วยพร็อกซีเซิร์ฟเวอร์ ให้ป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** ที่ถูกต้องลงในช่องที่เกี่ยวข้อง

ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง

ข้อมูลสำคัญ: โปรดอ่านข้อกำหนดและเงื่อนไขของการใช้งานผลิตภัณฑ์ที่กำหนดไว้ด้านล่างนี้อย่างถี่ถ้วนก่อนที่จะดาวน์โหลด ติดตั้ง คัดลอก หรือใช้งาน **เมื่อคุณดาวน์โหลด ติดตั้ง คัดลอก หรือใช้ซอฟต์แวร์นี้ จะถือว่าคุณแสดงความยินยอมตามข้อกำหนดและเงื่อนไขเหล่านี้และคุณยอมรับ** นโยบายความเป็นส่วนตัว.

ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง

ภายใต้ข้อกำหนดของข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง (ในที่นี้จะเรียกว่า “ข้อตกลง”) ที่ทำขึ้นโดยและระหว่าง ESET, spol. s r. o. ซึ่งมีสำนักงานที่จดทะเบียนอยู่ที่ Einsteinova 24, 85101 Bratislava, Slovak Republic และจดทะเบียนกับ Commercial Register ซึ่งมีการบริหารจัดการโดย Bratislava I District Court, Section Sro, Entry No 3586/B, หมายเลขทะเบียนการค้า: 31333532 (ในที่นี้จะเรียกว่า "ESET" หรือ “ผู้ให้บริการ”) กับคุณ ซึ่งเป็นบุคคลธรรมดาหรือนิติบุคคล (ในที่นี้จะเรียกว่า “คุณ" หรือ "ผู้ใช้ปลายทาง”) คุณได้รับสิทธิ์ให้สามารถใช้ซอฟต์แวร์ที่กำหนดในข้อ 1 ของข้อตกลงนี้ ซอฟต์แวร์ที่กำหนดในข้อ 1 ของข้อตกลงนี้อาจจัดเก็บอยู่ในสื่อจัดเก็บข้อมูล ส่งทางอีเมล ดาวน์โหลดจากอินเทอร์เน็ต ดาวน์โหลดจากเซิร์ฟเวอร์ของผู้ให้บริการ หรือได้รับจากแหล่งอื่นๆ ตามข้อกำหนดและเงื่อนไขที่ระบุไว้ด้านล่างนี้

ข้อตกลงนี้เป็นข้อตกลงเกี่ยวกับสิทธิของผู้ใช้ปลายทางและไม่ใช่ข้อตกลงสำหรับการจำหน่าย ผู้ให้บริการยังคงเป็นเจ้าของสำเนาของซอฟต์แวร์ และสื่อทางกายภาพที่บรรจุในบรรจุภัณฑ์เชิงพาณิชย์ รวมถึงสำเนาอื่นๆ ของซอฟต์แวร์ที่ผู้ใช้ปลายทางได้รับอนุญาตตามข้อตกลงนี้

เมื่อคลิกที่ตัวเลือก "ฉันยอมรับ" หรือ "ฉันยอมรับ..." ในระหว่างการติดตั้ง ดาวน์โหลด คัดลอก หรือใช้ซอฟต์แวร์ จะถือว่าคุณยอมรับข้อกำหนดและเงื่อนไขของข้อตกลงนี้ ถ้าคุณไม่ยอมรับข้อกำหนดและเงื่อนไขทั้งหมดของข้อตกลงนี้ 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 (ในที่นี้เรียกว่า "เอกสารประกอบ"); (iv) สำเนาของซอฟต์แวร์ การแก้ไขข้อผิดพลาดที่เป็นไปได้ในซอฟต์แวร์ ส่วนเพิ่มเติมซอฟต์แวร์ ส่วนขยาย เวอร์ชันดัดแปลงของซอฟต์แวร์ และการอัพเดทส่วนประกอบซอฟต์แวร์ ถ้ามี ตามที่ผู้ให้บริการให้อนุญาตแก่คุณตามข้อ 3 ของข้อตกลงนี้ ซอฟต์แวร์จะมีให้ในรูปแบบของรหัสวัตถุที่เรียกใช้งานได้เท่านั้น

2. **การติดตั้ง คอมพิวเตอร์ และรหัสใบอนุญาต ซอฟต์แวร์ที่อยู่ในสื่อจัดเก็บข้อมูล** ส่งทางอีเมล ดาวน์โหลดจากอินเทอร์เน็ต ดาวน์โหลดจากเซิร์ฟเวอร์ของผู้ให้บริการ หรือได้รับจากแหล่งอื่นๆ จะต้องมีการติดตั้ง คุณจะต้องติดตั้งซอฟต์แวร์ในคอมพิวเตอร์ที่ได้รับการกำหนดค่าอย่างถูกต้อง ตามข้อกำหนดขั้นต่ำที่ระบุไว้ในเอกสารประกอบ วิธีการติดตั้งจะมีระบุไว้ในเอกสารประกอบ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์หรือฮาร์ดแวร์ที่อาจมีผลเสียต่อซอฟต์แวร์ไว้ในคอมพิวเตอร์ที่คุณติดตั้งซอฟต์แวร์ คอมพิวเตอร์หมายถึงฮาร์ดแวร์ ซึ่งรวมถึงแต่ไม่จำกัดเพียง คอมพิวเตอร์ส่วนบุคคล แล็ปท็อป เวิร์กสเตชัน ปาล์มท็อปคอมพิวเตอร์ สมาร์ทโฟน อุปกรณ์อิเล็กทรอนิกส์แบบถือหรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆ ที่ซอฟต์แวร์ถูกออกแบบมาให้ใช้งานด้วย หรือที่ซอฟต์แวร์ถูกติดตั้งและ/หรือใช้งาน รหัสใบอนุญาตหมายถึงชุดของสัญลักษณ์ อักขระ หมายเลข หรือสัญลักษณ์พิเศษที่ไม่ซ้ำกันซึ่งจัดหาให้แก่ผู้ใช้ปลายทางเพื่ออนุญาตให้ใช้งานซอฟต์แวร์ เวอร์ชั่นเฉพาะ หรือส่วนขยายของข้อกำหนดของใบอนุญาตได้อย่างถูกกฎหมาย สอดคล้องกับข้อตกลงนี้

3. **ใบอนุญาต** ตามเงื่อนไขที่คุณยอมรับตามข้อกำหนดของข้อตกลงนี้และคุณปฏิบัติตามข้อกำหนดและเงื่อนไขทั้งหมดที่ระบุไว้ในที่นี้ ผู้ให้บริการจะให้สิทธิ์ (ในที่นี้จะเรียกว่า "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 (ในที่นี้จะเรียกว่า “MUA”) ถ้า MUA ยอมรับอีเมลและส่งต่อไปยังผู้ใช้หลายรายโดยอัตโนมัติ จำนวนของผู้ใช้ปลายทางจะพิจารณาตามจำนวนผู้ใช้ตามจริงที่มีการส่งอีเมลถึง ถ้าอีเมลเซิร์ฟเวอร์ดำเนินการเป็นเกตเวย์ของอีเมล จำนวนผู้ใช้ปลายทางจะต้องเท่ากับจำนวนผู้ใช้อีเมลเซิร์ฟเวอร์ที่เกตเวย์นั้นให้บริการอยู่ ถ้ามีการส่งอีเมลสำหรับที่อยู่อีเมลที่ไม่ได้ระบุจำนวนไปยังและยอมรับโดยผู้ใช้รายเดียว (เช่น ผ่านชื่อแทน) และข้อความนั้นไม่มีการส่งต่อโดยอัตโนมัติโดยไคลเอ็นต์ไปยังผู้ใช้จำนวนมาก จะต้องใช้ใบอนุญาตสำหรับคอมพิวเตอร์เครื่องเดียว คุณจะต้องไม่ใช้ใบอนุญาตเดียวกันในเวลาเดียวกันในคอมพิวเตอร์มากกว่าหนึ่งเครื่อง ผู้ใช้ปลายทางได้รับสิทธิ์ให้ป้อนรหัสใบอนุญาตไปยังซอฟต์แวร์ได้เฉพาะในขอบเขตเท่าที่มีสิทธิ์ใช้งานซอฟต์แวร์ ซึ่งสอดคล้องกับข้อจำกัดที่มีผลบังคับใช้จากจำนวนใบอนุญาตที่ได้รับจากผู้ให้บริการ รหัสใบอนุญาตจะถือว่าเป็นความลับ คุณต้องไม่แบ่งปันใบอนุญาตกับบุคคลที่สามหรืออนุญาติให้บุคคลที่สามใช้รหัสใบอนุญาตเว้นแต่จะได้รับอนุญาตจากข้อตกลงนี้หรือจากผู้ให้บริการ หากรหัสใบอนุญาตของคุณถูกบุกรุก โปรดแจ้งผู้ให้บริการทันที

ค) **Business Edition** ต้องมีซอฟต์แวร์รุ่น Business Edition เพื่อใช้ซอฟต์แวร์ในอีเมลเซิร์ฟเวอร์ เมลรีเลย์ เมลเกตเวย์

หรืออินเทอร์เน็ตเกตเวย์

ง) **ระยะเวลาของใบอนุญาต** สิทธิในการใช้ซอฟต์แวร์จะมีระยะเวลาจำกัด

จ) **ซอฟต์แวร์ของ OEM** ซอฟต์แวร์ของ 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** ผู้ให้บริการจะได้รับสิทธิตั้งแต่เวลาออกการอัพเดทซอฟต์แวร์ ("การอัพเดท") แต่จะไม่มีภาระหน้าที่ในการให้การอัพเดท ฟังก์ชันนี้จะถูกเปิดใช้งานภายใต้การตั้งค่ามาตรฐานของซอฟต์แวร์และจะได้รับการติดตั้งการอัพเดทโดยอัตโนมัติ ยกเว้นผู้ใช้ปลายทางจะปิดใช้งานการติดตั้งการอัพเดทโดยอัตโนมัติ เพื่อวัตถุประสงค์ในการให้การอัพเดท จะต้องใช้การตรวจสอบความถูกต้องของใบอนุญาต ซึ่งรวมถึงข้อมูลเกี่ยวกับคอมพิวเตอร์และ/หรือแพลตฟอร์มที่ติดตั้งซอฟต์แวร์นั้นตามนโยบายความเป็นส่วนตัว

ข) **การส่งต่อการแฝงตัวและข้อมูลแก่ผู้ให้บริการ** ซอฟต์แวร์นี้มีฟังก์ชันที่ทำหน้าที่เก็บตัวอย่างของไวรัสคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ที่เป็นอันตรายอื่นๆ และสิ่งที่น่าสงสัยซึ่งเป็นปัญหา ที่อาจไม่พึงประสงค์หรืออาจไม่ปลอดภัย เช่น ไฟล์ URL แพ็คเก็ต IP และค่าเฟรมอีเธอร์เน็ต (ในที่นี้จะเรียกว่า “การแฝงตัว”) และจะส่งตัวอย่างเหล่านี้ให้กับผู้ให้บริการ รวมถึงแต่ไม่จำกัดเฉพาะข้อมูลเกี่ยวกับกระบวนการติดตั้ง คอมพิวเตอร์และ/หรือแพลตฟอร์มที่ติดตั้งซอฟต์แวร์นั้น ข้อมูลเกี่ยวกับระบบปฏิบัติการและการทำงานของซอฟต์แวร์ และข้อมูลเกี่ยวกับอุปกรณ์ในเครือข่ายภายใน เช่น ชนิด ผู้ขาย รุ่น และ/หรือชื่อของอุปกรณ์ (ในที่นี้จะเรียกว่า "ข้อมูล") ข้อมูลและการแฝงตัวอาจประกอบด้วยข้อมูล (รวมถึงข้อมูลส่วนบุคคลที่ได้รับโดยการสุ่มหรือโดยบังเอิญ) เกี่ยวกับผู้ใช้ปลาย

ทางหรือผู้ใช้อื่นๆ 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 เพื่อการเรียกเก็บเงินและการปฏิบัติตามข้อตกลงนี้ รวมถึงการส่งการแจ้งเตือนในคอมพิวเตอร์ของคุณ คุณยอมรับในที่นี้ว่าจะรับการแจ้งเตือนและข้อความเกี่ยวกับผลิตภัณฑ์ รวมถึงแต่ไม่จำกัดเฉพาะข้อมูลด้านการตลาด

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 รวมถึงแต่ไม่จำกัดเพียงสิทธิในกรรมสิทธิและสิทธิในทรัพย์สินทางปัญญา

เป็นของ 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 ไม่ว่าการยุติข้อตกลงนี้จะเกิดขึ้นด้วยสาเหตุใด บทบัญญัติของข้อ 7, 8, 11, 13, 19 และ 21 จะยังคงมีผลบังคับโดยไม่จำกัดเวลา

11. **ประกาศของผู้ใช้ปลายทาง** ในฐานะที่เป็นผู้ใช้ปลายทาง คุณรับทราบว่าซอฟต์แวร์นี้มีให้แก่คุณแบบ "ตามสภาพ" โดยไม่มีการรับประกันทั้งโดยชัดแจ้งหรือโดยนัย ไม่ว่าในประเภทใดภายในขอบเขตสูงสุดที่กฎหมายอนุญาต ผู้ให้บริการ ผู้ให้การอนุญาตแก่ผู้ให้บริการหรือบริษัทในเครือ หรือผู้ถือลิขสิทธิ์ ไม่ได้ให้การรับรองหรือรับประกันทั้งโดยชัดแจ้งและโดยนัย ซึ่งจะรวมถึง แต่ไม่จำกัดเพียงการรับประกันการขาย หรือความเหมาะสมกับวัตถุประสงค์อย่างใดอย่างหนึ่งเป็นการเฉพาะ หรือการรับประกันว่าซอฟต์แวร์ไม่ได้ละเมิดสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้าหรือสิทธิอื่นๆ ของบุคคลที่สาม ผู้ให้บริการหรือบุคคลอื่นไม่มีการรับประกันใดๆ ว่าฟังก์ชันที่มีอยู่ในซอฟต์แวร์นี้จะเป็นไปตามความต้องการ หรือการทำงานของซอฟต์แวร์จะทำงานต่อเนื่องและปราศจากข้อผิดพลาด คุณต้องรับผิดชอบและรับความเสี่ยงทั้งหมดสำหรับการเลือกซอฟต์แวร์ เพื่อให้ได้ผลลัพธ์ตามเจตนารมณ์ของคุณ และสำหรับการติดตั้ง การใช้งาน และผลที่จะได้รับจากซอฟต์แวร์

12. **ไม่มีข้อผูกมัดอื่น** ข้อตกลงนี้ไม่ได้แสดงถึงภาระหน้าที่อื่นใดในส่วนของผู้ให้บริการและผู้ให้การอนุญาตแก่ผู้ให้บริการ ยกเว้นจะระบุไว้อย่างชัดเจนในที่นี้

13. **ข้อจำกัดความรับผิด** ภายในขอบเขตสูงสุดที่กฎหมายอนุญาต ไม่ว่าในกรณีใดๆ ผู้ให้บริการ พนักงาน หรือผู้ให้การอนุญาตจะไม่มีความรับผิดต่อการสูญเสียผลกำไร รายได้ การขาย ข้อมูล หรือค่าใช้จ่ายที่เกิดขึ้นเพื่อจัดหาสินค้าหรือบริการทดแทน ความเสียหายของสินทรัพย์ การบาดเจ็บของบุคคล การหยุดชะงักของธุรกิจ การสูญเสียข้อมูลธุรกิจหรือความเสียหายเป็นกรณีพิเศษ ทางตรง ทางอ้อม เกิดขึ้นเอง ทางเศรษฐกิจ การชดเชย บทลงโทษ หรือความเสียหายที่เป็นพิเศษหรือที่เกิดขึ้นในภายหลัง อันเกิดขึ้นด้วยวิธีใดๆ ก็ตามจากการทำสัญญา การละเมิด ความประมาทหรือข้อเท็จจริงอื่นๆ ที่แสดงถึงความรับผิด อันเกิดจากการใช้หรือไม่สามารถใช้ซอฟต์แวร์ แม้ในกรณีที่ผู้ให้บริการหรือผู้ให้การอนุญาตแก่ผู้ให้บริการหรือบริษัทในเครือได้รับแจ้งถึงโอกาสที่จะเกิดความเสียหายนั้นแล้วก็ตาม เนื่องจากในบางประเทศและบางเขตอำนาจศาลไม่อนุญาตให้มีการยกเว้นความรับผิด แต่อาจอนุญาตให้มีการจำกัดความรับผิด ในกรณีดังกล่าว ความรับผิดของผู้ให้บริการ พนักงาน หรือผู้ให้การอนุญาตหรือบริษัทในเครือจะจำกัดอยู่เพียงไม่เกินจำนวนเงินที่คุณชำระเป็นค่าใบอนุญาตเท่านั้น

14. ในข้อตกลงนี้จะไม่มีผลกระทบต่อสิทธิตามกฎหมายของฝ่ายใดที่มีฐานะเป็นผู้บริโภคถ้าเกิดข้อขัดแย้งในการทำงาน

15. **การสนับสนุนด้านเทคนิค** ESET หรือบุคคลที่สามที่กำหนดโดย ESET จะใช้ดุลยพินิจในการให้บริการสนับสนุนด้านเทคนิค โดยไม่มีการรับประกันหรือการประกาศใดๆ ผู้ใช้ปลายทางจะต้องสำรองข้อมูล ซอฟต์แวร์ และโปรแกรมที่มีอยู่ทั้งหมดก่อนการให้การสนับสนุนด้านเทคนิค ESET และ/หรือบุคคลที่สามที่กำหนดโดย ESET จะไม่ยอมรับการรับผิดสำหรับความเสียหายหรือการสูญเสียของข้อมูล สินทรัพย์ ซอฟต์แวร์ หรือฮาร์ดแวร์ หรือการสูญเสียผลกำไร อันเนื่องมาจากการให้การสนับสนุนด้านเทคนิค ESET และ/หรือบุคคลที่สามที่กำหนดโดย ESET ขอสงวนสิทธิ์ที่จะพิจารณาว่าการแก้ไขปัญหาอยู่นอกขอบเขตของการสนับสนุนด้านเทคนิค ESET ขอสงวนสิทธิ์ในการใช้ดุลยพินิจเพื่อปฏิเสธ พัก หรือยุติการให้การสนับสนุนด้านเทคนิค อาจจำเป็นต้องใช้ข้อมูลใบอนุญาต ข้อมูล และข้อมูลอื่นๆ ตามที่ระบุไว้ในนโยบายความเป็นส่วนตัว เพื่อวัตถุประสงค์ในการให้บริการสนับสนุนด้านเทคนิค

16. **การโอนใบอนุญาต** ซอฟต์แวร์สามารถโอนจากระบบคอมพิวเตอร์หนึ่งไปยังอีกระบบหนึ่ง ยกเว้นจะขัดกับข้อกำหนดของข้อตกลง ถ้าไม่ขัดกับข้อกำหนดของข้อตกลง ผู้ใช้ปลายทางจะได้รับสิทธิเฉพาะสำหรับการโอนใบอนุญาตอย่างถาวร และสิทธิทั้งหมดที่มาจากข้อตกลงนี้ไปยังผู้ใช้ปลายทางรายอื่น โดยมีความยินยอมของผู้ให้บริการ ตามเงื่อนไขว่า (i) ผู้ใช้ปลายทางเดิมต้องไม่เก็บสำเนาของซอฟต์แวร์ไว้ (ii) การโอนสิทธิจะต้องเป็นโดยตรง เช่น จากผู้ใช้ปลายทางเดิมไปยังผู้ใช้ปลายทางรายใหม่ (iii) ผู้ใช้ปลายทางรายใหม่ต้องถือสิทธิและภาระหน้าที่ทั้งหมดที่เป็นหน้าที่รับผิดชอบของผู้ใช้ปลายทางเดิมภายใต้ข้อกำหนดของข้อตกลงนี้ (iv) ผู้ใช้ปลายทางเดิมต้องให้เอกสารประกอบแก่ผู้ใช้ปลายทางรายใหม่ ซึ่งจะช่วยตรวจสอบซอฟต์แวร์ที่เป็นของแท้ดังที่ระบุภายใต้ข้อ 17

17. **การตรวจสอบซอฟต์แวร์ที่เป็นของแท้** ผู้ใช้ปลายทางสามารถพิสูจน์สิทธิ์ในการใช้ซอฟต์แวร์ได้โดยใช้วิธีการใดวิธีการหนึ่งต่อไปนี้: (i) ผ่านใบรับรองของใบอนุญาตที่ออกโดยผู้ให้บริการหรือบุคคลที่สามที่มีการกำหนดโดยผู้ให้บริการ (ii) ผ่านข้อตกลงใบอนุญาตที่เป็นลายลักษณ์อักษร ถ้ามีการสรุปข้อตกลงดังกล่าวไว้ (iii) 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 (ต่อไปนี้จะเรียกว่า "กฎหมายควบคุมการส่งออก") 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 (ต่อไปนี้จะเรียกว่า "กฎหมายลงโทษ")

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

21. **กฎหมายที่มีผลบังคับใช้** ข้อตกลงนี้อยู่ภายใต้อำนาจและมีการตีความตามกฎหมายของสาธารณรัฐสโลวัก ผู้ใช้ปลายทางและผู้ให้บริการยอมรับในที่นี้ว่าหลักการด้านข้อขัดแย้งของกฎหมายและอนุสัญญาสหประชาชาติว่าด้วยสัญญาการขายสินค้าระหว่างประเทศจะไม่มีผลบังคับ คุณยอมรับโดยชัดเจนว่าการพิพาทหรือการเรียกร้องที่มาจากข้อตกลงนี้กับผู้ให้บริการ หรือการพิพาทหรือการเรียกร้องที่เกี่ยวข้องกับการใช้ซอฟต์แวร์จะอยู่ภายใต้อำนาจของศาลเขต Bratislava I และคุณยอมรับอย่างชัดเจนต่อการใช้อำนาจศาลในศาลเขตดังกล่าว

22. **บทบัญญัติทั่วไป** ถ้าบทบัญญัติใดของข้อตกลงนี้ไม่มีผลบังคับหรือเป็นโมฆะ ข้อตกลงนี้จะไม่มีผลต่อความถูกต้องของบทบัญญัติอื่นๆ ในข้อตกลง ซึ่งจะมีผลบังคับและถูกต้องตามเงื่อนไขที่ระบุไว้ในที่นี้ ในกรณีที่มีความแตกต่างในระหว่างเวอร์ชันภาษาต่าง ๆ ของข้อตกลงนี้ ให้ยึดถือเวอร์ชันภาษาอังกฤษเป็นหลัก ข้อตกลงนี้สามารถแก้ไขได้ในรูปแบบที่เป็นลายลักษณ์อักษรเท่านั้น ลงชื่อโดยตัวแทนที่มีอำนาจของผู้ให้บริการ หรือบุคคลที่มีอำนาจอย่างชัดเจนในการดำเนินการนี้ภายใต้ข้อกำหนดของหนังสือมอบอำนาจ

ข้อตกลงทั้งหมดนี้เป็นข้อตกลงระหว่างผู้ให้บริการกับคุณเกี่ยวกับซอฟต์แวร์ และมีผลเหนือกว่าการรับรอง การแลกเปลี่ยนความคิดเห็น ภาระหน้าที่ การสื่อสาร หรือโฆษณาที่เกี่ยวข้องกับซอฟต์แวร์ทั้งหมดที่เกิดขึ้นก่อนหน้านี้

EULA ID: HOM-ECS-20-01

นโยบายความเป็นส่วนตัว

ESET, spol. s r. o., มีสำนักงานอยู่ที่ Einsteinova 24, 851 01 Bratislava, Slovak Republic ซึ่งจดทะเบียนในทะเบียนการค้าที่ได้รับการควบคุมดูแลโดย Bratislava I District Court, Section Sro, เลขที่ 3586/B หมายเลขทะเบียนธุรกิจ: 31333532 ในฐานะผู้ควบคุมข้อมูล ("ESET" หรือ "เรา") ต้องการให้มีความโปร่งใสในด้านการประมวลผลข้อมูลส่วนบุคคลและความเป็นส่วนตัวของลูกค้าของเรา เพื่อให้บรรลุเป้าหมายนี้ เราเผยแพร่นโยบายความเป็นส่วนตัวนี้โดยมีวัตถุประสงค์เพื่อแจ้งข้อมูลลูกค้าของเราเท่านั้น ("ผู้ใช้ปลายทาง" หรือ "คุณ") เกี่ยวกับหัวข้อต่อไปนี้:

• การประมวลผลข้อมูลส่วนบุคคล,

• การรักษาความลับของข้อมูล,

• สิทธิ์ของข้อมูล

การประมวลผลข้อมูลส่วนบุคคล

บริการที่ ESET นำเสนอในผลิตภัณฑ์ของเรามีให้ภายใต้ข้อกำหนดของข้อตกลงใบอนุญาตผู้ใช้ปลายทาง ("EULA") แต่บางผลิตภัณฑ์อาจต้องให้ความสนใจเป็นพิเศษ ราต้องการให้รายละเอียดเพิ่มเติมเกี่ยวกับการรวบรวมข้อมูลที่เกี่ยวข้องกับการให้บริการของเรา เราให้บริการต่างๆ ตามที่ได้อธิบายไว้ใน EULA และเอกสารเกี่ยวกับผลิตภัณฑ์ เช่น บริการอัพเดต/อัพเกรด ESET LiveGrid® การป้องกันการใช้ข้อมูลที่ไม่ถูกต้อง การสนับสนุน ฯลฯ เพื่อให้การทำงานทั้งหมด เราจำเป็นต้องรวบรวมข้อมูลต่อไปนี้:

• รายการอัพเดทและสถิติอื่นๆ ที่ครอบคลุมข้อมูลเกี่ยวกับกระบวนการติดตั้งและคอมพิวเตอร์ของคุณ รวมทั้งแพลตฟอร์มที่ติดตั้งผลิตภัณฑ์ของเราและข้อมูลเกี่ยวกับการดำเนินงานและฟังก์ชันการทำงานของผลิตภัณฑ์ของเรา เช่น ระบบปฏิบัติการ ข้อมูลฮาร์ดแวร์ ไอดีการติดตั้ง ไอดีใบอนุญาต ที่อยู่ IP ที่อยู่ MAC การตั้งค่าของผลิตภัณฑ์

• แฮชแบบวันเวย์ที่เกี่ยวกับการแทรกซึมที่เป็นส่วนหนึ่งของ ESET LiveGrid® Reputation System ซึ่งปรับปรุงประสิทธิภาพของโซลูชันการป้องกันมัลแวร์ของเราโดยการเปรียบเทียบไฟล์ที่ถูกสแกนกับฐานข้อมูลของรายการที่อยู่ในบัญชีขาวและบัญชีดำในคลาวด์

• ตัวอย่างและเมตาดาต้าที่น่าสงสัยจากภายนอกที่เป็นส่วนหนึ่งของ ESET LiveGrid® Feedback System ซึ่งช่วยให้ ESET สามารถตอบสนองต่อความต้องการของผู้ใช้ปลายทางของเราได้ทันที และช่วยให้เราสามารถตอบสนองต่อภัยคุกคามล่าสุดได้ เราจำเป็นต้องพึ่งพาข้อมูลที่คุณส่งให้เรา

  oการแทรกซึมต่างๆ เช่น ตัวอย่างของไวรัสและโปรแกรมที่เป็นอันตรายอื่นๆ และที่น่าสงสัย ปัญหา วัตถุที่อาจไม่เป็นที่ต้องการหรืออาจไม่ปลอดภัย เช่น ไฟล์ที่สามารถเปิดใช้งานได้ ข้อความอีเมลที่คุณเป็นผู้รายงานว่าเป็นสแปมหรือที่ผลิตภัณฑ์ของเราปักธงเตือน

  oข้อมูลเกี่ยวกับอุปกรณ์ในเครือข่ายภายใน เช่น ประเภท, ผู้จำหน่าย รุ่นและ/หรือชื่อของอุปกรณ์

  oข้อมูลที่เกี่ยวกับการใช้อินเทอร์เน็ต เช่น ที่อยู่ IP และข้อมูลเกี่ยวกับภูมิศาสตร์, แพ็คเกจ IP, URL และเฟรมอีเธอร์เน็ต

  oไฟล์แครชดัมป์และข้อมูลต่างๆ ที่มีอยู่

ไม่ไม่ได้ประสงค์ที่จะรวบรวมข้อมูลของคุณนอกเหนือจากขอบเขตที่ระบุนี้ แต่ในบางเวลาเราก็ไม่สามารถที่จะป้องกันได้ ข้อมูลที่เก็บรวบรวมโดยไม่ได้ตั้งใจอาจรวมอยู่ในตัวของมัลแวร์เอง (เก็บรวบรวมโดยไม่ได้แจ้งให้คุณทราบหรือคุณไม่ได้อนุมัติ) หรือที่ถูกเก็บรวบรวมโดยเป็นส่วนหนึ่งของชื่อไฟล์หรือ URL และเรามิได้ต้องการข้อมูลเหล่านั้นมาเป็นส่วนหนึ่งของระบบของเราหรือประมวลผลข้อมูลเหล่านั้นตามวัตถุประสงค์ที่แจ้งไว้ในนโยบายความเป็นส่วนตัวนี้

- การดูข้อมูลเช่นไอดีใบอนุญาตและข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล ที่อยู่ ที่อยู่อีเมล นั้นจำเป็นสำหรับวัตุประสงค์ในการเรียกเก็บเงิน ตรวจสอบว่าใบอนุญาตเป็นของแท้หรือไม่ และจัดเตรียมการให้บริการของเรา
- ข้อมูลติดต่อและข้อมูลที่อยู่ในคำขอการสนับสนุนของคุณอาจจำเป็นสำหรับการให้บริการสนับสนุน โดยขึ้นอยู่กับช่องทางที่คุณเลือกในการติดต่อเรา เราอาจเก็บรวบรวมข้อมูลที่อยู่อีเมล หมายเลขโทรศัพท์ ข้อมูลใบอนุญาต รายละเอียดผลิตภัณฑ์ และคำอธิบายของกรณีการสนับสนุนของคุณ คุณอาจถูกขอให้ระบุข้อมูลอื่นๆ เพื่อให้บริการสนับสนุนรวดเร็วมากยิ่งขึ้น

การรักษาความลับข้อมูล

ESET เป็นบริษัทที่ดำเนินธุรกิจทั่วโลกผ่านทางหน่วยงานในเครือหรือคู่ค้าเป็นส่วนหนึ่งของเครือข่ายการกระจาย การให้บริการ และการสนับสนุนของเรา ข้อมูลที่ ESET เป็นผู้ประมวลผลอาจได้รับการถ่ายโอนไปยังและจากหน่วยงานในเครือหรือคู่ค้าสำหรับประสิทธิภาพของ EULA เช่นการให้บริการหรือการสนับสนุนหรือการเรียกเก็บเงิน โดยขึ้นอยู่กับตำแหน่งและบริการของคุณที่คุณเลือกที่จะใช้ เราอาจจำเป็นต้องถ่ายโอนข้อมูลของคุณไปยังประเทศที่จำเป็นต้องได้รับการตัดสินใจจากคณะกรรมาธิการยุโรป แม้ในกรณีนี้ การถ่ายโอนข้อมูลทั้งหมดจะต้องเป็นไปตามข้อกำหนดของกฎหมายการป้องกันข้อมูลและจะเกิดขึ้นเฉพาะเมื่อจำเป็นเท่านั้น ข้อตกลงตามสัญญามาตรฐาน ข้อบังคับของบริษัทที่ผูกมัด หรือมาตรการป้องกันที่เหมาะสมอื่นๆ จะต้องมีการจัดตั้งขึ้นโดยไม่มีข้อยกเว้นใดๆ

เรากำลังทำอย่างสุดความสามารถเพื่อป้องกันไม่ให้ข้อมูลถูกจัดเก็บนานเกินความจำเป็น ในขณะที่สามารถให้บริการตามมาตรฐานของ EULA ได้ ระยะเวลาการเก็บรักษาข้อมูลของเราอาจยาวนานกว่าอายุของใบอนุญาตของคุณ ก็เพียงเพื่อให้คุณมีเวลาสำหรับการต่ออายุที่ง่ายดายและสะดวกสบาย สถิติและข้อมูลอื่นๆ จาก ESET LiveGrid® ที่ย่อลงให้เล็กที่สุดและไม่ได้ระบุชื่ออาจได้รับการประมวลผลเพิ่มเติมเพื่อวัตถุประสงค์ทางด้านสถิติ

ESET ใช้มาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมเพื่อให้แน่ใจว่ามีระดับความปลอดภัยที่เหมาะสมกับความเสี่ยงที่อาจเกิดขึ้น เรากำลังพยายามอย่างเต็มที่เพื่อให้มั่นใจได้ถึงการรักษาความลับที่ต่อเนื่อง ความสมบูรณ์ ความพร้อมใช้งาน และความยืดหยุ่นของระบบและบริการด้านการประมวลผล อย่างไรก็ตาม ในกรณีที่ข้อมูลถูกละเมิดจนเป็นผลทำให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของคุณ เราพร้อมที่จะแจ้งให้หน่วยงานกำกับดูแลทราบรวมถึงเจ้าของข้อมูลด้วย ในฐานะเจ้าของข้อมูล คุณมีสิทธิที่จะยื่นเรื่องร้องเรียนต่อหน่วยงานกำกับดูแล

สิทธิของเจ้าของข้อมูล

ESET มีหน้าที่ต้องปฏิบัติตามกฎหมายของประเทศสโลวาเกียและเราต้องปฏิบัติตามกฎหมายว่าด้วยการปกป้องข้อมูลในฐานะส่วนหนึ่งของสหภาพยุโรป คุณมีสิทธิ์ที่จะติดตามสิทธิ์ในฐานะเจ้าของข้อมูลภายใต้เงื่อนไขที่กำหนดโดยกฎหมายคุ้มครองข้อมูลที่บังคับใช้:

- สิทธิ์ในการขอเข้าถึงข้อมูลส่วนบุคคลของคุณจาก ESET
- สิทธิ์ในการแก้ไขข้อมูลส่วนบุคคลของคุณหากไม่ถูกต้อง (คุณมีสิทธิ์ที่จะกรอกข้อมูลส่วนตัวที่ไม่สมบูรณ์)
- สิทธิ์ในการขอลบข้อมูลส่วนบุคคลของคุณ
- สิทธิ์ในการขอข้อจำกัดในการประมวลผลข้อมูลส่วนบุคคลของคุณ
- สิทธิ์ในการคัดค้านการประมวลผล
- สิทธิ์ในการยื่นเรื่องร้องเรียนและ
- สิทธิ์ในการเคลื่อนย้ายข้อมูล

หากคุณประสงค์ที่จะใช้สิทธิ์ของคุณในฐานะที่เป็นเจ้าของข้อมูล หรือหากคุณมีข้อสงสัยหรือข้อกังวล โปรดส่งข้อความมาที่:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk