ESET NOD32 Antivirus

คู่มือผู้ใช้

คลิกที่นี่เพื่อแสดงเวอร์ชันออนไลน์ของเอกสารนี้

Digital Security
Progress. Protected.

ลิขสิทธิ์ ©2024 โดย ESET, spol. s r.o.

ESET NOD32 Antivirus ได้รับการพัฒนาจาก ESET, spol. s r.o.

สำหรับข้อมูลเพิ่มเติม โปรดไปที่ https://www.eset.com

สงวนลิขสิทธิ์ ส่วนหนึ่งส่วนใดของเอกสารนี้ไม่อนุญาตให้ทำซ้ำ จัดเก็บไว้ในระบบการดึงข้อมูล หรือส่งข้อมูลในรูปแบบหรือวิธีการใดๆ ไม่ว่าจะเป็นทางอิเล็กทรอนิกส์ กลไก การทำสำเนาเอกสาร การบันทึก การสแกน หรืออื่นใด โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้เขียน

ESET, spol. s r.o. ขอสงวนสิทธิ์ในการเปลี่ยนแปลงซอฟต์แวร์แอพพลิเคชันใดๆ ที่อธิบายไว้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

ฝ่ายสนับสนุนด้านเทคนิค: https://support.eset.com

REV. 12/4/2024

1 ESET NOD32 Antivirus 1
1.1 มีอะไรใหม่ 2
1.2 ฉันมีผลิตภัณฑ์ใดอยู่ 2
1.3 ความต้องการของระบบ 3
1.3 Microsoft Windows เวอร์ชันที่ล้าสมัย 4
1.4 การป้องกัน 5
1.5 หน้าวิธีใช้ 7
2 การติดตั้ง 8
2.1 โปรแกรมติดตั้งที่ใช้งานออนไลน์ 9
2.2 การติดตั้งแบบออฟไลน์ 10
2.2 การอัพเกรดการสมัครสมาชิก 12
2.2 การอัพเกรดผลิตภัณฑ์ 13
2.2 การดาวน์เกรดการสมัครสมาชิก 14
2.2 การดาวน์เกรดผลิตภัณฑ์ 15
2.3 การติดตั้งตัวแก้ไขปัญหา 16
2.4 สแกนครั้งแรกหลังจากการติดตั้ง 16
2.5 การอัพเกรดเป็นเวอร์ชันล่าสุด 17
2.5 การอัพเกรดอัตโนมัติสำหรับผลิตภัณฑ์ดั้งเดิม 18
2.5 ESET NOD32 Antivirus จะถูกติดตั้ง 18
2.5 เปลี่ยนเป็นผลิตภัณฑ์รุ่นอื่นๆ 19
2.5 การลงทะเบียน 19
2.5 ความคืบหน้าของการเปิดใช้งาน 19
2.5 เปิดใช้งานสำเร็จแล้ว 19
3 การเริ่มต้นใช้งาน 20
3.1 ไอคอนในถาดข้อมูลระบบ 20
3.2 แป้นพิมพ์ลัด 21
3.3 โปรไฟล์ 21
3.4 การอัพเดท 23
4 การเปิดใช้งานผลิตภัณฑ์ 24
4.1 การป้อนรหัสเปิดใช้งานของคุณในระหว่างการเปิดใช้งาน 25
4.2 ใช้บัญชี ESET HOME 26
4.3 เปิดใช้งานเวอร์ชันทดลองใช้ 27
4.4 รหัสเปิดใช้งาน ESET ฟรี 27
4.5 การเปิดใช้งานล้มเหลว-สถานการณ์ทั่วไป 29
4.6 สถานะการสมัครสมาชิก 29
4.6 เปิดใช้งานไม่สำเร็จเนื่องจากการสมัครสมาชิกถูกใช้เกินจำนวน 31
5 การทำงานกับ ESET NOD32 Antivirus 32
5.1 ภาพรวม 33
5.2 การสแกนคอมพิวเตอร์ 36
5.2 เครื่องมือเริ่มต้นการสแกนที่กำหนดเอง 39
5.2 ความคืบหน้าของการสแกน 42
5.2 บันทึกการสแกนคอมพิวเตอร์ 44

5.3 อัพเดท 46
5.3 หน้าต่างข้อความ - ต้องรีสตาร์ท 49
5.3 วิธีสร้างงานการอัพเดท 50
5.4 เครื่องมือ 50
5.4 ไฟล์บันทึก 51
5.4 การกรองบันทึก 54
5.4 กระบวนการที่ทำงานอยู่ 56
5.4 รายงานด้านความปลอดภัย 58
5.4 ESET SysInspector 59
5.4 เครื่องมือวางกำหนดการ 60
5.4 ตัวเลือกการสแกนตามกำหนดการ 63
5.4 ภาพรวมของงานตามกำหนดการ 64
5.4 รายละเอียดงาน 64
5.4 เวลางาน 65
5.4 เวลางาน - หนึ่งครั้ง 65
5.4 เวลางาน - รายวัน 65
5.4 เวลางาน - รายสัปดาห์ 66
5.4 เวลางาน - ตามเหตุการณ์ 66
5.4 งานที่ข้าม 66
5.4 รายละเอียดงาน - อัพเดท 67
5.4 รายละเอียดงาน - เรียกใช้แอพพลิเคชัน 67
5.4 เครื่องมือทำความสะอาดระบบ 68
5.4 กักเก็บ 69
5.4 เลือกตัวอย่างเพื่อวิเคราะห์ 72
5.4 เลือกตัวอย่างเพื่อวิเคราะห์ - ไฟล์ที่น่าสงสัย 73
5.4 เลือกตัวอย่างเพื่อวิเคราะห์-เว็บไซต์ที่น่าสงสัย 74
5.4 เลือกตัวอย่างเพื่อวิเคราะห์-การตรวจพบไฟล์ที่ผิดพลาด 74
5.4 เลือกตัวอย่างเพื่อวิเคราะห์-การตรวจสอบเว็บไซต์ที่ผิดพลาด 75
5.4 เลือกตัวอย่างเพื่อวิเคราะห์-อื่นๆ 75
5.5 การตั้งค่า 75
5.5 การป้องกันคอมพิวเตอร์ 76
5.5 ตรวจพบการแฝงตัว 78
5.5 การป้องกันอินเทอร์เน็ต 81
5.5 การป้องกันฟิชชิ่ง 83
5.5 นำเข้าและส่งออกการตั้งค่า 85
5.6 วิธีใช้และการสนับสนุน 86
5.6 เกี่ยวกับ ESET NOD32 Antivirus 87
5.6 ข่าวสารของ ESET 87
5.6 ส่งข้อมูลการกำหนดค่าระบบ 88
5.6 ฝ่ายสนับสนุนด้านเทคนิค 89
5.7 บัญชี ESET HOME 90
5.7 เชื่อมต่อกับ ESET HOME 91
5.7 ล็อคอินเข้าสู่ ESET HOME 92
5.7 ล็อคอินล้มเหลว - ข้อผิดพลาดทั่วไป 93

5.7 เพิ่มอุปกรณ์ใน ESET HOME 94
6 การตั้งค่าขั้นสูง 95
6.1 กลไกการตรวจจับ 96
6.1 การยกเว้น 96
6.1 การยกเว้นการทำงาน 97
6.1 เพิ่มหรือแก้ไขการยกเว้นการทำงาน 98
6.1 รูปแบบของการยกเว้นพาธ 100
6.1 การยกเว้นการตรวจหา 101
6.1 เพิ่มหรือแก้ไขการยกเว้นการตรวจหา 103
6.1 สร้างวิซาร์ดการยกเว้นการตรวจหา 104
6.1 ตัวเลือกขั้นสูงของกลไกการตรวจจับ 105
6.1 เครื่องมือสแกนการรับส่งข้อมูลเครือข่าย 105
6.1 การป้องกันแบบคลาวด์ 106
6.1 ตัวกรองการยกเว้นสำหรับการป้องกันระบบคลาวด์ 109
6.1 การสแกนมัลแวร์ 109
6.1 โปรไฟล์การสแกน 110
6.1 เป้าหมายการสแกน 111
6.1 การสแกนในสถานะไม่ใช้งาน 112
6.1 การตรวจหาสภาวะไม่ใช้งาน 113
6.1 การสแกนเมื่อเริ่มต้น 113
6.1 การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้น 114
6.1 สื่อที่ถอดเข้าออกได้ 115
6.1 การป้องกันเอกสาร 116
6.1 ระบบป้องกันการบุกรุกโฮสต์ (HIPS) 116
6.1 การยกเว้น HIPS 119
6.1 การตั้งค่า HIPS ขั้นสูง 120
6.1 อนุญาตให้โหลดไดรเวอร์ได้เสมอ 120
6.1 หน้าต่างโต้ตอบ HIPS 121
6.1 โหมดเรียนรู้ได้สิ้นสุดลง 122
6.1 ตรวจพบพฤติกรรมที่สงสัยว่าเป็นการทำงานของแรนซัมแวร์ 123
6.1 การจัดการกฎ HIPS 123
6.1 การตั้งค่ากฎ HIPS 124
6.1 เพิ่มแอพพลิเคชัน/พาธของรีจิสตรีสำหรับ HIPS 128
6.2 อัพเดท 129
6.2 การอัพเดทย้อนหลัง 131
6.2 ช่วงเวลาย้อนกลับ 133
6.2 การอัพเดทผลิตภัณฑ์ 134
6.2 ตัวเลือกการเชื่อมต่อ 134
6.3 การป้องกัน 135
6.3 การป้องกันระบบไฟล์แบบเรียลไทม์ 139
6.3 การยกเว้นกระบวนการ 142
6.3 เพิ่มหรือแก้ไขกระบวนการการยกเว้น 143
6.3 เมื่อใดควรแก้ไขการกำหนดค่าการป้องกันแบบเรียลไทม์ 143
6.3 การตรวจสอบการป้องกันแบบเรียลไทม์ 143

6.3 ควรทำอย่างไรเมื่อการป้องกันแบบเรียลไทม์ไม่ทำงาน 144
6.3 SSL/TLS 145
6.3 กฎการสแกนแอพพลิเคชัน 147
6.3 กฎใบรับรอง 148
6.3 การรับส่งข้อมูลทางเครือข่ายที่เข้ารหัส 149
6.3 การป้องกันอีเมลไคลเอ็นต์ 149
6.3 การป้องกันการส่งข้อมูลอีเมล 150
6.3 แอพพลิเคชันที่ยกเว้น 151
6.3 IP ที่ไม่รวม 152
6.3 การป้องกันกล่องจดหมาย 153
6.3 การรวม 154
6.3 แถบเครื่องมือ Microsoft Outlook 155
6.3 ข้อความยืนยัน 155
6.3 สแกนข้อความซ้ำ 155
6.3 การตอบกลับ 156
6.3 ThreatSense 157
6.3 การป้องกันการเข้าถึงเว็บ 161
6.3 แอพพลิเคชันที่ยกเว้น 163
6.3 IP ที่ไม่รวม 164
6.3 การจัดการรายการที่อยู่ URL 165
6.3 รายการที่อยู่ 167
6.3 สร้างรายการที่อยู่ใหม่ 168
6.3 วิธีการเพิ่มมาสก์ URL 169
6.3 การสแกนการรับส่งข้อมูล HTTP(S) 170
6.3 ThreatSense 170
6.3 การควบคุมอุปกรณ์ 174
6.3 เครื่องมือแก้ไขกฎการควบคุมอุปกรณ์ 176
6.3 อุปกรณ์ที่ตรวจพบ 177
6.3 การเพิ่มกฎการควบคุมอุปกรณ์ 177
6.3 กลุ่มอุปกรณ์ 180
6.3 ThreatSense 182
6.3 ระดับการกำจัด 187
6.3 รายการที่อยู่ที่ยกเว้นจากการตรวจสอบ 187
6.3 พารามิเตอร์ ThreatSense เพิ่มเติม 188
6.4 เครื่องมือ 189
6.4 รายการอัพเดทของ Microsoft Windows 189
6.4 หน้าต่างข้อความ - การอัพเดทระบบ 190
6.4 ข้อมูลการอัพเดท 190
6.4 ESET CMD 190
6.4 ไฟล์บันทึก 192
6.4 โหมดผู้เล่นเกม 193
6.4 การวินิจฉัย 194
6.4 ฝ่ายสนับสนุนด้านเทคนิค 196
6.5 การเชื่อมต่อ 196
6.6 ส่วนติดต่อกับผู้ใช้ 197

6.6 องค์ประกอบของส่วนติดต่อผู้ใช้ 198
6.6 ตั้งค่าการเข้าถึง 199
6.6 รหัสผ่านสำหรับการตั้งค่าขั้นสูง 200
6.6 การสนับสนุนโปรแกรมอ่านหน้าจอ 201
6.7 การแจ้งเตือน 201
6.7 หน้าต่างข้อความ - สถานะแอพพลิเคชัน 202
6.7 การแจ้งเตือนบนเดสก์ท็อป 203
6.7 รายการการแจ้งเตือนบนเดสก์ท็อป 204
6.7 การแจ้งเตือนแบบโต้ตอบ 206
6.7 ข้อความการยืนยัน 208
6.7 การส่งต่อ 209
6.8 การตั้งค่าความเป็นส่วนตัว 212
6.8 แปลงกลับเป็นการตั้งค่าเริ่มต้น 213
6.8 แปลงกลับการตั้งค่าทุกอย่างในส่วนปัจจุบัน 214
6.8 เกิดข้อผิดพลาดขณะบันทึกการกำหนดค่า 214
6.9 เครื่องมือสแกนของบรรทัดคำสั่ง 214
7 คำถามที่พบบ่อย 217
7.1 วิธีอัพเดท ESET NOD32 Antivirus 218
7.2 วิธีลบไวรัสออกจากคอมพิวเตอร์ 218
7.3 วิธีสร้างงานใหม่ในเครื่องมือวางกำหนดการ 219
7.4 วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์ 220
7.5 วิธีปลดล็อคการตั้งค่าขั้นสูง 221
7.6 วิธีแก้ปัญหาการปิดใช้งานผลิตภัณฑ์จาก ESET HOME 221
7.6 ปิดใช้งานผลิตภัณฑ์แล้ว ยกเลิกการเชื่อมต่ออุปกรณ์แล้ว 222
7.6 ยังไม่ได้เปิดใช้งานผลิตภัณฑ์ 223
8.1 โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า 223
8.2 ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง 224
8.3 นโยบายความเป็นส่วนตัว 240

ESET NOD32 Antivirus

ESET NOD32 Antivirus เป็นวิธีการใหม่ในการรักษาความปลอดภัยคอมพิวเตอร์ที่ผสานรวมอย่างแท้จริง กลไกการสแกนเวอร์ชันใหม่ล่าสุดของ ESET LiveGrid® ใช้ความเร็วและความแม่นยำเพื่อทำให้คอมพิวเตอร์ของคุณมีความปลอดภัย เป็นผลให้เกิดระบบอัจฉริยะที่ตื่นตัวอยู่เสมอต่อการโจมตีและซอฟต์แวร์ที่เป็นอันตรายซึ่งอาจก่อให้เกิดอันตรายต่อคอมพิวเตอร์ของคุณ

ESET NOD32 Antivirus เป็นโซลูชันการรักษาความปลอดภัยแบบสมบูรณ์ซึ่งผสมผสานการป้องกันขั้นสูงสุดและการใช้ทรัพยากรของระบบน้อยที่สุด เทคโนโลยีขั้นสูงของเราใช้ปัญญาประดิษฐ์เพื่อป้องกันการแฝงตัวจากไวรัส สปายแวร์ ม้าโทรจัน เวิร์ม แอดแวร์ รูทคิท และการโจมตีอื่นๆ โดยไม่ขัดขวางประสิทธิภาพการทำงานของระบบหรือรบกวนคอมพิวเตอร์ของคุณ

คุณลักษณะและคุณประโยชน์

ส่วนติดต่อผู้ใช้รูปแบบใหม่	ส่วนติดต่อผู้ใช้ในเวอร์ชันนี้ ได้รับการปรับรูปแบบใหม่อย่างเห็นได้ชัดและถูกทำให้ใช้ง่ายขึ้นซึ่งเป็นไปตามผลการทดสอบการใช้งาน การใช้คำและการแจ้งเตือนของ GUI ได้รับการทบทวนอย่างระมัดระวังและส่วนติดต่อให้การสนับสนุนภาษาที่อ่านจากขวาไปซ้ายเช่นฮิบรูและอารบิกแล้วในตอนนี้ ตัวช่วยออนไลน์ รวมเข้ากับ ESET NOD32 Antivirus แล้วในตอนนี้และให้เนื้อหาสนับสนุนที่ได้รับการอัพเดทอย่างต่อเนื่อง
โหมดสีเข้ม	ส่วนขยายที่ช่วยให้คุณสลับหน้าจอเป็นธีมสีเข้มได้อย่างรวดเร็ว คุณสามารถเลือกโทนสีที่คุณต้องการใน องค์ประกอบส่วนต่อประสานผู้ใช้ ได้
การป้องกันไวรัสและสปายแวร์	ตรวจหาและกำจัดไวรัส เวิร์ม โทรจัน และรูทคิททั้งที่รู้จักและไม่รู้จักในเชิงรุกได้มากกว่า การวิเคราะห์พฤติกรรมขั้นสูงจะกำหนดสถานะแม้กระทั่งมัลแวร์ที่ไม่เคยพบเห็นมาก่อน ซึ่งจะช่วยป้องกันคุณจากภัยคุกคามที่ไม่รู้จักและลดประสิทธิภาพภัยคุกคามก่อนที่จะก่อให้เกิดอันตราย การป้องกันการเข้าถึงเว็บไซต์และการป้องกันฟิชชิงทำงานโดยการตรวจสอบการสื่อสารระหว่างเบราว์เซอร์เว็บและเซิร์ฟเวอร์ระยะไกล (รวมถึง SSL) การป้องกันไคลเอ็นต์อีเมล ให้การควบคุมการสื่อสารทางอีเมลที่ได้รับผ่านโปรโตคอล POP3(S) และ IMAP(S)
การอัพเดทเป็นประจำ	การอัพเดทกลไกตรวจหา (ก่อนหน้านี้เรียกว่า "ฐานข้อมูลไวรัส") และโมดูลโปรแกรมเป็นประจำเป็นวิธีที่ดีที่สุดเพื่อให้แน่ใจว่าคอมพิวเตอร์ของคุณจะมีระดับการรักษาความปลอดภัยสูงสุด
ESET LiveGrid® (ความเชื่อถือที่อ้างอิงคลาวด์)	คุณ สามารถตรวจสอบความเชื่อถือของกระบวนการและไฟล์ที่ทำงานอยู่ได้โดยตรงจาก ESET NOD32 Antivirus
การควบคุมอุปกรณ์	สแกนอุปกรณ์ USB การ์ดหน่วยความจำ และซีดี/ดีวีดีทั้งหมดโดยอัตโนมัติ ปิดกั้นสื่อที่ถอดเข้าออกได้ตามประเภทของสื่อ ผู้ผลิต ขนาด และแอตทริบิวต์อื่นๆ
ฟังก์ชันการทำงานของ HIPS	คุณสามารถปรับแต่งการทำงานของระบบได้ละเอียดมากขึ้น ไม่ว่าจะเป็นระบุกฎสำหรับรีจิสตรีของระบบ กระบวนการและโปรแกรมที่ใช้งาน และปรับแต่งลักษณะการรักษาความปลอดภัยของคุณ
โหมดผู้เล่นเกม	เลื่อนหน้าต่างป๊อปอัปทั้งหมด การอัพเดท หรือกิจกรรมอื่นๆ ที่ต้องใช้ทรัพยากรระบบอย่างมากเพื่อเล่นเกมและทำกิจกรรมแบบเต็มหน้าจออื่นๆ

จำเป็นต้องเปิดใช้งานการสมัครสมาชิกเพื่อให้ฟีเจอร์ ESET NOD32 Antivirus ทำงานได้ตามปกติ เราขอแนะนำให้คุณ

ต่ออายุการสมัครสมาชิกของคุณหลายสัปดาห์ก่อนที่การสมัครสมาชิก ESET NOD32 Antivirus จะหมดอายุ

มีอะไรใหม่

มีอะไรใหม่ใน ESET NOD32 Antivirus 17.1

- การปรับปรุงเล็กน้อยในตัวตรวจสอบเครือข่าย
- การแก้ไขข้อบกพร่องเล็กน้อยและการปรับปรุงอื่นๆ

> i วิธีปิดใช้งาน **การแจ้งเตือนใหม่**:
> **1.**เปิด การตั้งค่าขั้นสูง > **การแจ้งเตือน** > **การแจ้งเตือนบนเดสก์ท็อป**
> **2.**คลิก **แก้ไข** ถัดจาก **การแจ้งเตือนบนเดสก์ท็อป**
> **3.**ยกเลิกเครื่องหมายที่ทำไว้ในช่อง **แสดงการแจ้งเตือนใหม่** แล้วคลิก **ตกลง**
> สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการแจ้งเตือน โปรดดูส่วน การแจ้งเตือน

> i หากต้องการทราบรายละเอียดของการเปลี่ยนแปลงใน ESET NOD32 Antivirus ให้ดู บันทึกการเปลี่ยนแปลงของ ESET NOD32 Antivirus

ฉันมีผลิตภัณฑ์ใดอยู่

ESET มีความปลอดภัยหลากหลายชั้นให้เลือกสรร พร้อมผลิตภัณฑ์ใหม่ๆ ตั้งแต่โซลูชันป้องกันไวรัสที่ทรงพลังและรวดเร็วไปจนถึงโซลูชันป้องกันไวรัสแบบครบวงจรซึ่งใช้ทรัพยากรของระบบน้อยที่สุด ดังนี้:

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

เพื่อระบุว่าคุณติดตั้งผลิตภัณฑ์ใดเอาไว้ ให้เปิด หน้าต่างโปรแกรมหลัก แล้วคุณจะเห็นชื่อของผลิตภัณฑ์ที่ด้านบนสุดของหน้าต่าง (โปรดดู บทความฐานความรู้)

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
กลไกการตรวจจับ	✔	✔	✔	✔
การเรียนรู้ของเครื่องขั้นสูง	✔	✔	✔	✔
การป้องกันการโจมตีแบบ Exploit	✔	✔	✔	✔
การป้องกันการโจมตีที่ใช้สคริปต์	✔	✔	✔	✔
การป้องกันฟิชชิ่ง	✔	✔	✔	✔
การป้องกันการเข้าถึงเว็บ	✔	✔	✔	✔
HIPS (รวมถึง การป้องกันแรนซั่มแวร์)	✔	✔	✔	✔
การป้องกันสแปม		✔	✔	✔
ไฟร์วอลล์		✔	✔	✔
ตรวจสอบเครือข่าย		✔	✔	✔
การป้องกัน Webcam		✔	✔	✔
การป้องกันการโจมตีเครือข่าย		✔	✔	✔
การป้องกันบอตเน็ต		✔	✔	✔
การธนาคารและการท่องเว็บอย่างปลอดภัย		✔	✔	✔
ความเป็นส่วนตัวและความปลอดภัยของเบราว์เซอร์		✔	✔	✔
การควบคุมเนื้อหา		✔	✔	✔
การป้องกันการโจรกรรม		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

ผลิตภัณฑ์ข้างต้นบางรายการอาจไม่สามารถใช้ได้สำหรับภาษา/ภูมิภาคของคุณ

ความต้องการของระบบ

เพื่อให้สามารถทำงานได้อย่างเหมาะสม ระบบของคุณควรเป็นไปตามข้อกำหนดด้านฮาร์ดแวร์และซอฟต์แวร์สำหรับ ESET NOD32 Antivirus ดังต่อไปนี้:

ตัวประมวลผลที่รองรับ

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

ตัวประมวลผล ARM64, 1 GHz หรือสูงกว่า

รองรับระบบปฏิบัติการ

Microsoft® Windows® 11

Microsoft® Windows® 10

จะต้องติดตั้งการสนับสนุนสำหรับ Azure Code Signing บนระบบปฏิบัติการ Windows ทั้งหมดเพื่อติดตั้งหรืออัพเกรดผลิตภัณฑ์ ESET ที่วางจำหน่ายหลังเดือนกรกฎาคม 2023 ข้อมูลเพิ่มเติม

โปรดพยายามอัพเดทระบบปฏิบัติการของคุณให้ทันสมัยเสมอ

ความต้องการของคุณลักษณะ ESET NOD32 Antivirus

ดูความต้องการของระบบสำหรับคุณลักษณะบางรายการของ ESET NOD32 Antivirus ในตารางด้านล่าง:

คุณลักษณะ	ความต้องการ
Intel® Threat Detection Technology	ดู ตัวประมวลผลที่รองรับ
พื้นหลังโปร่งใส	Windows 10 เวอร์ชัน RS4 ขึ้นไป
เครื่องมือทำความสะอาดเฉพาะทาง	ตัวประมวลผลที่ไม่ใช่ ARM64
เครื่องมือทำความสะอาดระบบ	ตัวประมวลผลที่ไม่ใช่ ARM64
การป้องกันการโจมตีแบบ Exploit	ตัวประมวลผลที่ไม่ใช่ ARM64
การตรวจสอบการทำงานเชิงลึก	ตัวประมวลผลที่ไม่ใช่ ARM64

อื่นๆ

ต้องใช้การเชื่อมต่ออินเทอร์เน็ตในการเปิดใช้งานและอัพเดท ESET NOD32 Antivirus เพื่อให้ทำงานได้อย่างปกติ

โปรแกรมป้องกันไวรัสสองโปรแกรมที่ทำงานพร้อมกันบนอุปกรณ์เดียวทำให้เกิดความขัดแย้งของทรัพยากรระบบที่หลีกเลี่ยงไม่ได้ เช่น การชะลอตัวของระบบเพื่อให้ไม่สามารถทำงานได้

Microsoft Windows เวอร์ชันที่ล้าสมัย

ปัญหา

- คุณต้องการติดตั้ง ESET NOD32 Antivirus เวอร์ชันล่าสุดบนคอมพิวเตอร์ที่ใช้ Windows 7, Windows 8 (8.1) หรือ Windows Home Server 2011

- ESET NOD32 Antivirus แสดงข้อผิดพลาด **ระบบปฏิบัติการล้าสมัย** ระหว่างการติดตั้ง

รายละเอียด

ESET NOD32 Antivirus เวอร์ชันล่าสุด ต้องใช้ระบบปฏิบัติการ Windows 10 หรือ Windows 11

โซลูชัน

การแก้ปัญหาที่ใช้ได้มีดังนี้:

อัพเกรดเป็น Windows 10 หรือ Windows 11

กระบวนการปรับรุ่นจะค่อนข้างง่าย และในหลายกรณีคุณสามารถทำได้โดยไม่สูญเสียไฟล์ของคุณ: ก่อนการอัพเกรดเป็น Windows 10:

1. การสำรองข้อมูลสำคัญ

2. อ่าน คำถามที่พบบ่อยเกี่ยวกับการอัพเกรดเป็น Windows 10 ของ Microsoft หรือ คำถามที่พบบ่อยในการอัพเกรดเป็น Windows 11 และอัพเดทระบบปฏิบัติการ Windows ของคุณ

ติดตั้ง ESET NOD32 Antivirus เวอร์ชัน 16.0

หากคุณไม่สามารถอัพเกรด Windows ได้ ให้ติดตั้ง ESET NOD32 Antivirus เวอร์ชัน 16.0 หากต้องการข้อมูลเพิ่มเติม โปรดดูที่วิธีใช้แบบออนไลน์ของ ESET NOD32 Antivirus เวอร์ชัน 16.0

การป้องกัน

เมื่อคุณทำงานกับคอมพิวเตอร์ของคุณ และโดยเฉพาะเมื่อคุณเรียกใช้อินเทอร์เน็ต โปรดระลึกไว้ว่าไม่มีระบบป้องกันไวรัสใดในโลกที่สามารถกำจัดความเสี่ยงจากการตรวจหา และ การโจมตีระยะไกล เมื่อต้องการเพิ่มการป้องกันและความสะดวกสูงสุด จึงจำเป็นที่คุณต้องใช้โซลูชันป้องกันไวรัสอย่างถูกต้องและปฏิบัติตามกฎที่มีประโยชน์ต่างๆ:

อัพเดทเป็นประจำ

ตามสถิติจาก ESET LiveGrid® การแฝงตัวแบบใหม่และไม่ซ้ำกันหลายพันแบบจะถูกสร้างขึ้นทุกวันเพื่อให้สามารถผ่าน

การวัดความปลอดภัยที่มีอยู่และสร้างผลกำไรให้กับผู้เขียนได้ โดยสร้างความเสียหายให้เกิดขึ้นกับผู้ใช้อื่น ผู้เชี่ยวชาญที่ห้องปฏิบัติการไวรัสของ ESET จะวิเคราะห์การคุกคามเหล่านี้ทุกวัน และจัดเตรียมและเผยแพร่การอัพเดทเพื่อปรับปรุงระดับการป้องกันอย่างต่อเนื่องสำหรับผู้ใช้ของเรา เพื่อให้แน่ใจว่าการอัพเดทเหล่านี้มีประสิทธิภาพสูงสุด จึงจำเป็นต้องกำหนดค่าการอัพเดทอย่างถูกต้องในระบบของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีกำหนดค่าการอัพเดท โปรดดูในบท [การตั้งค่าการอัพเดท]

ดาวน์โหลดโปรแกรมแก้ไขด้านความปลอดภัย

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

การสำรองข้อมูลสำคัญ

ผู้เขียนมัลแวร์จะไม่สนใจเกี่ยวกับความจำเป็นของผู้ใช้ และการทำงานของโปรแกรมที่เป็นอันตรายมักจะนำไปสู่การทำงานไม่ถูกต้องทั้งหมดของระบบปฏิบัติการและการสูญหายของข้อมูลสำคัญ ดังนั้นจึงต้องสำรองข้อมูลสำคัญและที่เป็นความลับของคุณไปยังแหล่งที่มาภายนอกอยู่เสมอ เช่น DVD หรือฮาร์ดไดรฟ์ภายนอก ซึ่งจะทำให้กู้คืนข้อมูลของคุณได้ง่ายดายและรวดเร็วยิ่งขึ้นในกรณีที่ระบบล้มเหลว

สแกนคอมพิวเตอร์เพื่อหาไวรัสเป็นประจำ

การตรวจหาไวรัส เวิร์ม โทรจัน และรูทคิทที่รู้จักและไม่รู้จักได้มากขึ้นจะมีการจัดการโดยโมดูลการป้องกันระบบไฟล์แบบเรียลไทม์ ซึ่งหมายความว่าทุกครั้งที่คุณเข้าถึงหรือเปิดไฟล์ ระบบจะสแกนเพื่อหากิจกรรมของมัลแวร์ เราขอแนะนำให้คุณเรียกใช้การสแกนคอมพิวเตอร์แบบเต็มรูปแบบอย่างน้อยเดือนละครั้ง เนื่องจากฐานข้อมูลมัลแวร์อาจหลากหลายและกลไกตรวจหาจะอัพเดทตัวเองทุกวัน

ปฏิบัติตามกฎการรักษาความปลอดภัยพื้นฐาน

กฎนี้เป็นกฎที่มีประโยชน์และมีประสิทธิภาพมากที่สุด ซึ่งผู้ใช้ควรให้ความสนใจอยู่เสมอ ในปัจจุบัน การบุกรุกจำนวนมากต้องการการดำเนินการของผู้ใช้เพื่อให้ระบบทำงานและกระจายการบุกรุก หากคุณมีความระมัดระวังเมื่อ

เปิดไฟล์ใหม่ คุณจะสามารถประหยัดเวลาและความพยายามที่จะต้องใช้ในการกำจัดการบุกรุกได้เป็นอย่างมาก คำแนะนำที่มีประโยชน์มีดังนี้:

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

หน้าวิธีใช้

ยินดีต้อนรับสู่คู่มือผู้ใช้ ESET NOD32 Antivirus ข้อมูลที่ให้ไว้นี้จะแนะนำคุณเกี่ยวกับผลิตภัณฑ์ของคุณและช่วยทำให้คอมพิวเตอร์ของคุณมีความปลอดภัยมากยิ่งขึ้น

การเริ่มต้นใช้งาน

ก่อนใช้ ESET NOD32 Antivirus คุณสามารถอ่านเกี่ยวกับ ประเภทของการตรวจหา และ การโจมตีจากระยะไกล หลายประเภทที่คุณอาจพบเมื่อใช้คอมพิวเตอร์ได้ เรายังได้รวบรวมรายการ คุณลักษณะใหม่ ที่เปิดตัวใน ESET NOD32 Antivirus อีกด้วย

เริ่มต้นด้วย การติดตั้ง ESET NOD32 Antivirus ถ้าคุณได้ติดตั้ง ESET NOD32 Antivirus แล้ว โปรดดู การทำงานกับ ESET NOD32 Antivirus

วิธีใช้หน้าวิธีใช้ของ ESET NOD32 Antivirus

ความช่วยเหลือออนไลน์แบ่งออกเป็นหลายบทและหลายบทย่อย กด **F1** ใน ESET NOD32 Antivirus เพื่อดูข้อมูลเกี่ยวกับหน้าต่างที่เปิดอยู่ในปัจจุบัน

โปรแกรมช่วยให้คุณค้นหาหัวข้อวิธีใช้ด้วยคำหลัก หรือค้นหาเนื้อหาโดยพิมพ์คำหรือวลี ความแตกต่างระหว่างสองวิธีนี้ก็คือ คำหลักนั้นอาจมีเนื้อหาเกี่ยวข้องกับหน้าวิธีใช้ที่ไม่ได้มีคำหลักนั้นๆ อยู่ในข้อความก็ได้ การค้นหาตามคำและวลีจะค้นหาเนื้อหาของหน้าวิธีใช้ทั้งหมด และแสดงเฉพาะที่มีคำหรือวลีนั้นๆ ในข้อความเท่านั้น

เพื่อความสอดคล้องและเพื่อป้องกันความสับสน คำศัพท์ที่ใช้ในคู่มือนี้จะขึ้นอยู่กับอินเทอร์เฟซผู้ใช้ของ ESET NOD32 Antivirus นอกจากนี้เรายังใช้ชุดรูปแบบสัญลักษณ์ชุดหนึ่งเพื่อเน้นหัวข้อต่างๆ ที่น่าสนใจเป็นพิเศษหรือมีความสำคัญ

บันทึกย่อเป็นเพียงการสำรวจสั้นๆ เท่านั้น ถึงแม้ว่าคุณจะสามารถข้ามได้ แต่บันทึกย่อมีข้อมูลที่มีประโยชน์อย่างยิ่ง เช่น คุณสมบัติที่เฉพาะเจาะจงหรือลิงก์ไปที่หัวข้อบางหัวข้อ

ซึ่งคุณควรให้ความใส่ใจกับบันทึกนี้ เราจึงขอแนะนำไม่ให้คุณข้าม ซึ่งโดยปกติแล้ว จะให้ข้อมูลที่ไม่ส่งผลกระทบร้ายแรง แต่เป็นข้อมูลที่สำคัญ

นี่เป็นข้อมูลที่ต้องให้ความใส่ใจและระมัดระวังเป็นพิเศษ มีการระบุคำเตือนไว้อย่างเจาะจงเพื่อป้องกันไม่ให้คุณทำสิ่งผิดพลาดที่อาจเป็นอันตราย อ่านและทำความเข้าใจข้อความ เนื่องจากเป็นการอ้างอิงถึงการตั้งค่าระบบที่มีความละเอียดอ่อนสูงหรือสิ่งที่มีความเสี่ยง

การดำเนินการนี้เป็นรูปแบบการใช้หรือตัวอย่างภาคปฏิบัติซึ่งมีวัตถุประสงค์เพื่อช่วยให้คุณเข้าใจว่าสามารถใช้ฟังก์ชันหรือคุณลักษณะบางอย่างได้อย่างไร

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

วิธีใช้ออนไลน์ เป็นแหล่งข้อมูลหลักของเนื้อหาวิธีใช้ วิธีใช้ออนไลน์เวอร์ชันล่าสุดจะแสดงโดยอัตโนมัติเมื่อคุณมีการเชื่อมต่ออินเทอร์เน็ตที่ใช้งานได้

การติดตั้ง

สามารถติดตั้ง ESET NOD32 Antivirus ในคอมพิวเตอร์ของคุณได้หลายวิธี วิธีการติดตั้งอาจแตกต่างกันไป ทั้งนี้ขึ้นอยู่กับประเทศและวิธีการแจกจ่าย:

- Live Installer — ดาวน์โหลดจากเว็บไซต์ของ ESET หรือ CD/DVD แพ็คเกจติดตั้งจะเหมือนกันสำหรับทุกภาษา (เลือกภาษาที่เหมาะสม) Live Installer เป็นไฟล์ขนาดเล็ก ไฟล์เพิ่มเติมที่จำเป็นในการติดตั้ง ESET NOD32 Antivirus จะถูกดาวน์โหลดโดยอัตโนมัติ

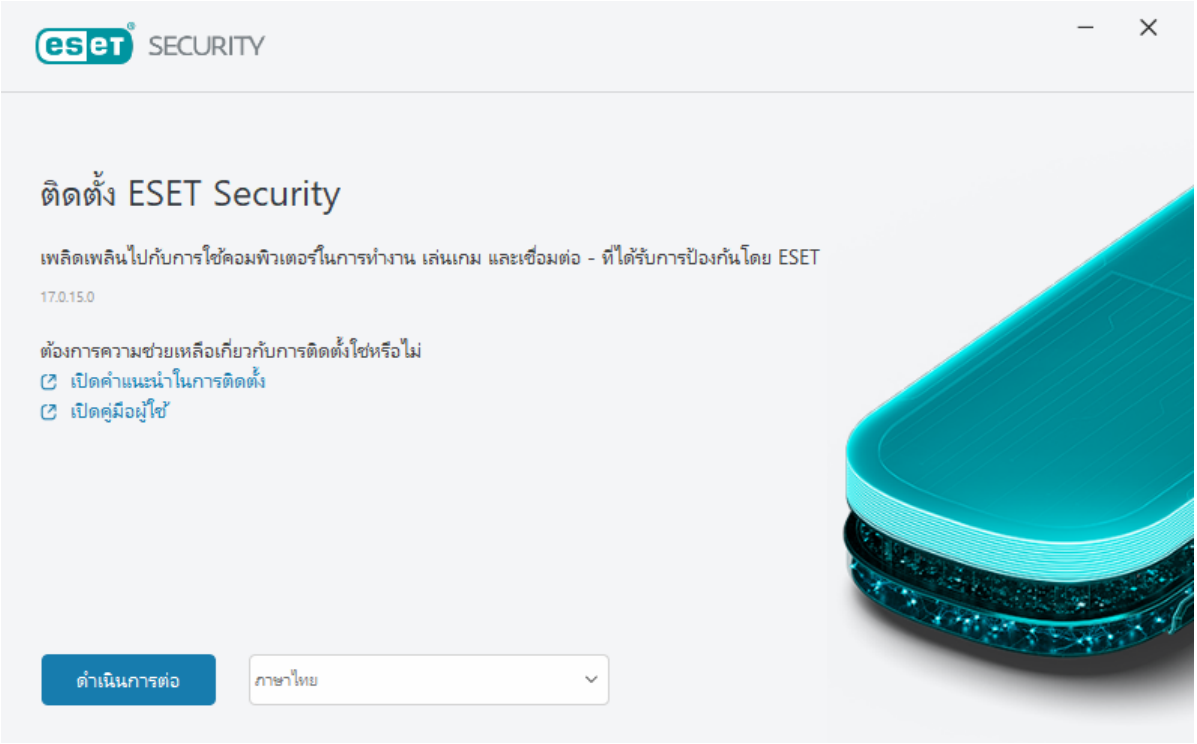
- การติดตั้งแบบออฟไลน์ — ใช้ไฟล์ .exe ที่มีขนาดใหญ่กว่าไฟล์ Live Installer และไม่จำเป็นต้องเชื่อมต่ออินเทอร์เน็ตหรือไฟล์เพิ่มเติมเพื่อดำเนินการติดตั้งให้เสร็จสมบูรณ์

โปรดตรวจสอบให้แน่ใจว่าไม่มีโปรแกรมป้องกันไวรัสอื่นติดตั้งอยู่บนคอมพิวเตอร์ของคุณก่อนที่คุณจะติดตั้ง ESET NOD32 Antivirus ถ้ามีการติดตั้งโซลูชันการป้องกันไวรัสสองชนิดขึ้นไปบนคอมพิวเตอร์เครื่องเดียว อาจมีการทำงานที่ขัดแย้งกัน ขอแนะนำให้คุณลบการติดตั้งโปรแกรมป้องกันไวรัสอื่นในระบบของคุณ โปรดดู บทความฐานความรู้ของ ESET สำหรับรายการของเครื่องมือถอนการติดตั้งสำหรับซอฟต์แวร์ป้องกันไวรัสที่ใช้กันทั่วไป (ให้บริการเป็นภาษาอังกฤษและภาษาอื่นๆ อีกมากมาย)

โปรแกรมติดตั้งที่ใช้งานออนไลน์

เมื่อคุณดาวน์โหลด แพ็คเกจติดตั้ง Live Installer เรียบร้อยแล้ว ให้คลิกสองครั้งที่ไฟล์การติดตั้งและทำตามคำแนะนำแบบทีละขั้นตอนในวิซาร์ดตัวติดตั้ง

สำหรับการติดตั้งประเภทนี้ คุณต้องเชื่อมต่ออินเทอร์เน็ต



1.เลือกภาษาที่เหมาะสมจากเมนูแบบเลื่อนลงแล้วคลิก **ดำเนินการต่อ**

หากคุณกำลังติดตั้งเวอร์ชันที่ใหม่กว่าทับเวอร์ชันก่อนหน้าที่มีการตั้งค่าที่ป้องกันด้วยรหัสผ่าน ให้ป้อนรหัสผ่านของคุณด้วย คุณสามารถกำหนดค่ารหัสผ่านการตั้งค่าได้ใน การตั้งค่าการเข้าถึง

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

- ESET LiveGrid® ระบบคำติชม

- แอพพลิเคชันที่อาจไม่พึงประสงค์
- โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า

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

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

4. หากคุณดำเนินการต่อโดยไม่เชื่อมต่อกับ ESET HOME ให้เลือกตัวเลือกการเปิดใช้งาน หากคุณกำลังติดตั้งเวอร์ชั่นที่ใหม่กว่าทับเวอร์ชั่นก่อนหน้า ระบบจะป้อน **รหัสเปิดใช้งาน** ให้โดยอัตโนมัติ

5. วิซาร์ดการติดตั้งจะกำหนดผลิตภัณฑ์ของ ESET ที่จะติดตั้งตามการสมัครสมาชิกของคุณ เวอร์ชันที่มีคุณลักษณะด้านความปลอดภัยมากที่สุดจะถูกเลือกไว้ล่วงหน้าเสมอ คลิก **เปลี่ยนผลิตภัณฑ์** หากคุณต้องการติดตั้งผลิตภัณฑ์ ESET เวอร์ชันอื่น คลิก **ดำเนินการต่อ** เพื่อเริ่มกระบวนการติดตั้ง ซึ่งอาจใช้เวลาสักครู่

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

6. คลิก**เสร็จสิ้น** เพื่อออกจากวิซาร์ดการติดตั้ง

การติดตั้งตัวแก้ไขปัญหา

> หลังจากที่ผลิตภัณฑ์ถูกติดตั้งและเปิดใช้งาน โมดูลจะเริ่มดาวน์โหลด การป้องกันกำลังเริ่มต้นและคุณสมบัติอาจยังทำงานได้ไม่เต็มที่จนกว่าการดาวน์โหลดจะเสร็จสมบูรณ์

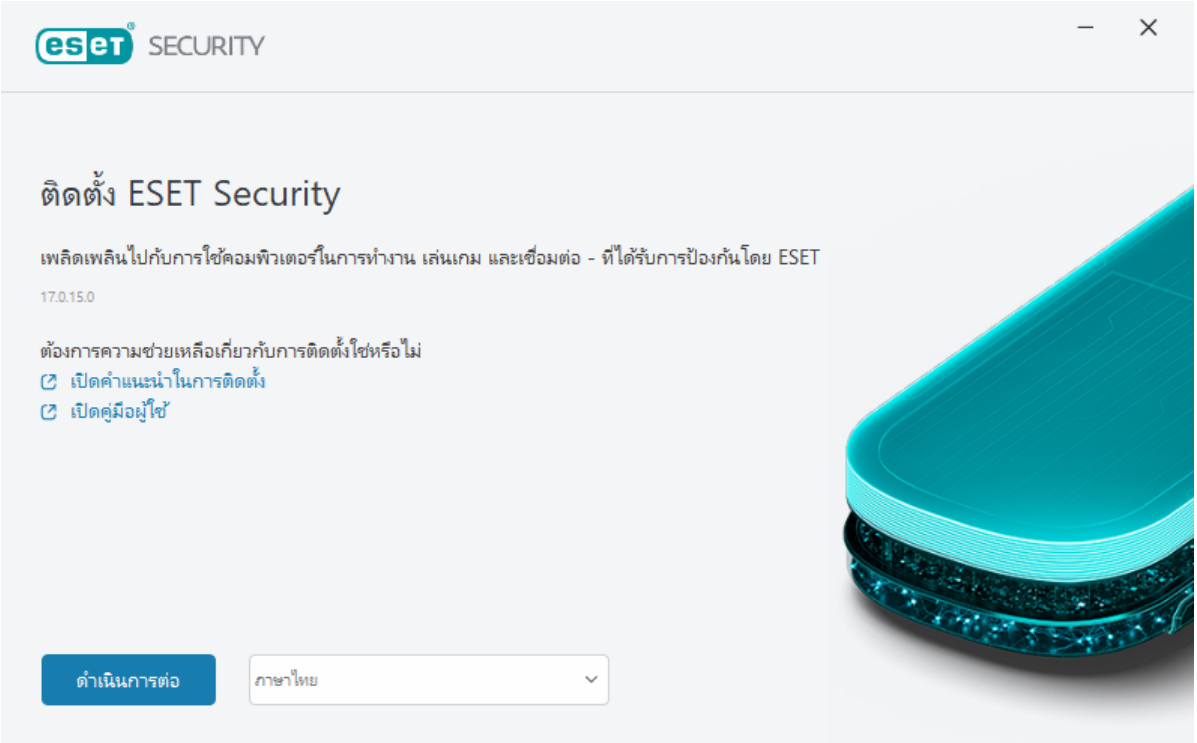
การติดตั้งแบบออฟไลน์

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

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

> หากคุณมีการเชื่อมต่ออินเทอร์เน็ตที่ใช้งานอยู่ ให้ ติดตั้งผลิตภัณฑ์ ESET ของคุณโดยใช้ Live Installer

เมื่อคุณเริ่มต้นตัวติดตั้งแบบออฟไลน์ (.exe) วิซาร์ดการติดตั้งจะนำคุณเข้าสู่กระบวนการตั้งค่า



1.เลือกภาษาที่เหมาะสมจากเมนูแบบเลื่อนลงแล้วคลิก **ดำเนินการต่อ**

> ℹ หากคุณกำลังติดตั้งเวอร์ชันที่ใหม่กว่าทับเวอร์ชันก่อนหน้าที่มีการตั้งค่าที่ป้องกันด้วยรหัสผ่าน ให้ป้อนรหัสผ่านของคุณด้วย คุณสามารถกำหนดค่ารหัสผ่านการตั้งค่าได้ใน การตั้งค่าการเข้าถึง

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

- ESET LiveGrid® ระบบคำติชม
- แอพพลิเคชันที่อาจไม่พึงประสงค์
- โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า

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

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

4. คลิก **ข้ามการเปิดใช้งาน** โดย ESET NOD32 Antivirus ต้องเปิดใช้งานหลังจากการติดตั้งเพื่อให้สามารถทำงานได้อย่างสมบูรณ์ การเปิดใช้งานผลิตภัณฑ์ ต้องมีการเชื่อมต่ออินเทอร์เน็ตที่ใช้งานอยู่

5. วิซาร์ดการติดตั้งจะแสดงผลิตภัณฑ์ ESET ที่จะติดตั้งตามตัวติดตั้งแบบออฟไลน์ที่ดาวน์โหลดมา คลิก **ดำเนิน**

การต่อ เพื่อเริ่มกระบวนการติดตั้ง ซึ่งอาจใช้เวลาสักครู่

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

6. คลิก**เสร็จสิ้น** เพื่อออกจากวิซาร์ดการติดตั้ง

⚠ การติดตั้งตัวแก้ไขปัญหา

การอัพเกรดการสมัครสมาชิก

หน้าต่างแจ้งเตือนนี้จะปรากฏขึ้นเมื่อการสมัครสมาชิกที่ใช้เปิดใช้งานผลิตภัณฑ์ ESET ของคุณมีการเปลี่ยนแปลง การสมัครสมาชิกที่มีการเปลี่ยนแปลงทำให้คุณสามารถเปิดใช้งานผลิตภัณฑ์ที่มีฟีเจอร์ความปลอดภัยมากขึ้นได้ หากไม่มีการดำเนินการใดๆ ESET NOD32 Antivirus จะแสดงหน้าต่างการแจ้งเตือนหนึ่งครั้ง ซึ่งเรียกว่า **เปลี่ยนไปใช้ผลิตภัณฑ์ที่มีคุณสมบัติมากกว่า**

ใช่ (แนะนำ) – จะติดตั้งผลิตภัณฑ์ที่มีคุณสมบัติความปลอดภัยมากกว่าให้โดยอัตโนมัติ

ไม่ ขอบคุณ –จะไม่ทำการเปลี่ยนแปลงใดๆ และการแจ้งเตือนจะหายไปอย่างถาวร

หากต้องการเปลี่ยนผลิตภัณฑ์ภายหลัง โปรดดูบทความฐานความรู้ ESET ของเรา หากต้องการข้อมูลเพิ่มเติมเกี่ยวกับการสมัครสมาชิก ESET โปรดดูที่ คำถามที่พบบ่อยเกี่ยวกับการสมัครสมาชิก

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
การป้องกันการโจมตีเครือข่าย		✔	✔	✔
การป้องกันบอตเน็ต		✔	✔	✔
การธนาคารและการท่องเว็บอย่างปลอดภัย		✔	✔	✔
ความเป็นส่วนตัวและความปลอดภัยของเบราว์เซอร์		✔	✔	✔
การควบคุมเนื้อหา		✔	✔	✔
การป้องกันการโจรกรรม		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

การอัพเกรดผลิตภัณฑ์

คุณได้ดาวน์โหลดโปรแกรมติดตั้งตามค่าเริ่มต้นและตัดสินใจเปลี่ยนแปลงผลิตภัณฑ์ที่จะเปิดใช้งาน หรือคุณต้องการเปลี่ยนผลิตภัณฑ์ที่ติดตั้งเป็นผลิตภัณฑ์ที่มีคุณสมบัติความปลอดภัยมากกว่า

เปลี่ยนแปลงผลิตภัณฑ์ในระหว่างการติดตั้ง

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
การป้องกันบอตเน็ต		✔	✔	✔
การธนาคารและการท่องเว็บอย่างปลอดภัย		✔	✔	✔
ความเป็นส่วนตัวและความปลอดภัยของเบราว์เซอร์		✔	✔	✔
การควบคุมเนื้อหา		✔	✔	✔
การป้องกันการโจรกรรม		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

การดาวน์เกรดการสมัครสมาชิก

หน้าต่างโต้ตอบนี้จะปรากฏขึ้นเมื่อการสมัครสมาชิกที่ใช้เปิดใช้งานผลิตภัณฑ์ ESET ของคุณมีการเปลี่ยนแปลง การสมัครสมาชิกที่มีการเปลี่ยนแปลงสามารถใช้ได้เฉพาะกับผลิตภัณฑ์ ESET อื่นที่มีฟีเจอร์ความปลอดภัยน้อยกว่าเท่านั้น ผลิตภัณฑ์นี้จะได้รับการเปลี่ยนโดยอัตโนมัติเพื่อไม่ให้คุณสูญเสียการป้องกัน

หากต้องการข้อมูลเพิ่มเติมเกี่ยวกับการสมัครสมาชิก ESET โปรดดูที่ คำถามที่พบบ่อยเกี่ยวกับการสมัครสมาชิก

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
การป้องกันบอตเน็ต		✔	✔	✔
การธนาคารและการท่องเว็บอย่างปลอดภัย		✔	✔	✔
ความเป็นส่วนตัวและความปลอดภัยของเบราว์เซอร์		✔	✔	✔
การควบคุมเนื้อหา		✔	✔	✔
การป้องกันการโจรกรรม		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

การดาวน์เกรดผลิตภัณฑ์

ผลิตภัณฑ์ที่คุณได้ติดตั้งในตอนนี้มีคุณสมบัติความปลอดภัยมากกว่าผลิตภัณฑ์ที่คุณกำลังจะเปิดใช้งาน

ตารางต่อไปนี้จะระบุรายละเอียดคุณลักษณะต่างๆ ที่มีอยู่ในผลิตภัณฑ์แต่ละรุ่น

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
กลไกการตรวจจับ	✔	✔	✔	✔
การเรียนรู้ของเครื่องขั้นสูง	✔	✔	✔	✔
การป้องกันการโจมตีแบบ Exploit	✔	✔	✔	✔
การป้องกันการโจมตีที่ใช้สคริปต์	✔	✔	✔	✔
การป้องกันฟิชชิ่ง	✔	✔	✔	✔
การป้องกันการเข้าถึงเว็บ	✔	✔	✔	✔
HIPS (รวมถึง การป้องกันแรนซั่มแวร์)	✔	✔	✔	✔
การป้องกันสแปม		✔	✔	✔
ไฟร์วอลล์		✔	✔	✔
ตรวจสอบเครือข่าย		✔	✔	✔
การป้องกัน Webcam		✔	✔	✔
การป้องกันการโจมตีเครือข่าย		✔	✔	✔
การป้องกันบอตเน็ต		✔	✔	✔
การธนาคารและการท่องเว็บอย่างปลอดภัย		✔	✔	✔
ความเป็นส่วนตัวและความปลอดภัยของเบราว์เซอร์		✔	✔	✔
การควบคุมเนื้อหา		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
การป้องกันการโจรกรรม		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

การติดตั้งตัวแก้ไขปัญหา

หากพบปัญหาในระหว่างการติดตั้ง วิซาร์ดการติดตั้งจะให้ตัวแก้ไขปัญหาที่จะช่วยแก้ปัญหาหากเป็นไปได้

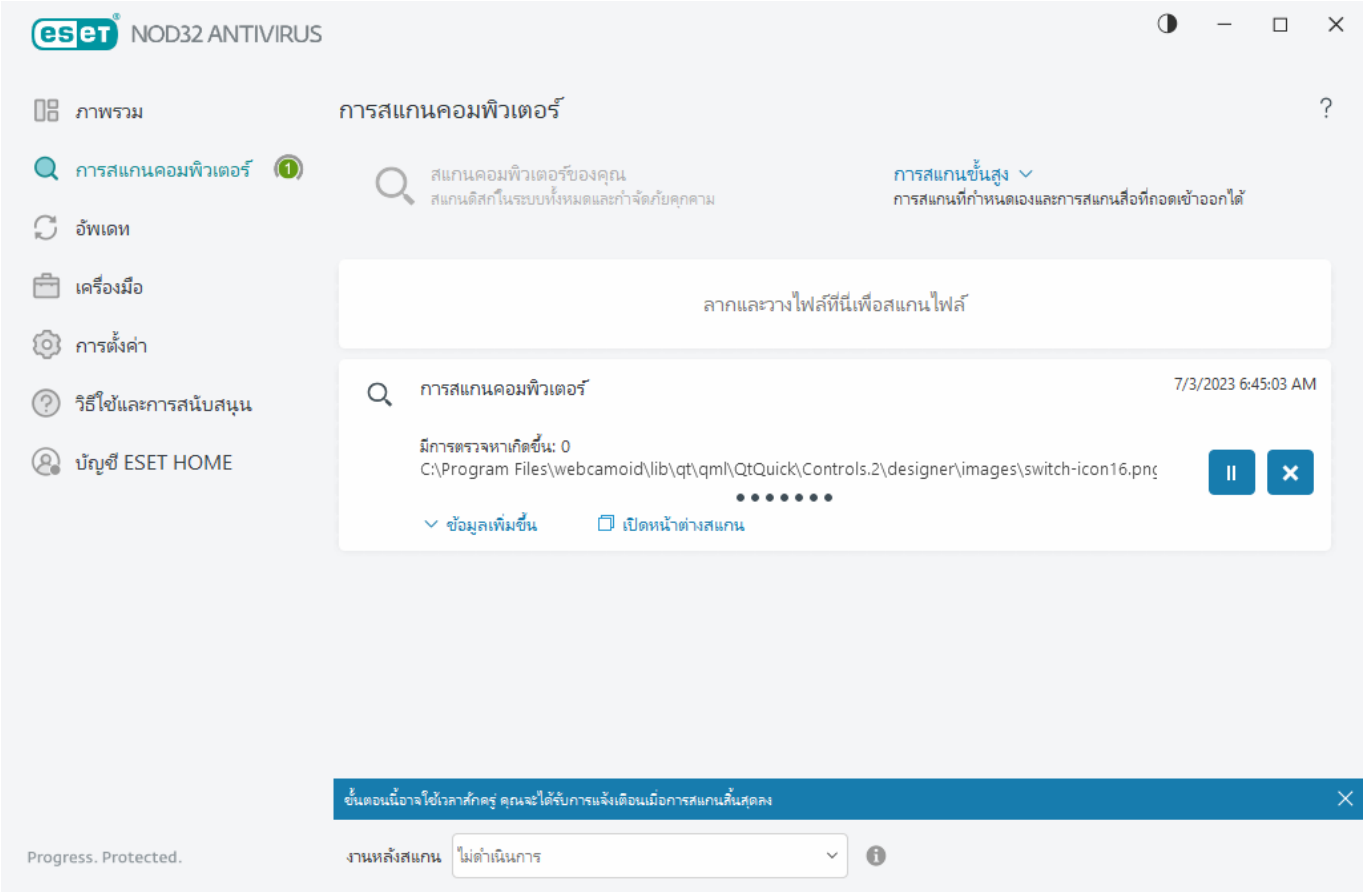
คลิก **เรียกใช้ตัวแก้ไขปัญหา** เพื่อให้ตัวแก้ไขปัญหาเริ่มทำงาน เมื่อดำเนินการเสร็จสิ้น โปรดดำเนินการตามโซลูชันที่แนะนำ

หากปัญหายังคงอยู่ โปรดดูรายการ ข้อผิดพลาดทั่งไปของการติดตั้งและวิธีแก้ไข

สแกนครั้งแรกหลังจากการติดตั้ง

หลังจากที่ติดตั้ง ESET NOD32 Antivirus การสแกนคอมพิวเตอร์จะเริ่มโดยอัตโนมัติหลังจากที่อัปเดตสำเร็จเพื่อตรวจสอบรหัสที่เป็นอันตราย

คุณยังสามารถเริ่มการสแกนคอมพิวเตอร์ด้วยตัวเองได้จาก หน้าต่างโปรแกรมหลัก โดยการคลิกที่ **การสแกนคอมพิวเตอร์** > **สแกนคอมพิวเตอร์ของคุณ** เมื่อต้องการข้อมูลเพิ่มเติมเกี่ยวกับการสแกนคอมพิวเตอร์ ให้ดูที่ การสแกนคอมพิวเตอร์



การอัพเกรดเป็นเวอร์ชันล่าสุด

ESET NOD32 Antivirus เวอร์ชันใหม่ได้ออกมาเพื่อปรับปรุงประสิทธิภาพหรือแก้ไขปัญหาที่ไม่สามารถแก้ไขได้โดยการอัพเดทอัตโนมัติของโมดูลโปรแกรม การอัพเกรดเป็นเวอร์ชันใหม่กว่าสามารถทำได้หลายวิธี:

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

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

3. ด้วยตนเอง โดยการดาวน์โหลดและ เวอร์ชันใหม่กว่าทับเวอร์ชันที่มีอยู่ก่อนหน้า

สำหรับข้อมูลเพิ่มเติมและคำแนะนำพร้อมภาพประกอบสามารถดูได้ที่:

- อัพเดทผลิตภัณฑ์ของ ESET—ตรวจสอบโมดูลผลิตภัณฑ์ล่าสุด
- อะไรคือความแตกต่างระหว่างผลิตภัณฑ์ของ ESET ประเภทอัพเดทและประเภทที่เผยแพร่ให้ใช้งาน

การอัพเกรดอัตโนมัติสำหรับผลิตภัณฑ์ดั้งเดิม

เวอร์ชันผลิตภัณฑ์ ESET ของคุณไม่รองรับอีกต่อไป และผลิตภัณฑ์ของคุณได้รับการอัพเกรดให้เป็นเวอร์ชันล่าสุด

⚠ ปัญหาการติดตั้งทั่วไป

> ℹ ผลิตภัณฑ์ ESET เวอร์ชันใหม่ในแต่ละเวอร์ชันจะมีการแก้ไขบั๊กและปรับปรุงหลายประการ ลูกค้าเดิมที่มีการสมัครสมาชิกผลิตภัณฑ์ ESET ที่ถูกต้องจะสามารถอัพเกรดผลิตภัณฑ์เดิมให้เป็นเวอร์ชันล่าสุดได้ฟรี

หากต้องการทำการติดตั้งให้เสร็จสิ้น:

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

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

3. หลังเปิดใช้งานผลิตภัณฑ์ ESET ใหม่ด้วย รหัสเปิดใช้งาน ของคุณ หน้าภาพรวมจะปรากฏขึ้น หากไม่พบข้อมูลการสมัครสมาชิก ให้ดำเนินการทดลองใช้ฟรีต่อ หากการสมัครสมาชิกของคุณที่ใช้กับผลิตภัณฑ์ก่อนหน้านี้ไม่ถูกต้อง ให้เปิดใช้งานผลิตภัณฑ์ ESET ของคุณ

4. ต้องรีสตาร์ทอุปกรณ์เพื่อดำเนินการติดตั้งให้เสร็จสมบูรณ์

ESET NOD32 Antivirus จะถูกติดตั้ง

หน้าต่างข้อความนี้สามารถแสดงได้:

- ระหว่างขั้นตอนการติดตั้ง – คลิก **ดำเนินการต่อ** เพื่อติดตั้ง ESET NOD32 Antivirus
- เมื่อเปลี่ยนการสมัครสมาชิกใน ESET NOD32 Antivirus ให้คลิก **เปิดใช้งาน** เพื่อเปลี่ยนการสมัครสมาชิกแล้วเปิดใช้งาน ESET NOD32 Antivirus

ตัวเลือก **เปลี่ยนผลิตภัณฑ์** ช่วยให้คุณสามารถสลับไปมาระหว่างผลิตภัณฑ์ ESET Windows สำหรับใช้งานในบ้านได้ตามการสมัครสมาชิก ESET ของคุณ ดูข้อมูลเพิ่มเติมได้ที่ ฉันมีผลิตภัณฑ์ใดบ้าง

เปลี่ยนเป็นผลิตภัณฑ์รุ่นอื่นๆ

คุณสามารถสลับไปมาระหว่างผลิตภัณฑ์ ESET Windows สำหรับใช้งานในบ้านหลายๆ ผลิตภัณฑ์ได้ตามการสมัครสมาชิก ESET ของคุณ ดูข้อมูลเพิ่มเติมได้ที่ ฉันมีผลิตภัณฑ์ใดบ้าง

การลงทะเบียน

โปรดลงทะเบียนการสมัครสมาชิกของคุณโดยกรอกช่องในแบบฟอร์มลงทะเบียนให้เสร็จสมบูรณ์แล้วคลิก **เปิดใช้งาน** โดยต้องกรอกช่องที่ทำเครื่องหมายว่าจำเป็นในวงเล็บ ข้อมูลนี้จะถูกใช้สำหรับกรณีที่เกี่ยวข้องกับการสมัครสมาชิก ESET ของคุณเท่านั้น

ความคืบหน้าของการเปิดใช้งาน

โปรดรอสักสองสามวินาทีเพื่อให้กระบวนการเปิดใช้งานเสร็จสมบูรณ์ (เวลาที่ต้องรออาจแตกต่างกันไปตามความเร็วของการเชื่อมต่ออินเทอร์เน็ตหรือคอมพิวเตอร์)

เปิดใช้งานสำเร็จแล้ว

กระบวนการเปิดใช้งานเสร็จสมบูรณ์

การอัพเดตโมดูลจะเริ่มขึ้นในอีกไม่กี่วินาที การอัพเดทปกติของ ESET NOD32 Antivirus จะเริ่มต้นทันที

การสแกนครั้งแรกจะเริ่มโดยอัตโนมัติภายใน 20 นาทีหลังจากการอัพเดทโมดูลนี้

> i กระบวนการเปิดใช้งานอาจถูกขัดจังหวะ หากข้อเสนอไม่เกี่ยวข้องกับ ESET HOME เข้าสู่ระบบ ESET HOME หรือสร้างบัญชี

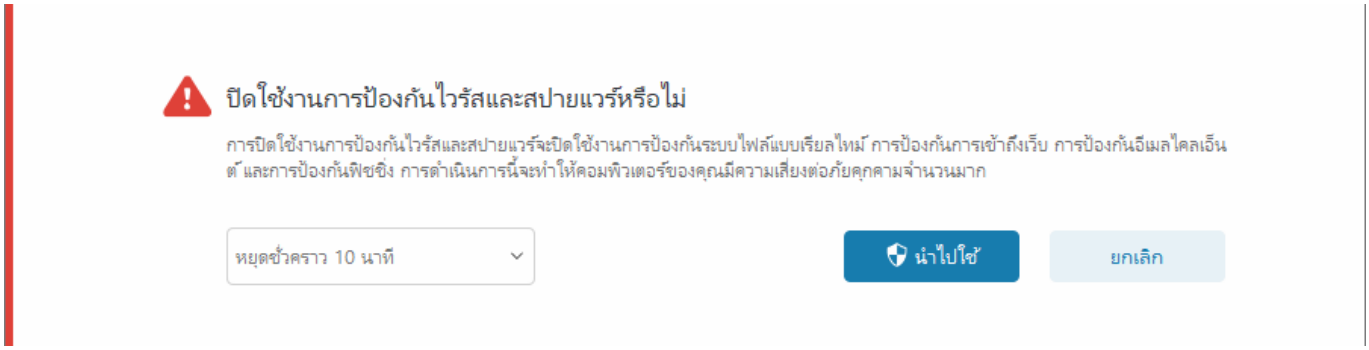
คู่มือสำหรับผู้เริ่มต้น

บทนี้จะให้ภาพรวมเริ่มต้นของ ESET NOD32 Antivirus และการตั้งค่าพื้นฐานของโปรแกรม

ไอคอนในถาดข้อมูลระบบ

มีตัวเลือกและคุณลักษณะของการตั้งค่าที่สำคัญที่สุดบางรายการสามารถใช้ได้ด้วยการคลิกขวาที่ไอคอนในถาดข้อมูลระบบ

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



การตั้งค่าขั้นสูง – เปิดการตั้งค่าขั้นสูงของ ESET NOD32 Antivirus หากต้องการเปิดการตั้งค่าขั้นสูงจาก หน้าต่างโปรแกรมหลัก ให้กด F5 บนแป้นพิมพ์หรือคลิก **การตั้งค่า** > **การตั้งค่าขั้นสูง**

ไฟล์บันทึก – ไฟล์บันทึก ประกอบไปด้วยข้อมูลเกี่ยวกับเหตุการณ์ของโปรแกรมสำคัญที่เกิดขึ้น และให้ภาพรวมของการตรวจพบ

เปิด ESET NOD32 Antivirus – เปิด หน้าต่างโปรแกรมหลัก ของ ESET NOD32 Antivirus

รีเซ็ตเค้าโครงหน้าต่าง - รีเซ็ตหน้าต่างของ ESET NOD32 Antivirus เป็นขนาดและตำแหน่งเริ่มต้นบนหน้าจอ

โหมดสี – เปิด การตั้งค่าส่วนต่อประสานผู้ใช้ ซึ่งคุณสามารถเปลี่ยนสีของ GUI ได้

ตรวจหาการอัปเดต เริ่มการอัพเดทโมดูลหรือการอัพเดทผลิตภัณฑ์เพื่อให้แน่ใจว่าคุณได้รับการป้องกัน ESET NOD32 Antivirus จะตรวจสอบการอัพเดทอัตโนมัติหลายครั้งต่อวัน

เกี่ยวกับ – ให้ข้อมูลระบบ, รายละเอียดเกี่ยวกับเวอร์ชันของ ESET NOD32 Antivirus ที่ติดตั้ง, โมดูลโปรแกรมที่ติดตั้ง และข้อมูลเกี่ยวกับระบบปฏิบัติการและทรัพยากรระบบ

แป้นพิมพ์ลัด

เพื่อให้การนำทางใน ESET NOD32 Antivirus ดียิ่งขึ้น คุณสามารถใช้แป้นพิมพ์ลัดต่อไปนี้ได้:

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

คุณยังสามารถใช้ปุ่มเมาส์ย้อนกลับหรือไปข้างหน้าสำหรับการนำทางได้ด้วยเช่นกัน

โปรไฟล์

ตัวจัดการโปรไฟล์ถูกใช้อยู่สองส่วนภายใน ESET NOD32 Antivirus ในส่วน **การสแกนตามต้องการ** และในส่วน **อัพเดท**

การสแกนคอมพิวเตอร์

โปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าใน ESET NOD32 Antivirus จะมีอยู่ด้วยกันทั้งหมด 4 รายการ:

- **การสแกนแบบสมาร์ท** - เป็นการสแกนขั้นสูงตามค่าเริ่มต้น โดยโปรไฟล์การสแกนแบบสมาร์ทใช้เทคโนโลยี Smart Optimization ซึ่งไม่รวมไฟล์ที่พบว่าปลอดภัยในการสแกนก่อนหน้านี้และไม่ได้ถูกแก้ไขตั้งแต่การสแกนครั้งก่อนหน้า วิธีนี้ช่วยให้เวลาในการสแกนลดลงโดยมีผลกระทบต่อความปลอดภัยของระบบน้อยที่สุด

- **การสแกนเมนูบริบท** - คุณสามารถเริ่มสแกนไฟล์ใดก็ได้จากเมนูบริบทได้ตามต้องการ โปรไฟล์การสแกนเมนูบริบทจะช่วยให้คุณกำหนดการกำหนดค่าการสแกนซึ่งจะใช้เมื่อคุณเปิดการสแกนวิธีนี้

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

- **การสแกนคอมพิวเตอร์** - เป็นโปรไฟล์ตามค่าเริ่มต้นที่ใช้ในการสแกนคอมพิวเตอร์มาตรฐาน

คุณสามารถบันทึกพารามิเตอร์การสแกนที่ต้องการได้เพื่อการสแกนในอนาคต ขอแนะนำให้คุณสร้างโปรไฟล์อีกโปรไฟล์หนึ่ง (ที่มีเป้าหมายการสแกน วิธีการสแกน และพารามิเตอร์อื่นๆ) สำหรับแต่ละการสแกนที่ใช้เป็นประจำ

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

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

อัพเดท

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

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

โปรไฟล์การอัพเดท – โปรไฟล์การอัพเดทที่ใช้อยู่ในขณะนี้ เมื่อต้องการเปลี่ยนแปลง ให้เลือกโปรไฟล์จากเมนูแบบเลื่อนลง

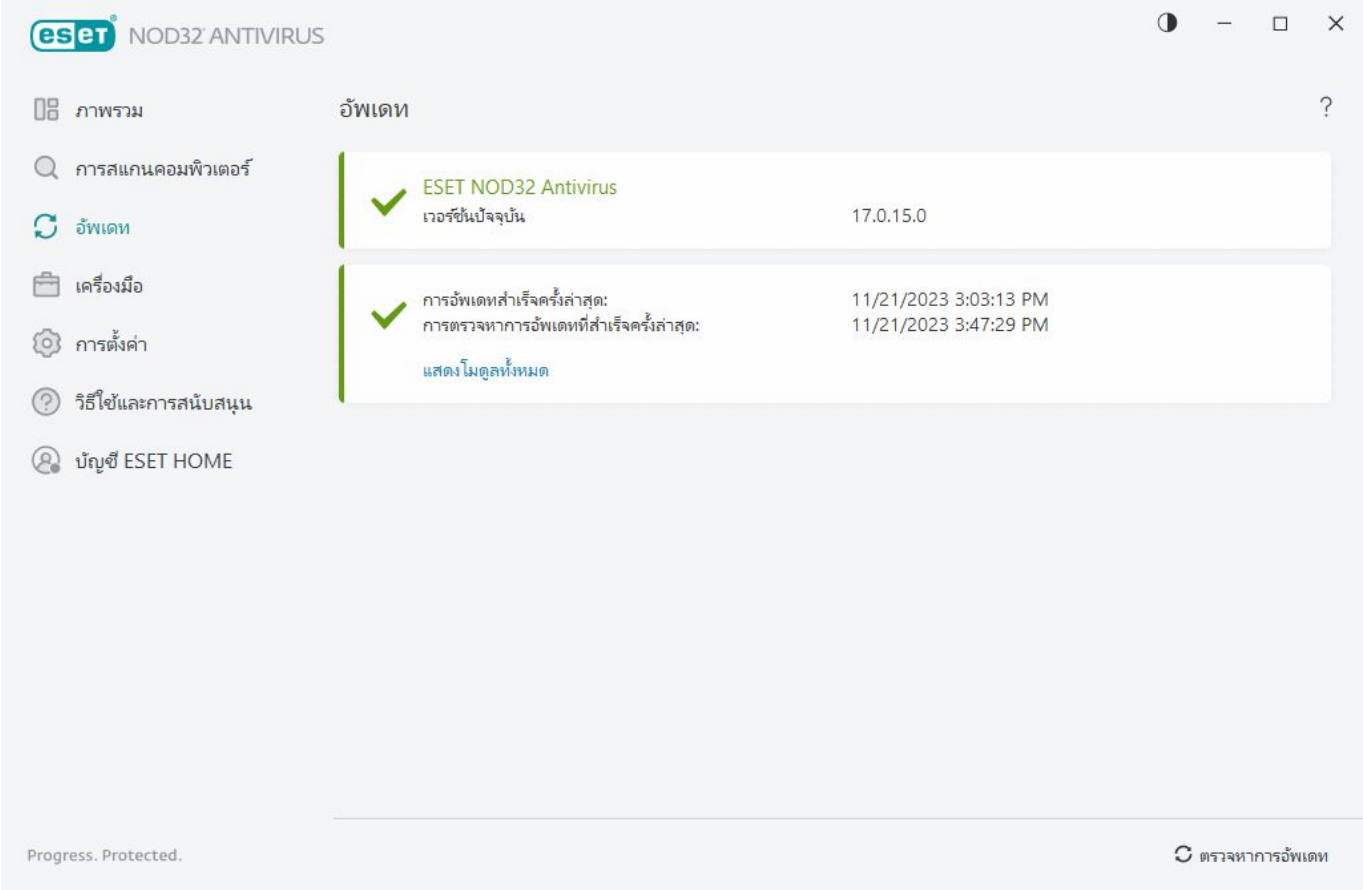
รายการของโปรไฟล์ – สร้างโปรไฟล์อัพเดทใหม่หรือลบโปรไฟล์อัพเดทที่มีอยู่

การอัพเดท

การอัพเดท ESET NOD32 Antivirus เป็นประจำเป็นวิธีการที่ดีที่สุดเพื่อให้มั่นใจว่าคอมพิวเตอร์มีระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัพเดทจะช่วยให้มั่นใจได้ว่าทั้งโมดูลโปรแกรมและส่วนประกอบของระบบจะอัพเดทอยู่เสมอ

เมื่อคลิก **อัพเดท** ในหน้าต่างโปรแกรมหลัก คุณสามารถดูสถานะการอัพเดทในปัจจุบัน รวมถึงวันที่และเวลาของการอัพเดทที่สำเร็จครั้งล่าสุด และดูว่าจะต้องมีการอัพเดทหรือไม่ได้

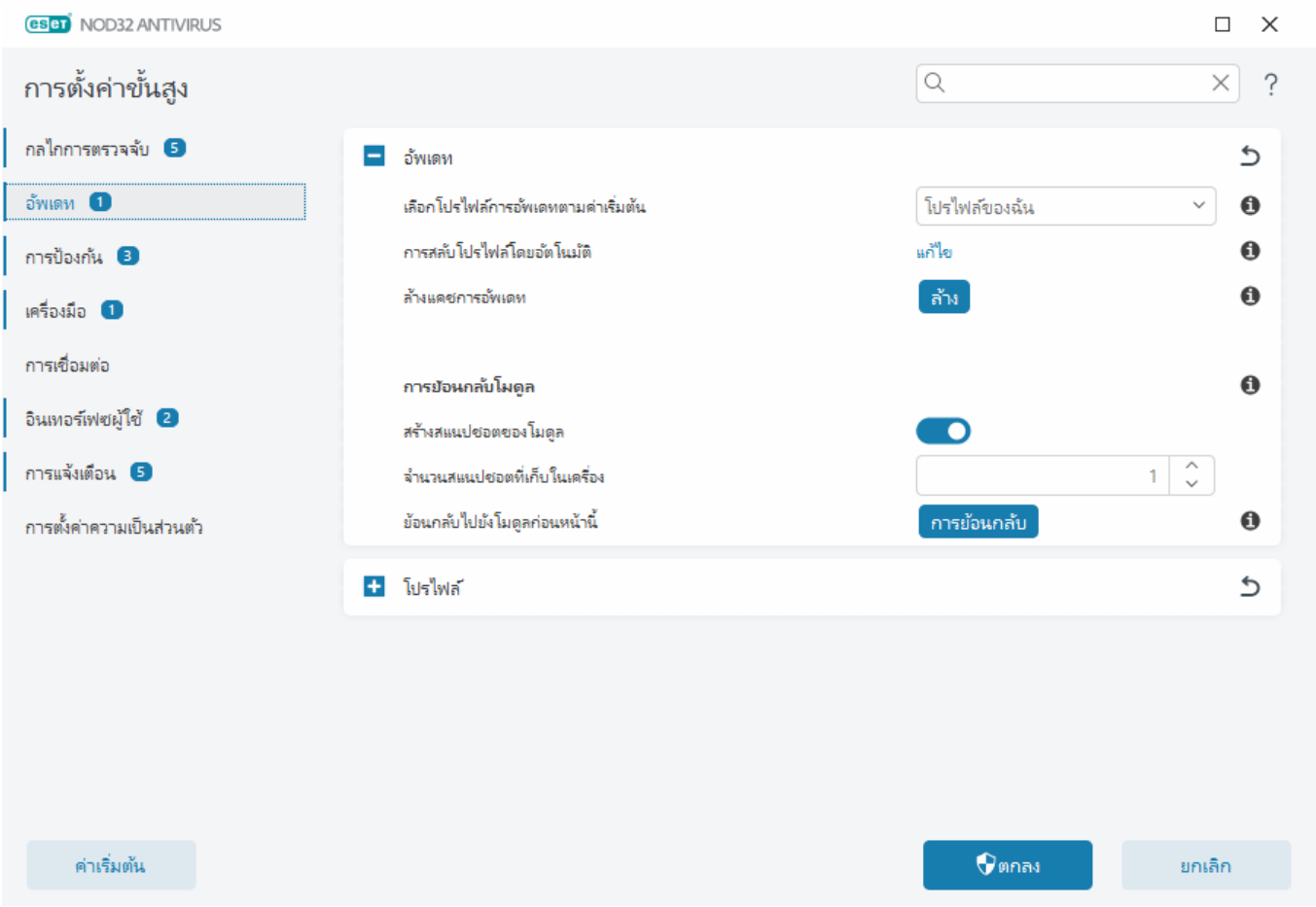
นอกเหนือจากการอัพเดทอัตโนมัติแล้ว คุณยังสามารถคลิก **ตรวจหาการอัพเดท** เพื่อเรียกใช้การอัพเดทด้วยตนเองได้



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

หากคุณประสบปัญหากับการอัพเดท ให้คลิกที่ **ล้าง** เพื่อล้างไฟล์แคชการอัพเดท หากยังคงไม่สามารถอัพเดทโมดูล

โปรแกรมได้ โปรดดูที่ส่วน ข้อความการแก้ไขปัญหาสำหรับ "การอัพเดทโมดูลล้มเหลว"



การเปิดใช้งานผลิตภัณฑ์

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

- หากคุณซื้อผลิตภัณฑ์ที่อยู่ในกล่องจากร้านค้าปลีกหรือได้รับอีเมลที่มีรายละเอียด การสมัครสมาชิก ให้เปิดใช้งานผลิตภัณฑ์ของคุณโดยคลิก **ใช้รหัสเปิดใช้งานที่ซื้อมา** คุณจะต้องป้อนรหัสเปิดใช้งานตามที่ได้รับมาเพื่อให้สามารถเปิดใช้งานได้สำเร็จ รหัสเปิดใช้งานคือชุดอักขระเฉพาะที่อยู่ในรูป XXXX-XXXX-XXXX-XXXX-XXXX หรือ XXXX-XXXXXXXX ซึ่งใช้เพื่อยืนยันตัวตนของเจ้าของ การสมัครสมาชิก และเพื่อการเปิดใช้งาน รหัสเปิดใช้งานมักจะอยู่ด้านในหรือด้านหลังบรรจุภัณฑ์ของผลิตภัณฑ์

- หลังจากเลือก ใช้บัญชี ESET HOME ระบบจะขอข้อมูลให้คุณเข้าสู่ระบบบัญชี ESET HOME ของคุณ

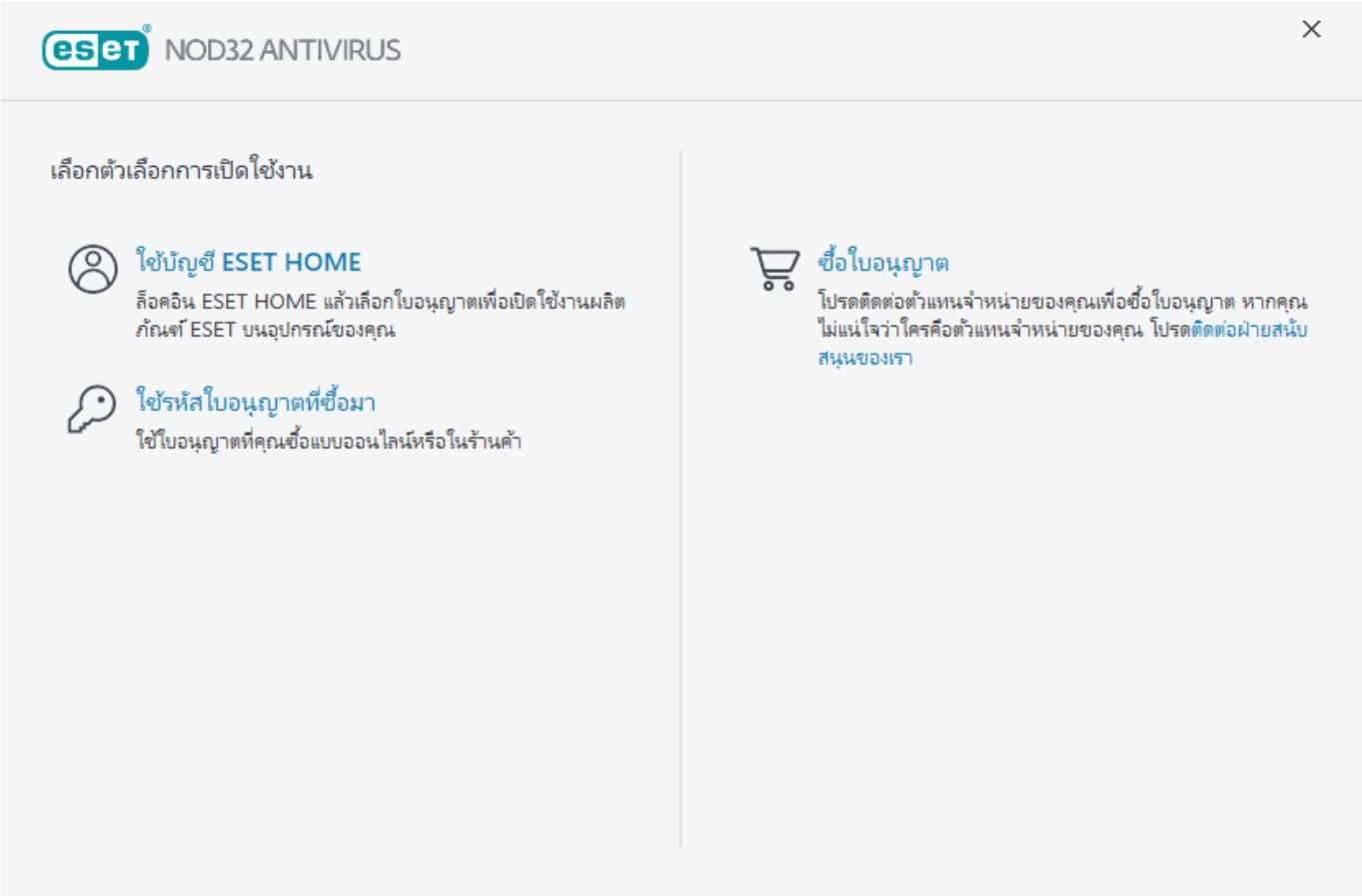
- หากคุณต้องการประเมิน ESET NOD32 Antivirus ก่อนตัดสินใจซื้อ ให้เลือก ทดลองใช้ฟรี ป้อนที่อยู่อีเมลและประเทศของคุณเพื่อเปิดใช้งาน ESET NOD32 Antivirus ในระยะเวลาที่จำกัด ระบบจะส่งเวอร์ชั่นทดลองใช้ฟรีไป

ให้คุณทางอีเมล เวอร์ชั่นทดลองใช้ฟรีจะสามารถเปิดใช้งานได้เพียงหนึ่งครั้งต่อลูกค้าหนึ่งรายเท่านั้น

• หากคุณไม่มีการสมัครสมาชิกและต้องการจะซื้อ ให้คลิก **ซื้อการสมัครสมาชิก** การดำเนินการนี้จะเปลี่ยนเส้นทางคุณไปยังเว็บไซต์ของตัวแทนจำหน่าย ESET ในพื้นที่ของคุณ การสมัครสมาชิกผลิตภัณฑ์ ESET Windows สำหรับใช้งานในบ้านนั้น ต้องเสียค่าใช้จ่าย

คุณสามารถเปลี่ยนแปลงการสมัครสมาชิกผลิตภัณฑ์ได้ทุกเมื่อ หากต้องการดำเนินการดังกล่าว ให้คลิก **วิธีใช้และการสนับสนุน** > **เปลี่ยนการสมัครสมาชิก** ใน หน้าต่างหลักของโปรแกรม คุณจะเห็น ID สาธารณะที่ใช้เพื่อระบุการสมัครสมาชิกของคุณให้กับฝ่ายสนับสนุนของ ESET

⚠ ไม่สามารถเปิดใช้งานผลิตภัณฑ์ได้ใช่หรือไม่



การป้อนรหัสเปิดใช้งานของคุณในระหว่างการเปิดใช้งาน

การอัพเดทอัตโนมัติมีความสำคัญต่อความปลอดภัยของคุณ ESET NOD32 Antivirus จะรับรายการอัพเดทต่างๆ หลังจากที่เปิดใช้งานแล้วเท่านั้น

เมื่อเข้าสู่ **รหัสเปิดใช้งาน** เป็นสิ่งสำคัญมากที่จะต้องป้อนให้ตรงตามที่ได้เขียนไว้ รหัสเปิดใช้งาน ของคุณคือชุดอักขระเฉพาะที่อยู่ในรูป XXXX-XXXX-XXXX-XXXX-XXXX ซึ่งใช้ในการระบุตัวตนเจ้าของและการเปิดใช้งานการสมัครสมาชิก

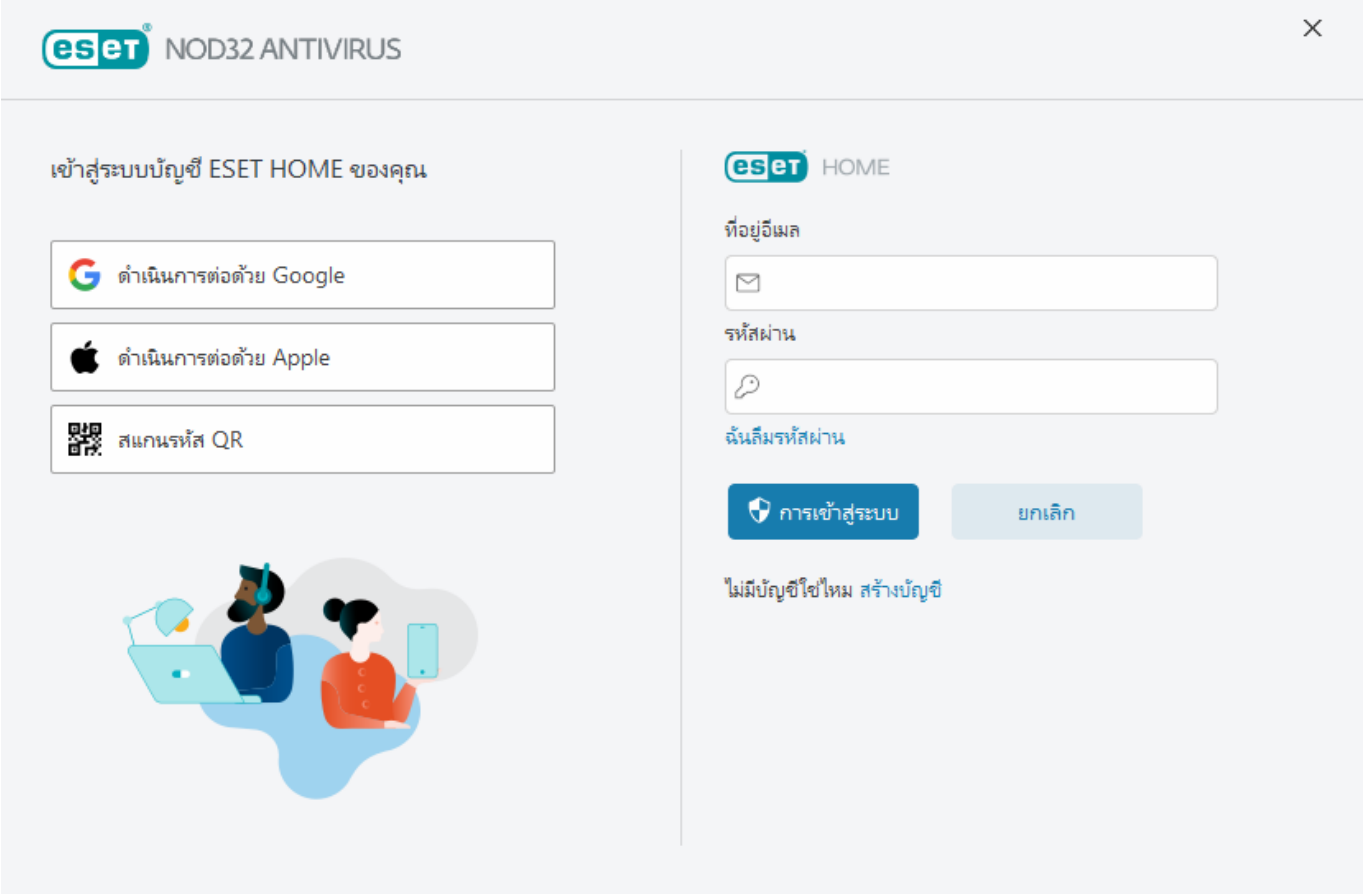
เราขอแนะนำให้คุณคัดลอก รหัสเปิดใช้งาน จากอีเมลลงทะเบียนของคุณไปวางเพื่อให้แน่ใจว่ารหัสถูกต้อง

หากคุณไม่ป้อน รหัสเปิดใช้งาน หลังติดตั้ง ผลิตภัณฑ์ของคุณจะไม่ได้รับการเปิดใช้งาน คุณสามารถเปิดใช้งาน ESET NOD32 Antivirus ได้ใน หน้าต่างโปรแกรมหลัก > **วิธีใช้และการสนับสนุน** > **เปิดใช้งานการสมัครสมาชิก**

การสมัครสมาชิกผลิตภัณฑ์ ESET Windows สำหรับใช้งานในบ้านนั้น ต้องเสียค่าใช้จ่าย

ใช้บัญชี ESET HOME

เชื่อมต่ออุปกรณ์ของคุณกับ ESET HOME เพื่อดูและจัดการการสมัครสมาชิกและอุปกรณ์ทั้งหมดของ ESET ที่เปิดใช้งานอยู่ คุณสามารถต่ออายุ อัพเกรด หรือขยายเวลาใช้งานการสมัครสมาชิกออกไปและดูรายละเอียดที่สำคัญของการสมัครสมาชิกได้ ในพอร์ทัลการจัดการหรือแอพมือถือของ ESET HOME คุณสามารถเพิ่มการสมัครสมาชิกอื่น ดาวน์โหลดผลิตภัณฑ์ไปยังอุปกรณ์ ตรวจสอบสถานะความปลอดภัยของผลิตภัณฑ์ หรือแชร์การสมัครสมาชิกผ่านอีเมลได้ สำหรับข้อมูลเพิ่มเติม โปรดไปที่ ความช่วยเหลือออนไลน์ของ ESET HOME



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

1. ล็อคอินเข้าสู่บัญชี ESET HOME ของคุณ

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

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

3. เลือกการสมัครสมาชิกเพื่อเปิดใช้งานหรือ เพิ่มการสมัครสมาชิกใหม่ คลิก **ดำเนินการต่อ** เพื่อเปิดใช้งาน ESET NOD32 Antivirus

เปิดใช้งานเวอร์ชันทดลองใช้

หากต้องการเปิดใช้งาน ESET NOD32 Antivirus เวอร์ชันทดลอง ให้ป้อนที่อยู่อีเมลที่ถูกต้องในช่อง **ที่อยู่อีเมล** และช่อง **ยืนยันที่อยู่อีเมล** หลังจากเปิดใช้งานแล้ว ระบบจะสร้างการสมัครสมาชิกของ ESET และส่งให้คุณทางอีเมล ที่อยู่อีเมลนี้ยังจะใช้สำหรับการแจ้งเตือนเกี่ยวกับการหมดอายุของผลิตภัณฑ์และการสื่อสารอื่นๆ กับ ESET อีกด้วย เวอร์ชั่นทดลองใช้ฟรีสามารถเปิดใช้งานได้เพียงครั้งเดียวเท่านั้น

เลือกประเทศของคุณจากเมนูแบบเลื่อนลง **ประเทศ** เพื่อลงทะเบียน ESET NOD32 Antivirus กับตัวแทนจำหน่ายในท้องถิ่นของคุณซึ่งจะให้การสนับสนุนด้านเทคนิค

รหัสเปิดใช้งาน ESET ฟรี

การสมัครสมาชิก ESET NOD32 Antivirus นั้นต้องเสียค่าใช้จ่าย

รหัสเปิดใช้งาน ของ ESET คือชุดตัวอักษรและหมายเลขเฉพาะที่คั่นด้วยเครื่องหมายขีดยาวซึ่ง ESET จัดหาให้เพื่ออนุญาตให้มีการใช้งาน ESET NOD32 Antivirus ได้อย่างถูกต้องตามกฎหมายโดยเป็นไปตาม ข้อตกลงการอนุญาตใช้งานสำหรับผู้ใช้ปลายทาง ผู้ใช้ปลายทางทุกรายมีสิทธิ์ในการใช้ รหัสเปิดใช้งาน ได้เฉพาะในขอบเขตเท่าที่มีสิทธิ์ใช้งาน ESET NOD32 Antivirus ซึ่งอิงจากจำนวนใบอนุญาตที่ ESET มอบให้เท่านั้น รหัสเปิดใช้งาน ถือเป็นความลับและไม่สามารถแชร์ได้ อย่างไรก็ตาม คุณสามารถ แชร์การสมัครสมาชิกได้โดยใช้ ESET HOME

อาจมีแหล่งข้อมูลทางอินเทอร์เน็ตที่ให้ รหัสเปิดใช้งาน ของ ESET แก่คุณ "ฟรีๆ" แต่โปรดจำไว้ว่า:

- การคลิกที่โฆษณา "การสมัครสมาชิกฟรีของ ESET" อาจทำให้คอมพิวเตอร์หรืออุปกรณ์ของคุณเสี่ยงต่อการถูก

บุกรุกและนำไปสู่การติดไวรัสมัลแวร์ได้ มัลแวร์สามารถซ่อนตัวอยู่ในคอนเทนต์โซเชียลมีเดียที่ไม่เป็นทางการ (เช่น วิดีโอ) เว็บไซต์ที่แสดงโฆษณาเพื่อรับเงินตามการเยี่ยมชมของคุณ และอื่นๆ โดยปกติแล้วเว็บไซต์เหล่านี้จะเป็นกับดัก

• ESET สามารถปิดใช้งานการสมัครสมาชิกที่ละเมิดลิขสิทธิ์ได้ทุกเมื่อ

• การใช้รหัสเปิดใช้งานที่ละเมิดลิขสิทธิ์นั้นขัดต่อ ข้อตกลงการอนุญาตใช้งานสำหรับผู้ใช้ปลายทาง ที่คุณต้องยอมรับเพื่อติดตั้ง ESET NOD32 Antivirus

• โปรดซื้อการสมัครสมาชิก ESET ผ่านช่องทางที่เป็นทางการเท่านั้น เช่น www.eset.com, ตัวแทนจำหน่ายหรือผู้ค้าปลีกของ ESET (อย่าซื้อการสมัครสมาชิกจากเว็บไซต์บุคคลภายนอกที่ไม่เป็นทางการ เช่น eBay หรือการสมัครสมาชิกที่ใช้งานร่วมกันจากบุคคลภายนอก)

• การดาวน์โหลด ESET NOD32 Antivirus นั้นไม่เสียค่าใช้จ่าย แต่การเปิดใช้งานระหว่างการติดตั้งจำเป็นต้องใช้รหัสเปิดใช้งานของ ESET ที่ถูกต้อง (คุณสามารถดาวน์โหลดและติดตั้งได้ตามปกติ แต่ถ้าไม่มีการเปิดใช้งานผลิตภัณฑ์จะไม่ทำงาน)

• อย่าแชร์การสมัครสมาชิกของคุณบนอินเทอร์เน็ตหรือสื่อสังคมออนไลน์ (เพราะอาจแพร่กระจายไปในวงกว้างได้)

หากต้องการระบุและรายงานการสมัครสมาชิก ESET ที่ละเมิดลิขสิทธิ์ โปรดไปที่บทความฐานความรู้ เพื่อดูวิธีการ

หากคุณมีความไม่แน่ใจเกี่ยวกับการซื้อผลิตภัณฑ์ด้านการรักษาความปลอดภัยของ ESET คุณสามารถใช้เวอร์ชั่นทดลองใช้ระหว่างตัดสินใจได้:

1. เปิดใช้งาน ESET NOD32 Antivirus โดยใช้เวอร์ชั่นทดลองฟรี

2. เข้าร่วมในโปรแกรมเบต้าของ ESET

3. ติดตั้ง ESET Mobile Security หากคุณใช้อุปกรณ์โทรศัพท์มือถือ Android โดยสามารถใช้งานในรูปแบบพรีเมียมได้ฟรี

หากต้องการรับส่วนลด / ต่ออายุใบอนุญาต ให้ ต่ออายุ ESET ของคุณ

การเปิดใช้งานล้มเหลว-สถานการณ์ทั่วไป

หากการเปิดใช้งาน ESET NOD32 Antivirus ไม่ประสบความสำเร็จ สถานการณ์ที่พบมากที่สุดคือ:

- รหัสเปิดใช้งานมีการใช้งานอยู่แล้ว
- คุณได้ป้อนรหัสการเปิดใช้งานที่ไม่ถูกต้อง
- ข้อมูลในแบบฟอร์มการเปิดใช้งานหายไปหรือไม่ถูกต้อง
- การสื่อสารกับเซิร์ฟเวอร์การเปิดใช้งานล้มเหลว
- ไม่มีหรือปิดใช้งานการเชื่อมต่อไปยังเซิร์ฟเวอร์การเปิดใช้งาน ESET

ตรวจสอบว่าคุณป้อน รหัสเปิดใช้งาน ที่ถูกต้องและมีการเชื่อมต่ออินเทอร์เน็ตอยู่ ลองเปิดใช้งาน ESET NOD32 Antivirus ใหม่อีกครั้ง หากคุณใช้บัญชี ESET HOME ในการเปิดใช้งาน โปรดดู การสมัครสมาชิก ESET HOME และการจัดการการสมัครสมาชิก - วิธีใช้แบบออนไลน์

> หากคุณได้รับข้อผิดพลาดข้อใดข้อหนึ่ง (เช่น การสมัครสมาชิกถูกระงับหรือการสมัครสมาชิกถูกใช้เกินจำนวน) ให้ทำตามคำแนะนำใน สถานะการสมัครสมาชิก

หากคุณยังคงไม่สามารถเปิดใช้งานได้ ตัวแก้ไขปัญหาการเปิดใช้งานของ ESET จะนำคุณไปรู้จักกับคำถามทั่วไป ข้อผิดพลาด ปัญหาที่เกี่ยวกับการเปิดใช้งานและการอนุญาต (พร้อมให้ใช้งานในรูปแบบภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษา)

สถานะการสมัครสมาชิก

การสมัครสมาชิกของคุณอาจมีสถานะที่แตกต่างกัน สามารถค้นหาสถานะการสมัครสมาชิกได้ใน ESET HOME หากต้องการเพิ่มการสมัครสมาชิกลงในบัญชี ESET HOME ให้ดูที่ เพิ่มการสมัครสมาชิก

> หากคุณไม่มีบัญชี ESET HOME คุณสามารถ สร้างบัญชี ESET HOME ใหม่ ได้

หากสถานะการสมัครสมาชิกไม่ใช่ **เปิดใช้งาน** คุณจะได้รับข้อผิดพลาดระหว่างการเปิดใช้งานหรือการแจ้งเตือนใน หน้าต่างโปรแกรมหลัก

หากต้องการปิดใช้งานการแจ้งเตือนสถานะการสมัครสมาชิก ให้เปิด การตั้งค่าขั้นสูง > **การแจ้งเตือน** > **สถานะแอ**

พพลิเคชัน คลิก **แก้ไข** ที่อยู่ถัดจาก **สถานะแอพพลิเคชัน** แล้วขยาย **การออกใบอนุญาต** และยกเลิกการเลือกกล่องทำเครื่องหมายที่อยู่ถัดจากการแจ้งเตือนที่คุณต้องการปิดใช้งาน การปิดใช้งานการแจ้งเตือนไม่สามารถแก้ปัญหาได้

ดูคำอธิบายและวิธีแก้ไขปัญหาที่แนะนำสำหรับสถานะการสมัครสมาชิกต่างๆ ในตารางด้านล่าง:

สถานะการสมัครสมาชิก	คำอธิบาย	โซลูชัน
เปิดใช้งาน	การสมัครสมาชิกถูกต้อง และคุณไม่จำเป็นต้องทำการโต้ตอบใดๆ ESET NOD32 Antivirus สามารถเปิดใช้งานได้ โดยดูรายละเอียดการสมัครสมาชิกได้ที่ หน้าต่างโปรแกรมหลัก > **วิธีใช้และการสนับสนุน**	
ถูกใช้เกินจำนวน	มีอุปกรณ์ใช้การสมัครสมาชิกนี้เกินกว่าจำนวนที่กำหนด คุณจะได้รับข้อผิดพลาดในการเปิดใช้งาน	โปรดดูข้อมูลเพิ่มเติมที่ เปิดใช้งานไม่สำเร็จเนื่องจากการสมัครสมาชิกถูกใช้เกินจำนวน
ถูกระงับ	การสมัครสมาชิกของคุณถูกระงับเนื่องด้วยปัญหาด้านการชำระเงิน หากต้องการใช้การสมัครสมาชิก โปรดตรวจสอบว่ารายละเอียดการชำระเงินใน ESET HOME เป็นข้อมูลล่าสุด หรือติดต่อผู้ค้าปลีกการสมัครสมาชิกของคุณ คุณจะได้รับข้อผิดพลาดนี้ระหว่างการเปิดใช้งานหรือใน หน้าต่างโปรแกรมหลัก	ผลิตภัณฑ์ที่ติดตั้ง – หากคุณมีบัญชี ESET HOME ในการแจ้งเตือนที่แสดงในหน้าต่างโปรแกรมหลัก ให้คลิก **จัดการการสมัครสมาชิกของคุณใน ESET HOME** แล้วตรวจสอบรายละเอียดการชำระเงินของคุณ ถ้าไม่อย่างนั้น ให้ติดต่อผู้ค้าปลีกการสมัครสมาชิกของคุณ ข้อผิดพลาดในการเปิดใช้งาน – หากคุณมีบัญชี ESET HOME ในหน้าต่างข้อผิดพลาดในการเปิดใช้งาน ให้คลิก **เปิด ESET HOME** และตรวจสอบรายละเอียดการชำระเงินของคุณ ถ้าไม่อย่างนั้น ให้ติดต่อผู้ค้าปลีกการสมัครสมาชิกของคุณ
หมดอายุแล้ว	การสมัครสมาชิกของคุณหมดอายุแล้ว และคุณไม่สามารถใช้การสมัครสมาชิกนี้เพื่อเปิดใช้งาน ESET NOD32 Antivirus ได้ คุณจะได้รับข้อผิดพลาดนี้ระหว่างการเปิดใช้งานหรือใน หน้าต่างโปรแกรมหลัก ถ้าคุณได้ติดตั้ง ESET NOD32 Antivirus ไว้แล้ว คอมพิวเตอร์ของคุณจะไม่ได้รับการป้องกันและการอัพเดท	ผลิตภัณฑ์ที่ติดตั้ง – ในการแจ้งเตือนที่ปรากฏในหน้าต่างโปรแกรมหลัก ให้คลิก **ต่ออายุการสมัครสมาชิก** และทำตามคำแนะนำใน ฉันจะต่ออายุการสมัครสมาชิกได้อย่างไร หรือคลิก **เปิดใช้งานผลิตภัณฑ์** แล้วเลือก วิธีการเปิดใช้งาน ของคุณ ข้อผิดพลาดในการเปิดใช้งาน – ในหน้าต่างข้อผิดพลาดในการเปิดใช้งาน ให้คลิก **ต่ออายุการสมัครสมาชิก** และทำตามคำแนะนำใน ฉันจะต่ออายุการสมัครสมาชิกได้อย่างไร หรือพิมพ์ รหัสเปิดใช้งาน ใหม่หรือที่ต่ออายุแล้ว จากนั้นคลิก **ต่ออายุการสมัครสมาชิก**
ยกเลิกแล้ว	การสมัครสมาชิกของคุณถูกยกเลิกโดย ESET หรือผู้ค้าปลีกการสมัครสมาชิกของคุณ	หากคุณได้รับข้อผิดพลาด ให้ทำดังนี้: ยกเลิกการสมัครสมาชิกใน หน้าต่างโปรแกรมหลัก หรือระหว่างการเปิดใช้งาน แล้วการสมัครสมาชิกของคุณน่าจะทำงานได้ตามปกติ โปรดติดต่อผู้ค้าปลีกการสมัครสมาชิกของคุณ

เปิดใช้งานไม่สำเร็จเนื่องจากการสมัครสมาชิกถูกใช้เกินจำนวน

ปัญหา

- การสมัครสมาชิกของคุณอาจถูกใช้เกินจำนวนหรือถูกใช้ในทางที่ผิด
- เปิดใช้งานไม่สำเร็จเนื่องจากการสมัครสมาชิกถูกใช้เกินจำนวน

โซลูชัน

มีอุปกรณ์ที่ใช้การสมัครสมาชิกนี้เกินกว่าจำนวนที่กำหนด คุณอาจตกเป็นเหยื่อของการปลอมแปลงหรือการละเมิดสิทธิ์ซอฟต์แวร์ การสมัครสมาชิกจะไม่สามารถใช้เพื่อเปิดใช้งานผลิตภัณฑ์อื่นๆ ของ ESET ได้ คุณสามารถแก้ปัญหานี้ได้โดยตรง หากคุณได้รับอนุญาตให้จัดการการสมัครสมาชิกในบัญชี ESET HOME ของคุณหรือซื้อการสมัครสมาชิกจากแหล่งที่ถูกต้องตามกฎหมาย ถ้าคุณยังไม่มีบัญชี ให้สร้างบัญชี

หากคุณเป็นเจ้าของการสมัครสมาชิกและคุณไม่ได้รับแจ้งให้ป้อนที่อยู่อีเมลของตนเอง:

1. ในการจัดการการสมัครสมาชิก ESET ให้เปิดเว็บเบราว์เซอร์แล้วไปยัง https://home.eset.com เข้าถึง ESET License Manager แล้วลบหรือปิดใช้งานที่นั่ง สำหรับข้อมูลเพิ่มเติม โปรดดู สิ่งที่ควรทำในกรณีที่การสมัครสมาชิกถูกใช้เกินจำนวน
2. หากต้องการระบุหรือรายงานการสมัครสมาชิกของ ESET ที่ละเมิดลิขสิทธิ์ โปรดไปที่บทความระบุและรายงานการสมัครสมาชิก ESET ที่ละเมิดลิขสิทธิ์ เพื่อดูวิธีการ
3. หากคุณไม่มั่นใจ คลิกย้อน **กลับ** และ ส่งอีเมลหาการสนับสนุนด้านเทคนิคของ ESET

หากคุณไม่ใช่เจ้าของการสมัครสมาชิก ให้ติดต่อเจ้าของการสมัครสมาชิกนี้เพื่อแจ้งข้อมูลว่าคุณไม่สามารถเปิดใช้งานผลิตภัณฑ์ ESET ได้เนื่องจากการสมัครสมาชิกถูกใช้เกินจำนวน เจ้าของใบอนุญาตสามารถแก้ไขปัญหาได้ในพอร์ทัล ESET HOME

หากได้รับแจ้งให้ยืนยันที่อยู่อีเมลของคุณ (ในบางกรณีเท่านั้น) ให้ป้อนที่อยู่อีเมลที่ใช้ซื้อหรือเปิดใช้งาน ESET NOD32 Antivirus ของคุณ

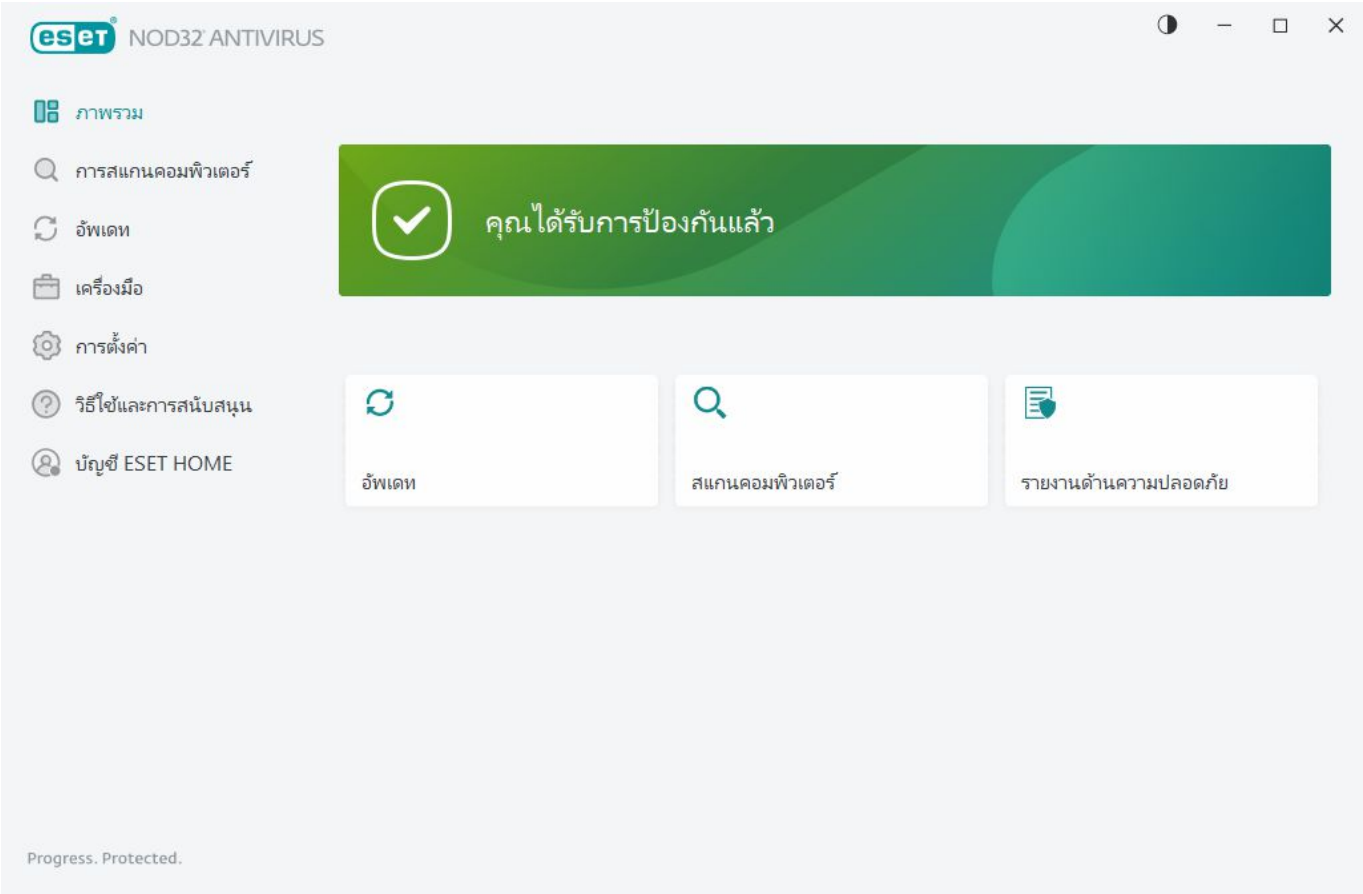
การทำงานกับ ESET NOD32 Antivirus

หน้าต่างโปรแกรมหลักของ ESET NOD32 Antivirus จะแบ่งออกเป็นสองส่วน หน้าต่างหลักที่ด้านขวาจะแสดงข้อมูลที่เกี่ยวข้องกับตัวเลือกที่เลือกจากเมนูหลักทางด้านซ้าย

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

คุณสามารถเลือกโทนสีของ ESET NOD32 Antivirus GUI ได้ที่มุมบนขวาของหน้าต่างโปรแกรมหลัก คลิกไอคอน**โทนสี** (ไอคอนจะเปลี่ยนไปตามโทนสีที่เลือกในปัจจุบัน) ถัดจากไอคอน**ย่อขนาด** และเลือกโทนสีจากเมนูแบบเลื่อนลง:

- **เหมือนกับสีของระบบ** ตั้งค่าโทนสี ESET NOD32 Antivirus ตามการตั้งค่าระบบปฏิบัติการของคุณ
- **มืด** ESET NOD32 Antivirus จะมีโทนสีเข้ม (โหมดมืด)
- **สว่าง** ESET NOD32 Antivirus จะมีโทนสีสว่าง ซึ่งเป็นโทนสีมาตรฐาน



ตัวเลือกเมนูหลัก:

ภาพรวม - ให้ข้อมูลเกี่ยวกับสถานะการป้องกันของ ESET NOD32 Antivirus

การสแกนคอมพิวเตอร์ - กำหนดค่าและเริ่มต้นสแกนคอมพิวเตอร์ของคุณหรือสร้างการสแกนแบบกำหนดเอง

อัพเดท – แสดงข้อมูลเกี่ยวกับโมดูลและการอัพเดทกลไกตรวจหา

เครื่องมือ – ให้การเข้าถึง ที่ช่วยให้การดูแลโปรแกรมง่ายขึ้นและเสนอตัวเลือกเพิ่มเติมสำหรับผู้ใช้ขั้นสูง

การตั้งค่า – มีตัวเลือกการกำหนดค่าสำหรับฟีเจอร์การป้องกันของ ESET NOD32 Antivirus (การป้องกันคอมพิวเตอร์และการป้องกันอินเทอร์เน็ต) และการเข้าถึง การตั้งค่าขั้นสูง

วิธีใช้และการสนับสนุน – แสดงข้อมูลเกี่ยวกับการสมัครสมาชิกของคุณ, ผลิตภัณฑ์ ESET ที่ติดตั้ง, และลิงก์ที่พาไปยัง วิธีใช้แบบออนไลน์ ฐานความรู้ ESET และ ฝ่ายสนับสนุนด้านเทคนิค

บัญชี ESET HOME — เชื่อมต่ออุปกรณ์ของคุณกับ ESET HOME หรือตรวจสอบสถานะการเชื่อมต่อบัญชี ESET HOME ใช้ ESET HOME เพื่อดูและจัดการกับการตั้งค่า การสมัครสมาชิกและอุปกรณ์ ESET ที่เปิดใช้งาน

ภาพรวม

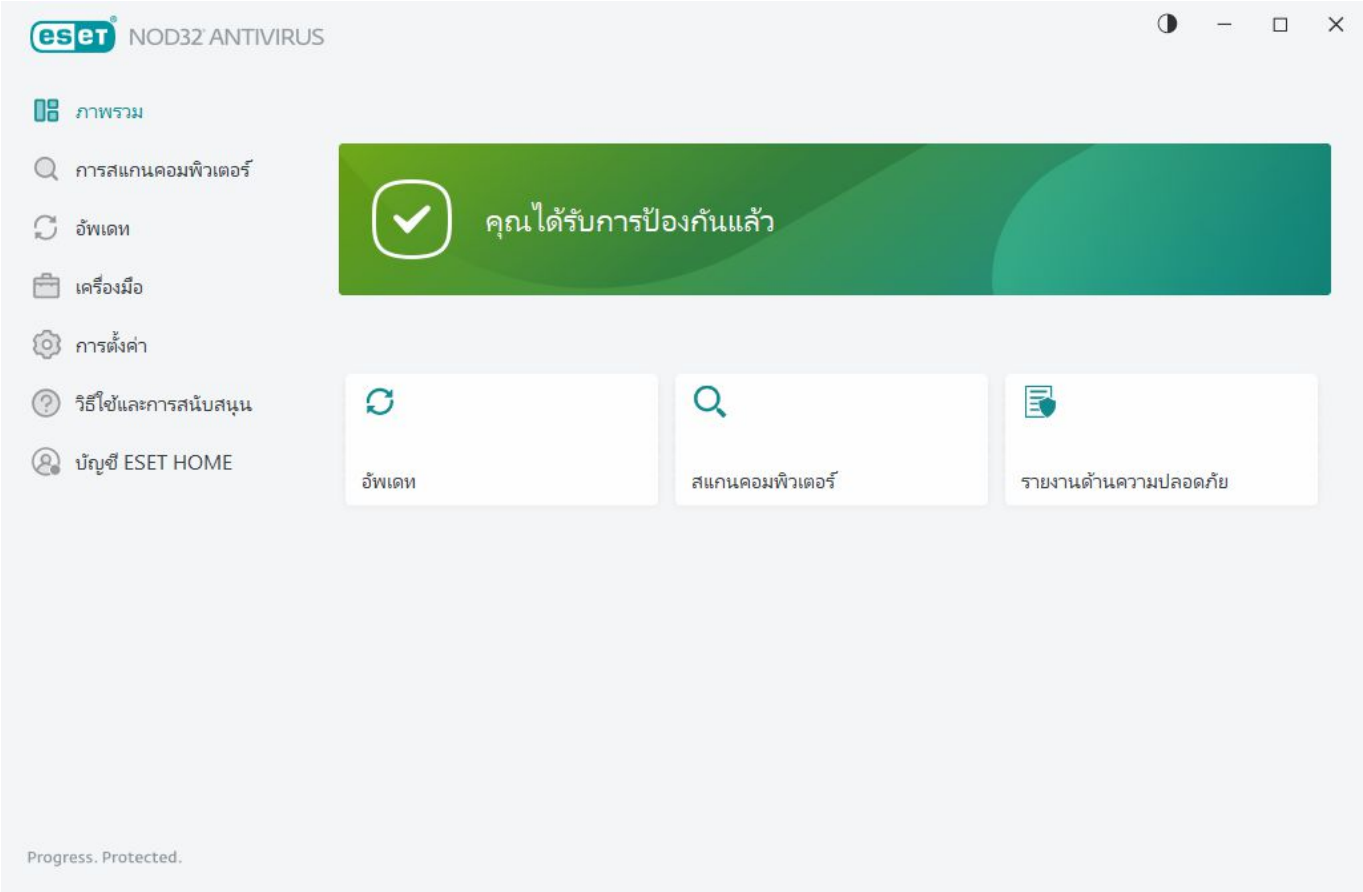
หน้าต่าง **ภาพรวม** จะแสดงข้อมูลเกี่ยวกับการป้องกันปัจจุบันของคอมพิวเตอร์ของคุณพร้อมกับลิงก์ด่วนไปยังคุณลักษณะด้านความปลอดภัยใน ESET NOD32 Antivirus

หน้าต่าง **ภาพรวม** จะแสดง การแจ้งเตือน พร้อมข้อมูลโดยละเอียดและวิธีแก้ไขปัญหาที่แนะนำเพื่อปรับปรุงความปลอดภัยของ ESET NOD32 Antivirus แล้วเปิดคุณลักษณะเพิ่มเติม หรือให้การปกป้องสูงสุด หากมีการแจ้งเตือนเพิ่มเติม ให้คลิก **X การแจ้งเตือนเพิ่มเติม** เพื่อขยายทั้งหมด

อัพเดท - เปิดหน้าอัพเดทและตรวจหาอัพเดท

สแกนคอมพิวเตอร์ของคุณ - เปิดหน้าการสแกนคอมพิวเตอร์และเริ่มทำการสแกนคอมพิวเตอร์มาตรฐาน

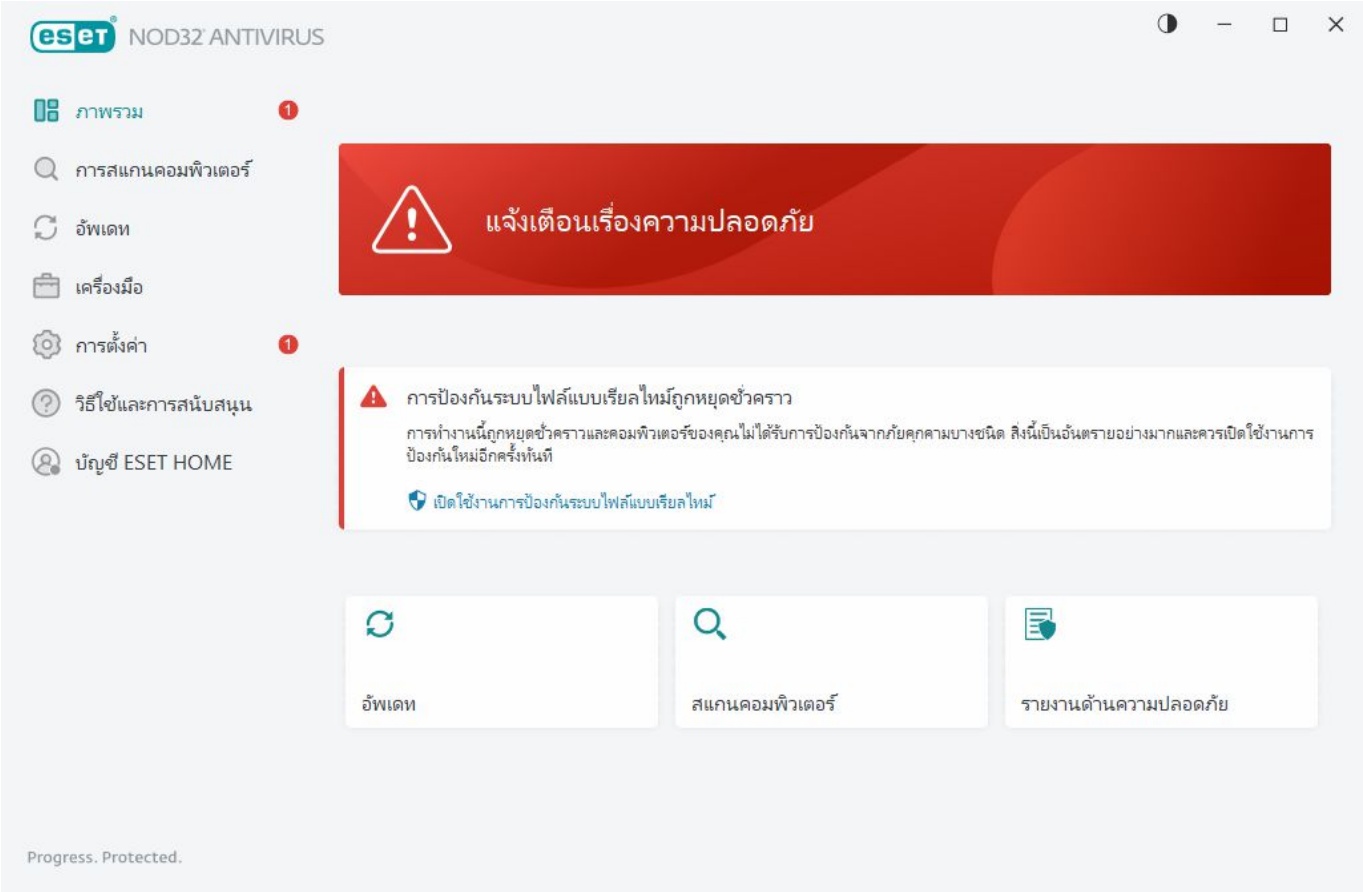
รายงานความปลอดภัย - เปิดรายงานด้านความปลอดภัย



ไอคอนสีเขียวและสถานะ **คุณได้รับการป้องกันแล้ว** สีเขียวแสดงว่ามีการป้องกันขั้นสูงสุด

ควรทำอย่างไรเมื่อโปรแกรมทำงานไม่ถูกต้อง

หากโมดูลการป้องกันที่ทำงานอยู่กำลังทำงานอย่างถูกต้อง ไอคอนสถานะการป้องกันจะเป็นสีเขียว เครื่องหมายอัศเจรีย์สีแดงหรือไอคอนการแจ้งเตือนสีส้มแสดงว่าไม่มีการป้องกันขั้นสูงสุด ข้อมูลเพิ่มเติมเกี่ยวกับสถานะการป้องกันของแต่ละโมดูล รวมทั้งวิธีแก้ปัญหาที่แนะนำสำหรับการกู้คืนการป้องกันแบบเต็มรูปแบบ จะแสดงเป็น การแจ้งเตือน ในหน้าต่าง **ภาพรวม** ในการเปลี่ยนสถานะของแต่ละโมดูล ให้คลิก **การตั้งค่า** แล้วเลือกโมดูลที่ต้องการ



ไอคอนสีแดงและสถานะ **แจ้งเตือนเรื่องความปลอดภัย** สีแดงจะหมายถึงปัญหาร้ายแรง มีเหตุผลหลายประการที่อาจทำให้สถานะนี้แสดงขึ้น ตัวอย่างเช่น:

- **ยังไม่ได้เปิดใช้งานผลิตภัณฑ์** หรือ **การสมัครสมาชิกหมดอายุแล้ว** – คุณจะทราบปัญหานี้ได้จากไอคอนสถานะการป้องกันที่เป็นสีแดง โปรแกรมจะไม่สามารถอัพเดทได้หลังจากการสมัครสมาชิกของคุณหมดอายุ ปฏิบัติตามคำแนะนำต่อไปนี้ในหน้าต่างแจ้งเตือนเพื่อต่ออายุการสมัครสมาชิก

- **กลไกตรวจหาไม่อัพเดท** – ข้อผิดพลาดจะปรากฏขึ้นหลังจากการพยายามอัพเดทกลไกตรวจหาที่ล้มเหลวหลายครั้ง ขอแนะนำให้คุณตรวจสอบการตั้งค่าการอัพเดท สาเหตุทั่วไปสำหรับข้อผิดพลาดนี้คือข้อมูลการตรวจสอบสิทธิ์ที่ป้อนไม่ถูกต้องหรือ การตั้งค่าการเชื่อมต่อ ที่กำหนดค่าไม่ถูกต้อง

- **การป้องกันระบบไฟล์แบบเรียลไทม์ถูกปิดใช้งาน** – การป้องกันระบบไฟล์แบบเรียลไทม์ถูกปิดใช้งานโดยผู้ใช้ คอมพิวเตอร์ของคุณไม่ได้รับการป้องกันจากภัยคุกคาม คลิก **เปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์** เพื่อเปิดใช้งานการทำงานนี้อีกครั้ง

- **การป้องกันไวรัสและการป้องกันสปายแวร์ถูกปิดใช้งาน** - คุณสามารถเปิดใช้งานการป้องกันไวรัสและการป้องกันสปายแวร์ได้อีกครั้งโดยคลิก **เปิดใช้งานการป้องกันไวรัสและสปายแวร์**

ไอคอนสีส้มระบุถึงการป้องกันที่จำกัด ยกตัวอย่างเช่น อาจเกิดปัญหาในการอัพเดทโปรแกรม หรือการสมัคร

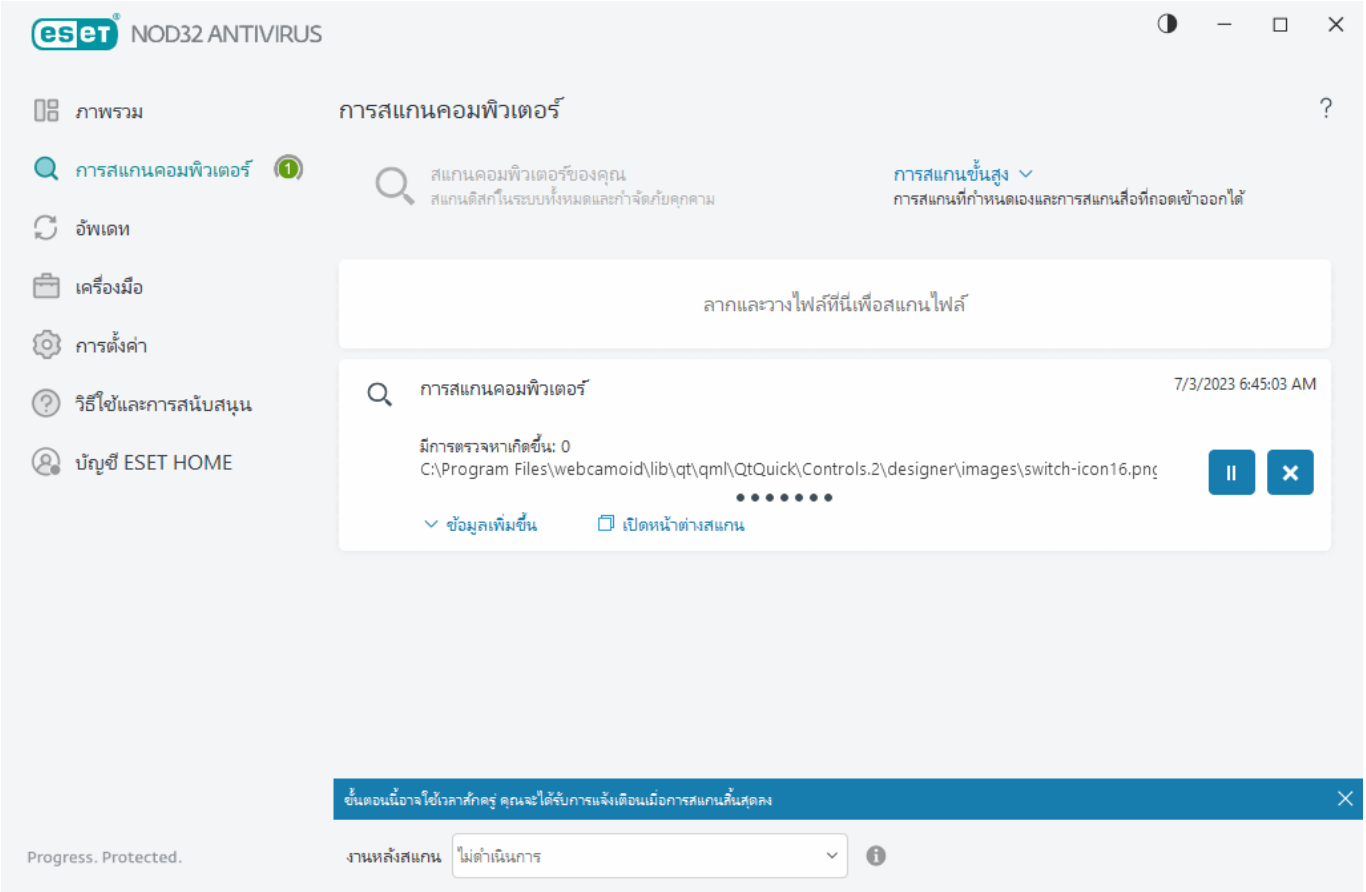
สมาชิกของคุณอาจใกล้ถึงวันหมดอายุ
มีเหตุผลหลายประการที่อาจทำให้สถานะนี้แสดงขึ้น ตัวอย่างเช่น:

- **โหมดผู้เล่นเกมเปิดใช้งานอยู่** - การเปิดใช้งาน โหมดผู้เล่นเกม อาจเกิดความเสี่ยงด้านความปลอดภัย การเปิดใช้งานคุณลักษณะนี้จะปิดใช้งานหน้าต่างแจ้งเตือน/เตือนภัยทั้งหมดและระงับงานตามกำหนดการลง
- **การสมัครสมาชิกของคุณใกล้หมดอายุแล้ว/การสมัครสมาชิกของคุณจะหมดอายุในวันนี้** – คุณจะทราบปัญหานี้ได้จากไอคอนสถานะการป้องกันที่มีเครื่องหมายอัศเจรีย์ใกล้กับนาฬิการะบบ หลังจากการสมัครสมาชิกหมดอายุลง โปรแกรมจะไม่สามารถอัพเดทได้ และไอคอนสถานะการป้องกันจะเปลี่ยนเป็นสีแดง

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

การสแกนคอมพิวเตอร์

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



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

โปรดดู ความคืบหน้าของการสแกน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับกระบวนการสแกน

> ℹ โดยค่าเริ่มต้น ESET NOD32 Antivirus จะพยายามทำความสะอาดหรือลบการตรวจหาที่พบในระหว่างการสแกนคอมพิวเตอร์โดยอัตโนมัติ ในบางกรณี หากไม่มีการกระทำใดสามารถทำได้ ผู้ใช้ปลายทางจะได้รับหน้าต่างโต้ตอบและต้องเลือกการดำเนินการทำความสะอาด (ตัวอย่างเช่น ลบ หรือ เพิกเฉย) หากต้องการเปลี่ยนแปลงระดับการทำความสะอาดและสำหรับข้อมูลแบบละเอียด โปรดดู การทำความสะอาด หากต้องการตรวจสอบการสแกนครั้งก่อนหน้า โปรดดู ไฟล์บันทึก

🔍 สแกนคอมพิวเตอร์

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

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

ตัวเลือกในการสแกนต่อไปนี้มีให้ใช้ที่ใต้ **การสแกนขั้นสูง**:

การสแกนที่กำหนดเอง

การสแกนที่กำหนดเองช่วยให้คุณสามารถระบุพารามิเตอร์การสแกน เช่น เป้าหมายและวิธีการสแกนได้ ข้อดีของ**การสแกนที่กำหนดเอง**คือคุณสามารถกำหนดค่าพารามิเตอร์โดยละเอียดได้ คุณสามารถบันทึกการกำหนดค่าไว้ไปยังโปรไฟล์การสแกนที่ผู้ใช้กำหนด ซึ่งจะเป็นประโยชน์ถ้ามีการสแกนซ้ำกับพารามิเตอร์เดียวกัน

การสแกนสื่อที่ถอดเข้าออกได้

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

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

ทำซ้ำการสแกนครั้งล่าสุด

อนุญาตให้คุณเริ่มต้นการสแกนที่ทำล่าสุดโดยใช้การตั้งค่าเดียวกับที่สแกนครั้งที่แล้ว

เมนูแบบเลื่อนลง **การทำงานหลังสแกน** ทำให้คุณสามารถตั้งค่าการทำงานที่จะดำเนินการโดยอัตโนมัติหลังจากการสแกนเสร็จสิ้นได้:

- **ไม่มีการทำงาน** – หลังจากสแกนเสร็จสิ้น จะไม่มีการดำเนินการใดๆ
- **ปิดระบบ** – คอมพิวเตอร์จะปิดหลังจากสแกนเสร็จสิ้น
- **รีสตาร์ทหากจำเป็น** – คอมพิวเตอร์จะรีสตาร์ทก็ต่อเมื่อจำเป็นเพื่อกำจัดภัยคุกคามที่ตรวจพบเท่านั้น
- **เริ่มต้นระบบใหม่** – ปิดโปรแกรมที่เปิดอยู่ทั้งหมด แล้วเริ่มต้นคอมพิวเตอร์ใหม่หลังจากสแกนเสร็จสิ้น
- **บังคับให้รีสตาร์ทเครื่องหากจำเป็น** – ระบบจะบังคับให้คอมพิวเตอร์รีสตาร์ทก็ต่อเมื่อจำเป็นเพื่อกำจัดภัย

คุกคามที่ตรวจพบเท่านั้น

• **บังคับให้รีบูต** – บังคับให้ปิดโปรแกรมที่เปิดอยู่ทั้งหมดโดยไม่ต้องรอการโต้ตอบของผู้ใช้และรีสตาร์ทคอมพิวเตอร์หลังจากการสแกนเสร็จสิ้น

• **พักเครื่อง** – บันทึกเซสชันของคุณและปรับคอมพิวเตอร์เข้าสู่สถานะการใช้พลังงานต่ำเพื่อให้คุณสามารถกลับมาทำงานต่อได้อย่างรวดเร็ว

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

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

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

> เราขอแนะนำให้คุณเรียกใช้การสแกนคอมพิวเตอร์อย่างน้อยเดือนละหนึ่งครั้ง การสแกนสามารถกำหนดค่าเป็นงานตามกำหนดการได้จาก **เครื่องมือ** > **เครื่องมือวางกำหนดการ** ฉันสามารถกำหนดเวลาการสแกนคอมพิวเตอร์รายสัปดาห์ได้อย่างไร

เครื่องมือเริ่มต้นการสแกนที่กำหนดเอง

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

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

โครงสร้างโฟลเดอร์ (แบบต้นไม้) ยังมีเป้าหมายการสแกนที่เฉพาะเจาะจงอีกด้วย

• **หน่วยความจำที่ใช้งาน** – สแกนกระบวนการและข้อมูลทั้งหมดที่ใช้อยู่ในปัจจุบันโดยหน่วยความจำที่ใช้งาน

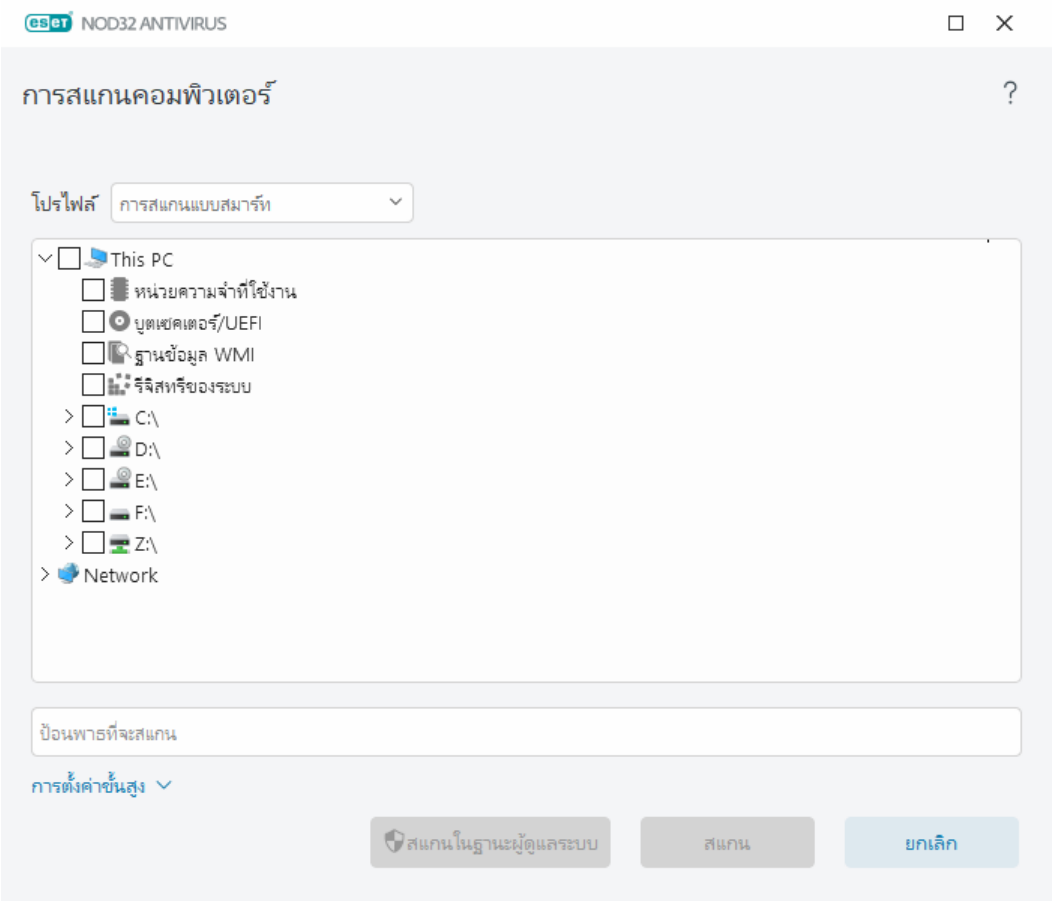
• **ส่วนการบูต/UEFI** – สแกนส่วนการบูตและ UEFI สำหรับมัลแวร์ที่มี อ่านเพิ่มเติมเกี่ยวกับเครื่องมือสแกน UEFI ได้ใน ประมวลศัพท์

• **ฐานข้อมูล WMI** – สแกนทั้งฐานข้อมูล Windows Management Instrumentation (WMI), เนมสเปซทั้งหมด, ตัวอย่างทุกระดับ และรวมถึงคุณสมบัติทั้งหมด การค้นหาสำหรับการอ้างอิงสำหรับไฟล์ที่ติดไวรัสหรือมัลแวร์ที่ฝังเป็นข้อมูล

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

หากต้องการไปยังเป้าหมายการสแกน (ไฟล์หรือโฟลเดอร์) อย่างรวดเร็ว ให้พิมพ์พาธของเป้าหมายดังกล่าวลงในช่องข้อความใต้ลำดับโครงสร้าง พาธต้องตรงตามตัวพิมพ์เล็กและใหญ่ โปรดเลือกกล่องกาเครื่องหมายในลำดับโครงสร้างหากต้องการให้ระบบสแกนเป้าหมายด้วย

> **i** วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์
> หากต้องการกำหนดตารางงานทั่วไป ให้อ่าน วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์



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

เมื่อเลือก **ละเว้นการยกเว้น** ไฟล์ที่มีนามสกุลไฟล์ที่ไม่ได้รับการสแกนก่อนหน้านี้จะถูกสแกนโดยไม่มีข้อยกเว้น

คลิก **สแกน** เพื่อเรียกใช้การสแกนโดยใช้พารามิเตอร์ที่กำหนดเองที่คุณตั้งค่าไว้

สแกนในฐานะผู้ดูแลระบบ อนุญาตให้คุณเรียกใช้การสแกนภายใต้บัญชีของผู้ดูแลระบบ ใช้ตัวเลือกนี้หากผู้ใช้ปัจจุบันไม่มีสิทธิ์ในการเข้าถึงไฟล์ที่คุณต้องการสแกน ปุ่มนี้จะไม่มีให้ใช้ได้หากผู้ใช้ปัจจุบันไม่สามารถเรียกการทำงาน UAC ในฐานะผู้ดูแลระบบได้

ℹ คุณสามารถดูบันทึกการสแกนคอมพิวเตอร์เมื่อสแกนเสร็จแล้วได้ด้วยการคลิกที่ แสดงบันทึก

ความคืบหน้าของการสแกน

หน้าต่างความคืบหน้าของการสแกนจะแสดงสถานะปัจจุบันของการสแกนและข้อมูลเกี่ยวกับจำนวนไฟล์ที่พบว่ามีรหัสที่เป็นอันตราย

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

> **วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์**
> หากต้องการกำหนดตารางงานทั่วไป ให้อ่าน วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์

ความคืบหน้าของการสแกน – แถบความคืบหน้าจะแสดงสถานะของการสแกนที่กำลังทำงานอยู่

เป้าหมาย – ชื่อของวัตถุที่สแกนและตำแหน่งของวัตถุในปัจจุบัน

การตรวจหาเกิดขึ้น - แสดงจำนวนทั้งหมดของไฟล์ที่สแกน ภัยคุกคามที่พบ และภัยคุกคามที่กำจัดระหว่างการสแกน

คลิก "ข้อมูลเพิ่มเติม" เพื่อแสดงข้อมูลต่อไปนี้:

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

ไอคอนหยุดชั่วคราว – หยุดการสแกนชั่วคราว

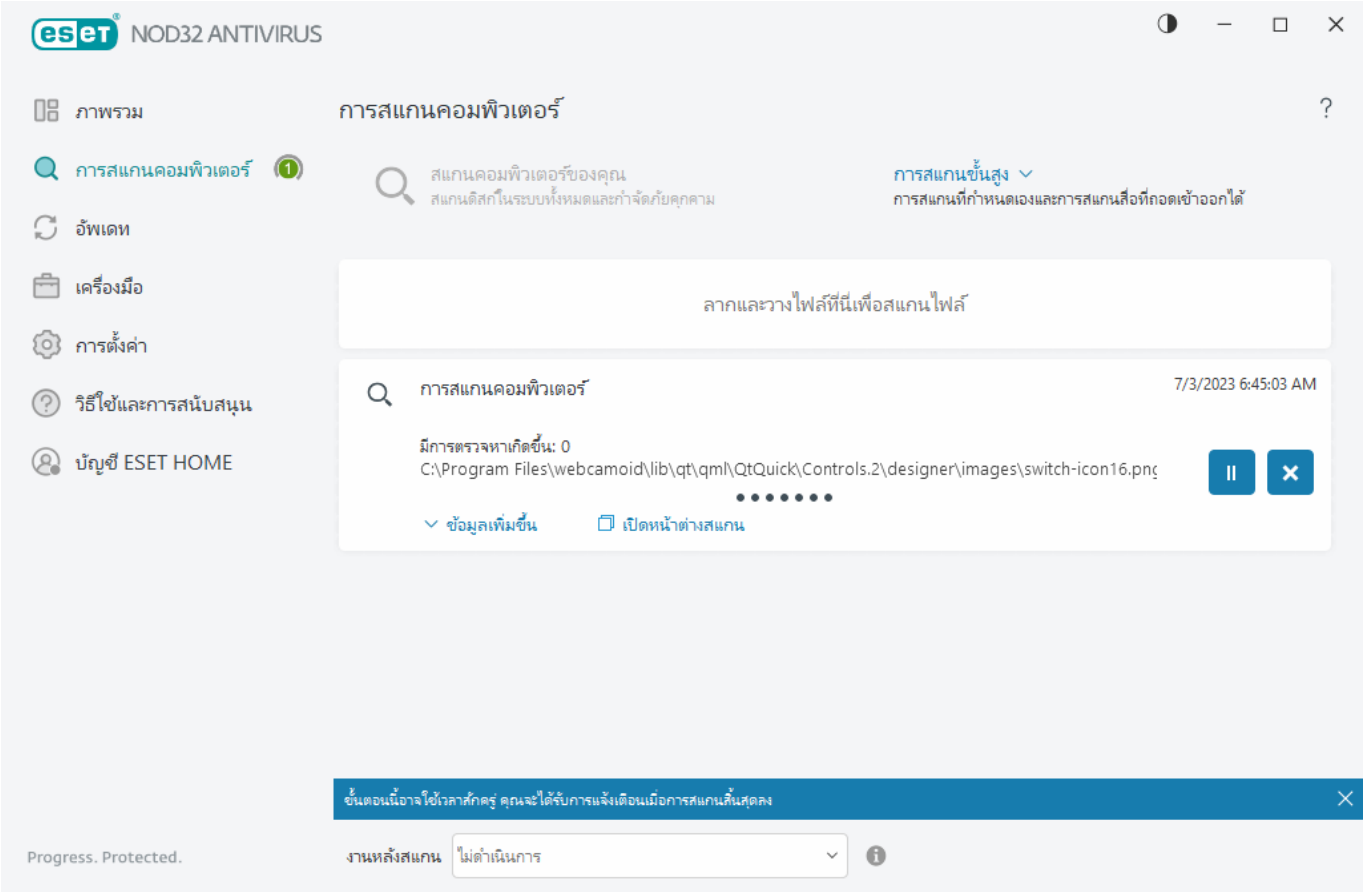
ไอคอนทำงานต่อ – ตัวเลือกนี้จะปรากฏเมื่อหยุดการสแกนไว้ชั่วคราว คลิกที่ไอคอนเพื่อทำการสแกนต่อไป

ไอคอนหยุด – สิ้นสุดการสแกน

คลิก **เปิดหน้าต่างการสแกน** เพื่อเปิด บันทึกการสแกนคอมพิวเตอร์ พร้อมรายละเอียดเพิ่มเติมเกี่ยวกับการสแกน

เลื่อนบันทึกการสแกน – ถ้าเปิดใช้งานตัวเลือกนี้ บันทึกการสแกนจะเลื่อนลงโดยอัตโนมัติเมื่อมีการเพิ่มรายการใหม่เพื่อให้รายการล่าสุดปรากฏขึ้น

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



เมนูแบบเลื่อนลง **การทำงานหลังสแกน** ทำให้คุณสามารถตั้งค่าการทำงานที่จะดำเนินการโดยอัตโนมัติหลังจากการสแกนเสร็จสิ้นได้:

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

คอมพิวเตอร์ของคุณจะปิด แต่จะกลับมายังสถานะก่อนหน้านี้ในครั้งต่อไปที่คุณเริ่มคอมพิวเตอร์อีกครั้ง

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

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

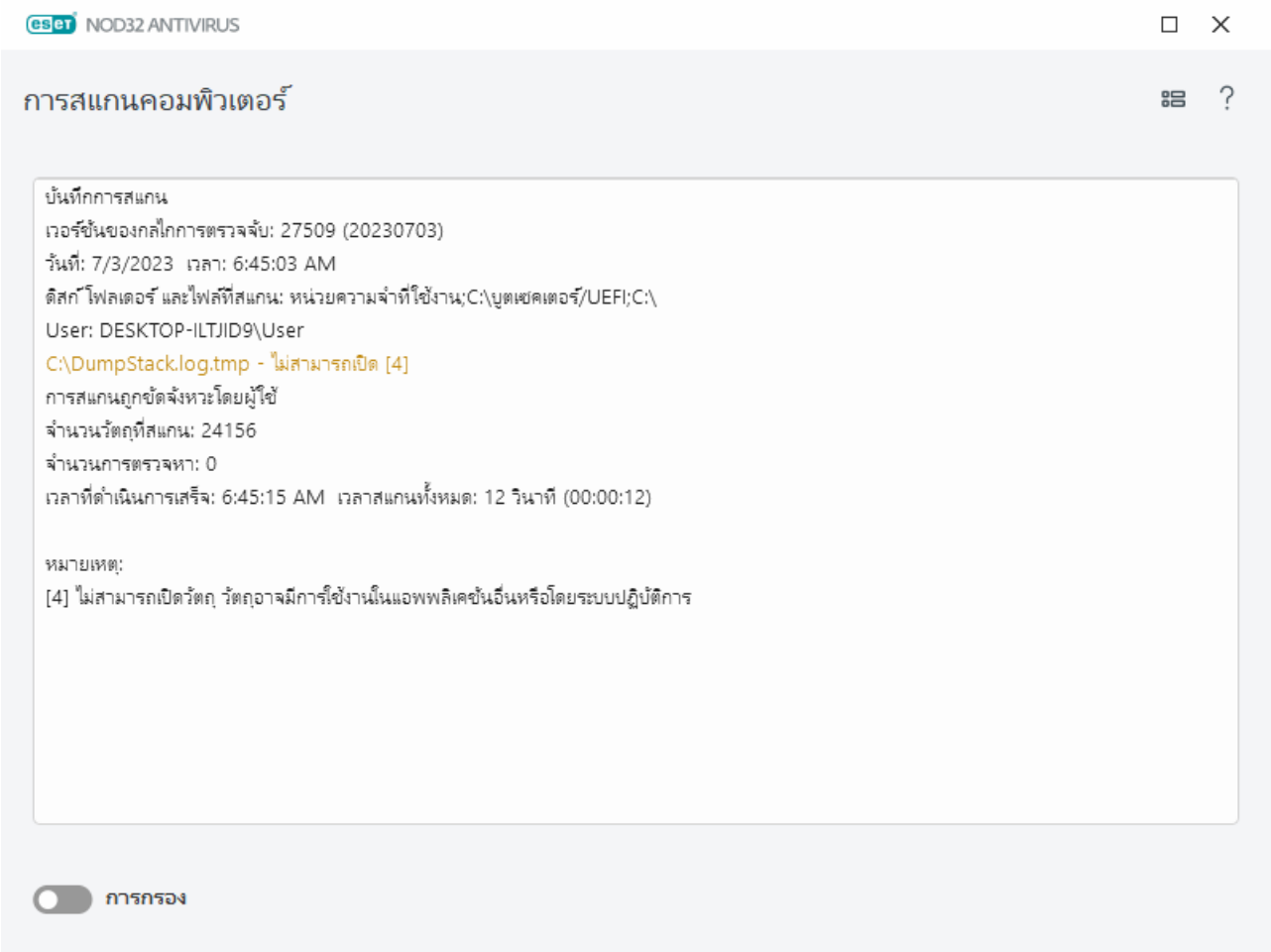
บันทึกการสแกนคอมพิวเตอร์

คุณสามารถดูข้อมูลโดยละเอียดที่เกี่ยวข้องกับการสแกนที่ต้องการได้ใน ไฟล์บันทึก บันทึกการสแกนประกอบด้วยข้อมูลต่อไปนี้:

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

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

ในการค้นหาบันทึกการสแกนก่อนหน้า ในหน้าต่างโปรแกรมหลัก ให้เลือก **เครื่องมือ** > **ไฟล์บันทึก** ในเมนูแบบเลื่อนลง ให้เลือก **การสแกนคอมพิวเตอร์** แล้วคลิกสองครั้งที่การบันทึกที่ต้องการ



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

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

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

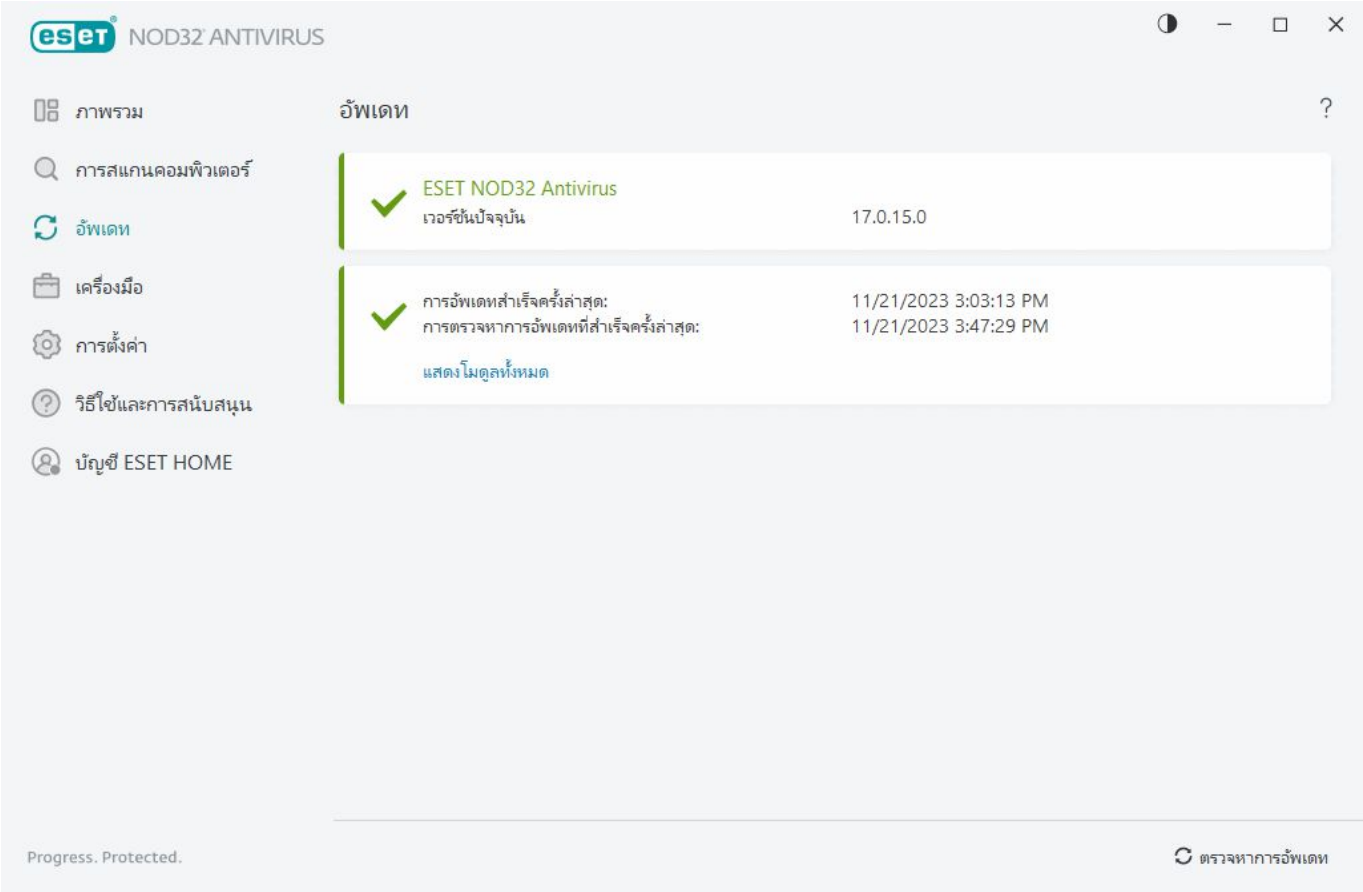
การทำงาน	การใช้งาน
คำอธิบายการตรวจหา	เปิดสารานุกรมภัยคุกคามของ ESET ซึ่งมีข้อมูลโดยละเอียดเกี่ยวกับอันตรายและอาการของการแฝงตัวที่ทำไฮไลต์ไว้

อัพเดท

การอัพเดท ESET NOD32 Antivirus เป็นประจำเป็นวิธีการที่ดีที่สุดเพื่อให้มั่นใจว่าคอมพิวเตอร์มีระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัพเดทจะช่วยให้มั่นใจได้ว่าทั้งโมดูลโปรแกรมและส่วนประกอบของระบบจะอัพเดทอยู่เสมอ

เมื่อคลิก **อัพเดท** ในหน้าต่างโปรแกรมหลัก คุณสามารถดูสถานะการอัพเดทในปัจจุบัน รวมถึงวันที่และเวลาของการอัพเดทที่สำเร็จครั้งล่าสุด และดูว่าจะต้องมีการอัพเดทหรือไม่ได้

นอกเหนือจากการอัพเดทอัตโนมัติแล้ว คุณยังสามารถคลิก **ตรวจหาการอัพเดท** เพื่อเรียกใช้การอัพเดทด้วยตนเองได้ การอัพเดทโมดูลและส่วนประกอบของโปรแกรมอย่างสม่ำเสมอเป็นสิ่งที่สำคัญในการรักษาการปกป้องอย่างแบบเต็มรูปแบบจากรหัสที่เป็นอันตราย โปรดให้ความสนใจในการกำหนดค่าและการทำงานของโปรแกรม คุณต้องเปิดใช้งานผลิตภัณฑ์ของคุณโดยใช้ รหัสเปิดใช้งาน เพื่อรับการอัพเดท หากคุณไม่ได้อัพเดทในระหว่างการติดตั้ง คุณจะต้อง เปิดใช้งาน ESET NOD32 Antivirus เพื่อเข้าถึงเซิร์ฟเวอร์อัพเดทของ ESET ระบบได้ส่ง รหัสเปิดใช้งาน ไปให้คุณในอีเมลที่ได้จาก ESET หลังทำการซื้อ ESET NOD32 Antivirus



เวอร์ชันปัจจุบัน – แสดงหมายเลขเวอร์ชันของผลิตภัณฑ์เวอร์ชันปัจจุบันที่คุณได้ติดตั้ง

การอัพเดทสำเร็จครั้งล่าสุด – แสดงวันที่อัพเดทสำเร็จครั้งล่าสุด หากคุณไม่พบวันที่ล่าสุด แสดงว่าโมดูลผลิตภัณฑ์ของคุณอาจไม่ใช่โมดูลปัจจุบัน

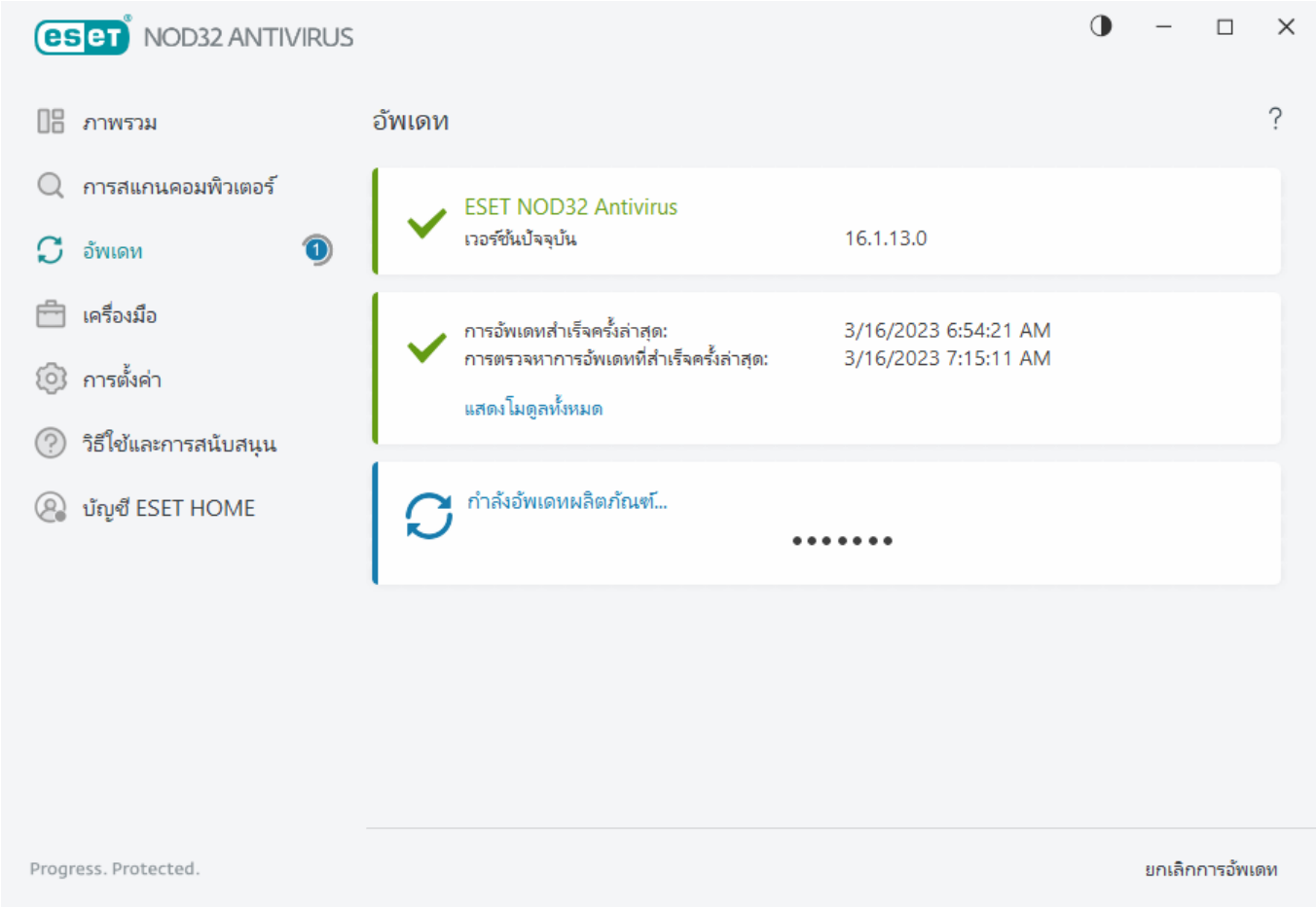
ตรวจหาการอัพเดทสำเร็จครั้งล่าสุด – แสดงวันที่ตรวจหาการอัพเดทสำเร็จครั้งล่าสุด

แสดงโมดูลทั้งหมด – แสดงรายการโมดูลโปรแกรมที่ติดตั้งแล้ว

คลิก **ตรวจสอบการอัพเดท** เพื่อตรวจดู ESET NOD32 Antivirus เวอร์ชันล่าสุดที่ใช้ได้

กระบวนการอัพเดท

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



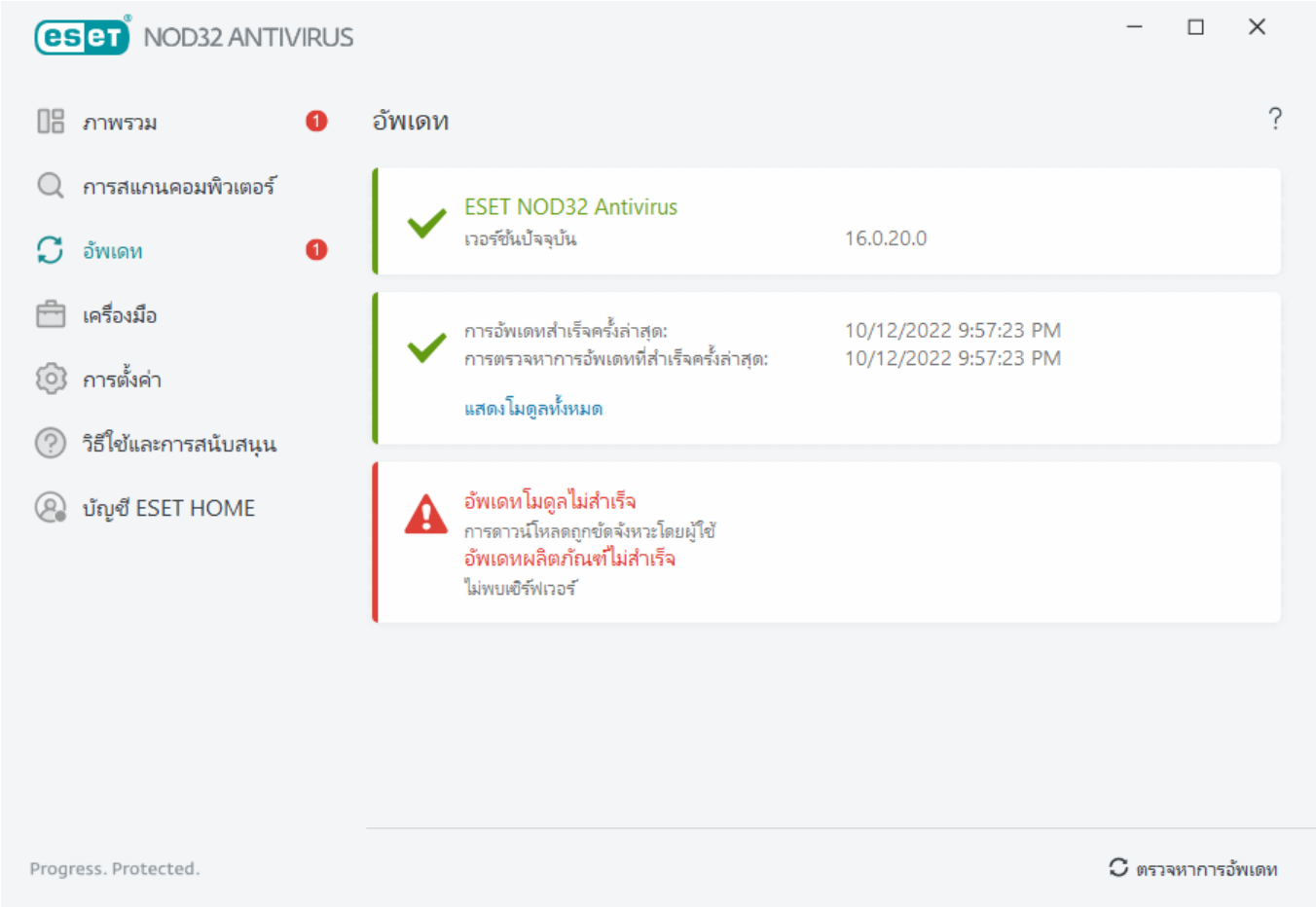
ในสถานการณ์ปกติ คุณจะเห็นเครื่องหมายถูกสีเขียวในหน้าต่าง **อัพเดท** ที่ระบุว่าโปรแกรมนั้นอัพเดทแล้ว หากไม่มีเครื่องหมายถูกสีเขียว แสดงว่าโปรแกรมไม่ได้อัพเดท และมีความเสี่ยงมากขึ้นในการติดไวรัส โปรดอัพเดทโมดูลเร็วที่สุดเท่าที่ทำได้

การอัพเดทที่ไม่สำเร็จ

หากคุณได้รับข้อความการอัพเดทโมดูลที่ไม่สำเร็จ ข้อความนี้อาจเกิดจากปัญหาต่อไปนี้:

1. **การสมัครสมาชิกไม่ถูกต้อง** – การสมัครสมาชิกที่ใช้ในการเปิดใช้งานไม่ถูกต้องหรือหมดอายุแล้ว ใน หน้าต่างโปรแกรมหลัก ให้คลิก **วิธีใช้และการสนับสนุน** > **เปลี่ยนการสมัครสมาชิก** แล้วเปิดใช้งานผลิตภัณฑ์

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



คุณต้องรีสตาร์ทคอมพิวเตอร์ใหม่หลังจากที่อัพเดท ESET NOD32 Antivirus เป็นเวอร์ชันผลิตภัณฑ์ที่ใหม่กว่าสำเร็จ เพื่อให้แน่ใจว่าโมดูลโปรแกรมทั้งหมดได้รับการอัพเดทอย่างถูกต้อง ไม่จำเป็นต้องรีสตาร์ทคอมพิวเตอร์ของคุณหลังการอัพเดทโมเดลเป็นประจำ

สำหรับข้อมูลเพิ่มเติม โปรดไปที่ การแก้ไขปัญหาสำหรับข้อความ "อัพเดทโมดูลไม่สำเร็จ"

หน้าต่างข้อความ - ต้องเริ่มระบบใหม่

จำเป็นต้องรีสตาร์ทคอมพิวเตอร์หลังจากอัพเดท ESET NOD32 Antivirus เป็นเวอร์ชันใหม่ ESET NOD32 Antivirus เวอร์ชันใหม่ได้ออกมาเพื่อปรับปรุงประสิทธิภาพหรือแก้ไขปัญหาที่การอัพเดทอัตโนมัติของโมดูลโปรแกรมไม่สามารถแก้ไขได้

ESET NOD32 Antivirus เวอร์ชันใหม่สามารถติดตั้งอัตโนมัติได้ โดยขึ้นอยู่กับการตั้งค่าการอัพเดทโปรแกรมของคุณ หรือติดตั้งด้วยตนเองได้โดยดาวน์โหลดและติดตั้งเวอร์ชันใหม่ทับเวอร์ชันก่อนหน้า

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

วิธีสร้างงานการอัพเดท

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

การอัพเดทยังสามารถเรียกใช้งานเป็นงานตามกำหนดการ หากต้องการการกำหนดค่างานตามกำหนดการ ให้คลิก **เครื่องมือ** > **เครื่องมือวางกำหนดการณ์** ตามค่าเริ่มต้น งานการอัพเดทต่อไปนี้จะมีการเปิดใช้งานใน ESET NOD32 Antivirus:

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

งานการอัพเดทแต่ละงานจะสามารถแก้ไขได้เพื่อให้เหมาะกับความต้องการของคุณ นอกเหนือจากงานการอัพเดทเริ่มต้นแล้ว คุณสามารถสร้างงานการอัพเดทใหม่ด้วยการกำหนดค่าที่ผู้ใช้กำหนดได้ สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการสร้างและการกำหนดค่างานการอัพเดท โปรดดูที่ เครื่องมือวางกำหนดการ

เครื่องมือ

เมนู**เครื่องมือ**มีคุณลักษณะที่จะมอบความปลอดภัยเพิ่มเติมและช่วยลดความยุ่งยากในการบริหารจัดการ ESET NOD32 Antivirus เครื่องมือต่อไปนี้สามารถใช้งานได้:

ไฟล์บันทึก

กระบวนการที่ทำงานอยู่ (หาก ESET LiveGrid® ได้เปิดใช้อยู่ใน ESET NOD32 Antivirus)

รายงานด้านความปลอดภัย

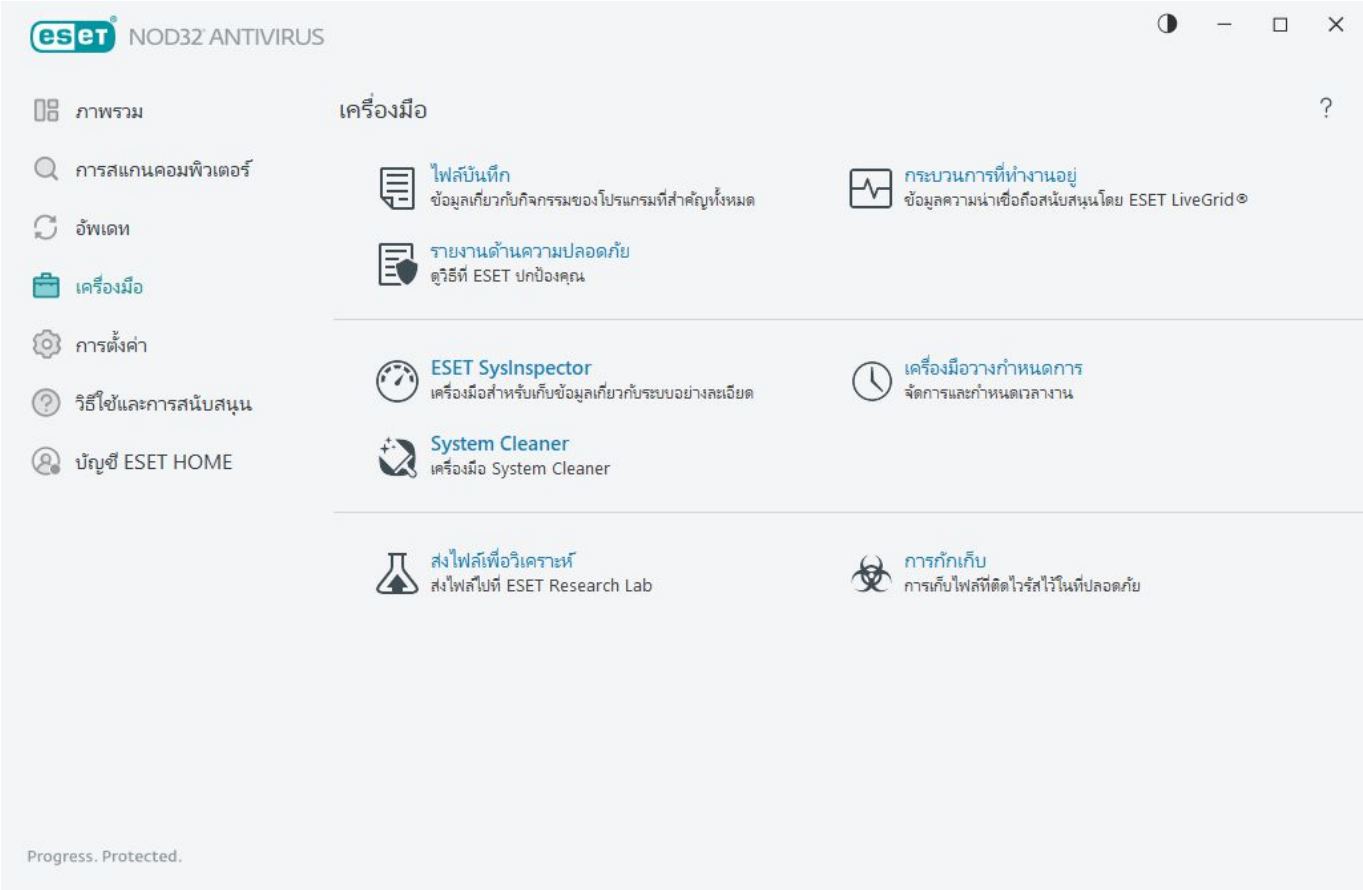
ESET SysInspector

เครื่องมือวางกำหนดการ

เครื่องมือทำความสะอาดระบบ

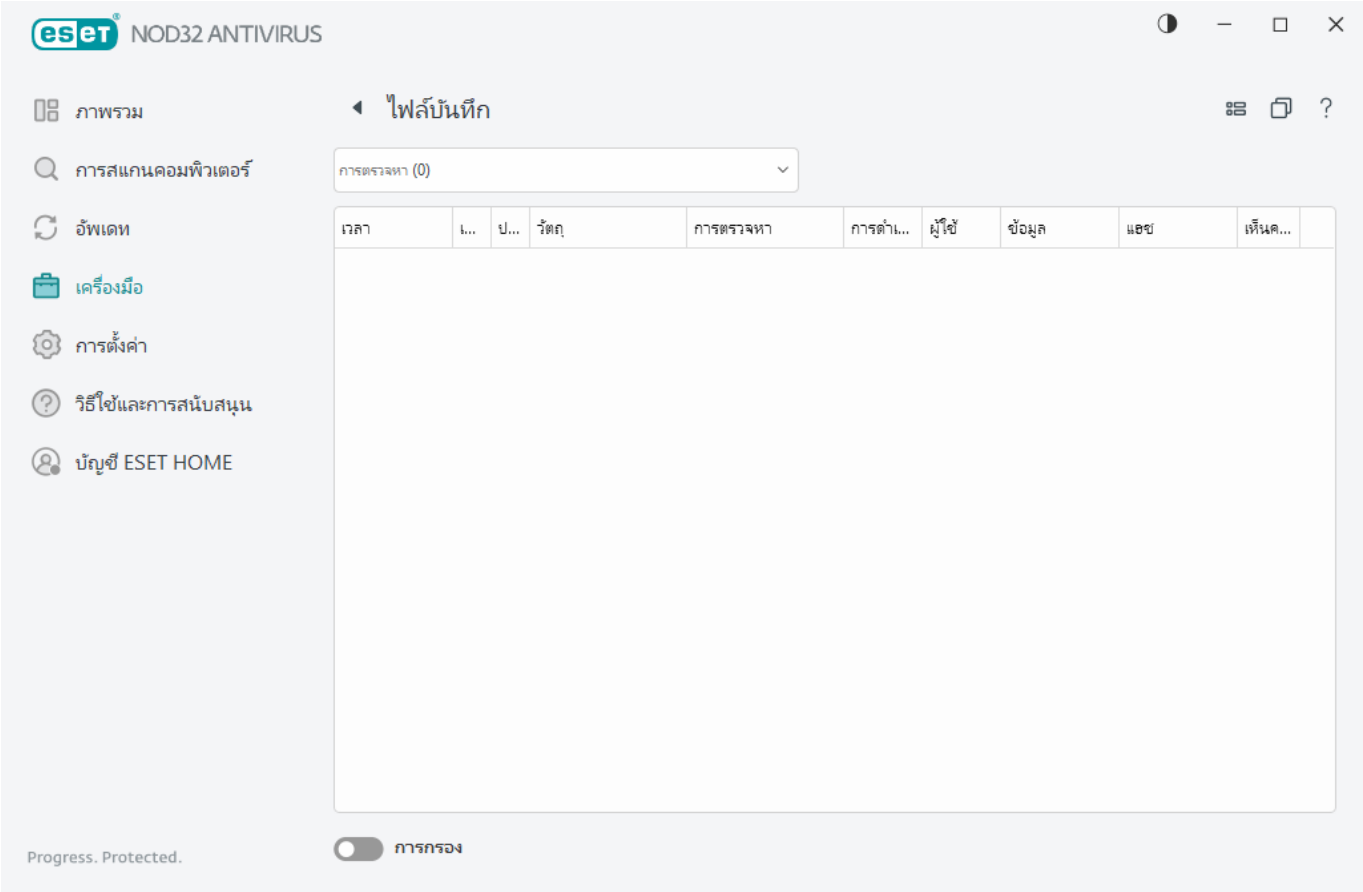
ส่งตัวอย่างเพื่อทำการวิเคราะห์ (อาจไม่สามารถใช้งานได้ตามการกำหนดค่า ESET LiveGrid® ของคุณ)

การกักเก็บ



ไฟล์บันทึก

ไฟล์บันทึกประกอบด้วยข้อมูลเกี่ยวกับเหตุการณ์ของโปรแกรมที่สำคัญที่เกิดขึ้น และให้ภาพรวมของภัยคุกคามที่พบ การบันทึกเป็นส่วนที่จำเป็นในการวิเคราะห์ระบบ การตรวจหาภัยคุกคาม และการแก้ไขปัญหา การบันทึกนั้นดำเนินการในพื้นหลังโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ข้อมูลจะถูกบันทึกตามการตั้งค่าความละเอียดของการบันทึกปัจจุบัน ผู้ใช้สามารถดูข้อความและบันทึกได้โดยตรงจากระบบ ESET NOD32 Antivirus และสามารถอาร์ไคฟ์การบันทึกได้



สามารถเข้าถึงไฟล์บันทึกได้จากหน้าต่างโปรแกรมหลักโดยคลิก**เครื่องมือ** > **ไฟล์บันทึก** เลือกประเภทการบันทึกที่ต้องการโดยใช้เมนูแบบเลื่อนลง บันทึก

- **การตรวจหา** บันทึกนี้จะให้ข้อมูลเกี่ยวกับการตรวจหาและการแฝงตัวที่ตรวจพบโดย ESET NOD32 Antivirus ข้อมูลบันทึกจะประกอบด้วยเวลาที่ตรวจพบ ประเภทเครื่องมือสแกน ประเภทวัตถุ ตำแหน่งของวัตถุ ชื่อของการตรวจหา การดำเนินการ และชื่อของผู้ใช้ที่เข้าสู่ระบบเมื่อการแฝงตัวถูกตรวจพบ แฮช และการปรากฏครั้งแรก การแฝงตัวที่ยังไม่ถูกกำจัดจะถูกทำเครื่องหมายด้วยข้อความสีแดงบนพื้นหลังสีแดงอ่อนเสมอ การแฝงตัวที่ถูกกำจัดแล้วจะถูกทำเครื่องหมายด้วยข้อความสีเหลืองบนพื้นหลังสีขาว PUA ที่ไม่ถูกกำจัดหรือแอปพลิเคชั่นที่อาจไม่ปลอดภัยถูกทำเครื่องหมายด้วยข้อความสีเหลืองบนพื้นหลังสีขาว

- **เหตุการณ์** – การทำงานที่สำคัญทั้งหมดซึ่งดำเนินการโดย ESET NOD32 Antivirus จะบันทึกไว้ในบันทึกเหตุการณ์ บันทึกเหตุการณ์จะมีข้อมูลเกี่ยวกับเหตุการณ์และข้อผิดพลาดที่เกิดขึ้นในโปรแกรม ตัวเลือกนี้ได้รับการออกแบบมาสำหรับผู้ดูแลระบบและผู้ใช้เพื่อแก้ไขปัญหา ข้อมูลที่พบในส่วนนี้มักจะช่วยให้คุณพบทางแก้ปัญหาที่เกิดขึ้นในโปรแกรม

- **การสแกนคอมพิวเตอร์** – ผลลัพธ์ของการสแกนครั้งก่อนหน้าทั้งหมดจะแสดงในหน้าต่างนี้ แต่ละบรรทัดจะแสดงถึงการควบคุมคอมพิวเตอร์หนึ่งรายการ คลิกสองครั้งที่รายการใดก็ได้เพื่อดูรายละเอียดของการสแกนที่เลือก

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

• **เว็บไซต์ที่ถูกกรอง** – รายการนี้จะเป็นประโยชน์เมื่อคุณต้องการดูรายการเว็บไซต์ที่ถูกบล็อกโดย การป้องกันการเข้าถึงเว็บไซต์ ในแต่ละบันทึกจะมีดูข้อมูลเวลา ที่อยู่ URL ผู้ใช้และแอพพลิเคชันที่สร้างการเชื่อมต่อกับเว็บไซต์หนึ่ง

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

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

คลิก **การกรอง** เพื่อเปิดหน้าต่าง การกรองบันทึก ที่ซึ่งคุณสามารถกำหนดเกณฑ์การกรองได้

คลิกขวาบนบันทึกใดบันทึกหนึ่งเพื่อเปิดเมนูบริบท ตัวเลือกต่อไปนี้จะสามารถใช้ได้ในเมนูบริบท:

• **แสดง** – แสดงข้อมูลโดยละเอียดยิ่งขึ้นเกี่ยวกับบันทึกที่เลือกในหน้าต่างใหม่

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

• **กรอง** – หลังจากคลิกตัวเลือกนี้ หน้าต่าง การกรองบันทึก จะอนุญาตให้คุณกำหนดเกณฑ์การกรองสำหรับรายการบันทึกที่ระบุ

• **เปิดใช้งานตัวกรอง** – เปิดใช้งานการตั้งค่าตัวกรอง

• **ปิดใช้งานการกรอง** - ล้างการตั้งค่าตัวกรองทั้งหมด (ดังที่อธิบายไว้ที่ด้านบน)

• **คัดลอก/คัดลอกทั้งหมด** – คัดลอกข้อมูลเกี่ยวกับบันทึกที่เลือกบนหน้าต่าง

• **คัดลอกเซลล์** คัดลอกเนื้อหาของเซลล์ที่คลิกขวา

• **ลบ/ลบทั้งหมด** – ลบบันทึกที่เลือกหรือบันทึกทั้งหมดที่ปรากฏ การดำเนินการนี้ต้องใช้สิทธิ์ของผู้ดูแลระบบ

• **ส่งออก/ส่งออกทั้งหมด** – ส่งออกข้อมูลเกี่ยวกับบันทึกที่เลือกหรือบันทึกทั้งหมดในรูปแบบ XML

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

• **คำอธิบายการตรวจหา** – เปิดสารานุกรมภัยคุกคามของ ESET ซึ่งมีข้อมูลโดยละเอียดเกี่ยวกับอันตรายและอาการของการแฝงตัวที่บันทึกไว้

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

• **เพิ่มไปยังรายการอนุญาตสำหรับการป้องกันเบราว์เซอร์** - เปิดหน้าต่างรายการอนุญาตสำหรับการป้องกันเบราว์เซอร์และเพิ่มรายการที่ต้องการลงในรายการ

การกรองบันทึก

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

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

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

ค้นหาข้อความ

พิมพ์สตริง (คำหรือส่วนหนึ่งของคำ) จะแสดงเฉพาะบันทึกที่มีสตริงนี้ บันทึกอื่นๆ จะถูกยกเว้น

ค้นหาในคอลัมน์

เลือกคอลัมน์ที่จะได้รับการพิจารณาเมื่อทำการค้นหา คุณสามารถตรวจสอบหนึ่งคอลัมน์ที่จะใช้ในการค้นหาได้

ประเภทบันทึก

เลือกการบันทึกหนึ่งประเภทจากเมนูแบบเลื่อนลง:

- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- **มีข้อมูล** – บันทึกข้อความแจ้งข้อมูล รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน
- **ข้อผิดพลาด** – ข้อผิดพลาด เช่น "เกิดข้อผิดพลาดขณะดาวน์โหลดไฟล์" และข้อผิดพลาดร้ายแรงจะถูกบันทึก
- **ร้ายแรง** – บันทึกเฉพาะข้อผิดพลาดร้ายแรง (ข้อผิดพลาดในการเริ่มต้นการป้องกันไวรัส

ช่วงเวลา

ระบุช่วงเวลาที่คุณต้องการให้แสดงผลลัพธ์

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

ตรงทั้งคำเท่านั้น

ใช้ช่องทำเครื่องหมายนี้ถ้าคุณต้องการค้นหาทั้งคำเพื่อให้ได้ผลลัพธ์ที่แม่นยำยิ่งขึ้น

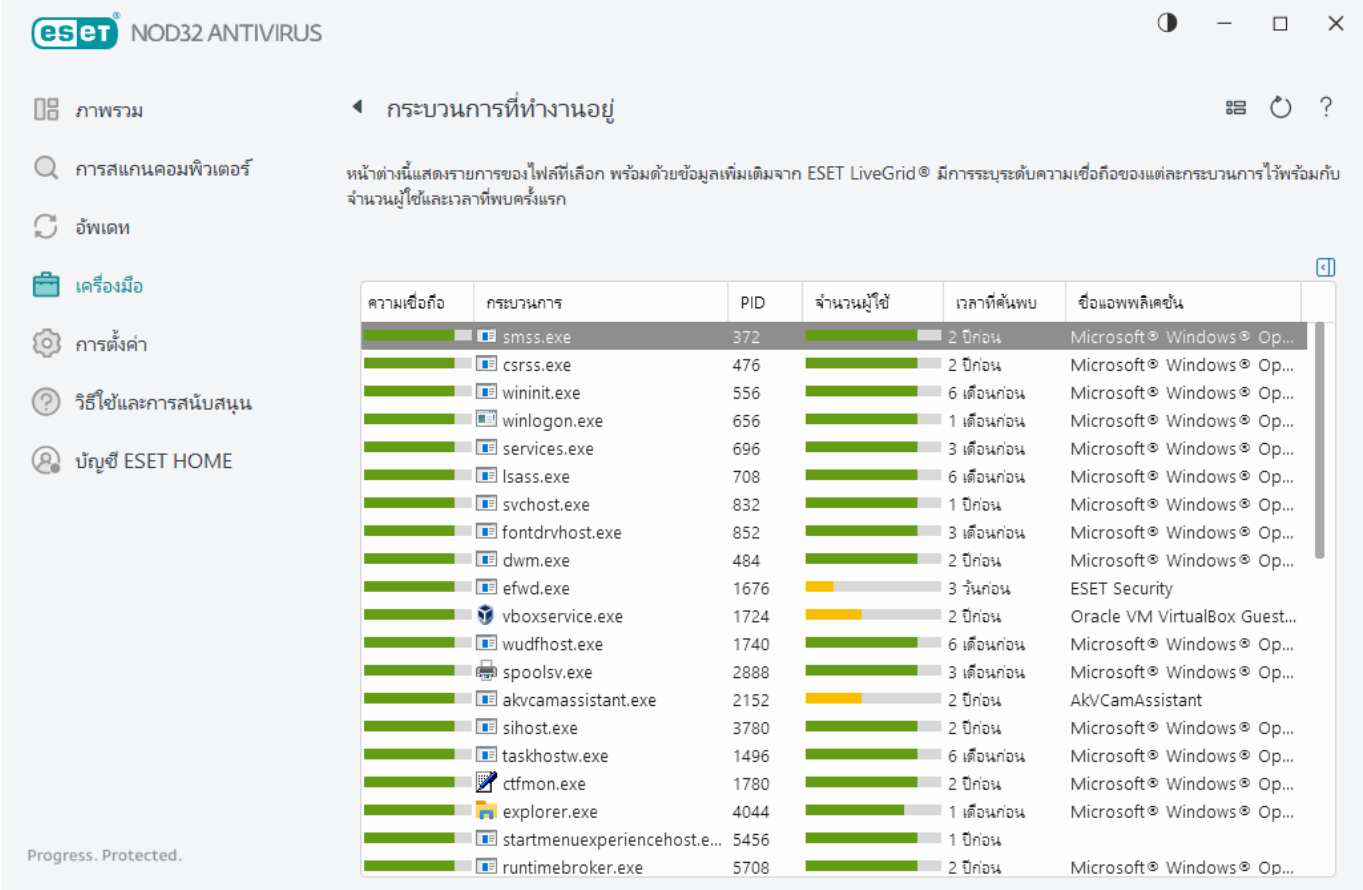
ตรงตามตัวพิมพ์

เปิดใช้งาน ตัวเลือกนี้ หากคุณจำเป็นต้องใช้ตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ในขณะกรอง เมื่อคุณกำหนดค่าตัวเลือกการกรอง/การค้นหาแล้ว ให้คลิก**ตกลง** เพื่อแสดงบันทึกการกรองหรือ**ค้นหา** เพื่อเริ่มการค้นหา ไฟล์บันทึกจะถูกค้นหาจากบนลงล่าง เริ่มจากตำแหน่งปัจจุบันของคุณ (บันทึกที่ถูกไฮไลท์) การค้นหาจะหยุดเมื่อค้นหาบันทึกที่ตรง

กันอย่างแรก กด**F3** เพื่อค้นหาบันทึกถัดไปหรือคลิกขวา แล้วเลือก**ค้นหา** เพื่อระบุตัวเลือกการค้นหาของคุณอีกครั้ง

กระบวนการที่ทำงานอยู่

กระบวนการที่ทำงานอยู่จะแสดง โปรแกรมหรือกระบวนการ ที่ทำงานอยู่ในคอมพิวเตอร์ของคุณ และทำให้ ESET ได้รับรู้ข้อมูลเกี่ยวกับการบุกรุกใหม่ได้ทันทีและต่อเนื่อง ESET NOD32 Antivirus จะแสดงข้อมูลโดยละเอียดเกี่ยวกับกระบวนการที่ทำงานอยู่เพื่อคุ้มครองผู้ใช้ด้วยเทคโนโลยี ESET LiveGrid®



ความเชื่อถือ – ในกรณีส่วนใหญ่ ESET NOD32 Antivirus และเทคโนโลยี ESET LiveGrid® จะกำหนดระดับความเสี่ยงให้กับวัตถุ (ไฟล์ กระบวนการ รหัสรีจิสตรี เป็นต้น) โดยใช้ชุดกฎการวิเคราะห์พฤติกรรมที่ตรวจสอบลักษณะของวัตถุแต่ละรายการ จากนั้นจะชั่งน้ำหนักโอกาสที่จะเป็นกิจกรรมที่เป็นอันตราย จากการวิเคราะห์พฤติกรรมเหล่านี้ วัตถุจะได้รับการกำหนดระดับความเสี่ยงตั้งแต่ 1 – ดี (สีเขียว) จนถึง 9 – มีความเสี่ยง (สีแดง)

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

แป้นพิมพ์

> แอพพลิเคชันที่รู้จักและถูกทำเครื่องหมายเป็น ดี (สีเขียว) เพื่อแสดงว่ามีความปลอดภัย (อยู่ในรายการที่ปลอดภัย) และจะไม่รวมในการสแกนเพื่อปรับปรุงประสิทธิภาพ

PID - หมายเลขตัวบ่งชี้กระบวนการอาจถูกใช้เป็นพารามิเตอร์ในการเรียกฟังก์ชันต่างๆ เช่น การปรับลำดับความสำคัญของกระบวนการ

จำนวนผู้ใช้ – จำนวนผู้ใช้ที่ใช้แอพพลิเคชันที่ระบุ ข้อมูลนี้ได้รับการรวบรวมโดยเทคโนโลยี ESET LiveGrid®

เวลาที่ค้นพบ – ระยะเวลาตั้งแต่เทคโนโลยี ESET LiveGrid® ค้นพบแอพพลิเคชัน

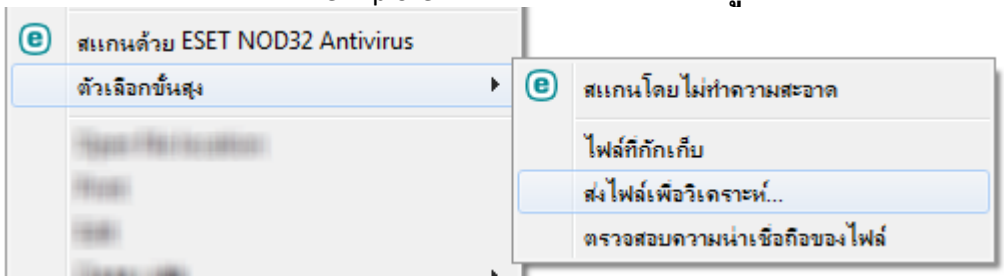
> แอพพลิเคชันที่ถูกทำเครื่องหมายเป็น ไม่ทราบ (สีส้ม) ไม่ได้หมายความว่าจะเป็นซอฟต์แวร์ที่เป็นอันตรายเสมอไป โดยปกติแล้วจะเป็นแอพพลิเคชันใหม่ หากคุณไม่แน่ใจเกี่ยวกับไฟล์ คุณสามารถ ส่งไฟล์สำหรับการวิเคราะห์ ไปที่ ESET Research Lab หากตรวจพบว่าไฟล์เป็นแอพพลิเคชันที่เป็นอันตราย ข้อมูลการตรวจพบไฟล์นี้จะถูกเพิ่มในการอัพเดทที่กำลังจะมีขึ้น

ชื่อแอพพลิเคชัน – ชื่อที่กำหนดของโปรแกรมหรือกระบวนการ

คลิกที่แอพพลิเคชันหนึ่งเพื่อแสดงรายละเอียดต่อไปนี้ของแอพพลิเคชันดังกล่าว:

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

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



รายงานด้านความปลอดภัย

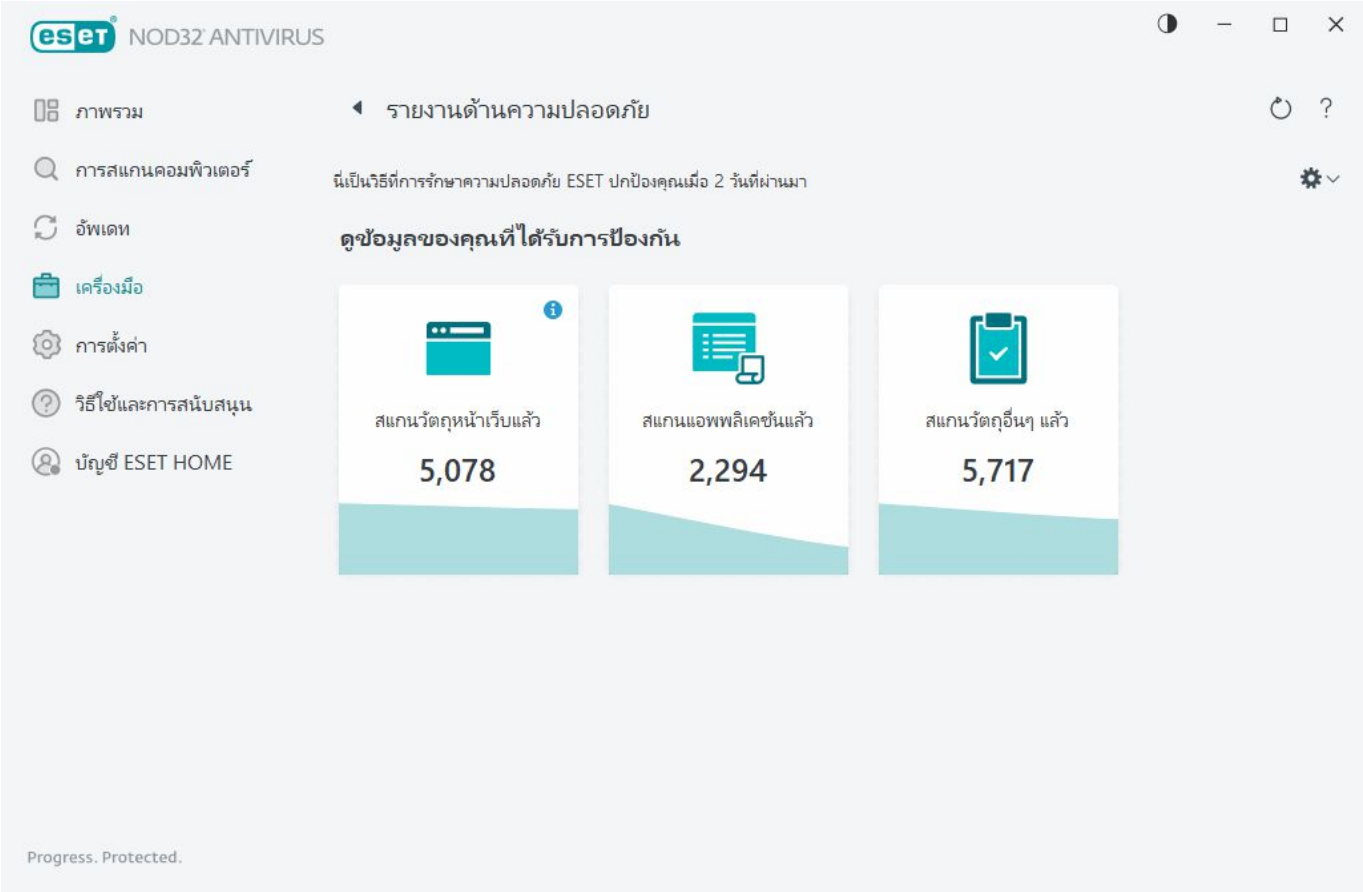
คุณลักษณะนี้จะให้ภาพรวมสถิติสำหรับประเภทต่อไปนี้:

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

ลำดับของประเภทเหล่านี้จะเป็นไปตามค่าตัวเลขจากสูงสุดไปต่ำสุด ประเภทที่มีค่าเป็นศูนย์จะไม่ถูกแสดง คลิก **แสดงเพิ่มขึ้น** เพื่อขยายและแสดงประเภทที่ซ่อนอยู่

เมื่อคุณลักษณะนี้ถูกเปิดใช้งาน คุณลักษณะดังกล่าวจะไม่แสดงเป็นไม่ทำงานในรายงานด้านความปลอดภัยอีกต่อไป

เมื่อคลิกที่ล้อเฟือง ที่มุมขวาบน คุณจะสามารถ **เปิด/ปิดใช้งานการแจ้งเตือนรายงานด้านความปลอดภัย** หรือเลือกว่าจะให้โปรแกรมแสดงข้อมูลจาก 30 วันที่ผ่านมาหรือนับจากที่คุณเริ่มเปิดใช้งานผลิตภัณฑ์ได้ หากคุณติดตั้ง ESET NOD32 Antivirus เป็นเวลาน้อยกว่า 30 วัน คุณจะสามารถเลือกจำนวนวันนับจากที่คุณเริ่มติดตั้งผลิตภัณฑ์ได้เท่านั้น ช่วงเวลา 30 วันจะถูกเลือกตามค่าเริ่มต้น



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

ESET SysInspector

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

หน้าต่าง ESET SysInspector จะแสดงข้อมูลเกี่ยวกับบันทึกดังต่อไปนี้:

- **เวลา** – เวลาของการสร้างบันทึก
- **ความคิดเห็น** – ความคิดเห็นสั้นๆ
- **ผู้ใช้** – ชื่อของผู้ใช้ที่สร้างบันทึก

- **สถานะ** – สถานะของการสร้างบันทึก

การทำงานที่ใช้ได้มีดังนี้:

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

รายการต่อไปนี้จะนำมาใช้ได้จากเมนูบริบทเมื่อเลือกไฟล์บันทึกหนึ่งไฟล์หรือหลายไฟล์:

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

เครื่องมือวางกำหนดการ

เครื่องมือวางกำหนดการจะจัดการและเรียกใช้งานตามกำหนดการโดยใช้การกำหนดค่าและคุณสมบัติที่กำหนดไว้ล่วงหน้า

เครื่องมือวางกำหนดการณ์นั้นสามารถเข้าถึงได้จาก หน้าต่างโปรแกรมหลัก ของ ESET NOD32 Antivirus โดยคลิก **เครื่องมือ** > **เครื่องมือวางกำหนดการณ์ เครื่องมือวางกำหนดการ** มีรายการงานตามกำหนดการทั้งหมด และคุณสมบัติของการกำหนดค่า เช่น วันที่ที่กำหนดไว้ล่วงหน้า เวลา และโปรไฟล์การสแกนที่ใช้

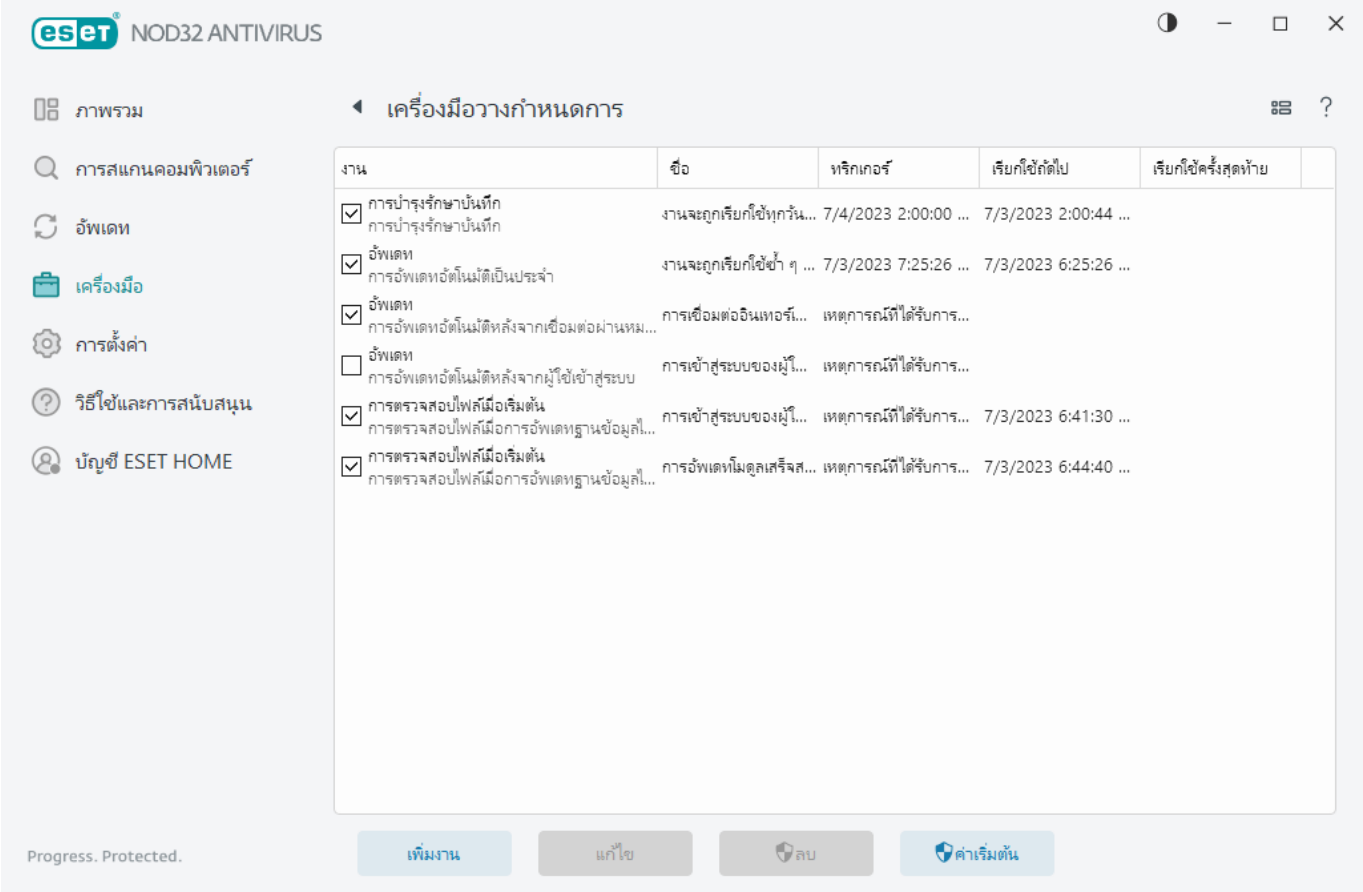
เครื่องมือวางกำหนดการจะทำหน้าที่ในการวางกำหนดการงานต่อไปนี้: การอัพเดทโมดูล การสแกนงาน การตรวจสอบไฟล์การเริ่มต้นของระบบ และการบำรุงรักษาบันทึก คุณสามารถเพิ่มหรือลบงานได้โดยตรงจากหน้าต่างของเครื่องมือวางกำหนดการหลัก (คลิก **เพิ่มงาน** หรือ **ลบ** ที่ส่วนล่างของหน้าต่าง) คุณสามารถคืนค่ารายการงานตาม

กำหนดการเป็นค่าเริ่มต้นและลบการเปลี่ยนแปลงทั้งหมดโดยคลิก **ค่าเริ่มต้น** คลิกขวาที่ใดก็ได้ในหน้าต่างของเครื่องมือวางกำหนดการเพื่อดำเนินการดังต่อไปนี้: แสดงข้อมูลเป็นรายละเอียด ทำงานทันที เพิ่มงานใหม่ และลบงานที่มีอยู่ ใช้ช่องทำเครื่องหมายที่ด้านหน้าของแต่ละรายการเพื่อเปิด/ปิดการทำงาน

ตามค่าเริ่มต้น งานตามกำหนดการต่อไปนี้จะปรากฏใน **เครื่องมือวางกำหนดการ**:

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

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



เพิ่มงานใหม่

1. คลิกที่ **เพิ่มงาน** ที่ส่วนล่างของหน้าต่าง

2. ป้อนชื่อของงาน

3. เลือกงานที่ต้องการจากเมนูแบบเลื่อนลง:

- **เรียกใช้แอพพลิเคชันภายนอก** – วางกำหนดการเรียกใช้แอพพลิเคชันภายนอก

- **การบำรุงรักษาบันทึก** - ไฟล์บันทึกยังมีข้อมูลที่เหลืออยู่จากบันทึกที่ลบแล้ว งานนี้จะช่วยเพิ่มประสิทธิภาพการบันทึกในไฟล์บันทึกเป็นประจำเพื่อให้มีประสิทธิภาพการทำงานเพิ่มขึ้น

- **การตรวจสอบไฟล์เมื่อเริ่มต้น** – ตรวจสอบไฟล์ที่อนุญาตให้เรียกใช้ได้เมื่อเริ่มต้นระบบหรือเข้าสู่ระบบ

- **สร้างสแนปชอตสถานะของคอมพิวเตอร์** – สร้างสแนปชอตคอมพิวเตอร์ของ ESET SysInspector โดยรวบรวมข้อมูลโดยละเอียดเกี่ยวกับองค์ประกอบของระบบ (ตัวอย่างเช่น ไดรเวอร์ แอพพลิเคชัน) และประเมินระดับความเสี่ยงขององค์ประกอบแต่ละรายการ

- **การสแกนคอมพิวเตอร์ตามต้องการ** – ดำเนินการสแกนคอมพิวเตอร์ของไฟล์และโฟลเดอร์บนคอมพิวเตอร์ของคุณ

- **อัพเดท** – วางกำหนดการงานการอัพเดทโดยการอัพเดทโมดูลเหล่านี้

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

- **หนึ่งครั้ง** – งานจะดำเนินการตามวันและเวลาที่กำหนดไว้ล่วงหน้า

- **ซ้ำ** – งานจะดำเนินการตามระยะเวลาที่กำหนด

- **รายวัน** – งานจะเรียกใช้ซ้ำทุกวันตามเวลาที่กำหนด

- **รายสัปดาห์** – งานจะเรียกใช้ตามวันที่และเวลาที่เลือก

- **ตามเหตุการณ์** – งานจะดำเนินการตามเหตุการณ์ที่กำหนด

5. เลือก **ข้ามงานเมื่อทำงานด้วยแบตเตอรี่** เพื่อลดการใช้ทรัพยากรของระบบในขณะที่แล็ปท็อปทำงานด้วยพลังงานแบตเตอรี่ งานจะถูกเรียกใช้ตามวันที่และเวลาที่ระบุในช่อง **การเรียกใช้งาน** หากงานไม่สามารถทำงาน

ได้ตามเวลาที่กำหนดไว้ล่วงหน้า คุณสามารถระบุช่วงเวลาที่จะให้มีการดำเนินการอีกครั้ง:

- **เมื่อเวลาที่กำหนดไว้ครั้งต่อไป**
- **เร็วที่สุดเท่าที่ทำได้**
- **ทันที หากระยะเวลาตั้งแต่เรียกใช้ครั้งล่าสุดเกิน (ชั่วโมง)** – หมายถึงเวลาที่ผ่านไปนับตั้งแต่ข้ามการเรียกใช้งานนี้เป็นครั้งแรก หากเกินเวลานี้ งานจะดำเนินการทันที ตั้งเวลาโดยใช้ตัวหมุนด้านล่าง

หากต้องการตรวจสอบงานที่กำหนดเวลาไว้ ให้คลิกขวาที่งานแล้วคลิก **แสดงรายละเอียดงาน**

ตัวเลือกการสแกนตามกำหนดการ

ในหน้าต่างนี้คุณสามารถระบุตัวเลือกขั้นสูงสำหรับงานสแกนคอมพิวเตอร์ที่กำหนดเวลาได้

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

เมื่อเลือก **ละเว้นการยกเว้น** ไฟล์ที่มีนามสกุลไฟล์ที่ไม่ได้รับการสแกนก่อนหน้านี้จะถูกสแกนโดยไม่มีข้อยกเว้น

เมนูแบบเลื่อนลง **การทำงานหลังสแกน** ทำให้คุณสามารถตั้งค่าการทำงานที่จะดำเนินการโดยอัตโนมัติหลังจากการสแกนเสร็จสิ้นได้:

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

กลับมาทำงานต่อได้อย่างรวดเร็ว

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

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

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

เลือก **ไม่สามารถยกเลิกการสแกนได้** เพื่อปฏิเสธผู้ใช้ที่ไม่ได้รับสิทธิ์ให้หยุดการดำเนินการหลังจากการสแกน

เลือกตัวเลือก **ผู้ใช้สามารถหยุดการสแกนเป็นเวลา (นาที)** หากคุณต้องการให้ผู้ใช้ในจำนวนที่จำกัดหยุดสแกนคอมพิวเตอร์ชั่วความตามระยะเวลาที่กำหนดไว้

ดูเพิ่มเติมที่ ความคืบหน้าของการสแกน

ภาพรวมของงานตามกำหนดการ

หน้าต่างข้อความนี้จะแสดงข้อมูลอย่างละเอียดเกี่ยวกับงานตามกำหนดการที่เลือกเมื่อคุณคลิกสองครั้งที่งานที่กำหนดเองหรือคลิกขวาที่งานตามกำหนดการที่กำหนดเองแล้วคลิก **แสดงรายละเอียดงาน**

รายละเอียดงาน

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

• **เรียกใช้แอพพลิเคชันภายนอก** – วางกำหนดการเรียกใช้แอพพลิเคชันภายนอก

• **การบำรุงรักษาบันทึก** - ไฟล์บันทึกยังมีข้อมูลที่เหลืออยู่จากบันทึกที่ลบแล้ว งานนี้จะช่วยเพิ่มประสิทธิภาพการบันทึกในไฟล์บันทึกเป็นประจำเพื่อให้มีประสิทธิภาพการทำงานเพิ่มขึ้น

• **การตรวจสอบไฟล์เมื่อเริ่มต้น** – ตรวจสอบไฟล์ที่อนุญาตให้เรียกใช้ได้เมื่อเริ่มต้นระบบหรือเข้าสู่ระบบ

- **สร้างสแนปชอตสถานะของคอมพิวเตอร์** – สร้างสแนปชอตคอมพิวเตอร์ของ ESET SysInspector โดยรวบรวมข้อมูลโดยละเอียดเกี่ยวกับองค์ประกอบของระบบ (ตัวอย่างเช่น ไดรเวอร์ แอพพลิเคชัน) และประเมินระดับความเสี่ยงขององค์ประกอบแต่ละรายการ

- **การสแกนคอมพิวเตอร์ตามต้องการ** – ดำเนินการสแกนคอมพิวเตอร์ของไฟล์และโฟลเดอร์บนคอมพิวเตอร์ของคุณ

- **อัพเดท** – วางกำหนดการงานการอัพเดทโดยการอัพเดทโมดูลเหล่านี้

เวลางาน

งานจะเริ่มดำเนินการซ้ำๆ ตามระยะเวลาที่กำหนดไว้ เลือกหนึ่งในตัวเลือกเวลาต่อไปนี้:

- **หนึ่งครั้ง** – งานจะดำเนินการเพียงครั้งเดียวตามวันที่และเวลาที่กำหนดไว้ล่วงหน้า

- **ซ้ำ** – งานจะเริ่มดำเนินการตามช่วงเวลาที่ระบุ (เป็นชั่วโมง)

- **รายวัน** – งานจะเรียกใช้ทุกวันตามเวลาที่กำหนด

- **รายสัปดาห์** – งานจะเรียกใช้อย่างน้อยหนึ่งครั้งต่อสัปดาห์ตามวันและเวลาที่เลือกไว้

- **ตามเหตุการณ์** – งานจะดำเนินการหลังจากเหตุการณ์ที่กำหนด

ข้ามงานเมื่อทำงานด้วยแบตเตอรี่ – งานจะไม่เริ่มต้นดำเนินการ ถ้าคอมพิวเตอร์ของคุณใช้แบตเตอรี่ในขณะที่งานควรเริ่มต้น นอกจากนี้ยังมีผลกับคอมพิวเตอร์ที่ใช้ UPS ด้วย

เวลางาน - หนึ่งครั้ง

การเรียกใช้งาน – งานที่ระบุจะถูกเรียกใช้งานเพียงครั้งเดียวในวันที่และเวลาที่ระบุ

เวลางาน - รายวัน

งานจะเรียกใช้ทุกวันตามเวลาที่กำหนด

เวลางาน - รายสัปดาห์

งานจะดำเนินการซ้ำทุกสัปดาห์ในวันและเวลาที่เลือกไว้

เวลางาน - ตามเหตุการณ์

งานจะถูกเรียกโดยเหตุการณ์หนึ่งดังต่อไปนี้:

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

เมื่อการวางกำหนดการงานถูกเรียกโดยเหตุการณ์ คุณสามารถระบุช่วงเวลาต่ำสุดระหว่างการทำงานเสร็จทั้งสองงาน ตัวอย่างเช่น หากคุณเข้าสู่คอมพิวเตอร์ของคุณหลายครั้งในหนึ่งวัน ให้เลือก 24 ชั่วโมง เพื่อให้ดำเนินการเฉพาะแค่ในครั้งแรกที่เข้าสู่ระบบของวันดังกล่าวและวันถัดไป

งานที่ข้าม

งานสามารถข้ามได้เมื่อคอมพิวเตอร์ทำงานด้วยพลังงานแบตเตอรี่หรือเมื่อปิดเครื่องอยู่ เลือกช่วงเวลาที่จะเรียกใช้งานที่ข้ามไปจากตัวเลือกใดตัวเลือกหนึ่งต่อไปนี้แล้วคลิก **ถัดไป**:

- **เมื่อเวลาที่กำหนดไว้ครั้งต่อไป** – งานจะดำเนินการหากคอมพิวเตอร์เปิดเครื่องอยู่เมื่อถึงเวลาที่กำหนดไว้ครั้งต่อไป
- **เร็วที่สุดเท่าที่ทำได้** – งานจะดำเนินการเมื่อคอมพิวเตอร์เปิดเครื่อง

• **ทันที หากระยะเวลาตั้งแต่เรียกใช้ตามกำหนดการครั้งล่าสุดเกิน (ชั่วโมง)** – หมายถึงเวลาที่ผ่านไปนับตั้งแต่ข้ามการเรียกใช้งานนี้เป็นครั้งแรก หากเกินเวลานี้ งานจะดำเนินการทันที

ทันที หากระยะเวลาตั้งแต่เรียกใช้ตามกำหนดการครั้งล่าสุดเกิน (ชั่วโมง) - ตัวอย่าง

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

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

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

รายละเอียดงาน - อัพเดท

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

รายละเอียดงาน - เรียกใช้แอพพลิเคชัน

งานนี้จะวางกำหนดการเรียกใช้แอพพลิเคชันภายนอก

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

โฟลเดอร์การทำงาน – กำหนดไดเรกทอรีการทำงานของแอพพลิเคชันภายนอก ไฟล์ชั่วคราวทั้งหมดของ **ไฟล์ที่เรียกใช้ได้** ที่เลือกไว้จะสร้างขึ้นภายในไดเรกทอรีนี้

พารามิเตอร์ – พารามิเตอร์ของบรรทัดคำสั่งสำหรับแอพพลิเคชัน (ไม่จำเป็น)

คลิก **สิ้นสุด** เพื่อใช้งาน

เครื่องมือทำความสะอาดระบบ

เครื่องมือทำความสะอาดระบบเป็นเครื่องมือที่จะช่วยให้คุณกู้คืนคอมพิวเตอร์ให้อยู่ในสภาพที่ใช้งานได้หลังจากกำจัดภัยคุกคามแล้ว มัลแวร์สามารถปิดใช้งานโปรแกรมอรรถประโยชน์ของระบบได้ เช่น Registry Editor, โปรแกรมจัดการงาน หรือการอัพเดท Windows เครื่องมือทำความสะอาดระบบจะกู้คืนค่าและการตั้งค่าเริ่มต้นของระบบดังกล่าวด้วยการคลิกเพียงครั้งเดียว

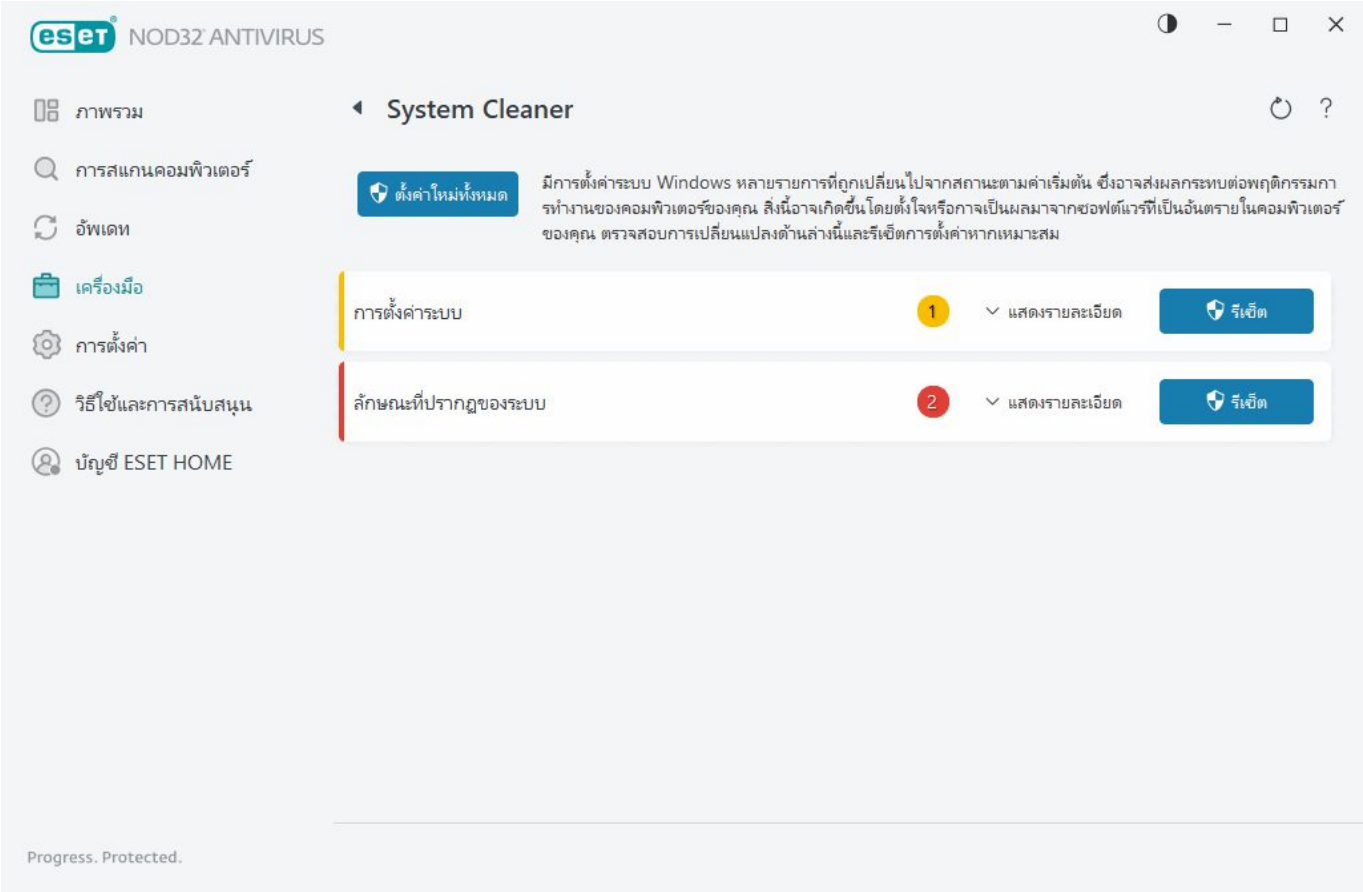
เครื่องมือทำความสะอาดระบบจะรายงานปัญหาจากประเภทการตั้งค่าห้าประเภท:

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

สามารถเรียกใช้เครื่องมือกำจัดไวรัสในระบบได้เมื่อ:

- พบภัยคุกคาม
- ผู้ใช้คลิก **รีเซ็ต**

คุณสามารถตรวจสอบการเปลี่ยนแปลงและรีเซ็ตการตั้งค่าได้หากเหมาะสม



เฉพาะผู้ใช้ที่มีสิทธิ์ของผู้ดูแลระบบที่สามารถดำเนินการในเครื่องมือทำความสะอาดระบบได้

กักเก็บ

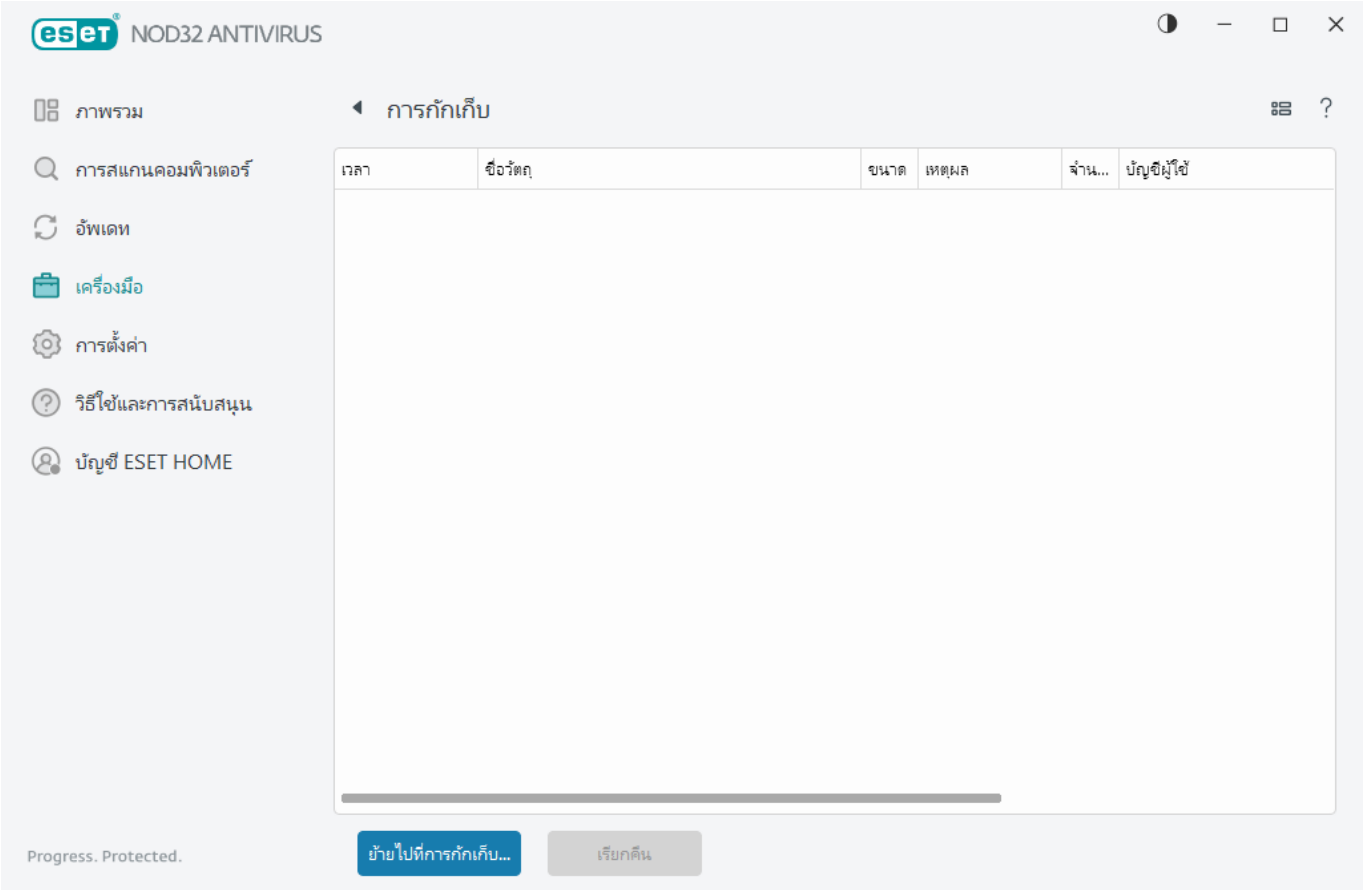
ฟังก์ชันหลักของการกักเก็บคือการจัดเก็บวัตถุที่มีการรายงานไว้อย่างปลอดภัย (เช่น มัลแวร์ ไฟล์ที่ติดไวรัสหรือแอปพลิเคชั่นที่อาจไม่พึงประสงค์)

การกักเก็บนั้นสามารถเข้าถึงได้จาก หน้าต่างโปรแกรมหลัก ของ ESET NOD32 Antivirus โดยการคลิก **เครื่องมือ > การกักเก็บ**

ไฟล์ที่เก็บไว้ในโฟลเดอร์กักเก็บนั้นสามารถดูได้ในตารางที่แสดง:

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

• และจำนวนครั้งในการตรวจหา (ตัวอย่างเช่น การตรวจหาซ้ำในไฟล์เดียวกันหรือหากเป็นอาร์ไคฟ์ที่มีการบุกรุกหลายครั้ง)



การกักเก็บไฟล์

ESET NOD32 Antivirus จะกักเก็บไฟล์ที่ลบโดยอัตโนมัติ (หากคุณไม่ได้ยกเลิกตัวเลือกนี้ใน หน้าต่างเตือนภัย)

ไฟล์เพิ่มเติมที่ควรถูกกักเก็บหาก:

a.ไม่สามารถกำจัดได้

b.หากเป็นไฟล์ที่ไม่ปลอดภัยหรือระบบแนะนำให้ลบ

c.หากมีการตรวจพบด้วยความผิดพลาดโดย ESET NOD32 Antivirus

d.หรือหากไฟล์ทำงานน่าสงสัยแต่ไม่มีการตรวจพบโดย การป้องกัน

คุณมีตัวเลือกหลายประการในการกักเก็บไฟล์:

a.คุณสามารถใช้คุณสมบัติลากและวางเพื่อกักเก็บไฟล์ด้วยตัวเองได้ โดยให้คลิกที่ไฟล์หรือโฟลเดอร์ แล้วเลื่อนตัวชี้เมาส์ไปยังบริเวณที่ทำเครื่องหมายขณะที่กดปุ่มเมาส์ค้างไว้ จากนั้นจึงปล่อยนิ้ว หลังจากนั้น

แอพพลิเคชันจะเลื่อนมาที่เบื้องหน้า

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

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

d.นอกจากนี้ยังสามารถใช้เมนูบริบทเพื่อการทำงานนี้ โดยให้คลิกขวาในหน้าต่าง **กักเก็บ** และเลือก **กักเก็บ**

การเรียกคืนจากการกักเก็บ

นอกจากนี้ไฟล์ที่ถูกกักเก็บยังสามารถเรียกคืนไปยังตำแหน่งดั้งเดิมได้อีกด้วย:

• ใช้คุณสมบัติ **เรียกคืน** สำหรับการดำเนินการดังกล่าว ซึ่งสามารถใช้งานได้จากเมนูบริบทโดยคลิกไฟล์ที่ต้องการในการกักเก็บ

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

• นอกจากนี้เมนูบริบทยังมีตัวเลือก **เรียกคืนไปที่** ซึ่งช่วยให้คุณสามารถเรียกคืนไฟล์ไปยังตำแหน่งอื่นนอกเหนือจากตำแหน่งที่ถูกลบได้

• ในบางกรณีจะไม่สามารถใช้งานฟังก์ชันการเรียกคืนได้ ตัวอย่างเช่น ไฟล์ที่ตั้งอยู่ในการแชร์เครือข่ายที่อ่านได้อย่างเดียวเท่านั้น

การลบจากการกักเก็บ

คลิกขวารายการที่ระบุ แล้วเลือก **ลบจากการกักเก็บ** หรือเลือกรายการที่คุณต้องการลบแล้วกด **ลบ** บนแป้นพิมพ์ของคุณ หากคุณต้องการเลือกและลบรายการทั้งหมดในการกักเก็บ คุณสามารถกด **Ctrl + A** แล้วกด **Delete** บนแป้นพิมพ์ได้ รายการที่ถูกลบจะถูกนำออกจากอุปกรณ์ของคุณและการกักเก็บอย่างถาวร

การส่งไฟล์จากการกักเก็บ

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

คำอธิบายการตรวจหา

คลิกขวาที่รายการและคลิก **คำอธิบายการตรวจหา** เพื่อเปิดสารานุกรมภัยคุกคามของ ESET ซึ่งมีข้อมูลโดยละเอียดเกี่ยวกับอันตรายและอาการของการแฝงตัวที่บันทึกไว้

> **คำแนะนำพร้อมภาพประกอบ**
> บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
> - เรียกคืนไฟล์ที่กักเก็บใน ESET NOD32 Antivirus
> - ลบไฟล์ที่กักเก็บใน ESET NOD32 Antivirus
> - ผลิตภัณฑ์ My ESET แจ้งเตือนการตรวจหาให้ฉันทราบ—ฉันควรทำอย่างไร

การกักเก็บล้มเหลว

เหตุผลที่ไฟล์บางไฟล์ไม่สามารถย้ายไปยังการกักเก็บมีดังต่อไปนี้:

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

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

เลือกตัวอย่างเพื่อวิเคราะห์

หากคุณพบไฟล์ที่มีพฤติกรรมน่าสงสัยในคอมพิวเตอร์ของคุณหรือเว็บไซต์ที่น่าสงสัยในอินเทอร์เน็ต คุณสามารถส่งไปยังห้องปฏิบัติการวิจัย ESET เพื่อรับการวิเคราะห์ได้ (อาจไม่สามารถใช้งานได้ขึ้นอยู่กับการตั้งค่า ESET LiveGrid® ของคุณ)

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

คุณสามารถส่งตัวอย่าง (ไฟล์หรือเว็บไซต์) ไปยัง ESET เพื่อวิเคราะห์โดยใช้หนึ่งในวิธีดังต่อไปนี้:

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

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

3. หากต้องการรายงานสแปมหรือสแปมการตรวจพบที่ผิดพลาด โปรดอ่าน บทความฐานความรู้ ESET ของเรา

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

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

ไฟล์/ไซต์ – พาธไปยังไฟล์หรือเว็บไซต์ที่คุณต้องการส่ง

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

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

เลือกตัวอย่างเพื่อวิเคราะห์ – ไฟล์ที่น่าสงสัย

สัญญาณและอาการที่พบของการติดไวรัสจากมัลแวร์ – ป้อนคำอธิบายเกี่ยวกับการทำงานของไฟล์ที่น่าสงสัยที่พบในคอมพิวเตอร์ของคุณ

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

หมายเหตุและข้อมูลเพิ่มเติม – คุณสามารถเพิ่มข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยในการประมวลผลไฟล์ที่น่าสงสัยได้

> ℹ พารามิเตอร์แรก – จำเป็นต้องมี **สัญญาณและอาการที่พบของการติดไวรัสจากมัลแวร์** แต่การให้ข้อมูลเพิ่มเติมจะช่วยห้องปฏิบัติการของเราในการระบุกระบวนการและประมวลผลตัวอย่างได้เป็นอย่างมาก

เลือกตัวอย่างเพื่อวิเคราะห์-เว็บไซต์ที่น่าสงสัย

โปรดเลือกตัวเลือกใดตัวเลือกหนึ่งต่อไปนี้จากเมนูแบบเลื่อนลง **เกิดอะไรขึ้นกับไซต์นี้**:

- **ที่ติดไวรัส** – เว็บไซต์ที่มีไวรัสหรือมัลแวร์อื่นๆ ที่แจกจ่ายโดยวิธีต่างๆ
- **การฟิชชิ่ง** มักใช้เพื่อเข้าถึงข้อมูลที่ละเอียดอ่อน เช่น หมายเลขบัญชีธนาคาร, PIN และอื่นๆ อ่านเพิ่มเติมเกี่ยวกับการโจมตีประเภทนี้ได้ใน ประมวลศัพท์
- **การสแกม** เป็นเว็บไซต์ที่หลอกลวงหรือเว็บไซต์ฉ้อโกง ซึ่งมีจุดประสงค์หลักเพื่อการแสวงหากำไรอย่างรวดเร็ว
- เลือก **อื่นๆ** หากตัวเลือกข้างต้นไม่สื่อถึงไซต์ที่คุณจะส่ง

หมายเหตุและข้อมูลเพิ่มเติม คุณสามารถพิมพ์ข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยวิเคราะห์เว็บไซต์ที่น่าสงสัยได้

เลือกตัวอย่างเพื่อวิเคราะห์-การตรวจพบไฟล์ที่ผิดพลาด

เราขอให้คุณส่งไฟล์ที่ตรวจพบว่าติดไวรัส แต่จริงๆ ไม่ได้ติดไวรัส เพื่อปรับปรุงประสิทธิภาพกลไกการป้องกันไวรัสและสปายแวร์ของเราและช่วยให้ผู้อื่นได้รับการป้องกัน การตรวจพบที่ผิดพลาด (FP) อาจเกิดขึ้นเมื่อรูปแบบของไฟล์ตรงกับรูปแบบเดียวกับที่อยู่ในกลไกตรวจหา

ชื่อและเวอร์ชันของแอพพลิเคชัน – ชื่อและเวอร์ชันของโปรแกรม (ตัวอย่างเช่น ตัวเลข ชื่อแทน หรือชื่อรหัส)

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

วัตถุประสงค์ของแอพพลิเคชัน – คำอธิบายทั่วไปของแอพพลิเคชัน ประเภทของแอพพลิเคชัน (เช่น เบราว์เซอร์ เครื่องเล่นสื่อ เป็นต้น) และฟังก์ชันการทำงาน

หมายเหตุและข้อมูลเพิ่มเติม – คุณสามารถเพิ่มข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยในการประมวลผลไฟล์ที่น่าสงสัยได้

> ℹ ต้องใช้สามพารามิเตอร์แรกเพื่อระบุแอพพลิเคชันที่ถูกต้องและแยกแอพพลิเคชันเหล่านั้นออกจากรหัสที่เป็นอันตราย การให้ข้อมูลเพิ่มเติมจะเป็นการช่วยห้องปฏิบัติการของเราในการระบุและประมวลผลตัวอย่าง

เลือกตัวอย่างเพื่อวิเคราะห์-การตรวจสอบเว็บไซต์ที่ผิดพลาด

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

หมายเหตุและข้อมูลเพิ่มเติม – คุณสามารถเพิ่มข้อมูลเพิ่มเติมหรือคำอธิบายที่จะช่วยในการประมวลผลเว็บไซต์ที่น่าสงสัยได้

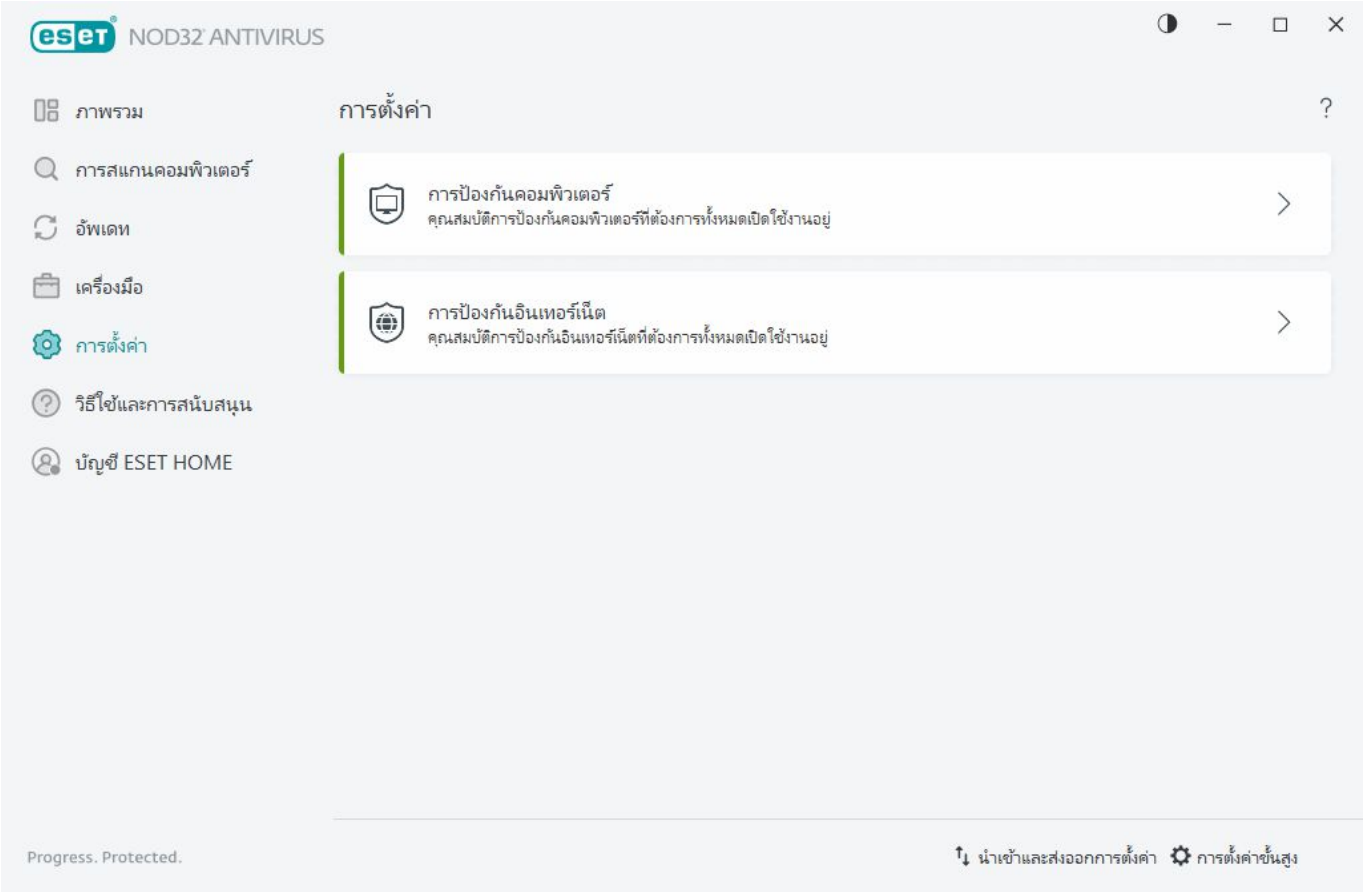
เลือกตัวอย่างเพื่อวิเคราะห์-อื่นๆ

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

เหตุผลสำหรับการส่งไฟล์ – โปรดป้อนคำอธิบายโดยละเอียดและเหตุผลในการส่งไฟล์

การตั้งค่า

คุณสามารถค้นหากลุ่มของฟีเจอร์การป้องกันที่พร้อมใช้งาน ใน หน้าต่างโปรแกรมหลัก > **การตั้งค่า**



เมนู **การตั้งค่า** แบ่งออกเป็นส่วนต่างๆ ดังต่อไปนี้:

การป้องกันคอมพิวเตอร์

การป้องกันอินเทอร์เน็ต

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

การป้องกันคอมพิวเตอร์

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

- การป้องกันระบบไฟล์แบบเรียลไทม์ – โปรแกรมจะสแกนไฟล์ทั้งหมดเพื่อหารหัสที่เป็นอันตรายเมื่อเปิด สร้าง หรือเรียกใช้ไฟล์
- การควบคุมอุปกรณ์ - โมดูลนี้อนุญาตให้คุณสแกน ปิดกั้น หรือปรับตัวกรอง/การอนุญาตเพิ่มเติมแล้วเลือกวิธี

ที่ผู้ใช้จะสามารถเข้าถึงและใช้อุปกรณ์ที่ให้ (ซีดี/ดีวีดี/USB...) ได้

• HIPS - ระบบHIPS จะตรวจสอบเหตุการณ์ภายในระบบปฏิบัติการและตอบสนองเหตุการณ์ตามชุดของกฎที่กำหนดเอง

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

หากต้องการหยุดชั่วคราวหรือปิดใช้งานโมดูลการป้องกันแต่ละโมดูล ให้คลิกไอคอนปุ่มสลับ

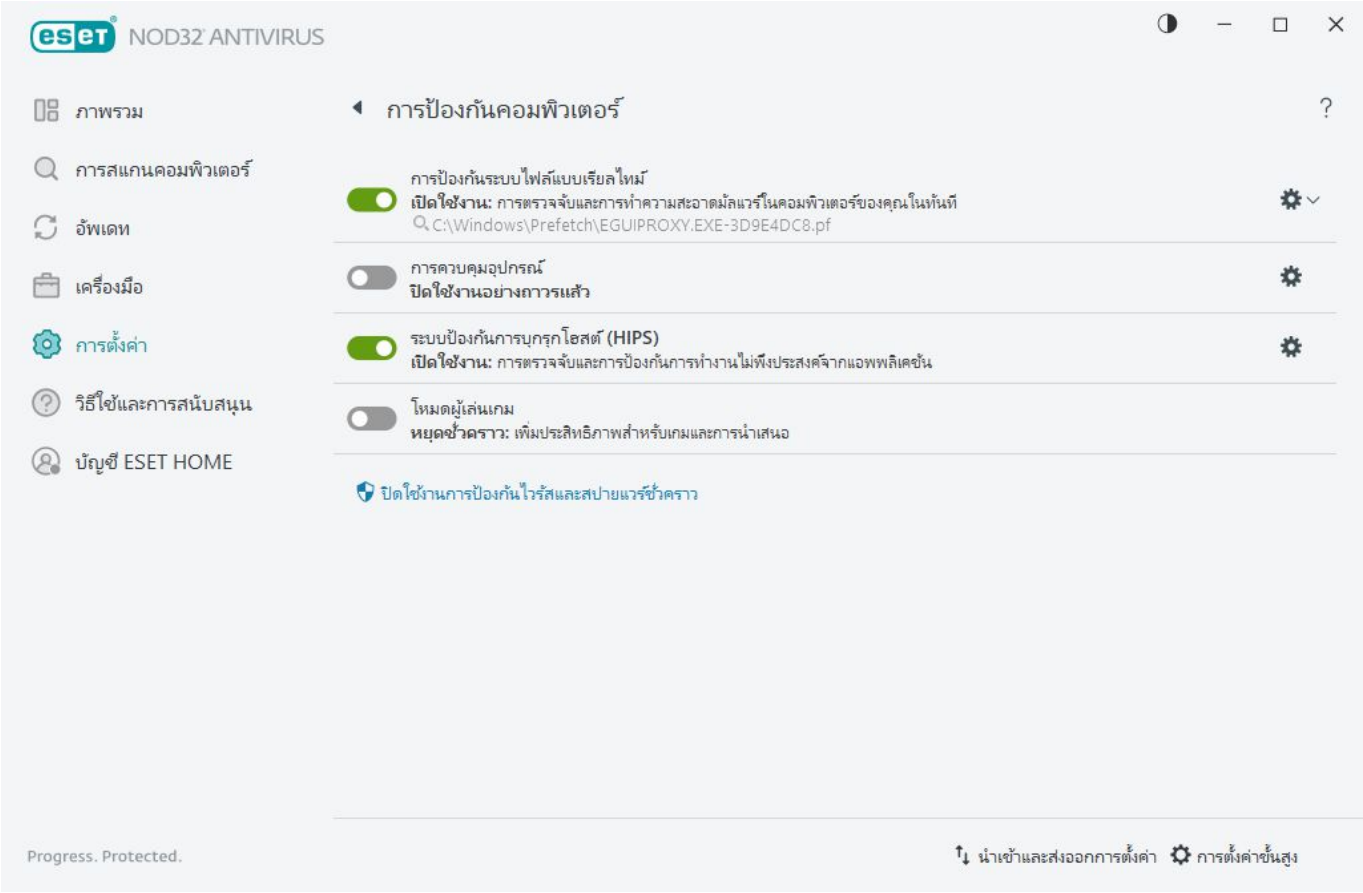
⚠ การปิดโมดูลการป้องกันอาจลดระดับการป้องกันของคอมพิวเตอร์ของคุณ

คลิกไอคอนฟันเฟือง ⚙ ที่อยู่ถัดจากโมดูลการป้องกันเพื่อเข้าถึงการตั้งค่าขั้นสูงสำหรับโมดูลนั้น

สำหรับการ **ป้องกันระบบไฟล์แบบเรียลไทม์** ให้คลิกไอคอนฟันเฟือง ⚙ และเลือกจากตัวเลือกต่อไปนี้:

• **กำหนดค่า** – เปิดการตั้งค่าขั้นสูงสำหรับการป้องกันระบบไฟล์แบบเรียลไทม์

• **แก้ไขการยกเว้น** – เปิด หน้าต่างการตั้งค่าการยกเว้น เพื่อให้คุณสามารถยกเว้นไฟล์และโฟลเดอร์จากการสแกนได้



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

ตรวจพบการแฝงตัว

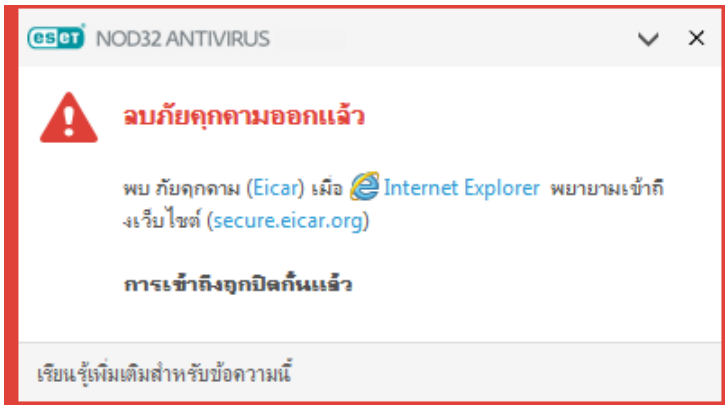
การบุกรุกสามารถเข้าสู่ระบบได้จากจุดเข้าใช้ต่างๆ เช่น หน้าเว็บ โฟลเดอร์ที่ใช้ร่วมกัน ผ่านอีเมล หรือจากอุปกรณ์ที่ถอดเข้าออกได้ (USB, ดิสก์ภายนอก, ซีดี, ดีวีดี เป็นต้น)

พฤติกรรมมาตรฐาน

สำหรับตัวอย่างทั่วไปของวิธีจัดการกับการบุกรุกโดย ESET NOD32 Antivirus ระบบจะตรวจพบการบุกรุกโดยใช้:

- การป้องกันระบบไฟล์แบบเรียลไทม์
- การป้องกันการเข้าถึงเว็บ
- การป้องกันอีเมลไคลเอ็นต์
- การสแกนคอมพิวเตอร์ตามต้องการ

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



การสแกนคอมพิวเตอร์เพื่อค้นหาไฟล์ที่ติดไวรัส

ถ้าคอมพิวเตอร์ของคุณแสดงสัญญาณการติดไวรัสจากมัลแวร์ เช่น ทำงานช้า ค้างบ่อยๆ เป็นต้น เราขอแนะนำให้คุณดำเนินการดังนี้:

1.เปิด ESET NOD32 Antivirus แล้วคลิก**การสแกนคอมพิวเตอร์**

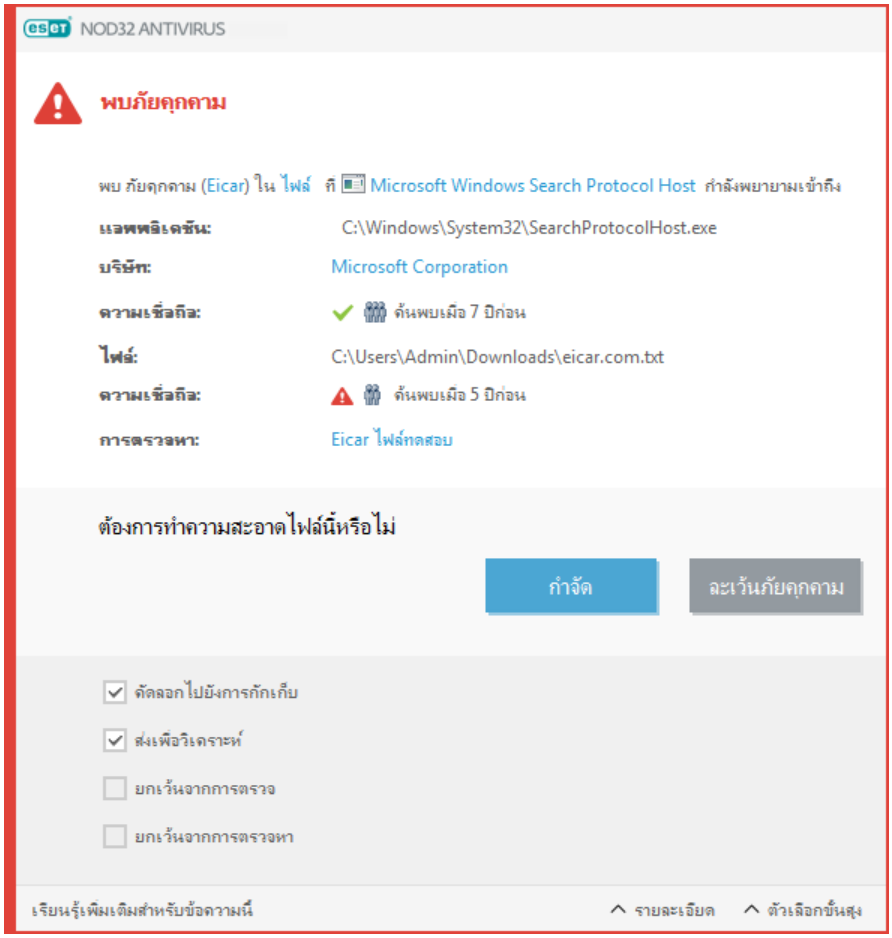
2.คลิก **สแกนคอมพิวเตอร์ของคุณ** (สำหรับข้อมูลเพิ่มเติม ให้ดูที่ การสแกนคอมพิวเตอร์)

3.หลังจากสแกนเสร็จสิ้นแล้ว ให้ตรวจดูบันทึกสำหรับจำนวนไฟล์ที่สแกน ไฟล์ที่ติดไวรัส และไฟล์ที่มีการกำจัดไวรัส

หากคุณต้องการสแกนเฉพาะบางส่วนของดิสก์ ให้คลิก **การสแกนที่กำหนดเอง** และเลือกเป้าหมายที่จะสแกนหาไวรัส

การกำจัดและการลบ

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



ใช้การกำจัดถ้าไฟล์ถูกโจมตีโดยไวรัส ซึ่งทำให้มีการแนบรหัสที่เป็นอันตรายกับไฟล์นั้น ในกรณีนี้ ขั้นแรกให้พยายามกำจัดไฟล์ที่ติดไวรัส เพื่อคืนกลับสู่สภาวะเดิม ถ้าไฟล์มีเฉพาะรหัสที่เป็นอันตราย ไฟล์ดังกล่าวจะถูกลบ

ถ้าไฟล์ที่ติดไวรัสถูก "ล็อค" หรือมีการใช้งานโดยกระบวนการของระบบ โดยปกติโปรแกรมจะลบไฟล์นี้หลังจากที่ใช้งานแล้ว (โดยทั่วไปมักจะลบหลังจากเริ่มต้นระบบใหม่)

การเรียกคืนจากการกักเก็บ

การกักเก็บนั้นสามารถเข้าถึงได้จาก หน้าต่างโปรแกรมหลัก ของ ESET NOD32 Antivirus โดยการคลิก **เครื่องมือ** > **การกักเก็บ**

นอกจากนี้ไฟล์ที่ถูกกักเก็บยังสามารถเรียกคืนไปยังตำแหน่งดั้งเดิมได้อีกด้วย:

- ใช้คุณสมบัติ **เรียกคืน** สำหรับการดำเนินการดังกล่าว ซึ่งสามารถใช้งานได้จากเมนูบริบทโดยคลิกไฟล์ที่ต้องการในการกักเก็บ
- หากไฟล์ถูกทำเครื่องหมายเป็น แอพพลิเคชันที่อาจไม่พึงประสงค์ ตัวเลือก **เรียกคืนและยกเว้นจากการสแกน** จะเปิดใช้งาน ทั้งนี้โปรดดู การยกเว้น

• นอกจากนี้เมนูบริบทยังมีตัวเลือก **เรียกคืนไปที่** ซึ่งช่วยให้คุณสามารถเรียกคืนไฟล์ไปยังตำแหน่งอื่นนอกเหนือจากตำแหน่งที่ถูกลบได้

• ในบางกรณีจะไม่สามารถใช้งานฟังก์ชันการเรียกคืนได้ ตัวอย่างเช่น ไฟล์ที่ตั้งอยู่ในการแชร์เครือข่ายที่อ่านได้อย่างเดียวเท่านั้น

มีภัยคุกคามหลายรายการ

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

การลบไฟล์ในอาร์ไคฟ์

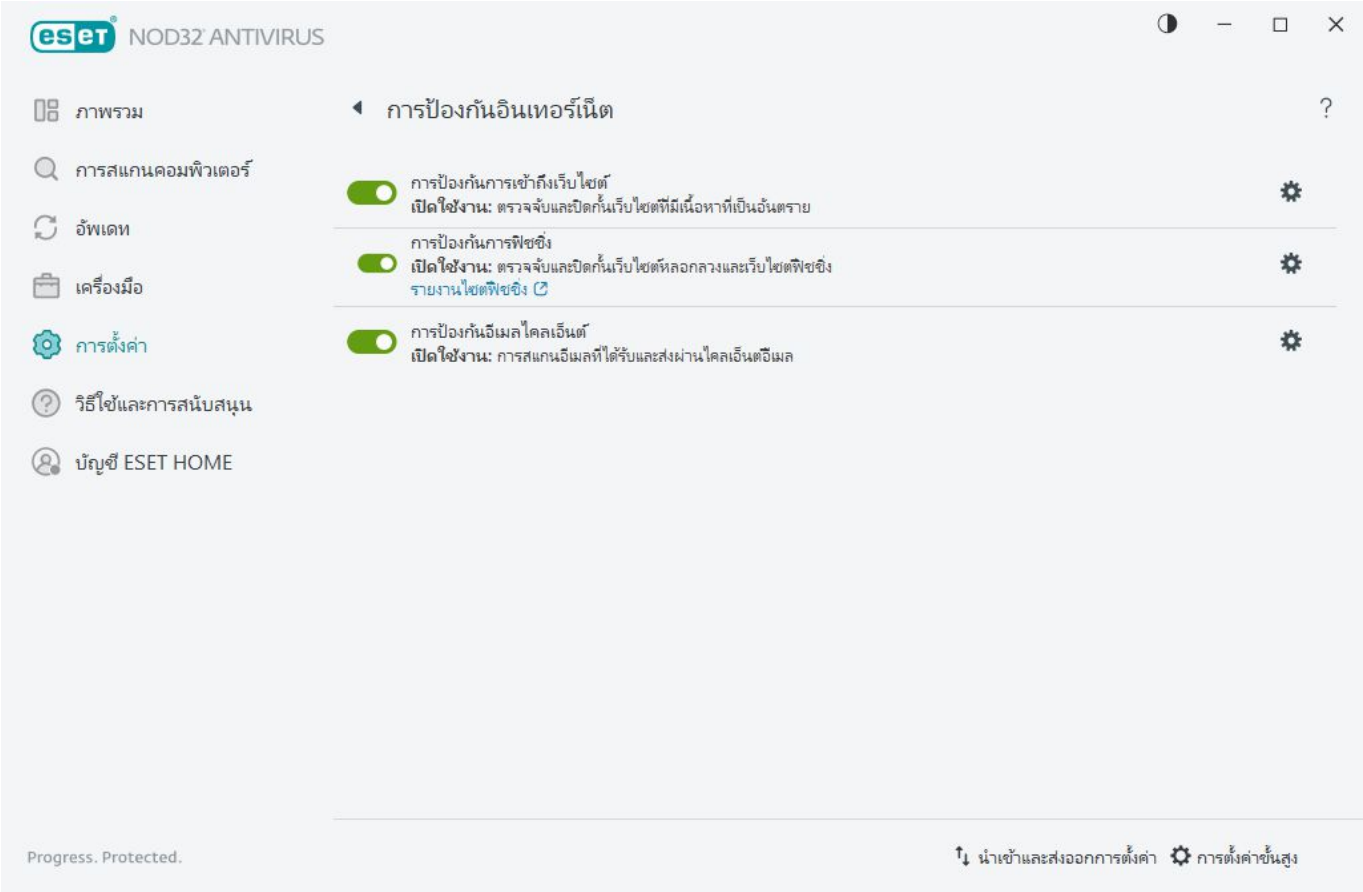
ในโหมดการกำจัดเริ่มต้น ระบบจะลบทั้งอาร์ไคฟ์ต่อเมื่อมีไฟล์ที่ติดไวรัส และไม่มีไฟล์ที่ปลอดไวรัสเลย กล่าวอีกนัยหนึ่งก็คือ โปรแกรมจะไม่ลบอาร์ไคฟ์ ถ้ายังมีไฟล์ที่ไม่เป็นอันตรายรวมอยู่ด้วย โปรดใช้ความระมัดระวังเมื่อสแกนการกำจัดอย่างเข้มงวด เมื่อเปิดใช้งานการกำจัดอย่างเข้มงวด โปรแกรมจะลบอาร์ไคฟ์แม้ว่าจะมีไฟล์ที่ติดไวรัสเพียงไฟล์เดียวก็ตาม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

การป้องกันอินเทอร์เน็ต

การเชื่อมต่ออินเทอร์เน็ตเป็นคุณลักษณะมาตรฐานในคอมพิวเตอร์ส่วนบุคคลส่วนใหญ่ แต่น่าเสียดายที่คุณลักษณะนี้กลายเป็นสื่อหลักสำหรับการถ่ายโอนรหัสที่เป็นอันตราย เปิด หน้าต่างโปรแกรมหลัก > **การตั้งค่า** > **การป้องกันอินเทอร์เน็ต** เพื่อกำหนดค่าฟีเจอร์ใน ESET NOD32 Antivirus ที่เพิ่มการป้องกันอินเทอร์เน็ตของคุณ

หากต้องการหยุดชั่วคราวหรือปิดใช้งานโมดูลการป้องกันแต่ละโมดูล ให้คลิกไอคอนปุ่มสลับ

⚠ การปิดโมดูลการป้องกันอาจลดระดับการป้องกันของคอมพิวเตอร์ของคุณ



คลิกไอคอนฟันเฟือง ⚙ ที่อยู่ถัดจากโมดูลการป้องกันเพื่อเข้าถึงการตั้งค่าขั้นสูงสำหรับโมดูลนั้น

การป้องกันการเข้าถึงเว็บไซต์ จะสแกนหามัลแวร์และฟิชชิ่งในการสื่อสาร HTTP/HTTPS แนะนำให้ปิดการป้องกันการเข้าถึงเว็บไซต์ก็ต่อเมื่อต้องการแก้ไขปัญหาเท่านั้น

การป้องกันฟิชชิ่ง อนุญาตให้คุณปิดกั้นหน้าเว็บที่ทราบว่ามีการแจกจ่ายเนื้อหาการฟิชชิ่ง เราขอแนะนำให้คุณเปิดใช้งานการป้องกันฟิชชิ่งทิ้งไว้

รายงานเว็บไซต์ฟิชชิ่ง – รายงานเว็บไซต์ฟิชชิ่ง/ที่เป็นอันตรายไปยัง ESET เพื่อวิเคราะห์

> ℹ ก่อนส่งเว็บไซต์ไปยัง ESET โปรดตรวจสอบว่าเว็บไซต์ตรงตามเกณฑ์อย่างน้อยหนึ่งข้อดังต่อไปนี้:
> • ไม่มีการตรวจพบเว็บไซต์เลย
> • มีการตรวจพบเว็บไซต์ว่าเป็นภัยคุกคามโดยเป็นข้อผิดพลาด ในกรณีนี้ คุณสามารถ รายงานหน้าที่ถูกปิดกั้นอย่างไม่ถูกต้อง

การป้องกันอีเมลไคลเอ็นต์ จะมีการควบคุมการสื่อสารทางอีเมลที่ได้รับผ่านโปรโตคอล POP3(S) และ IMAP(S) เมื่อใช้โปรแกรมปลั๊กอินสำหรับอีเมลไคลเอ็นต์ ESET NOD32 Antivirus มีการควบคุมการสื่อสารทั้งหมดจากอีเมลไคลเอ็นต์

การป้องกันฟิชชิ่ง

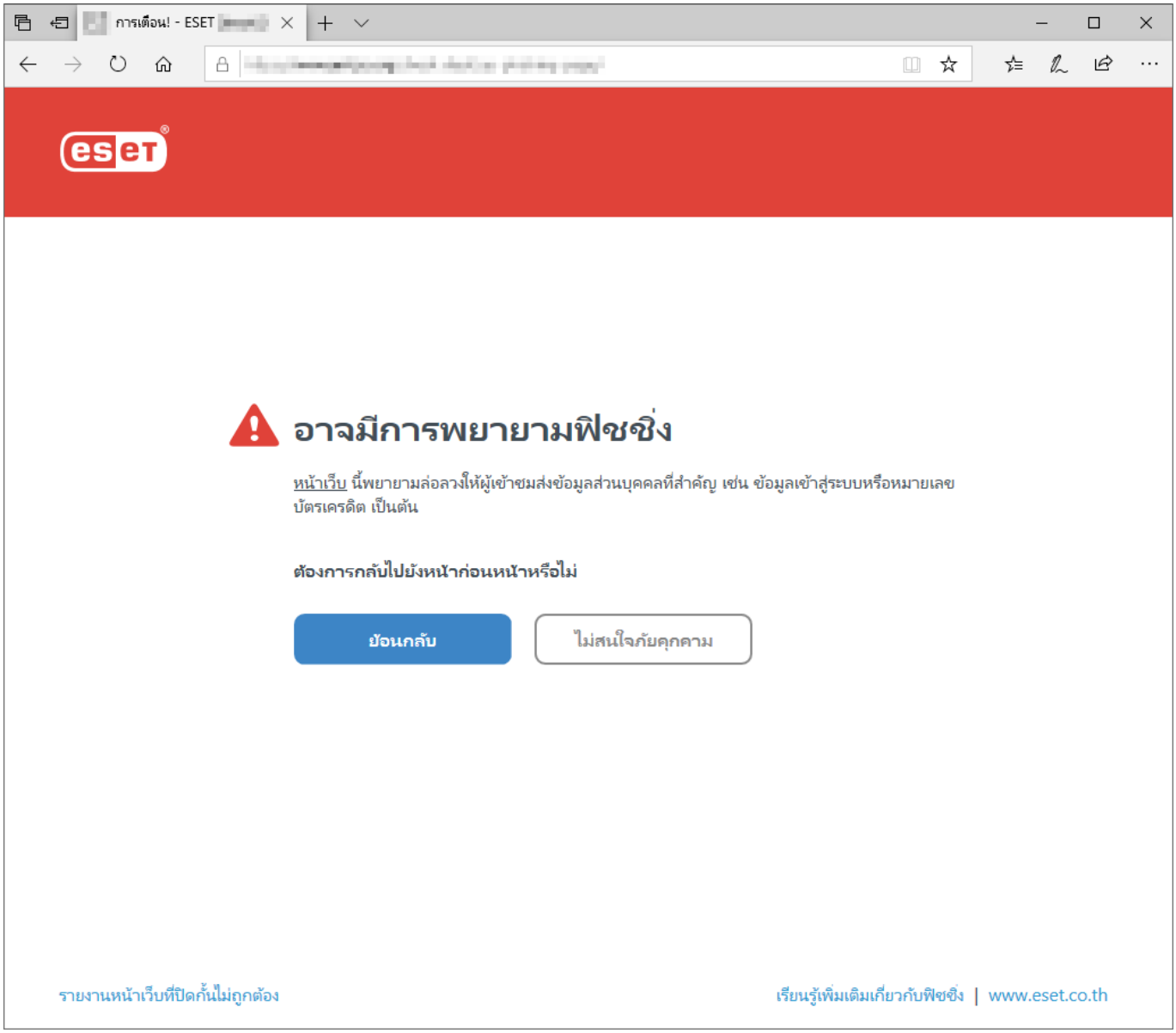
ฟิชชิ่งเป็นกิจกรรมที่ผิดกฎหมายซึ่งใช้กลลวงทางสังคม (การจัดการผู้ใช้เพื่อให้ได้ข้อมูลที่เป็นความลับ) ฟิชชิ่งถูกใช้เพื่อให้ได้รับสิทธิ์การเข้าถึงข้อมูลสำคัญ เช่น หมายเลขบัญชีธนาคาร หมายเลข PIN เป็นต้น ดูข้อมูลเพิ่มเติมได้ใน ประมวลศัพท์ ESET NOD32 Antivirus มีการป้องกันฟิชชิ่ง ซึ่งจะปิดกั้นหน้าเว็บที่เผยแพร่เนื้อหาประเภทดังกล่าว

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

โปรดไปที่ บทความฐานความรู้ ของเราหากต้องการข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันฟิชชิ่งใน ESET NOD32 Antivirus

การเข้าถึงเว็บไซต์ฟิชชิ่ง

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



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

รายงานไซต์ฟิชชิ่ง

ลิงก์ **หน้ารายงานที่ถูกบล็อกไม่ถูกต้อง** ช่วยให้คุณรายงานเว็บไซต์ที่ตรวจพบอย่างไม่ถูกต้องว่าเป็นภัยคุกคามได้

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

นำเข้าและส่งออกการตั้งค่า

คุณสามารถนำเข้าหรือส่งออกไฟล์การกำหนดค่า .xml ของ ESET NOD32 Antivirus ที่กำหนดเองของคุณจากเมนู **การตั้งค่า**

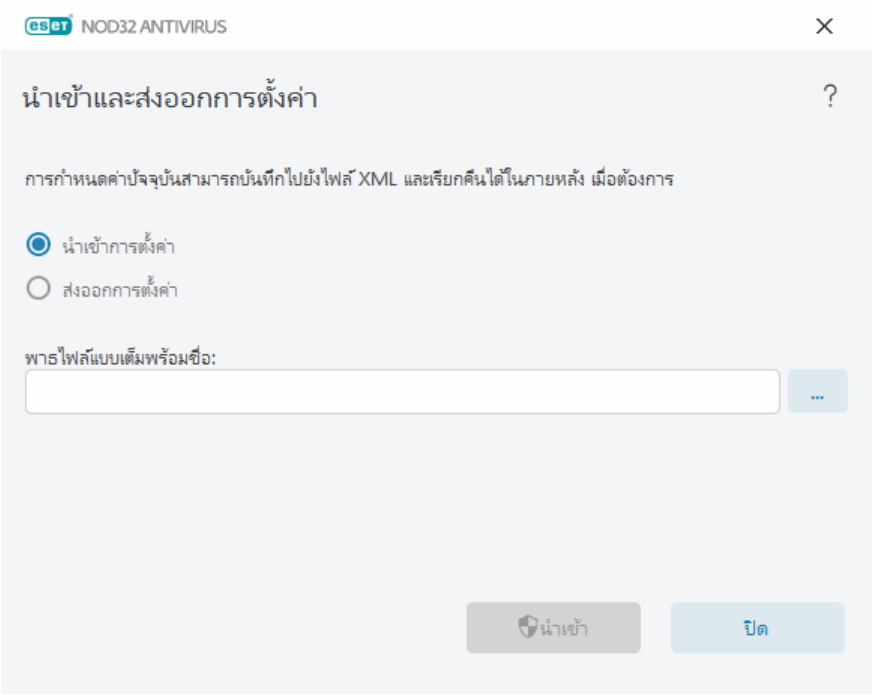
> **คำแนะนำพร้อมภาพประกอบ**
> ดู นำเข้าหรือส่งออกการตั้งค่าการกำหนดค่า ESET โดยใช้ไฟล์ .xml สำหรับคำแนะนำพร้อมภาพประกอบที่แสดงในภาษาอังกฤษและภาษาอื่นๆ

การนำเข้าและการส่งออกไฟล์การกำหนดค่าจะมีประโยชน์ในกรณีที่คุณต้องสำรองการกำหนดค่าปัจจุบันของ ESET NOD32 Antivirus เพื่อใช้งานในภายหลัง ตัวเลือกการตั้งค่าการส่งออกยังใช้งานได้สะดวกเมื่อคุณต้องการใช้การกำหนดค่าที่ต้องการในระบบต่างๆ คุณสามารถนำเข้าไฟล์ .xml ได้อย่างง่ายดายเพื่อส่งการตั้งค่าดังกล่าว

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

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

> คุณอาจพบข้อผิดพลาดในขณะส่งออกการตั้งค่า ถ้าคุณไม่มีสิทธิ์เพียงพอในการเขียนไฟล์ที่ส่งออกไปยังไดเรกทอรีที่ระบุ



วิธีใช้และการสนับสนุน

คลิก **วิธีใช้และการสนับสนุน** ใน หน้าต่างหลักของโปรแกรม เพื่อแสดงข้อมูลสนับสนุนและเครื่องมือแก้ไขปัญหา ซึ่งจะช่วยคุณแก้ปัญหาที่คุณอาจพบ

การสมัครสมาชิก

- การแก้ไขปัญหาการสมัครสมาชิก – คลิกลิงก์นี้เพื่อค้นหาวิธีแก้ไขปัญหาเกี่ยวกับการเปิดใช้งานหรือการเปลี่ยนแปลงการสมัครสมาชิก

- เปลี่ยนการสมัครสมาชิก – คลิกเพื่อเรียกใช้หน้าต่างเปิดใช้งาน แล้วเปิดใช้งานผลิตภัณฑ์ของคุณ หากอุปกรณ์ของคุณ เชื่อมต่ออยู่กับ ESET HOME ให้เลือก การสมัครสมาชิก จากบัญชี ESET HOME ของคุณหรือเพิ่มรายการใหม่

ผลิตภัณฑ์ที่ติดตั้ง

- มีอะไรใหม่–โปรดคลิกรายการนี้เพื่อเปิดหน้าต่างเกี่ยวกับคุณสมบัติใหม่ที่ได้รับการปรับปรุง

- เกี่ยวกับESET NOD32 Antivirus – แสดงข้อมูลเกี่ยวกับสำเนา ESET NOD32 Antivirus ของคุณ

- การแก้ไขปัญหาผลิตภัณฑ์ – คลิกลิงก์นี้เพื่อค้นหาวิธีแก้ไขสำหรับปัญหาที่พบบ่อยที่สุด

- **เปลี่ยนผลิตภัณฑ์** – คลิกเพื่อดูว่าสามารถเปลี่ยน ESET NOD32 Antivirus เป็น ผลิตภัณฑ์รุ่นอื่น ที่มี การสมัครสมาชิก ในปัจจุบันได้หรือไม่

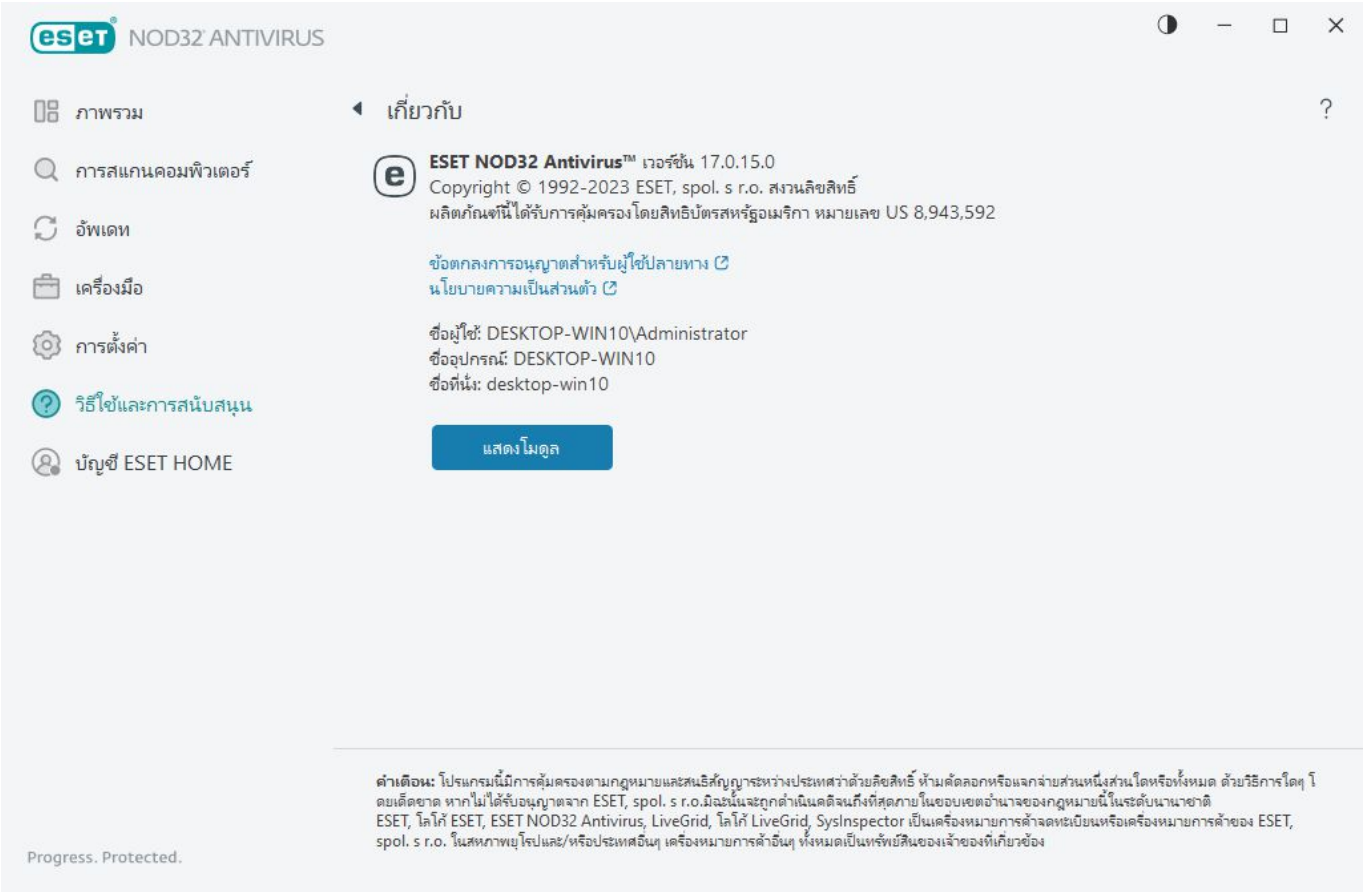
หน้าวิธีใช้ – คลิกลิงค์นี้เพื่อเริ่มต้นหน้าวิธีใช้ ESET NOD32 Antivirus

ฝ่ายสนับสนุนด้านเทคนิค

ฐานความรู้ – ฐานความรู้ของ ESET มีคำตอบสำหรับคำถามที่พบบ่อยที่สุด รวมถึงทางแก้ไขที่แนะนำสำหรับปัญหาต่างๆ ผู้เชี่ยวชาญด้านเทคนิคของ ESET จะอัพเดทข้อมูลนี้เป็นประจำ เพื่อให้ฐานความรู้เป็นเครื่องมือที่มีประสิทธิภาพสูงสุดสำหรับการแก้ไขปัญหาประเภทต่างๆ

เกี่ยวกับ ESET NOD32 Antivirus

หน้าต่างนี้จะแสดงรายละเอียดเกี่ยวกับ ESET NOD32 Antivirus เวอร์ชันที่ติดตั้งและคอมพิวเตอร์ของคุณ



คลิก **แสดงโมดูล** เพื่อดูข้อมูลเกี่ยวกับรายชื่อโมดูลโปรแกรมที่โหลด

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

ข่าวสารของ ESET

ในหน้าต่างนี้ ESET NOD32 Antivirus จะแจ้งให้คุณทราบเกี่ยวกับข่าวของ ESET เป็นประจำ

การส่งข้อความในผลิตภัณฑ์ไม่ได้ออกแบบมาเพื่อแจ้งข่าวสารและการติดต่อสื่อสารอื่นๆ ของ ESET ให้ผู้ใช้ทราบ การส่งข้อความการตลาดจะต้องได้รับการยินยอมจากผู้ใช้ ดังนั้นการส่งข้อความการตลาดจะไม่ถูกส่งให้ผู้ใช้โดยค่าเริ่ม

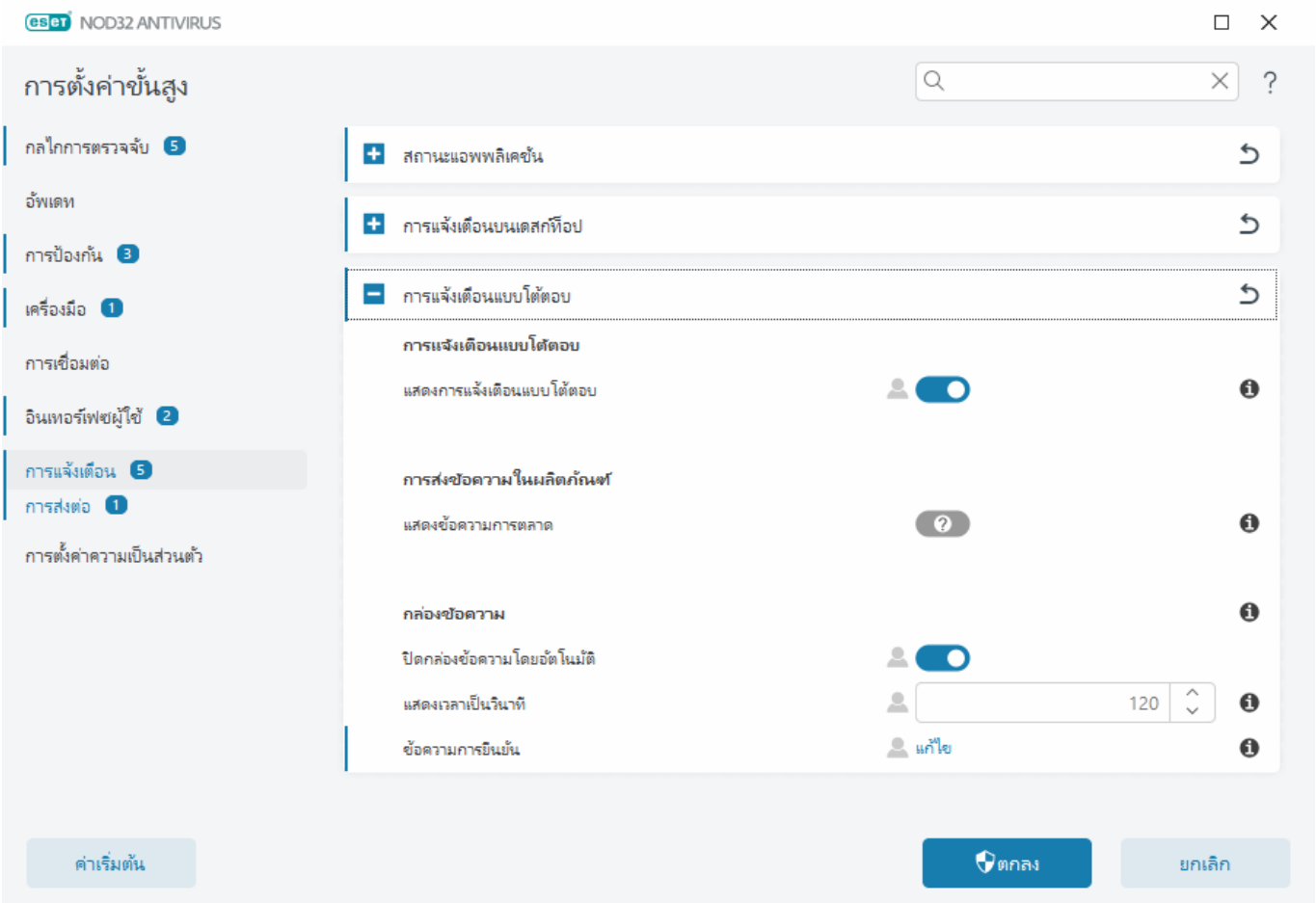
ต้น (แสดงในเครื่องหมายคำถาม) โดยการเปิดใช้งานตัวเลือกนี้ คุณยอมที่จะรับข้อความการตลาดของ ESET หากคุณไม่สนใจที่จะรับข้อมูลทางการตลาดของ ESET ให้ปิดใช้งานตัวเลือก **แสดงข้อความด้านการตลาด**

หากต้องการเปิดหรือปิดใช้งานการรับข้อความด้านการตลาดผ่านหน้าต่างแจ้งเตือน ให้ทำตามคำแนะนำด้านล่าง

1. เปิด การตั้งค่าขั้นสูง

2. คลิก **การแจ้งเตือน** > **การแจ้งเตือนแบบโต้ตอบ**

3. ปรับเปลี่ยนตัวเลือก **แสดงข้อความด้านการตลาด**



ส่งข้อมูลการกำหนดค่าระบบ

ESET จำเป็นต้องขอข้อมูลเกี่ยวกับการกำหนดค่า ESET NOD32 Antivirus, ข้อมูลระบบโดยละเอียดและกระบวนการที่ทำงานอยู่ (ไฟล์บันทึก ESET SysInspector) และข้อมูลรีจิสตรีเพื่อการช่วยเหลืออย่างรวดเร็วและถูกต้องที่สุดเท่าที่จะทำได้ ESET จะใช้ข้อมูลนี้เพื่อให้ความช่วยเหลือด้านเทคนิคแก่ลูกค้าเพียงอย่างเดียว

หลังจากที่คุณส่ง แบบฟอร์มเว็บ ข้อมูลการกำหนดค่าระบบของคุณจะถูกส่งให้กับ ESET เลือก **ส่งข้อมูลนี้เสมอ** หาก

คุณต้องการจำการดำเนินการนี้สำหรับกระบวนการนี้ เมื่อส่ง แบบฟอร์มเว็บ โดยไม่ได้ส่งข้อมูลใดๆ ให้คลิก **ไม่ต้องส่งข้อมูล** และดำเนินการต่อ

คุณสามารถกำหนดค่าการส่งข้อมูลการกำหนดค่าระบบได้ ใน การตั้งค่าขั้นสูง > **เครื่องมือ** > **การวินิจฉัย** ฝ่ายสนับสนุนด้านเทคนิค

> หากคุณตัดสินใจที่จะส่งข้อมูลการกำหนดค่าระบบ คุณจำเป็นต้องกรอกและส่งแบบฟอร์มเว็บ มิฉะนั้นตั๋วของคุณจะไม่ถูกสร้างและข้อมูลการกำหนดค่าระบบของคุณจะหายไป หากไม่สามารถส่งข้อมูลการกำหนดค่าระบบได้ ให้กรอกแบบฟอร์มเว็บและรอคำแนะนำจากฝ่ายสนับสนุนด้านเทคนิค

ฝ่ายสนับสนุนด้านเทคนิค

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

ติดต่อฝ่ายสนับสนุนด้านเทคนิค

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

รับข้อมูลสำหรับฝ่ายสนับสนุนด้านเทคนิค

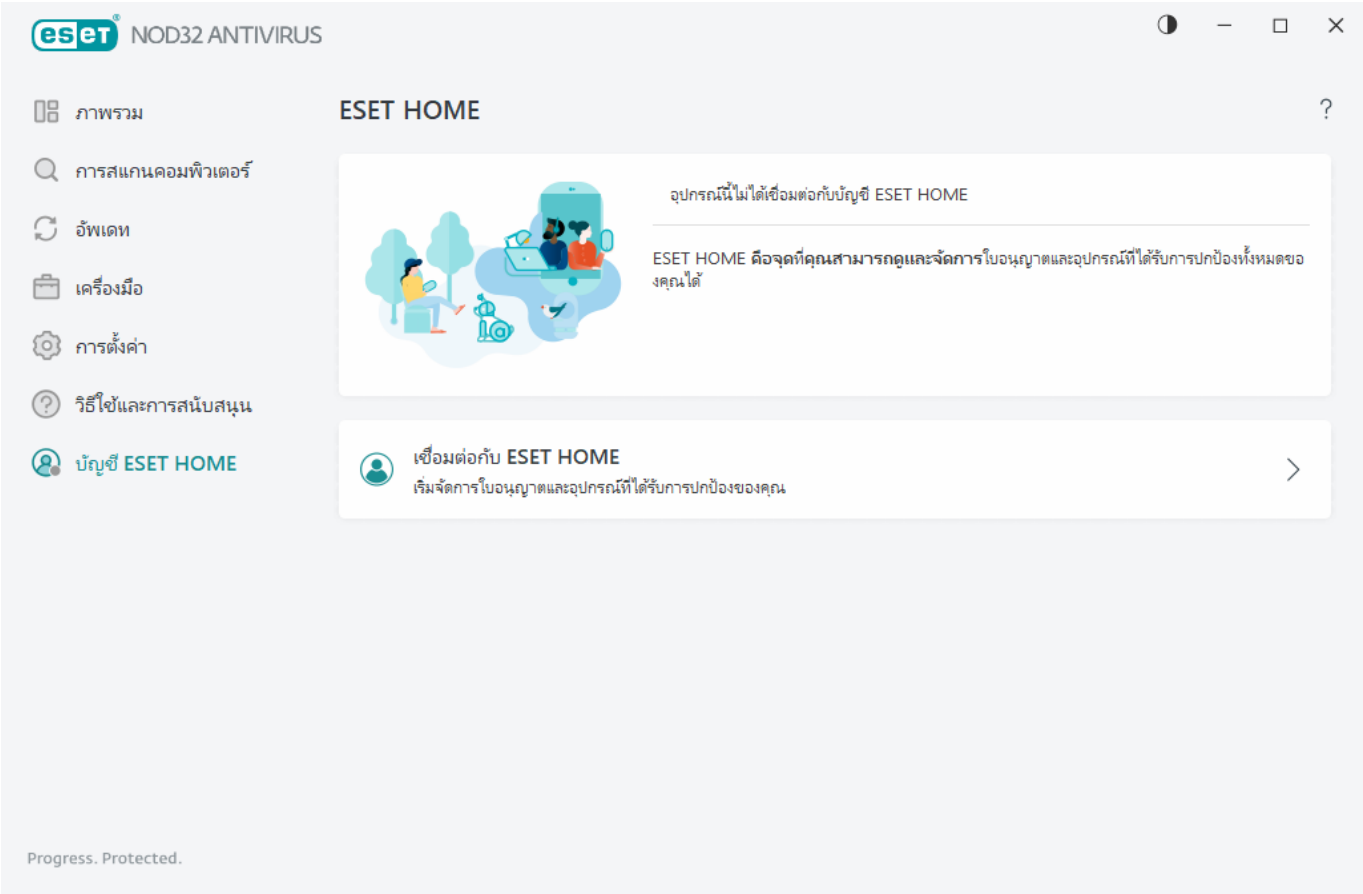
รายละเอียดสำหรับการสนับสนุนด้านเทคนิค – เมื่อได้รับแจ้ง คุณสามารถคัดลอกและส่งข้อมูลไปที่ฝ่ายสนับสนุนด้านเทคนิคของ ESET (เช่น รายละเอียดการสมัครสมาชิก ชื่อผลิตภัณฑ์ เวอร์ชั่นผลิตภัณฑ์ ระบบปฏิบัติการ และข้อมูลคอมพิวเตอร์) ได้

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

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

บัญชี ESET HOME

คุณสามารถตรวจสอบสถานะการเชื่อมต่อบัญชี ESET HOME ใน หน้าต่างโปรแกรมหลัก > **บัญชี ESET HOME**



อุปกรณ์นี้ไม่ได้เชื่อมต่อกับบัญชี ESET HOME

คลิก เชื่อมต่อกับ ESET HOME เพื่อเชื่อมต่ออุปกรณ์ของคุณกับ ESET HOME รวมทั้งจัดการการสมัครสมาชิกและอุปกรณ์ที่มีการป้องกัน คุณสามารถต่ออายุ อัพเกรด หรือขยายเวลาใช้งานการสมัครสมาชิกและดูรายละเอียดที่สำคัญได้ ในพอร์ทัลการจัดการหรือแอพมือถือของ ESET HOME คุณสามารถเพิ่มการสมัครสมาชิกอื่น ดาวน์โหลดผลิตภัณฑ์ไปยังอุปกรณ์ของคุณ ตรวจสอบสถานะความปลอดภัยของผลิตภัณฑ์ หรือแชร์การสมัครสมาชิกผ่านอีเมลได้ สำหรับข้อมูลเพิ่มเติม โปรดไปที่ ความช่วยเหลือออนไลน์ของ ESET HOME

อุปกรณ์นี้เชื่อมต่อกับบัญชี ESET HOME

คุณสามารถจัดการความปลอดภัยของอุปกรณ์ของคุณจากระยะไกลโดยใช้ พอร์ทัล ESET HOME หรือแอปมือถือได้ คลิก **App Store** หรือ **Google Play** เพื่อแสดงรหัส QR ที่คุณสามารถสแกนด้วยโทรศัพท์มือถือของคุณเพื่อดาวน์โหลดแอปมือถือ ESET HOME จาก App Store หรือ Google Play ได้

บัญชี ESET HOME ชื่อบัญชี ESET HOME ของคุณ

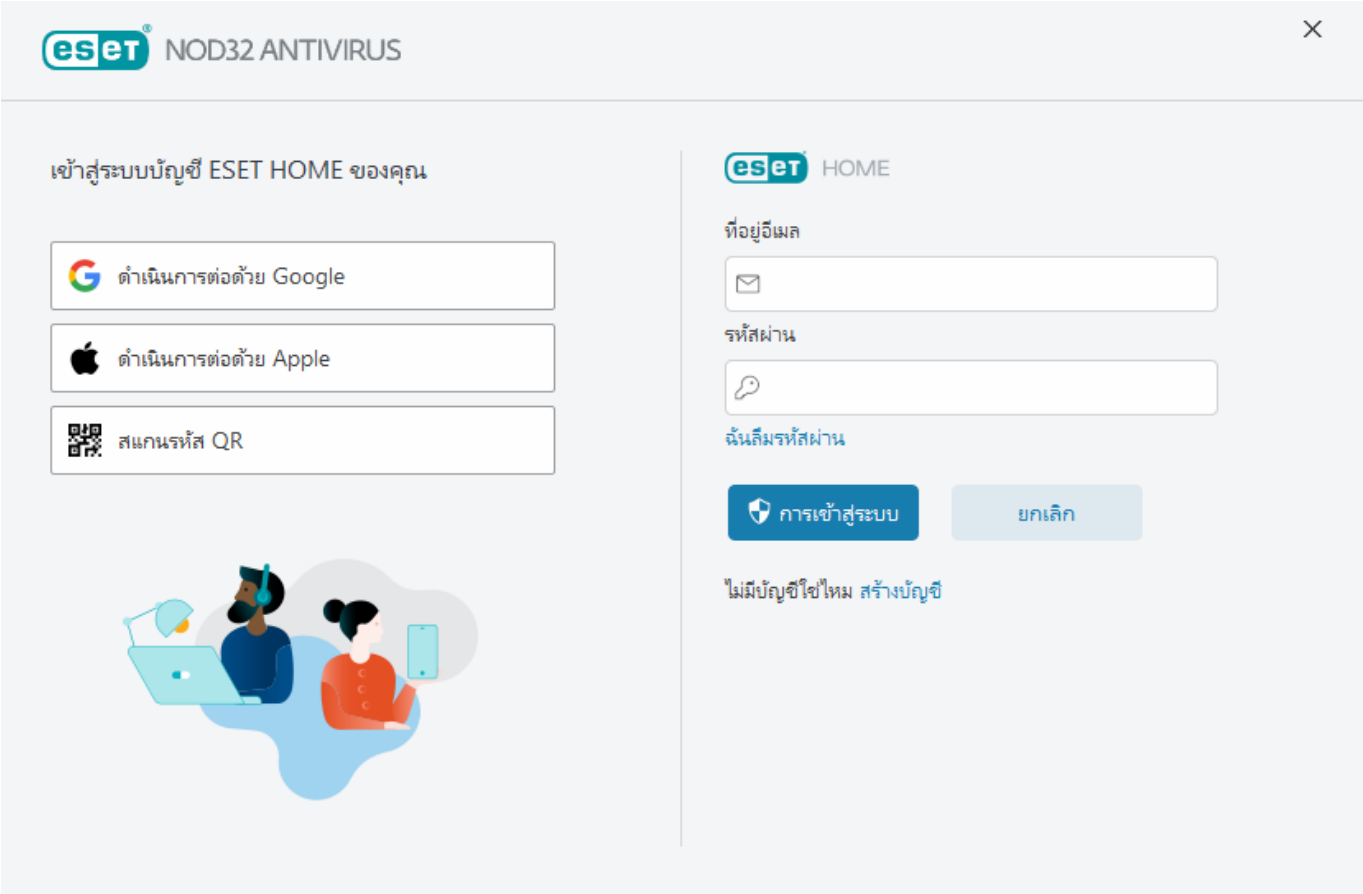
ชื่ออุปกรณ์ ชื่ออุปกรณ์นี้ที่แสดงอยู่ในบัญชี ESET HOME

เปิด ESET HOME – เปิดพอร์ทัลการจัดการ ESET HOME

หากต้องการยกเลิกการเชื่อมต่ออุปกรณ์จากบัญชี ESET HOME ของคุณ ให้คลิก **ยกเลิกการเชื่อมต่ออุปกรณ์จาก ESET HOME** > **ยกเลิกการเชื่อมต่อ** การสมัครสมาชิกที่ใช้สำหรับการเปิดใช้งานจะยังคงใช้งานอยู่ และอุปกรณ์ของคุณจะได้รับการป้องกัน

เชื่อมต่อกับ ESET HOME

เชื่อมต่ออุปกรณ์ของคุณกับ ESET HOME เพื่อดูและจัดการการสมัครสมาชิกและอุปกรณ์ทั้งหมดของ ESET ที่เปิดใช้งานอยู่ คุณสามารถต่ออายุ อัพเกรด หรือขยายเวลาใช้งานการสมัครสมาชิกออกไปและดูรายละเอียดที่สำคัญของการสมัครสมาชิกได้ ในพอร์ทัลการจัดการหรือแอพมือถือของ ESET HOME คุณสามารถเพิ่มการสมัครสมาชิกอื่น ดาวน์โหลดผลิตภัณฑ์ไปยังอุปกรณ์ ตรวจสอบสถานะความปลอดภัยของผลิตภัณฑ์ หรือแชร์การสมัครสมาชิกผ่านอีเมลได้ สำหรับข้อมูลเพิ่มเติม โปรดไปที่ ความช่วยเหลือออนไลน์ของ ESET HOME



หากต้องการเชื่อมต่ออุปกรณ์ของคุณกับ ESET HOME:

> หากคุณกำลังเชื่อมต่อกับ ESET HOME ในระหว่างการติดตั้งหรือเมื่อเลือก **ใช้บัญชี ESET HOME** เป็นวิธีการเปิดใช้งาน ให้ทำตามคำแนะนำในหัวข้อ ใช้บัญชี ESET HOME
> หากคุณได้ติดตั้งและเปิดใช้งาน ESET NOD32 Antivirus ด้วยการสมัครสมาชิกที่เพิ่มเข้าในบัญชี ESET HOME ของคุณเรียบร้อยแล้ว คุณจะสามารถเชื่อมต่ออุปกรณ์ของคุณเข้ากับ ESET HOME ได้โดยใช้พอร์ทัล ESET HOME โปรดดำเนินการตามคำแนะนำใน คู่มือความช่วยเหลือออนไลน์สำหรับ ESET HOME และ อนุญาตการเชื่อมต่อใน ESET NOD32 Antivirus

1.ใน หน้าต่างโปรแกรมหลัก ให้คลิก **บัญชี ESET HOME** > **เชื่อมต่อกับ ESET HOME** หรือคลิก **เชื่อมต่อกับ ESET HOME** ในการแจ้งเตือน **เชื่อมต่ออุปกรณ์นี้กับบัญชี ESET HOME**

2.ล็อคอินเข้าสู่บัญชี ESET HOME ของคุณ

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

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

4.หลังจากการเชื่อมต่อสำเร็จหน้าต่างรายละเอียดจะปรากฏขึ้น ให้คลิก **เสร็จสิ้น**

ล็อคอินเข้าสู่ ESET HOME

คุณสามารถล็อคอินเข้าสู่บัญชี ESET HOME ของคุณ ได้หลายวิธีดังนี้:

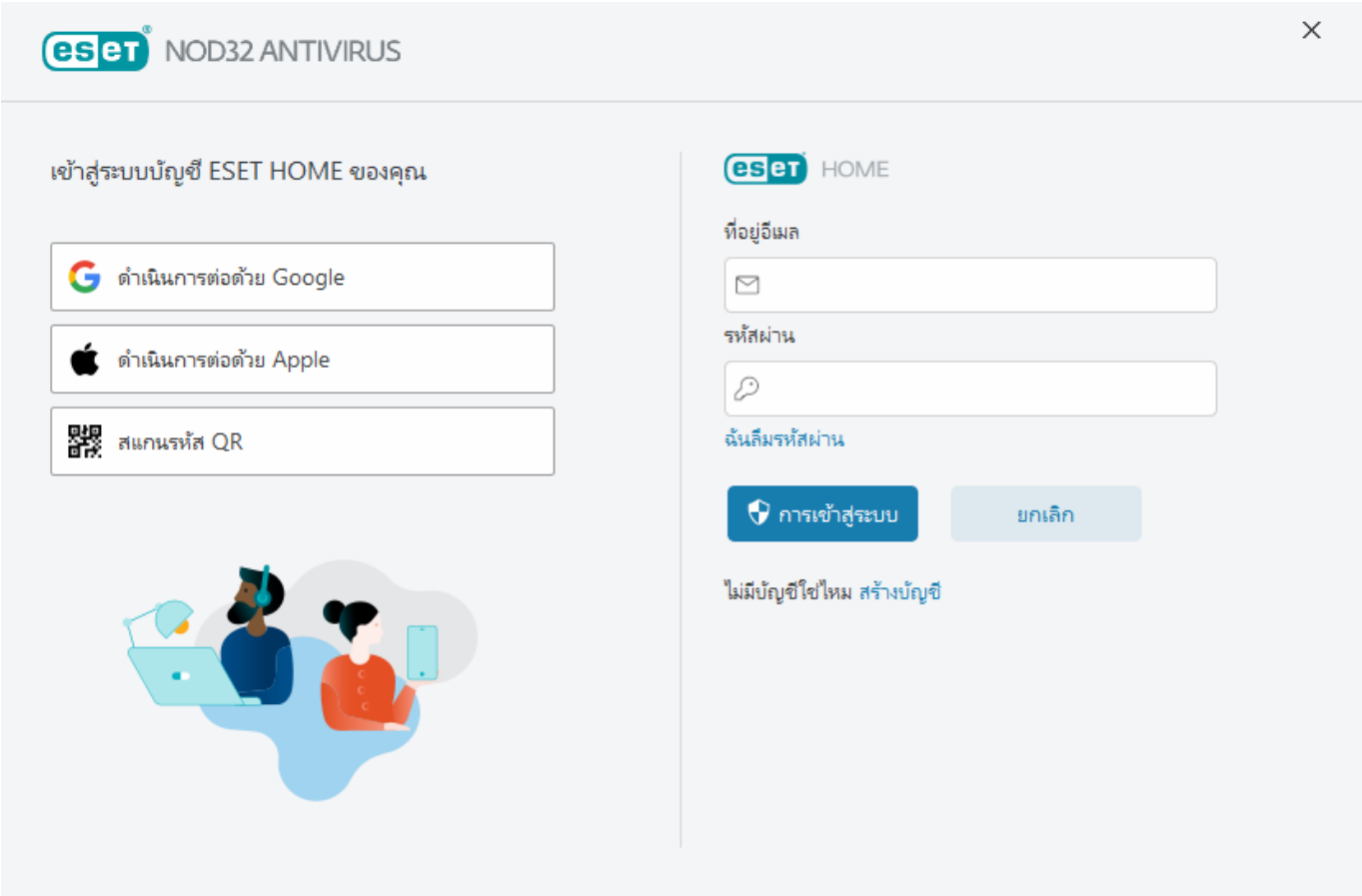
- **ใช้ที่อยู่อีเมล ESET HOME และรหัสผ่านของคุณ** – พิมพ์ **ที่อยู่อีเมล** และ **รหัสผ่าน** ที่คุณใช้สร้างบัญชี ESET HOME แล้วคลิก **ล็อคอิน**

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

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

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

ล็อคอินล้มเหลว - ข้อผิดพลาดทั่วไป



ล็อคอินล้มเหลว - ข้อผิดพลาดทั่วไป

เราไม่พบบัญชีที่ตรงกับที่อยู่อีเมลที่ป้อน

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

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

ชื่อผู้ใช้และรหัสผ่านไม่ตรงกัน

รหัสผ่านที่พิมพ์ไม่ตรงกับที่อยู่อีเมลที่ป้อน คลิก **ย้อนกลับ** พิมพ์รหัสผ่านที่ถูกต้องและตรวจสอบว่าที่อยู่อีเมลที่พิมพ์ถูกต้อง หากคุณยังไม่สามารถล็อคอินได้ ให้คลิก **ย้อนกลับ** > **ฉันลืมรหัสผ่าน** เพื่อรีเซ็ตรหัสผ่านแล้วปฏิบัติตามขั้นตอนบนหน้าจอหรือดู ฉันลืมรหัสผ่าน ESET HOME

ตัวเลือกการเข้าสู่ระบบที่เลือกไม่ตรงกับบัญชีของคุณ

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

รหัสผ่านไม่ถูกต้อง

ข้อผิดพลาดนี้จะเกิดขึ้นเฉพาะเมื่อ ESET NOD32 Antivirus เชื่อมต่ออยู่กับ ESET HOME อยู่แล้วและคุณได้ทำการเปลี่ยนแปลงที่จำเป็นต้องใช้การล็อคอิน (ตัวอย่างเช่น การปิดใช้งาน Anti-Theft) และรหัสผ่านที่คุณป้อนไม่ตรงกับบัญชี คลิก **ย้อนกลับ** แล้วป้อนรหัสผ่านที่ถูกต้อง หากคุณยังไม่สามารถล็อคอินได้ ให้คลิก **ย้อนกลับ** > **ฉันลืมรหัสผ่าน** เพื่อรีเซ็ตรหัสผ่านแล้วปฏิบัติตามขั้นตอนบนหน้าจอหรือดู ฉันลืมรหัสผ่าน ESET HOME

เพิ่มอุปกรณ์ใน ESET HOME

หากคุณได้ติดตั้งและเปิดใช้งาน ESET NOD32 Antivirus ด้วยการสมัครสมาชิกที่เพิ่มเข้าในบัญชี ESET HOME ของคุณเรียบร้อยแล้ว คุณจะสามารถเชื่อมต่ออุปกรณ์ของคุณเข้ากับ ESET HOME ได้โดยใช้พอร์ทัล ESET HOME:

1. ส่งคำขอเชื่อมต่อไปยังอุปกรณ์ของคุณ

2. ESET NOD32 Antivirus จะแสดงหน้าต่างข้อความ **เชื่อมต่ออุปกรณ์นี้เข้ากับบัญชี ESET HOME** พร้อมชื่อบัญชี ESET HOME โปรดคลิก **อนุญาต** เพื่อเชื่อมต่ออุปกรณ์เข้ากับบัญชี ESET HOME ที่กล่าวถึงนั้น

> i หากไม่ได้ดำเนินการ คำขอเชื่อมต่อจะถูกยกเลิกโดยอัตโนมัติหลังจากประมาณ 30 นาที

การตั้งค่าขั้นสูง

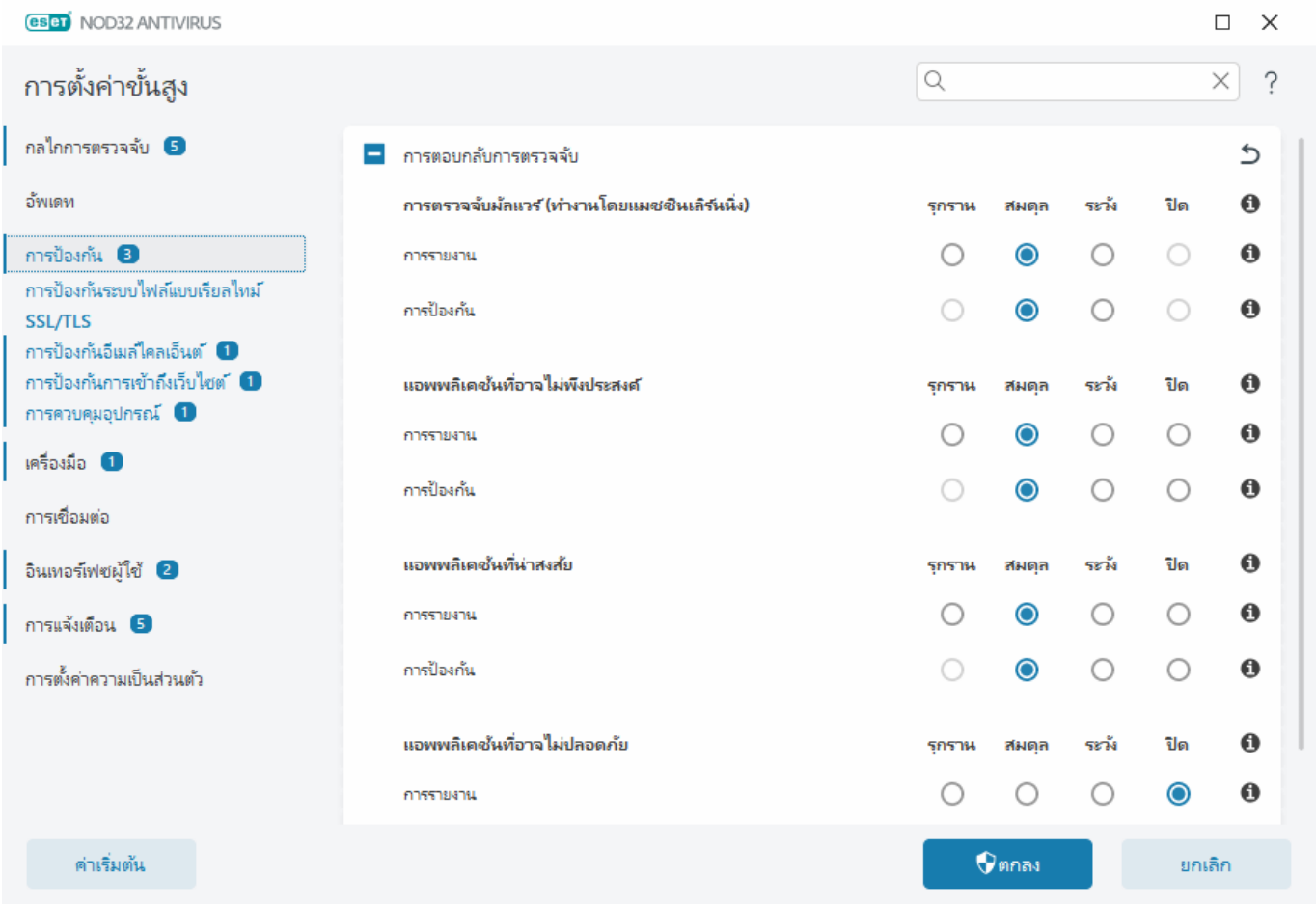
การตั้งค่าขั้นสูงช่วยให้คุณสามารถกำหนดการตั้งค่า ESET NOD32 Antivirus โดยละเอียดเพื่อให้เหมาะกับความต้องการของคุณ

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

ระบบอาจให้คุณกรอกรหัสผ่านเพื่อเปิดการตั้งค่าขั้นสูง โดยขึ้นอยู่กับ การตั้งค่าการเข้าถึง ของคุณ

คุณสามารถกำหนดการตั้งค่าต่อไปนี้ในการตั้งค่าขั้นสูงได้:

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



กลไกการตรวจจับ

การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** ช่วยให้คุณสามารถกำหนดค่าตัวเลือกต่อไปนี้:

- การยกเว้น
- ตัวเลือกขั้นสูง
- เครื่องมือสแกนการรับส่งข้อมูลเครือข่าย

การยกเว้น

การยกเว้น จะช่วยให้คุณสามารถยกเว้นวัตถุจากกลไกการตรวจจับได้ ในการทำให้แน่ใจว่าจะมีการสแกนวัตถุทั้งหมด เราขอแนะนำให้สร้างข้อยกเว้นต่อเมื่อจำเป็นจริง ๆ เท่านั้น สถานการณ์ที่คุณอาจต้องยกเว้นวัตถุ ซึ่งอาจรวมถึงการสแกนรายการฐานข้อมูลขนาดใหญ่ที่จะทำให้คอมพิวเตอร์ทำงานช้าในระหว่างการสแกนหรือซอฟต์แวร์ที่ขัดแย้งกับการสแกน

การยกเว้นการทำงาน ซึ่งจะยกเว้นไฟล์และโฟลเดอร์จากการสแกนได้ การยกเว้นการทำงานมีประโยชน์ในการยกเว้นการสแกนระดับไฟล์ของแอพพลิเคชันเกมหรือเมื่อเกิดพฤติกรรมของระบบที่ไม่ปกติหรือมีการทำงานเพิ่มขึ้น

การยกเว้นการตรวจหา ช่วยให้คุณยกเว้นวัตถุจากการตรวจหาโดยใช้ชื่อ พาธ หรือแฮชของการตรวจหา การยกเว้นการตรวจหาไม่ได้ยกเว้นไฟล์และโฟลเดอร์จากการสแกนเช่นเดียวกับการยกเว้นการทำงาน การยกเว้นการตรวจหาจะยกเว้นวัตถุเมื่อถูกตรวจจับโดยกลไกการตรวจจับและมีกฎที่เหมาะสมแสดงอยู่ในรายการการยกเว้นเท่านั้น

โปรดอย่าสับสนกับประเภทการยกเว้นอื่นๆ:

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

การยกเว้นการทำงาน

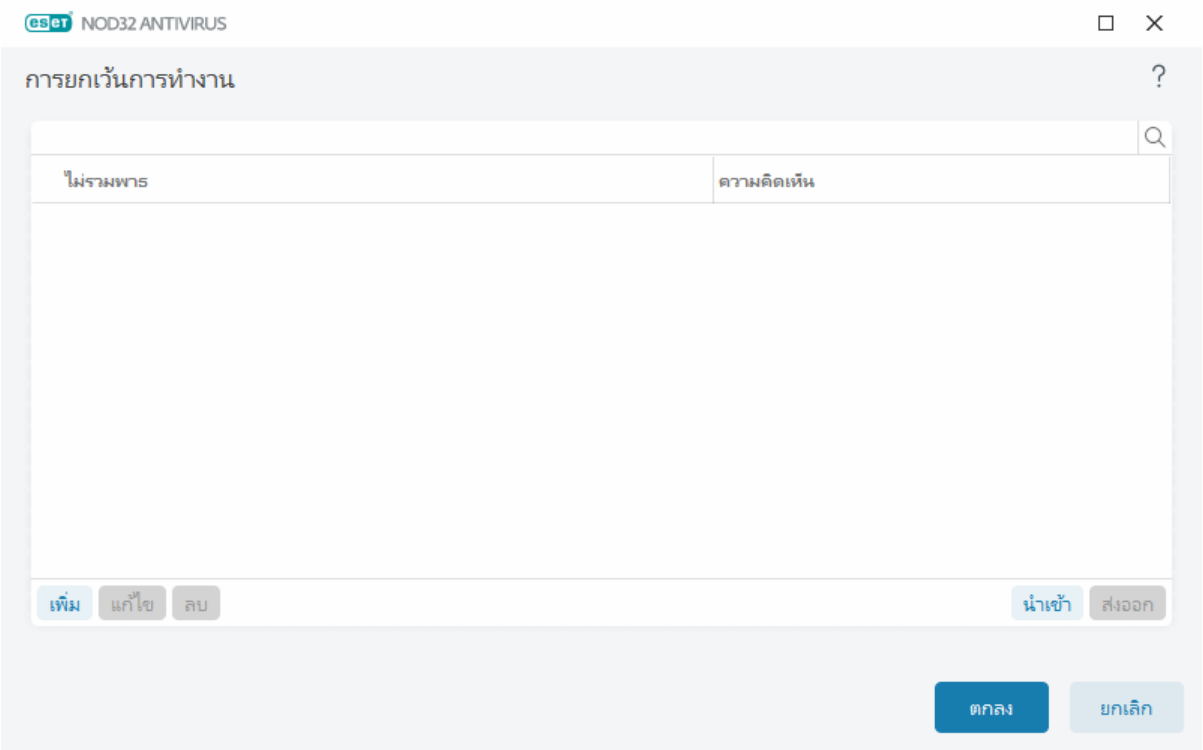
การยกเว้นการทำงาน ช่วยให้คุณยกเว้นไฟล์และโฟลเดอร์จากการสแกน

หากต้องการทำให้แน่ใจว่าจะมีการสแกนวัตถุทั้งหมดเพื่อหาภัยคุกคาม เราขอแนะนำให้สร้างการยกเว้นต่อเมื่อจำเป็นจริงๆ เท่านั้น แต่ยังมีบางสถานการณ์ที่คุณอาจจำเป็นต้องยกเว้นวัตถุ ตัวอย่างเช่น รายการฐานข้อมูลขนาดใหญ่ที่จะทำให้คอมพิวเตอร์ทำงานช้าในระหว่างการสแกนหรือซอฟต์แวร์ที่ขัดแย้งกับการสแกน

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

> ℹ อย่าสับสนกับ การยกเว้นการตรวจหา นามสกุลไฟล์ที่ยกเว้น การยกเว้น HIPS หรือ การยกเว้นกระบวนการ

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



> **โมดูลการป้องกันระบบไฟล์แบบเรียลไทม์** หรือ**โมดูลการสแกนคอมพิวเตอร์** จะไม่สามารถตรวจพบภัยคุกคามภายในไฟล์ได้ถ้าไฟล์ตรงตามเกณฑ์สำหรับการยกเว้นจากการสแกน

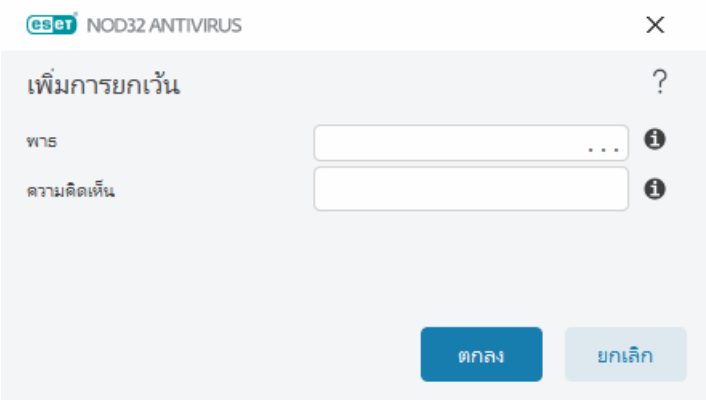
องค์ประกอบการควบคุม

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

เพิ่มหรือแก้ไขการยกเว้นการทำงาน

หน้าต่างข้อความนี้จะยกเว้นพาธแบบเฉพาะ (ไฟล์หรือไดเรกทอรี) สำหรับคอมพิวเตอร์เครื่องนี้

> เลือกพาธหรือป้อนด้วยตัวเอง
> ในการเลือกพาธที่เหมาะสม ให้คลิก **...** ในช่อง **พาธ**
> เมื่อพิมพ์ด้วยตนเอง โปรดดู ตัวอย่างรูปแบบของการยกเว้น เพิ่มเติมที่ด้านล่าง



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

รูปแบบของการยกเว้น

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

ตัวอย่าง:

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

ตัวแปรของระบบในการยกเว้น

คุณสามารถใช้ระบบตัวแปรได้ เช่น %PROGRAMFILES% เพื่อระบุข้อยกเว้นการสแกน

• หากไม่ต้องการรวมโฟลเดอร์ Program Files โดยใช้ระบบตัวแปร ให้ใช้พาธ *%PROGRAMFILES%** (จำไว้ว่าให้เพิ่มเครื่องหมายคั่นหลังและดอกจันที่ด้านหลังสุดของพาธ) เมื่อเพิ่มข้อยกเว้น

• หากต้องการยกเว้นไฟล์และโฟลเดอร์ทั้งหมดในไดเรกทอรีย่อยของ *%PROGRAMFILES%* ให้ใช้พาธ *%PROGRAMFILES%\Excluded_Directory**

รายการขยายที่รองรับตัวแปรของระบบ

ตัวแปรต่อไปนี้สามารถใช้ได้ในพาธของรูปแบบการยกเว้น:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

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

ไม่รองรับสัญลักษณ์แทนในช่วงกลางของพาธ

การใช้สัญลักษณ์แทนในช่วงกลางของพาธ (ตัวอย่างเช่น *C:\Tools*\Data\file.dat*) อาจใช้การได้ แต่ไม่รองรับอย่างเป็นทางการสำหรับการยกเว้นการทำงาน

จะไม่มีข้อกำหนดเพื่อใช้สัญลักษณ์แทนในช่วงกลางของพาธเมื่อใช้ การยกเว้นการตรวจหา

คำสั่งของการยกเว้น

• ไม่มีตัวเลือกเพื่อปรับระดับความสำคัญของการยกเว้นโดยใช้ปุ่มบนสุด/ล่าสุด

• เมื่อใช้กฎที่สามารถใช้ได้ครั้งแรกตรงกับเครื่องมือสแกน กฎที่สามารถใช้ได้ครั้งที่สองจะไม่ได้รับการประเมิน

• ยิ่งมีกฎน้อย ประสิทธิภาพการสแกนยิ่งดีขึ้น

• หลีกเลี่ยงการสร้างกฎที่ทำพร้อมกัน

รูปแบบของการยกเว้นพาธ

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

รูปแบบของการยกเว้น

• หากคุณต้องการยกเว้นไฟล์และโฟลเดอร์ย่อยทั้งหมดในโฟลเดอร์ ให้พิมพ์พาธไปยังโฟลเดอร์ และใช้มาสก์ *

• หากคุณต้องการยกเว้นเฉพาะไฟล์ doc ให้ใช้มาสก์ **.doc*

• หากชื่อของไฟล์ที่เรียกใช้ได้มีอักขระจำนวนหนึ่ง (ที่มีอักขระแตกต่างกัน) และคุณทราบเฉพาะอักขระตัวแรก (เช่น "D") ให้ใช้รูปแบบต่อไปนี้:

D????.exe (เครื่องหมายคำถามจะแทนที่อักขระที่ขาดหายไป/ไม่ทราบ

ตัวอย่าง:

• *C:\Tools** – พาธต้องจบด้วยเครื่องหมายคั่นหลัง (\) และดอกจัน (*) เพื่อระบุว่าเป็นโฟลเดอร์ และเนื้อหาของโฟลเดอร์ (ไฟล์และโฟลเดอร์ย่อย) ทั้งหมดนั้นจะถูกยกเว้น

• *C:\Tools*.** – มีพฤติกรรมเช่นเดียวกับ *C:\Tools**

• *C:\Tools* – โฟลเดอร์ *Tools* จะไม่ถูกยกเว้น จากมุมมองของเครื่องมือสแกน *Tools* สามารถเป็นชื่อไฟล์ได้เช่นเดียวกัน

• *C:\Tools*.dat* – สิ่งนี้จะยกเว้นไฟล์.dat ในโฟลเดอร์ *Tools*

• *C:\Tools\sg.dat* – นี่จะยกเว้นไฟล์ที่เฉพาะเจาะจงที่อยู่ในพาธนี้เท่านั้น

ตัวแปรของระบบในการยกเว้น

คุณสามารถใช้ระบบตัวแปรได้ เช่น %PROGRAMFILES% เพื่อระบุข้อยกเว้นการสแกน

• หากไม่ต้องการรวมโฟลเดอร์ Program Files โดยใช้ระบบตัวแปร ให้ใช้พาธ*%PROGRAMFILES%** (จำไว้ว่าให้เพิ่มเครื่องหมายคั่นหลังและดอกจันที่ด้านหลังสุดของพาธ) เมื่อเพิ่มข้อยกเว้น

• หากต้องการยกเว้นไฟล์และโฟลเดอร์ทั้งหมดในไดเรกทอรีย่อยของ*%PROGRAMFILES%* ให้ใช้พาธ *%PROGRAMFILES%\Excluded_Directory**

รายการขยายที่รองรับตัวแปรของระบบ

ตัวแปรต่อไปนี้สามารถใช้ได้ในพาธของรูปแบบการยกเว้น:

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

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

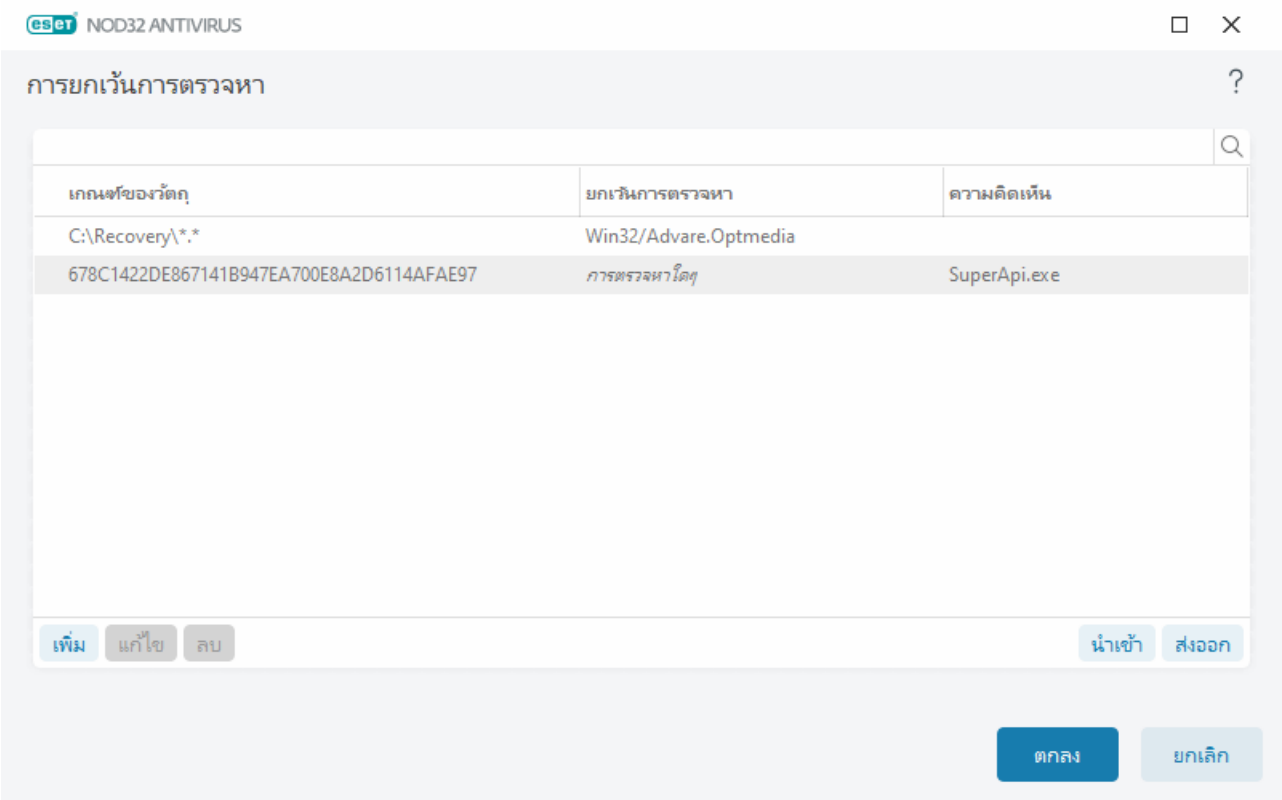
การยกเว้นการตรวจหา

การยกเว้นการตรวจหาช่วยให้คุณยกเว้นวัตถุจากการตรวจจับโดยการกรองชื่อการตรวจหา พาธของวัตถุ หรือแฮช

วิธีการทำงานของการยกเว้นการตรวจหา

การยกเว้นการตรวจหาไม่ได้ยกเว้นไฟล์และโฟลเดอร์จากการสแกนเช่นเดียวกับการยกเว้นการทำงาน การยกเว้นการตรวจหาจะยกเว้นวัตถุเมื่อถูกตรวจจับโดยกลไกการตรวจจับและมีกฎที่เหมาะสมแสดงอยู่ในรายการการยกเว้นเท่านั้น

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



เพื่อให้แน่ใจว่าภัยคุกคามทั้งหมดถูกตรวจหา เราแนะนำให้สร้างการยกเว้นการตรวจหาเมื่อจำเป็นจริงๆ เท่านั้น

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

> ℹ อย่าสับสนกับ การยกเว้นการการทำงาน นามสกุลไฟล์ที่ยกเว้น การยกเว้น HIPS หรือ การยกเว้นกระบวนการ

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

สำหรับ แอพพลิเคชันที่อาจไม่พึงประสงค์ และ แอพพลิเคชันที่อาจไม่ปลอดภัย สามารถสร้างการยกเว้นด้วยชื่อการตรวจจับดังนี้:

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

เกณฑ์การยกเว้นการตรวจหาของวัตถุ

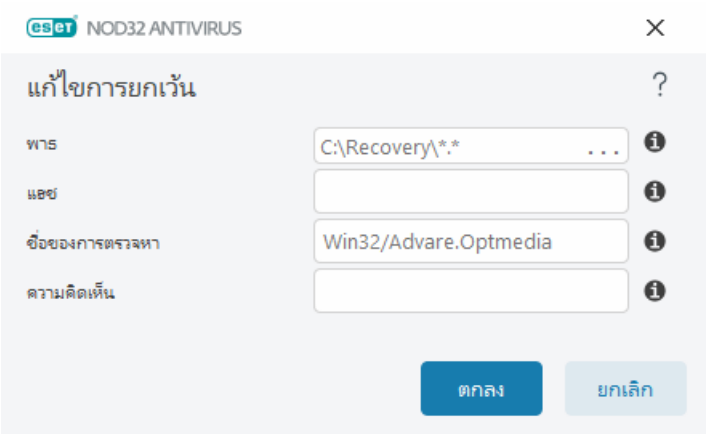
- **พาธ** – จำกัดการยกเว้นการตรวจหาสำหรับพาธเฉพาะ (หรือพาธใดๆ)
- **ชื่อของการตรวจหา** - หากมีชื่อของ การตรวจหา ถัดจากไฟล์ที่ยกเว้น หมายความว่า ไฟล์ดังกล่าวจะถูกยกเว้นสำหรับการตรวจหาที่กำหนดเท่านั้น แต่ไม่ใช่ทั้งหมด หากไฟล์นั้นติดไวรัสมัลแวร์อื่นๆ ในภายหลัง ไฟล์จะถูกตรวจพบ
- **แฮช** – ยกเว้นไฟล์ที่อิงจากแฮชที่ระบุไว้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

เพิ่มหรือแก้ไขการยกเว้นการตรวจหา

ยกเว้นการตรวจหา

ควรให้ชื่อของการตรวจหาของ ESET ที่ถูกต้อง สำหรับชื่อของการตรวจหาที่ถูกต้อง ให้ดู ไฟล์บันทึก แล้วเลือก **การตรวจหา** จากไฟล์บันทึกเมนูแบบเลื่อนลง จะเป็นประโยชน์เมื่อ ตัวอย่างของการตรวจพบที่ผิดพลาด ถูกตรวจพบใน ESET NOD32 Antivirus การยกเว้นสำหรับการแฝงตัวแบบจริงจะเป็นสิ่งที่อันตรายมาก ให้พิจารณาให้ยกเว้นเฉพาะไฟล์ / ไดเรกทอรีที่ได้รับผลกระทบ โดยคลิก **...** ในช่อง **พาธ** และ/หรือเฉพาะช่วงชั่วคราว การยกเว้นยังใช้กับ แอพพลิเคชันที่อาจไม่พึงประสงค์ แอพพลิเคชันที่อาจไม่ปลอดภัยและแอพพลิเคชันที่น่าสงสัย

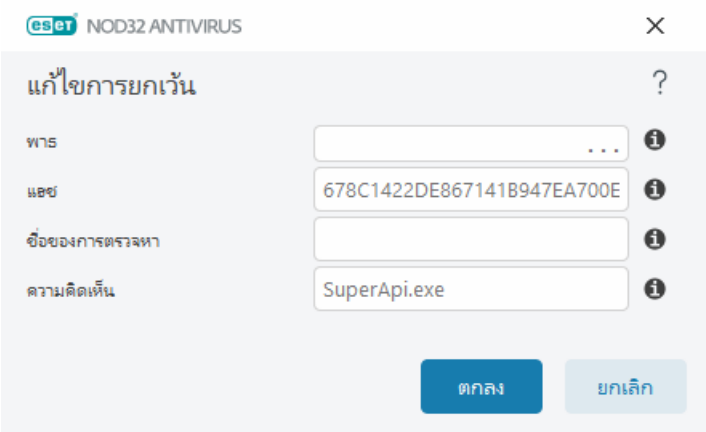
โปรดดู รูปแบบของการยกเว้นพาธ



โปรดดู ตัวอย่างการยกเว้นการตรวจหา ด้านล่าง

ไม่รวมแฮช

ยกเว้นไฟล์ที่อิงจากแฮชที่ระบุไว้ SHA-1 ไม่ว่าจะเป็นประเภทของไฟล์ ตำแหน่ง ชื่อ หรือส่วนขยายของไฟล์



> **การยกเว้นโดยอิงจากชื่อของการตรวจหา**
> หากต้องการยกเว้นการตรวจหาโดยอิงจากชื่อ ให้ป้อนชื่อของการตรวจหาที่ถูกต้อง:
> Win32/Adware.Optmedia
> คุณสามารถใช้รูปแบบต่อไปนี้ได้เมื่อคุณไม่รวมการตรวจหาจากหน้าต่างการเตือนESET NOD32 Antivirus:
> @NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
> @NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
> @NAME=Win32/Bagle.D@TYPE=worm

องค์ประกอบการควบคุม

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

สร้างวิซาร์ดการยกเว้นการตรวจหา

การยกเว้นการตรวจหายังสามารถสร้างจากเมนูบริบท ไฟล์บันทึก ได้อีกด้วย (ไม่สามารถใช้งานได้กับการตรวจหามัลแวร์):

1. ในหน้าต่างโปรแกรมหลัก ให้คลิก**เครื่องมือ** > **ไฟล์บันทึก**
2. คลิกขวาที่การตรวจหาใน **บันทึกการตรวจหา**

3.คลิก **สร้างการยกเว้น**

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

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

ตัวเลือกที่แนะนำถูกเลือกไว้ล่วงหน้าโดยอิงตามประเภทการตรวจหา

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

ตัวเลือกขั้นสูงของกลไกการตรวจจับ

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

เครื่องมือสแกนการรับส่งข้อมูลเครือข่าย

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

เปิดใช้งานเครื่องมือสแกนการรับส่งข้อมูลเครือข่าย – หากคุณปิดใช้งานตัวเลือกนี้ โปรโตคอล HTTP(S), POP3(S) และ IMAP(S) จะไม่ถูกสแกน โปรดทราบว่าฟีเจอร์ของ ESET NOD32 Antivirus ต่อไปนี้จำเป็นต้องเปิดใช้งานเครื่องมือสแกนการรับส่งข้อมูลบนเครือข่าย:

- การป้องกันการเข้าถึงเว็บไซต์
- SSL/TLS

- การป้องกันฟิชชิ่ง
- การป้องกันอีเมลไคลเอ็นต์

การป้องกันแบบคลาวด์

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

ตัวเลือกที่ใช้ได้มีดังนี้:

เปิดใช้งานระบบความเชื่อถือ ESET LiveGrid®

ระบบความเชื่อของ ESET LiveGrid® ให้บัญชีปลอดภัยและบัญชีดำในระบบคลาวด์

ตรวจสอบความเชื่อถือของกระบวนการที่ทำงานอยู่และไฟล์ได้โดยตรงจากส่วนติดต่อของโปรแกรมหรือเมนูบริบทที่มีข้อมูลเพิ่มเติมจาก ESET LiveGrid®

เปิดใช้งานระบบคำติชม ESET LiveGrid®

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

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

ตามค่าเริ่มต้น ESET NOD32 Antivirus จะได้รับการกำหนดค่าเพื่อส่งไฟล์ที่น่าสงสัยไปที่ห้องปฏิบัติการไวรัสของ ESET

เพื่อวิเคราะห์โดยละเอียด ไฟล์ที่มีนามสกุลบางอย่าง เช่น *.doc* หรือ *.xls* จะถูกยกเว้นเสมอ นอกจากนี้คุณยังสามารถเพิ่มนามสกุลอื่นๆ ถ้ามีไฟล์ชนิดใดที่คุณหรือองค์กรของคุณไม่ต้องการส่ง

ℹ อ่านเพิ่มเติมเกี่ยวกับการส่งข้อมูลที่เกี่ยวข้องใน นโยบายความเป็นส่วนตัว

คุณสามารถเลือกจะไม่เปิดใช้งาน ESET LiveGrid® ได้

คุณจะไม่สูญเสียฟังก์ชันการทำงานใดๆ ในซอฟต์แวร์ แต่ในบางกรณี ESET NOD32 Antivirus อาจสามารถตอบสนองต่อการคุกคามใหม่ได้เร็วขึ้นเมื่อคุณเปิดใช้งาน ESET LiveGrid® หากคุณเคยใช้ ESET LiveGrid® ก่อนหน้านี้และปิดใช้งานไปแล้ว อาจยังคงมีแพ็คเกจข้อมูลที่ต้องส่ง แม้ว่าจะปิดใช้งานแล้ว โปรแกรมจะส่งแพ็คเกจดังกล่าวไปยัง ESET เมื่อส่งข้อมูลปัจจุบันทั้งหมดแล้ว โปรแกรมจะไม่สร้างแพ็คเกจเพิ่มเติมอีก

ℹ อ่านเพิ่มเติมเกี่ยวกับ ESET LiveGrid® ใน ประมวลศัพท์
โปรดดู คำแนะนำพร้อมภาพประกอบ ของเราซึ่งมีให้แบบภาษาอังกฤษและภาษาอื่นๆ อีกหลายภาษาเกี่ยวกับการเปิดหรือปิดใช้งาน ESET LiveGrid® ใน ESET NOD32 Antivirus

---

การกำหนดค่าการป้องกันแบบระบบคลาวด์ในการตั้งค่าขั้นสูง

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

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

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

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

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

• **อีเมลที่ติดต่อ (ไม่จำเป็น)** – อีเมลที่ติดต่อของคุณจะถูกส่งพร้อมกับไฟล์ที่น่าสงสัย และอาจใช้เพื่อติดต่อคุณในกรณีต้องการข้อมูลเพิ่มเติมเพื่อการวิเคราะห์ คุณจะไม่ได้รับการตอบกลับจาก ESET ยกเว้นกรณีที่ต้องการข้อมูลเพิ่มเติม

การส่งตัวอย่าง

การส่งตัวอย่างด้วยตนเอง – เปิดใช้ตัวเลือกในการส่งตัวอย่างไปยัง ESET ด้วยตนเองจากเมนูบริบท การกักเก็บ หรือ เครื่องมือ

ส่งตัวอย่างที่ตรวจพบโดยอัตโนมัติ

เลือกประเภทของตัวอย่างที่จะส่งไปยัง ESET เพื่อการวิเคราะห์และเพื่อปรับปรุงการตรวจหา (ขนาดสูงสุดของตัวอย่างตามค่าเริ่มต้นคือ 64MB) ในอนาคต ตัวเลือกที่ใช้ได้มีดังนี้:

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

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

• **ไม่ส่ง** – วัตถุต่างๆ ที่ตรวจพบจะไม่ส่งไปยัง ESET

ส่งตัวอย่างที่น่าสงสัยโดยอัตโนมัติ

ตัวอย่างเหล่านี้จะถูกส่งไปยัง ESET ในกรณีที่กลไกการตรวจจับตรวจไม่พบ ตัวอย่างเช่น ตัวอย่างที่เกือบจะพลาดการตรวจหาหรือหนึ่งใน โมดูลการป้องกัน ของ ESET NOD32 Antivirus พิจารณาตัวอย่างเหล่านี้ว่าน่าสงสัยหรือมีพฤติกรรมที่ไม่ชัดเจน (ขนาดสูงสุดของตัวอย่างตามค่าเริ่มต้นคือ 64 MB)

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

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

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

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

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

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

ขยายรายการประเภทไฟล์เอกสารที่รวมทั้งหมด

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

การยกเว้น

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

✔ หากต้องการแยกไฟล์ที่ดาวน์โหลดจาก `download.domain.com` ให้ไปที่ การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **การป้องกันแบบระบบคลาวด์** > **การส่งตัวอย่าง** แล้วคลิก **แก้ไข** ถัดจาก **การยกเว้น** เพิ่มการยกเว้น `download.domain.com`

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

ตัวกรองการยกเว้นสำหรับการป้องกันระบบคลาวด์

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

ℹ คุณลักษณะนี้จะมีประโยชน์ในการยกเว้นไฟล์ที่อาจมีข้อมูลลับเฉพาะ เช่น เอกสารหรือสเปรดชีท

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

การสแกนมัลแวร์

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

การสแกนตามต้องการ

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

หลังจากที่คุณเลือกโปรไฟล์การสแกนแล้วคุณสามารถกำหนดค่าตัวเลือกต่อไปนี้:

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

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

ThreatSense – ตัวเลือกการตั้งค่าขั้นสูง เช่น นามสกุลไฟล์ที่คุณต้องการควบคุมและวิธีการตรวจหาที่ใช้ ดูรายละเอียดเพิ่มเติมที่ ThreatSense

โปรไฟล์การสแกน

โปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าใน ESET NOD32 Antivirus จะมีอยู่ด้วยกันทั้งหมด 4 รายการ:

- **การสแกนแบบสมาร์ท** - เป็นการสแกนขั้นสูงตามค่าเริ่มต้น โดยโปรไฟล์การสแกนแบบสมาร์ทใช้เทคโนโลยี Smart Optimization ซึ่งไม่รวมไฟล์ที่พบว่าปลอดภัยในการสแกนก่อนหน้านี้และไม่ได้ถูกแก้ไขตั้งแต่การสแกนครั้งก่อนหน้า วิธีนี้ช่วยให้เวลาในการสแกนลดลงโดยมีผลกระทบต่อความปลอดภัยของระบบน้อยที่สุด

- **การสแกนเมนูบริบท** - คุณสามารถเริ่มสแกนไฟล์ใดก็ได้จากเมนูบริบทได้ตามต้องการ โปรไฟล์การสแกนเมนูบริบทจะช่วยให้คุณกำหนดการกำหนดค่าการสแกนซึ่งจะใช้เมื่อคุณเปิดการสแกนวิธีนี้

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

- **การสแกนคอมพิวเตอร์** - เป็นโปรไฟล์ตามค่าเริ่มต้นที่ใช้ในการสแกนคอมพิวเตอร์มาตรฐาน

คุณสามารถบันทึกพารามิเตอร์การสแกนที่ต้องการได้เพื่อการสแกนในอนาคต ขอแนะนำให้คุณสร้างโปรไฟล์อีกโปรไฟล์หนึ่ง (ที่มีเป้าหมายการสแกน วิธีการสแกน และพารามิเตอร์อื่นๆ) สำหรับแต่ละการสแกนที่ใช้เป็นประจำ

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

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

เป้าหมายการสแกน

คุณสามารถเลือกเป้าหมายการสแกนที่กำหนดไว้ล่วงหน้าจากเมนูแบบเลื่อนลง **เป้าหมายการสแกน**

- **ตามการตั้งค่าโปรไฟล์** - เลือกเป้าหมายที่ระบุในโปรไฟล์การสแกนที่เลือก
- **สื่อที่ถอดเข้าออกได้** – เลือกดิสเก็ตต์, อุปกรณ์เก็บข้อมูล USB, ซีดี/ดีวีดี
- **ไดรฟ์ในเครื่อง** – เลือกฮาร์ดไดรฟ์ของระบบทั้งหมด
- **ไดรฟ์เครือข่าย** – เลือกไดรฟ์เครือข่ายที่แมปทั้งหมด
- **การเลือกแบบกำหนดเอง** – ยกเลิกการเลือกก่อนหน้านี้ทั้งหมด

โครงสร้างโฟลเดอร์ (แบบต้นไม้) ยังมีเป้าหมายการสแกนที่เฉพาะเจาะจงอีกด้วย

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

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

หากต้องการไปยังเป้าหมายการสแกน (ไฟล์หรือโฟลเดอร์) อย่างรวดเร็ว ให้พิมพ์พาธของเป้าหมายดังกล่าวลงในช่องข้อความใต้ลำดับโครงสร้าง พาธต้องตรงตามตัวพิมพ์เล็กและใหญ่ โปรดเลือกกล่องกาเครื่องหมายในลำดับโครงสร้างหากต้องการให้ระบบสแกนเป้าหมายด้วย

การสแกนในสถานะไม่ใช้งาน

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

การสแกนในสถานะไม่ใช้งาน

เปิดใช้งานปุ่มสลับที่อยู่ถัดจาก **เปิดใช้งานการสแกนในสถานะไม่ใช้งาน** เพื่อเปิดใช้งานฟีเจอร์นี้ เมื่อคอมพิวเตอร์อยู่ในสถานะที่ไม่ได้ใช้งาน การสแกนคอมพิวเตอร์แบบเงียบจะดำเนินการบนไดรฟ์ในระบบทั้งหมด

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

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

การตรวจหาสภาวะไม่ใช้งาน

ดู การตรวจหาสภาวะไม่ใช้งาน สำหรับรายการแบบเต็มของเงื่อนไขที่จะต้องให้ตรง เพื่อเรียกใช้เครื่องเครื่องสแกนที่มีสถานะไม่ใช้งาน

ThreatSense – ตัวเลือกการตั้งค่าขั้นสูง เช่น นามสกุลไฟล์ที่คุณต้องการควบคุมและวิธีการตรวจหาที่ใช้ ดูรายละเอียดเพิ่มเติมที่ ThreatSense

การตรวจหาสภาวะไม่ใช้งาน

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

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

ใช้ปุ่มสลับสำหรับแต่ละสถานะที่สอดคล้องกันเพื่อเปิดหรือปิดใช้งานการเรียกใช้การตรวจหาสถานะไม่ได้ใช้งาน

การสแกนเมื่อเริ่มต้น

ตามค่าเริ่มต้น การตรวจสอบไฟล์เมื่อเริ่มต้นระบบอัตโนมัติจะดำเนินการเมื่อเริ่มต้นระบบและในระหว่างการอัพเดทกลไกตรวจหา การสแกนนี้จะขึ้นอยู่กับ การกำหนดค่าเครื่องมือวางกำหนดการและงาน

ตัวเลือกการสแกนเมื่อเริ่มต้น เป็นส่วนหนึ่งของงานของเครื่องมือวางกำหนดการ **การตรวจสอบไฟล์เมื่อเริ่มต้นระบบ** ในการแก้ไขการตั้งค่า ให้ไปที่**เครื่องมือ** > **เครื่องมือวางกำหนดการ** แล้วคลิกที่**การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้นอัตโนมัติ** จากนั้นก็**แก้ไข** ในขั้นตอนสุดท้าย หน้าต่าง การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้น จะปรากฏขึ้น สำหรับคำแนะนำโดยละเอียดเกี่ยวกับการสร้างและการจัดการงานของเครื่องมือวางกำหนดการ โปรดดูที่ การสร้างงานใหม่

ThreatSense – ตัวเลือกการตั้งค่าขั้นสูง เช่น นามสกุลไฟล์ที่คุณต้องการควบคุมและวิธีการตรวจหาที่ใช้ ดูรายละเอียดเพิ่มเติมที่ ThreatSense

การตรวจสอบไฟล์เมื่อการอัพเดทฐานข้อมูลไวรัส

เสร็จสิ้น

เมื่อสร้างงานตามกำหนดการ การตรวจสอบไฟล์เมื่อเริ่มต้นระบบ คุณจะมีตัวเลือกมากมายเพื่อปรับพารามิเตอร์ต่อไปนี้:

เมนูแบบเลื่อนลง **เป้าหมายการสแกน** จะระบุความลึกของการสแกนสำหรับไฟล์ที่เรียกใช้เมื่อเริ่มต้นระบบโดยดูจากอัลกอริทึมที่สลับซับซ้อนและเป็นความลับ ไฟล์จะจัดเรียงในลำดับมากไปหาน้อยตามไฟล์ต่อไปนี้:

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

กลุ่มเฉพาะสองกลุ่มที่รวมอยู่ด้วยคือ:

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

รายการไฟล์ที่จะสแกนจะมีการแก้ไขสำหรับแต่ละกลุ่มข้างต้น หากคุณเลือกสแกนไฟล์ที่เรียกใช้เมื่อเริ่มต้นระบบด้วยการสแกนที่มีความลึกต่ำกว่า ไฟล์ที่ไม่ได้สแกนจะถูกสแกนเมื่อเปิดหรือดำเนินการ

ความสำคัญของการสแกน – ระดับความสำคัญที่ใช้เพื่อกำหนดเวลาที่จะเริ่มต้นสแกน:

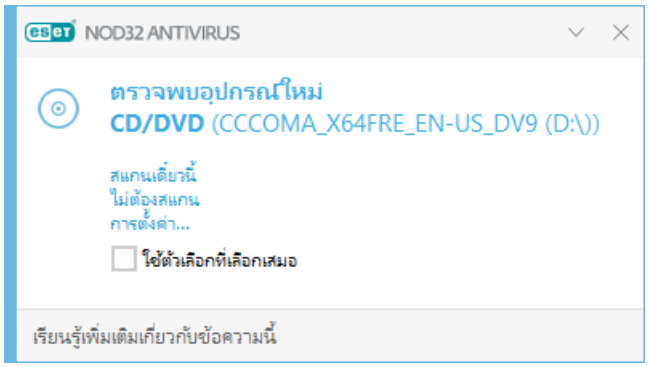
- **เมื่อไม่ได้ใช้งาน** – งานจะดำเนินการเฉพาะเมื่อระบบไม่ได้ใช้งาน
- **ต่ำที่สุด** - การโหลดระบบในระดับต่ำที่สุด
- **ต่ำกว่า** – การโหลดระบบในระดับต่ำ

- **ปกติ** – การโหลดระบบในระดับเฉลี่ย

สื่อที่ถอดเข้าออกได้

ESET NOD32 Antivirus จะทำการสแกนสื่อแบบถอดได้ (ซีดี/ดีวีดี/USB/...) โดยอัตโนมัติเมื่อใส่สื่อเข้าไปในคอมพิวเตอร์ ซึ่งอาจเป็นประโยชน์ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์ต้องการป้องกันไม่ให้ผู้ใช้ใช้งานสื่อที่ถอดเข้าออกได้ที่มีเนื้อหาที่ไม่พึงประสงค์

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



ตัวเลือกสำหรับกล่องโต้ตอบนี้:

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

นอกจากนี้ ESET NOD32 Antivirus จะมีคุณลักษณะของฟังก์ชันการควบคุมอุปกรณ์ ซึ่งช่วยให้คุณสามารถกำหนดกฎในการใช้งานอุปกรณ์ภายนอกบนเครื่องคอมพิวเตอร์ที่ระบุได้ สามารถดูรายละเอียดเพิ่มเติมเกี่ยวกับการควบคุมอุปกรณ์ได้ในส่วน สื่อที่ถอดเข้าออกได้

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

สแกนมัลแวร์ > สื่อที่ถอดเข้าออกได้

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

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

การป้องกันเอกสาร

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

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

ThreatSense – ตัวเลือกการตั้งค่าขั้นสูง เช่น นามสกุลไฟล์ที่คุณต้องการควบคุมและวิธีการตรวจหาที่ใช้ ดูรายละเอียดเพิ่มเติมที่ ThreatSense

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

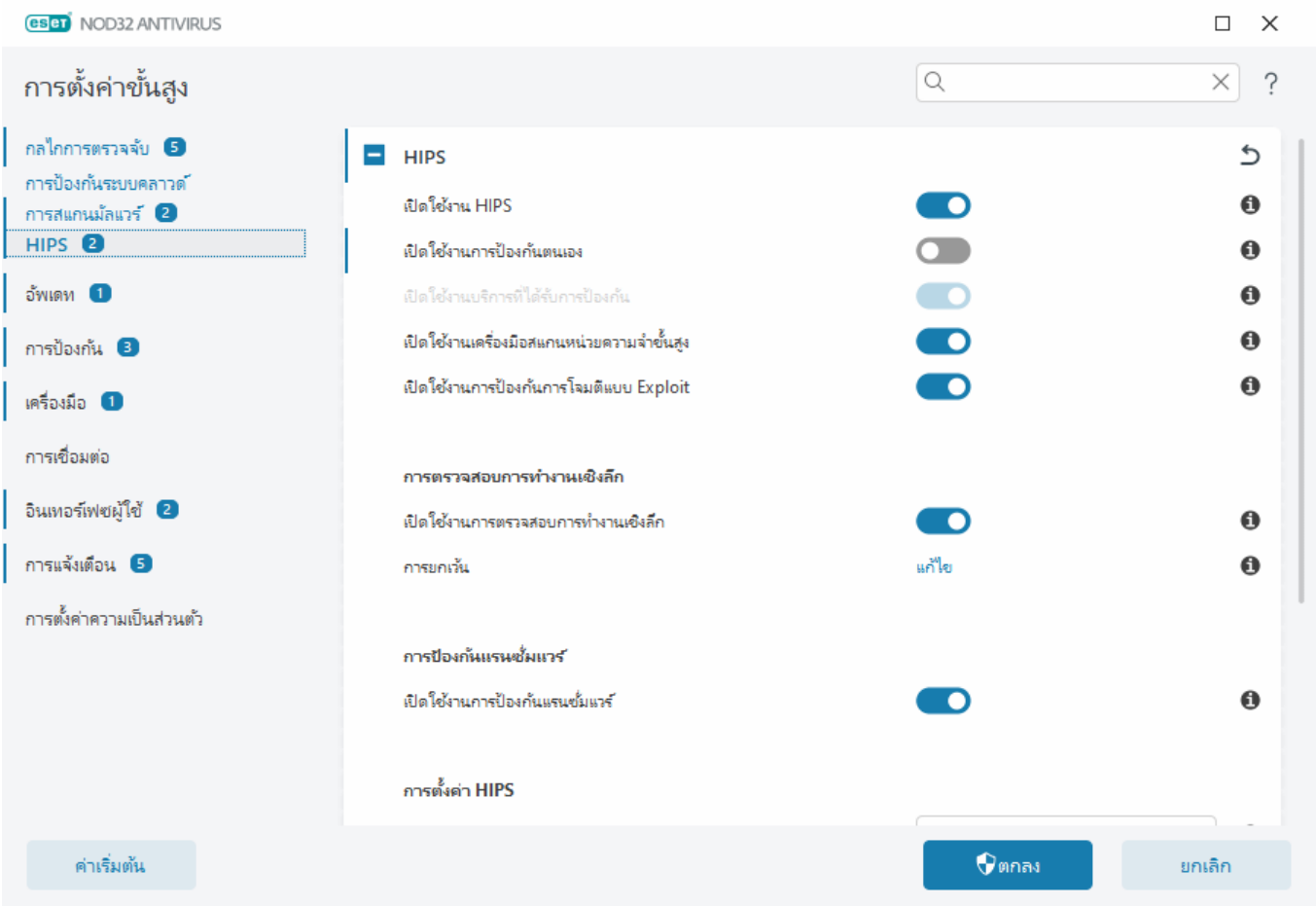
ระบบป้องกันการบุกรุกโฮสต์ (HIPS)

> การเปลี่ยนเป็นการตั้งค่า HIPS ควรดำเนินการโดยผู้ใช้ที่มีประสบการณ์ในการใช้งานเท่านั้น การกำหนดค่าที่ไถูกต้องของการตั้งค่า HIPS จะทำให้ระบบมีปัญหาด้านเสถียรภาพ

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

นั้น

คุณสามารถกำหนดการตั้งค่า HIPS ได้ใน การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **HIPS** > **ระบบป้องกันการบุกรุกโฮสต์** สถานะของ HIPS (เปิดใช้งาน/ปิดใช้งาน) จะปรากฏใน หน้าต่างโปรแกรมหลัก ESET NOD32 Antivirus > **การตั้งค่า** > **การป้องกันคอมพิวเตอร์**



HIPS

เปิดใช้งาน HIPS – เปิดใช้งาน HIPS เป็นค่าเริ่มต้นในESET NOD32 Antivirus การปิด HIPS จะปิดการใช้งานคุณลักษณะของ HIPS ที่เหลือ เช่น การป้องกันการโจมตีแบบ Exploit

เปิดใช้งานการป้องกันตนเอง – ESET NOD32 Antivirus ใช้เทคโนโลยี**การป้องกันตนเอง** ในตัว ซึ่งเป็นส่วนหนึ่งของ HIPS เพื่อป้องกันซอฟต์แวร์ที่เป็นอันตรายจากความเสียหายหรือการเปิดใช้งานการป้องกันไวรัสและสปายแวร์ การป้องกันตนเองจะป้องกันระบบที่สำคัญและกระบวนการของ ESET รหัสรีจิสตรีและไฟล์ต่างๆ จากการถูกเปลี่ยนแปลง

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

เครื่องสแกนหน่วยความจำขั้นสูง ทำงานผสมผสานกับการปิดกั้นการโจมตีเบราเซอร์เพื่อเสริมสร้างการป้องกันมัลแวร์ที่ถูกออกแบบมาเพื่อหลบเลี่ยงการตรวจหาของผลิตภัณฑ์การป้องกันมัลแวร์ด้วยวิธี obfuscation หรือการเข้ารหัส เครื่องมือสแกนหน่วยความจำขั้นสูงจะเปิดใช้งานตามค่าเริ่มต้น อ่านข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้ใน ประมวลศัพท์

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

การตรวจสอบการทำงานเชิงลึก

การตรวจสอบการทำงานเชิงลึก เป็นระดับการปกป้องอีกชั้นหนึ่งซึ่งทำงานโดยเป็นส่วนหนึ่งของคุณสมบัติ HIPS ส่วนขยายของ HIPS นี้จะวิเคราะห์พฤติกรรมของโปรแกรมทั้งหมดที่เรียกใช้บนคอมพิวเตอร์ และเตือนคุณหากพฤติกรรมของกระบวนการเป็นอันตราย

การยกเว้น HIPS จากการตรวจสอบการทำงานเชิงลึก จะช่วยให้คุณสามารถยกเว้นกระบวนการจากการวิเคราะห์ได้ ในการทำให้แน่ใจว่าจะมีการสแกนกระบวนการทำงานทั้งหมดเพื่อหาภัยคุกคาม เราขอแนะนำให้สร้างข้อยกเว้นต่อเมื่อจำเป็นจริงๆ เท่านั้น

โล่ห์ป้องกันแรนซัมแวร์

เปิดโล่ห์ป้องกันโปรแกรมเรียกค่าไถ่ – เป็นระดับการป้องกันอีกชั้นหนึ่งที่ทำงานเป็นส่วนหนึ่งของคุณลักษณะ HIPS คุณจะต้องเปิดใช้งานระบบความเชื่อถือ ESET LiveGrid® เอาไว้จึงจะสามารถใช้งานโล่ห์ป้องกันโปรแกรมเรียกค่าไถ่ได้ อ่านเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้

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

การตั้งค่า HIPS

โหมดการกรอง สามารถทำงานได้ในหนึ่งในโหมดต่อไปนี้:

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

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

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

การยกเว้น HIPS

การยกเว้นทำให้คุณยกเว้นกระบวนการต่างๆ จากการตรวจสอบการทำงานเชิงลึกของ HIPS ได้

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

> i อย่าสับสนกับ นามสกุลไฟล์ที่ยกเว้น การตรวจหานามสกุลไฟล์ การยกเว้นการทำงาน หรือ การยกเว้นกระบวนการ

หากต้องการยกเว้นวัตถุ ให้คลิก **เพิ่ม** แล้วป้อนพาธไปยังวัตถุหรือเลือกวัตถุในโครงสร้าง คุณยังสามารถแก้ไขหรือลบรายการที่เลือกไว้ได้ด้วย

การตั้งค่า HIPS ขั้นสูง

ตัวเลือกต่อไปนี้มีประโยชน์สำหรับการแก้ไขข้อบกพร่องและการวิเคราะห์ลักษณะของแอพพลิเคชัน:

อนุญาตให้โหลดไดรเวอร์ได้เสมอ – ไดรเวอร์ที่เลือกจะได้รับอนุญาตให้โหลดเสมอโดยไม่คำนึงถึงโหมดการกรองที่กำหนดค่าไว้ เว้นแต่จะมีการปิดกั้นอย่างชัดเจนโดยกฎของผู้ใช้

บันทึกการดำเนินการที่ปิดกั้นทั้งหมด – การดำเนินการที่ปิดกั้นทั้งหมดจะถูกเขียนไปที่บันทึก HIPS ใช้คุณลักษณะนี้เฉพาะเมื่อแก้ไขปัญหาหรือร้องขอโดยฝ่ายสนับสนุนด้านเทคนิคของ ESET เนื่องจากการดำเนินการนี้อาจสร้างไฟล์บันทึกขนาดใหญ่และทำให้คอมพิวเตอร์ของคุณช้าลง

แจ้งเมื่อมีการเปลี่ยนแปลงในแอพพลิเคชันการเริ่มต้น – แสดงการแจ้งเตือนบนเดสก์ท็อปในแต่ละครั้งที่มีการเพิ่มหรือลบแอพพลิเคชันจากการเริ่มต้นระบบ

อนุญาตให้โหลดไดรเวอร์ได้เสมอ

ไดรเวอร์ที่แสดงในรายการนี้จะได้รับอนุญาตให้โหลดเสมอโดยไม่คำนึงถึงโหมดการกรอง HIPS เว้นแต่จะมีการปิดกั้นอย่างชัดเจนโดยกฎของผู้ใช้

เพิ่ม – เพิ่มไดรเวอร์ใหม่

แก้ไข – แก้ไขไดรเวอร์ที่เลือก

ลบออก – ลบไดรเวอร์ออกจากรายการ

รีเซ็ต – โหลดชุดของไดรเวอร์ระบบอีกครั้ง

> คลิก **รีเซ็ต** หากคุณไม่ต้องการให้รวมไดรเวอร์ที่คุณได้เพิ่มเอง ตัวเลือกนี้มีประโยชน์หากคุณเพิ่มไดรเวอร์หลายตัวและคุณไม่สามารถลบไดรเวอร์เหล่านั้นออกจากรายการ

> หลังจากติดตั้งแล้ว รายการไดรเวอร์จะว่างเปล่า ESET NOD32 Antivirus จะกรอกรายการดังกล่าวโดยอัตโนมัติเมื่อเวลาผ่านไป

หน้าต่างโต้ตอบ HIPS

หน้าต่างการแจ้งเตือน HIPS จะช่วยให้คุณสร้างกฎตามการทำงานใหม่ที่ HIPS ตรวจพบแล้วระบุเงื่อนไขต่างๆ ว่าจะอนุญาตหรือปฏิเสธการทำงานนั้น

กฎที่สร้างจากหน้าต่างการแจ้งเตือนจะถูกพิจารณาให้เทียบเท่ากับกฎที่สร้างด้วยตนเอง กฎที่สร้างจากหน้าต่างการแจ้งเตือนสามารถมีความเจาะจงได้น้อยกว่ากฎที่เรียกหน้าต่างข้อความนั้นได้ ซึ่งหมายความว่าหลังจากที่สร้างกฎในกล่องข้อความแล้ว การดำเนินการเดียวกันสามารถเรียกใช้หน้าต่างเดียวกันได้ สำหรับข้อมูลเพิ่มเติม ให้ดู ลำดับความสำคัญสำหรับกฎ HIPS

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

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

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

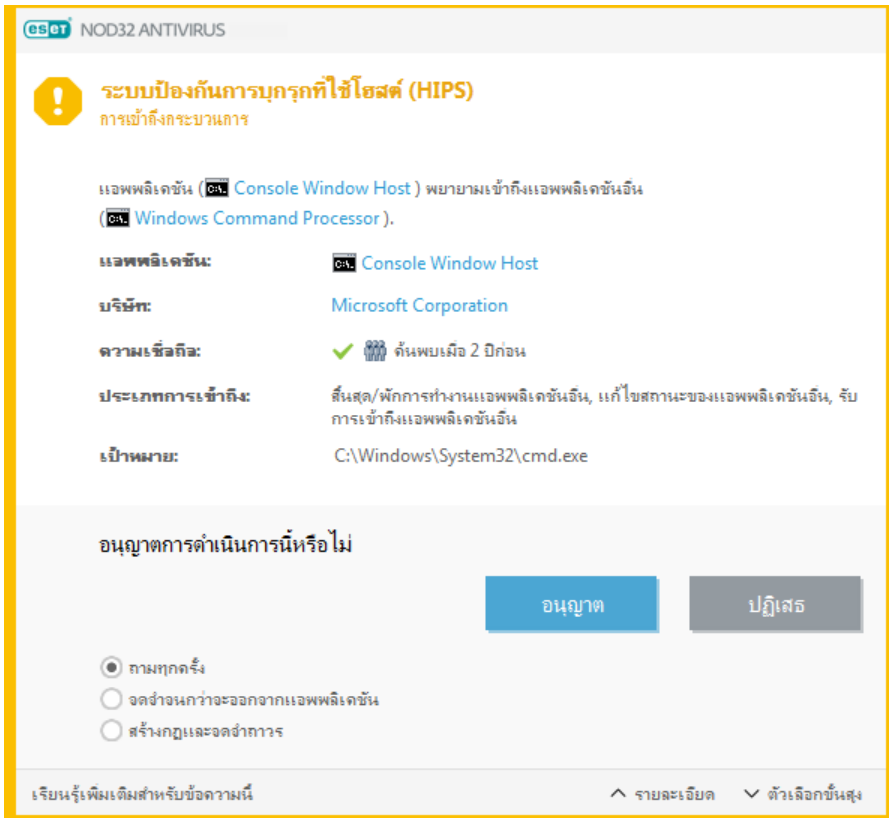
คลิก **รายละเอียด** ที่ด้านล่างสุดเพื่อดูสิ่งที่แอพพลิเคชันเรียกใช้การทำงาน ความเชื่อถือของไฟล์คืออะไร หรือการทำงานใดที่คุณถูกขอให้อนุญาตหรือปฏิเสธ

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

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

การแจ้งเตือน HIPS แบบไม่มีจุดสิ้นสุดหรือไม่

หากต้องการหยุดการแจ้งเตือนที่แสดง เปลี่ยนโหมดการกรองเป็น **อัตโนมัติ** ใน การตั้งค่าขั้นสูง > **กลไกการตรวจจับ** > **HIPS** > **ระบบป้องกันการบุกรุกโฮสต์**



โหมดเรียนรู้ได้สิ้นสุดลง

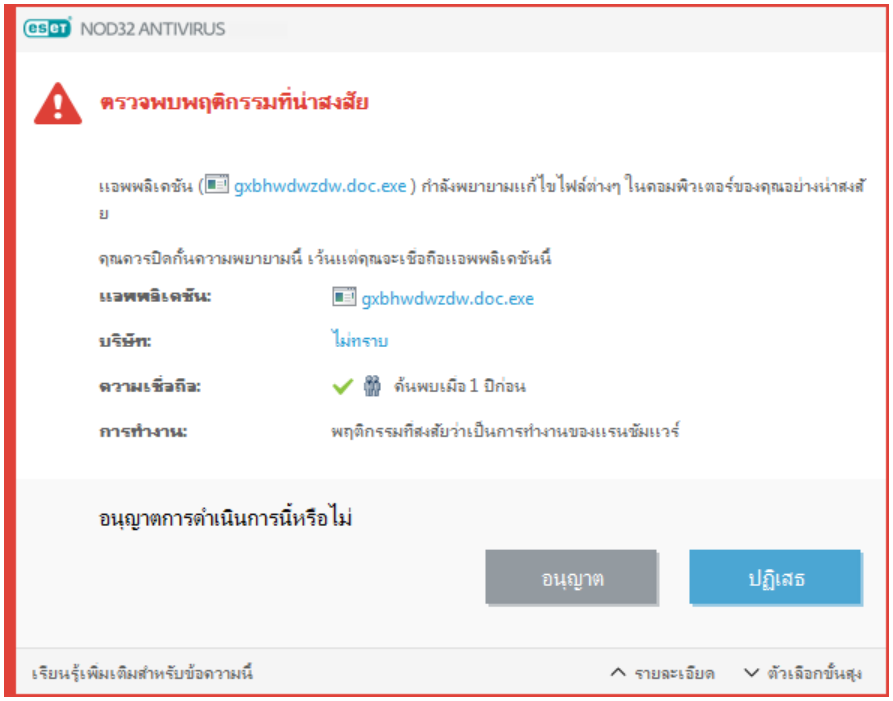
โหมดเรียนรู้จะสร้างและบันทึกกฎโดยอัตโนมัติ คุณสามารถตรวจสอบกฎที่สร้างขึ้นทั้งหมดได้ใน การตั้งค่ากฎ HIPS โดยโหมดนี้เหมาะสำหรับการกำหนดค่า HIPS เป็นครั้งแรก แต่ควรเปิดใช้งานในระยะเวลาสั้นๆ เท่านั้น ผู้ใช้ไม่จำเป็นต้องดำเนินการใดๆ เนื่องจาก ESET NOD32 Antivirus จะบันทึกกฎตามพารามิเตอร์ที่กำหนดไว้ล่วงหน้า เปลี่ยนเป็นโหมด **โต้ตอบ** หรือ **โหมดอ้างอิงตามนโยบาย** หลังจากได้สร้างกฎทั้งหมดสำหรับกระบวนการที่จำเป็นซึ่งทำงานอยู่ภายในระบบปฏิบัติการเพื่อเลี่ยงความเสี่ยงด้านความปลอดภัยแล้ว

คุณสามารถเลื่อนการตัดสินใจนี้ออกไปได้ หากไม่ต้องการเปลี่ยนการตั้งค่า

ตรวจพบพฤติกรรมที่สงสัยว่าเป็นการทำงานของแร

นซัมแวร์

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



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

ESET LiveGrid® ต้องเปิดใช้งานเอาไว้เพื่อให้สามารถใช้งานการป้องกันแรนซัมแวร์ได้อย่างถูกต้อง

การจัดการกฎ HIPS

รายการกฎที่ผู้ใช้กำหนดและเพิ่มโดยอัตโนมัติจากระบบ HIPS สามารถดูรายละเอียดเพิ่มเติมเกี่ยวกับการสร้างกฎและการดำเนินการของ HIPS ได้ใน การตั้งค่ากฎ HIPS ดูหลักการทั่วไปของ HIPS

คอลัมน์

กฎ – ชื่อกฎที่ผู้ใช้กำหนดหรือเลือกโดยอัตโนมัติ

เปิดใช้งาน – ปิดใช้งานแถบเลื่อนนี้หากคุณต้องการคงกฎไว้ในรายการแต่ไม่ต้องการใช้

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

ที่มา – ระบบจะใช้กฎนี้ต่อเมื่อแอพพลิเคชันเรียกเหตุการณ์

เป้าหมาย – จะมีการใช้กฎก็ต่อเมื่อการดำเนินการเกี่ยวข้องกับไฟล์ แอพพลิเคชัน หรือรายการรีจิสตรีบางรายการ

ความละเอียดของการบันทึก – ถ้าคุณเปิดใช้งานตัวเลือกนี้ ข้อมูลเกี่ยวกับกฎนี้จะถูกเขียนไปที่ บันทึก HIPS

แจ้งเตือน – หน้าต่างแจ้งเตือนขนาดเล็กจะปรากฏที่มุมขวาล่าง หากมีการเรียกเหตุการณ์

องค์ประกอบการควบคุม

เพิ่ม – สร้างกฎใหม่

แก้ไข – ช่วยให้คุณสามารถแก้ไขรายการที่เลือกได้

ลบออก – ลบรายการที่เลือกออก

จัดอันดับความสำคัญของกฎ HIPS

ไม่มีตัวเลือกเพื่อปรับระดับความสำคัญของกฎ HIPS โดยใช้ปุ่มบนสุด/ล่าสุด

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

แก้ไขกฎ HIPS

ดู การจัดการกฎ HIPS ก่อน

ชื่อกฎ – ชื่อกฎที่ผู้ใช้กำหนดหรือเลือกโดยอัตโนมัติ

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

การดำเนินการที่ได้ผล – คุณต้องเลือกประเภทของการดำเนินการที่กฎจะนำมาปรับใช้ ระบบจะใช้กฎนี้เฉพาะสำหรับการดำเนินการประเภทนี้เท่านั้นและสำหรับเป้าหมายที่เลือก

เปิดใช้งาน – ปิดใช้งานปุ่มสลับนี้หากคุณต้องการคงกฎไว้ในรายการแต่ไม่ปรับใช้

ความละเอียดของการบันทึก – ถ้าคุณเปิดใช้งานตัวเลือกนี้ ข้อมูลเกี่ยวกับกฎนี้จะถูกเขียนไปที่ บันทึก HIPS

แจ้งเตือนผู้ใช้ – หน้าต่างแจ้งเตือนขนาดเล็กจะปรากฏที่มุมขวาล่าง หากมีการเรียกเหตุการณ์

กฎประกอบด้วยส่วนต่างๆ ซึ่งจะอธิบายเงื่อนไขที่เรียกใช้งานกฎนี้:

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

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

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

รายการรีจิสตรี – ระบบจะใช้กฎนี้ต่อเมื่อการดำเนินการเกี่ยวข้องกับเป้าหมายนี้ เลือก **รายการเฉพาะ** จากเมนูแบบเลื่อนลงแล้วคลิก **เพิ่ม** เพื่อป้อนข้อมูลด้วยตัวเอง หรือคุณสามารถคลิก **เปิดตัวแก้ไขรีจิสตรี** เพื่อเลือกรหัสจากรีจิสตรี นอกจากนี้ คุณยังสามารถเลือก **รายการทั้งหมด** จากเมนูแบบเลื่อนลงเพื่อเพิ่มแอพพลิเคชันทั้งหมดได้

> i การดำเนินการของกฎบางอย่างที่กำหนดไว้ล่วงหน้าโดย HIPS จะไม่สามารถปิดกั้นหรืออนุญาตได้ตามค่าเริ่มต้น นอกจากนี้ HIPS จะไม่ตรวจสอบการดำเนินการทั้งหมดของระบบ HIPS ตรวจสอบการดำเนินการที่อาจพิจารณาว่าไม่ปลอดภัย

คำอธิบายของการดำเนินการที่สำคัญ:

การดำเนินการของไฟล์

- **ลบไฟล์** – แอพพลิเคชันจะสอบถามเกี่ยวกับการอนุญาตให้ลบไฟล์เป้าหมาย

• **เขียนไปยังไฟล์** – แอพพลิเคชันจะสอบถามเกี่ยวกับการอนุญาตให้เขียนไฟล์เป้าหมาย

• **การเข้าถึงดิสก์โดยตรง** – แอพพลิเคชันจะพยายามอ่านจากหรือเขียนไปยังดิสก์ด้วยวิธีที่ไม่เป็นมาตรฐาน ซึ่งจะหลีกเลี่ยงขั้นตอนทำงานทั่วไปของ Windows ซึ่งอาจส่งผลให้ไฟล์ได้รับการแก้ไขโดยไม่ใช้แอพพลิเคชันของกฎที่สอดคล้องกัน การดำเนินการนี้อาจมีสาเหตุจากการที่มัลแวร์พยายามหลบเลี่ยงการตรวจหา ซอฟต์แวร์สำรองข้อมูลพยายามที่จะทำสำเนาของดิสก์ หรือโปรแกรมจัดการพาร์ติชันพยายามจัดระเบียบไดรฟ์ข้อมูลของดิสก์ใหม่

• **ติดตั้งฮุคร่วม** – อ้างถึงการเรียกฟังก์ชัน SetWindowsHookEx จากไลบรารี MSDN

• **โหลดไดรเวอร์** – การติดตั้งและการโหลดไดรเวอร์ลงในระบบ

การดำเนินการของแอพพลิเคชัน

• **แก้ไขแอพพลิเคชันอื่น** – การใส่เครื่องมือแก้ไขปัญหาในการดำเนินการ ในขณะที่มีการแก้ไขปัญหาของแอพพลิเคชัน ระบบจะตรวจสอบและแก้ไขรายละเอียดต่างๆ ของการทำงาน และจะมีการเข้าถึงข้อมูลการทำงาน

• **ดักฟังเหตุการณ์จากแอพพลิเคชันอื่น** – แอพพลิเคชันที่มาจะพยายามตรวจจับเหตุการณ์ที่มีการกำหนดเป้าหมายไปยังแอพพลิเคชันเฉพาะ (ตัวอย่างเช่น เครื่องมือบันทึกการกดแป้นพิมพ์ที่พยายามตรวจจับเหตุการณ์ของเบราว์เซอร์)

• **สิ้นสุด/พักการทำงานแอพพลิเคชันอื่น** – การพัก การทำงานต่อ หรือการสิ้นสุดกระบวนการ (สามารถเข้าถึงได้โดยตรงจากช่อง Process Explorer หรือ Processes)

• **เริ่มต้นแอพพลิเคชันใหม่** – การเริ่มต้นแอพพลิเคชันหรือกระบวนการใหม่

• **แก้ไขสถานะของแอพพลิเคชันอื่น** – แอพพลิเคชันที่มาจะพยายามเขียนข้อมูลไปยังหน่วยความจำของแอพพลิเคชันเป้าหมายหรือเรียกใช้รหัสในนามของตนเอง ฟังก์ชันการทำงานนี้อาจเป็นประโยชน์เพื่อป้องกันแอพพลิเคชันสำคัญ ด้วยการกำหนดค่าเป็นแอพพลิเคชันเป้าหมายในกฎที่ปิดกั้นการใช้การดำเนินการนี้

การดำเนินการของรีจิสตรี

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

- **ลบจากรีจิสตรี** – การลบรหัสรีจิสตรีหรือค่าของรหัสรีจิสตรี

- **เปลี่ยนชื่อรหัสรีจิสตรี** – การเปลี่ยนชื่อรหัสรีจิสตรี

- **แก้ไขรีจิสตรี** – การสร้างค่าใหม่ของรหัสรีจิสตรี การเปลี่ยนค่าที่มีอยู่ การย้ายข้อมูลในโครงสร้างฐานข้อมูล หรือการตั้งค่าสิทธิ์ของผู้ใช้หรือกลุ่มสำหรับรหัสรีจิสตรี

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

> ⚠ หากคุณสร้างกฎที่กว้างมาก คำเตือนเกี่ยวกับกฎประเภทนี้จะปรากฏขึ้น

ในตัวอย่างต่อไปนี้ เราจะสาธิตวิธีจำกัดการทำงานที่ไม่พึงประสงค์ของแอพพลิเคชันที่ระบุ:

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

2. เลือกแถบตัวเลื่อนที่อยู่ถัดจาก **แจ้งเตือนผู้ใช้** เพื่อแสดงการแจ้งเตือนเมื่อมีการนำกฎไปใช้

3. เลือกการดำเนินการอย่างน้อยหนึ่งอย่าง ในส่วน**การดำเนินการที่ได้ผล** ว่าจะใช้กฎใด

4. คลิก**ถัดไป**

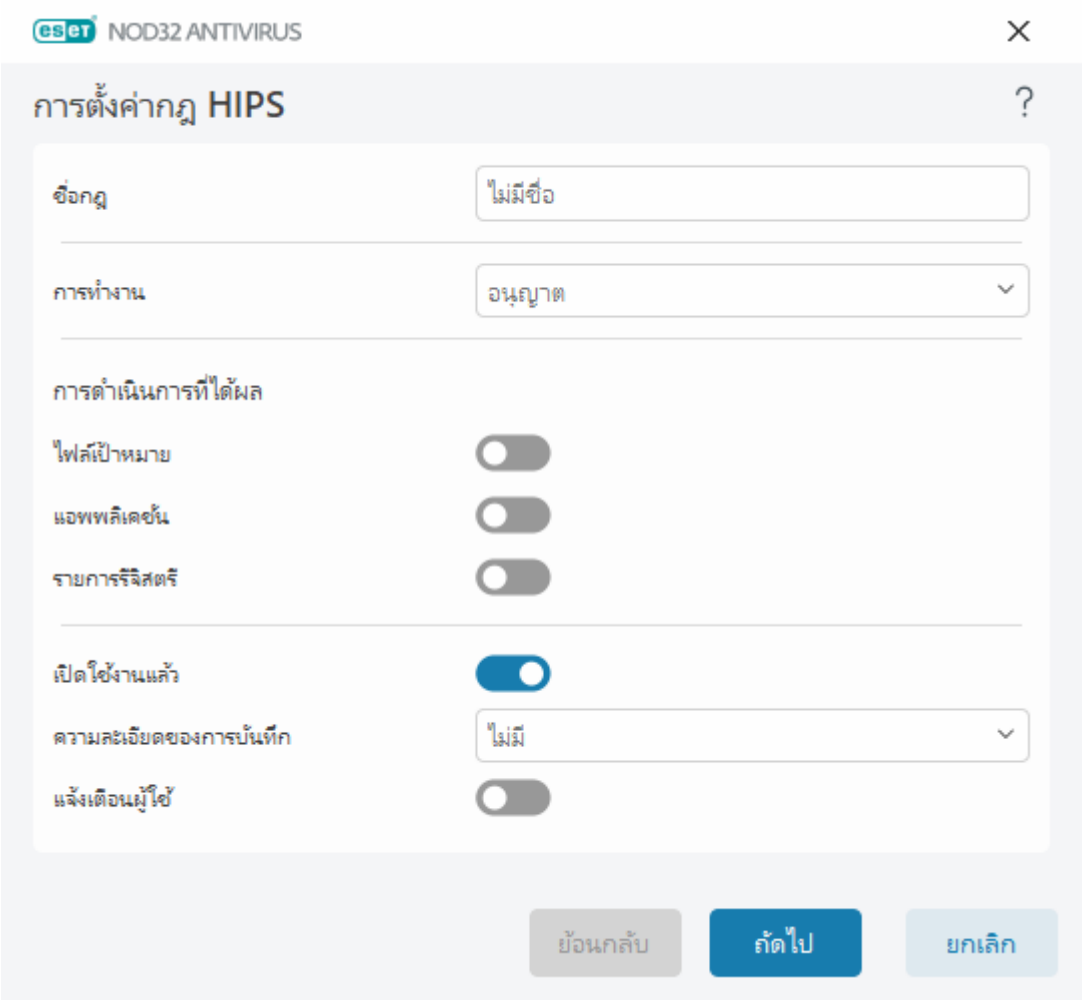
5. ในหน้าต่าง **แอพพลิเคชันที่มา** เลือก **แอพพลิเคชันที่เจาะจง** จากเมนูแบบเลื่อนลงเพื่อใช้กฎใหม่กับแอพพลิเคชันทั้งหมดที่พยายามจะทำงานกับแอพพลิเคชันที่เลือกไว้บนแอพพลิเคชันที่คุณระบุ

6. คลิก**เพิ่ม** และ **...** เพื่อเลือกพาธไปยังแอพพลิเคชันที่เจาะจง แล้วกด**ตกลง** เพิ่มแอพพลิเคชันหากคุณต้องการ ตัวอย่างเช่น: *C:\Program Files (x86)\Untrusted application\application.exe*

7. เลือก**เขียนข้อมูลในไฟล์** การทำงาน

8. เลือก**ไฟล์ทั้งหมด** จากเมนูแบบเลื่อนลง วิธีนี้จะปิดกั้นความพยายามใดๆ เพื่อเขียนไฟล์โดยแอพพลิเคชันที่เลือกไว้จากขั้นตอนก่อนหน้านี้

9. คลิก **เสร็จสิ้น** เพื่อบันทึกกฎใหม่ของคุณ



เพิ่มแอพพลิเคชัน/พาธของรีจิสตรีสำหรับ HIPS

เลือกพาธแอพพลิเคชันของไฟล์ด้วยการคลิกตัวเลือก **...** เมื่อเลือกโฟลเดอร์ แอพพลิเคชันทั้งหมดที่อยู่ในตำแหน่งนี้จะถูกรวมไว้ด้วย

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

ตัวอย่างพาธของไฟล์หรือรีจิสตรี:

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

อัพเดท

ตัวเลือกการตั้งค่าการอัพเดทจะพร้อมใช้งานใน การตั้งค่าขั้นสูง > **การอัปเดต** ส่วนนี้จะระบุข้อมูลที่มาของการอัพเดทเหมือนกับการใช้เซิร์ฟเวอร์อัพเดทและข้อมูลการตรวจสอบสิทธิ์สำหรับเซิร์ฟเวอร์เหล่านี้

อัพเดท

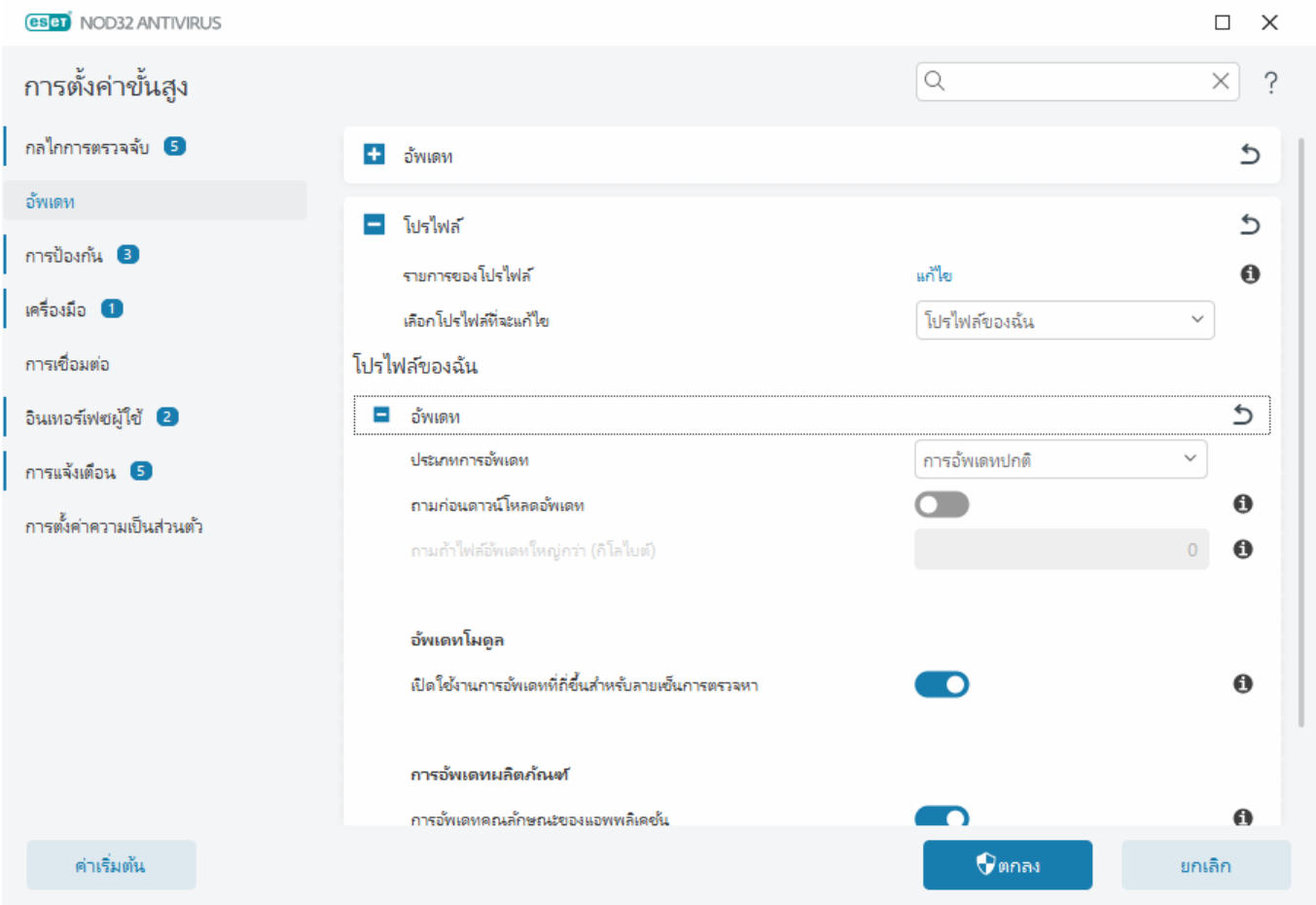
โปรไฟล์การอัพเดทที่กำลังใช้งานอยู่แสดงอยู่ในเมนู **เลือกโปรไฟล์การอัพเดทค่าเริ่มต้น** แบบเลื่อนลง

หากต้องการสร้างโปรไฟล์ใหม่ ให้ดูส่วน โปรไฟล์การอัพเดท

หากคุณพบปัญหาขณะพยายามดาวน์โหลดกลไกการตรวจจับหรือการอัพเดทโมดูล ให้คลิก **ล้าง** ถัดจาก **ล้างแคชการอัพเดท** เพื่อล้างไฟล์/แคชการอัพเดทชั่วคราว

การย้อนกลับโมดูล

หากคุณสงสัยว่าการอัพเดทใหม่ของกลไกตรวจหาและ/หรือโมดูลโปรแกรมอาจไม่เสถียรหรือเสียหาย คุณสามารถ ย้อนกลับไปเป็นเวอร์ชันก่อนหน้า ได้ แล้วปิดการใช้งานการอัพเดทสำหรับช่วงเวลาที่ตั้งค่าไว้



คุณต้องป้อนพารามิเตอร์ที่อัพเดททั้งหมดให้ถูกต้อง เพื่อให้ระบบดาวน์โหลดการอัพเดทอย่างถูกต้อง ถ้าคุณใช้ไฟร์วอลล์ โปรดตรวจสอบให้แน่ใจว่าโปรแกรม ESET ของคุณได้รับอนุญาตให้สื่อสารกับอินเทอร์เน็ต (ตัวอย่างเช่น การเชื่อมต่อ HTTP)

โปรไฟล์

โปรไฟล์การอัพเดทสามารถสร้างขึ้นเพื่อการกำหนดค่าและงานการอัพเดทต่างๆ การสร้างโปรไฟล์การอัพเดทจะเป็นประโยชน์อย่างมากสำหรับผู้ใช้ที่ต้องเดินทางบ่อย ที่ต้องการโปรไฟล์สำรองสำหรับคุณสมบัติการเชื่อมต่ออินเทอร์เน็ตที่มีการเปลี่ยนแปลงเป็นประจำ

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

การอัพเดท

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

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

ถามก่อนที่จะดาวน์โหลดอัพเดท – โปรแกรมจะแสดงการแจ้งเตือนที่คุณสามารถเลือกที่จะยืนยันหรือปฏิเสธการดาวน์โหลดไฟล์อัพเดท

ถามหากไฟล์อัพเดทใหญ่กว่า (กิโลไบต์) – โปรแกรมจะแสดงข้อความยืนยันหากขนาดไฟล์อัพเดทใหญ่กว่าค่าที่กำหนด หากขนาดไฟล์อัพเดทถูกตั้งค่าเป็น 0 กิโลไบต์ โปรแกรมจะแสดงข้อความยืนยันเสมอ

การอัพเดทโมดูล

เปิดใช้งานการอัพเดทฐานข้อมูลการตรวจหาให้บ่อยขึ้น – ฐานข้อมูลการตรวจหาจะถูกอัพเดทในช่วงเวลาที่สั้นลง การปิดใช้งานการตั้งค่านี้อาจส่งผลกระทบทางลบต่ออัตราการตรวจจับ

การอัพเดทผลิตภัณฑ์

การอัพเดทคุณลักษณะของแอพพลิเคชัน – ติดตั้ง ESET NOD32 Antivirus เวอร์ชันใหม่โดยอัตโนมัติ

ตัวเลือกการเชื่อมต่อ

หากต้องการใช้พร็อกซีเซิร์ฟเวอร์เพื่อดาวน์โหลดการอัพเดท โปรดดูส่วนตัวเลือกการเชื่อมต่อ

การอัพเดทย้อนหลัง

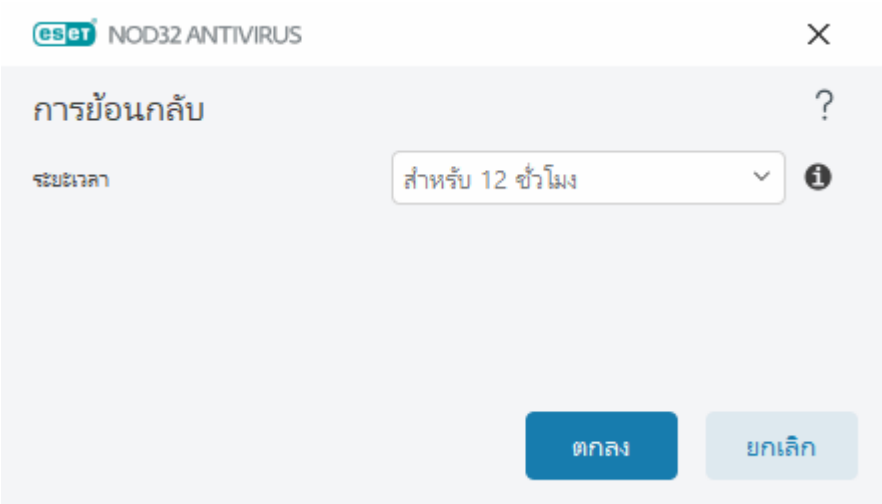
หากคุณสงสัยว่าการอัพเดทใหม่ของกลไกตรวจหาหรือโมดูลโปรแกรมอาจไม่เสถียรหรือเสียหาย คุณสามารถย้อนกลับเป็นเวอร์ชันก่อนหน้าและปิดใช้งานการอัพเดทชั่วคราว หรือมิฉะนั้น คุณสามารถเปิดใช้งานการอัพเดทที่ปิดใช้งานไว้ก่อนหน้านั้น ถ้าคุณได้เลื่อนการอัพเดทไว้อย่างไม่มีกำหนด

ESET NOD32 Antivirus จะบันทึกสแนปชอตของกลไกการตรวจหาและโมดูลโปรแกรมเพื่อใช้กับคุณลักษณะ การย้อนกลับ หากต้องการสร้างสแนปชอตของฐานข้อมูลไวรัส ให้เปิดใช้งาน **สร้างสแนปชอตของโมดูล** ไว้ เมื่อ **สร้างสแนปชอตของโมดูล** เปิดใช้งาน สแนปชอตแรกจะถูกสร้างขึ้นในการอัพเดทครั้งแรก และสแนปชอตถัดไปจะถูก

สร้างขึ้นหลังจากนั้น 48 ชั่วโมง ช่อง **จำนวนสแนปชอตที่เก็บในเครื่อง** จะระบุจำนวนของสแนปชอตกลไกการตรวจหาที่เก็บไว้

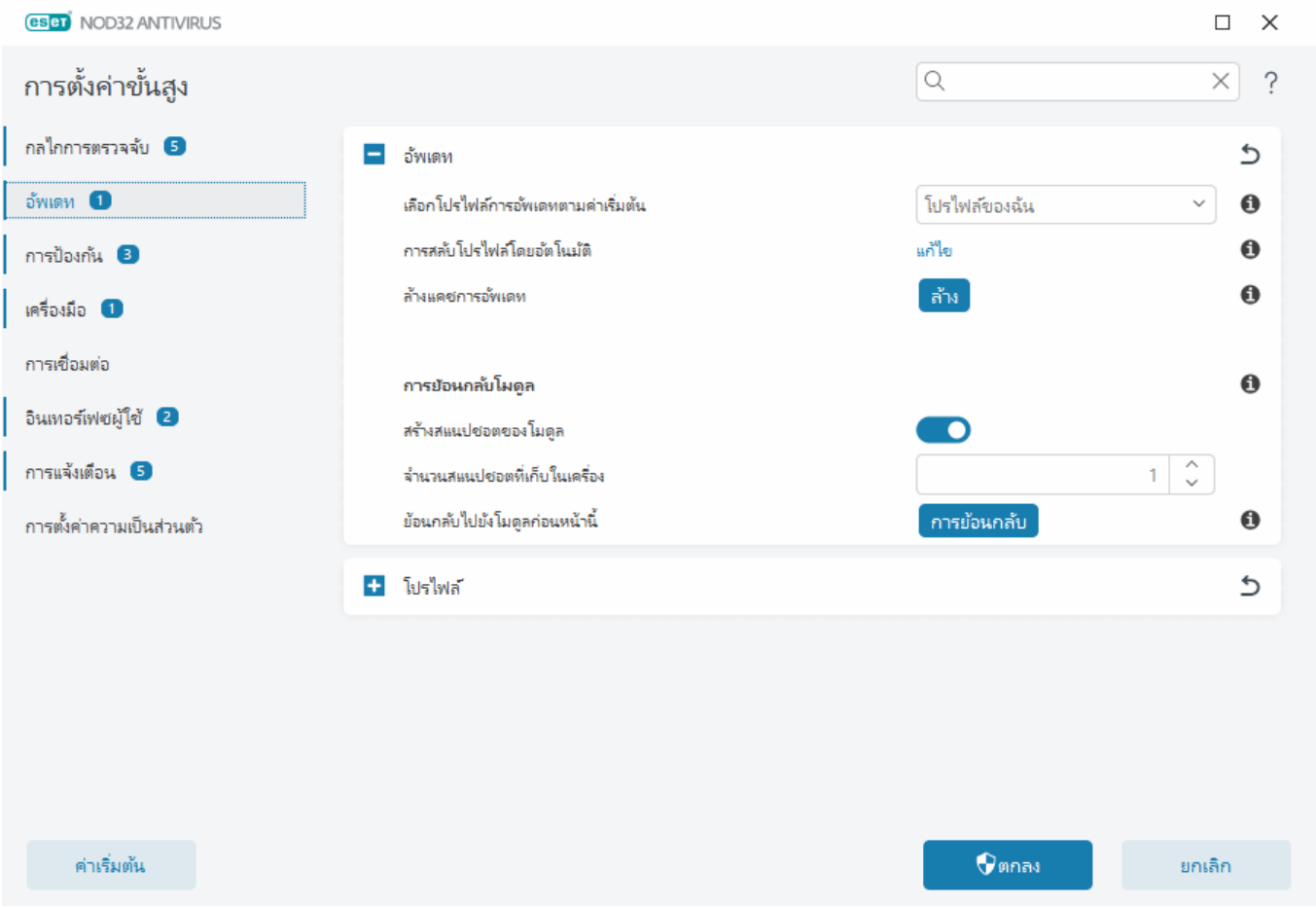
> เมื่อถึงจำนวนสูงสุดของสแนปชอต (เช่น สามภาพ) สแนปชอตที่เก่าที่สุดจะถูกแทนที่ด้วยสแนปชอตใหม่ทุก 48 ชั่วโมง ESET NOD32 Antivirus จะย้อนกลับกลไกการตรวจหาและรุ่นการปรับปรุงโมดูลโปรแกรมไปยังสแนปชอตที่เก่าที่สุด

หากคุณคลิก **ย้อนกลับ** ใน การตั้งค่าขั้นสูง > **อัพเดท** > **อัพเดท** คุณต้องเลือกช่วงเวลาจากเมนูแบบเลื่อนลง **ระยะเวลา** ที่แสดงระยะเวลาที่จะมีการหยุดการอัพเดทกลไกตรวจหาและโมดูลโปรแกรมไว้ชั่วคราว



เลือก **จนกว่าจะยกเลิก** เพื่อเลื่อนการอัพเดทเป็นประจำออกไปโดยไม่มีกำหนดจนกว่าคุณจะเรียกการทำงานของการอัพเดทด้วยตนเอง เนื่องจากจะมีความเสี่ยงด้านความปลอดภัย ESET จึงไม่แนะนำให้เลือกตัวเลือกนี้

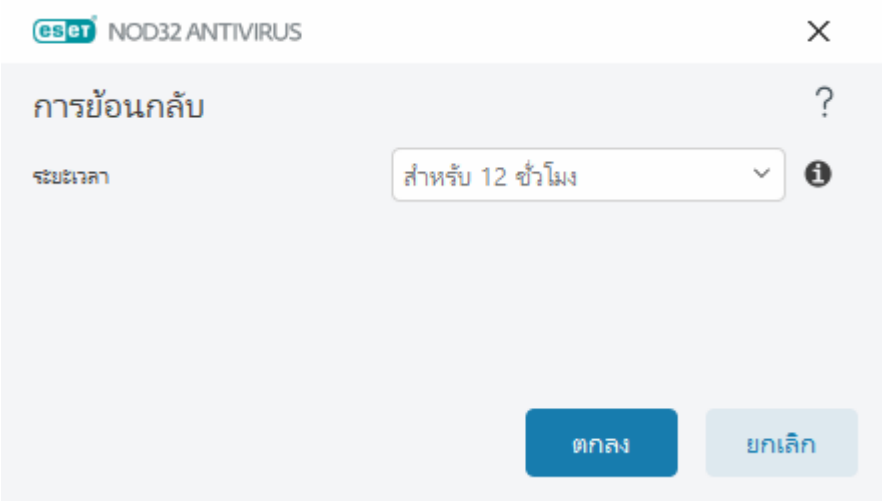
หากทำการย้อนกลับ ปุ่ม **การย้อนกลับ** จะเปลี่ยนเป็น **อนุญาตการอัพเดท** โดยจะไม่สามารถอัพเดทได้ในช่วงเวลาที่เลือกจากเมนู **ระงับการอัพเดท** แบบเลื่อนลง เวอร์ชันของกลไกตรวจหาจะถูกดาวน์เกรดมาเป็นรุ่นเก่าที่สุดที่มีและเก็บไว้เป็นสแนปชอตในระบบไฟล์ของเครื่องคอมพิวเตอร์



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

ช่วงเวลาย้อนกลับ

หากคุณคลิก **ย้อนกลับ** ใน การตั้งค่าขั้นสูง > **อัพเดท** > **อัพเดท** คุณต้องเลือกช่วงเวลาจากเมนูแบบเลื่อนลง **ระยะเวลา** ที่แสดงระยะเวลาที่จะมีการหยุดการอัพเดทกลไกตรวจหาและโมดูลโปรแกรมไว้ชั่วคราว



เลือก **จนกว่าจะยกเลิก** เพื่อเลื่อนการอัพเดทเป็นประจำออกไปโดยไม่มีกำหนดจนกว่าคุณจะเรียกการทำงานของการอัพเดทด้วยตนเอง เนื่องจากจะมีความเสี่ยงด้านความปลอดภัย ESET จึงไม่แนะนำให้เลือกตัวเลือกนี้

การอัพเดทผลิตภัณฑ์

ส่วน **การอัพเดทผลิตภัณฑ์** ทำให้คุณสามารถติดตั้งการอัพเดทคุณลักษณะใหม่เมื่อพร้อมใช้งานได้โดยอัตโนมัติ

การอัพเดทคุณลักษณะของแอพพลิเคชันจะนำมาซึ่งคุณลักษณะใหม่ หรือการเปลี่ยนแปลงคุณลักษณะที่มีในอยู่เวอร์ชันก่อนหน้านี้ การอัพเกรดสามารถทำได้โดยอัตโนมัติโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ หรือคุณสามารถเลือกให้มีการแจ้งเตือนได้ หลังจากการติดตั้งการอัพเดทคุณลักษณะของแอพพลิเคชันแล้ว อาจจำเป็นต้องรีสตาร์ทคอมพิวเตอร์

การอัพเดทคุณลักษณะของแอพพลิเคชัน – เมื่อเปิดใช้งาน ระบบจะดำเนินการอัพเดทคุณลักษณะของแอพพลิเคชันโดยอัตโนมัติ

ตัวเลือกการเชื่อมต่อ

หากต้องการเข้าถึงตัวเลือกการตั้งค่าพร็อกซีเซิร์ฟเวอร์สำหรับโปรไฟล์การอัพเดทที่เฉพาะเจาะจง ให้เปิด การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์** > **อัพเดท** > **ตัวเลือกการเชื่อมต่อ** คลิกเมนูแบบเลื่อนลง **โหมดพร็อกซี** แล้วเลือกหนึ่งในสามตัวเลือกต่อไปนี้:

- ไม่ใช้พร็อกซีเซิร์ฟเวอร์
- การเชื่อมต่อผ่านพร็อกซีเซิร์ฟเวอร์

• ใช้การตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วม

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

เลือก **ไม่ใช้เซิร์ฟเวอร์พร็อกซี** เพื่อระบุว่าจะไม่ใช้พร็อกซีเซิร์ฟเวอร์ในการอัพเดท ESET NOD32 Antivirus

ควรเลือกตัวเลือก **การเชื่อมต่อผ่านพร็อกซีเซิร์ฟเวอร์** ไว้ถ้า:

• ระบบใช้พร็อกซีเซิร์ฟเวอร์อื่นนอกเหนือจากที่ระบุไว้ใน การตั้งค่าขั้นสูง > **การเชื่อมต่อ** ในการอัพเดท ESET NOD32 Antivirus ในการกำหนดค่านี้ ควรระบุข้อมูลสำหรับพร็อกซีใหม่ไว้ในที่อยู่ **พร็อกซีเซิร์ฟเวอร์**, **พอร์ต** การสื่อสาร (3128 ตามค่าเริ่มต้น) และ **ชื่อผู้ใช้** และ **รหัสผ่าน** สำหรับพร็อกซีเซิร์ฟเวอร์ หากต้องใช้

• การตั้งค่าพร็อกซีเซิร์ฟเวอร์ไม่ได้ถูกตั้งค่าให้ใช้ร่วมกัน แต่ ESET NOD32 Antivirus จะเชื่อมต่อกับพร็อกซีเซิร์ฟเวอร์เพื่อการอัพเดท

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

การตั้งค่าเริ่มต้นสำหรับพร็อกซีเซิร์ฟเวอร์คือ **ใช้การตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วม**

ใช้การเชื่อมต่อโดยตรงหากพร็อกซีไม่สามารถใช้งานได้ – พร็อกซีจะถูกข้ามระหว่างการอัพเดทถ้าไม่สามารถเข้าถึงได้

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

การป้องกัน

การป้องกันช่วยปกป้องการโจมตีระบบที่ประสงค์ร้ายโดยการควบคุมไฟล์ อีเมล และการติดต่อสื่อสารทางอินเทอร์เน็ต ตัวอย่างเช่น หากวัตถุที่จัดประเภทเป็นมัลแวร์ถูกตรวจจับ การปรับปรุงแก้ไขจะเริ่มต้นขึ้น การป้องกันสามารถลบวัตถุได้โดยการบล็อกวัตถุก่อน แล้วจึงกำจัด ลบ หรือย้ายไปยังการกักเก็บ

หากต้องการกำหนดค่าการป้องกันโดยละเอียด ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน**

การเปลี่ยนแปลงในส่วนการป้องกันควรดำเนินการโดยผู้ใช้ที่มีประสบการณ์ในการใช้งานเท่านั้น การกำหนดค่าที่ไม่ถูกต้องของการตั้งค่าจะลดระดับความสามารถในการป้องกัน

ในส่วนนี้:

- การตอบกลับการตรวจจับ
- การตั้งค่าการรายงาน
- การตั้งค่าการป้องกัน

การตอบกลับการตรวจจับ

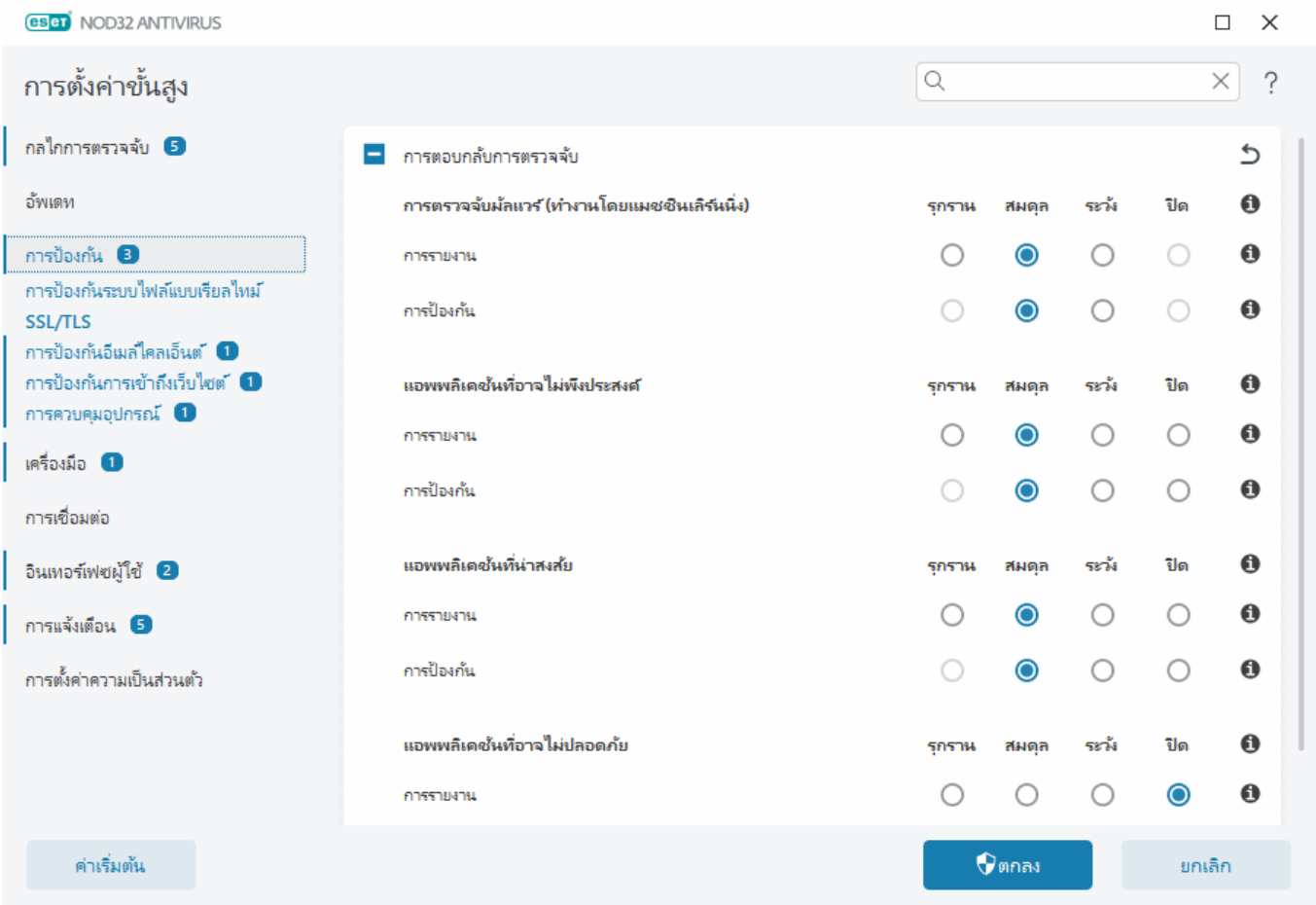
การตอบสนองการตรวจจับช่วยให้คุณสามารถกำหนดค่าระดับการรายงานและการป้องกันของการทำงานประเภทต่อไปนี้:

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

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

- **แอพพลิเคชันที่น่าสงสัย** – จะรวมถึงโปรแกรมต่างๆ ที่บีบอัดด้วย แพ็คเกอร์ หรือตัวป้องกันต่างๆ ตัวป้องกันเหล่านี้มักถูกโจมตีโดยผู้เขียนมัลแวร์เพื่อหลบเลี่ยงการตรวจหา

- **แอพพลิเคชันที่อาจไม่ปลอดภัย** – หมายถึงซอฟต์แวร์เชิงพาณิชย์ที่ถูกต้องที่อาจถูกนำไปใช้ในทางที่ผิดเพื่อวัตถุประสงค์ที่เป็นอันตราย ตัวอย่างของแอพพลิเคชันที่อาจไม่ปลอดภัยประกอบด้วยเครื่องมือเข้าถึงระยะไกล แอพพลิเคชันที่พยายามค้นหารหัสผ่าน และเครื่องมือบันทึกการกดแป้นพิมพ์ (โปรแกรมที่บันทึกการใช้แป้นพิมพ์ของผู้ใช้) อ่านเพิ่มเติมเกี่ยวกับแอพพลิเคชันประเภทนี้ได้ใน ประมวลศัพท์



> **การป้องกันที่ปรับปรุง**
> ในตอนนี้ แมชชีนเลิร์นนิงขั้นสูงเป็นส่วนหนึ่งของการป้องกันในฐานะชั้นการป้องกันขั้นสูง ซึ่งช่วยปรับปรุงการตรวจหาโดยอิงจากแมชชีนเลิร์นนิง อ่านข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันประเภทนี้ใน ประมวลศัพท์

การตั้งค่าการรายงาน

เมื่อมีการตรวจหาเกิดขึ้น (เช่น ภัยคุกคามถูกพบและจัดประเภทเป็นมัลแวร์) ข้อมูลจะถูกบันทึกไปยัง บันทึกการตรวจหา และ การแจ้งเตือนบนเดสก์ท็อป จะเกิดขึ้นเมื่อถูกกำหนดค่าใน ESET NOD32 Antivirus

เกณฑ์การรายงานจะกำหนดค่าสำหรับแต่ละประเภท (เรียกว่า "ประเภท"):

1.การตรวจหามัลแวร์

2.แอพพลิเคชันที่อาจไม่พึงประสงค์

3.อาจไม่ปลอดภัย

4.แอพพลิเคชันที่น่าสงสัย

การรายงานจะทำงานด้วยกลไกการตรวจจับ รวมถึงองค์ประกอบการเรียนรู้ของเครื่อง คุณสามารถกำหนดเกณฑ์การรายงานที่สูงกว่าเกณฑ์ การป้องกัน ในปัจจุบันได้ การตั้งค่าการรายงานเหล่านี้ไม่ส่งผลกระทบต่อการปิดกั้น การกำจัด หรือการลบวัตถุ

โปรดอ่านข้อความต่อไปนี้ก่อนแก้ไขเกณฑ์ (หรือระดับ) สำหรับการรายงานประเภท:

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

ความพร้อมของโมดูลการป้องกัน ESET NOD32 Antivirus

ความพร้อม (เปิดใช้งาน หรือ ปิดใช้งาน) ของโมดูลการป้องกันสำหรับเกณฑ์ประเภทที่เลือกมีดังต่อไปนี้:

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

*ไม่แนะนำ

ระบุเวอร์ชันผลิตภัณฑ์ โมดูลโปรแกรม และวันที่สร้าง

1.คลิก **วิธีใช้และการสนับสนุน** > **เกี่ยวกับ ESET NOD32 Antivirus**
2.ในหน้าจอ **เกี่ยวกับ** บรรทัดแรกของข้อความจะแสดงหมายเลขเวอร์ชันของผลิตภัณฑ์ ESET ของคุณ
3.คลิก **องค์ประกอบที่ติดตั้ง** เพื่อเข้าถึงข้อมูลเกี่ยวกับโมดูลเฉพาะ

Keynotes

Keynotes จำนวนหนึ่งเมื่อตั้งค่าเกณฑ์ที่เหมาะสมสำหรับสภาพแวดล้อมของคุณ:

- เกณฑ์**สมดุล**เป็นที่แนะนำสำหรับการตั้งค่าส่วนใหญ่
- ยิ่งเกณฑ์การรายงานสูงเท่าใด อัตราการตรวจหาก็สูงเท่านั้น แต่ก็มีโอกาสที่จะเป็นวัตถุที่รายงานผิดพลาดได้มากกว่าเช่นเดียวกัน

• จากมุมมองของโลกแห่งความเป็นจริง ไม่มีการรับประกันอัตราการตรวจหา 100% เช่นเดียวกับที่มีโอกาส 0% ที่จะหลีกเลี่ยงไม่ให้มีการจัดประเภทวัตถุที่ไม่ติดไวรัสอย่างผิดๆ ว่าเป็นมัลแวร์

• ทำให้ ESET NOD32 Antivirus และโมดูลอัพเดทอยู่เสมอ เพื่อทำให้เกิดความสมดุลสูงสุด ระหว่างการทำงานและความถูกต้องของอัตราการตรวจหา และจำนวนวัตถุที่รายงานผิดพลาด

การตั้งค่าการป้องกัน

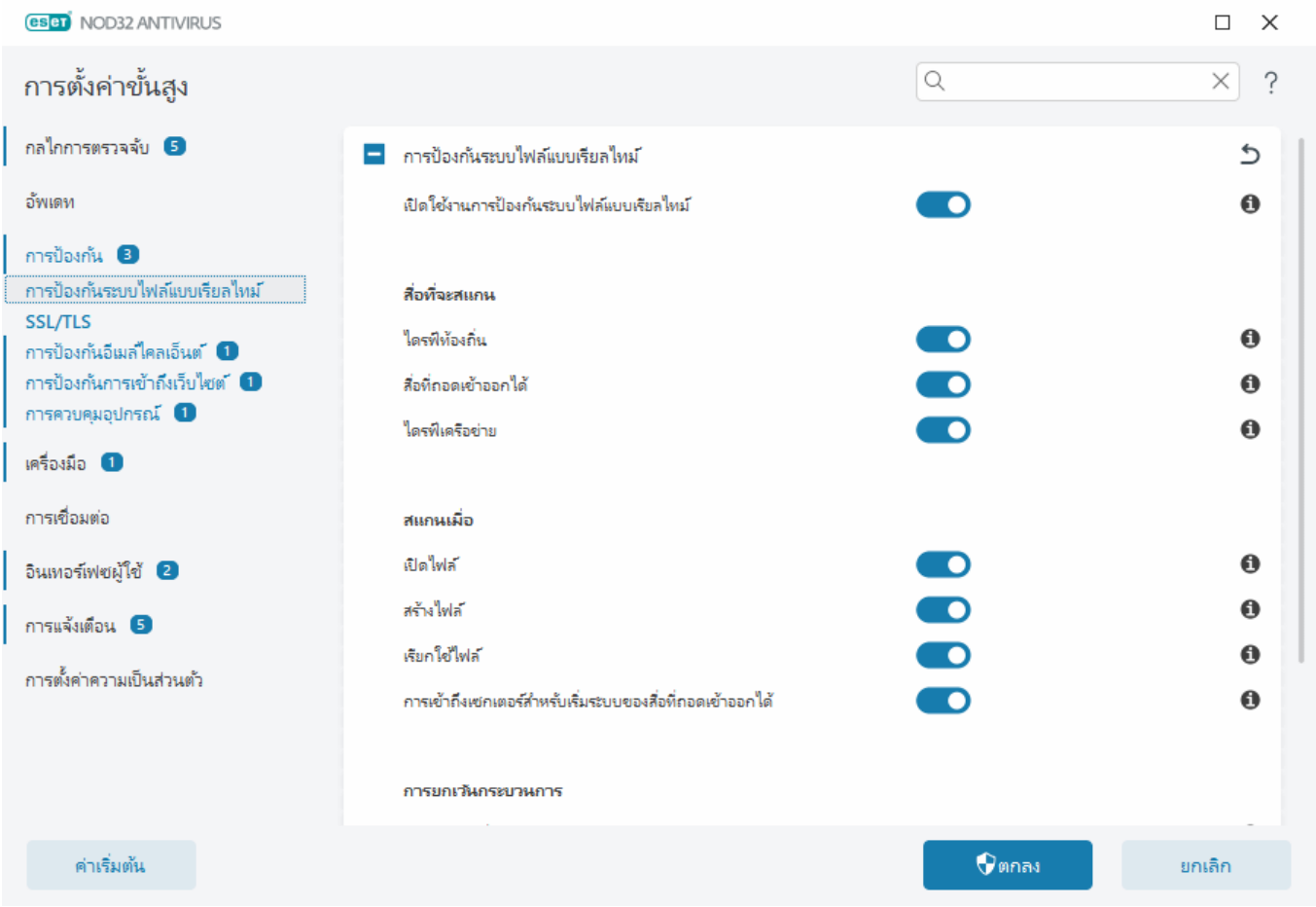
หากวัตถุที่ถูกจัดประเภทเป็นประเภทถูกรายงาน โปรแกรมจะปิดกั้นวัตถุและ กำจัด ลบ หรือย้ายวัตถุไปยัง การกักเก็บ

โปรดอ่านข้อความต่อไปนี้ก่อนแก้ไขเกณฑ์ (หรือระดับ) สำหรับการป้องกันประเภท:

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

การป้องกันระบบไฟล์แบบเรียลไทม์

การป้องกันระบบไฟล์แบบเรียลไทม์จะควบคุมไฟล์ทั้งหมดในระบบสำหรับรหัสที่เป็นอันตรายเมื่อเปิด สร้าง หรือเรียกใช้



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

สื่อที่จะสแกน

ตามค่าเริ่มต้น โปรแกรมจะสแกนสื่อทุกประเภทเพื่อหาสิ่งที่อาจเป็นภัยคุกคาม:

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

เราขอแนะนำให้คุณใช้การตั้งค่าเริ่มต้น และแก้ไขการตั้งค่าเฉพาะบางกรณีเท่านั้น เช่น เมื่อการสแกนสื่อบางชนิดทำให้การรับส่งข้อมูลช้าลงอย่างมาก

สแกนเมื่อ

ตามค่าเริ่มต้น ไฟล์ทั้งหมดจะถูกสแกนเมื่อเปิด สร้าง หรือดำเนินการ ขอแนะนำให้คุณคงการตั้งค่าเริ่มต้นเหล่านี้ไว้ เนื่องจากการตั้งค่าเหล่านี้จะให้การป้องกันแบบเรียลไทม์ในระดับสูงสุดสำหรับคอมพิวเตอร์ของคุณ:

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

การยกเว้นกระบวนการ

ดู การยกเว้นกระบวนการ

ThreatSense

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

เพื่อให้มีการใช้ทรัพยากรของระบบน้อยที่สุดเมื่อใช้การป้องกันระบบไฟล์แบบเรียลไทม์ ไฟล์ที่ผ่านการสแกนแล้วจะไม่มีการสแกนซ้ำอีก (ยกเว้นกรณีที่มีการแก้ไข) ไฟล์จะถูกสแกนอีกครั้งในทันทีหลังจากอัพเดทกลไกตรวจหาแต่ละครั้ง สามารถควบคุมการทำงานแบบนี้ได้ด้วยการใช้ **การเพิ่มประสิทธิภาพแบบสมาร์ท** หากปิดใช้งาน **การเพิ่มประสิทธิภาพแบบสมาร์ท** ไฟล์ทั้งหมดจะถูกสแกนในแต่ละครั้งที่มีการเข้าถึง หากต้องการแก้ไขการตั้งค่านี้ ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน**> **การป้องกันระบบไฟล์แบบเรียลไทม์** คลิก **ThreatSense** > **อื่น ๆ** แล้วเลือกหรือไม่เลือก **เปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท**

การป้องกันระบบไฟล์แบบเรียลไทม์ยังช่วยให้คุณสามารถกำหนดค่า พารามิเตอร์ ThreatSense เพิ่มเติม ได้

การยกเว้นกระบวนการ

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

อย่าสับสนกับ นามสกุลไฟล์ที่ยกเว้น การยกเว้น HIPS การตรวจหานามสกุลไฟล์ หรือ การตรวจหาการทำงาน

การยกเว้นกระบวนการจะช่วยลดความเสี่ยงของข้อขัดแย้งและที่อาจเกิดขึ้นได้และปรับปรุงประสิทธิภาพของแอพพลิเคชันที่ยกเว้น ซึ่งจะกลายเป็นผลกระทบด้านบวกกับประสิทธิภาพโดยรวมและความมั่นคงของระบบปฏิบัติการ ข้อยกเว้นของกระบวนการ / แอพพลิเคชันเป็นข้อยกเว้นของไฟล์ที่สามารถยกเว้นได้ (*.exe*)

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

คุณลักษณะนี้ได้รับการออกแบบมาเพื่อแยกเครื่องมือการสำรองข้อมูล การยกเว้นกระบวนการของเครื่องมือสำรองข้อมูลจากการสแกนจะไม่ใช่เพียงทำให้มั่นใจเรื่องความมั่นคงของระบบเท่านั้น แต่ยังจะไม่มีผลกระทบต่อประสิทธิภาพของการสำรองข้อมูล ซึ่งการสำรองจะไม่ทำงานช้าลงในขณะที่กำลังใช้งานอยู่

คลิก **แก้ไข** เพื่อเปิดหน้าต่างการจัดการ **ข้อยกเว้นของกระบวนการ** ที่คุณสามารถ เพิ่มข้อยกเว้นต่างๆ และเรียกใช้ไฟล์ที่สามารถยกเว้นได้ (ตัวอย่างเช่น *Backup-tool.exe*) ซึ่งจะแยกออกจากการสแกน เมื่อไฟล์ *.exe* ถูกเพิ่มไปยังข้อยกเว้นแล้ว กิจกรรมของกระบวนการนี้จะไม่ใช่ได้รับการตรวจสอบโดย ESET NOD32 Antivirus และจะไม่มีการสแกนเพื่อทำงานบนการปฏิบัติการของไฟล์ใดที่ดำเนินการโดยกระบวนการนี้

หากคุณไม่ใช้ฟังก์ชันเรียกดูเมื่อเลือกกระบวนการที่สามารถยกเว้นได้ คุณจำเป็นต้องป้อนพาธแบบเต็มให้เป็นแบบยกเว้นได้ด้วยตนเอง มิเช่นนั้น ข้อยกเว้นจะไม่ทำงานอย่างถูกต้องและ HIPS อาจรายงานข้อผิดพลาด

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

การป้องกันการเข้าถึงเว็บไซต์จะไม่พิจารณาให้เป็นข้อยกเว้น ดังนั้น หากคุณยกเว้นไฟล์ที่สามารถยกเว้นของเว็บเบราว์เซอร์ของคุณได้ ไฟล์ที่ดาวน์โหลดแล้วจะยังคงสแกนอยู่ วิธีนี้การแฝงตัวจะยังสามารถตรวจพบได้ สถานการณ์นี้เป็นเพียงตัวอย่างเท่านั้น และเราจะไม่แนะนำให้คุณสร้างข้อยกเว้นสำหรับเว็บเบราว์เซอร์

เพิ่มหรือแก้ไขกระบวนการการยกเว้น

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

เลือกพาธไฟล์ของแอพพลิเคชันที่ได้รับการยกเว้นโดยการคลิก... อย่าป้อนชื่อของแอพพลิเคชัน เมื่อไฟล์ *.exe* ถูกเพิ่มไปยังข้อยกเว้นแล้ว กิจกรรมของกระบวนการนี้จะไม่ใช่ได้รับการตรวจสอบโดย ESET NOD32 Antivirus และจะไม่มีการสแกนเพื่อทำงานบนการปฏิบัติการของไฟล์ใดที่ดำเนินการโดยกระบวนการนี้

หากคุณไม่ใช้ฟังก์ชันเรียกดูเมื่อเลือกกระบวนการที่สามารถยกเว้นได้ คุณจำเป็นต้องป้อนพาธแบบเต็มให้เป็นแบบยกเว้นได้ด้วยตนเอง มิเช่นนั้น ข้อยกเว้นจะไม่ทำงานอย่างถูกต้องและ HIPS อาจรายงานข้อผิดพลาด

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

เมื่อใดควรแก้ไขการกำหนดค่าการป้องกันแบบเรียลไทม์

การป้องกันแบบเรียลไทม์เป็นองค์ประกอบที่สำคัญที่สุดในการรักษาระบบที่ปลอดภัย โปรดระมัดระวังเมื่อแก้ไขพารามิเตอร์ทุกครั้ง เราขอแนะนำให้คุณแก้ไขพารามิเตอร์ในกรณีพิเศษเท่านั้น

หลังจากการติดตั้ง ESET NOD32 Antivirus การตั้งค่าทั้งหมดจะได้รับการเพิ่มประสิทธิภาพเพื่อให้การรักษาความปลอดภัยให้กับระบบในระดับสูงสุดสำหรับผู้ใช้ หากต้องการคืนค่าการตั้งค่าเริ่มต้น คลิก ↩ ถัดจาก การตั้งค่าขั้นสูง > **การป้องกัน** > **การตอบสนองการตรวจจับ**

การตรวจสอบการป้องกันแบบเรียลไทม์

เมื่อต้องการตรวจสอบว่าการป้องกันแบบเรียลไทม์กำลังทำงานและตรวจหาไวรัส ให้ใช้ไฟล์ทดสอบจาก *www.eicar.com* ไฟล์ทดสอบนี้เป็นไฟล์ที่ปลอดภัยซึ่งสามารถตรวจพบโดยโปรแกรมป้องกันไวรัสทุกประเภท ไฟล์นี้

สร้างขึ้นโดยบริษัท EICAR (European Institute for Computer Antivirus Research) เพื่อทดสอบการทำงานของโปรแกรมป้องกันไวรัส

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

ควรทำอย่างไรเมื่อการป้องกันแบบเรียลไทม์ไม่ทำงาน

ในบทนี้ เราจะอธิบายปัญหาที่อาจเกิดขึ้นเมื่อใช้การป้องกันแบบเรียลไทม์ และวิธีการแก้ปัญหาดังกล่าวด้วย

การป้องกันแบบเรียลไทม์ถูกปิดใช้งาน

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

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

ถ้าการป้องกันแบบเรียลไทม์ไม่พบหรือไม่กำจัดการแฝงตัว

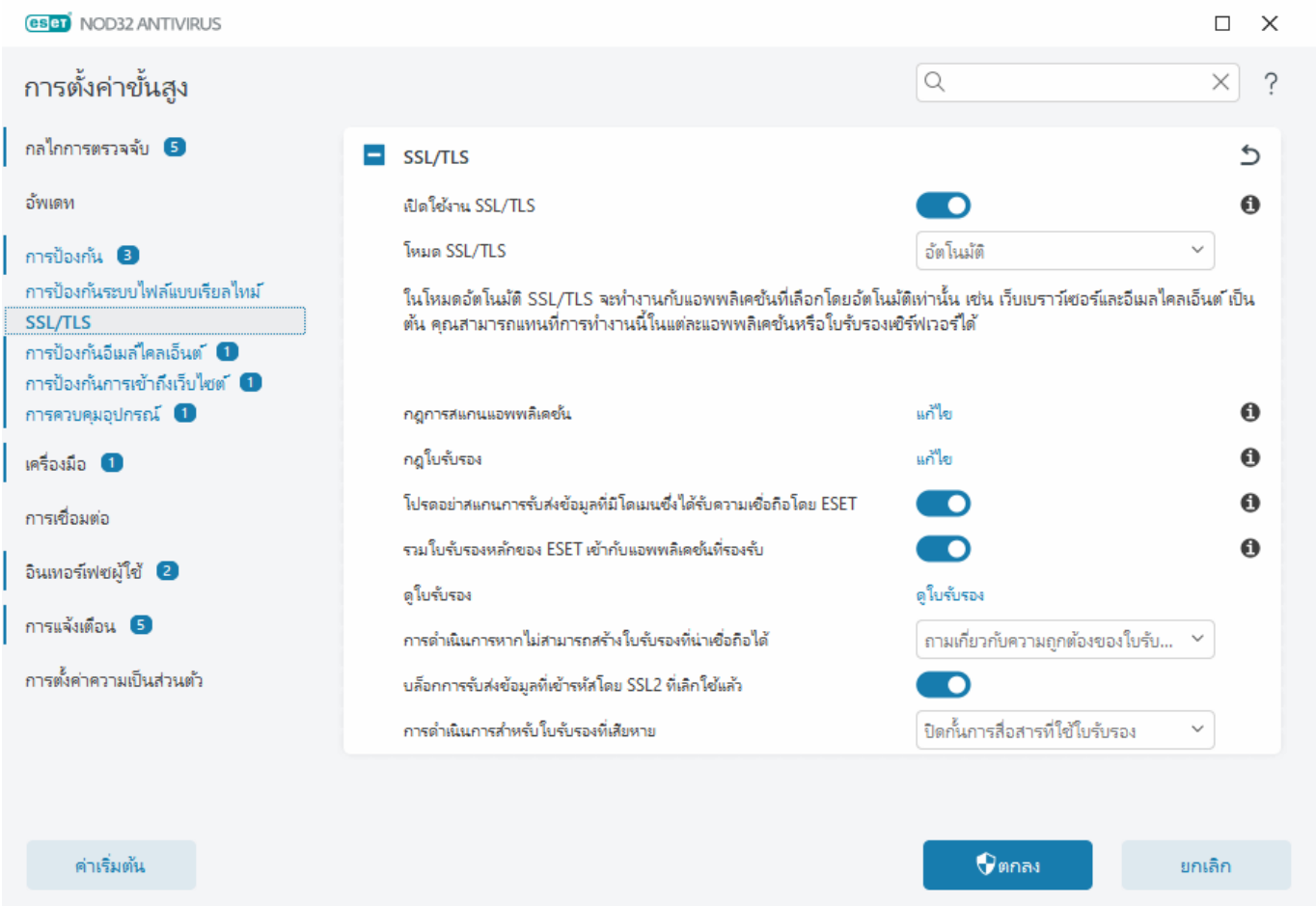
ตรวจสอบว่าไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอื่นในคอมพิวเตอร์ของคุณ หากโปรแกรมป้องกันไวรัสสองโปรแกรมถูกติดตั้งในเวลาเดียวกัน อาจเกิดความขัดแย้งขึ้นได้ ขอแนะนำให้คุณลบการติดตั้งโปรแกรมป้องกันไวรัสอื่นในระบบของคุณก่อนติดตั้ง ESET

การป้องกันแบบเรียลไทม์ไม่เริ่มต้นทำงาน

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

SSL/TLS

ESET NOD32 Antivirus สามารถตรวจสอบภัยคุกคามการสื่อสารที่ใช้โปรโตคอล SSL คุณสามารถใช้โหมดการกรองต่างๆ เพื่อตรวจสอบการสื่อสารที่ป้องกันด้วย SSL ด้วยใบรับรองที่เชื่อถือ ใบรับรองที่ไม่รู้จัก หรือใบรับรองที่ถูกยกเว้นจากการตรวจสอบของการสื่อสารที่ป้องกันด้วย SSL หากต้องการแก้ไขการตั้งค่า SSL/TLS ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **SSL/TLS**



เปิดใช้งานSSL/TLS – หากปิดใช้งาน ESET NOD32 Antivirus จะไม่สแกนการสื่อสารผ่าน SSL/TLS

โหมด SSL/TLS สามารถใช้งานได้ในตัวเลือกดังต่อไปนี้:

โหมดการกรอง	คำอธิบาย
อัตโนมัติ	โหมดเริ่มต้นจะสแกนเฉพาะแอพพลิเคชันที่เหมาะสมเท่านั้น เช่น เว็บเบราว์เซอร์และอีเมลไคลเอ็นต์ คุณสามารถแทนที่ได้โดยการเลือกแอพพลิเคชันที่มีการสแกนการสื่อสาร
แบบมีการโต้ตอบ	หากคุณเข้าสู่ไซต์ที่ป้องกันด้วย SSL ใหม่ (ที่มีใบรับรองที่ไม่รู้จัก) ระบบจะแสดงข้อความการเลือกการทำงาน โหมดนี้อนุญาตให้คุณสร้างรายการของใบรับรอง SSL / แอพพลิเคชันที่จะถูกยกเว้นจากการสแกน

โหมดการกรอง	คำอธิบาย
อ้างอิงตามนโยบาย	โหมดนโยบาย - เลือกตัวเลือกนี้เพื่อสแกนการสื่อสารที่ป้องกันด้วย SSL ทั้งหมด ยกเว้นการสื่อสารที่ป้องกันโดยใบรับรองที่ยกเว้นจากการตรวจสอบ ถ้ามีการสร้างการสื่อสารใหม่ที่ใช้ใบรับรองที่ไม่รู้จักและลงชื่อแล้ว คุณจะไม่ได้รับแจ้ง และการสื่อสารดังกล่าวจะถูกกรองโดยอัตโนมัติ เมื่อคุณเข้าถึงเซิร์ฟเวอร์ที่มีใบรับรองที่ไม่เชื่อถือ ซึ่งได้ทำเครื่องหมายไว้ว่าน่าเชื่อถือ (ใบรับรองดังกล่าวอยู่ในรายการใบรับรองที่เชื่อถือ) ระบบจะอนุญาตให้มีการสื่อสารกับเซิร์ฟเวอร์ และเนื้อหาของช่องทางการสื่อสารจะถูกกรอง

กฎการสแกนแอพพลิเคชัน – ช่วยให้คุณสามารถปรับแต่งการทำงานของ ESET NOD32 Antivirus สำหรับแอพพลิเคชันที่ต้องการได้

กฎการใบรับรอง – ช่วยให้คุณสามารถปรับแต่งการทำงานของ ESET NOD32 Antivirus สำหรับใบรับรอง SSL ที่ต้องการได้

อย่าสแกนการรับส่งข้อมูลผ่านโดเมนที่ ESET เชื่อถือได้ – เมื่อเปิดใช้งาน ระบบจะแยกการสื่อสารกับโดเมนที่เชื่อถือได้ออกจากการสแกน รายการที่อนุญาตในตัวที่จัดการโดย ESET จะใช้บ่งบอกถึงความน่าเชื่อถือของโดเมน

รวมใบรับรองหลักของ ESET เข้ากับแอพพลิเคชันที่รองรับ – เพื่อให้การสื่อสาร SSL ทำงานอย่างถูกต้องในเบราว์เซอร์/อีเมลไคลเอ็นต์ของคุณ จะต้องมีการเพิ่มใบรับรองหลักสำหรับ ESET ในรายการใบรับรองหลักที่รู้จัก (ผู้เผยแพร่) เมื่อเปิดใช้งาน ESET NOD32 Antivirus จะเพิ่มใบรับรอง ESET SSL Filter CA ลงในเบราว์เซอร์ที่รู้จักโดยอัตโนมัติ (ตัวอย่างเช่น Opera) สำหรับเบราว์เซอร์ที่ต้องใช้ที่เก็บใบรับรองของระบบ โปรแกรมจะเพิ่มใบรับรองโดยอัตโนมัติ ตัวอย่างเช่น Firefox จะกำหนดค่าการอนุญาต Trust Root ในที่เก็บใบรับรองของระบบโดยอัตโนมัติ

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

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

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

คุณสามารถเลือก **ปิดกั้นการสื่อสารที่ใช้ใบรับรอง** เพื่อสิ้นสุดการเชื่อมต่อที่เข้ารหัสไปยังไซต์ที่ใช้ใบรับรองที่ไม่ได้ยืนยันเสมอ

บล็อกการรับส่งข้อมูลที่เข้ารหัสโดย SSL2 ที่ล้าสมัย การสื่อสารโดยใช้ – โปรโตคอล SSL เวอร์ชันก่อนหน้าจะถูกบล็อกโดยอัตโนมัติ

การดำเนินการสำหรับใบรับรองที่เสียหาย – ใบรับรองที่เสียหายหมายถึงใบรับรองเป็นรูปแบบที่ ESET NOD32 Antivirus ไม่รู้จัก หรือได้รับความเสียหาย (ตัวอย่างเช่น ถูกเขียนทับโดยข้อมูลแบบสุ่ม) ในกรณีนี้ เราขอแนะนำให้ให้เลือก **ปิดกั้นการสื่อสารที่ใช้ใบรับรอง** ไว้ หากเลือก **สอบถามเกี่ยวกับความถูกต้องของใบรับรอง** ผู้ใช้จะได้รับข้อความเตือนให้เลือกการดำเนินการที่จะเกิดขึ้นเมื่อมีการสร้างการสื่อสารที่เข้ารหัส

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

กฎการสแกนแอพพลิเคชัน

กฎการสแกนแอพพลิเคชัน สามารถใช้เพื่อปรับแต่งพฤติกรรมของ ESET NOD32 Antivirus สำหรับแอพพลิเคชันบางแอพพลิเคชัน และจดจำการดำเนินการที่เลือกเมื่อ **โหมด SSL/TLS** อยู่ใน **โหมดโต้ตอบ** คุณสามารถดูและแก้ไขรายการได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **SSL/TLS** > **กฎการสแกนแอพพลิเคชัน** > **แก้ไข**

หน้าต่าง **กฎการสแกนแอพพลิเคชัน** ประกอบด้วยส่วนต่างๆ ต่อไปนี้:

คอลัมน์

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

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

องค์ประกอบการควบคุม

เพิ่ม – เพิ่มแอพพลิเคชันที่กรอง

แก้ไข – เลือกแอพพลิเคชันที่คุณต้องการกำหนดค่าแล้วคลิก **แก้ไข**

ลบออก – เลือกแอพพลิเคชันที่คุณต้องการลบแล้วคลิก **ลบออก**

นำเข้า/ส่งออก – นำเข้าแอพพลิเคชันจากไฟล์ หรือบันทึกรายการแอพพลิเคชันปัจจุบันของคุณลงในไฟล์

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

กฎใบรับรอง

กฎใบรับรอง สามารถใช้เพื่อปรับแต่งการทำงานของ ESET NOD32 Antivirus สำหรับใบรับรอง SSL บางรายการ และจดจำการดำเนินการที่เลือกเมื่อ **โหมด SSL/TLS** อยู่ใน **โหมดโต้ตอบ** คุณสามารถดูและแก้ไขรายการได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **SSL/TLS** > **กฎใบรับรอง** > **แก้ไข**

หน้าต่าง **กฎใบรับรอง** ประกอบด้วยส่วนต่างๆ ดังนี้:

คอลัมน์

ชื่อ – ชื่อของใบรับรอง

ผู้ออกใบรับรอง – ชื่อของผู้สร้างใบรับรอง

หัวเรื่องของใบรับรอง – ช่องหัวเรื่องระบุถึงเอนทิตีที่เกี่ยวข้องกับคีย์สาธารณะที่เก็บไว้ในช่องหัวเรื่องคีย์สาธารณะ

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

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

องค์ประกอบการควบคุม

เพิ่ม - เพิ่มใบรับรองใหม่แล้วปรับการตั้งค่าของใบรับรองเกี่ยวกับตัวเลือกในการเข้าถึงและการสแกน

แก้ไข – เลือกใบรับรองที่คุณต้องการกำหนดค่าแล้วคลิก **แก้ไข**

ลบ – เลือกใบรับรองที่คุณต้องการลบแล้วคลิก **ลบออก**

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

การรับส่งข้อมูลทางเครือข่ายที่เข้ารหัส

หากระบบของคุณได้รับการกำหนดค่าให้ใช้การสแกน SSL/TLS ระบบจะแสดงหน้าต่างข้อความให้คุณเลือกการดำเนินการปรากฏขึ้นมาในสองสถานการณ์ ได้แก่:

สถานการณ์แรก ถ้าเว็บไซต์ใช้ใบรับรองที่ไม่สามารถตรวจสอบได้หรือไม่ถูกต้อง และ ESET NOD32 Antivirus ได้รับการกำหนดค่าให้ถามผู้ใช้ในกรณีดังกล่าว (ตามค่าเริ่มต้น ใช่สำหรับใบรับรองที่ไม่สามารถตรวจสอบได้ ไม่สำหรับใบรับรองที่ไม่ถูกต้อง) กล่องข้อความจะถามคุณว่าคุณต้องการ **อนุญาต** หรือ **ปิดกั้น** การเชื่อมต่อนั้น หากใบรับรองไม่ได้อยู่ใน Trusted Root Certification Authorities store (TRCA) จึงสามารถพิจารณาได้ว่าไม่เชื่อถือ

สถานการณ์ที่สอง หาก**โหมด SSL/TLS** ถูกตั้งค่าเป็น **โหมดโต้ตอบ** กล่องข้อความของแต่ละเว็บไซต์จะถามว่าจะ **สแกน** หรือ **ละเว้น** การรับส่งข้อมูล บางแอพพลิเคชันตรวจสอบว่าการรับส่งข้อมูล SSL ของตนไม่ได้รับการแก้ไขหรือตรวจสอบจากผู้ใดเลย ในกรณีนี้ ESET NOD32 Antivirus ต้อง **ละเว้น** การรับส่งข้อมูลดังกล่าวและปล่อยให้แอพพลิเคชันทำงาน

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

ในทั้งสองกรณี ผู้ใช้สามารถเลือกที่จะจดจำการทำงานที่เลือกได้ การดำเนินการที่บันทึกไว้จะถูกเก็บไว้ใน กฎของใบรับรอง

การป้องกันอีเมลไคลเอ็นต์

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

- การป้องกันการส่งข้อมูลอีเมล
- การป้องกันกล่องจดหมาย

- ThreatSense

การป้องกันการส่งข้อมูลอีเมล

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

ESET NOD32 Antivirus มีการป้องกันโปรโตคอลเหล่านี้ โดยไม่พิจารณาถึงอีเมลไคลเอ็นต์ที่ใช้ และไม่ได้กำหนดให้ต้องกำหนดค่าอีเมลไคลเอ็นต์อีกครั้ง ตามค่าเริ่มต้น การติดต่อสื่อสารผ่านโปรโตคอล POP3 และ IMAP ทั้งหมดจะถูกสแกน โดยไม่คำนึงถึงค่าเริ่มต้นหมายเลขพอร์ต POP3/IMAP
โปรโตคอล MAPI ไม่ถูกสแกน อย่างไรก็ตาม การสื่อสารกับเซิร์ฟเวอร์ Microsoft Exchange สามารถสแกนได้โดยใช้ โมดูลการรวม ในอีเมลไคลเอ็นต์ เช่น Microsoft Outlook

> ESET NOD32 Antivirus ยังสนับสนุนการสแกนโปรโตคอล IMAPS (585, 993) และ POP3S (995) ที่จะใช้ช่องทางที่เข้ารหัสเพื่อโอนข้อมูลระหว่างเซิร์ฟเวอร์กับไคลเอ็นต์ ESET NOD32 Antivirus จะตรวจสอบการสื่อสารโดยใช้โปรโตคอล SSL (Secure Socket Layer) และ TLS (Transport Layer Security)
> การสื่อสารที่เข้ารหัสจะถูกสแกนตามค่าเริ่มต้น หากต้องการดูการตั้งค่าเครื่องมือสแกน ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > SSL/TLS

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

เปิดใช้งานการป้องกันการส่งข้อมูลอีเมล – เมื่อเปิดใช้งาน ESET NOD32 Antivirus จะสแกนการส่งข้อมูลอีเมล

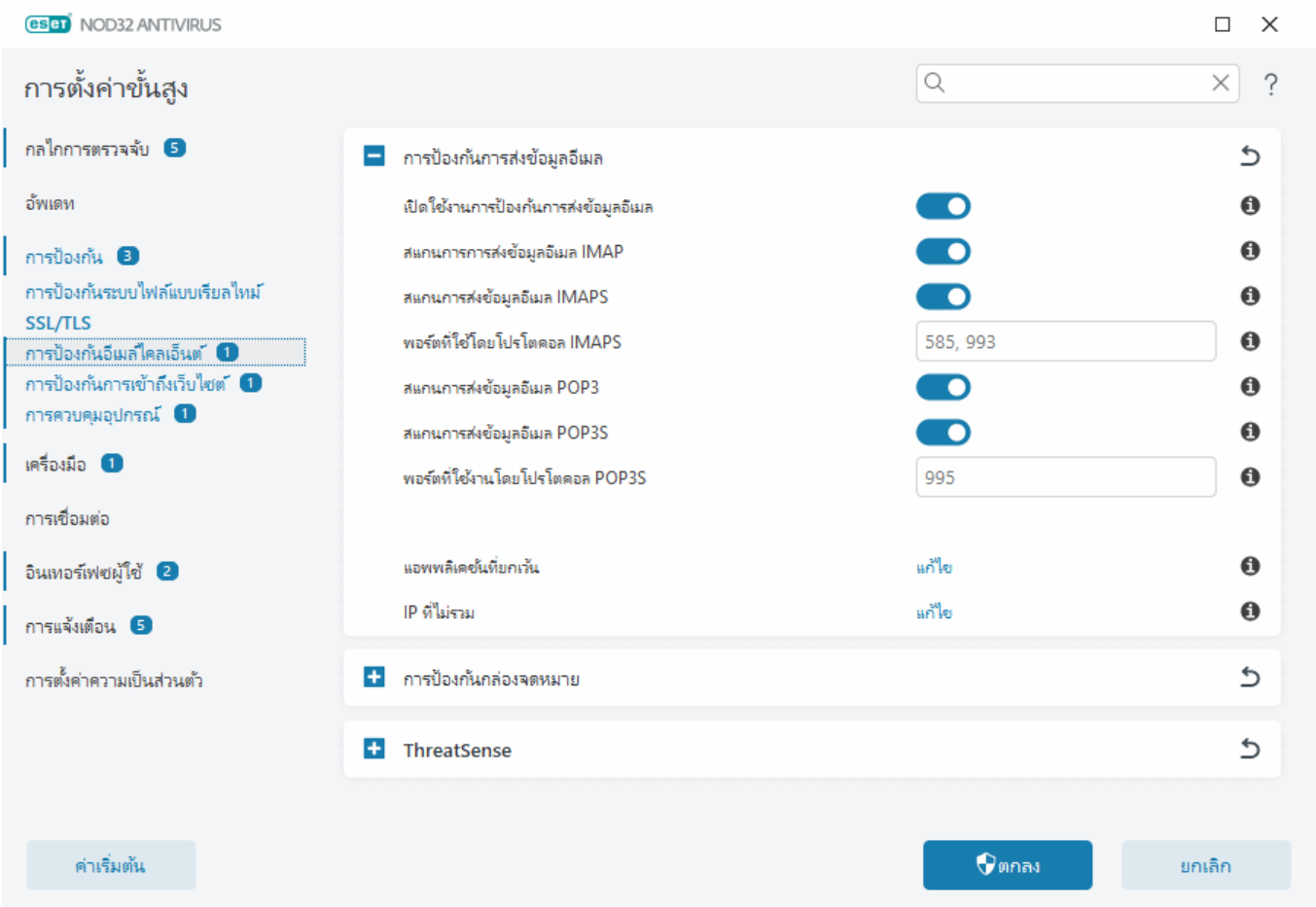
คุณสามารถเลือกโปรโตคอลการส่งจดหมายที่ต้องการสแกนได้โดยคลิกปุ่มสลับถัดจากตัวเลือกต่อไปนี้ (ระบบจะสแกนโปรโตคอลทั้งหมดตามค่าเริ่มต้น):

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

โดยค่าเริ่มต้น, ESET NOD32 Antivirus จะสแกนการส่งข้อมูลแบบ IMAPS และ POP3S บนพอร์ตมาตรฐาน หากต้องการเพิ่มพอร์ตที่กำหนดเองสำหรับโปรโตคอล IMAPS และ POP3S ให้เพิ่มพอร์ตเหล่านั้นลงในช่องถัดจาก **พอร์ตที่ใช้โดยโปรโตคอล IMAPS** หรือ **พอร์ตที่ใช้โดยโปรโตคอล POP3S** เลขที่พอร์ตหลายเลขที่ต้องคั่นด้วยเครื่องหมายคอมมา

แอพพลิเคชันที่ยกเว้น – ช่วยให้คุณสามารถแยกแอพพลิเคชันบางแอพออกจากการสแกนโดยฟีเจอร์การป้องกันการส่งข้อมูลอีเมลได้ ซึ่งจะมีประโยชน์เมื่อการป้องกันการเข้าถึงเว็บไซต์ทำให้เกิดปัญหาด้านความเข้ากันได้

IP ที่ยกเว้น – ช่วยให้คุณสามารถแยกที่อยู่ระยะไกลที่ต้องการออกจากการสแกนโดยการป้องกันการส่งข้อมูลอีเมล ซึ่งจะมีประโยชน์เมื่อการป้องกันการเข้าถึงเว็บไซต์ทำให้เกิดปัญหาด้านความเข้ากันได้



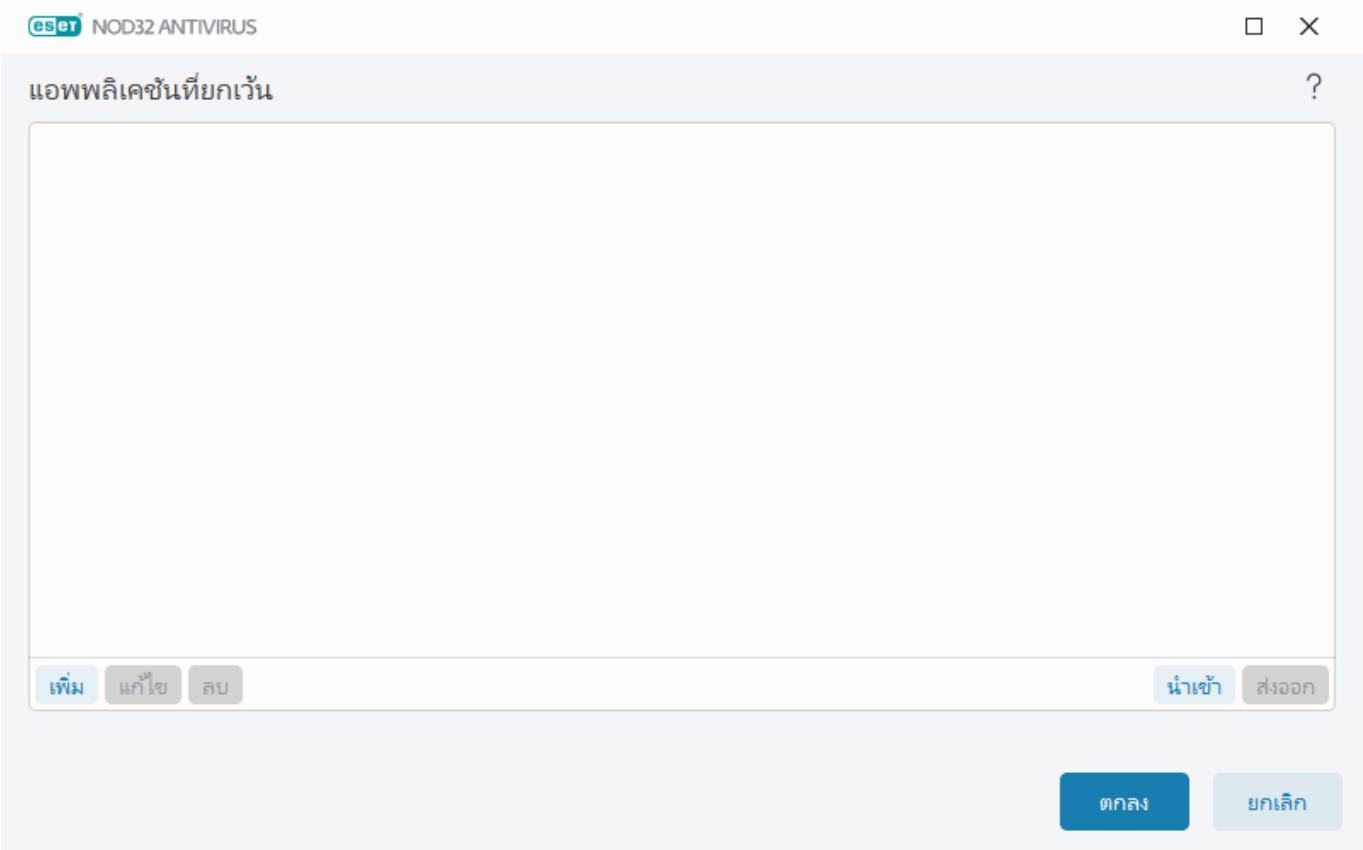
แอพพลิเคชันที่ยกเว้น

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

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

แก้ไข – แก้ไขรายการที่เลือกจากรายการ

ลบออก – ลบรายการที่เลือกออกจากรายการ



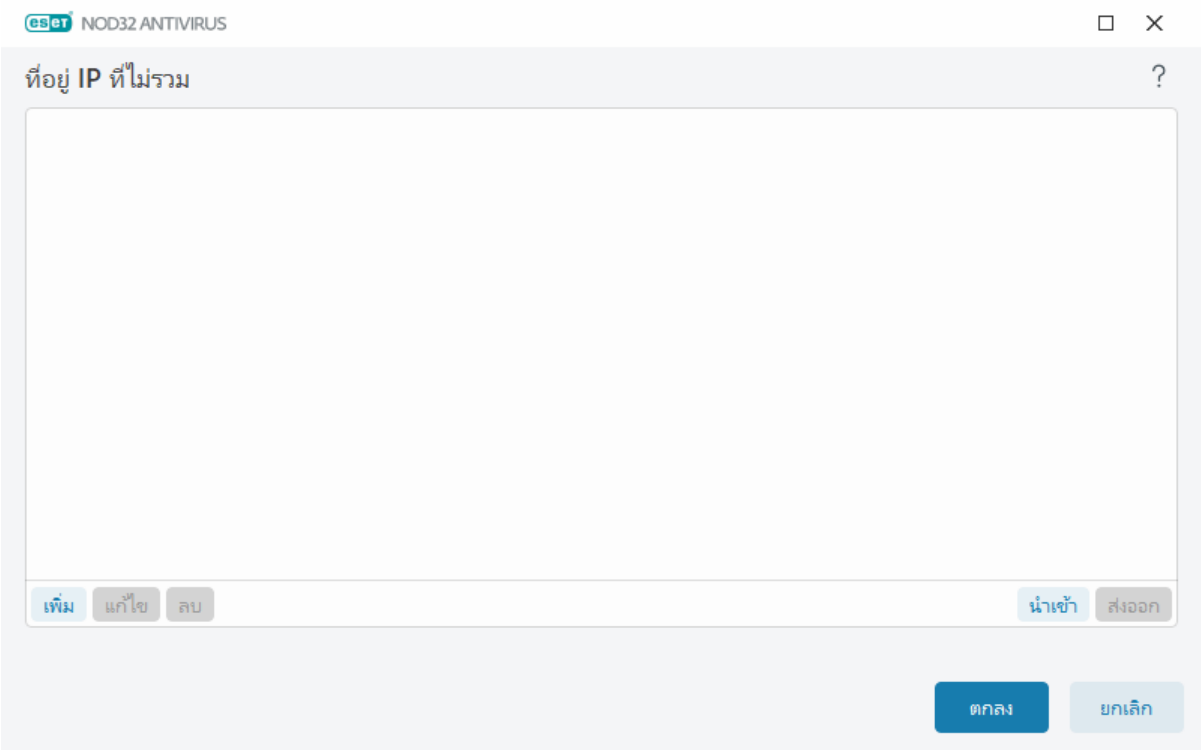
IP ที่ไม่รวม

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

คลิก **เพิ่ม** เพื่อยกเว้นที่อยู่ IP/ช่วงของที่อยู่/ซับเน็ตของจุดเชื่อมต่อระยะไกล

คลิก **แก้ไข** เพื่อเปลี่ยนที่อยู่ IP ที่เลือก

คลิก**ลบออก** เพื่อลบรายการที่เลือกออกจากรายการ



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

การป้องกันกล่องจดหมาย

การผสานการทำงาน ESET NOD32 Antivirus กับกล่องจดหมายจะเพิ่มระดับการป้องกันโค้ดที่เป็นอันตรายในข้อความอีเมล

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

เปิดใช้งานการปกป้องอีเมลโดยปลั๊กอินไคลเอ็นต์ – เมื่อปิดใช้งาน การป้องกันโดยอีเมลปลั๊กอินไคลเอ็นต์จะปิด

เลือกอีเมลที่จะสแกน:

- **อีเมลที่ได้รับ**

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

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

การปรับการจัดการสิ่งที่แนบมาให้เหมาะสม – หากคุณได้ปิดใช้งานการปรับให้เหมาะสมไว้ ระบบจะสแกนสิ่งที่แนบมาโดยทันที คุณอาจประสบกับประสิทธิภาพการทำงานของอีเมลไคลเอ็นต์ที่ช้าลง

การผสานการทำงาน – ช่วยให้คุณสามารถผสานการป้องกันกล่องจดหมายเข้ากับอีเมลไคลเอ็นต์ของคุณได้ ดูข้อมูลเพิ่มเติมได้ที่ การผสานการทำงาน

การตอบสนอง – ช่วยให้คุณปรับแต่งการจัดการข้อความสแปมได้ ดูรายละเอียดเพิ่มเติมได้ที่ การตอบสนอง

การรวม

การรวม ESET NOD32 Antivirus กับอีเมลไคลเอ็นต์ของคุณจะเพิ่มระดับการป้องกันรหัสที่เป็นอันตรายในข้อความอีเมล หากอีเมลไคลเอ็นต์ของคุณได้รับการรองรับ คุณสามารถเปิดใช้งานการรวมใน ESET NOD32 Antivirus ได้ เมื่อรวมเข้าอีเมลไคลเอ็นต์ของคุณ แถบเครื่องมือของ ESET NOD32 Antivirus จะถูกแทรกลงในอีเมลไคลเอ็นต์ โดยตรง ซึ่งจะทำให้การป้องกันอีเมลมีประสิทธิภาพมากยิ่งขึ้น เมื่อต้องการแก้ไขการตั้งค่าการผสานการทำงาน ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันอีเมลไคลเอ็นต์** > **การป้องกันกล่องจดหมาย** > **การผสานการทำงาน**

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

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

แถบเครื่องมือ Microsoft Outlook

การป้องกัน Microsoft Outlook ทำงานเป็นโมดูลปลั๊กอิน หลังจากติดตั้ง ESET NOD32 Antivirus แล้ว แถบเครื่องมือนี้จะได้รับการป้องกันไวรัส ลงใน Microsoft Outlook:

ESET NOD32 Antivirus – ดับเบิลคลิกที่ไอคอนเพื่อเปิดหน้าต่างหลักของ ESET NOD32 Antivirus

สแกนข้อความซ้ำ – ช่วยให้คุณสามารถเริ่มต้นการตรวจสอบอีเมลด้วยตนเองได้ คุณสามารถระบุข้อความที่จะตรวจสอบ และคุณสามารถเปิดใช้การสแกนซ้ำอีเมลที่ได้รับ ดูข้อมูลเพิ่มเติมได้ที่ การป้องกันกล่องจดหมาย

การตั้งค่าเครื่องมือสแกน – แสดงตัวเลือกการตั้งค่า การป้องกันกล่องจดหมาย

ข้อความยืนยัน

การแจ้งเตือนนี้จะทำหน้าที่ตรวจสอบว่าผู้ใช้ต้องการดำเนินการที่เลือกจริงหรือไม่ ซึ่งจะช่วยป้องกันการดำเนินการผิดพลาดได้

แต่ในหน้าต่างข้อความนี้จะมีตัวเลือกเพื่อปิดใช้การยืนยันอยู่ด้วย

สแกนข้อความซ้ำ

แถบเครื่องมือของ ESET NOD32 Antivirus ที่รวมอยู่ในอีเมลไคลเอ็นต์จะช่วยให้ผู้ใช้สามารถระบุตัวเลือกต่างๆ สำหรับการตรวจสอบอีเมลได้ ตัวเลือก **สแกนข้อความซ้ำ** มีโหมดการสแกนอยู่สองโหมด:

ข้อความทั้งหมดในโฟลเดอร์ปัจจุบัน – สแกนข้อความในโฟลเดอร์ที่แสดงอยู่ในปัจจุบัน

เฉพาะข้อความที่เลือก – สแกนเฉพาะข้อความที่ผู้ใช้ทำเครื่องหมายเท่านั้น

ช่องทำเครื่องหมาย **สแกนข้อความที่สแกนแล้วซ้ำ** จะมีตัวเลือกให้ผู้ใช้สามารถเรียกใช้การสแกนข้อความที่ได้สแกนแล้วก่อนหน้านี้

การตอบกลับ

ESET NOD32 Antivirus สามารถย้ายข้อความที่สแกนหรือเพิ่มข้อความที่กำหนดเองไปยังหัวเรื่องได้ โดยขึ้นอยู่กับผลการสแกนข้อความ คุณสามารถกำหนดการตั้งค่าเหล่านี้ได้ใน การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันอีเมลไคลเอ็นต์** > **การป้องกันกล่องจดหมาย** > **การตอบกลับ**

หากมีข้อความที่มีการพบไวรัส โดยค่าเริ่มต้น ESET NOD32 Antivirus จะพยายามกำจัดไวรัสในข้อความดังกล่าว หากไม่สามารถกำจัดไวรัสในข้อความได้ คุณสามารถเลือก **การดำเนินการหากไม่สามารถกำจัดไวรัสได้** จากตัวเลือกต่อไปนี้:

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

โฟลเดอร์ – ระบุโฟลเดอร์แบบกำหนดเองที่คุณต้องการย้ายอีเมลที่ติดไวรัสเมื่อตรวจพบ

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

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

อัพเดทหัวเรื่องอีเมลที่ได้รับและอ่านแล้ว/ อัพเดทหัวเรื่องของอีเมลที่ส่งแล้ว – เปิดใช้งานตัวเลือกนี้เพื่อเพิ่มข้อความที่กำหนดเองที่ระบุไว้ด้านล่างลงในข้อความ

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

ThreatSense

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

ตัวเลือกการตั้งค่าของเทคโนโลยี ThreatSense ช่วยให้ผู้ใช้สามารถระบุพารามิเตอร์การสแกนต่างๆ ได้:

- ประเภทไฟล์และนามสกุลที่จะสแกน
- การใช้วิธีการตรวจหาต่างๆ ร่วมกัน
- ระดับการกำจัด เป็นต้น

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

- การป้องกันระบบไฟล์แบบเรียลไทม์
- การสแกนขณะอยู่ในสถานะไม่ใช้งาน
- การสแกนเมื่อเริ่มต้น
- การป้องกันเอกสาร
- การป้องกันอีเมลไคลเอ็นต์

- การป้องกันการเข้าถึงเว็บ
- การสแกนคอมพิวเตอร์

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

วัตถุที่จะสแกน

ส่วนนี้จะช่วยให้คุณสามารถกำหนดว่าจะสแกนหาการแฝงตัวจากองค์ประกอบและไฟล์คอมพิวเตอร์ใด

หน่วยความจำที่ใช้งาน – สแกนหาภัยคุกคามที่โจมตีหน่วยความจำที่ใช้งานของระบบ

ส่วนการบูต/UEFI – การสแกนบูตเซคเตอร์สำหรับมัลแวร์ที่มีอยู่ในบันทึกการบูตหลัก [อ่านเพิ่มเติมเกี่ยวกับ UEFI ในประมวลศัพท์]

ไฟล์อีเมล – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: DBX (Outlook Express) และ EML

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

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

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

ตัวเลือกการสแกน

เลือกวิธีที่ใช้เมื่อสแกนหาการแฝงตัวบนระบบ ตัวเลือกที่ใช้ได้มีดังนี้:

การวิเคราะห์พฤติกรรม – การวิเคราะห์พฤติกรรมเป็นอัลกอริทึมที่วิเคราะห์การทำงาน (ที่เป็นอันตราย) ของโปรแกรม ข้อได้เปรียบสำคัญของเทคโนโลยีนี้คือความสามารถในการระบุซอฟต์แวร์ที่เป็นอันตรายซึ่งไม่มีอยู่ก่อนหน้า

นั้น หรือไม่เป็นที่รู้จักของกลไกตรวจหาก่อนหน้า ข้อเสียคือมีโอกาสที่จะเกิดการเตือนผิดพลาด (แม้จะน้อยมากก็ตาม)

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

การกำจัด

การตั้งค่าการกำจัด จะเป็นตัวกำหนดการทำงานของ ESET NOD32 Antivirus ขณะกำจัดวัตถุ การกำจัดมี 4 ระดับ:

ThreatSense มีระดับการปรับปรุงแก้ไข (เช่น การกำจัด) ดังต่อไปนี้

การปรับปรุงแก้ไขใน ESET NOD32 Antivirus

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

การยกเว้น

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่า ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะสแกน

อื่นๆ

เมื่อกำหนดค่าพารามิเตอร์กลไก ThreatSenseสำหรับการสแกนคอมพิวเตอร์ตามต้องการ จะสามารถใช้ตัวเลือกในส่วน **อื่นๆ** ได้ดังต่อไปนี้:

สแกนสตรีมข้อมูลสำรอง (ADS) – สตรีมข้อมูลสำรองที่ใช้งานโดยระบบไฟล์ NTFS เป็นการเชื่อมโยงไฟล์และโฟลเดอร์ซึ่งจะไม่ปรากฏสำหรับเทคนิคการสแกนทั่วไป การแฝงตัวจำนวนมากพยายามหลีกเลี่ยงการตรวจหานี้ โดยปลอมแปลงตัวเองเป็นสตรีมข้อมูลสำรอง

เรียกใช้การสแกนเบื้องหลังโดยมีลำดับความสำคัญต่ำ – ลำดับการสแกนแต่ละลำดับจะใช้ทรัพยากรของระบบจำนวนหนึ่ง หากคุณทำงานกับโปรแกรมที่ใช้ทรัพยากรระบบจำนวนมาก คุณสามารถเปิดใช้การสแกนเบื้องหลังที่มีลำดับความสำคัญต่ำ และประหยัดทรัพยากรไว้สำหรับแอพพลิเคชันของคุณ

บันทึกวัตถุทั้งหมด – บันทึกการสแกน จะแสดงไฟล์ที่สแกนแล้วทั้งหมดในอาร์ไคฟ์ที่ขยายในตัว รวมถึงไฟล์ที่ไม่ติดไวรัส (อาจสร้างข้อมูลบันทึกการสแกนจำนวนมากและเพิ่มขนาดไฟล์บันทึกการสแกน)

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

เก็บบันทึกการลงเวลาเข้าถึงล่าสุด – เลือกตัวเลือกนี้เพื่อเก็บเวลาแรกเริ่มที่เข้าถึงไฟล์ที่สแกนแทนการอัพเดทเวลาเหล่านั้น (ตัวอย่างเช่น สำหรับใช้กับระบบสำรองข้อมูล)

ขีดจำกัด

ส่วนขีดจำกัดช่วยให้คุณสามารถระบุขนาดสูงสุดของวัตถุ และระดับของอาร์ไคฟ์ที่ซ้อนที่จะสแกน:

การตั้งค่าวัตถุ

ขนาดวัตถุสูงสุด – กำหนดขนาดสูงสุดของวัตถุที่จะสแกน โมดูลป้องกันไวรัสที่กำหนดจะสแกนเฉพาะวัตถุที่เล็กกว่าขนาดที่ระบุเท่านั้น ผู้ที่สามารถแก้ไขตัวเลือกนี้ควรเป็นผู้ใช้ขั้นสูง ซึ่งอาจมีเหตุผลบางอย่างสำหรับการยกเว้นวัตถุขนาดใหญ่จากการสแกน ค่าเริ่มต้น: ไม่จำกัด

เวลาสแกนสูงสุดสำหรับวัตถุ (วินาที) – กำหนดค่าสูงสุดสำหรับสแกนไฟล์ในวัตถุที่มีการบรรจุ (เช่น อาร์ไคฟ์ RAR/ZIP หรืออีเมลที่มีไฟล์แนบหลายรายการ) การตั้งค่านี้จะไม่ถูกปรับใช้สำหรับไฟล์สแตนด์อโลน การสแกนจะหยุดทันทีหากมีการป้อนค่าที่ผู้ใช้กำหนดและพ้นระยะเวลาดังกล่าว โดยไม่คำนึงว่าการสแกนแต่ละไฟล์ในวัตถุที่มีการบรรจุจะเสร็จสิ้นแล้วหรือไม่

ในกรณีที่อาร์ไคฟ์บรรจุไฟล์ขนาดใหญ่ การสแกนจะหยุดช้ากว่าไฟล์ที่ถูกดึงข้อมูลจากอาร์ไคฟ์ (ตัวอย่างเช่น เมื่อตัวแปรที่ผู้ใช้กำหนดคือ 3 วินาที แต่การดึงข้อมูลของไฟล์คือ 5 วินาที) ไฟล์ที่เหลือในอาร์ไคฟ์จะไม่ถูกสแกนเมื่อพ้นระยะเวลาดังกล่าว

หากต้องการจำกัดเวลาในการสแกน ซึ่งรวมถึงอาร์ไคฟ์ขนาดใหญ่ ให้ใช้ **ขนาดวัตถุสูงสุด** และ **ขนาดไฟล์สูงสุดในอาร์ไคฟ์** (ไม่แนะนำให้ใช้เนื่องจากความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นได้)

ค่าเริ่มต้น: ไม่จำกัด

ตั้งค่าการสแกนอาร์ไคฟ์

ระดับการซ้อนของอาร์ไคฟ์ – ระบุความลึกสูงสุดของการสแกนอาร์ไคฟ์ ค่าเริ่มต้น: 10

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

> i เราไม่แนะนำให้แก้ไขค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดที่จะต้องแก้ไขค่านี้ในสถานการณ์ปกติ

การป้องกันการเข้าถึงเว็บ

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

เปิดใช้งานการป้องกันการเข้าถึงเว็บ – เมื่อปิดใช้งาน จะไม่มีการเรียกใช้การป้องกันการเข้าถึงเว็บไซต์และการป้องกันฟิชชิ่ง

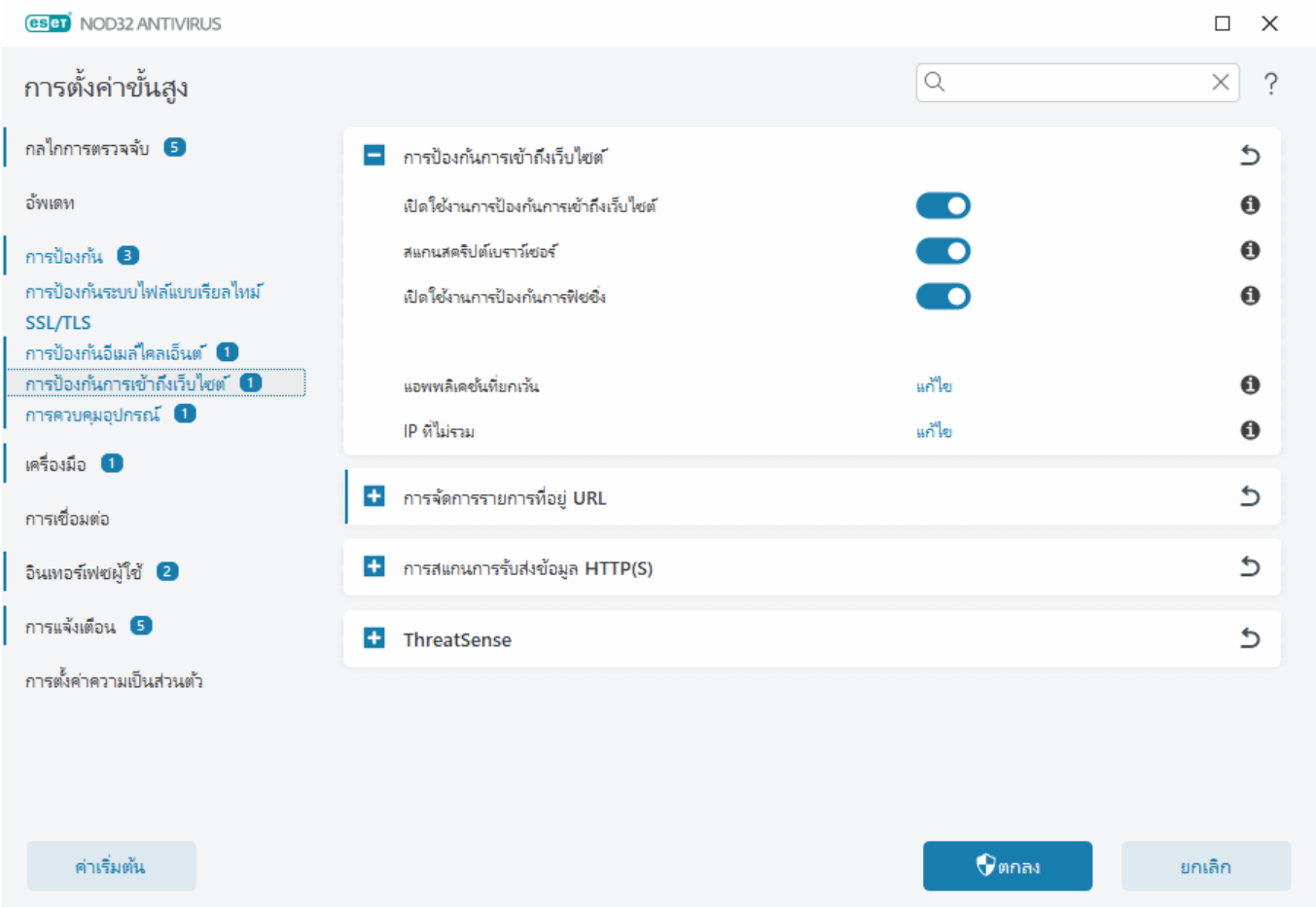
> i เราขอแนะนำให้คุณเปิดใช้งานการป้องกันการเข้าถึงเว็บไซต์และไม่ยกเว้นแอพพลิเคชันหรือที่อยู่ IP ตามค่าเริ่มต้นใดๆ

สแกนสคริปต์เบราว์เซอร์ – เมื่อเปิดใช้งาน กลไกการตรวจจับจะตรวจสอบโปรแกรม JavaScript ทั้งหมดที่เรียกใช้โดยเว็บเบราว์เซอร์

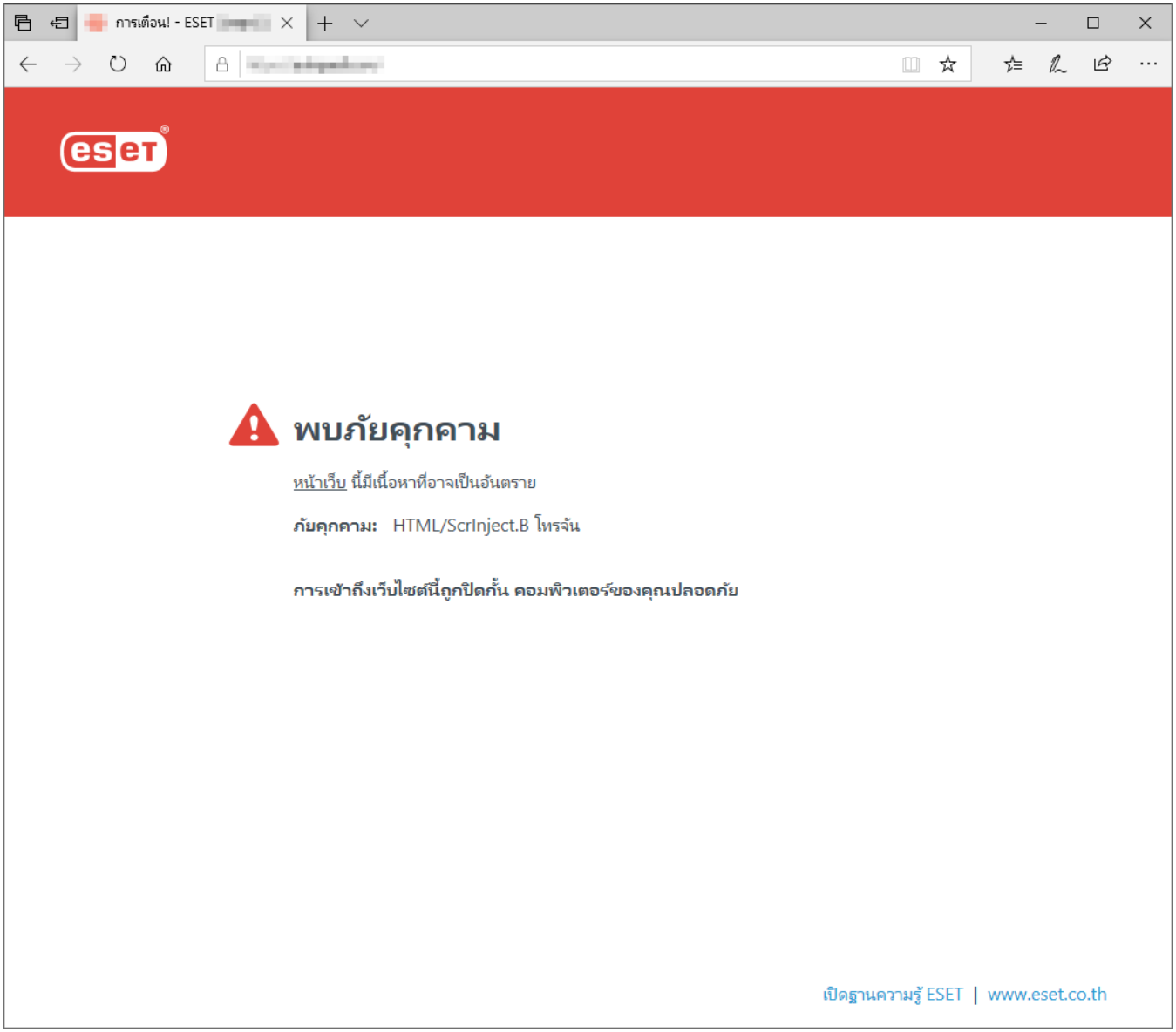
เปิดใช้งานการป้องกันฟิชชิ่ง – เมื่อเปิดใช้งาน หน้าเว็บฟิชชิ่งจะถูกบล็อก โปรดดู การป้องกันการฟิชชิ่ง สำหรับข้อมูลเพิ่มเติม

แอพพลิเคชันที่ยกเว้น – ช่วยให้คุณสามารถแยกแอพพลิเคชันบางแอพออกจากการสแกนโดยฟีเจอร์การป้องกันการเข้าถึงเว็บไซต์ได้ ซึ่งจะมีประโยชน์เมื่อการป้องกันการเข้าถึงเว็บไซต์ทำให้เกิดปัญหาความเข้ากันได้

IP ที่ยกเว้น – ช่วยให้คุณสามารถแยกที่อยู่ระยะไกลที่ต้องการออกจากการสแกนโดยการป้องกันการเข้าถึงเว็บไซต์ ซึ่งมีประโยชน์เมื่อการป้องกันการเข้าถึงเว็บไซต์ทำให้เกิดปัญหาความเข้ากันได้



การป้องกันการเข้าถึงเว็บไซต์จะแสดงข้อความต่อไปนี้ในเบราว์เซอร์ของคุณเมื่อเว็บไซต์ถูกปิดกั้น:



คำแนะนำพร้อมภาพประกอบ

บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:

- ยกเว้นเว็บไซต์ที่ปลอดภัยไม่ให้ถูกบล็อกโดยการป้องกันการเข้าถึงเว็บไซต์
- บล็อกเว็บไซต์ที่ใช้ ESET NOD32 Antivirus

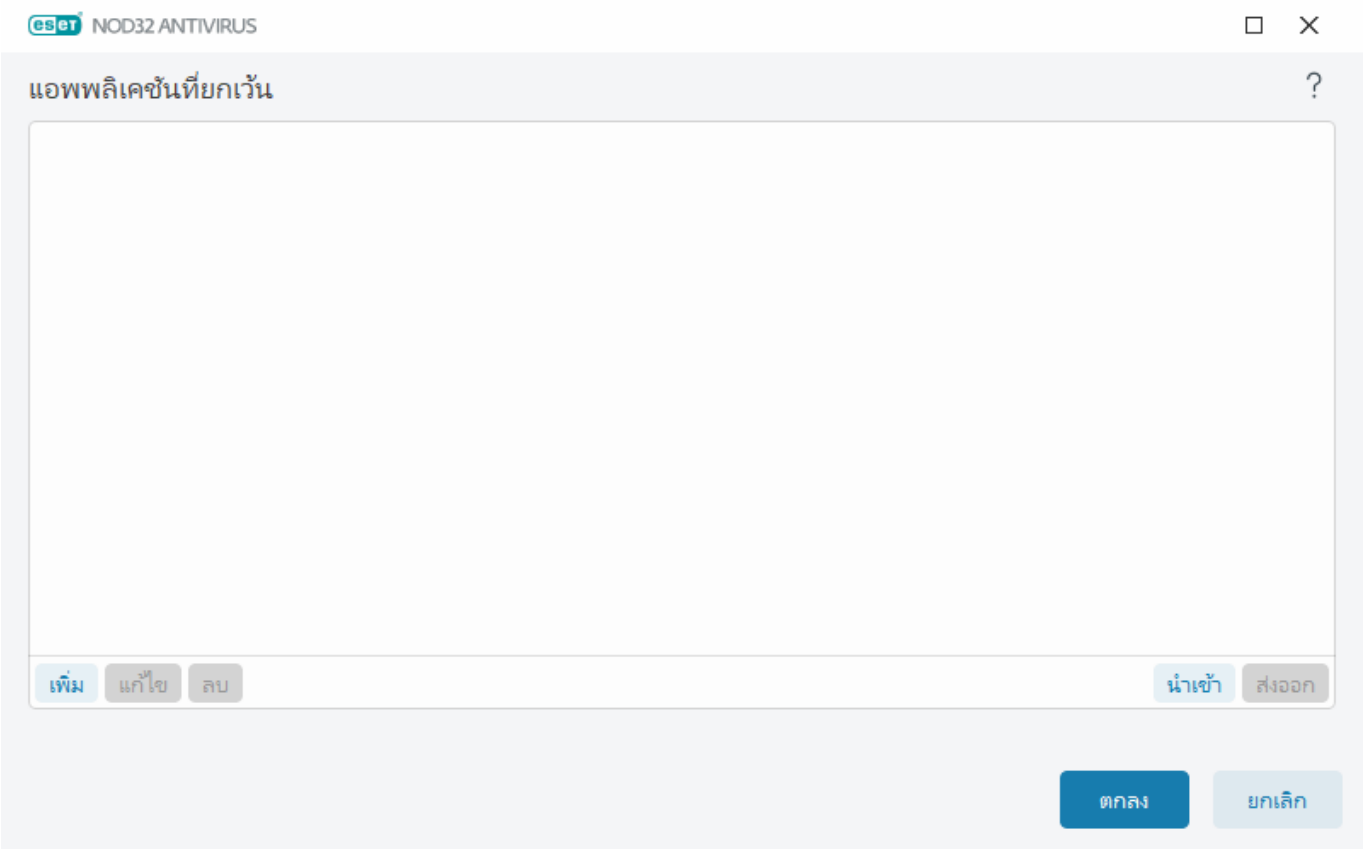
แอพพลิเคชันที่ยกเว้น

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

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

แก้ไข – แก้ไขรายการที่เลือกจากรายการ

ลบออก – ลบรายการที่เลือกออกจากรายการ



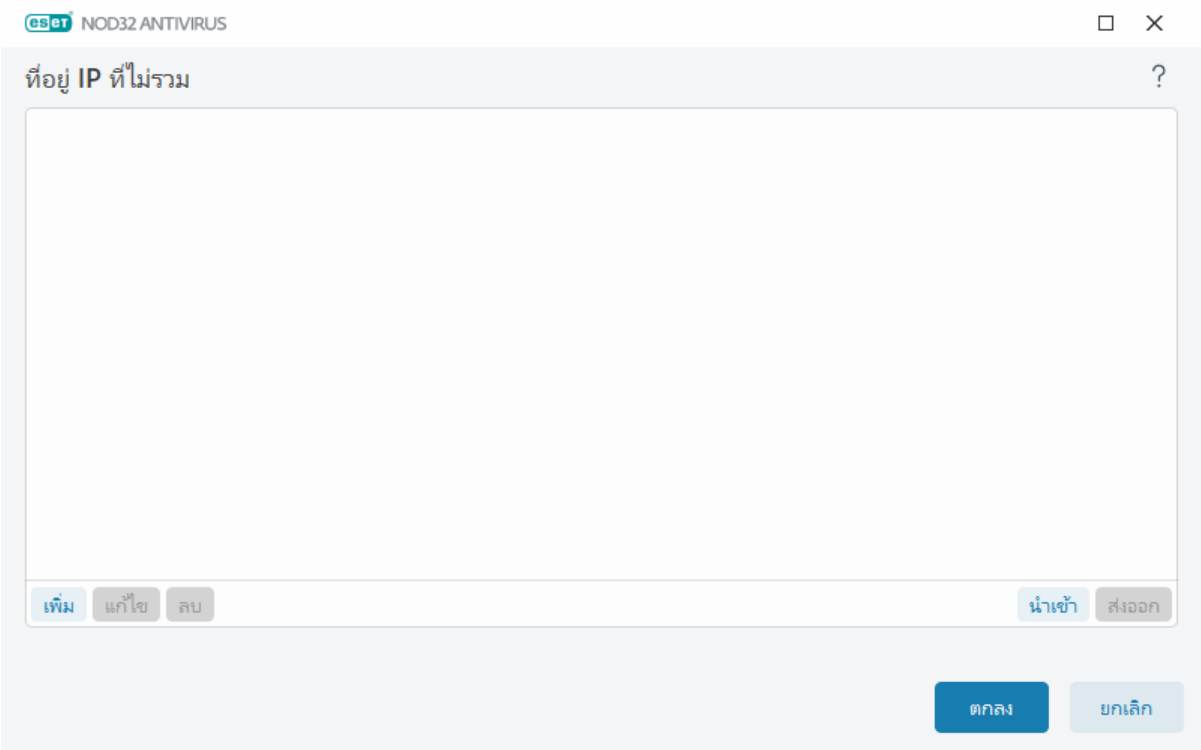
IP ที่ไม่รวม

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

คลิก **เพิ่ม** เพื่อยกเว้นที่อยู่ IP/ช่วงของที่อยู่/ซับเน็ตของจุดเชื่อมต่อระยะไกล

คลิก **แก้ไข** เพื่อเปลี่ยนที่อยู่ IP ที่เลือก

คลิก**ลบออก** เพื่อลบรายการที่เลือกออกจากรายการ



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

การจัดการรายการที่อยู่ URL

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

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

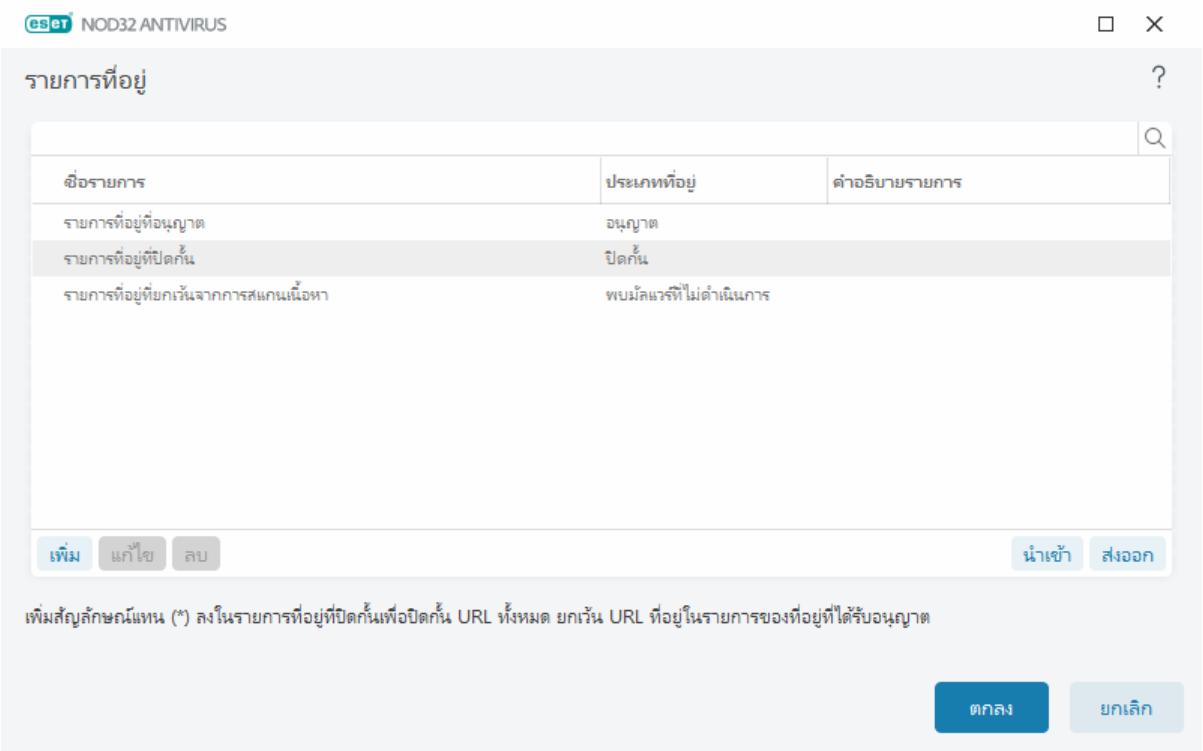
เว็บไซต์ใน **รายการที่อยู่ที่ปิดกั้น** จะไม่สามารถเข้าถึงได้เว้นแต่จะอยู่ใน **รายการที่อยู่ที่อนุญาต** ด้วยเช่นกัน เว็บไซต์ใน **รายการที่อยู่ที่ยกเว้นจากการสแกนเนื้อหา** จะไม่ถูกสแกนหารหัสที่เป็นอันตรายเมื่อเข้าถึง

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

อยู่ที่ปิดกั้น ที่ใช้งาน

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

> ที่อยู่ที่ ESET เชื่อถือ
> หากเปิดใช้งาน **อย่าสแกนการรับส่งข้อมูลผ่านโดเมนที่ ESET เชื่อถือ** ใน SSL/TLS ไว้ โดเมนในรายการที่อนุญาตที่ ESET จัดการจะไม่ได้รับผลกระทบจากการกำหนดค่าการจัดการรายชื่อ URL



องค์ประกอบการควบคุม

เพิ่ม – สร้างรายการใหม่เพิ่มเติมจากรายการที่กำหนดไว้ล่วงหน้า ส่วนนี้จะมีประโยชน์เมื่อคุณต้องการแยกที่อยู่ออกเป็นกลุ่มๆ ตัวอย่างเช่น รายการของที่อยู่ที่ปิดกั้นรายการหนึ่งอาจประกอบด้วยที่อยู่จากบัญชีดำสาธารณะภายนอก และรายการถัดไปอาจประกอบด้วยบัญชีดำของคุณเอง ซึ่งทำให้ง่ายขึ้นต่อการอัพเดทรายการภายนอกในขณะที่เก็บส่วนของคุณไว้เหมือนเดิม

แก้ไข – แก้ไขรายการที่มีอยู่ ใช้สิ่งนี้ในการเพิ่มหรือลบที่อยู่ออก

ลบ – ลบรายการที่มีอยู่ สามารถใช้งานได้กับรายการที่สร้างด้วย **เพิ่ม** เท่านั้น ไม่สามารถใช้กับรายการตามค่าเริ่มต้นได้

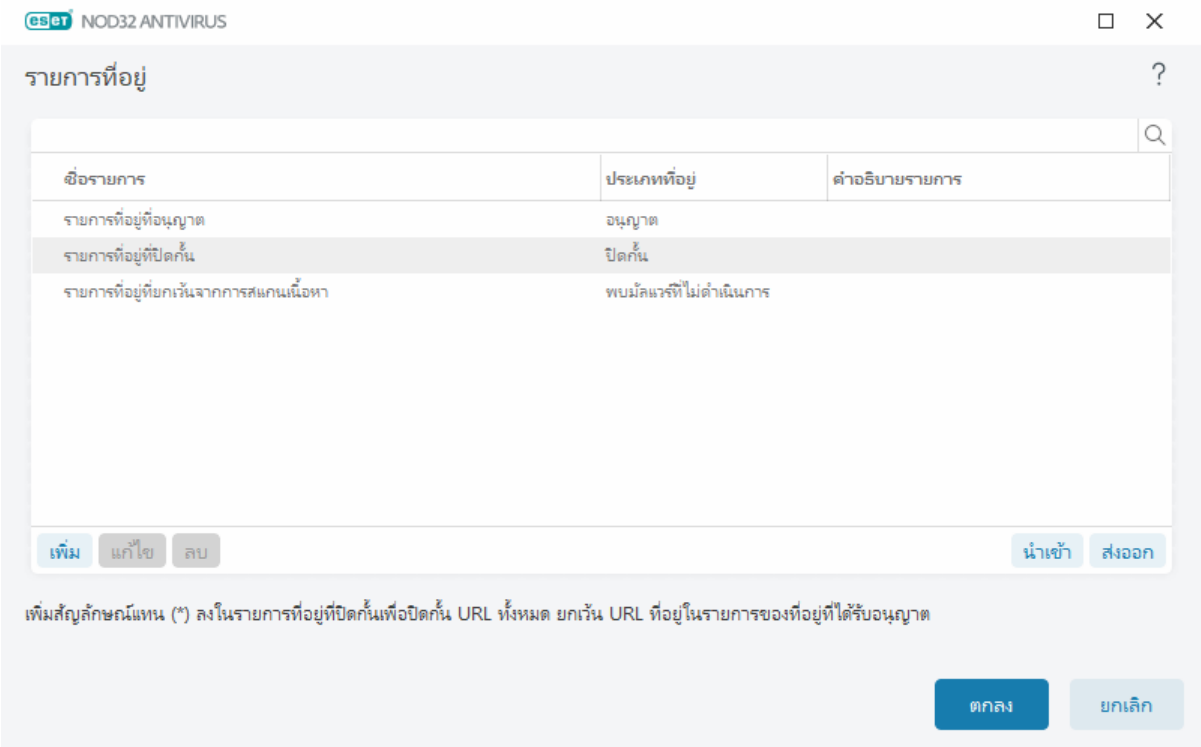
รายการที่อยู่

ในส่วนนี้ คุณสามารถระบุรายการของที่อยู่ HTTP(S) ที่จะถูกปิดกั้น อนุญาต หรือยกเว้นจากการตรวจสอบ

ตามค่าเริ่มต้นแล้ว จะมีสามรายการดังต่อไปนี้:

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

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



> **คำแนะนำพร้อมภาพประกอบ**
> บทความฐานความรู้ ESET ต่อไปนี้อาจมีให้เป็นภาษาอังกฤษเท่านั้น:
> • ยกเว้นเว็บไซต์ที่ปลอดภัยไม่ให้ถูกบล็อกโดยการป้องกันการเข้าถึงเว็บไซต์
> • ปิดกั้นเว็บไซต์โดยใช้งานผลิตภัณฑ์ ESET Windows สำหรับใช้งานในบ้าน

ดูข้อมูลเพิ่มเติมได้ที่ การจัดการรายการ URL

สร้างรายการที่อยู่ใหม่

หน้าต่างข้อความนี้ทำให้คุณสามารถกำหนดค่า รายการของที่อยู่/มาสก์ URL ที่จะถูกปิดกั้น อนุญาต หรือยกเว้นจากการตรวจสอบ

คุณสามารถกำหนดค่าตัวเลือกต่อไปนี้ได้:

ประเภทรายการที่อยู่ - มีประเภทรายการสามประเภท:

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

ชื่อรายการ – ระบุชื่อของรายการ ช่องนี้จะไม่มีให้ใช้งานขณะแก้ไขหนึ่งในรายการที่กำหนดไว้ล่วงหน้า

คำอธิบายรายการ - พิมพ์คำอธิบายโดยย่อสำหรับรายการ (ไม่จำเป็น) ไม่มีให้ใช้งานขณะแก้ไขหนึ่งในรายการที่กำหนดไว้ล่วงหน้า

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

ความรุนแรงของการบันทึก ซึ่งเป็นข้อมูลเกี่ยวกับรายการเฉพาะที่ใช้เมื่อเข้าถึงเว็บไซต์สามารถเขียนลงใน แฟ้มบันทึก ได้

องค์ประกอบการควบคุม

เพิ่ม – เพิ่มที่อยู่ URL ใหม่ไปยังรายการ (ป้อนค่าได้หลายค่าโดยใส่ตัวคั่น)

แก้ไข – แก้ไขที่อยู่ที่มีอยู่ในรายการ มีให้ใช้งานสำหรับที่อยู่ที่สร้างด้วย **เพิ่ม** เท่านั้น

ลบออก – ลบที่อยู่ที่มีอยู่ในรายการ มีให้ใช้งานสำหรับที่อยู่ที่สร้างด้วย **เพิ่ม** เท่านั้น

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

วิธีการเพิ่มมาสก์ URL

โปรดดูคำแนะนำในหน้าต่างข้อความนี้ก่อนป้อนที่อยู่ที่ต้องการ/มาสก์ของโดเมน

ESET NOD32 Antivirus ให้ผู้ใช้สามารถปิดกั้นการเข้าถึงเว็บไซต์ที่ระบุ และป้องกันไม่ให้เบราว์เซอร์อินเทอร์เน็ตแสดงเนื้อหา นอกจากนี้ ยังให้ผู้ใช้สามารถระบุที่อยู่ ซึ่งต้องการยกเว้นจากการตรวจสอบ หากไม่ทราบชื่อเต็มของเซิร์ฟเวอร์ระยะไกล หรือผู้ใช้ต้องการระบุทั้งกลุ่มของเซิร์ฟเวอร์ระยะไกล คุณสามารถใช้มาสก์เพื่อระบุกลุ่มดังกล่าวได้ มาสก์นี้ได้แก่สัญลักษณ์ "?" และ "*":

- ใช้ ? เพื่อแทนสัญลักษณ์
- ใช้ * เพื่อแทนสตริงข้อความ

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

สัญลักษณ์ '*.' ที่อยู่ด้านหน้าของลำดับจะแสดงผลเป็นพิเศษหากใช้ขึ้นต้นชื่อโดเมน แรกสุด สัญลักษณ์แทน * ต้องไม่ตรงกับเครื่องหมายทับ ('/') ในกรณีนี้ ทั้งนี้เพื่อกันไม่ให้หลีกเลี่ยงมาสก์ ตัวอย่างเช่น มาสก์ **.domain.com* จะไม่ตรงกับ *http://anydomain.com/anypath#.domain.com* (คำต่อท้ายเหล่านี้สามารถต่อท้าย URL ใดๆ โดยไม่ส่งผลต่อการดาวน์โหลด) ถัดมา สัญลักษณ์ "*." ยังต้องตรงกับสตริงเปล่าในกรณีพิเศษนี้ ทั้งนี้เพื่อทำให้ทั้งโดเมนรวมถึงโดเมนย่อยทั้งหมดตรงกันโดยใช้มาสก์เดียวร่วมกัน ตัวอย่างเช่น มาสก์ **.domain.com* ยังตรงกับ *http://domain.com* อีกด้วย การใช้ **domain.com* จะไม่ถูกต้อง เนื่องจากมาสก์ดังกล่าวจะไปตรงกับ *http://anotherdomain.com* เช่นกัน

การสแกนการรับส่งข้อมูล HTTP(S)

โดยค่าเริ่มต้น ESET NOD32 Antivirus มีการกำหนดค่าให้สแกน HTTP และ HTTPS การจราจรซึ่งใช้โดยเบราว์เซอร์อินเทอร์เน็ตและแอพพลิเคชันอื่นๆ คุณควรปิดใช้งานการสแกนการรับส่งข้อมูลเฉพาะในกรณีที่คุณกำลังประสบปัญหากับซอฟต์แวร์ของบริษัทอื่นและต้องการทราบว่าปัญหาดังกล่าวเกิดจาก ESET NOD32 Antivirus หรือไม่

เปิดใช้งานการสแกนการรับส่งข้อมูล HTTP – การรับส่งข้อมูล HTTP จะถูกตรวจสอบบนพอร์ตทั้งหมดสำหรับแอพพลิเคชั่นทั้งหมดเสมอ

เปิดใช้งานการสแกนการรับส่งข้อมูล HTTPS – การรับส่งข้อมูล HTTPS จะใช้ช่องทางที่เข้ารหัสเพื่อโอนข้อมูลระหว่างเซิร์ฟเวอร์กับไคลเอ็นต์ โดย ESET NOD32 Antivirus จะตรวจสอบการสื่อสารด้วยโปรโตคอล SSL (Secure Socket Layer) และ TLS (Transport Layer Security) โปรแกรมจะสแกนเฉพาะการรับส่งข้อมูลในพอร์ตที่กำหนดใน **พอร์ตที่ใช้งานโดยโปรโตคอล HTTPS** โดยไม่คำนึงถึงเวอร์ชันของระบบปฏิบัติการ (คุณสามารถเพิ่มพอร์ตไปยัง 443 และ 0-65535 ที่กำหนดไว้ล่วงหน้าได้)

ThreatSense

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

ตัวเลือกการตั้งค่าของเทคโนโลยี ThreatSense ช่วยให้ผู้ใช้สามารถระบุพารามิเตอร์การสแกนต่างๆ ได้:

- ประเภทไฟล์และนามสกุลที่จะสแกน
- การใช้วิธีการตรวจหาต่างๆ ร่วมกัน
- ระดับการกำจัด เป็นต้น

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

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

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

วัตถุที่จะสแกน

ส่วนนี้จะช่วยให้คุณสามารถกำหนดว่าจะสแกนหาการแฝงตัวจากองค์ประกอบและไฟล์คอมพิวเตอร์ใด

หน่วยความจำที่ใช้งาน – สแกนหาภัยคุกคามที่โจมตีหน่วยความจำที่ใช้งานของระบบ

ส่วนการบูต/UEFI – การสแกนบูตเซคเตอร์สำหรับมัลแวร์ที่มีอยู่ในบันทึกการบูตหลัก [อ่านเพิ่มเติมเกี่ยวกับ UEFI ในประมวลศัพท์]

ไฟล์อีเมล – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: DBX (Outlook Express) และ EML

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

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

รันไทม์แพ็คเกอร์ – หลังจากเรียกใช้แล้ว รันไทม์แพ็คเกอร์ (ไม่เหมือนกับประเภทที่เก็บเอกสารมาตรฐาน) จะ

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

ตัวเลือกการสแกน

เลือกวิธีที่ใช้เมื่อสแกนหาการแฝงตัวบนระบบ ตัวเลือกที่ใช้ได้มีดังนี้:

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

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

การกำจัด

การตั้งค่าการกำจัด จะเป็นตัวกำหนดการทำงานของ ESET NOD32 Antivirus ขณะกำจัดวัตถุ การกำจัดมี 4 ระดับ:

ThreatSense มีระดับการปรับปรุงแก้ไข (เช่น การกำจัด) ดังต่อไปนี้

การปรับปรุงแก้ไขใน ESET NOD32 Antivirus

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

ระดับการกำจัด	คำอธิบาย
ถามผู้ใช้ปลายทางเสมอ	ผู้ใช้ปลายทางจะได้รับหน้าต่างโต้ตอบขณะล้างวัตถุและต้องเลือกการดำเนินการการปรับปรุงแก้ไข (ตัวอย่างเช่น ลบ หรือ เพิกเฉย) ระดับนี้ได้รับการออกแบบสำหรับผู้ใช้ขั้นสูงขึ้นซึ่งรู้ว่าควรใช้วิธีใดเมื่อมีการตรวจหา

การยกเว้น

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่า ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะสแกน

อื่นๆ

เมื่อกำหนดค่าพารามิเตอร์กลไก ThreatSenseสำหรับการสแกนคอมพิวเตอร์ตามต้องการ จะสามารถใช้ตัวเลือกในส่วน **อื่นๆ** ได้ดังต่อไปนี้:

สแกนสตรีมข้อมูลสำรอง (ADS) – สตรีมข้อมูลสำรองที่ใช้งานโดยระบบไฟล์ NTFS เป็นการเชื่อมโยงไฟล์และโฟลเดอร์ซึ่งจะไม่ปรากฏสำหรับเทคนิคการสแกนทั่วไป การแฝงตัวจำนวนมากพยายามหลีกเลี่ยงการตรวจหานี้ โดยปลอมแปลงตัวเองเป็นสตรีมข้อมูลสำรอง

เรียกใช้การสแกนเบื้องหลังโดยมีลำดับความสำคัญต่ำ – ลำดับการสแกนแต่ละลำดับจะใช้ทรัพยากรของระบบจำนวนหนึ่ง หากคุณทำงานกับโปรแกรมที่ใช้ทรัพยากรระบบจำนวนมาก คุณสามารถเปิดใช้การสแกนเบื้องหลังที่มีลำดับความสำคัญต่ำ และประหยัดทรัพยากรไว้สำหรับแอพพลิเคชันของคุณ

บันทึกวัตถุทั้งหมด – บันทึกการสแกน จะแสดงไฟล์ที่สแกนแล้วทั้งหมดในอาร์ไคฟ์ที่ขยายในตัว รวมถึงไฟล์ที่ไม่ติดไวรัส (อาจสร้างข้อมูลบันทึกการสแกนจำนวนมากและเพิ่มขนาดไฟล์บันทึกการสแกน)

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

เก็บบันทึกการลงเวลาเข้าถึงล่าสุด – เลือกตัวเลือกนี้เพื่อเก็บเวลาแรกเริ่มที่เข้าถึงไฟล์ที่สแกนแทนการอัพเดทเวลาเหล่านั้น (ตัวอย่างเช่น สำหรับใช้กับระบบสำรองข้อมูล)

ขีดจำกัด

ส่วนขีดจำกัดช่วยให้คุณสามารถระบุขนาดสูงสุดของวัตถุ และระดับของอาร์ไคฟ์ที่ซ้อนที่จะสแกน:

การตั้งค่าวัตถุ

ขนาดวัตถุสูงสุด – กำหนดขนาดสูงสุดของวัตถุที่จะสแกน โมดูลป้องกันไวรัสที่กำหนดจะสแกนเฉพาะวัตถุที่เล็กกว่าขนาดที่ระบุเท่านั้น ผู้ที่สามารถแก้ไขตัวเลือกนี้ควรเป็นผู้ใช้ขั้นสูง ซึ่งอาจมีเหตุผลบางอย่างสำหรับการยกเว้นวัตถุขนาดใหญ่จากการสแกน ค่าเริ่มต้น: ไม่จำกัด

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

ตั้งค่าการสแกนอาร์ไคฟ์

ระดับการซ้อนของอาร์ไคฟ์ – ระบุความลึกสูงสุดของการสแกนอาร์ไคฟ์ ค่าเริ่มต้น: 10

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

> i เราไม่แนะนำให้แก้ไขค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดที่จะต้องแก้ไขค่านี้ในสถานการณ์ปกติ

การควบคุมอุปกรณ์

ESET NOD32 Antivirus มอบฟังก์ชันการควบคุมแบบอัตโนมัติกับอุปกรณ์ (CD/DVD/USB/ฯลฯ) โมดูลนี้จะช่วยให้คุณสามารถปิดกั้นหรือปรับตัวกรอง/สิทธิ์ที่ขยาย และกำหนดความสามารถของผู้ใช้ในการเข้าถึงและทำงานกับอุปกรณ์

เหล่านี้ได้ คุณลักษณะนี้เป็นประโยชน์ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์ต้องการป้องกันไม่ให้ผู้ใช้ใช้งานอุปกรณ์ซึ่งมีเนื้อหาที่ไม่พึงประสงค์

อุปกรณ์ภายนอกที่สนับสนุน:

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

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

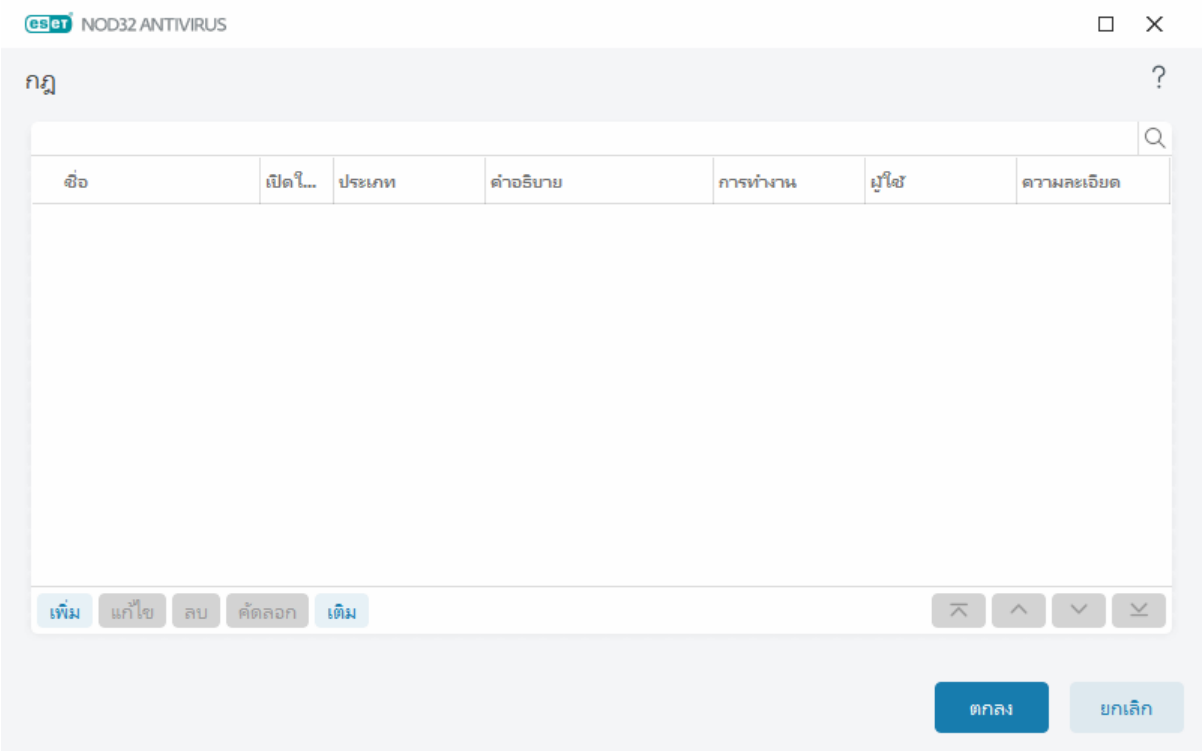
คลิกปุ่มสลับ **เปิดใช้การควบคุมอุปกรณ์** เพื่อเปิดใช้งานฟีเจอร์การควบคุมอุปกรณ์ใน ESET NOD32 Antivirus คุณต้องรีสตาร์ทคอมพิวเตอร์เพื่อให้การเปลี่ยนแปลงนี้มีผล เมื่อเปิดใช้งานการควบคุมอุปกรณ์แล้ว คุณจะสามารถกำหนด **กฎ** ในหน้าต่าง ตัวแก้ไขกฎ ได้

> คุณสามารถสร้างกลุ่มอุปกรณ์หลายๆ กลุ่มที่ปรับใช้กฎที่แตกต่างกัน นอกจากนี้แล้วคุณยังสามารถสร้างอุปกรณ์ที่จะนำกฎที่มีการทำงาน **อนุญาต** หรือ **เขียนบล็อก** ไปใช้ วิธีนี้จะช่วยปิดกั้นอุปกรณ์ที่การควบคุมอุปกรณ์ไม่รู้จักเมื่อต่อเข้ากับคอมพิวเตอร์ของคุณ

ถ้ามีการใส่อุปกรณ์ที่ถูกปิดกั้นโดยกฎที่มีอยู่ จะมีหน้าต่างการแจ้งเตือนปรากฏและไม่ได้รับสิทธิ์ให้เข้าถึงอุปกรณ์

เครื่องมือแก้ไขกฎการควบคุมอุปกรณ์

หน้าต่าง **เครื่องมือแก้ไขกฎการควบคุมอุปกรณ์** จะแสดงกฎที่มีอยู่ และช่วยให้สามารถทำการควบคุมอุปกรณ์ภายนอกที่ผู้ใช้ใช้ในการเชื่อมต่อกับคอมพิวเตอร์ได้อย่างแม่นยำ



สามารถทำการอนุญาตหรือปิดกั้นอุปกรณ์บางชนิดได้ตามผู้ใช้หรือกลุ่มผู้ใช้ และอิงตามพารามิเตอร์อุปกรณ์เพิ่มเติมซึ่งสามารถระบุไว้ในการกำหนดค่ากฎได้ รายการของกฎประกอบด้วยคำอธิบายของกฎหลายรายการ เช่น ชื่อ ประเภทอุปกรณ์ภายนอก การดำเนินการที่จะทำหลังจากเชื่อมต่ออุปกรณ์ภายนอกกับคอมพิวเตอร์ของคุณ และความรุนแรงของบันทึก โปรดดูที่ การเพิ่มกฎการควบคุมอุปกรณ์

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

โดยการกด **CTRL** และคลิก คุณสามารถเลือกหลายกฎและใช้การทำงานกับกฎที่เลือกไว้ทั้งหมด เช่น ลบ หรือเลื่อนขึ้นลงในรายการ กล่องทำเครื่องหมาย**เปิดใช้งาน**จะปิดใช้งานหรือเปิดใช้งานกฎ ซึ่งจะเป็นประโยชน์ถ้าคุณต้องการเก็บกฎไว้

คลิก **เติม** เพื่อเติมพารามิเตอร์ของอุปกรณ์สื่อที่ถอดเข้าออกได้สำหรับอุปกรณ์ที่เชื่อมต่อกับคอมพิวเตอร์ของคุณโดยอัตโนมัติ

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

สามารถดูรายการบันทึกได้ในหน้าต่างโปรแกรมหลัก > **เครื่องมือ** > ไฟล์บันทึก

บันทึกการควบคุมอุปกรณ์ จะบันทึกเหตุการณ์ทั้งหมดที่ได้ทริกเกอร์การควบคุมอุปกรณ์

อุปกรณ์ที่ตรวจพบ

ปุ่ม **เติม** จะแสดงภาพรวมของอุปกรณ์ทั้งหมดที่เชื่อมต่อในปัจจุบันพร้อมข้อมูลเกี่ยวกับ: ประเภทอุปกรณ์ เกี่ยวกับผู้ขายอุปกรณ์ รุ่นและหมายเลขซีเรียล (หากมี) หากต้องการดูอุปกรณ์ที่ซ่อนไว้ทั้งหมด ให้เลือก **แสดงอุปกรณ์ที่ซ่อนไว้**

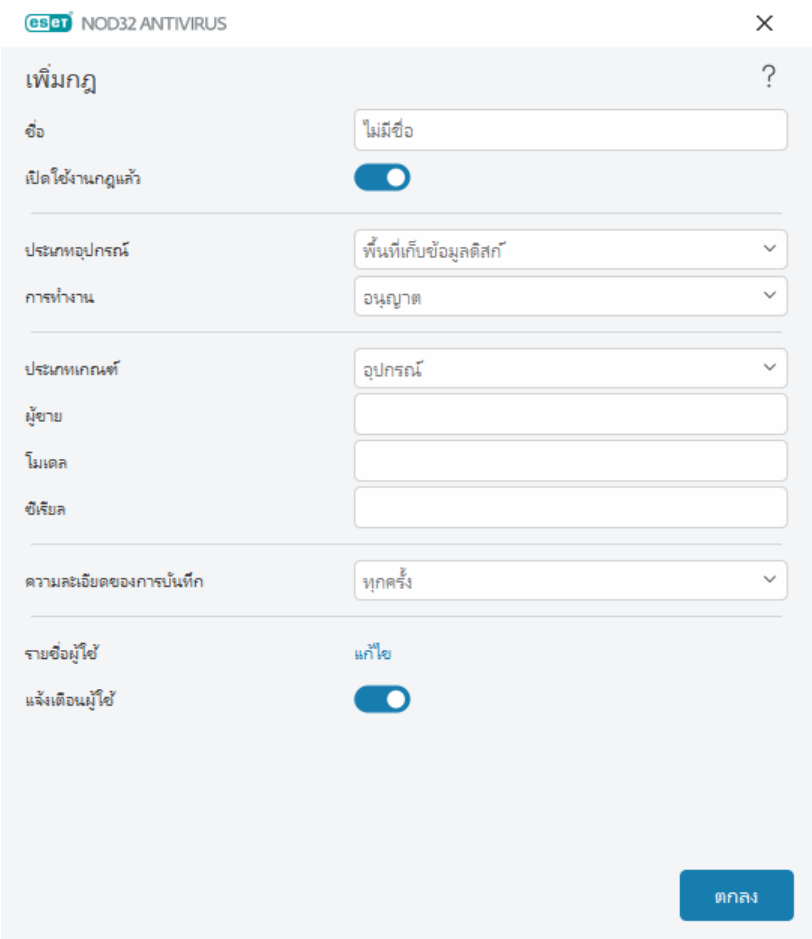
เลือกอุปกรณ์จากรายการอุปกรณ์ที่ตรวจพบ แล้วคลิก **ตกลง** เพื่อ เพิ่มกฎการควบคุมอุปกรณ์ ที่มีข้อมูลที่กำหนดไว้ล่วงหน้า (คุณสามารถปรับการตั้งค่าทุกค่าได้)

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

- เชื่อมต่อกับอุปกรณ์อีกครั้ง
- ใช้อุปกรณ์ (ตัวอย่างเช่น เริ่มแอพกล้องใน Windows เพื่อปลุกเว็บแคม)

การเพิ่มกฎการควบคุมอุปกรณ์

กฎการควบคุมอุปกรณ์จะกำหนดการทำงานเมื่ออุปกรณ์ที่ตรงตามเกณฑ์กฎเชื่อมต่อกับคอมพิวเตอร์



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

ประเภทอุปกรณ์

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

การทำงาน

สามารถอนุญาตหรือปิดกั้นการเข้าถึงอุปกรณ์ที่ไม่ใช่อุปกรณ์เก็บข้อมูลได้ ในทางตรงกันข้าม กฎสำหรับอุปกรณ์เก็บข้อมูลช่วยให้คุณสามารถเลือกได้จากหนึ่งในการตั้งค่าสิทธิ์ต่อไปนี้:

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

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

ประเภทเกณฑ์

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

พารามิเตอร์เพิ่มเติมที่แสดงด้านล่างสามารถใช้เพื่อปรับแต่งกฎสำหรับอุปกรณ์ต่างๆ ได้ พารามิเตอร์ทั้งหมดจะต้องตรงตามตัวพิมพ์ใหญ่-เล็กและรองรับอักขระตัวแทน (*,?):

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

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

> i หากต้องการดูข้อมูลเกี่ยวกับอุปกรณ์ ให้สร้างกฎสำหรับอุปกรณ์ประเภทนั้น เชื่อมต่ออุปกรณ์กับคอมพิวเตอร์ของคุณ และตรวจสอบรายละเอียดของอุปกรณ์ใน บันทึกการควบคุมอุปกรณ์

ความละเอียดของการบันทึก

ESET NOD32 Antivirus จะบันทึกเหตุการณ์สำคัญทั้งหมดไว้ในไฟล์บันทึก ซึ่งจะสามารถดูได้โดยตรงจากเมนูหลัก คลิก **เครื่องมือ** > **ไฟล์บันทึก** จากนั้นเลือก**ควบคุมอุปกรณ์** จาก **บันทึก** ในเมนูแบบเลื่อนลง

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

รายชื่อผู้ใช้

สามารถจำกัดกฎสำหรับผู้ใช้บางคนหรือผู้ใช้บางกลุ่มได้โดยการเพิ่มกฎลงในรายชื่อผู้ใช้ โดยคลิกที่ **แก้ไข** ที่อยู่ถัดจาก **รายชื่อผู้ใช้**

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

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

แจ้งเตือนผู้ใช้ – หากอุปกรณ์ถูกปิดกั้นด้วยการแทรกกฎที่มีอยู่แล้ว หน้าต่างการแจ้งเตือนจะปรากฏขึ้น

กลุ่มอุปกรณ์

อุปกรณ์ที่ต่อเข้ากับคอมพิวเตอร์ของคุณอาจก่อให้เกิดความเสี่ยงด้านความปลอดภัย

หน้าต่างกลุ่มอุปกรณ์แบ่งออกเป็นสองส่วน ด้านขวาของหน้าต่างแสดงรายชื่ออุปกรณ์ที่เป็นของกลุ่มที่เกี่ยวข้อง และด้านซ้ายของหน้าต่างประกอบด้วยกลุ่มที่สร้างขึ้น เลือกกลุ่มเพื่อแสดงอุปกรณ์ในบานหน้าต่างด้านขวา

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

องค์ประกอบการควบคุม

เพิ่ม – คุณสามารถเพิ่มกลุ่มโดยการพิมพ์ชื่อหรืออุปกรณ์ลงในกลุ่มที่มีอยู่ ทั้งนี้ขึ้นอยู่กับว่าคุณคลิกปุ่มที่ส่วนใดของหน้าต่าง

แก้ไข – ให้คุณเปลี่ยนชื่อของกลุ่มที่เลือกหรือพารามิเตอร์ของอุปกรณ์ (ผู้ขาย รุ่น หมายเลขซีเรียล)

ลบ – ลบกลุ่มหรืออุปกรณ์ที่เลือกโดยขึ้นอยู่กับว่าคุณคลิกปุ่มที่ส่วนใดของหน้าต่าง

นำเข้า – นำเข้ารายการอุปกรณ์จากไฟล์ข้อความ การนำเข้าอุปกรณ์จากไฟล์ข้อความต้องมีการจัดรูปแบบที่ถูกต้อง:

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

ตัวอย่างของเนื้อหาไฟล์ข้อความได้แก่:

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

ส่งออก – ส่งออกรายการอุปกรณ์ไปยังไฟล์

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

เพิ่มอุปกรณ์

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

- **ผู้ขาย** – กรองตามชื่อหรือ ID ของผู้ขาย

- **รุ่น** – ชื่อของอุปกรณ์ที่กำหนด

- **ซีเรียล** – อุปกรณ์ภายนอกมักจะมีหมายเลขซีเรียลของตนเอง ในกรณีของ CD/DVD หมายถึงหมายเลขซีเรียลของสื่อ ไม่ใช่ไดรฟ์ CD

- **คำอธิบาย** คำอธิบายเกี่ยวกับอุปกรณ์เพื่อการจัดระเบียบที่ดีขึ้น

> หากไม่ได้ระบุพารามิเตอร์เหล่านี้ กฎจะละเว้นช่องเหล่านี้ขณะที่จับคู่ พารามิเตอร์การกรองในช่องข้อความทั้งหมดจะต้องเป็นตัวพิมพ์ใหญ่และรองรับอักขระตัวแทน (เครื่องหมายคำถาม [?] แสดงถึงอักขระตัวเดียว ในขณะที่เครื่องหมายดอกจัน [*] แทนสตริงที่มีศูนย์อักขระหรือมากกว่า)

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

> หลังจากสร้างกลุ่มอุปกรณ์ คุณต้อง เพิ่มกฎการควบคุมอุปกรณ์ใหม่ สำหรับกลุ่มอุปกรณ์ที่สร้างขึ้นและเลือกการทำงานที่จะเกิดขึ้น

โปรดทราบว่ามีบางการทำงาน (การอนุญาต) เท่านั้นที่สามารถใช้งานได้กับอุปกรณ์ทุกประเภท การทำงานทั้งสี่จะพร้อมใช้งานถ้าเป็นอุปกรณ์ที่เป็นอุปกรณ์จัดเก็บข้อมูล สำหรับอุปกรณ์ที่ไม่ใช่อุปกรณ์จัดเก็บข้อมูล จะมีการทำงานเพียงสามอย่างเท่านั้นที่สามารถใช้งานได้ (เช่น **เขียนบล็อก** ไม่สามารถใช้งานกับ Bluetooth ได้ ดังนั้นอุปกรณ์ Bluetooth จะสามารถเลือกได้เพียง อนุญาต บล็อก หรือเตือนเท่านั้น)

ThreatSense

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

ตัวเลือกการตั้งค่าของเทคโนโลยี ThreatSense ช่วยให้ผู้ใช้สามารถระบุพารามิเตอร์การสแกนต่างๆ ได้:

- ประเภทไฟล์และนามสกุลที่จะสแกน

- การใช้วิธีการตรวจหาต่างๆ ร่วมกัน

- ระดับการกำจัด เป็นต้น

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

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

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

วัตถุที่จะสแกน

ส่วนนี้จะช่วยให้คุณสามารถกำหนดว่าจะสแกนหาการแฝงตัวจากองค์ประกอบและไฟล์คอมพิวเตอร์ใด

หน่วยความจำที่ใช้งาน – สแกนหาภัยคุกคามที่โจมตีหน่วยความจำที่ใช้งานของระบบ

ส่วนการบูต/UEFI – การสแกนบูตเซคเตอร์สำหรับมัลแวร์ที่มีอยู่ในบันทึกการบูตหลัก อ่านเพิ่มเติมเกี่ยวกับ UEFI ในประมวลศัพท์

ไฟล์อีเมล – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: DBX (Outlook Express) และ EML

อาร์ไคฟ์ – โปรแกรมสนับสนุนนามสกุลไฟล์ต่อไปนี้: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME,

NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE และอื่นๆ อีกมากมาย

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

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

ตัวเลือกการสแกน

เลือกวิธีที่ใช้เมื่อสแกนหาการแฝงตัวบนระบบ ตัวเลือกที่ใช้ได้มีดังนี้:

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

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

การกำจัด

การตั้งค่าการกำจัด จะเป็นตัวกำหนดการทำงานของ ESET NOD32 Antivirus ขณะกำจัดวัตถุ การกำจัดมี 4 ระดับ:

ThreatSense มีระดับการปรับปรุงแก้ไข (เช่น การกำจัด) ดังต่อไปนี้

การปรับปรุงแก้ไขใน ESET NOD32 Antivirus

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

การยกเว้น

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่า ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะสแกน

อื่นๆ

เมื่อกำหนดค่าพารามิเตอร์กลไก ThreatSenseสำหรับการสแกนคอมพิวเตอร์ตามต้องการ จะสามารถใช้ตัวเลือกในส่วน **อื่นๆ** ได้ดังต่อไปนี้:

สแกนสตรีมข้อมูลสำรอง (ADS) – สตรีมข้อมูลสำรองที่ใช้งานโดยระบบไฟล์ NTFS เป็นการเชื่อมโยงไฟล์และโฟลเดอร์ซึ่งจะไม่ปรากฏสำหรับเทคนิคการสแกนทั่วไป การแฝงตัวจำนวนมากพยายามหลีกเลี่ยงการตรวจหานี้ โดยปลอมแปลงตัวเองเป็นสตรีมข้อมูลสำรอง

เรียกใช้การสแกนเบื้องหลังโดยมีลำดับความสำคัญต่ำ – ลำดับการสแกนแต่ละลำดับจะใช้ทรัพยากรของระบบจำนวนหนึ่ง หากคุณทำงานกับโปรแกรมที่ใช้ทรัพยากรระบบจำนวนมาก คุณสามารถเปิดใช้การสแกนเบื้องหลังที่มีลำดับความสำคัญต่ำ และประหยัดทรัพยากรไว้สำหรับแอพพลิเคชันของคุณ

บันทึกวัตถุทั้งหมด – บันทึกการสแกน จะแสดงไฟล์ที่สแกนแล้วทั้งหมดในอาร์ไคฟ์ที่ขยายในตัว รวมถึงไฟล์ที่ไม่ติดไวรัส (อาจสร้างข้อมูลบันทึกการสแกนจำนวนมากและเพิ่มขนาดไฟล์บันทึกการสแกน)

เปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท – เมื่อเปิดใช้การเพิ่มประสิทธิภาพแบบสมาร์ท ระบบจะใช้การตั้งค่าที่มีประสิทธิภาพที่สุดเพื่อให้แน่ใจว่าการสแกนจะมีประสิทธิภาพและความเร็วสูงสุดไปพร้อมกัน ซึ่งโมดูลการป้องกันต่างๆ จะสแกนข้อมูลอย่างชาญฉลาด โดยใช้ประโยชน์จากวิธีการสแกนต่างๆ และนำมาใช้งานกับประเภท

ไฟล์ที่ระบุ หากคุณปิดใช้งานการเพิ่มประสิทธิภาพแบบสมาร์ท เราจะใช้เฉพาะการตั้งค่าที่ผู้ใช้กำหนดไว้ในแกน ThreatSense ของโมดูลเฉพาะเมื่อทำการสแกนเท่านั้น

เก็บบันทึกการลงเวลาเข้าถึงล่าสุด – เลือกตัวเลือกนี้เพื่อเก็บเวลาแรกเริ่มที่เข้าถึงไฟล์ที่สแกนแทนการอัพเดทเวลาเหล่านั้น (ตัวอย่างเช่น สำหรับใช้กับระบบสำรองข้อมูล)

ขีดจำกัด

ส่วนขีดจำกัดช่วยให้คุณสามารถระบุขนาดสูงสุดของวัตถุ และระดับของอาร์ไคฟ์ที่ซ้อนที่จะสแกน:

การตั้งค่าวัตถุ

ขนาดวัตถุสูงสุด – กำหนดขนาดสูงสุดของวัตถุที่จะสแกน โมดูลป้องกันไวรัสที่กำหนดจะสแกนเฉพาะวัตถุที่เล็กกว่าขนาดที่ระบุเท่านั้น ผู้ที่สามารถแก้ไขตัวเลือกนี้ควรเป็นผู้ใช้ขั้นสูง ซึ่งอาจมีเหตุผลบางอย่างสำหรับการยกเว้นวัตถุขนาดใหญ่จากการสแกน ค่าเริ่มต้น: ไม่จำกัด

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

ตั้งค่าการสแกนอาร์ไคฟ์

ระดับการซ้อนของอาร์ไคฟ์ – ระบุความลึกสูงสุดของการสแกนอาร์ไคฟ์ ค่าเริ่มต้น: 10

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

> i เราไม่แนะนำให้แก้ไขค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดที่จะต้องแก้ไขค่านี้ในสถานการณ์ปกติ

ระดับการกำจัด

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

ThreatSense มีระดับการปรับปรุงแก้ไข (เช่น การกำจัด) ดังต่อไปนี้

การปรับปรุงแก้ไขใน ESET NOD32 Antivirus

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

รายการที่อยู่ที่ยกเว้นจากการตรวจสอบ

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

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่า ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะสแกนได้

> ℹ อย่าสับสนกับ การยกเว้นกระบวนการ, การยกเว้น HIPS หรือ การยกเว้นไฟล์/โฟลเดอร์

ทุกไฟล์จะถูกสแกนตามค่าเริ่มต้น คุณสามารถเพิ่มนามสกุลในรายการไฟล์ที่จะยกเว้นจากการสแกน

ในบางครั้ง การยกเว้นไฟล์จากการสแกนจะเป็นสิ่งจำเป็น หากไฟล์บางประเภทของการสแกนป้องกันโปรแกรมที่ใช้นามสกุลบางประเภทเพื่อไม่ให้ทำงานอย่างถูกต้อง ตัวอย่างเช่น อาจมีการแนะนำให้ยกเว้นนามสกุล `.edb`, `.eml`

และ `.tmp` เมื่อใช้เซิร์ฟเวอร์ Microsoft Exchange

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

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

พารามิเตอร์ ThreatSense เพิ่มเติม

หากต้องการแก้ไขการตั้งค่าเหล่านี้ ให้เปิด การตั้งค่าขั้นสูง > **การป้องกัน** > **การป้องกันระบบไฟล์แบบเรียลไทม์** > **พารามิเตอร์ ThreatSense เพิ่มเติม**

พารามิเตอร์ ThreatSense เพิ่มเติมสำหรับไฟล์ที่สร้างใหม่และแก้ไข

ไฟล์ที่สร้างใหม่หรือแก้ไขมีความเป็นไปได้ที่จะติดไวรัสมากกว่าไฟล์ที่มีอยู่ ด้วยเหตุผลนี้ โปรแกรมจะตรวจสอบไฟล์เหล่านี้ด้วยพารามิเตอร์การสแกนเพิ่มเติม ESET NOD32 Antivirus จะใช้การวิเคราะห์พฤติกรรมขั้นสูงที่สามารถตรวจหาภัยคุกคามใหม่ก่อนที่จะมีการปล่อยการอัพเดทกลไกการตรวจจับพร้อมกับวิธีสแกนโดยใช้ฐานข้อมูล

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

พารามิเตอร์ ThreatSense เพิ่มเติมสำหรับไฟล์ที่เรียกใช้

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

การวิเคราะห์พฤติกรรมขั้นสูงเมื่อเรียกใช้ไฟล์จากสื่อที่ถอดเข้าออกได้ - การวิเคราะห์พฤติกรรมขั้นสูงจะจำลองรหัสในสิ่งแวดล้อมเสมือนและประเมินพฤติกรรมก่อนจะให้อนุญาตให้ใช้งานรหัสจากสื่อที่ถอดออกได้

เครื่องมือ

คุณสามารถกำหนดการตั้งค่าขั้นสูงสำหรับฟีเจอร์ที่มีความปลอดภัยเพิ่มเติม และช่วยลดความยุ่งยากในการดูแลระบบของ ESET NOD32 Antivirus ใน การตั้งค่าขั้นสูง > **เครื่องมือ**

- รายการอัพเดทของ Microsoft Windows
- ESET CMD
- ไฟล์บันทึก
- โหมดผู้เล่นเกม
- การวินิจฉัย

รายการอัพเดทของ Microsoft Windows

คุณลักษณะการอัพเดท Windows เป็นองค์ประกอบสำคัญสำหรับการป้องกันผู้ใช้ให้พ้นจากซอฟต์แวร์ที่เป็นอันตราย ด้วยเหตุนี้ การติดตั้งการอัพเดทของ Microsoft Windows ให้เร็วที่สุดเมื่อมีการเผยแพร่จึงเป็นสิ่งที่สำคัญ ESET NOD32 Antivirus จะแจ้งคุณเกี่ยวกับการอัพเดทที่ขาดหายไป ตามระดับที่คุณระบุใน การตั้งค่าขั้นสูง > **เครื่องมือ** ระดับที่ใช้ได้มีดังนี้:

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

หน้าต่างข้อความ - การอัพเดทระบบ

หากมีการอัพเดทสำหรับระบบปฏิบัติการของคุณ ESET NOD32 Antivirus จะแสดงการแจ้งเตือนใน หน้าต่างโปรแกรมหลัก > **ภาพรวม** คลิก **ข้อมูลเพิ่มเติม** เพื่อเปิดหน้าต่างการอัพเดทระบบ

หน้าต่างการอัพเดทระบบจะแสดงรายการอัพเดทที่พร้อมสำหรับการดาวน์โหลดและติดตั้ง ประเภทการอัพเดทจะปรากฏถัดจากชื่อของการอัพเดทนั้น

คลิกสองครั้งที่แถวของการอัพเดทแถวใดก็ได้เพื่อแสดงหน้าต่างข้อมูลการอัพเดทที่มีข้อมูลเพิ่มเติม

คลิก **เรียกใช้การอัพเดทระบบปฏิบัติการ** เพื่อดาวน์โหลดและติดตั้งการอัพเดทระบบปฏิบัติการที่แสดงในรายการทั้งหมด

ข้อมูลการอัพเดท

หน้าต่างการอัพเดทระบบจะแสดงรายการอัพเดทที่พร้อมสำหรับการดาวน์โหลดและติดตั้ง ระดับความสำคัญของการอัพเดทจะปรากฏถัดจากชื่อของการอัพเดทนั้น

คลิกที่ **เรียกใช้การอัพเดทระบบ** เพื่อเริ่มต้นดาวน์โหลดและติดตั้งการอัพเดทระบบปฏิบัติการ

คลิกขวาที่แถวการอัพเดท และคลิก**แสดงข้อมูล**เพื่อแสดงหน้าต่างใหม่พร้อมด้วยข้อมูลเพิ่มเติม

ESET CMD

นี่เป็นคุณลักษณะที่ทำให้สามารถใช้คำสั่ง ecmd แบบขั้นสูงได้ ซึ่งจะช่วยให้คุณสามารถส่งออกและนำเข้าการตั้งค่าได้โดยใช้บรรรทัดคำสั่ง (ecmd.exe) ตอนนี้ คุณจะสามารถส่งออกการตั้งค่าได้โดยใช้ GUI เท่านั้น ส่วนการกำหนดค่า ESET NOD32 Antivirus สามารถส่งออกไปเป็นไฟล์ *.xml* ได้

เมื่อคุณเปิดใช้งาน ESET CMD แล้ว จะสามารถใช้วิธีการให้สิทธิ์ได้ทั้งหมดสองวิธี

- **ไม่มี** - ไม่มีสิทธิ์ เราไม่แนะนำให้คุณใช้วิธีการนี้เนื่องจากวิธีการดังกล่าวอนุญาตให้มีการนำเข้าการกำหนดค่าใดๆ ที่ไม่ได้ลงชื่อ ซึ่งค่อนข้างมีความเสี่ยง

- **รหัสผ่านการตั้งค่าขั้นสูง** – ต้องใช้รหัสผ่านเพื่อนำเข้าการกำหนดค่าจากไฟล์ .xml ไฟล์นี้จะต้องลงชื่อ (ดูการลงชื่อการกำหนดค่าไฟล์ .xml ด้านล่าง) รหัสผ่านที่ระบุใน ตั้งค่าการเข้าถึง จะต้องใส่ก่อนที่จะสามารถ

นำเข้าการกำหนดค่าใหม่ได้ หากไม่ได้เปิดใช้งานการตั้งค่าการเข้าถึงไว้ รหัสผ่านไม่ตรงกัน หรือไม่มีการลงชื่อไฟล์การกำหนดค่า .xml การกำหนดค่าจะไม่ถูกนำเข้า

เมื่อเปิดใช้งาน ESET CMD อยู่ คุณจะสามารถใช้บรรทัดคำสั่งสำหรับส่งออกหรือนำเข้าการกำหนดค่า ESET NOD32 Antivirus ได้ คุณสามารถทำขั้นตอนนี้ได้ด้วยตนเอง หรือสร้างสคริปต์เพื่อจุดประสงค์ด้านระบบอัตโนมัติ

หากต้องการใช้คำสั่ง ecmd ขั้นสูง คุณต้องใช้งานคำสั่งเหล่านั้นด้วยสิทธิ์ของผู้ดูแลระบบ หรือเปิด Windows Command Prompt (cmd) โดยใช้ **เรียกใช้ในฐานะผู้ดูแล** มิฉะนั้น คุณจะได้รับข้อความ **Error executing command** และเมื่อส่งออกการกำหนดค่า จะต้องมีโฟลเดอร์ปลายทางด้วย คำสั่งส่งออกจะยังคงทำงานได้เมื่อการตั้งค่า ESET CMD ถูกปิด

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

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

คำสั่ง ecmd ขั้นสูงสามารถเรียกใช้ในระบบได้เท่านั้น

การลงชื่อไฟล์การกำหนดค่า *.xml*:

1. ดาวน์โหลดไฟล์ที่เรียกใช้ XmlSignTool

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

3. ไปที่ตำแหน่งที่บันทึก `xmlsigntool.exe`

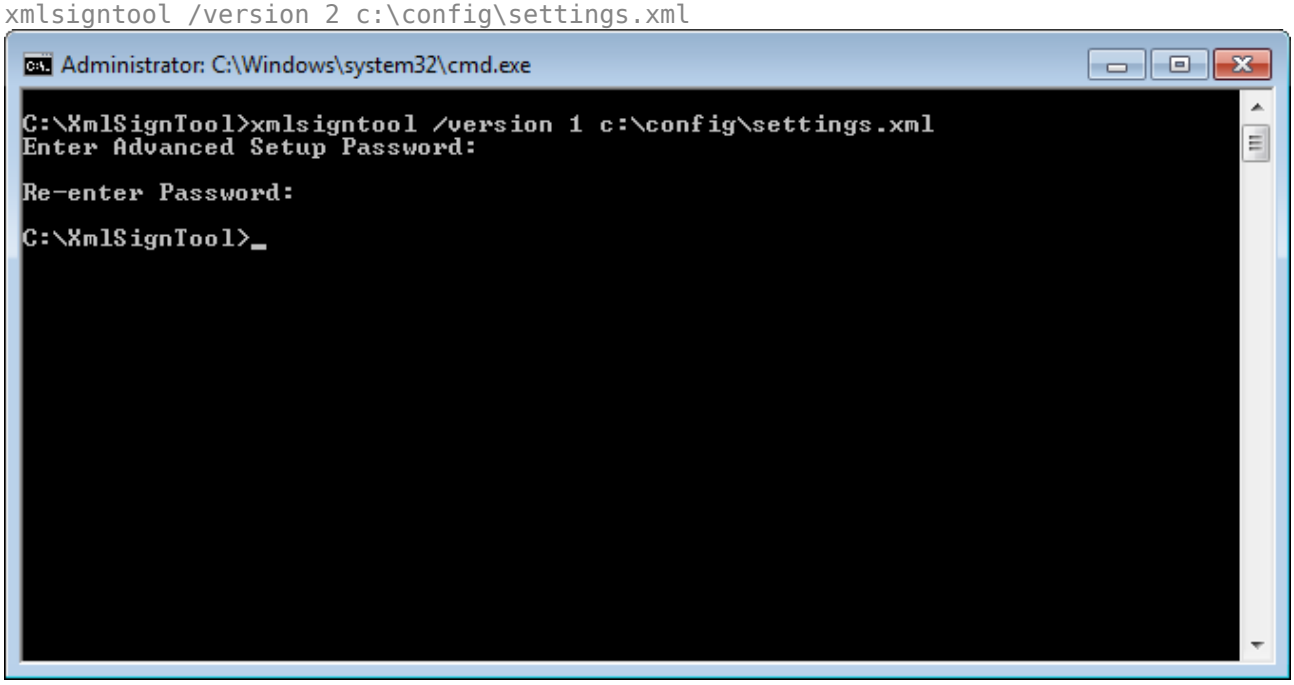
4. ดำเนินการคำสั่งเพื่อลงชื่อไฟล์การกำหนดค่า *.xml* การใช้งาน: `xmlsigntool /version 1|2 <xml_file_path>`

ค่าพารามิเตอร์ของ `/version` จะขึ้นอยู่กับเวอร์ชันของ ESET NOD32 Antivirus ใช้ `/version 1` กับ ESET NOD32 Antivirus เวอร์ชันเก่ากว่า 11.1 ใช้ `/version 2` สำหรับ ESET NOD32 Antivirus เวอร์ชันปัจจุบัน

5. พิมพ์รหัสผ่านการตั้งค่าขั้นสูงแล้วพิมพ์อีกครั้งตามที่ได้รับแจ้งจาก XmlSignTool ไฟล์การกำหนดค่า *.xml* ของคุณได้รับการลงชื่อแล้วตอนนี้ และสามารถใช้นำเข้าในอีกอินสแตนซ์หนึ่งของ ESET NOD32 Antivirus ด้วย ESET CMD ได้โดยใช้วิธีการให้สิทธิ์รหัสผ่าน

คำสั่งลงชื่อไฟล์การกำหนดค่าที่ส่งออก:

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



หากรหัสผ่าน ตั้งค่าการเข้าถึง ของคุณเปลี่ยนและคุณต้องการนำเข้าการกำหนดค่าที่ลงชื่อไว้ก่อนหน้าด้วยรหัสเก่า คุณจะต้องลงชื่อไฟล์การตั้งค่า *.xml* อีกครั้งโดยใช้รหัสผ่านปัจจุบันของคุณ การดำเนินการนี้จะทำให้คุณสามารถใช้ไฟล์การกำหนดค่าเก่าโดยไม่ต้องส่งออกไปอีกเครื่องที่กำลังเรียกใช้ ESET NOD32 Antivirus ก่อนที่จะนำเข้า

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

ไฟล์บันทึก

คุณสามารถค้นหาการกำหนดค่าการบันทึกของ ESET NOD32 Antivirus ได้ใน การตั้งค่าขั้นสูง > **เครื่องมือ** > **ไฟล์บันทึก** ส่วนบันทึกนี้ใช้เพื่อกำหนดวิธีจัดการบันทึก โปรแกรมจะลบบันทึกเก่าโดยอัตโนมัติ เพื่อประหยัดพื้นที่บนฮาร์ดดิสก์ คุณสามารถระบุตัวเลือกต่อไปนี้สำหรับไฟล์บันทึก:

ความละเอียดขั้นต่ำในการบันทึก – ระบุระดับความละเอียดขั้นต่ำของเหตุการณ์ที่จะบันทึก:

- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- **มีข้อมูล** – บันทึกข้อความแจ้งข้อมูล รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน
- **ข้อผิดพลาด** – ข้อผิดพลาด เช่น "เกิดข้อผิดพลาดขณะดาวน์โหลดไฟล์" และข้อผิดพลาดร้ายแรงจะถูกบันทึก

• **ร้ายแรง** – บันทึกเฉพาะข้อผิดพลาดร้ายแรง (ข้อผิดพลาดในการเริ่มต้นการป้องกันไวรัส ฯลฯ...)

> ℹ การเชื่อมต่อที่ปิดกั้นจะบันทึกไว้เมื่อคุณเลือกระดับค่าความละเอียดของ การวินิจฉัย

รายการบันทึกที่เก่ากว่าจำนวนวันที่ระบุในช่อง **ลบอัตโนมัติสำหรับบันทึกที่เก่ากว่า (วัน)** จะถูกลบโดยอัตโนมัติ

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

คลิก **ปรับปรุงประสิทธิภาพ** เพิ่มเริ่มต้นการจัดระเบียบบันทึกไฟล์ใหม่ รายการบันทึกที่ว่างเปล่าทั้งหมดจะถูกลบออกระหว่างกระบวนการนี้ ซึ่งช่วยปรับปรุงประสิทธิภาพและบันทึกความเร็วของการประมวลผล การปรับปรุงนี้จะเห็นได้ชัดโดยเฉพาะถ้าบันทึกมีรายการจำนวนมาก

เปิดใช้งานโปรโตคอลข้อความ เปิดใช้งานการบันทึกในรูปแบบอื่นแยกจาก ไฟล์บันทึก:

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

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

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

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

โหมดผู้เล่นเกม

โหมดผู้เล่นเกมเป็นคุณลักษณะสำหรับผู้ใช้ที่ต้องการใช้ซอฟต์แวร์อย่างต่อเนื่องไม่ขาดสาย ไม่ต้องการถูกหน้าต่างแจ้งเตือน/เตือนภัยรบกวน และต้องการลดการใช้งาน CPU ลง โหมดผู้เล่นเกมสามารถใช้ระหว่างการนำเสนอที่ไม่ควรมีการขัดจังหวะโดยกิจกรรมการป้องกันไวรัส เมื่อเปิดใช้งานคุณลักษณะนี้ หน้าต่างป๊อปอัปทั้งหมดจะถูกปิดใช้

งาน และกิจกรรมของเครื่องมือวางกำหนดการจะหยุดทำงานโดยสิ้นเชิง การป้องกันระบบจะยังทำงานอยู่ในพื้นหลัง แต่ผู้ใช้ไม่ต้องดำเนินการใดๆ

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

เปิดใช้งาน **เปิดใช้งานโหมดผู้เล่นเกมเมื่อเรียกใช้แอพพลิเคชันในโหมดเต็มหน้าจอโดยอัตโนมัติ** > การตั้งค่าขั้นสูง > **เครื่องมือ** > **โหมดผู้เล่นเกม** เพื่อให้โหมดผู้เล่นเกมเริ่มต้นเมื่อใดก็ตามที่คุณเริ่มใช้งานแอพพลิเคชันแบบเต็มหน้าจอและหยุดหลังจากที่คุณออกจากแอพพลิเคชันนั้น

เปิดใช้งาน **ปิดใช้งานโหมดผู้เล่นเกมโดยอัตโนมัติหลังจาก** เพื่อระบุช่วงเวลาที่โหมดผู้เล่นเกมจะปิดใช้งานโดยอัตโนมัติ

การวินิจฉัย

การวินิจฉัยจะให้บันทึกข้อมูลความล้มเหลวของแอพพลิเคชันของกระบวนการ ESET (ekrn เป็นต้น) หากแอพพลิเคชันล่ม บันทึกข้อมูลความล้มเหลวจะถูกสร้างขึ้น สิ่งนี้สามารถช่วยให้นักพัฒนาแก้ไขปัญหาและปรับแก้ปัญหาต่างๆ ของ ESET NOD32 Antivirus ได้

คลิกเมนูแบบเลื่อนลงที่อยู่ถัดจาก **ชนิดดัมพ์** แล้วเลือกหนึ่งในสามตัวเลือกที่มีให้:

- เลือก**ปิดใช้งาน** เพื่อปิดใช้งานคุณลักษณะนี้
- **เล็ก** ค่าเริ่มต้น – บันทึกข้อมูลที่เป็นประโยชน์ไว้ในปริมาณที่น้อยที่สุด ซึ่งอาจช่วยระบุสาเหตุที่ทำให้แอพพลิเคชันเสียหายโดยไม่คาดหมาย ไฟล์ดัมพ์ชนิดนี้จะมีประโยชน์เมื่อมีพื้นที่ว่างจำกัด แต่เนื่องจากมีข้อมูลที่จำกัด การวิเคราะห์ไฟล์นี้อาจไม่พบข้อผิดพลาดที่ไม่ได้เกิดโดยตรงจากเธรดที่ทำงานอยู่เมื่อเกิดปัญหา
- **เต็ม** - บันทึกเนื้อหาทั้งหมดของหน่วยความจำระบบเมื่อแอพพลิเคชันหยุดทำงานโดยไม่คาดคิด ดัมพ์หน่วยความจำแบบสมบูรณ์อาจมีข้อมูลจากกระบวนการที่ทำงานอยู่เมื่อมีการรวบรวมดัมพ์หน่วยความจำ

ไดเรกทอรีเป้าหมาย – ไดเรกทอรีที่ดัมพ์ในระหว่างที่เกิดความเสียหายถูกสร้างขึ้น

เปิดโฟลเดอร์การวินิจฉัย – คลิก **เปิด** เพื่อเปิดไดเรกทอรีนี้ในหน้าต่าง *Windows explorer* ใหม่

สร้างดัมพ์การวินิจฉัย - คลิก **สร้าง** เพื่อสร้างไฟล์ดัมพ์การวินิจฉัยใน **ไดเรกทอรีเป้าหมาย**

การบันทึกขั้นสูง

เปิดใช้งานการบันทึกขั้นสูงในข้อความทางการตลาด – บันทึกเหตุการณ์ทั้งหมดที่เกี่ยวข้องกับข้อความทางการตลาดภายในผลิตภัณฑ์

เปิดใช้งานการบันทึกขั้นสูงสำหรับเครื่องมือสแกน – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นระหว่างการสแกนไฟล์และโฟลเดอร์โดยการสแกนคอมพิวเตอร์

เปิดใช้งานการบันทึกขั้นสูงสำหรับการควบคุมเนื้อหา – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการควบคุมอุปกรณ์ ซึ่งจะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับการควบคุมอุปกรณ์ได้

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

เปิดใช้งานการบันทึกขั้นสูงของการป้องกันเอกสาร – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการป้องกันเอกสารเพื่ออนุญาตการวินิจฉัยและการแก้ไขปัญหา

เปิดใช้งานการบันทึกขั้นสูงของการป้องกันอีเมลไคลเอ็นต์ - บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในการป้องกันอีเมลไคลเอ็นต์และปลั๊กอินอีเมลไคลเอ็นต์เพื่อให้สามารถดำเนินการวินิจฉัยและแก้ปัญหาได้

เปิดใช้งานการบันทึกขั้นสูงสำหรับเคอร์เนล – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในเคอร์เนล ESET (ekrn)

เปิดใช้งานการอนุญาตการบันทึกขั้นสูง – บันทึกการสื่อสารทั้งหมดของผลิตภัณฑ์ด้วยการเปิดใช้งาน ESET หรือเซิร์ฟเวอร์ ESET License Manager

เปิดใช้งานการติดตามหน่วยความจำ - บันทึกเหตุการณ์ทั้งหมดที่จะช่วยนักพัฒนาในการวินิจฉัยปัญหาหน่วยความจำรั่ว

เปิดใช้การบันทึกขั้นสูงของเครื่องมือสแกนการรับส่งข้อมูลเครือข่าย – บันทึกข้อมูลทั้งหมดที่ส่งผ่านเครื่องมือสแกนการรับส่งข้อมูลเครือข่ายในรูปแบบ PCAP เพื่อช่วยให้นักพัฒนาวินิจฉัยและแก้ไขปัญหาที่เกี่ยวข้องกับเครื่องมือสแกนการรับส่งข้อมูลเครือข่าย

เปิดใช้งานการบันทึกขั้นสูงสำหรับระบบปฏิบัติการ – บันทึกข้อมูลเพิ่มเติมเกี่ยวกับระบบปฏิบัติการ เช่น กระบวนการที่ทำงานอยู่ กิจกรรม CPU และการทำงานของดิสก์ ซึ่งสามารถช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวกับผลิตภัณฑ์ ESET ที่ทำงานอยู่ในระบบปฏิบัติการของคุณได้

เปิดใช้งานการบันทึกขั้นสูงสำหรับการส่งข้อความแบบพุช – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในระหว่างการส่งข้อความแบบพุช

เปิดใช้งานการบันทึกขั้นสูงสำหรับการป้องกันระบบไฟล์แบบเรียลไทม์ – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นระหว่างการสแกนไฟล์และโฟลเดอร์โดยการป้องกันระบบไฟล์แบบเรียลไทม์

เปิดใช้งานการบันทึกขั้นสูงสำหรับกลไกอัพเดท – บันทึกเหตุการณ์ทั้งหมดที่เกิดขึ้นในกระบวนการอัพเดท ซึ่งการทำเช่นนี้จะช่วยให้นักพัฒนาสามารถวินิจฉัยและแก้ไขปัญหาที่เกี่ยวข้องกับกลไกการอัพเดทได้

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

ฝ่ายสนับสนุนด้านเทคนิค

เมื่อ ติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET จาก ESET NOD32 Antivirus แล้ว คุณสามารถส่งข้อมูลการกำหนดค่าระบบได้ เลือก **ส่งเสมอ** จากเมนูแบบเลื่อนลง **ส่งข้อมูลการกำหนดค่าระบบ** เพื่อส่งข้อมูลโดยอัตโนมัติ หรือเลือก **ถามก่อนส่ง** เพื่อให้ได้รับข้อความเตือนก่อนจะส่งข้อมูล

การเชื่อมต่อ

ในบางรูปแบบเครือข่าย พร็อกซีเซิร์ฟเวอร์สามารถควบคุมการสื่อสารระหว่างคอมพิวเตอร์ของคุณกับอินเทอร์เน็ตได้ หากคุณต้องการใช้พร็อกซีเซิร์ฟเวอร์ คุณต้องกำหนดการตั้งค่าต่อไปนี้ มิฉะนั้น ESET NOD32 Antivirus และโมดูลจะไม่อัพเดทโดยอัตโนมัติ ใน ESET NOD32 Antivirus การตั้งค่าพร็อกซีเซิร์ฟเวอร์จะพร้อมให้ใช้งานในส่วนสองส่วนของ การตั้งค่าขั้นสูง

โดยจะกำหนดการตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วมได้ใน การตั้งค่าขั้นสูง > **การเชื่อมต่อ** > **พร็อกซีเซิร์ฟเวอร์** การระบุพร็อกซีเซิร์ฟเวอร์ที่ระดับนี้จะกำหนดการตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วมสำหรับ ESET NOD32 Antivirus ทั้งหมด พารามิเตอร์ในที่นี้จะถูกนำมาใช้โดยโมดูลทั้งหมดที่ต้องการการเชื่อมต่ออินเทอร์เน็ต

หากต้องการระบุการตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วมแบบเฉพาะเจาะจง ให้เปิดใช้งาน **ใช้พร็อกซีเซิร์ฟเวอร์** และพิมพ์ที่อยู่ของ **พร็อกซีเซิร์ฟเวอร์**พร้อมกับหมายเลข **พอร์ต** ของพร็อกซีเซิร์ฟเวอร์

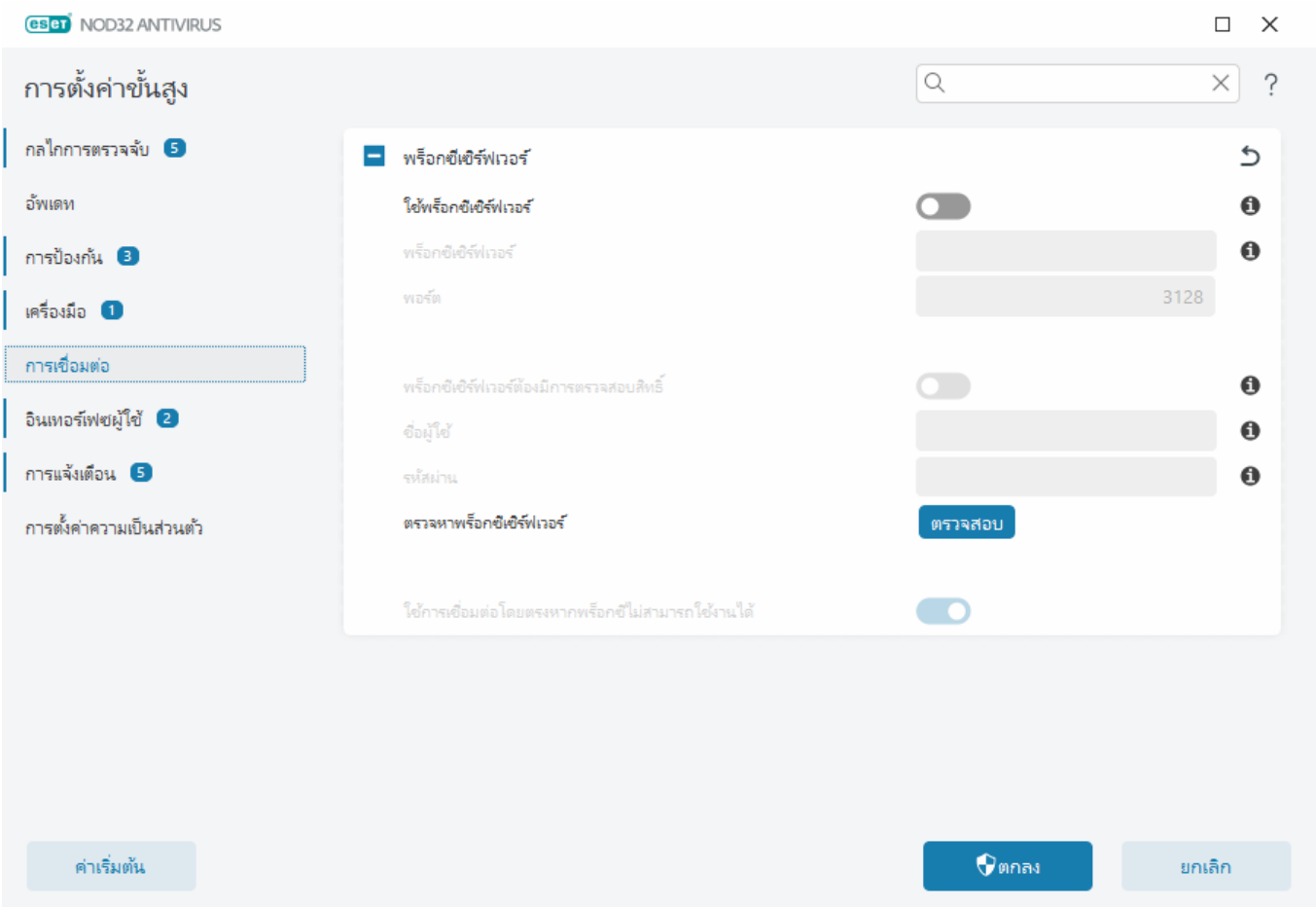
หากการสื่อสารกับพร็อกซี่เซิร์ฟเวอร์ที่จำเป็นต้องมีการตรวจสอบสิทธิ์ ให้เลือก**พร็อกซี่เซิร์ฟเวอร์ต้องมีการตรวจสอบสิทธิ์** แล้วป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** ที่ถูกต้องลงในช่องที่สอดคล้องกัน คลิก **ตรวจหาพร็อกซีเซิร์ฟเวอร์** เพื่อตรวจหา และเพิ่มข้อมูลการตั้งค่าพร็อกซีเซิร์ฟเวอร์โดยอัตโนมัติ ESET NOD32 Antivirus จะคัดลอกพารามิเตอร์ที่

ระบุไว้ในตัวเลือกอินเทอร์เน็ตสำหรับ Internet Explorer หรือ Google Chrome

> คุณต้องป้อนชื่อผู้ใช้และรหัสผ่านของคุณลงในการตั้งค่า **พร็อกซีเซิร์ฟเวอร์** ด้วยตัวเอง

ใช้การเชื่อมต่อโดยตรงหากพร็อกซีไม่สามารถใช้งานได้ – หาก ESET NOD32 Antivirus ถูกกำหนดค่าผ่านพร็อกซี่และไม่สามารถเข้าถึงพร็อกซี่ได้ESET NOD32 Antivirus จะข้ามพร็อกซี่และสื่อสารกับเซิร์ฟเวอร์ ESET โดยตรง

นอกจากนี้ ยังสามารถกำหนดการตั้งค่าพร็อกซีเซิร์ฟเวอร์เริ่มต้นได้โดยไปที่ การตั้งค่าขั้นสูง > **อัพเดท** > **โปรไฟล์** > **อัพเดท** > **ตัวเลือกการเชื่อมต่อ** แล้วเลือก **การเชื่อมต่อผ่านพร็อกซีเซิร์ฟเวอร์** จากเมนูแบบเลื่อนลงสำหรับ **โหมดพร็อกซี** การกำหนดค่านี้ใช้ได้กับการอัพเดทเท่านั้น และแนะนำสำหรับแล็ปท็อปที่ได้รับการอัพเดทโมดูลจากตำแหน่งระยะไกล อ่านข้อมูลเพิ่มเติมได้ที่ การตั้งค่าการอัพเดทขั้นสูง



ส่วนติดต่อกับผู้ใช้

หากต้องการกำหนดค่าอินเทอร์เฟซผู้ใช้แบบกราฟิก (GUI) ของโปรแกรม ให้เปิด การตั้งค่าขั้นสูง > **อินเทอร์เฟซผู้ใช้**

คุณสามารถปรับรูปลักษณ์และเอฟเฟ็กต์ของโปรแกรมได้ใน องค์ประกอบส่วนติดต่อกับผู้ใช้ ของหน้าจอการตั้งค่าขั้น

สูง

เพื่อให้มีการรักษาความปลอดภัยสูงสุดจากซอฟต์แวร์การรักษาความปลอดภัย คุณสามารถป้องกันการถอนการติดตั้งหรือการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตได้โดยปกป้องการตั้งค่าด้วยรหัสผ่านโดยใช้เครื่องมือ ตั้งค่าการเข้าถึง

> หากต้องการกำหนดค่าลักษณะการทำงานของการแจ้งเตือนระบบ การเตือนการตรวจหา และสถานะแอพพลิเคชัน ให้ดูที่ส่วน การแจ้งเตือน

องค์ประกอบของส่วนติดต่อผู้ใช้

คุณสามารถปรับสภาพแวดล้อมการทำงานของ ESET NOD32 Antivirus (GUI) ให้เหมาะกับความต้องการของคุณได้ใน การตั้งค่าขั้นสูง > **อินเทอร์เฟซผู้ใช้** > **องค์ประกอบอินเทอร์เฟซผู้ใช้**

โหมดสี เลือกโทนสีของ ESET NOD32 Antivirus GUI จากเมนูแบบเลื่อนลง:

- **เหมือนกับสีของระบบ** ตั้งค่าโทนสี ESET NOD32 Antivirus ตามการตั้งค่าระบบปฏิบัติการของคุณ
- **มืด** ESET NOD32 Antivirus จะมีโทนสีเข้ม (โหมดมืด)
- **สว่าง** ESET NOD32 Antivirus จะมีโทนสีสว่าง ซึ่งเป็นโทนสีมาตรฐาน

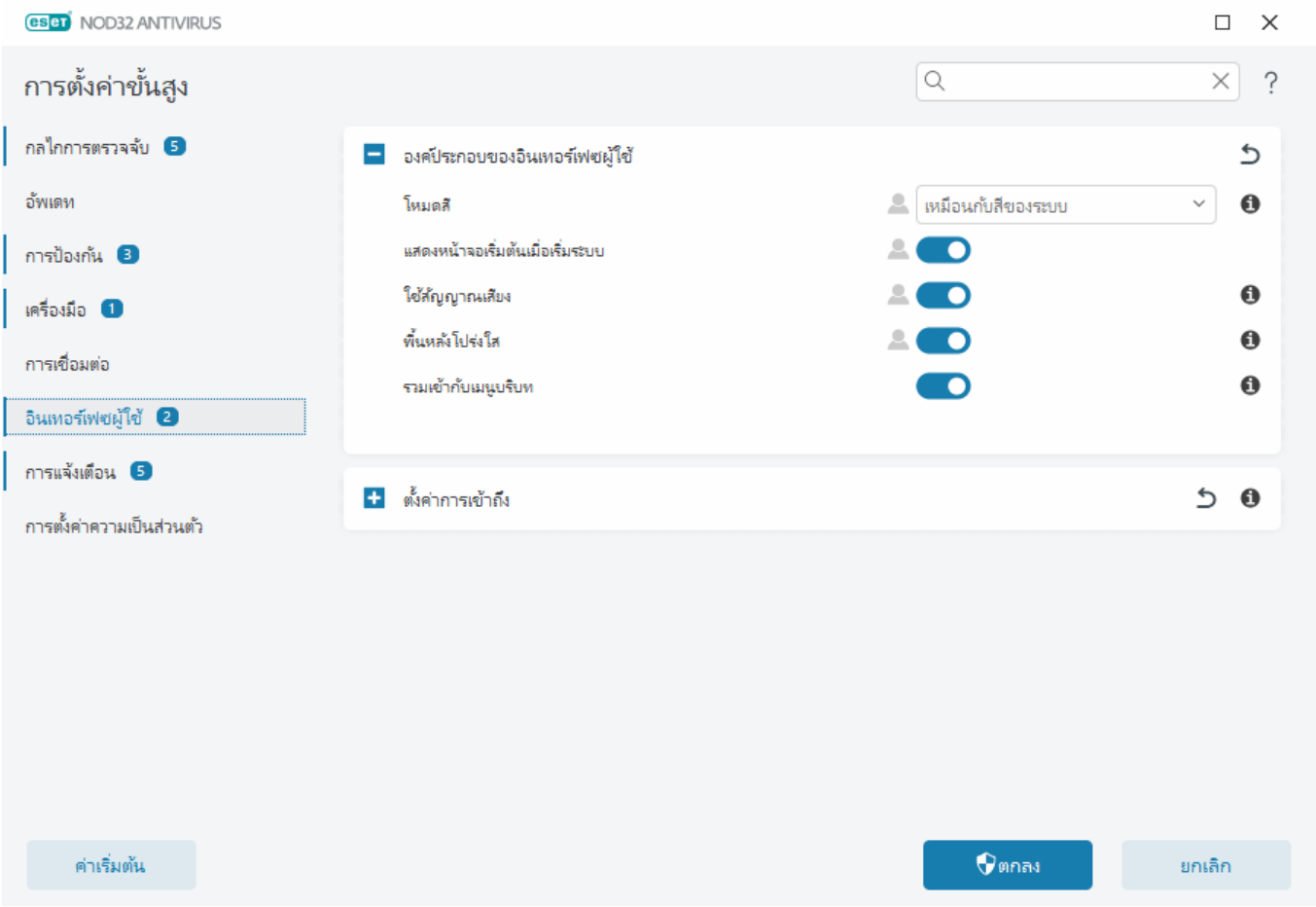
> นอกจากนี้คุณยังสามารถเลือกโทนสีของ ESET NOD32 Antivirus GUI ได้ที่มุมขวาบนของหน้าต่างโปรแกรมหลัก

แสดงหน้าจอเริ่มต้นเมื่อเริ่มต้นระบบ แสดงหน้าจอเริ่มต้นของ ESET NOD32 Antivirus ระหว่างการเริ่มต้นระบบ

ใช้สัญญาณเสียง – เล่นเสียงเมื่อมีเหตุการณ์สำคัญเกิดขึ้นระหว่างการสแกน ตัวอย่างเช่น เมื่อพบภัยคุกคามหรือเมื่อการสแกนเสร็จสิ้น

พื้นหลังโปร่งใส เปิดใช้งานเอฟเฟ็กต์พื้นหลังโปร่งใสสำหรับ หน้าต่างโปรแกรมหลัก พื้นหลังโปร่งใสจะใช้ได้เฉพาะกับ Windows เวอร์ชันล่าสุด (RS4 ขึ้นไป)

รวมเข้ากับเมนูบริบท – รวมองค์ประกอบการควบคุม ESET NOD32 Antivirus ไว้ในเมนูบริบท



ตั้งค่าการเข้าถึง

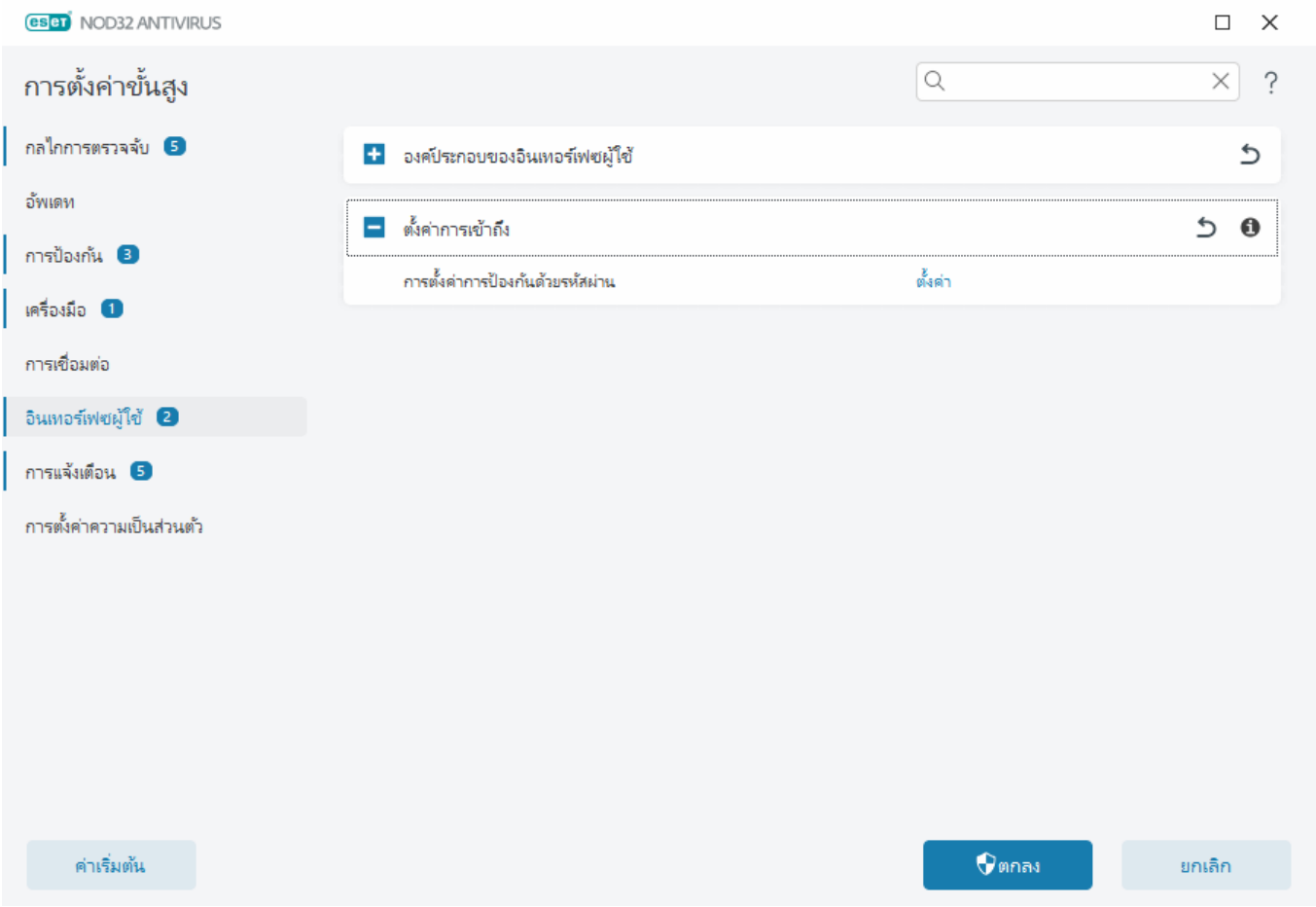
การตั้งค่า ESET NOD32 Antivirus เป็นส่วนสำคัญของนโยบายรักษาความปลอดภัย การแก้ไขโดยไม่ได้รับอนุญาตอาจเป็นอันตรายต่อเสถียรภาพและการป้องกันระบบของคุณ เมื่อต้องการหลีกเลี่ยงการแก้ไขที่ไม่ได้รับอนุญาต คุณสามารถป้องกันพารามิเตอร์การตั้งค่าและการลบการติดตั้ง ESET NOD32 Antivirus ด้วยรหัสผ่านได้ สามารถกำหนดการตั้งค่าการเข้าถึงได้ใน การตั้งค่าขั้นสูง > **อินเทอร์เฟซผู้ใช้** > **การตั้งค่าการเข้าถึง**

หากต้องการตั้งรหัสผ่านเพื่อป้องกันพารามิเตอร์การตั้งค่าและการลบการติดตั้ง ESET NOD32 Antivirus ให้คลิก **ตั้งค่า** ถัดจาก **การตั้งค่าการป้องกันด้วยรหัสผ่าน**

> เมื่อคุณเข้าใช้การตั้งค่าขั้นสูงที่มีการป้องกัน หน้าต่างสำหรับป้อนรหัสผ่านจะแสดงขึ้น หากคุณลืมหรือทำรหัสผ่านหาย ให้คลิกตัวเลือก **เรียกคืนรหัสผ่าน** ด้านล่างแล้วใส่ที่อยู่อีเมลที่คุณใช้ในการลงทะเบียนการสมัครสมาชิก ESET จะส่งอีเมลที่มีรหัสยืนยันความถูกต้องและคำแนะนำเกี่ยวกับวิธีรีเซ็ตรหัสผ่านของคุณ
> • วิธีปลดล็อคการตั้งค่าขั้นสูง

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

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



รหัสผ่านสำหรับการตั้งค่าขั้นสูง

ในการปกป้องการตั้งค่า ESET NOD32 Antivirus ขั้นสูงและเพื่อหลีกเลี่ยงการแก้ไขโดยไม่ได้รับอนุญาต ให้พิมพ์รหัสผ่านใหม่ของคุณในช่อง **รหัสผ่านใหม่** และช่อง **ยืนยันรหัสผ่าน** คลิก**ตกลง**

เมื่อคุณต้องการเปลี่ยนแปลงรหัสผ่านที่มีอยู่แล้ว:

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

รหัสผ่านนี้จำเป็นสำหรับการเข้าถึงการตั้งค่าขั้นสูง

หากคุณลืมรหัสผ่าน โปรดดู ปลดล็อกรหัสผ่านการตั้งค่าของคุณในผลิตภัณฑ์ ESET สำหรับใช้งานในบ้าน

หากต้องการกู้คืน รหัสเปิดใช้งาน ESET ที่สูญหายไป วันที่การสมัครสมาชิกหมดอายุ หรือข้อมูลการสมัครสมาชิกอื่นๆ สำหรับ ESET NOD32 Antivirus โปรดดูที่ ฉันทำรหัสเปิดใช้งานหาย

การสนับสนุนโปรแกรมอ่านหน้าจอ

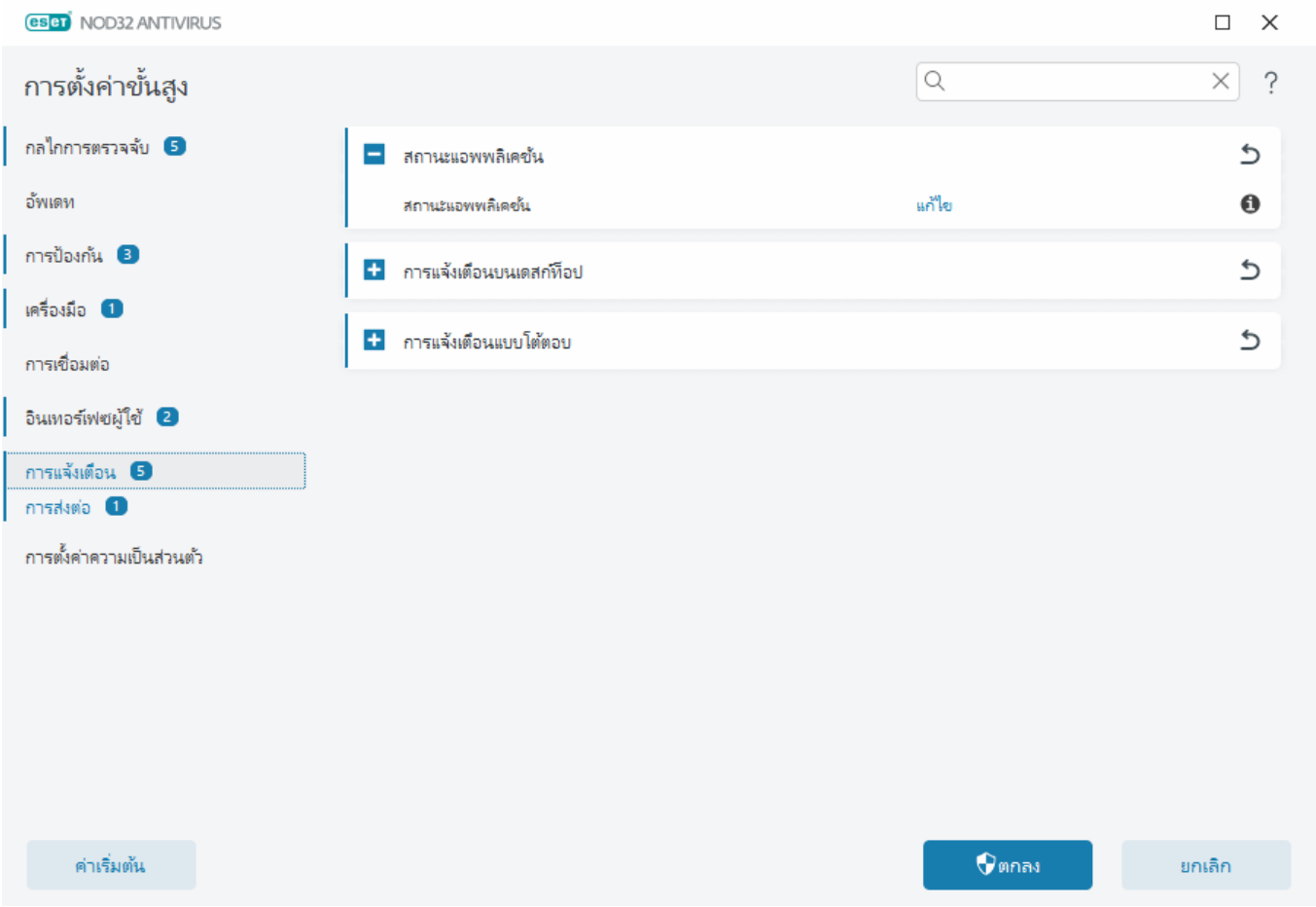
ESET NOD32 Antivirus สามารถใช้งานร่วมกับโปรแกรมอ่านหน้าจอเพื่อให้ผู้ใช้ ESET ที่มีความบกพร่องทางสายตาสามารถนำทางผลิตภัณฑ์หรือตั้งค่าการตั้งค่าได้ โปรแกรมอ่านหน้าจอต่อไปนี้รองรับใน (JAWS, NVDA, Narrator)

เพื่อให้แน่ใจว่าซอฟต์แวร์โปรแกรมอ่านหน้าจอสามารถเข้าถึง GUI ของ ESET NOD32 Antivirus ได้อย่างถูกต้อง ให้ดำเนินการตามคำแนะนำในบทความฐานความรู้ของเรา

การแจ้งเตือน

ในการจัดการการแจ้งเตือนใน ESET NOD32 Antivirus ให้เปิด การตั้งค่าขั้นสูง > **การแจ้งเตือน** คุณสามารถกำหนดค่าการแจ้งเตือนประเภทต่อไปนี้ได้:

- สถานะแอพพลิเคชัน – การแจ้งเตือนที่แสดงใน หน้าต่างโปรแกรมหลัก > **ภาพรวม**
- การแจ้งเตือนบนเดสก์ท็อป – การแจ้งเตือนขนาดเล็กถัดจากแถบงานของระบบ
- การแจ้งเตือนแบบโต้ตอบ – หน้าต่างการเตือนและกล่องข้อความที่ต้องการการโต้ตอบของผู้ใช้
- การส่งต่อ การแจ้งเตือนทางอีเมล – การแจ้งเตือนทางอีเมลจะถูกส่งไปยังที่อยู่อีเมลที่ระบุ



สถานะแอพพลิเคชัน

สถานะแอพพลิเคชัน – คลิก **แก้ไข** เพื่อเลือกสถานะแอพพลิเคชันที่จะแสดงในส่วนหน้าแรกของหน้าต่างโปรแกรมหลัก > **ภาพรวม**

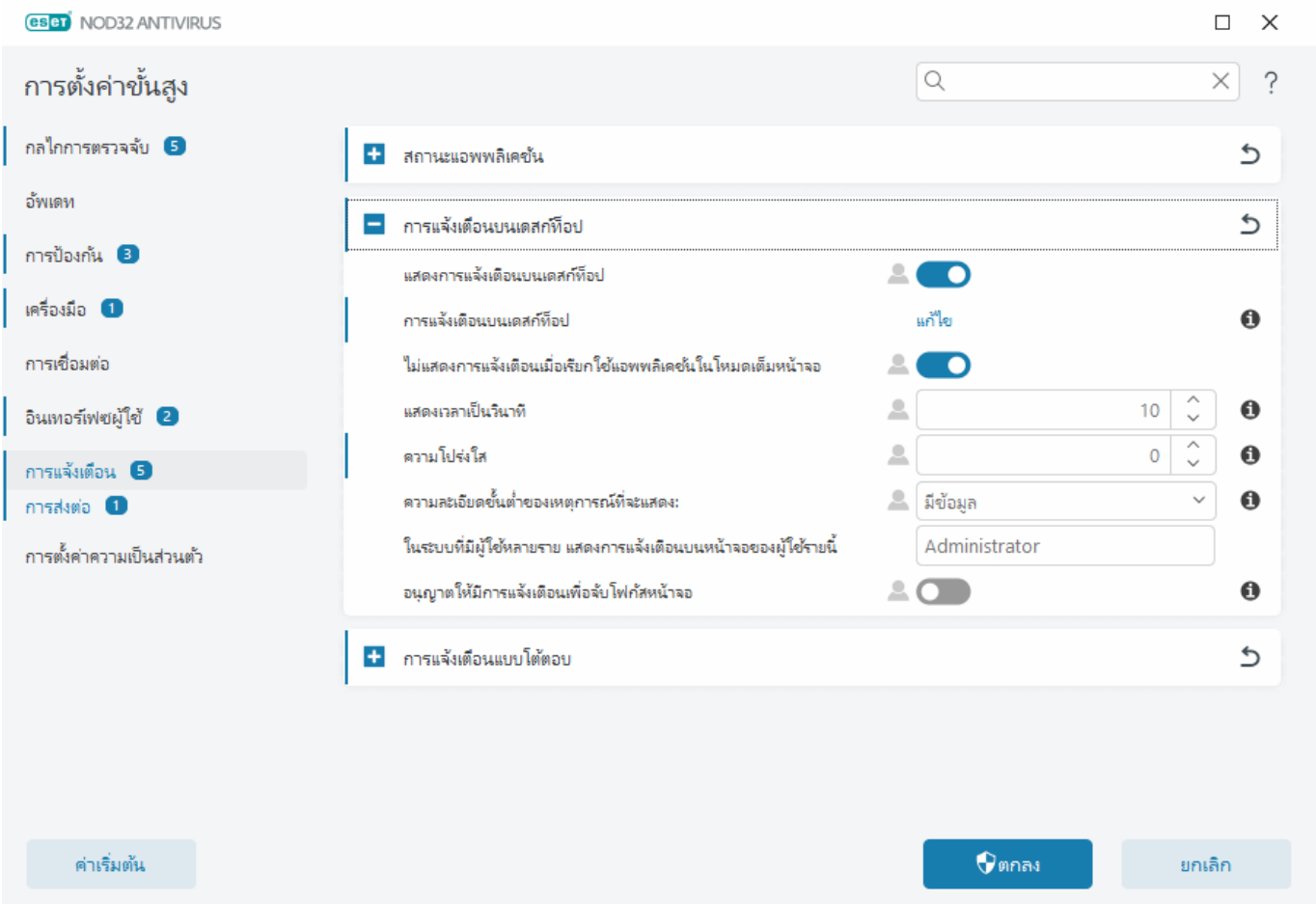
หน้าต่างข้อความ – สถานะแอพพลิเคชัน

ในหน้าต่างข้อความนี้ คุณสามารถเลือกสถานะแอพพลิเคชันที่จะแสดงได้ ตัวอย่างเช่น เมื่อคุณหยุดการป้องกันไวรัสและสปายแวร์ชั่วคราว หรือเปิดใช้งานโหมดผู้เล่นเกมส์

สถานะแอพพลิเคชันจะปรากฏขึ้นด้วย หากผลิตภัณฑ์ของคุณไม่ได้เปิดใช้งานอยู่หรือการสมัครสมาชิกของคุณหมดอายุแล้ว

การแจ้งเตือนบนเดสก์ท็อป

การแจ้งเตือนบนเดสก์ท็อปจะแสดงด้วยหน้าต่างแจ้งเตือนเล็กๆ ซึ่งอยู่ถัดจากแถบงานระบบ ซึ่งถูกตั้งค่าให้แสดงเป็นเวลา 10 วินาทีโดยค่าเริ่มต้น ก่อนจะค่อยๆ หายไปอย่างช้าๆ การแจ้งเตือนจะประกอบด้วยการอัพเดทผลิตภัณฑ์ที่เสร็จสิ้น อุปกรณ์ใหม่ที่เชื่อมต่อ งานด้านการสแกนไวรัสที่เสร็จสมบูรณ์ หรือการค้นพบภัยคุกคามใหม่



แสดงการแจ้งเตือนบนเดสก์ท็อป – เราขอแนะนำให้เปิดใช้งานตัวเลือกนี้เพื่อให้ผลิตภัณฑ์สามารถแจ้งให้คุณทราบเมื่อมีเหตุการณ์ใหม่เกิดขึ้น

การแจ้งเตือนบนเดสก์ท็อป – คลิก **แก้ไข** เพื่อเปิดใช้งานหรือปิดใช้งาน การแจ้งเตือนบนเดสก์ท็อป ที่ต้องการ

อย่าแสดงการแจ้งเตือนเมื่อเรียกใช้แอพพลิเคชันในโหมดเต็มหน้าจอ – ระงับการแจ้งเตือนที่ไม่โต้ตอบทั้งหมดเมื่อเรียกใช้แอพพลิเคชันในโหมดเต็มหน้าจอ

แสดงเวลาเป็นวินาที – ตั้งค่าระยะเวลาที่สามารถมองเห็นการแจ้งเตือนได้ โดยค่านี้จะต้องอยู่ระหว่าง 3-30 วินาที

ความโปร่งใส – ตั้งค่าเปอร์เซ็นต์ความโปร่งใสของการแจ้งเตือน ค่านี้จะรองรับช่วงตั้งแต่ 0 (ไม่โปร่งใส) ไปจนถึง 80 (ความโปร่งใสสูงมาก)

ความละเอียดขั้นต่ำของเหตุการณ์ที่จะแสดง – ตั้งค่าระดับความรุนแรงเริ่มต้นของการแจ้งเตือนที่จะแสดง จากเมนูแบบเลื่อนลง ให้เลือกตัวเลือกต่อไปนี้:

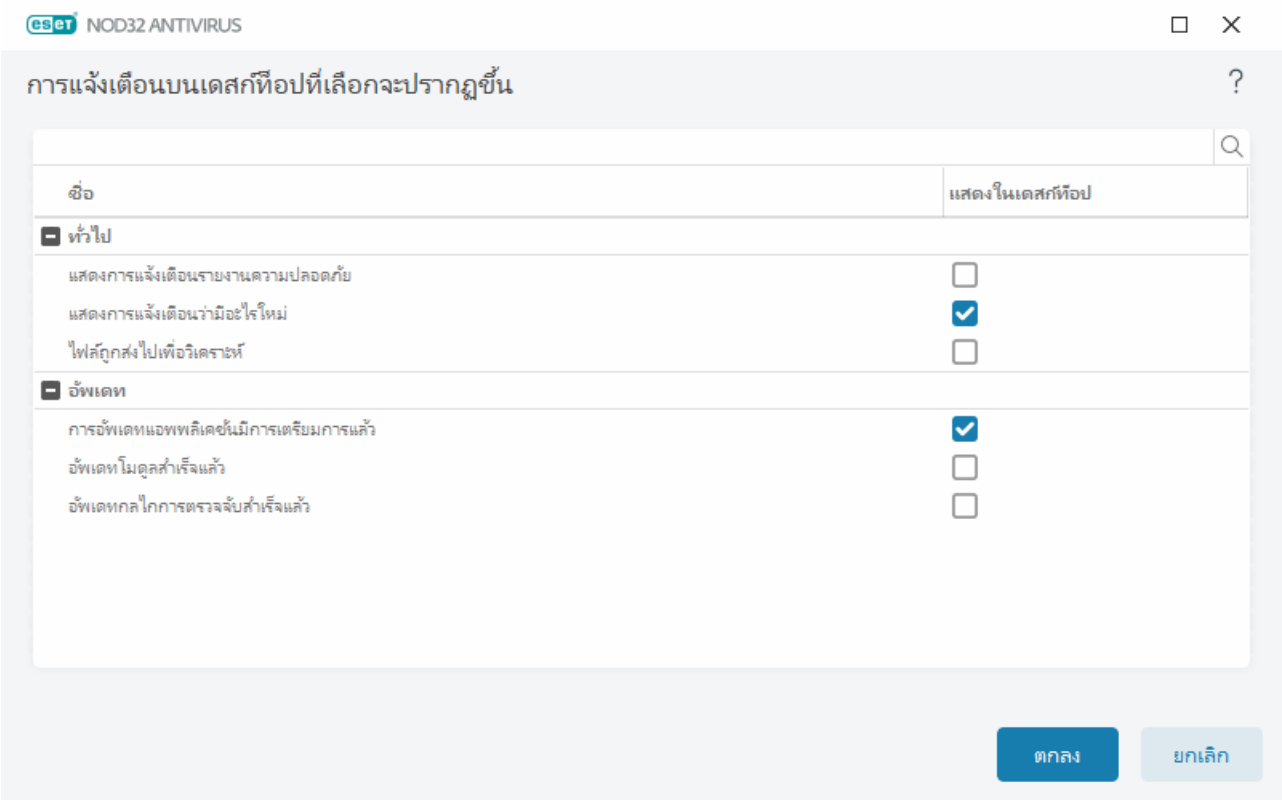
- **การวินิจฉัย** – แสดงข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- **แจ้งข้อมูล** – แสดงข้อความแจ้งข้อมูล เช่น กิจกรรมเครือข่ายที่ไม่ปกติ รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – แสดงข้อความเตือน ข้อผิดพลาด และข้อผิดพลาดร้ายแรง (เช่น อัพเดทไม่สำเร็จ)
- **ข้อผิดพลาด** – แสดงข้อผิดพลาด (เช่น การป้องกันไฟล์เอกสารไม่เริ่มต้นทำงาน) และข้อผิดพลาดร้ายแรง
- **ร้ายแรง** – แสดงเฉพาะข้อผิดพลาดร้ายแรง (พบข้อผิดพลาดในการเริ่มต้นการป้องกันไวรัสหรือระบบที่ติดไวรัส และอื่นๆ)

ในระบบที่มีผู้ใช้หลายราย แสดงการแจ้งเตือนบนหน้าจอของผู้ใช้รายนี้ – อนุญาตให้บัญชีที่เลือกสามารถรับการแจ้งเตือนบนเดสก์ท็อปได้ ตัวอย่างเช่น หากคุณไม่ได้ใช้บัญชีผู้ดูแลระบบ ให้พิมพ์ชื่อเต็มของบัญชี จากนั้นระบบจะแสดงการแจ้งเตือนบนเดสก์ท็อปสำหรับบัญชีที่ระบุ โดยจะมีเพียงบัญชีเดียวเท่านั้นที่สามารถรับการแจ้งเตือนบนเดสก์ท็อปได้

อนุญาตให้การแจ้งเตือนจับโฟกัสหน้าจอได้ – อนุญาตให้การแจ้งเตือนจับโฟกัสหน้าจอและเข้าถึงได้ด้วยเมนู **ALT + Tab**

รายการการแจ้งเตือนบนเดสก์ท็อป

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



ทั่วไป

แสดงการแจ้งเตือนรายงานความปลอดภัย – รับการแจ้งเตือนเมื่อมีการสร้าง รายงานความปลอดภัย ใหม่

แสดงการแจ้งเตือนว่ามีอะไรใหม่ – การแจ้งเตือนเกี่ยวกับคุณลักษณะของเวอร์ชันผลิตภัณฑ์ล่าสุดที่ได้รับการปรับปรุงใหม่ทั้งหมด

ไฟล์ถูกส่งไปเพื่อการวิเคราะห์ - รับการแจ้งเตือนทุกครั้งที่ ESET NOD32 Antivirus ส่งไฟล์สำหรับการวิเคราะห์

ตรวจสอบเครือข่าย

แจ้งเตือนเกี่ยวกับอุปกรณ์เครือข่ายที่เพิ่งค้นพบ - รับการแจ้งเตือนเมื่ออุปกรณ์ใหม่เชื่อมต่อกับเครือข่าย

การป้องกันเครือข่าย

โปรไฟล์เครือข่ายเปลี่ยนแปลง - รับการแจ้งเตือนเมื่อมีการเปลี่ยนโปรไฟล์เครือข่าย

คำเตือนการป้องกัน Wifi > รับการแจ้งเตือนเมื่อคุณพยายามเชื่อมต่อกับเครือข่าย Wi-Fi ที่มีรหัสผ่านที่ไม่รัดกุมหรือไม่มีเลย

อัพเดท

เตรียมอัปเดตแอพพลิเคชันแล้ว – รับการแจ้งเตือนเมื่อมีการอัปเดตเป็นเวอร์ชันใหม่ ESET NOD32 Antivirus ที่เตรียมไว้แล้ว

กลไกการตรวจหาได้รับการปรับปรุงเรียบร้อยแล้ว – รับการแจ้งเตือนเมื่อผลิตภัณฑ์การอัพเดทโมดูลกลไกการตรวจจับ

โมดูลได้รับการปรับปรุงเรียบร้อยแล้ว - รับการแจ้งเตือนเมื่อผลิตภัณฑ์อัพเดทส่วนประกอบของโปรแกรม

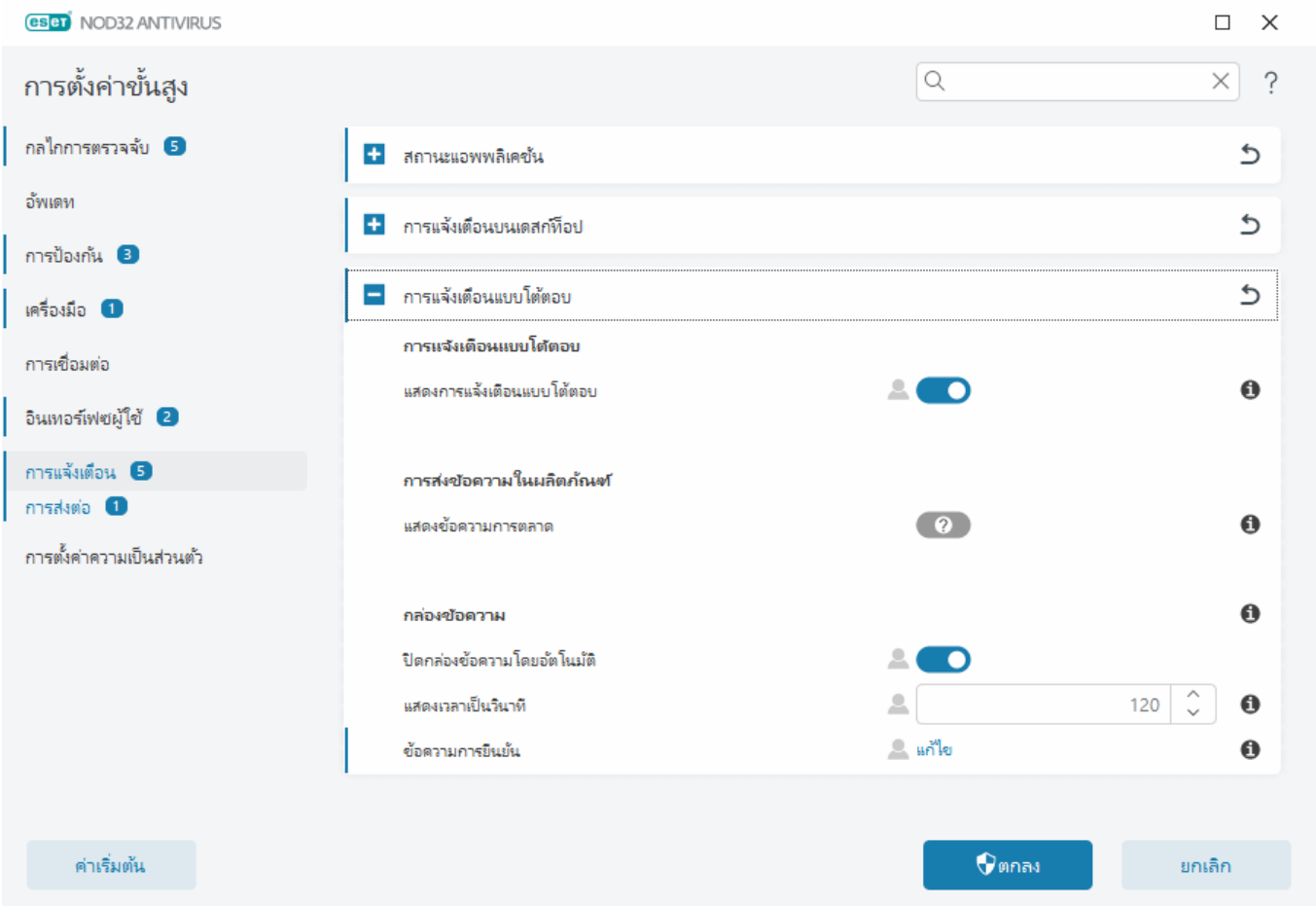
หากต้องการตั้งค่าทั่วไปสำหรับการแจ้งเตือนบนเดสก์ท็อป ตัวอย่างเช่น ข้อความจะปรากฏขึ้นนานเพียงใดหรือความละเอียดขั้นต่ำของเหตุการณ์ที่จะแสดง ดูที่ การแจ้งเตือนบนเดสก์ท็อป ใน การตั้งค่าขั้นสูง > **การแจ้งเตือน**

การแจ้งเตือนแบบโต้ตอบ

มองหาข้อมูลเกี่ยวกับการเตือนและการแจ้งเตือนทั่วไปอยู่ใช่ไหม

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

ส่วน **การแจ้งเตือนแบบโต้ตอบ** ใน การตั้งค่าขั้นสูง > **การแจ้งเตือน** ช่วยให้คุณสามารถกำหนดค่าวิธีการที่กล่องข้อความและการแจ้งเตือนแบบโต้ตอบสำหรับการตรวจจับ ซึ่งจำเป็นต้องมีการตัดสินใจโดยผู้ใช้ (ตัวอย่างเช่น เว็บไซต์ที่อาจเป็นการฟิชชิ่ง) จะได้รับการจัดการโดย ESET NOD32 Antivirus



การแจ้งเตือนแบบโต้ตอบ

การปิดใช้งาน **แสดงการแจ้งเตือนแบบโต้ตอบ** จะซ่อนหน้าต่างการเตือนและข้อความในเบราว์เซอร์ทั้งหมด และจะเหมาะสำหรับสถานการณ์เฉพาะที่มีจำนวนจำกัดเท่านั้น เราขอแนะนำให้เปิดใช้งานตัวเลือกนี้ไว้

การส่งข้อความในผลิตภัณฑ์

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

กล่องข้อความ

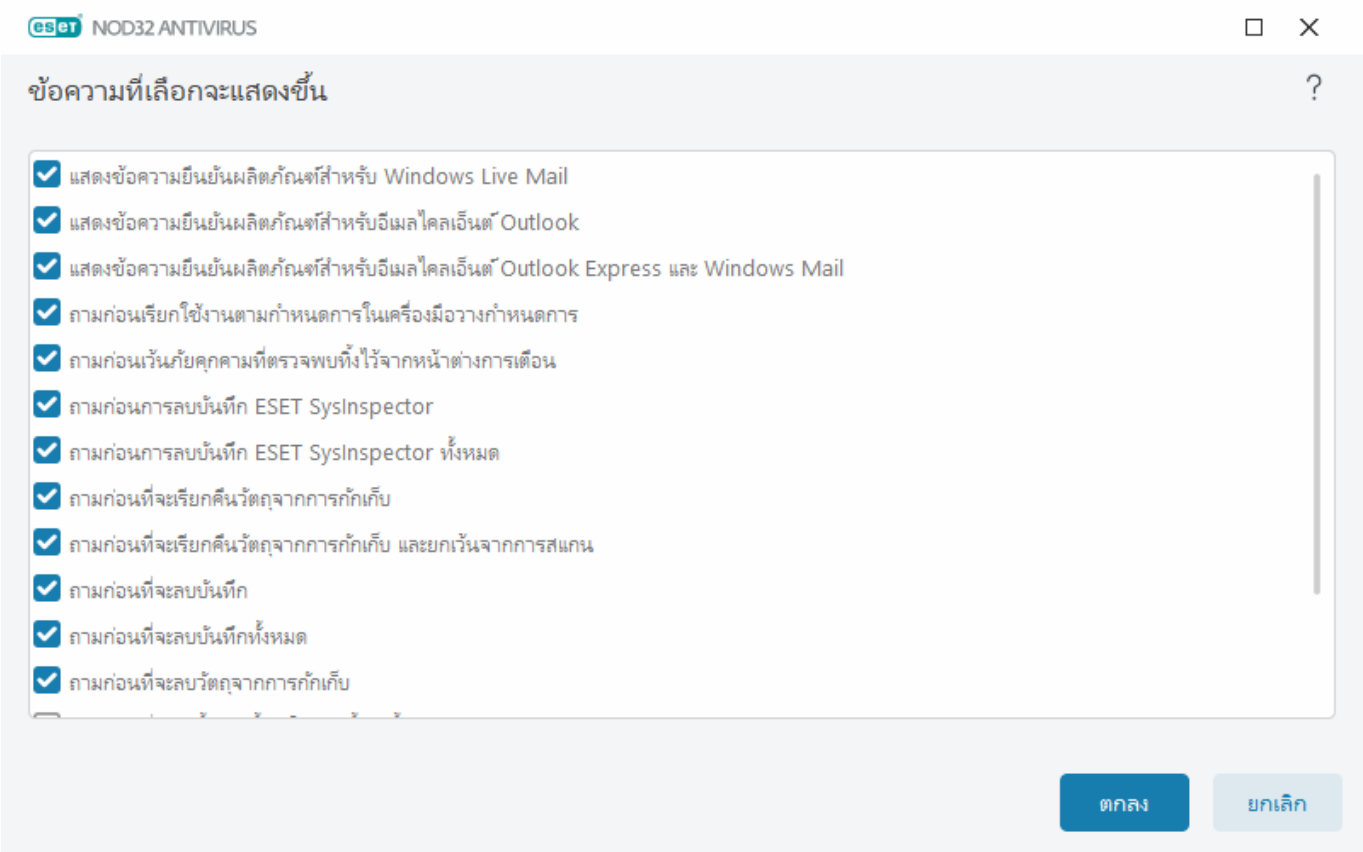
หากต้องการปิดกล่องข้อความโดยอัตโนมัติหลังจากปรากฏมาเป็นระยะเวลาหนึ่ง ให้เลือก **ปิดกล่องข้อความโดยอัตโนมัติ** หากไม่ปิดหน้าต่างดังกล่าวด้วยตนเอง หน้าต่างการเตือนจะปิดโดยอัตโนมัติหลังจากหมดเวลาตามที่กำหนด

แสดงเวลาเป็นวินาที – ตั้งค่าระยะเวลาที่สามารถมองเห็นการเตือนได้ โดยค่านี้จะต้องอยู่ระหว่าง 10-999 วินาที

ข้อความการยืนยัน – คลิก **แก้ไข** เพื่อแสดง รายการของข้อความการยืนยัน ซึ่งคุณสามารถเลือกให้แสดงหรือไม่แสดงก็ได้

ข้อความการยืนยัน

ในการปรับข้อความการยืนยัน ให้ไปที่ การตั้งค่าขั้นสูง > **การแจ้งเตือน** > **การแจ้งเตือนแบบโต้ตอบ** และคลิก **แก้ไข** ถัดจาก **ข้อความการยืนยัน**



หน้าต่างข้อความนี้แสดงข้อความการยืนยันที่ ESET NOD32 Antivirus จะแสดงขึ้นมาก่อนที่จะดำเนินการทำงานใดๆ เลือกหรือยกเลิกการเลือกกล่องทำเครื่องหมายที่อยู่ถัดจากแต่ละข้อความการยืนยันเพื่ออนุญาตหรือปิดใช้งานข้อความเหล่านั้น

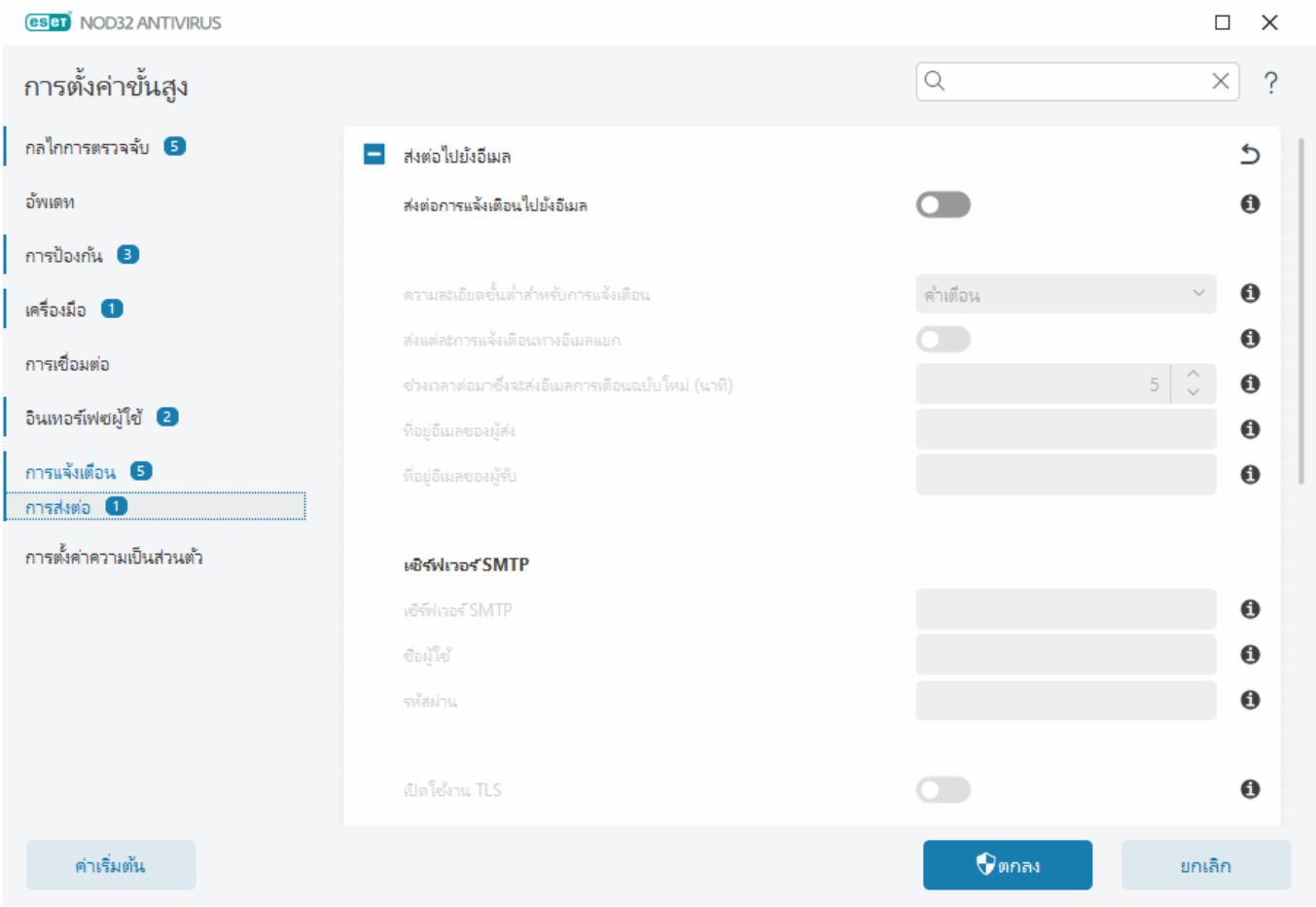
เรียนรู้เพิ่มเติมเกี่ยวกับคุณลักษณะเฉพาะที่เกี่ยวข้องกับข้อความการยืนยัน:

- ถามก่อนที่จะลบบันทึก ESET SysInspector
- ถามก่อนที่จะลบบันทึก ESET SysInspector ทั้งหมด
- ถามก่อนที่จะลบวัตถุจากการกักเก็บ

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

การส่งต่อ

ESET NOD32 Antivirus สามารถส่งอีเมลแจ้งเตือนได้โดยอัตโนมัติหากมีเหตุการณ์ที่มีระดับความละเอียดที่เลือกไว้เกิดขึ้น เปิด การตั้งค่าขั้นสูง > **การแจ้งเตือน** > **การส่งต่อ** และเปิดใช้งาน **ส่งต่อการแจ้งเตือนไปยังอีเมล** เพื่อเปิดใช้งานการแจ้งเตือนทางอีเมล



จากเมนูแบบเลื่อนลง **ความละเอียดขั้นต่ำสำหรับการแจ้งเตือน** คุณสามารถเลือกระดับความรุนแรงเริ่มต้นของการแจ้งเตือนที่จะส่ง

- **การวินิจฉัย** – บันทึกข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรม และบันทึกทั้งหมดข้างต้น
- **มีข้อมูล** – บันทึกข้อความแจ้งข้อมูล เช่น กิจกรรมเครือข่ายที่ไม่ได้มาตรฐาน รวมถึงข้อความการอัพเดทที่เสร็จสมบูรณ์ และบันทึกทั้งหมดข้างต้น
- **คำเตือน** – บันทึกข้อผิดพลาดร้ายแรงและข้อความเตือน (เช่น อัพเดทไม่สำเร็จ)
- **ข้อผิดพลาด** – ข้อผิดพลาด (ไม่ได้เริ่มต้นการป้องกันเอกสาร) และข้อผิดพลาดร้ายแรงจะถูกบันทึก
- **ร้ายแรง** – บันทึกเฉพาะข้อผิดพลาดร้ายแรง (เช่น พบข้อผิดพลาดในการเริ่มต้นการป้องกันไวรัส หรือ พบภัยคุกคาม)

ส่งการแจ้งเตือนแต่ละรายการทางอีเมลแยก – เมื่อเปิดใช้งาน ผู้รับจะได้รับอีเมลใหม่สำหรับแต่ละการแจ้งเตือน ซึ่งอาจส่งผลให้ได้รับอีเมลจำนวนมากในระยะเวลาอันสั้น

ช่วงเวลาต่อมาซึ่งจะส่งอีเมลการเตือนฉบับใหม่ (นาที) – ช่วงเวลาต่อมาเป็นนาทีซึ่งจะส่งการเตือนฉบับใหม่ไป

ยังอีเมล ช่วงเวลาต่อมาซึ่ฉบับใหม่ไปยังอีเมล หากคุณตั้งค่านี้เป็น 0 การแจ้งเตือนเหล่านั้นจะถูกส่งในทันที

ที่อยู่ของผู้ส่ง – ระบุที่อยู่ของผู้ส่งซึ่งจะแสดงที่ส่วนหัวของอีเมลการแจ้งเตือน

ที่อยู่ของผู้รับ – ระบุที่อยู่ของผู้รับที่จะแสดงในส่วนหัวของอีเมลการแจ้งเตือน รองรับหลายค่า ใช้เครื่องหมายอัฒภาคเป็นตัวคั่น

SMTP เซิร์ฟเวอร์

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

i เซิร์ฟเวอร์ SMTP ที่มีการเข้ารหัส TLS นั้น ได้รับการสนับสนุนโดย ESET NOD32 Antivirus

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

เปิดใช้งาน TLS – Secure Alert และข้อความการแจ้งเตือนโดยไม่ใช้การเข้ารหัส TLS

ทดสอบการเชื่อมต่อ SMTP – อีเมลทดสอบจะถูกส่งไปยังที่อยู่อีเมลของผู้รับ จะต้องเติมเซิร์ฟเวอร์ SMTP ชื่อผู้ใช้ รหัสผ่าน ที่อยู่ของผู้ส่ง และที่อยู่ของผู้รับ

รูปแบบข้อความ

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

รูปแบบของข้อความเหตุการณ์ – รูปแบบข้อความของเหตุการณ์ที่แสดงบนคอมพิวเตอร์ระยะไกล

รูปแบบของข้อความเตือนภัยคุกคาม – ข้อความการเตือนและข้อความการแจ้งเตือนภัยคุกคามจะมีรูปแบบเริ่มต้นที่กำหนดไว้ล่วงหน้า เราขอแนะนำให้เก็บรูปแบบที่กำหนดล่วงหน้านี้ไว้ แต่ในบางกรณี (ตัวอย่างเช่น หากคุณมีระบบประมวลผลอีเมลอัตโนมัติ) คุณอาจต้องการเปลี่ยนรูปแบบข้อความ

Charset – แปลงข้อความอีเมลเป็นการเข้ารหัสอักขระแบบ ANSI ตามการตั้งค่า Windows Regional (ตัวอย่างเช่น windows-1250, Unicode (UTF-8), ACSII 7-bit หรือภาษาญี่ปุ่น (ISO-2022-JP)) ซึ่งทำให้ "á" จะถูกเปลี่ยนเป็น "a" และสัญลักษณ์ที่ไม่รู้จักจะเปลี่ยนเป็น "?"

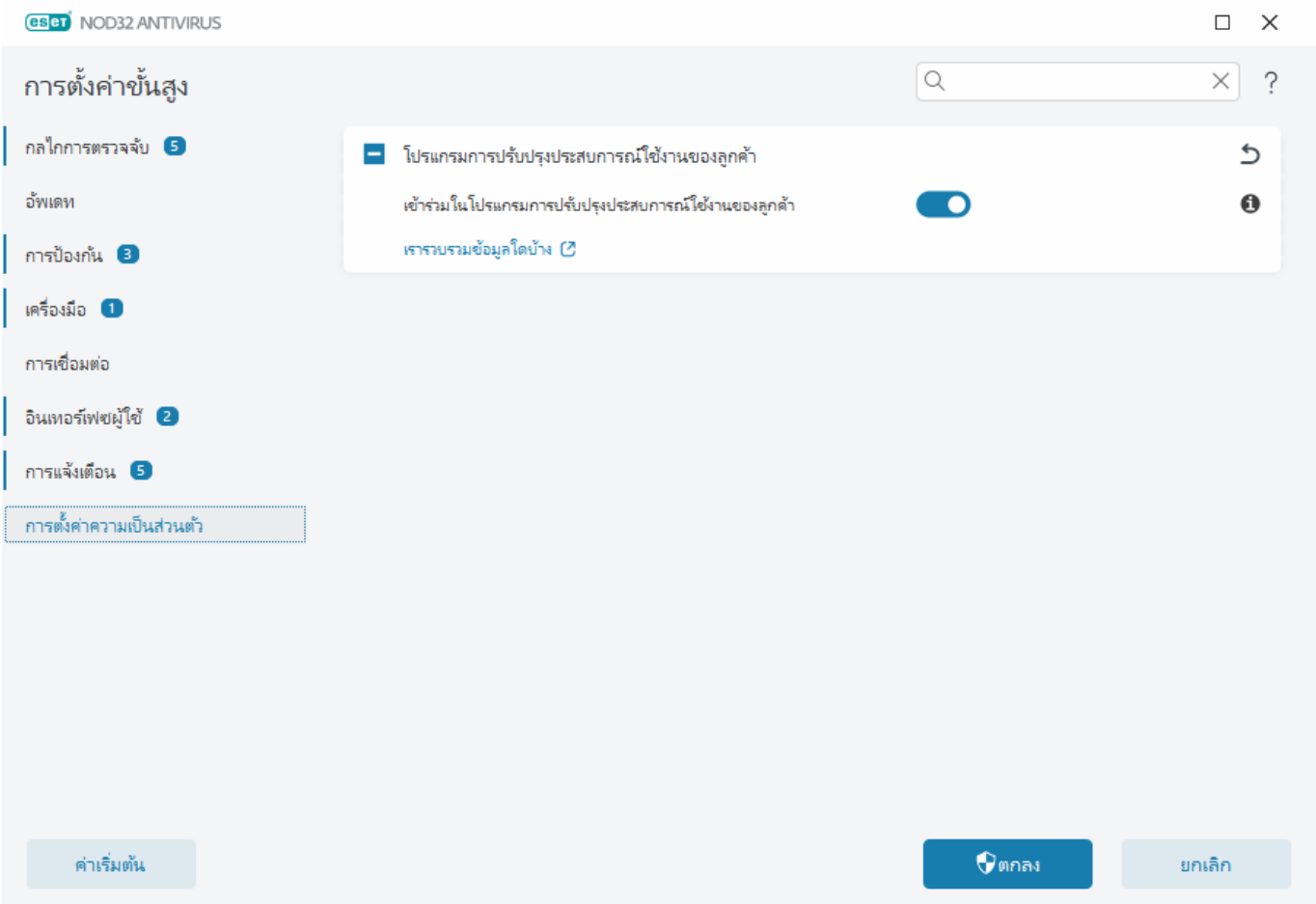
ใช้การเข้ารหัสในรูปแบบ Quoted-printable - ที่มาของข้อความอีเมลจะถูกเข้ารหัสในรูปแบบ Quoted-printable (QP) ซึ่งใช้อักขระ ASCII และสามารถส่งอักขระพิเศษของภาษาทางอีเมลได้อย่างถูกต้องในรูปแบบ 8 บิต (áéíóú)

- **%TimeStamp%** - วันที่และเวลาของเหตุการณ์
- **%Scanner%** -โมดูลที่เกี่ยวข้อง
- **%ComputerName%** - ชื่อคอมพิวเตอร์ซึ่งมีการเตือนเกิดขึ้น
- **%ProgramName%** - โปรแกรมที่สร้างการเตือน
- **%InfectedObject%** – ชื่อของไฟล์ ข้อความ หรือรายการอื่นๆ ที่ติดไวรัส
- **%VirusName%** - การระบุการติดไวรัส
- **%Action%** – การทำงานที่ควบคุมการแฝงตัว
- **%ErrorDescription%** - คำอธิบายเหตุการณ์ที่ไม่ใช่ไวรัส

คำหลัก **%InfectedObject%** และ **%VirusName%** จะใช้เฉพาะสำหรับข้อความเตือนภัยคุกคามเท่านั้น และ **%ErrorDescription%** จะใช้เฉพาะในข้อความของเหตุการณ์

การตั้งค่าความเป็นส่วนตัว

เปิด การตั้งค่าขั้นสูง > **การตั้งค่าความเป็นส่วนตัว**



โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า

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

แปลงกลับเป็นการตั้งค่าเริ่มต้น

คลิก **ค่าเริ่มต้น** การตั้งค่าขั้นสูง เพื่อแปลงการตั้งค่าโปรแกรมทั้งหมดสำหรับโมดูลทั้งหมดกลับ สิ่งนี้จะถูกรีเซ็ตกลับเป็นสถานะที่เคยมีหลังการติดตั้งใหม่

โปรดดู การตั้งค่าการนำเข้าและส่งออก

แปลงกลับการตั้งค่าทุกอย่างในส่วนปัจจุบัน

คลิกลูกศรโค้ง เพื่อแปลงกลับการตั้งค่าทุกอย่างในส่วนปัจจุบันไปเป็นการตั้งค่าเริ่มต้นที่กำหนดโดย ESET

โปรดทราบว่า การเปลี่ยนแปลงใดๆ ที่ดำเนินการไว้จะสูญหายหลังจากที่คุณคลิก **แปลงกลับเป็นค่าเริ่มต้น**

แปลงกลับสารบัญ – เมื่อเปิดใช้งานตัวเลือกนี้ กฎ งานหรือโปรไฟล์ที่ได้เพิ่มด้วยตนเองหรือโดยอัตโนมัติจะสูญหาย

โปรดดู [การตั้งค่าการนำเข้าและส่งออก]

เกิดข้อผิดพลาดขณะบันทึกการกำหนดค่า

ข้อความแสดงข้อผิดพลาดนี้ระบุว่าระบบไม่ได้บันทึกการตั้งค่าอย่างถูกต้อง เนื่องจากเกิดข้อผิดพลาด

ซึ่งมักหมายความว่าผู้ใช้ที่พยายามจะปรับแต่งพารามิเตอร์โปรแกรมจะ:

- มีสิทธิ์การเข้าถึงไม่เพียงพอหรือไม่มีสิทธิ์พิเศษของระบบปฏิบัติการที่จำเป็นต้องใช้ในการปรับแต่งไฟล์การกำหนดค่าและรีจิสทรีระบบ
  > ในการดำเนินการแก้ไขตามต้องการ ผู้ดูแลระบบต้องลงชื่อเข้า

- ได้เปิดใช้งานโหมดการเรียนรู้ใน HIPS หรือไฟร์วอลล์ และพยายามจะเปลี่ยนแปลงการตั้งค่าขั้นสูง
  > ในการบันทึกการกำหนดค่าและหลีกเลี่ยงข้อขัดแย้งในการกำหนดค่า ให้ปิดการตั้งค่าขั้นสูงโดยไม่บันทึกและพยายามเปลี่ยนแปลงตามต้องการอีกครั้ง

สาเหตุทั่วไปลำดับที่สองอาจเป็นการที่โปรแกรมไม่สามารถทำงานได้อย่างถูกต้อง เกิดความเสียหาย และต้องติดตั้งใหม่

เครื่องมือสแกนของบรรทัดคำสั่ง

โมดูลป้องกันไวรัสของ ESET NOD32 Antivirus นั้นสามารถเรียกใช้ผ่านบรรทัดคำสั่ง ทั้งด้วยตนเอง (โดยใช้คำสั่ง "ecls") หรือใช้ไฟล์แบทช์ ("bat")

การใช้เครื่องสแกนบรรทัดคำสั่งของ ESET:

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

คุณสามารถใช้พารามิเตอร์และสวิตช์ต่อไปนี้ขณะที่เรียกใช้เครื่องมือสแกนตามต้องการจากบรรทัดคำสั่ง:

ตัวเลือก

/base-dir=โฟลเดอร์	โหลดโมดูลจากโฟลเดอร์
/quar-dir=โฟลเดอร์	โฟลเดอร์กักเก็บ
/exclude=มาสก์	ยกเว้นไฟล์ที่ตรงกับมาสก์ในการสแกน
/subdir	สแกนโฟลเดอร์ย่อย (เริ่มต้น)
/no-subdir	ไม่สแกนโฟลเดอร์ย่อย
/max-subdir-level=LEVEL	จำนวนระดับย่อยสูงสุดของโฟลเดอร์ภายในโฟลเดอร์ที่จะสแกน
/symlink	ตามลิงค์สัญลักษณ์ (เริ่มต้น)
/no-symlink	ข้ามลิงค์สัญลักษณ์
/ads	สแกน ADS (เริ่มต้น)
/no-ads	ไม่สแกน ADS
/log-file=ไฟล์	บันทึกผลลัพธ์ไปที่ไฟล์
/log-rewrite	เขียนทับไฟล์ผลลัพธ์ (เริ่มต้น - ต่อท้าย)
/log-console	บันทึกผลลัพธ์ไปที่คอนโซล (เริ่มต้น)
/no-log-console	ไม่บันทึกผลลัพธ์ไปที่คอนโซล
/log-all	บันทึกไฟล์ที่ไม่ติดไวรัส
/no-log-all	ไม่บันทึกไฟล์ที่ไม่ติดไวรัส (เริ่มต้น)
/aind	แสดงสัญลักษณ์ของการทำงาน
/auto	สแกนและกำจัดโดยอัตโนมัติดิสก์ภายในเครื่องทั้งหมด

ตัวเลือกเครื่องมือสแกน

/files	สแกนไฟล์ (เริ่มต้น)
/no-files	ไม่สแกนไฟล์
/memory	สแกนหน่วยความจำ
/boots	สแกนบูตเซคเตอร์
/no-boots	ไม่สแกนบูตเซคเตอร์ (เริ่มต้น)
/arch	สแกนที่เก็บเอกสาร (เริ่มต้น)
/no-arch	ไม่สแกนที่เก็บเอกสาร
/max-obj-size=ขนาด	สแกนเฉพาะไฟล์ที่เล็กกว่า SIZE เมกะไบต์ (เริ่มต้น 0 = ไม่จำกัด)
/max-arch-level=LEVEL	จำนวนระดับย่อยสูงสุดของที่เก็บเอกสารภายในที่เก็บเอกสาร (ที่เก็บเอกสารซ้อน) ที่จะสแกน
/scan-timeout=จำกัด	สแกนที่เก็บเอกสารเป็นเวลาสูงสุดไม่เกิน LIMIT วินาที
/max-arch-size=ขนาด	สแกนไฟล์ในที่เก็บเอกสารเฉพาะเมื่อไฟล์มีขนาดเล็กกว่า SIZE (เริ่มต้น 0 = ไม่จำกัด)

/max-sfx-size=ขนาด	สแกนเฉพาะไฟล์ในที่เก็บเอกสารที่ขยายในตัว ถ้ามีขนาดเล็กกว่า SIZE เมกะไบต์ (เริ่มต้น 0 = ไม่จำกัด)
/mail	สแกนไฟล์อีเมล (เริ่มต้น)
/no-mail	ไม่สแกนไฟล์อีเมล
/mailbox	สแกนกล่องจดหมาย (เริ่มต้น)
/no-mailbox	ไม่สแกนกล่องจดหมาย
/sfx	สแกนที่เก็บเอกสารที่ขยายในตัว (เริ่มต้น)
/no-sfx	ไม่สแกนที่เก็บเอกสารที่ขยายในตัว
/rtp	สแกนรันไทม์แพ็คเกอร์ (เริ่มต้น)
/no-rtp	ไม่สแกนรันไทม์แพ็คเกอร์
/unsafe	สแกนหาแอพพลิเคชันที่อาจไม่ปลอดภัย
/no-unsafe	ไม่สแกนหาแอพพลิเคชันที่อาจไม่ปลอดภัย (เริ่มต้น)
/unwanted	สแกนหาแอพพลิเคชันที่อาจไม่พึงประสงค์
/no-unwanted	ไม่สแกนหาแอพพลิเคชันที่อาจไม่พึงประสงค์ (เริ่มต้น)
/suspicious	สแกนหาแอพพลิเคชันที่น่าสงสัย (ค่าเริ่มต้น)
/no-suspicious	ไม่สแกนหาแอพพลิเคชันที่อาจน่าสงสัย
/pattern	ใช้ฐานข้อมูล (เริ่มต้น)
/no-pattern	ไม่ใช้ฐานข้อมูล
/heur	เปิดใช้งานการวิเคราะห์พฤติกรรม (เริ่มต้น)
/no-heur	ปิดใช้งานการวิเคราะห์พฤติกรรม
/adv-heur	เปิดใช้งานการวิเคราะห์พฤติกรรมขั้นสูง (เริ่มต้น)
/no-adv-heur	ปิดใช้งานการวิเคราะห์พฤติกรรมขั้นสูง
/ext-exclude=ส่วนขยาย	ไม่รวมไฟล์ EXTENSIONS ที่คั่นด้วยเครื่องหมายโคลอนในการสแกน
/clean-mode=โหมด	ใช้โหมดการกำจัดสำหรับวัตถุที่ติดไวรัส ตัวเลือกที่ใช้ได้มีดังนี้: • none (ค่าเริ่มต้น) – จะไม่มีการกำจัดโดยอัตโนมัติ • standard – ecls.exe จะพยายามกำจัดหรือลบไฟล์ที่ติดไวรัสโดยอัตโนมัติ • เข้มงวด - ecls.exe จะพยายามกำจัดหรือลบไฟล์ที่ติดไวรัสโดยอัตโนมัติโดยไม่ต้องมีการดำเนินการโดยผู้ใช้ (คุณจะไม่ได้รับข้อความก่อนที่ไฟล์จะถูกลบ) • เคร่งครัด - ecls.exe จะลบไฟล์โดยไม่พยายามกำจัดไม่ว่าจะเป็นไฟล์อะไรก็ตาม • ลบ - ecls.exe จะลบไฟล์โดยไม่พยายามกำจัดแต่จะระงับการลบไฟล์ที่ละเอียดอ่อน เช่น ไฟล์ระบบ Windows
/quarantine	คัดลอกไฟล์ที่ติดไวรัส (ถ้ากำจัดแล้ว) ไปยังส่วนกักเก็บ (เสริมการทำงานที่ดำเนินการขณะกำจัด)
/no-quarantine	ไม่คัดลอกไฟล์ที่ติดไวรัสไปยังส่วนกักเก็บ

ตัวเลือกทั่วไป

/help	แสดงวิธีใช้และออก
/version	แสดงข้อมูลเวอร์ชันและออก
/preserve-time	เก็บบันทึกการลงเวลาเข้าถึงล่าสุด

รหัสการออกจากการทำงาน

0	ไม่พบภัยคุกคาม
1	พบภัยคุกคามและกำจัดแล้ว
10	ไม่สามารถสแกนบางไฟล์ได้ (อาจเป็นภัยคุกคาม)
50	พบภัยคุกคาม
100	ข้อผิดพลาด

i รหัสการออกจากการทำงานที่มากกว่า 100 หมายความว่าไม่มีการสแกนไฟล์และอาจมีการติดไวรัส

คำถามที่พบบ่อย

คุณสามารถดูคำถามที่พบบ่อยและปัญหาที่พบได้ที่ด้านล่างนี้ คลิกที่ชื่อหัวข้อเพื่อค้นหาวิธีแก้ไขปัญหา:

- วิธีอัพเดท ESET NOD32 Antivirus
- ESET NOD32 Antivirus ตรวจพบภัยคุกคาม
- วิธีลบไวรัสออกจากคอมพิวเตอร์
- วิธีสร้างงานใหม่ในเครื่องมือวางกำหนดการ
- วิธีวางกำหนดการงานสแกน (รายสัปดาห์)
- วิธีปลดล็อคการตั้งค่าขั้นสูง
- วิธีแก้ปัญหาการปิดใช้งานผลิตภัณฑ์จาก ESET HOME

หากปัญหาของคุณไม่ได้รวมอยู่ในรายการด้านบนนี้ ให้ลองค้นหาในวิธีใช้ออนไลน์ของ ESET NOD32 Antivirus

หากคุณไม่พบทางแก้ไขสำหรับปัญหา/คำถามในวิธีใช้ออนไลน์ของ ESET NOD32 Antivirus คุณสามารถไปที่ฐานความรู้ของ ESET แบบออนไลน์ที่มีการอัพเดทเป็นประจำของพวกเราได้ ลิงก์ไปยังบทความฐานความรู้ที่ได้รับความนิยมของพวกเราอยู่ที่ด้านล่างนี้:

- ฉันจะต่ออายุการสมัครสมาชิกได้อย่างไร
- ฉันได้รับข้อผิดพลาดของการเปิดใช้งานขณะติดตั้งผลิตภัณฑ์ ESET หมายความว่าอย่างไร
- เปิดใช้งานผลิตภัณฑ์ ESET Windows สำหรับใช้งานในบ้านโดยใช้รหัสเปิดใช้งาน

- ถอนการติดตั้งหรือติดตั้งผลิตภัณฑ์ ESET Windows สำหรับใช้ที่บ้านของฉันใหม่อีกครั้ง
- ฉันได้รับข้อความว่าการติดตั้ง ESET ของฉันเสร็จสิ้นอย่างไม่สมบูรณ์
- เมื่อต่ออายุการสมัครสมาชิกเสร็จแล้วฉันต้องทำอะไรต่อ (ผู้ใช้เริ่มต้น)
- จะเกิดอะไรขึ้นหากฉันเปลี่ยนที่อยู่อีเมลของฉัน
- ย้ายผลิตภัณฑ์ ESET ของฉันไปยังคอมพิวเตอร์หรืออุปกรณ์เครื่องใหม่
- จะเริ่ม Windows ในโหมดปลอดภัยหรือโหมดปลอดภัยที่มีเครือข่ายได้อย่างไร
- ยกเว้นเว็บไซต์ที่ปลอดภัยไม่ให้ถูกบล็อก
- อนุญาตการเข้าถึงสำหรับซอฟต์แวร์ตัวอ่านหน้าจอไปยัง ESET GUI

หากจำเป็น คุณสามารถติดต่อฝ่ายสนับสนุนด้านเทคนิคของเรา ได้หากคุณมีคำถามหรือปัญหา

วิธีอัพเดท ESET NOD32 Antivirus

การอัพเดท ESET NOD32 Antivirus สามารถดำเนินการได้ทั้งด้วยตนเองหรือโดยอัตโนมัติ ในการเรียกการอัพเดท ให้คลิก **อัพเดท** ในหน้าต่างโปรแกรมหลักแล้วคลิก **ตรวจหาการอัพเดท**

การตั้งค่าการติดตั้งเริ่มต้นจะสร้างงานการอัพเดทอัตโนมัติ ซึ่งสามารถทำงานเป็นประจำในแต่ละชั่วโมง ถ้าคุณต้องการเปลี่ยนระยะเวลา ให้ไปที่ **เครื่องมือ** > เครื่องมือวางกำหนดการ

วิธีลบไวรัสออกจากคอมพิวเตอร์

ถ้าคอมพิวเตอร์ของคุณแสดงอาการการติดไวรัสจากมัลแวร์ ตัวอย่างเช่น ทำงานช้า ค้างบ่อยๆ เราขอแนะนำให้คุณดำเนินการดังนี้:

1.ใน หน้าต่างโปรแกรมหลัก ให้คลิก **การสแกนคอมพิวเตอร์**

2.คลิก **การสแกนคอมพิวเตอร์ของคุณ** เพื่อเริ่มต้นการสแกนระบบของคุณ

3.หลังจากสแกนเสร็จสิ้นแล้ว ให้ตรวจดูบันทึกสำหรับจำนวนไฟล์ที่สแกน ไฟล์ที่ติดไวรัส และไฟล์ที่กำจัด

4.หากคุณต้องการสแกนเฉพาะส่วนที่เลือกในดิสก์ของคุณ ให้คลิก **การสแกนแบบกำหนดเอง** และเลือกเป้าหมายที่จะสแกนหาไวรัส

หากต้องการข้อมูลเพิ่มเติม โปรดดู:

- บทความฐานความรู้ ESET
- กักเก็บ

วิธีสร้างงานใหม่ในเครื่องมือวางกำหนดการ

เมื่อต้องการสร้างงานใหม่ใน **เครื่องมือ** > **เครื่องมือวางกำหนดการ** ให้คลิก **เพิ่มงาน** หรือคลิกขวาและเลือก **เพิ่ม** ที่เมนูบริบท มีงานตามกำหนดการห้าประเภท:

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

เนื่องจาก **อัพเดท** เป็นงานตามกำหนดการที่ใช้บ่อยที่สุดงานหนึ่ง ดังนั้นเราจะอธิบายวิธีเพิ่มงานการอัพเดทใหม่ดังด้านล่างนี้:

จากเมนูแบบหล่นลง **งานที่มีกำหนดการ** เลือก **อัพเดท** ป้อนชื่อของงานลงในช่อง **ชื่องาน** แล้วคลิก **ถัดไป** เลือกความถี่ของงาน ตัวเลือกที่ใช้ได้มีดังนี้: **หนึ่งครั้ง ซ้ำ รายวัน รายสัปดาห์** และ **ตามเหตุการณ์** เลือก **ข้ามงานเมื่อทำงานด้วยแบตเตอรี่** เพื่อลดการใช้ทรัพยากรของระบบในขณะที่แล็ปท็อปทำงานด้วยพลังงานแบตเตอรี่ งานจะ

ถูกเรียกใช้ตามวันที่และเวลาที่ระบุในช่อง **การเรียกใช้งาน** ขั้นตอนถัดไป ให้กำหนดการทำงานที่ต้องการหากไม่สามารถดำเนินการกับงานหรือทำงานให้สำเร็จตามเวลาในกำหนดกา ตัวเลือกที่ใช้ได้มีดังนี้:

- **เมื่อเวลาที่กำหนดไว้ครั้งต่อไป**
- **เร็วที่สุดเท่าที่ทำได้**
- **ทันที หากเวลานับตั้งแต่การเรียกใช้งานครั้งสุดท้ายเกินค่าที่ระบุไว้** (สามารถกำหนดช่วงเวลาได้โดยใช้กล่องเลื่อน **เวลานับตั้งแต่การเรียกใช้งานครั้งสุดท้าย (ชั่วโมง)**)

ในขั้นถัดไป โปรแกรมจะแสดงข้อมูลสรุปพร้อมด้วยข้อมูลเกี่ยวกับงานตามกำหนดการปัจจุบัน คลิก **สิ้นสุด** เมื่อคุณแก้ไขจนเสร็จสิ้นแล้ว

หน้าต่างข้อความจะปรากฏ เพื่อให้คุณเลือกโปรไฟล์ที่จะใช้สำหรับงานตามกำหนดการ ในที่นี้คุณจะสามารถตั้งค่าโปรไฟล์หลักและโปรไฟล์รอง โปรไฟล์รองจะใช้ในกรณีที่ไม่สามารถทำงานให้เสร็จสมบูรณ์โดยใช้โปรไฟล์หลัก ยืนยันด้วยการคลิก **สิ้นสุด** และงานตามกำหนดการใหม่จะถูกเพิ่มในรายการของงานตามกำหนดการปัจจุบัน

วิธีกำหนดตารางการสแกนคอมพิวเตอร์รายสัปดาห์

หากต้องการวางกำหนดการงานทั่วไป ให้เปิดหน้าต่างโปรแกรมหลักและคลิก **เครื่องมือ** > **เครื่องมือวางกำหนดการณ์** ที่ด้านล่างคือคู่มือสั้นๆ เกี่ยวกับวิธีการวางกำหนดงานที่จะสแกนไดรฟ์ในระบบของคุณในทุกสัปดาห์ ให้ดู บทความฐานความรู้ สำหรับคำแนะนำอย่างละเอียดเพิ่มเติม

เมื่อต้องการวางกำหนดการงานสแกน:

1. คลิก **เพิ่ม** ในหน้าจอเครื่องมือวางกำหนดการหลัก
2. ป้อนชื่อสำหรับงานแล้วเลือก **สแกนคอมพิวเตอร์ตามความต้องการ** จากเมนูแบบเลื่อนลง **ประเภทงาน**
3. เลือก **รายสัปดาห์** เป็นความถี่ของงาน
4. ตั้งวันและเวลาที่จะทำงาน
5. เลือก **เรียกใช้งานให้เร็วที่สุดเท่าที่ทำได้** เพื่อทำงานในภายหลังในกรณีที่การเรียกใช้งานตามกำหนดการไม่ทำงานด้วยสาเหตุใดก็ตาม (ตัวอย่างเช่น หากคอมพิวเตอร์ถูกปิดในเวลานั้น)
6. ดูข้อมูลสรุปของงานตามกำหนดการ และคลิกที่ **สิ้นสุด**

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

8. คลิก **สิ้นสุด** เพื่อใช้งาน

วิธีปลดล็อคการตั้งค่าขั้นสูงที่มีการป้องกันด้วยรหัสผ่าน

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

เรียกคืนรหัสผ่านผ่านบัญชี ESET HOME – ใช้ตัวเลือกนี้หากการสมัครสมาชิกที่ใช้สำหรับการเปิดใช้งานเชื่อมโยงอยู่กับบัญชี ESET HOME ของคุณ โปรดพิมพ์อีเมลที่คุณใช้ล็อคอินบัญชี ESET HOME ของคุณ

หากคุณจำที่อยู่อีเมลไม่ได้หรือพบความยากลำบากในการเรียกคืนรหัสผ่าน ให้คลิก **ติดต่อฝ่ายสนับสนุนด้านเทคนิค** ระบบจะเปลี่ยนเส้นทางคุณไปยังเว็บไซต์ ESET เพื่อติดต่อฝ่ายสนับสนุนด้านเทคนิค

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

สำหรับข้อมูลเพิ่มเติม โปรดดู ปลดล็อกการตั้งค่ารหัสผ่านผลิตภัณฑ์ ESET สำหรับ Windows สำหรับใช้งานในบ้าน

วิธีแก้ปัญหาการปิดใช้งานผลิตภัณฑ์จาก ESET HOME

ยังไม่ได้เปิดใช้งานผลิตภัณฑ์

ข้อความแสดงข้อผิดพลาดนี้จะปรากฏขึ้นเมื่อเจ้าของการสมัครสมาชิกปิดการใช้งาน ESET NOD32 Antivirus ของคุณจากพอร์ทัล ESET HOME หรือเมื่อไม่มีการแชร์การสมัครสมาชิกที่ใช้ร่วมกับบัญชี ESET HOME ของคุณอีกต่อไป หากต้องการแก้ไขปัญหานี้ ให้:

- คลิก **เปิดใช้งาน** และใช้หนึ่งใน วิธีการเปิดใช้งาน เพื่อเปิดใช้งาน ESET NOD32 Antivirus

• ติดต่อเจ้าของการสมัครสมาชิกเพื่อแจ้งข้อมูลว่า ESET NOD32 Antivirus ของคุณถูกปิดใช้งานโดยเจ้าของการสมัครสมาชิก หรือแจ้งว่าไม่มีการแชร์การสมัครสมาชิกกับคุณอีกต่อไป เจ้าของสามารถแก้ปัญหาใน ESET HOME ได้

ปิดใช้งานผลิตภัณฑ์แล้ว ยกเลิกการเชื่อมต่ออุปกรณ์แล้ว

ข้อความแสดงข้อผิดพลาดนี้จะปรากฏขึ้นหลังจาก นำอุปกรณ์ออกจากบัญชี ESET HOME หากต้องการแก้ไขปัญหานี้ให้:

• คลิก **เปิดใช้งาน** และใช้หนึ่งใน วิธีการเปิดใช้งาน เพื่อเปิดใช้งาน ESET NOD32 Antivirus

• ติดต่อเจ้าของการสมัครสมาชิกเพื่อแจ้งข้อมูลว่า ESET NOD32 Antivirus ของคุณถูกปิดใช้งาน และอุปกรณ์ถูกตัดการเชื่อมต่อจาก ESET HOME

• หากคุณเป็นเจ้าของการสมัครสมาชิกและไม่ทราบถึงการเปลี่ยนแปลงเหล่านี้ ให้ตรวจสอบ ฟีดการทำงานของ ESET HOME หากคุณพบกิจกรรมที่น่าสงสัย ให้ เปลี่ยนรหัสผ่านบัญชี ESET HOME ของคุณ และ ติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET

ปิดใช้งานผลิตภัณฑ์แล้วยกเลิกการเชื่อมต่ออุปกรณ์แล้ว

ข้อความแสดงข้อผิดพลาดนี้จะปรากฏขึ้นหลังจาก นำอุปกรณ์ออกจากบัญชี ESET HOME หากต้องการแก้ไขปัญหานี้ให้:

• คลิก **เปิดใช้งาน** และใช้หนึ่งใน วิธีการเปิดใช้งาน เพื่อเปิดใช้งาน ESET NOD32 Antivirus

• ติดต่อเจ้าของการสมัครสมาชิกเพื่อแจ้งข้อมูลว่า ESET NOD32 Antivirus ของคุณถูกปิดใช้งาน และอุปกรณ์ถูกตัดการเชื่อมต่อจาก ESET HOME

• หากคุณเป็นเจ้าของการสมัครสมาชิกและไม่ทราบถึงการเปลี่ยนแปลงเหล่านี้ ให้ตรวจสอบ ฟีดการทำงานของ ESET HOME หากคุณพบกิจกรรมที่น่าสงสัย ให้ เปลี่ยนรหัสผ่านบัญชี ESET HOME ของคุณ และ ติดต่อฝ่ายสนับสนุนด้านเทคนิคของ ESET

ยังไม่ได้เปิดใช้งานผลิตภัณฑ์

ข้อความแสดงข้อผิดพลาดนี้จะปรากฏขึ้นเมื่อเจ้าของการสมัครสมาชิกปิดการใช้งาน ESET NOD32 Antivirus ของคุณจากพอร์ทัล ESET HOME หรือเมื่อไม่มีการแชร์การสมัครสมาชิกที่ใช้ร่วมกับบัญชี ESET HOME ของคุณอีกต่อไป หากต้องการแก้ไขปัญหานี้ ให้:

- คลิก **เปิดใช้งาน** และใช้หนึ่งใน วิธีการเปิดใช้งาน เพื่อเปิดใช้งาน ESET NOD32 Antivirus
- ติดต่อเจ้าของการสมัครสมาชิกเพื่อแจ้งข้อมูลว่า ESET NOD32 Antivirus ของคุณถูกปิดใช้งานโดยเจ้าของการสมัครสมาชิก หรือแจ้งว่าไม่มีการแชร์การสมัครสมาชิกกับคุณอีกต่อไป เจ้าของสามารถแก้ปัญหาใน ESET HOME ได้

0

โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า

เมื่อเข้าร่วมโปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า คุณจะมอบข้อมูลแบบไม่ระบุตัวตนเกี่ยวกับวิธีใช้ผลิตภัณฑ์ของเราให้แก่ ESET สามารถดูข้อมูลเพิ่มเติมเกี่ยวกับการประมวลผลข้อมูลได้ใน นโยบายความเป็นส่วนตัว

คำยินยอมของคุณ

โปรแกรมนี้เปิดให้เข้าร่วมโดยสมัครใจและขึ้นอยู่กับความยินยอมของคุณ หลังจากที่เข้าร่วมแล้ว การมีส่วนร่วมทั้งหมดจะเป็นแบบไม่ต้องโต้ตอบ ซึ่งหมายความว่าคุณไม่จำเป็นต้องดำเนินการเพิ่มเติมใดๆ คุณสามารถถอนความยินยอมของคุณได้ทุกเมื่อด้วยการเปลี่ยนการตั้งค่าผลิตภัณฑ์ ซึ่งจะเป็นการยุติไม่ให้เราประมวลผลข้อมูลแบบไม่ระบุตัวตนของคุณอีกต่อไป

คุณสามารถถอนความยินยอมของคุณได้ทุกเมื่อด้วยการเปลี่ยนการตั้งค่าผลิตภัณฑ์

- เปลี่ยนแปลงการตั้งค่าโปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้าในผลิตภัณฑ์ ESET Windows สำหรับใช้ในบ้าน

เรารวบรวมข้อมูลประเภทใดบ้าง

ข้อมูลเกี่ยวกับการโต้ตอบกับผลิตภัณฑ์

ข้อมูลนี้จะช่วยให้เราทราบเพิ่มเติมว่าผลิตภัณฑ์ของเราถูกใช้งานอย่างไร ข้อมูลนี้ทำให้เราทราบสิ่งต่างๆ เช่น มักใช้การทำงานแบบใด ผู้ใช้แก้ไขการตั้งค่าใดบ้าง หรือผู้ใช้ใช้งานผลิตภัณฑ์เป็นเวลาเท่าใด

ข้อมูลเกี่ยวกับอุปกรณ์

เราเก็บรวบรวมข้อมูลนี้เพื่อทำความเข้าใจว่าอุปกรณ์ใดและที่ใดบ้างที่ผลิตภัณฑ์ของเราได้รับการใช้งาน ตัวอย่างทั่วไปคือ รุ่นของอุปกรณ์ ประเทศ เวอร์ชัน และชื่อของระบบปฏิบัติการ

การวินิจฉัยข้อมูลข้อผิดพลาด

เราเก็บรวบรวมข้อมูลเกี่ยวกับข้อผิดพลาดและสถานการณ์ความล้มเหลวต่างๆ เช่น เกิดข้อผิดพลาดใดบ้างและการกระทำใดที่ส่งผลให้เกิดข้อผิดพลาดนั้น

เหตุใดเราจึงรวบรวมข้อมูลนี้

ข้อมูลแบบไม่ระบุตัวตนนี้ช่วยให้เราสามารถปรับปรุงผลิตภัณฑ์ให้คุณซึ่งเป็นผู้ใช้ของเรา ทำให้มีความเกี่ยวข้อง ใช้งานง่าย และไร้ข้อผิดพลาดมากขึ้นเท่าที่จะทำได้

ใครควบคุมข้อมูลนี้

ESET, spol. s r.o. คือผู้ควบคุมการเก็บรวบรวมข้อมูลในโปรแกรมนี้แต่เพียงผู้เดียว ซึ่งข้อมูลนี้จะไม่เปิดเผยให้บุคคลที่สาม

ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง

มีผลตั้งแต่วันที่ 19 ตุลาคม 2021

ข้อมูลสำคัญ: โปรดอ่านข้อกำหนดและเงื่อนไขของการใช้งานผลิตภัณฑ์ที่กำหนดไว้ด้านล่างนี้อย่างถี่ถ้วนก่อนที่จะดาวน์โหลด ติดตั้ง คัดลอก หรือใช้งาน **เมื่อคุณดาวน์โหลด ติดตั้ง คัดลอก หรือใช้ซอฟต์แวร์นี้ จะถือว่าคุณแสดงความยินยอมตามข้อกำหนดและเงื่อนไขเหล่านี้และคุณยอมรับ** [นโยบายความเป็นส่วนตัว]

ข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง

ภายใต้ข้อตกลงการอนุญาตใช้งานสำหรับผู้ใช้ปลายทาง ("ข้อตกลง") นี้ ดำเนินการโดยและระหว่าง ESET, spol. s r. o. ซึ่งมีสำนักงานที่จดทะเบียนอยู่ที่ Einsteinova 24, 85101 Bratislava, Slovak Republic และจดทะเบียนในทะเบียนการค้าที่ได้รับการควบคุมดูแลโดย Bratislava I District Court, Section Sro, เลขที่ 3586/B หมายเลขทะเบียนธุรกิจ: 31333532 ("ESET" หรือ “ผู้ให้บริการ”) กับคุณ ซึ่งเป็นบุคคลธรรมดาหรือนิติบุคคล (“คุณ" หรือ "ผู้ใช้ปลายทาง”) คุณได้รับสิทธิ์ให้สามารถใช้ซอฟต์แวร์ที่กำหนดในข้อ 1 ของข้อตกลงนี้ ซอฟต์แวร์ที่กำหนดในข้อ 1 ของข้อตกลงนี้อาจจัดเก็บอยู่ในสื่อจัดเก็บข้อมูล ส่งทางอีเมล ดาวน์โหลดจากอินเทอร์เน็ต ดาวน์โหลดจากเซิร์ฟเวอร์ของผู้ให้บริการ หรือได้รับจากแหล่งอื่นๆ ตามข้อกำหนดและเงื่อนไขที่ระบุไว้ด้านล่างนี้

ข้อตกลงนี้เป็นข้อตกลงเกี่ยวกับสิทธิของผู้ใช้ปลายทางและไม่ใช่ข้อตกลงสำหรับการจำหน่าย ผู้ให้บริการยังคงเป็นเจ้าของสำเนาของซอฟต์แวร์ และสื่อทางกายภาพที่บรรจุในบรรจุภัณฑ์เชิงพาณิชย์ รวมถึงสำเนาอื่นๆ ของซอฟต์แวร์ที่ผู้ใช้ปลายทางได้รับอนุญาตตามข้อตกลงนี้

เมื่อคลิกที่ตัวเลือก "ฉันยอมรับ" หรือ "ฉันยอมรับ..." ในระหว่างการติดตั้ง ดาวน์โหลด คัดลอก หรือใช้ซอฟต์แวร์ จะถือว่าคุณยอมรับข้อกำหนดและเงื่อนไขของข้อตกลงนี้และรับทราบถึงนโยบายความเป็นส่วนตัว ถ้าคุณไม่ยอมรับข้อกำหนดและเงื่อนไขทั้งหมดของข้อตกลงนี้และ/หรือนโยบายความเป็นส่วนตัว โปรดคลิกที่ตัวเลือกการยกเลิกทันที ยกเลิกการติดตั้งหรือการดาวน์โหลด หรือทำลายหรือส่งคืนซอฟต์แวร์ สื่อการติดตั้ง รวมทั้งเอกสารประกอบ และใบเสร็จจากการจำหน่ายให้แก่ผู้ให้บริการหรือสถานที่ซึ่งคุณได้รับซอฟต์แวร์

คุณยอมรับว่าการใช้ซอฟต์แวร์ของคุณแสดงว่าคุณได้อ่านข้อตกลงนี้ ทำความเข้าใจและยอมรับที่จะมีข้อผูกพันตามข้อกำหนดและเงื่อนไขของข้อตกลงนี้

1. **ซอฟต์แวร์** ในข้อตกลงนี้ "ซอฟต์แวร์" หมายถึง (i) โปรแกรมคอมพิวเตอร์ที่มากับข้อตกลงนี้และองค์ประกอบทั้งหมดของโปรแกรม; (ii) เนื้อหาทั้งหมดของดิสก์ CD-ROM, DVD อีเมลและไฟล์แนบใดๆ หรือสื่ออื่นๆ ที่ข้อตกลงนี้มีให้ รวมถึงรหัสวัตถุของซอฟต์แวร์ที่มาพร้อมกับสื่อจัดเก็บข้อมูล ผ่านอีเมลหรือดาวน์โหลดผ่านอินเทอร์เน็ต; (iii) สื่อสิ่งพิมพ์ประกอบการอธิบายใดๆ และเอกสารอื่นๆ ใดๆ ที่เกี่ยวข้องกับซอฟต์แวร์ นอกเหนือจากคำอธิบายใดๆ ของซอฟต์แวร์ ข้อมูลทางเทคนิค คำอธิบายคุณสมบัติหรือการใช้งานซอฟต์แวร์ใดๆ คำอธิบายถึงสภาพแวดล้อมในการใช้งานซอฟต์แวร์ คำแนะนำสำหรับการใช้งานหรือการติดตั้งซอฟต์แวร์หรือคำอธิบายใดๆ ถึงวิธีการใช้งานซอฟต์แวร์ ("เอกสารประกอบ"); (iv) สำเนาของซอฟต์แวร์ การแก้ไขข้อผิดพลาดที่เป็นไปได้ในซอฟต์แวร์ ส่วนเพิ่มเติมซอฟต์แวร์ ส่วนขยาย เวอร์ชันดัดแปลงของซอฟต์แวร์ และการอัพเดทส่วนประกอบซอฟต์แวร์ ถ้ามี ตามที่ผู้ให้บริการให้อนุญาตแก่คุณตามข้อ 3 ของข้อตกลงนี้ ซอฟต์แวร์จะมีให้ในรูปแบบของรหัสวัตถุที่เรียกใช้งานได้เท่านั้น

2. **การติดตั้ง คอมพิวเตอร์ และรหัสใบอนุญาต ซอฟต์แวร์ที่อยู่ในสื่อจัดเก็บข้อมูล** ส่งทางอีเมล ดาวน์โหลด

จากอินเทอร์เน็ต ดาวน์โหลดจากเซิร์ฟเวอร์ของผู้ให้บริการ หรือได้รับจากแหล่งอื่นๆ จะต้องมีการติดตั้ง คุณจะต้องติดตั้งซอฟต์แวร์ในคอมพิวเตอร์ที่ได้รับการกำหนดค่าอย่างถูกต้อง ตามข้อกำหนดขั้นต่ำที่ระบุไว้ในเอกสารประกอบ วิธีการติดตั้งจะมีระบุไว้ในเอกสารประกอบ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์หรือฮาร์ดแวร์ที่อาจมีผลเสียต่อซอฟต์แวร์ไว้ในคอมพิวเตอร์ที่คุณติดตั้งซอฟต์แวร์ คอมพิวเตอร์หมายถึงฮาร์ดแวร์ ซึ่งรวมถึงแต่ไม่จำกัดเพียง คอมพิวเตอร์ส่วนบุคคล แล็ปท็อป เวิร์กสเตชัน ปาล์มท็อปคอมพิวเตอร์ สมาร์ทโฟน อุปกรณ์อิเล็กทรอนิกส์แบบถือ หรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆ ที่ซอฟต์แวร์ถูกออกแบบมาให้ใช้งานด้วย หรือที่ซอฟต์แวร์ถูกติดตั้งและ/หรือใช้งาน รหัสใบอนุญาตหมายถึงชุดของสัญลักษณ์ อักขระ หมายเลข หรือสัญลักษณ์พิเศษที่ไม่ซ้ำกันซึ่งจัดหาให้แก่ผู้ใช้ปลายทางเพื่ออนุญาตให้ใช้งานซอฟต์แวร์ เวอร์ชั่นเฉพาะ หรือส่วนขยายของข้อกำหนดของใบอนุญาตได้อย่างถูกกฎหมาย สอดคล้องกับข้อตกลงนี้

3. **ใบอนุญาต** ตามเงื่อนไขที่คุณยอมรับตามข้อกำหนดของข้อตกลงนี้ คุณจะต้องชำระค่าใบอนุญาตภายในระยะเวลาที่ครบกำหนด และคุณจะต้องปฏิบัติตามข้อกำหนดและเงื่อนไขทั้งหมดที่ระบุไว้ในที่นี้ ผู้ให้บริการจะให้สิทธิ์ ("ใบอนุญาต") ต่อไปนี้แก่คุณ:

ก) **การติดตั้งและการใช้งาน** คุณจะมีสิทธิที่ไม่จำกัดเฉพาะตัวและไม่สามารถโอนสิทธิได้ในการติดตั้งซอฟต์แวร์ในฮาร์ดดิสก์ของคอมพิวเตอร์ หรือสื่อถาวรอื่นๆ สำหรับการจัดเก็บข้อมูล การติดตั้ง และการจัดเก็บซอฟต์แวร์ในหน่วยความจำของระบบคอมพิวเตอร์ และในการปรับใช้งาน จัดเก็บ และแสดงซอฟต์แวร์

ข) **ข้อกำหนดของจำนวนใบอนุญาต** สิทธิในการใช้ซอฟต์แวร์จะมีข้อผูกพันตามจำนวนของผู้ใช้ปลายทาง ผู้ใช้ปลายทางหนึ่งราย จะมีความหมายดังนี้: (i) การติดตั้งซอฟต์แวร์ในระบบคอมพิวเตอร์หนึ่งระบบ หรือ (ii) ถ้าขอบเขตของใบอนุญาตเชื่อมโยงกับจำนวนกล่องจดหมาย คำว่า ผู้ใช้ปลายทางหนึ่งราย จะมีความหมายว่าผู้ใช้คอมพิวเตอร์หนึ่งรายที่ยอมรับอีเมลผ่านทางโปรแกรมตัวแทนผู้ใช้อีเมล (“MUA”) ถ้า MUA ยอมรับอีเมลและส่งต่อไปยังผู้ใช้หลายรายโดยอัตโนมัติ จำนวนของผู้ใช้ปลายทางจะพิจารณาตามจำนวนผู้ใช้ตามจริงที่มีการส่งอีเมลถึง ถ้าอีเมลเซิร์ฟเวอร์ดำเนินการเป็นเกตเวย์ของอีเมล จำนวนผู้ใช้ปลายทางจะต้องเท่ากับจำนวนผู้ใช้อีเมลเซิร์ฟเวอร์ที่เกตเวย์นั้นให้บริการอยู่ ถ้ามีการส่งอีเมลสำหรับที่อยู่อีเมลที่ไม่ได้ระบุจำนวนไปยังและยอมรับโดยผู้ใช้รายเดียว (เช่น ผ่านชื่อแทน) และข้อความนั้นไม่มีการส่งต่อโดยอัตโนมัติโดยไคลเอ็นต์ไปยังผู้ใช้จำนวนมาก จะต้องใช้ใบอนุญาตสำหรับคอมพิวเตอร์เครื่องเดียว คุณจะต้องไม่ใช้ใบอนุญาตเดียวกันในเวลาเดียวกันในคอมพิวเตอร์มากกว่าหนึ่งเครื่อง ผู้ใช้ปลายทางได้รับสิทธิ์ให้ป้อนรหัสใบอนุญาตไปยังซอฟต์แวร์ได้เฉพาะในขอบเขตเท่าที่ผู้ใช้ปลายทางมีสิทธิ์ใช้งานซอฟต์แวร์ ซึ่งสอดคล้องกับข้อจำกัดที่มีผลบังคับใช้จากจำนวนใบอนุญาตที่ได้รับจากผู้ให้บริการ รหัสใบอนุญาตจะถือว่าเป็นความลับ คุณต้องไม่แบ่งปันใบอนุญาตกับบุคคลที่สามหรืออนุญาติให้บุคคลที่สามใช้รหัสใบอนุญาตเว้นแต่จะได้รับอนุญาตจากข้อตกลงนี้หรือจากผู้ให้บริการ หากรหัสใบอนุญาตของคุณถูกบุกรุก โปรดแจ้งผู้ให้บริการทันที

ค) **เวอร์ชั่นใช้กับบ้าน/ธุรกิจ** ซอฟต์แวร์เวอร์ชั่นใช้กับบ้านจะใช้เฉพาะในสภาพแวดล้อมการแบบส่วนบุคคลและ

/หรือแบบไม่ใช่เชิงพาณิชย์ในบ้านและในครอบครัวเท่านั้น การรับซอฟต์แวร์เวอร์ชั่นใช้กับธุรกิจต้องเป็นไปเพื่อนำไปใช้ในสภาพแวดล้อมเชิงพาณิชย์ และเพื่อใช้ซอฟต์แวร์ในอีเมลเซิร์ฟเวอร์ เมลรีเลย์ เมลเกตเวย์ หรืออินเทอร์เน็ตเกตเวย์

ง) **ระยะเวลาของใบอนุญาต** สิทธิในการใช้ซอฟต์แวร์จะมีระยะเวลาจำกัด

จ) **ซอฟต์แวร์ของ OEM** ซอฟต์แวร์ที่จัดประเภทว่าเป็น "OEM" จะจำกัดเฉพาะคอมพิวเตอร์ที่คุณได้รับซอฟต์แวร์มาด้วย ไม่สามารถโอนซอฟต์แวร์ไปยังคอมพิวเตอร์เครื่องอื่นได้

ฉ) **NFR, ซอฟต์แวร์ทดลองใช้** ซอฟต์แวร์ที่ถูกจัดเป็น "ไม่ใช่สำหรับจำหน่าย" ซึ่งเรียกว่า NFR หรือทดลองใช้ ไม่สามารถกำหนดไว้สำหรับการชำระเงิน และต้องใช้สำหรับการสาธิตหรือการทดสอบคุณลักษณะของซอฟต์แวร์เท่านั้น

ช) **การยุติใบอนุญาต** ใบอนุญาตจะยุติโดยอัตโนมัติเมื่อสิ้นสุดระยะเวลาที่ได้รับสิทธิ ถ้าคุณไม่ปฏิบัติตามบทบัญญัติของข้อตกลงนี้ ผู้ให้บริการจะได้รับสิทธิให้เพิกถอนจากข้อตกลงนี้ โดยไม่มีผลกระทบต่อสิทธิหรือการเยียวยาทางกฎหมายที่เปิดไว้ให้กับผู้ให้บริการสำหรับกรณีดังกล่าว ในกรณีของการยกเลิกใบอนุญาต คุณจะต้องลบ ทำลาย หรือส่งคืนซอฟต์แวร์และสำเนาการสำรองข้อมูลทั้งหมดแก่ ESET หรือสถานที่ซึ่งคุณได้รับซอฟต์แวร์ โดยเป็นผู้ออกค่าใช้จ่ายเอง เมื่อสิ้นสุดระยะเวลาที่ได้รับสิทธิใช้ใบอนุญาต ผู้ให้บริการมีสิทธิในการยกเลิกการให้สิทธิของผู้ใช้ปลายทางสำหรับการใช้ฟังก์ชันของซอฟต์แวร์ที่ต้องเชื่อมต่อกับเซิร์ฟเวอร์ของผู้ให้บริการหรือเซิร์ฟเวอร์ของบุคคลที่สาม

4. **ฟังก์ชันที่ต้องใช้การรวบรวมข้อมูลและการเชื่อมต่ออินเทอร์เน็ต** เพื่อให้การทำงานถูกต้อง ซอฟต์แวร์ต้องมีการเชื่อมต่ออินเทอร์เน็ต และต้องเชื่อมต่อกับเซิร์ฟเวอร์ของผู้ให้บริการหรือเซิร์ฟเวอร์ของบุคคลที่สามและการรวบรวมข้อมูลที่เกี่ยวข้องเป็นประจำตามนโยบายความเป็นส่วนตัว การเชื่อมต่อกับอินเทอร์เน็ตและการรวบรวมข้อมูลที่เกี่ยวข้องมีความสำคัญสำหรับคุณลักษณะของซอฟต์แวร์ดังต่อไปนี้:

ก) **การอัพเดทซอฟต์แวร์** ผู้ให้บริการจะได้รับสิทธิ์ตั้งแต่เวลาออกการอัพเดทหรืออัพเกรดซอฟต์แวร์ ("การอัพเดท") แต่จะไม่มีภาระหน้าที่ในการให้การอัพเดท ฟังก์ชันนี้จะถูกเปิดใช้งานภายใต้การตั้งค่ามาตรฐานของซอฟต์แวร์และจะได้รับการติดตั้งการอัพเดทโดยอัตโนมัติ ยกเว้นผู้ใช้ปลายทางจะปิดใช้งานการติดตั้งการอัพเดทโดยอัตโนมัติ สำหรับการจัดหาการอัพเดท จะต้องใช้การตรวจสอบความถูกต้องของใบอนุญาต ซึ่งรวมถึงข้อมูลเกี่ยวกับคอมพิวเตอร์และ/หรือแพลตฟอร์มที่ติดตั้งซอฟต์แวร์นั้นตามนโยบายความเป็นส่วนตัว

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

ข) **การส่งต่อการแฝงตัวและข้อมูลแก่ผู้ให้บริการ** ซอฟต์แวร์นี้มีฟังก์ชันที่ทำหน้าที่เก็บตัวอย่างของไวรัส

คอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ที่เป็นอันตรายอื่นๆ และสิ่งที่น่าสงสัยซึ่งเป็นปัญหา ที่อาจไม่พึงประสงค์หรืออาจไม่ปลอดภัย เช่น ไฟล์ URL แพ็คเก็ต IP และค่าเฟรมอีเธอร์เน็ต (“การแฝงตัว”) และจะส่งตัวอย่างเหล่านี้ให้กับผู้ให้บริการ รวมถึงแต่ไม่จำกัดเฉพาะข้อมูลเกี่ยวกับกระบวนการติดตั้ง คอมพิวเตอร์และ/หรือแพลตฟอร์มที่ติดตั้งซอฟต์แวร์นั้น และข้อมูลเกี่ยวกับระบบปฏิบัติการและการทำงานของซอฟต์แวร์ ("ข้อมูล") ข้อมูลและการแฝงตัวอาจประกอบด้วยข้อมูล (รวมถึงข้อมูลส่วนบุคคลที่ได้รับโดยการสุ่มหรือโดยบังเอิญ) เกี่ยวกับผู้ใช้ปลายทางหรือผู้ใช้อื่นๆ ที่ใช้คอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ และไฟล์ที่ได้รับผลกระทบจากการแฝงตัวรวมถึงเมตาดาต้าที่เกี่ยวข้อง

ข้อมูลและการแฝงตัวอาจรวบรวมได้โดยฟังก์ชันซอฟต์แวร์ต่อไปนี้:

i. ฟังก์ชันระบบความเชื่อถือ LiveGrid ประกอบด้วยการรวบรวมและการส่งแฮชที่เกี่ยวข้องกับการแฝงตัวแบบทางเดียวให้กับผู้ให้บริการ โดยฟังก์ชันนี้จะถูกเปิดใช้งานภายใต้การตั้งค่ามาตรฐานของซอฟต์แวร์

ii. ฟังก์ชันระบบตรวจสอบป้อนกลับของ LiveGrid ประกอบด้วยการรวบรวมและการส่งข้อมูลการบุกรุกพร้อมด้วยเมตาดาต้าและข้อมูลที่เกี่ยวข้องให้กับผู้ให้บริการ โดยฟังก์ชันนี้จะถูกเปิดใช้งานโดยผู้ใช้ปลายทางระหว่างกระบวนการติดตั้งซอฟต์แวร์

ผู้ให้บริการจะใช้ข้อมูลและการบุกรุกที่ได้รับเพื่อการวิเคราะห์และการวิจัยเกี่ยวกับการบุกรุก การปรับปรุงซอฟต์แวร์และการตรวจสอบความถูกต้องของใบอนุญาต และจะใช้มาตรการที่เหมาะสมเพื่อดำเนินการให้มั่นใจว่าการบุกรุกและข้อมูลที่ได้รับจะคงปลอดภัย เมื่อเปิดใช้งานฟังก์ชันนี้ของซอฟต์แวร์ ผู้ให้บริการจะเก็บรวบรวมและดำเนินการกับการบุกรุกและข้อมูลตามที่ระบุไว้ในนโยบายความเป็นส่วนตัวและตามระเบียบข้อบังคับตามกฎหมายที่เกี่ยวข้อง คุณสามารถปิดการทำงานของฟังก์ชันนี้ได้ทุกเมื่อ

สำหรับวัตถุประสงค์ของข้อตกลงนี้ จะจำเป็นต้องเก็บรวบรวม ประมวลผล และจัดเก็บข้อมูล เพื่อให้ผู้ให้บริการสามารถระบุตัวคุณได้ตามที่ระบุไว้ในนโยบายความเป็นส่วนตัว คุณรับทราบว่าผู้ให้บริการสามารถตรวจสอบว่าคุณใช้ซอฟต์แวร์ตามบทบัญญัติของข้อตกลงนี้หรือไม่ โดยใช้วิธีการของผู้ให้บริการเอง ในที่นี้จะถือว่าคุณรับทราบว่าตามวัตถุประสงค์ของข้อตกลงนี้แล้ว จำเป็นที่จะต้องถ่ายโอนข้อมูลของคุณขณะที่มีการสื่อสารระหว่างซอฟต์แวร์และระบบคอมพิวเตอร์ของผู้ให้บริการ หรือกับหุ้นส่วนธุรกิจที่เป็นส่วนหนึ่งของภาคการจัดจำหน่ายของผู้ให้บริการตลอดจนเครือข่ายที่รองรับ ทั้งนี้เพื่อตรวจสอบถึงฟังก์ชันการใช้งานและการได้รับอนุญาตให้ใช้ซอฟต์แวร์และเพื่อคุ้มครองสิทธิ์ของผู้ให้บริการ

ตามข้อสรุปของข้อตกลงนี้ ผู้ให้บริการหรือหุ้นส่วนธุรกิจที่เป็นส่วนหนึ่งของภาคการจัดจำหน่ายของผู้ให้บริการและเครือข่ายที่รองรับจะได้รับสิทธิ์ให้โอน ประมวลผล และจัดเก็บข้อมูลสำคัญที่จะระบุตัวคุณ เพื่อการเรียกเก็บเงินและการปฏิบัติตามข้อตกลงนี้ รวมถึงการส่งการแจ้งเตือนในคอมพิวเตอร์ของคุณ

สามารถดูรายละเอียดเกี่ยวกับการป้องกันความเป็นส่วนตัว ข้อมูลส่วนบุคคล และสิทธิ์ของคุณในแง่ของ

ข้อมูลได้ในนโยบายความเป็นส่วนตัวซึ่งอยู่ในเว็บไซต์ของผู้ให้บริการและสามารถเข้าถึงได้โดยตรงจากกระบวนการติดตั้ง 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 หรือแจกจ่ายรหัสใบอนุญาตที่

ทำซ้ำหรือสร้างขึ้น 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 สำเนาการสำรอง ข้อมูลทั้งหมด ตลอดจนเอกสารที่เกี่ยวข้องทั้งหมดที่คุณได้รับจากผู้ให้บริการหรือจากหุ้นส่วนธุรกิจของผู้ให้บริการ โดยเป็นผู้ออกค่าใช้จ่ายเอง สิทธิ์ในการใช้ซอฟต์แวร์และคุณลักษณะใดๆ ของซอฟต์แวร์อาจอยู่ภายใต้นโยบาย EOL สิทธิ์ในการใช้ซอฟต์แวร์ของคุณจะสิ้นสุดลงหลังจากซอฟต์แวร์หรือคุณลักษณะใดๆ ของซอฟต์แวร์ถึงวันสิ้นสุดอายุการใช้งานที่กำหนดไว้ในนโยบาย EOL ไม่ว่าการยุติข้อตกลงนี้จะเกิดขึ้นด้วยสาเหตุใด บทบัญญัติของข้อ 7, 8, 11, 13, 19 และ 21 จะยังคงมีผลบังคับโดยไม่จำกัดเวลา

11. **ประกาศของผู้ใช้ปลายทาง** ในฐานะที่เป็นผู้ใช้ปลายทาง คุณรับทราบว่าซอฟต์แวร์นี้มีให้แก่คุณแบบ "ตามสภาพ" โดยไม่มีการรับประกันทั้งโดยชัดแจ้งหรือโดยนัย ไม่ว่าในประเภทใดภายในขอบเขตสูงสุดที่กฎหมายอนุญาต ผู้ให้บริการ ผู้ให้การอนุญาตแก่ผู้ให้บริการหรือบริษัทในเครือ หรือผู้ถือลิขสิทธิ์ ไม่ได้ให้การรับรองหรือรับประกันทั้งโดยชัดแจ้งและโดยนัย ซึ่งจะรวมถึง แต่ไม่จำกัดเพียงการรับประกันการขาย หรือความเหมาะสมกับวัตถุประสงค์อย่างใดอย่างหนึ่งเป็นการเฉพาะ หรือการรับประกันว่าซอฟต์แวร์ไม่ได้ละเมิดสิทธิบัตร ลิขสิทธิ์

เครื่องหมายการค้าหรือสิทธิอื่นๆ ของบุคคลที่สาม ผู้ให้บริการหรือบุคคลอื่นไม่มีการรับประกันใดๆ ว่าฟังก์ชันที่มีอยู่ในซอฟต์แวร์นี้จะเป็นไปตามความต้องการ หรือการทำงานของซอฟต์แวร์จะทำงานต่อเนื่องและปราศจากข้อผิดพลาด คุณต้องรับผิดชอบและรับความเสี่ยงทั้งหมดสำหรับการเลือกซอฟต์แวร์ เพื่อให้ได้ผลลัพธ์ตามเจตนารมณ์ของคุณ และสำหรับการติดตั้ง การใช้งาน และผลที่จะได้รับจากซอฟต์แวร์

12. **ไม่มีข้อผูกมัดอื่น** ข้อตกลงนี้ไม่ได้แสดงถึงภาระหน้าที่อื่นใดในส่วนของผู้ให้บริการและผู้ให้การอนุญาตแก่ผู้ให้บริการ ยกเว้นจะระบุไว้อย่างชัดเจนในที่นี้

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

14. ในข้อตกลงนี้จะไม่มีผลกระทบต่อสิทธิตามกฎหมายของฝ่ายใดที่มีฐานะเป็นผู้บริโภคถ้าเกิดข้อขัดแย้งในการทำงาน

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

16. **การโอนใบอนุญาต** ซอฟต์แวร์สามารถโอนจากระบบคอมพิวเตอร์หนึ่งไปยังอีกระบบหนึ่ง ยกเว้นจะขัดกับข้อ

กำหนดของข้อตกลง ถ้าไม่ขัดกับข้อกำหนดของข้อตกลง ผู้ใช้ปลายทางจะได้รับสิทธิเฉพาะสำหรับการโอนใบอนุญาตอย่างถาวร และสิทธิทั้งหมดที่มาจากข้อตกลงนี้ไปยังผู้ใช้ปลายทางรายอื่น โดยมีความยินยอมของผู้ให้บริการ ตามเงื่อนไขว่า (i) ผู้ใช้ปลายทางเดิมต้องไม่เก็บสำเนาของซอฟต์แวร์ไว้ (ii) การโอนสิทธิจะต้องเป็นโดยตรง เช่น จากผู้ใช้ปลายทางเดิมไปยังผู้ใช้ปลายทางรายใหม่ (iii) ผู้ใช้ปลายทางรายใหม่ต้องถือสิทธิและภาระหน้าที่ทั้งหมดที่เป็นหน้าที่รับผิดชอบของผู้ใช้ปลายทางเดิมภายใต้ข้อกำหนดของข้อตกลงนี้ (iv) ผู้ใช้ปลายทางเดิมต้องให้เอกสารประกอบแก่ผู้ใช้ปลายทางรายใหม่ ซึ่งจะช่วยตรวจสอบซอฟต์แวร์ที่เป็นของแท้ดังที่ระบุภายใต้ข้อ 17

17. **การตรวจสอบซอฟต์แวร์ที่เป็นของแท้** ผู้ใช้ปลายทางสามารถพิสูจน์สิทธิ์ในการใช้ซอฟต์แวร์ได้โดยใช้วิธีการใดวิธีการหนึ่งต่อไปนี้: (i) ผ่านใบรับรองของใบอนุญาตที่ออกโดยผู้ให้บริการหรือบุคคลที่สามที่มีการกำหนดโดยผู้ให้บริการ (ii) ผ่านข้อตกลงใบอนุญาตที่เป็นลายลักษณ์อักษร ถ้ามีการสรุปข้อตกลงดังกล่าวไว้ (iii) ผ่านการส่งอีเมลที่ส่งไปยังผู้ให้บริการซึ่งมีรายละเอียดของการอนุญาต (ชื่อผู้ใช้และรหัสผ่าน) อาจจำเป็นต้องใช้ข้อมูลใบอนุญาตและข้อมูลอัตลักษณ์ผู้ใช้ปลายทางตามที่ระบุไว้ในนโยบายความเป็นส่วนตัว เพื่อวัตถุประสงค์ในการตรวจสอบความเป็นของแท้ของซอฟต์แวร์

18. **การอนุญาตสำหรับหน่วยงานของรัฐที่มีอำนาจและรัฐบาลของสหรัฐอเมริกา** หน่วยงานของรัฐที่มีอำนาจรวมถึงรัฐบาลของสหรัฐอเมริกา จะได้รับซอฟต์แวร์นี้พร้อมด้วยสิทธิการอนุญาตและข้อจำกัดที่อธิบายไว้ในข้อตกลงนี้

19. **การปฏิบัติตามการควบคุมด้านการค้า**

ก) คุณจะไม่ส่งออก ส่งออกซ้ำ ถ่ายโอนหรือทำให้บุคคลใดๆ ใช้งานซอฟต์แวร์นี้ได้ ไม่ว่าทางตรงหรือทางอ้อม หรือใช้งานในลักษณะใด ๆ หรือมีส่วนร่วมในการกระทำใด ๆ ที่อาจส่งผลให้ ESET หรือบริษัทผู้ถือหุ้น กิจการในเครือของบริษัทผู้ถือหุ้น รวมถึงหน่วยงานที่ควบคุมโดยบริษัทผู้ถือหุ้น (ซึ่งต่อไปนี้จะเรียกว่า "บริษัทในเครือ") มีการล่วงละเมิดหรือได้รับผลกระทบด้านลบภายใต้กฎหมายการควบคุมการค้าซึ่งรวมถึง

i. กฎหมายใด ๆ ที่ควบคุม จำกัด หรือบังคับใช้ข้อกำหนดด้านใบอนุญาตเกี่ยวกับการส่งออก การส่งออกซ้ำหรือโอนย้ายสินค้า ซอฟต์แวร์ เทคโนโลยี หรือบริการที่ออกหรือนำไปใช้โดยรัฐบาล ภาครัฐ หรือหน่วยงานซึ่งมีอำนาจกำกับดูแลของสหรัฐอเมริกา สิงคโปร์ สหราชอาณาจักร สหภาพยุโรป หรือประเทศสมาชิกหรือประเทศใด ๆ ที่มีข้อผูกพันภายใต้ข้อตกลงที่จะต้องดำเนินการหรือที่ ESET หรือบริษัทในเครือใด ๆ จัดตั้งขึ้นหรือดำเนินการ และ

ii. การลงโทษทางเศรษฐกิจ การเงิน การค้าหรือทางด้านอื่น ๆ การจำกัด คำสั่งห้ามค้าขาย การห้ามนำเข้าหรือส่งออก การห้ามโอนเงินหรือทรัพย์สินหรือการให้บริการ หรือมาตรการที่เทียบเท่าที่กำหนดโดยรัฐบาล ภาครัฐ หรือหน่วยงานซึ่งมีอำนาจกำกับดูแลของสหรัฐอเมริกา สิงคโปร์ สหราชอาณาจักร สหภาพยุโรป หรือประเทศสมาชิกใด ๆ หรือประเทศใด ๆ ที่มีข้อผูกพันภายใต้ข้อตกลงที่จะต้องดำเนินการหรือที่ ESET หรือบริษัทในเครือใด ๆ จัดตั้งขึ้นหรือ

ดำเนินการ

(การกระทำทางกฎหมายที่อ้างถึงในจุดที่ i และ ii ข้างต้นร่วมกัน เรียกว่า “กฎหมายการควบคุมการค้า”)

ข) ESET มีสิทธิ์ระงับข้อผูกพันภายใต้ หรือยุติข้อกำหนดเหล่านี้โดยมีผลทันทีในกรณีที่:

i. ESET พิจารณาโดยอิงจากความเห็นที่สมเหตุสมผลว่าผู้ใช้ละเมิดหรือมีแนวโน้มที่จะละเมิดบทบัญญัติของข้อ 19 ก ของข้อตกลง หรือ

ii. ผู้ใช้ปลายทางและ/หรือซอฟต์แวร์ต้องอยู่ภายใต้กฎหมายควบคุมการค้าและ ด้วยเหตุนี้ ESET จะพิจารณาโดยอิงจากความเห็นที่สมเหตุสมผลว่า การปฏิบัติตามภาระหน้าที่ภายใต้ข้อตกลงนี้ต่อไปอาจส่งผลให้ ESET หรือ บริษัทในมีการล่วงละเมิดหรือได้รับผลกระทบด้านลบภายใต้กฎหมายควบคุมการค้า

ค) ไม่มีสิ่งใดในข้อตกลงที่มีจุดมุ่งหมาย และไม่มีสิ่งใดที่ควรแปลความหมายหรือตีความ ไปในทางชักชวนหรือกำหนดให้ฝ่ายหนึ่งฝ่ายใดกระทำการหรืองดเว้นการกระทำ (หรือตกลงที่จะกระทำหรือละเว้นจากการกระทำ) ในลักษณะใด ๆ ซึ่งไม่สอดคล้องกับ ผิดหรือต้องห้ามภายใต้กฎหมายควบคุมการค้าใดๆ ที่บังคับใช้

20. **การแจ้งเตือน** การแจ้งเตือนและการส่งคืนซอฟต์แวร์และเอกสารประกอบทั้งหมดจะต้องส่งถึง: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic โดยไม่กระทบต่อสิทธิ์ของ ESET ในการแจ้งการเปลี่ยนแปลงใดๆ ในข้อตกลงนี้ นโยบายความเป็นส่วนตัว นโยบาย EOL และเอกสารประกอบ ตามข้อ 22 ของข้อตกลงนี้ ESET อาจส่งอีเมลถึงคุณ แจ้งเตือนในแอพผ่านซอฟต์แวร์ หรือโพสต์การสื่อสารบนเว็บไซต์ของเรา คุณตกลงที่จะรับการสื่อสารทางกฎหมายจาก ESET ในรูปแบบอิเล็กทรอนิกส์ รวมถึงการสื่อสารใดๆ เกี่ยวกับการเปลี่ยนแปลงข้อกำหนด ข้อกำหนดพิเศษ หรือนโยบายความเป็นส่วนตัว ข้อเสนอสัญญา/การยอมรับ หรือคำเชิญใดๆ ในการดำเนินการ ประกาศ หรือการสื่อสารทางกฎหมายอื่นๆ โดยจะถือว่าได้รับการสื่อสารทางอิเล็กทรอนิกส์ดังกล่าวในรูปแบบเป็นลายลักษณ์อักษร เว้นแต่กฎหมายที่บังคับใช้จะกำหนดให้มีการสื่อสารในรูปแบบอื่นโดยเฉพาะ

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

22. **บทบัญญัติทั่วไป** ถ้าบทบัญญัติใดของข้อตกลงนี้ไม่มีผลบังคับหรือเป็นโมฆะ ข้อตกลงนี้จะไม่มีผลต่อความถูกต้องของบทบัญญัติอื่นๆ ในข้อตกลง ซึ่งจะมีผลบังคับและถูกต้องตามเงื่อนไขที่ระบุไว้ในที่นี้ ข้อตกลงนี้ดำเนินการเป็นภาษาอังกฤษ ในกรณีที่การแปลข้อตกลงนี้จัดทำขึ้นเพื่อความสะดวกหรือวัตถุประสงค์อื่นใด หรือในกรณีที่มี

ความแตกต่างในระหว่างเวอร์ชันภาษาต่างๆ ของข้อตกลงนี้ ให้ยึดถือเวอร์ชันภาษาอังกฤษเป็นหลัก

ESET ขอสงวนสิทธิ์ในการเปลี่ยนแปลงซอฟต์แวร์ เช่นเดียวกับสงวนสิทธิ์ในการแก้ไขข้อตกลง ส่วนเพิ่มเติม ภาคผนวก นโยบายความเป็นส่วนตัว นโยบาย EOL และเอกสารเพิ่มเติม หรือส่วนใดส่วนหนึ่งของรายการดังกล่าวได้ตลอดเวลาโดยอัพเดทเอกสารที่เกี่ยวข้อง (i) เพื่อสะท้อนถึงการเปลี่ยนแปลงซอฟต์แวร์หรือวิธีที่ ESET ดำเนินธุรกิจ (ii) ด้วยเหตุผลด้านกฎหมาย ด้านข้อบังคับหรือความปลอดภัย หรือ (iii) เพื่อป้องกันการละเมิดหรืออันตราย คุณจะได้รับการแจ้งล่วงหน้าถึงการเปลี่ยนแปลงใดๆ ของข้อตกลงนี้ทางอีเมล การแจ้งเตือนภายในแอพ หรือทางอิเล็กทรอนิกส์ในรูปแบบอื่นๆ หากคุณไม่เห็นด้วยกับการเปลี่ยนแปลงที่เสนอในข้อตกลงคุณ สามารถยกเลิกข้อตกลงได้ตามข้อ 10 ภายใน 30 วันหลังจากได้รับหนังสือแจ้งการเปลี่ยนแปลง การเปลี่ยนแปลงที่เสนอจะถือว่าได้รับการยอมรับและมีผลบังคับใช้ต่อคุณ ณ วันที่คุณได้รับแจ้งการเปลี่ยนแปลง เว้นแต่คุณจะยุติข้อตกลงภายในระยะเวลาที่กำหนดไว้นี้

ข้อตกลงทั้งหมดนี้เป็นข้อตกลงระหว่างผู้ให้บริการกับคุณเกี่ยวกับซอฟต์แวร์ และมีผลเหนือกว่าการรับรอง การแลกเปลี่ยนความคิดเห็น ภาระหน้าที่ การสื่อสาร หรือโฆษณาที่เกี่ยวข้องกับซอฟต์แวร์ทั้งหมดที่เกิดขึ้นก่อนหน้านี้

ส่วนเพิ่มเติมสำหรับข้อตกลง

การประเมินความปลอดภัยของอุปกรณ์ที่เชื่อมต่อกับเครือข่าย บทบัญญัติเพิ่มเติมจะนำไปใช้กับการประเมินความปลอดภัยของอุปกรณ์ที่เชื่อมต่อกับเครือข่ายดังต่อไปนี้:

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

การป้องกันการใช้ข้อมูลในทางที่ผิด บทบัญญัติเพิ่มเติมจะนำไปใช้กับการป้องกันการใช้ข้อมูลในทางที่ผิดดังต่อไปนี้:

ซอฟต์แวร์ประกอบด้วยฟังก์ชันที่ป้องกันการสูญหายหรือการใช้ข้อมูลสำคัญผิดวัตถุประสงค์ ซึ่งเชื่อมโยงโดยตรงกับการโจรกรรมคอมพิวเตอร์ ฟังก์ชันนี้จะถูกปิดไว้ในการตั้งค่าเริ่มต้นของซอฟต์แวร์ คุณจำเป็นต้องสร้างบัญชี ESET HOME ขึ้นเพื่อเปิดใช้งาน ซึ่งฟังก์ชั่นนี้จะเปิดใช้งานการเก็บข้อมูลในกรณีที่คอมพิวเตอร์ถูกโจรกรรม ถ้าคุณเลือกที่จะเปิดใช้งานฟังก์ชันนี้ของซอฟต์แวร์ ข้อมูลเกี่ยวกับคอมพิวเตอร์ที่ถูกโจรกรรมจะถูกส่งให้แก่ผู้ให้บริการซึ่งอาจรวมถึงข้อมูลเกี่ยวกับตำแหน่งเครือข่ายของคอมพิวเตอร์ ข้อมูลเกี่ยวกับเนื้อหาที่แสดงบนหน้าจอคอมพิวเตอร์

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

ESET Secure Data บทบัญญัติเพิ่มเติมจะนำไปใช้กับ ESET Secure Data ดังต่อไปนี้:

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

ก) "ข้อมูล"ข้อมูลหรือข้อมูลใดๆ ที่เข้ารหัสหรือถอดรหัสโดยใช้ซอฟต์แวร์;

ข) "ผลิตภัณฑ์" ซอฟต์แวร์ ESET Secure Data และเอกสารประกอบ;

ค) "ESET Secure Data"ซอฟต์แวร์หนึ่งหรือหลายซอฟต์แวร์ที่ใช้เพื่อเข้ารหัสหรือถอดรหัสข้อมูลอิเล็กทรอนิกส์;

การอ้างอิงข้อความที่เป็นพหูพจน์ทั้งหมดต้องมีเอกพจน์รวมอยู่ด้วย และการอ้างอิงข้อความที่หมายถึงเพศชายทั้งหมดต้องมีเพศหญิงและความไม่มีเพศรวมอยู่ด้วย หรือในทางกลับกัน คำต่างๆ ที่ไม่มีคำนิยามเฉพาะจะถูกใช้ตามคำนิยามที่ระบุไว้ในข้อตกลงนี้

2. คำประกาศของผู้ใช้ปลายทางเพิ่มเติม คุณรับทราบและยอมรับ ดังนี้

ก) เป็นหน้าที่ของคุณที่ต้องปกป้อง รักษา และสำรองข้อมูล;

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

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

ง) คุณต้องรับผิดชอบต่อการใช้งานผลิตภัณฑ์ ผู้ให้บริการจะไม่มีส่วนรับผิดต่อการสูญเสีย การกล่าวอ้าง หรือความเสียหายที่เป็นผลมาจากการเข้ารหัสหรือถอดรหัสข้อมูลหรือข้อมูลอื่นๆ อย่างผิดพลาดหรือไม่ได้รับอนุญาต ไม่ว่าข้อมูลดังกล่าวจะเก็บไว้ที่ใดหรือเก็บไว้อย่างไรก็ตาม;

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

ฉ) เป็นหน้าที่ของผู้ใช้ปลายทางที่ต้องตรวจสอบให้แน่ใจว่าระดับความปลอดภัยและการเข้ารหัสที่ผลิตภัณฑ์มีให้นั้นเหมาะสมกับความต้องการของคุณเอง;

ช) คุณต้องรับผิดชอบต่อการใช้งานผลิตภัณฑ์นี้หรือผลิตภัณฑ์ใดๆ ของคุณ ซึ่งรวมถึงแต่ไม่จำกัดเพียงการตรวจสอบให้แน่ใจว่าการใช้งานดังกล่าวตรงตามกฎหมายและข้อบังคับที่มีผลบังคับใช้ของสาธารณรัฐสโลวักหรือประเทศ ภูมิภาค หรือรัฐอื่นใดที่นำผลิตภัณฑ์นี้ไปใช้งาน คุณจำเป็นต้องตรวจสอบให้แน่ใจว่าก่อนลงมือใช้ผลิตภัณฑ์ใดๆ นั้น คุณได้ตรวจสอบให้แน่ใจแล้วว่าจะไม่เป็นการฝ่าฝืนต่อคำสั่งห้ามตามกฎหมายของรัฐบาลใดๆ (ในสาธารณรัฐสโลวักหรือที่อื่นใด);

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

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

บทบัญญัติเพิ่มเติมสำหรับ ESET Secure Data จะบังคับใช้เฉพาะสำหรับผู้ใช้ปลายทางของ ESET Smart Security Premium เท่านั้น

Password Managerซอฟต์แวร์. บทบัญญัติเพิ่มเติมจะนำไปใช้กับซอฟต์แวร์ Password Manager ดังต่อไปนี้:

1. คำประกาศของผู้ใช้ปลายทางเพิ่มเติม คุณรับทราบและยอมรับว่าคุณจะไม่สามารถทำสิ่งต่างๆ ดังนี้

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

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

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

2. ข้อจำกัดความรับผิด PASSWORD MANAGER SOFTWARE นี้ได้จัดหาให้แก่คุณแบบ "ตามสภาพ" โดยไม่มีการรับประกันทั้งโดยชัดแจ้งหรือโดยนัย คุณใช้งานซอฟต์แวร์นี้โดยรับความเสี่ยงด้วยตัวคุณเอง ผู้ให้บริการจะไม่มีความรับผิดต่อการสูญเสียข้อมูล ความเสียหาย การจำกัดการเปิดให้บริการ ซึ่งรวมถึงข้อมูลใดๆ ที่ส่งโดย PASSWORD MANAGER SOFTWARE ไปยังพื้นที่เก็บข้อมูลภายนอกโดยมีวัตถุประสงค์เพื่อซิงโครไนซ์และสำรองข้อมูล การเข้ารหัสข้อมูลโดยใช้ PASSWORD MANAGER SOFTWARE ไม่ได้หมายความว่าผู้ให้บริการต้องรับผิดชอบต่อความปลอดภัยของข้อมูลดังกล่าว คุณยอมรับโดยตรงว่าข้อมูลที่ได้รับ ใช้ เข้ารหัส จัดเก็บ ซิงโครไนซ์ หรือส่งโดยใช้ PASSWORD MANAGER SOFTWARE นั้นสามารถจัดเก็บลงในเซิร์ฟเวอร์ของบุคคลที่สามได้ (มีผลเฉพาะกับการใช้งาน

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

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

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

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

ข้อมูลที่มอบให้ผ่านทาง PASSWORD MANAGER SOFTWARE ซึ่งรวมถึงราคาเสนอหุ้น บทวิเคราะห์ ข้อมูลตลาด ข่าวสาร และข้อมูลทางการเงินอาจมีความล่าช้า ไม่แม่นยำ หรือมีข้อผิดพลาดหรือส่วนที่ขาดหาย และบุคลากรและผู้

ให้การอนุญาตของผู้ให้บริการจะไม่มีส่วนรับผิดชอบต่อสิ่งต่างๆ ดังกล่าว ผู้ให้บริการอาจเปลี่ยนหรือหยุดพัฒนาส่วนหรือคุณลักษณะใดๆ ของ PASSWORD MANAGER SOFTWARE หรือการใช้งานของคุณลักษณะหรือเทคโนโลยีใดๆ ใน PASSWORD MANAGER SOFTWARE ได้ทุกเมื่อโดยไม่ต้องแจ้งให้คุณทราบล่วงหน้า

หากเงื่อนไขในบทความนี้เป็นโมฆะไม่ว่าด้วยเหตุผลใดก็ตาม หรือมีการถือให้ผู้ให้บริการมีหน้าที่รับผิดชอบต่อความสูญเสีย ความเสียหาย ฯลฯ ภายใต้กฎหมายที่บังคับใช้ ทุกฝ่ายจะยอมรับว่าความรับผิดชอบที่ผู้ให้บริการมีต่อคุณจะจำกัดอยู่เพียงเท่ากับยอดรวมค่าใบอนุญาตทั้งหมดที่คุณได้ชำระเท่านั้น

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

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

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

สูญเสียข้อมูลอันเป็นผลมาจากการดาว์นโหลดและ/หรือใช้งานเนื้อหาหรือบริการดังกล่าว เพื่อเป็นการลดความเสี่ยงต่อการสูญเสียข้อมูลที่สำคัญ ผู้ให้บริการขอแนะนำให้ลุกค้าทำการสำรองข้อมูลในฐานข้อมูลและไฟล์ที่ละเอียดอ่อนอื่นๆ ไปยังไดรฟ์ภายนอกเป็นระยะๆ ผู้ให้บริการไม่สามารถมอบความช่วยเหลือในการกู้คืนข้อมูลที่สูญหายหรือเสียหายใดๆ ได้ หากผู้ให้บริการมอบบริการสำรองข้อมูลสำหรับไฟล์ฐานข้อมูลผู้ใช้ในกรณีที่เกิดความเสียต่อหรือการลบไฟล์ในพีซีของผู้ใช้ บริการสำรองข้อมูลดังกล่าวจะไม่มีการรับประกันใดๆ และไม่ได้มีนัยว่าผู้ให้บริการต้องมีความรับผิดชอบใดๆ ต่อคุณแต่อย่างใด

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

5. ข้อมูลและคำแนะนำเกี่ยวกับการถอนการติดตั้ง คุณต้องส่งออกข้อมูลใดๆ ที่คุณต้องการเก็บจากฐานข้อมูลก่อนที่จะถอนการติดตั้ง Password Manager Software

บทบัญญัติเพิ่มเติมสำหรับซอฟต์แวร์ Password Manager จะบังคับใช้เฉพาะสำหรับผู้ใช้ปลายทางของ ESET Smart Security Premium เท่านั้น

ESET LiveGuard. บทบัญญัติเพิ่มเติมจะนำไปใช้กับ ESET LiveGuard ดังต่อไปนี้:

ซอฟต์แวร์มีฟังก์ชั่นการวิเคราะห์ไฟล์ที่ส่งโดยผู้ใช้ปลายทางเพิ่มเติม ผู้ให้บริการจะใช้เฉพาะไฟล์ที่ส่งโดยผู้ใช้ปลายทางและผลการวิเคราะห์ที่สอดคล้องกับนโยบายความเป็นส่วนตัวและสอดคล้องกับข้อบังคับทางกฎหมายที่เกี่ยวข้องเท่านั้น

บทบัญญัติเพิ่มเติมสำหรับ ESET LiveGuard จะบังคับใช้เฉพาะสำหรับผู้ใช้ปลายทางของ ESET Smart Security Premium เท่านั้น

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

นโยบายความเป็นส่วนตัว

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

ต้องการปฏิบัติตามข้อกำหนดด้านความโปร่งใสตามมาตรฐานทางกฎหมาย ภายใต้ระเบียบการคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป ("GDPR") เพื่อให้บรรลุเป้าหมายนี้ เราเผยแพร่นโยบายความเป็นส่วนตัวนี้โดยมีวัตถุประสงค์เพื่อแจ้งข้อมูลลูกค้าของเราเท่านั้น ("ผู้ใช้ปลายทาง" หรือ "คุณ") ในฐานะเจ้าของข้อมูล เกี่ยวกับหัวข้อการปกป้องข้อมูลส่วนบุคคลต่อไปนี้:

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

พื้นฐานทางกฎหมายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

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

- พื้นฐานทางกฎหมายด้านผลประโยชน์ที่ชอบด้วยกฎหมาย (มาตรา 6 (1) (f) GDPR) ซึ่งช่วยให้เราสามารถประมวลผลข้อมูลเกี่ยวกับวิธีที่ลูกค้าของเราใช้บริการและความพึงพอใจของลูกค้า เพื่อให้ผู้ใช้ของเราได้รับการคุ้มครอง การสนับสนุน และประสบการณ์ที่ดีที่สุดที่เราสามารถนำเสนอได้ แม้แต่การตลาดก็ได้รับการยอมรับจากกฎหมายที่เกี่ยวข้องว่าเป็นประโยชน์โดยชอบด้วยกฎหมาย ด้วยเหตุนี้เราจึงมักพึ่งพาคุกกี้นี้เพื่อสื่อสารด้านการตลาดกับลูกค้าของเรา
- เราอาจร้องขอความยินยอม (มาตรา 6 (1) (a) GDPR) จากคุณในสถานการณ์ที่เฉพาะเจาะจง เมื่อเราเล็งเห็นว่าพื้นฐานทางกฎหมายนี้เป็นพื้นฐานที่เหมาะสมที่สุด หรือหากกฎหมายกำหนดไว้
- ความสอดคล้องกับข้อผูกมัดทางกฎหมาย (มาตรา 6 (1) (c) GDPR) เช่น ความต้องการด้านการกำหนดเงื่อนไขสำหรับการติดต่อสื่อสารทางอิเล็กทรอนิกส์ การเก็บรักษาเอกสารใบแจ้งหนี้หรือใบเรียกเก็บเงิน

การแชร์ข้อมูลและการรักษาความลับ

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

ESET จะประมวลผลข้อมูลในสหภาพยุโรป (EU) ถ้าเป็นไปได้ อย่างไรก็ตาม เราอาจจำเป็นต้องถ่ายโอนข้อมูลของคุณไปยังประเทศที่อยู่นอกสหภาพยุโรปโดยขึ้นอยู่กับตำแหน่งที่ตั้งของคุณ (การใช้ผลิตภัณฑ์และ/หรือบริการของเราที่อยู่นอกสหภาพยุโรป) และ/หรือบริการที่คุณเลือก ตัวอย่างเช่น เราใช้บริการของบริษัทอื่นในการเชื่อมต่อกับการประมวลผลแบบคลาวด์ ในกรณีเหล่านี้ เราจะเลือกผู้ให้บริการของเราอย่างรอบคอบ และรับรองว่ามีการป้องกันข้อมูลในระดับที่เหมาะสมผ่านมาตรการทางสัญญา เช่นเดียวกับมาตรการทางเทคนิคและองค์กร ตามกฎแล้ว เรายอมรับข้อสัญญามาตรฐานของสหภาพยุโรป โดยมีข้อบังคับเพิ่มเติมทางสัญญาหากจำเป็น

สำหรับบางประเทศนอกสหภาพยุโรป เช่น สหราชอาณาจักรและสวิตเซอร์แลนด์ สหภาพยุโรปได้กำหนดระดับการคุ้มครองข้อมูลไว้ในระดับที่เทียบเคียงกันได้แล้ว เนื่องจากมีการป้องกันข้อมูลในระดับที่เทียบเคียงกันได้ การถ่ายโอนข้อมูลไปยังประเทศเหล่านี้จึงไม่จำเป็นต้องมีการอนุญาตหรือข้อตกลงพิเศษใดๆ

การรักษาความปลอดภัยของข้อมูล

ESET ใช้มาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมเพื่อให้แน่ใจว่ามีระดับความปลอดภัยที่เหมาะสมกับความเสี่ยงที่อาจเกิดขึ้น เรากำลังพยายามอย่างเต็มที่เพื่อให้มั่นใจได้ถึงการรักษาความลับที่ต่อเนื่อง ความสมบูรณ์ ความพร้อมใช้งาน และความยืดหยุ่นของระบบและบริการด้านการประมวลผล อย่างไรก็ตาม ในกรณีที่ข้อมูลถูกละเมิดจนเป็นผลทำให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของคุณ เราพร้อมที่จะแจ้งให้หน่วยงานกำกับดูแลที่เกี่ยวข้องทราบรวมถึงผู้ใช้ปลายทางที่เป็นเจ้าของข้อมูลด้วย

สิทธิของเจ้าของข้อมูล

สิทธิของผู้ใช้ปลายทางทุกคนมีความสำคัญ และเราขอแจ้งให้คุณทราบว่าผู้ใช้ปลายทางทั้งหมด (จากประเทศในสหภาพยุโรปหรือไม่ใช่สหภาพยุโรป) จะได้รับการรับประกันสิทธิดังต่อไปนี้ที่ ESET หากต้องการใช้สิทธิ์ในการเป็นเจ้าของข้อมูลของคุณ คุณสามารถติดต่อเราผ่านแบบฟอร์มการสนับสนุนหรือทางอีเมลได้ที่ dpo@eset.sk เราจะขอข้อมูลต่อไปนี้จากคุณเพื่อวัตถุประสงค์ในการระบุตัวตน ชื่อ ที่อยู่อีเมล และรหัสใบอนุญาตหรือหมายเลขลูกค้าและบริษัทที่เป็นเครือข่าย หากมี โปรดอย่าส่งข้อมูลส่วนบุคคลอื่นๆ เช่น วันเดือนปีเกิด ให้แก่เรา เราขอชี้ว่า เราจะ

ประมวลผลข้อมูลส่วนบุคคลของคุณเพื่อให้สามารถดำเนินการตามคำขอของคุณได้ รวมถึงเพื่อวัตถุประสงค์ในการระบุตัวตน

สิทธิในการเพิกถอนความยินยอม สิทธิในการเพิกถอนความยินยอมจะใช้ได้ในกรณีที่มีการประมวลผลตามความยินยอมเท่านั้น หากเราประมวลผลข้อมูลส่วนบุคคลตามความยินยอมของคุณ คุณมีสิทธิที่จะเพิกถอนความยินยอมได้ทุกเมื่อโดยไม่ต้องให้เหตุผล การเพิกถอนความยินยอมของคุณจะมีผลเฉพาะในอนาคต และไม่มีผลต่อความชอบด้วยกฎหมายของข้อมูลที่ประมวลผลก่อนการเพิกถอนดังกล่าว

สิทธิในการคัดค้าน สิทธิในการคัดค้านการประมวลผลจะใช้ได้ในกรณีที่มีการประมวลผลตามผลประโยชน์ที่ชอบด้วยกฎหมายของ ESET หรือบริษัทอื่นเท่านั้น หากเราประมวลผลข้อมูลส่วนบุคคลของคุณเพื่อปกป้องผลประโยชน์ที่ชอบด้วยกฎหมาย คุณในฐานะเจ้าของข้อมูลมีสิทธิคัดค้านผลประโยชน์ที่ชอบด้วยกฎหมายที่เรากำหนดให้ และคัดค้านการประมวลผลข้อมูลส่วนบุคคลของคุณได้ตลอดเวลา การคัดค้านของคุณจะมีผลเฉพาะในอนาคต และไม่มีผลต่อความถูกต้องตามกฎหมายของข้อมูลที่ประมวลผลก่อนการคัดค้านดังกล่าว หากเราประมวลผลข้อมูลส่วนบุคคลของคุณเพื่อวัตถุประสงค์ทางการตลาดทางตรง คุณไม่จำเป็นต้องให้เหตุผลในการคัดค้านของคุณ ความนี้ยังใช้กับการสร้างโปรไฟล์ ตราบเท่าที่มีการเชื่อมต่อกับการตลาดทางตรงดังกล่าวอีกด้วย ในกรณีอื่นๆ เราขอให้คุณแจ้งให้เราทราบสั้นๆ เกี่ยวกับข้อร้องเรียนว่าด้วยผลประโยชน์ที่ชอบด้วยกฎหมายของ ESET ในการประมวลผลข้อมูลส่วนบุคคลของคุณ

โปรดทราบว่าในบางกรณี เรามีสิทธิประมวลผลข้อมูลส่วนบุคคลของคุณต่อไปบนพื้นฐานของพื้นฐานทางกฎหมายอื่นๆ ตัวอย่างเช่น เพื่อการปฏิบัติตามสัญญา แม้จะมีการเพิกถอนความยินยอมจากคุณก็ตาม

สิทธิในการเข้าถึง ในฐานะเจ้าของข้อมูล คุณมีสิทธิที่จะได้รับข้อมูลเกี่ยวกับข้อมูลของคุณที่ ESET จัดเก็บโดยไม่เสียค่าใช้จ่ายได้ตลอดเวลา

สิทธิในการแก้ให้ถูกต้อง หากเราประมวลผลข้อมูลส่วนบุคคลที่ไม่ถูกต้องเกี่ยวกับคุณโดยไม่ได้ตั้งใจ คุณมีสิทธิที่จะแก้ไขข้อมูลดังกล่าว

สิทธิในการลบและสิทธิในการจำกัดการประมวลผล ในฐานะเจ้าของข้อมูล คุณมีสิทธิร้องขอให้ลบหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลของคุณ หากเราประมวลผลข้อมูลส่วนบุคคลของคุณ ตัวอย่างเช่น ด้วยความยินยอมของคุณ และคุณเพิกถอนความยินยอมนั้นโดยไม่มีพื้นฐานทางกฎหมายอื่นๆ ตัวอย่างเช่น สัญญา เราจะลบข้อมูลส่วนบุคคลของคุณทันที ข้อมูลส่วนบุคคลของคุณจะถูกลบทันทีที่ไม่จำเป็นต้องใช้ตามวัตถุประสงค์ที่ระบุไว้ เมื่อสิ้นสุดระยะเวลาการเก็บรักษาข้อมูล

หากเราใช้ข้อมูลส่วนบุคคลของคุณเพื่อวัตถุประสงค์ในการตลาดทางตรง และคุณได้เพิกถอนความยินยอมของคุณหรือคัดค้านผลประโยชน์ที่ชอบด้วยกฎหมายของ ESET เราจะจำกัดการประมวลผลข้อมูลส่วนบุคคลของคุณเท่าที่เรา

รวบรวมข้อมูลติดต่อของคุณไว้ได้ในบัญชีดำภายในของเรา ทั้งนี้เพื่อหลีกเลี่ยงการติดต่อที่ไม่พึงประสงค์ มิฉะนั้นข้อมูลส่วนบุคคลของคุณจะถูกลบ

โปรดทราบว่าเราอาจจำเป็นต้องเก็บข้อมูลของคุณไว้จนกว่าภาระผูกพันในการเก็บรักษาและระยะเวลา ซึ่งออกโดยสมาชิกสภานิติบัญญัติหรือหน่วยงานกำกับดูแล จะหมดอายุ ภาระผูกพันในการเก็บรักษาและระยะเวลานี้อาจเป็นผลมาจากกฎหมายของสโลวะเกีย หลังจากนั้น ข้อมูลที่เกี่ยวข้องจะถูกลบเป็นประจำ

สิทธิ์ในการเคลื่อนย้ายข้อมูล เรายินดีที่จะมอบข้อมูลส่วนบุคคลที่ประมวลผลโดย ESET ในรูปแบบ xls ให้แก่คุณซึ่งเป็นเจ้าของข้อมูล

สิทธิในการยื่นเรื่องร้องเรียน ในฐานะเจ้าของข้อมูล คุณมีสิทธิที่จะยื่นเรื่องร้องเรียนต่อหน่วยงานกำกับดูแลได้ตลอดเวลา ESET มีหน้าที่ต้องปฏิบัติตามกฎหมายของประเทศสโลวาเกียและเราต้องปฏิบัติตามกฎหมายว่าด้วยการปกป้องข้อมูลในฐานะส่วนหนึ่งของสหภาพยุโรป หน่วยงานกำกับดูแลข้อมูลที่เกี่ยวข้องคือสำนักงานคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสโลวัก ซึ่งตั้งอยู่ที่ Hraničná 12, 82007 Bratislava 27, Slovak Republic

การประมวลผลข้อมูลส่วนบุคคลของคุณ

บริการที่ ESET นำเสนอในผลิตภัณฑ์ของเรามีให้ภายใต้ข้อกำหนดของ EULAแต่อาจต้องให้ความสนใจบางผลิตภัณฑ์เป็นพิเศษ ราต้องการให้รายละเอียดเพิ่มเติมเกี่ยวกับการรวบรวมข้อมูลที่เกี่ยวข้องกับการให้บริการของเรา เราให้บริการต่างๆ ตามที่ได้อธิบายไว้ใน EULA และผลิตภัณฑ์ เอกสารประกอบ. เพื่อให้การทำงานทั้งหมด เราจำเป็นต้องรวบรวมข้อมูลต่อไปนี้:

ข้อมูลการออกใบอนุญาตและการเรียกเก็บเงิน ESET จะเก็บรวบรวมและประมวลผลชื่อ ที่อยู่อีเมล รหัสใบอนุญาตและที่อยู่ (หากมี) บริษัทในเครือและข้อมูลการชำระเงิน เพื่ออำนวยความสะดวกในการเปิดใช้งานใบอนุญาต การส่งมอบรหัสใบอนุญาต การแจ้งเตือนเกี่ยวกับการหมดอายุ คำขอสนับสนุน การตรวจสอบความถูกต้องของใบอนุญาต การให้บริการของเรา และการแจ้งเตือนอื่นๆ รวมถึงข้อความทางการตลาดที่สอดคล้องกับกฎหมายที่บังคับใช้ หรือความยินยอมของคุณ ESET มีหน้าที่ตามกฎหมายในการเก็บรักษาข้อมูลการเรียกเก็บเงินเป็นระยะเวลา 10 ปี อย่างไรก็ตาม ข้อมูลการออกใบอนุญาตจะไม่ระบุตัวตนภายใน 12 เดือนหลังจากใบอนุญาตหมดอายุ

รายการอัพเดทและสถิติอื่นๆ ข้อมูลที่ประมวลผลได้แก่ข้อมูลเกี่ยวกับกระบวนการติดตั้งและคอมพิวเตอร์ของคุณรวมทั้งแพลตฟอร์มที่ติดตั้งผลิตภัณฑ์ของเราและข้อมูลเกี่ยวกับการดำเนินงานและฟังก์ชันการทำงานของผลิตภัณฑ์ของเรา เช่น ระบบปฏิบัติการ, ข้อมูลฮาร์ดแวร์, ไอดีการติดตั้ง, ไอดีใบอนุญาต, ที่อยู่ IP, ที่อยู่ MAC, การตั้งค่าของผลิตภัณฑ์ ซึ่งจะถูกประมวลผลเพื่อวัตถุประสงค์ในการให้บริการอัพเดทและอัพเกรด และเพื่อวัตถุประสงค์ในการบำรุงรักษา การรักษาความปลอดภัย และการปรับปรุงโครงสร้างพื้นฐานแบ็กเอนด์ของเรา

ข้อมูลนี้จะถูกเก็บไว้โดยแยกจากข้อมูลประจำตัวที่จำเป็นสำหรับวัตถุประสงค์ในการออกใบอนุญาตและการเรียกเก็บเงิน เนื่องจากไม่จำเป็นต้องระบุตัวตนของผู้ใช้ปลายทาง โดยมีระยะเวลาการเก็บรักษาไม่เกิน 4 ปี

ระบบตรวจสอบความเชื่อถือ ESET LiveGrid® แฮชแบบวันเวย์ที่เกี่ยวกับการแทรกซึมเพื่อวัตถุประสงค์ในการใช้งานระบบตรวจสอบความเชื่อถือ ESET LiveGrid® ซึ่งปรับปรุงประสิทธิภาพของโซลูชันการป้องกันมัลแวร์ของเราโดยการเปรียบเทียบไฟล์ที่สแกนกับฐานข้อมูลของรายการที่อยู่ใน Whitelist และ Blacklist ในคลาวด์ ผู้ใช้ปลายทางจะไม่ถูกระบุตัวตนในระหว่างกระบวนการนี้

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

- การแทรกซึมต่างๆ เช่น ตัวอย่างของไวรัสและโปรแกรมที่เป็นอันตรายอื่นๆ และที่น่าสงสัย ปัญหา วัตถุที่อาจไม่เป็นที่ต้องการหรืออาจไม่ปลอดภัย เช่น ไฟล์ที่สามารถเปิดใช้งานได้ ข้อความอีเมลที่คุณเป็นผู้รายงานว่าเป็นสแปมหรือที่ผลิตภัณฑ์ของเราปักธงเตือน
- ข้อมูลที่เกี่ยวกับการใช้อินเทอร์เน็ต เช่น ที่อยู่ IP และข้อมูลเกี่ยวกับภูมิศาสตร์, แพ็คเกจ IP, URL และเฟรมอีเธอร์เน็ต
- ไฟล์แครชดัมป์และข้อมูลต่างๆ ที่มีอยู่

ไม่ไม่ได้ประสงค์ที่จะรวบรวมข้อมูลของคุณนอกเหนือจากขอบเขตที่ระบุนี้ แต่ในบางเวลาเราก็ไม่สามารถที่จะป้องกันได้ ข้อมูลที่เก็บรวบรวมโดยไม่ได้ตั้งใจอาจรวมอยู่ในตัวของมัลแวร์เอง (เก็บรวบรวมโดยไม่ได้แจ้งให้คุณทราบหรือคุณไม่ได้อนุมัติ) หรือที่ถูกเก็บรวบรวมโดยเป็นส่วนหนึ่งของชื่อไฟล์หรือ URL และเรามิได้ต้องการข้อมูลเหล่านั้นมาเป็นส่วนหนึ่งของระบบของเราหรือประมวลผลข้อมูลเหล่านั้นตามวัตถุประสงค์ที่แจ้งไว้ในนโยบายความเป็นส่วนตัวนี้

ข้อมูลทั้งหมดที่ได้รับและประมวลผลผ่านระบบคำติชม ESET LiveGrid® จะถูกนำมาใช้โดยไม่มีการระบุตัวตนของผู้ใช้ปลายทาง

การประเมินความปลอดภัยของอุปกรณ์ที่เชื่อมต่อกับเครือข่าย เพื่อมอบฟังก์ชันในการประเมินความปลอดภัย เราจะประมวลผลชื่อของเครือข่ายภายในระบบและข้อมูลเกี่ยวกับอุปกรณ์ในเครือข่ายภายในระบบ เช่น การมีอยู่, ประเภท, ชื่อ, ที่อยู่ IP และที่อยู่ MAC ของอุปกรณ์ในเครือข่ายภายในระบบที่เชื่อมต่อโดยมีข้อมูลใบอนุญาต ข้อมูลดังกล่าวยังรวมถึงประเภทความปลอดภัยไร้สายและประเภทการเข้ารหัสไร้สายของอุปกรณ์เราเตอร์ด้วย ข้อมูลใบอนุญาตที่ระบุตัวตนของผู้ใช้ปลายทางจะไม่ระบุตัวตนภายใน 12 เดือนหลังจากใบอนุญาตหมดอายุ

การสนับสนุนด้านเทคนิค ข้อมูลติดต่อ ข้อมูลการอนุญาต และข้อมูลที่อยู่ในคำขอการสนับสนุนของคุณอาจจำเป็นสำหรับการให้บริการสนับสนุน โดยขึ้นอยู่กับช่องทางที่คุณเลือกในการติดต่อเรา เราอาจเก็บรวบรวมข้อมูลที่อยู่อีเมล หมายเลขโทรศัพท์ ข้อมูลใบอนุญาต รายละเอียดผลิตภัณฑ์ และคำอธิบายของกรณีการสนับสนุนของคุณ คุณอาจถูกขอให้ระบุข้อมูลอื่นๆ เพื่อให้บริการสนับสนุนรวดเร็วมากยิ่งขึ้น ข้อมูลที่ใช้ประมวลผลสำหรับการสนับสนุนด้านเทคนิคจะถูกเก็บไว้เป็นเวลา 4 ปี

การป้องกันการใช้ข้อมูลในทางที่ผิด หากมีการสร้างบัญชี ESET HOME ใน https://home.eset.com และเปิดใช้งานฟังก์ชันโดยผู้ใช้ปลายทางซึ่งเกี่ยวข้องกับการโจรกรรมคอมพิวเตอร์ จะมีการรวบรวมและประมวลผลข้อมูลดังต่อไปนี้: ข้อมูลเกี่ยวกับตำแหน่งที่ตั้ง ภาพหน้าจอ ข้อมูลเกี่ยวกับการกำหนดค่าคอมพิวเตอร์ และข้อมูลที่บันทึกโดยกล้องของคอมพิวเตอร์ ข้อมูลที่ถูกเก็บรวบรวมจะจัดเก็บไว้ในเซิร์ฟเวอร์ของเราหรือในเซิร์ฟเวอร์ของผู้ให้บริการของเราโดยมีระยะเวลาการเก็บรักษาเป็นเวลา 3 เดือน

Password Manager. หากคุณเลือกเปิดใช้งานฟังก์ชันของ Password Manager ข้อมูลที่เกี่ยวข้องกับรายละเอียดการเข้าสู่ระบบของคุณจะถูกจัดเก็บในรูปแบบที่เข้ารหัสเฉพาะในคอมพิวเตอร์ของคุณหรืออุปกรณ์ที่กำหนดเท่านั้น หากคุณเปิดใช้งานบริการซิงโครไนซ์ ข้อมูลที่เข้ารหัสจะถูกจัดเก็บในเซิร์ฟเวอร์ของเราหรือในเซิร์ฟเวอร์ของผู้ให้บริการของเราเพื่อรับประกันบริการดังกล่าว ทั้ง ESET และผู้ให้บริการจะไม่สามารถเข้าถึงข้อมูลที่เข้ารหัสได้ มีเพียงคุณเท่านั้นที่มีกุญแจในการไขรหัสข้อมูลนั้น ข้อมูลจะถูกลบออกเมื่อปิดใช้งานฟังก์ชัน

ESET LiveGuard. หากคุณเลือกเปิดใช้งานฟังก์ชัน ESET LiveGuard จะต้องส่งตัวอย่าง เช่น ไฟล์ที่กำหนดไว้ล่วงหน้าและเลือกโดยผู้ใช้ปลายทาง ตัวอย่างที่คุณเลือกสำหรับการวิเคราะห์ระยะไกลจะอัพโหลดไปยังบริการ ESET และผลการวิเคราะห์จะถูกส่งกลับไปยังคอมพิวเตอร์ของคุณ ตัวอย่างที่น่าสงสัยใดๆ จะประมวลผลในลักษณะของข้อมูลที่เก็บรวบรวมโดยระบบคำติชม ESET LiveGrid®

โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า หากคุณเลือกที่จะเปิดใช้งาน โปรแกรมการปรับปรุงประสบการณ์ใช้งานของลูกค้า เราจะเก็บรวบรวมและใช้ข้อมูลทางไกลแบบไม่ระบุตัวตนที่เกี่ยวกับการใช้งานของผลิตภัณฑ์ของเราที่อิงจากการยินยอมของคุณ

โปรดทราบว่าหากบุคคลที่ใช้ผลิตภัณฑ์และบริการของเราไม่ใช่ผู้ใช้ปลายทางที่ซื้อผลิตภัณฑ์หรือบริการและได้เข้าร่วม EULA กับเรา (เช่น พนักงานของผู้ใช้ปลายทาง สมาชิกในครอบครัว หรือบุคคลที่ได้รับอนุญาตให้ใช้ผลิตภัณฑ์หรือบริการโดยผู้ใช้ปลายทางตาม EULA การประมวลผลข้อมูลจะดำเนินการตามผลประโยชน์ที่ชอบด้วยกฎหมายของ ESET ภายใต้นิยามของมาตรา 6 (1) f) GDPR เพื่อให้ผู้ใช้ที่ได้รับอนุญาตจากผู้ใช้ปลายทางสามารถใช้ผลิตภัณฑ์และบริการที่เราจัดหาให้ได้ตาม EULA

ข้อมูลติดต่อ

หากคุณประสงค์ที่จะใช้สิทธิ์ของคุณในฐานะที่เป็นเจ้าของข้อมูล หรือหากคุณมีข้อสงสัยหรือข้อกังวล โปรดส่งข้อความมาที่:

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