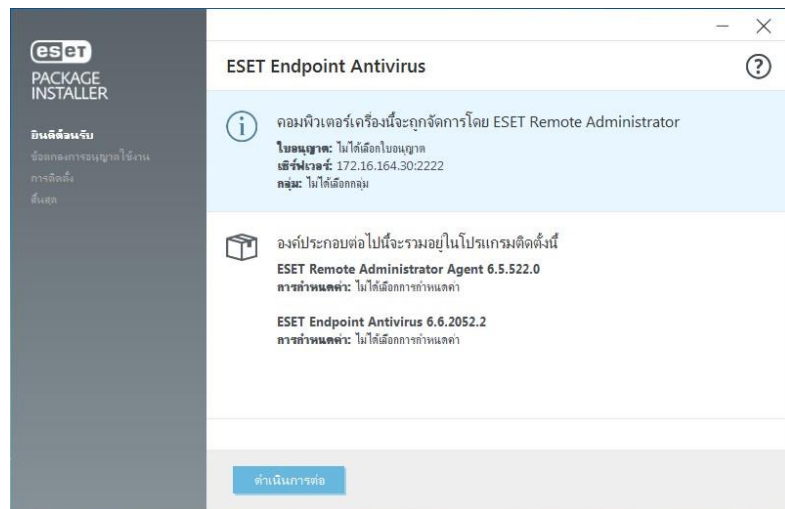
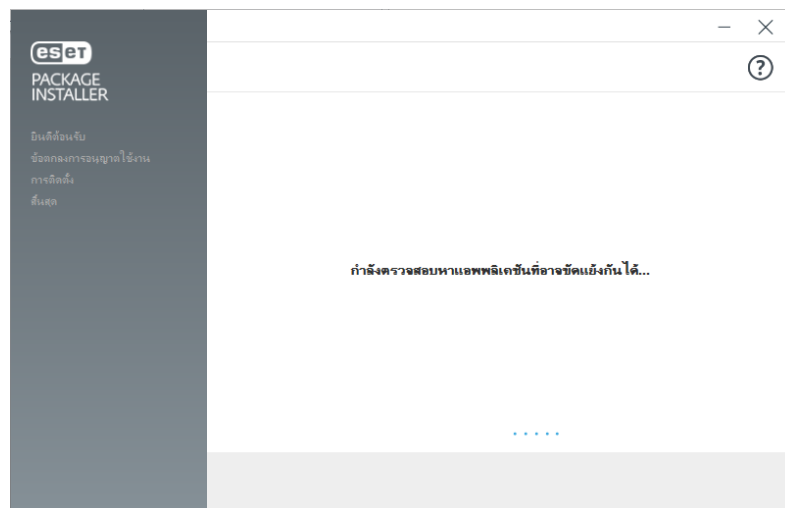


## คู่มือการติดตั้งโปรแกรม Antivirus ESET Endpoint Antivirus

1. ทำการดาวน์โหลดไฟล์ติดตั้ง ESET Endpoint Antivirus  
<http://www.rmutsv.ac.th/th/ITHelpdesk>  
[http://www.rmutsv.ac.th/antivirus/TH/EEA\\_Installer\\_x64\\_th\\_TH.exe](http://www.rmutsv.ac.th/antivirus/TH/EEA_Installer_x64_th_TH.exe)
2. Save ไฟล์ที่ดาวน์โหลดไว้บนหน้าจอ Desktop
3. Double-click ไฟล์ที่ดาวน์โหลด เพื่อเข้าสู่หน้าต่าง Setup Wizard หากมีการใช้งาน Windows User Account  
Control (UAC) คุณจะได้รับแจ้งจากกล่องโต้ตอบเพิ่มเติมระหว่างการติดตั้ง เมื่อได้รับแจ้งยืนยันว่าคุณต้องการที่จะติดตั้ง จึงจะสามารถทำการติดตั้งต่อไปได้
4. ในหน้าจอ Setup Wizard คลิกที่ **ดำเนินการต่อ**

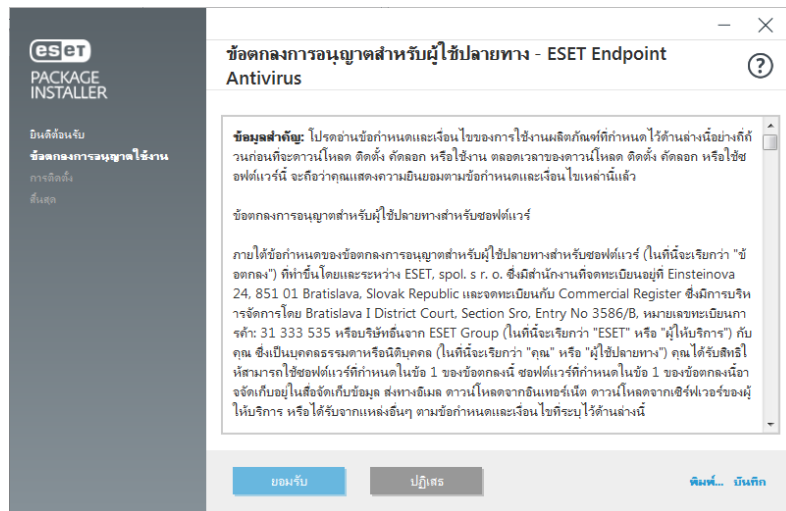


5. ขั้นตอนการค้นหาแอปพลิเคชันอื่นๆ ที่ขัดแย้งกัน เมื่อเจอแอปพลิเคชันให้ทำการลบแอปพลิเคชันที่มีการติดตั้งอยู่บน เครื่องคอมพิวเตอร์ หากค้นหาไม่เจอ หน้าจอ Setup Wizard จะข้ามขั้นตอนนี้ไป

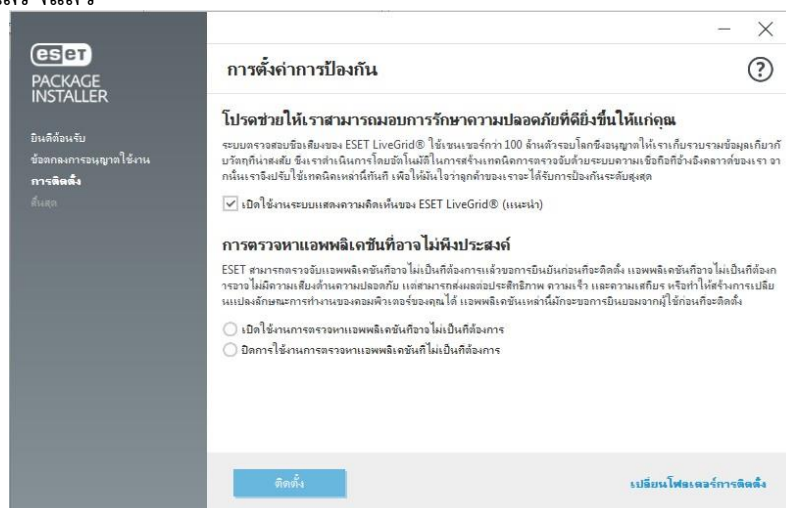


(ในขั้นตอนนี้จะค้นหาแอปพลิเคชันเจอบางเวอร์ชัน จะช่วยป้องกันความขัดแย้งทางซอฟต์แวร์และทำให้แน่ใจว่าผลิตภัณฑ์ ESET ของคุณจะทำงานอย่างถูกต้อง )

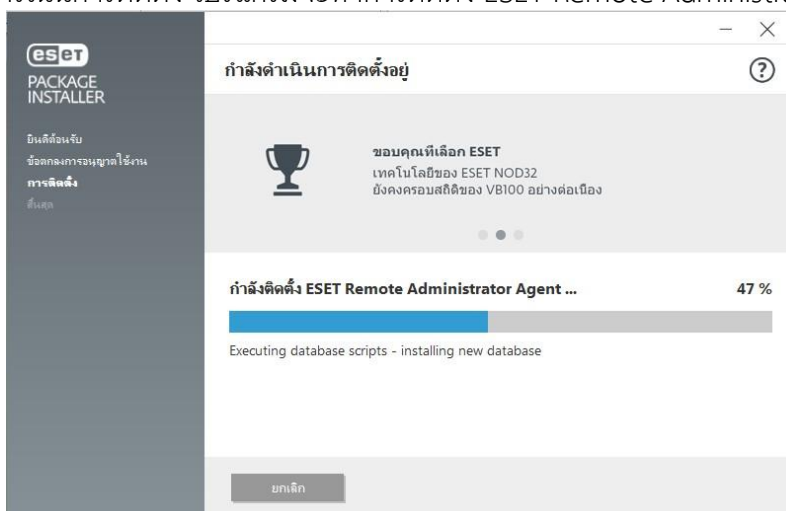
6. อ่านและรับทราบ ESET End User License Agreement กดเลือกหัวข้อ **ยอมรับ**



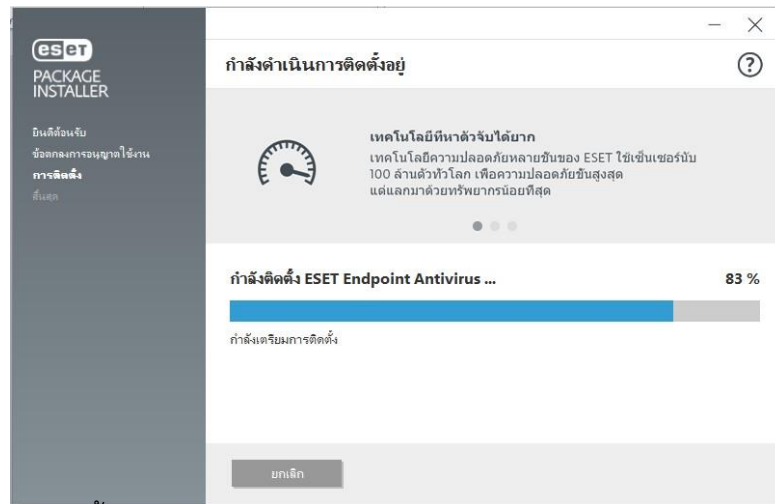
7. ในการตรวจสอบของหน้าต่างโปรแกรมที่ไม่พึงประสงค์ เลือกตัวเลือกที่ต้องการ และคลิก **ติดตั้ง** หากคุณตัดสินใจใน ภายหลังจากที่คุณต้องการที่จะเปลี่ยนการตั้งค่านี้คุณจะสามารถแก้ไขได้โดยเข้าไปตั้งค่าที่ การตั้งค่าขั้นสูง หลังจากติดตั้ง เสร็จแล้ว



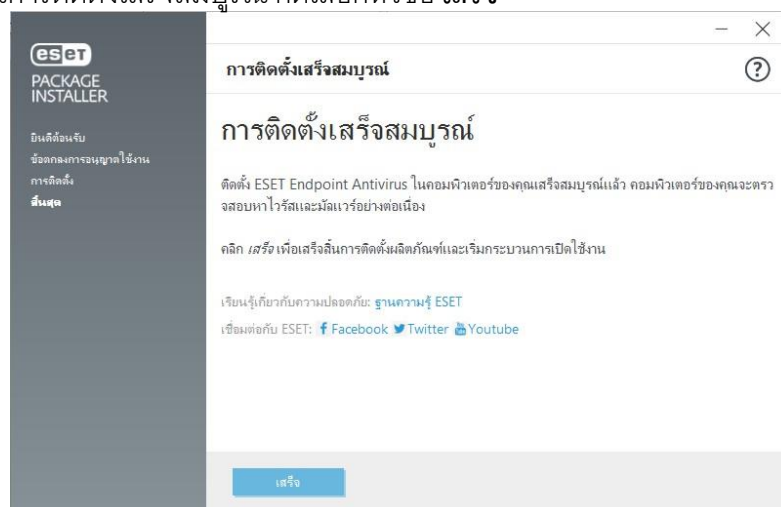
8. ขั้นตอนการเนิการติดตั้ง โปรแกรมจะทำการติดตั้ง ESET Remote Administrator Agent



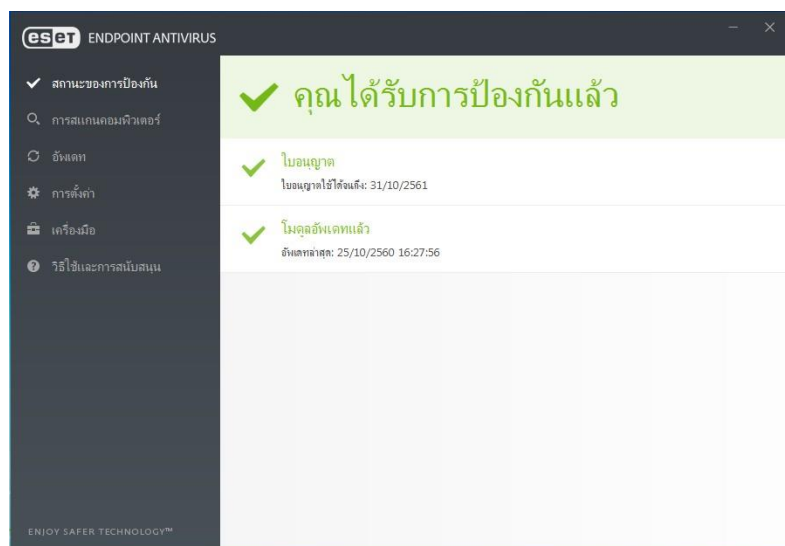
## 9. ขั้นตอนการดำเนินการติดตั้ง โปรแกรมจะทำการติดตั้ง ESET Endpoint Antivirus



## 10. ขั้นตอนการติดตั้งเสร็จสมบูรณ์ กดเลือกหัวข้อ เสร็จ



## 11. ขั้นตอนสุดท้ายในการติดตั้งโปรแกรม สถานะใบอนุญาต จะมีเครื่องหมายถูกสีเขียว

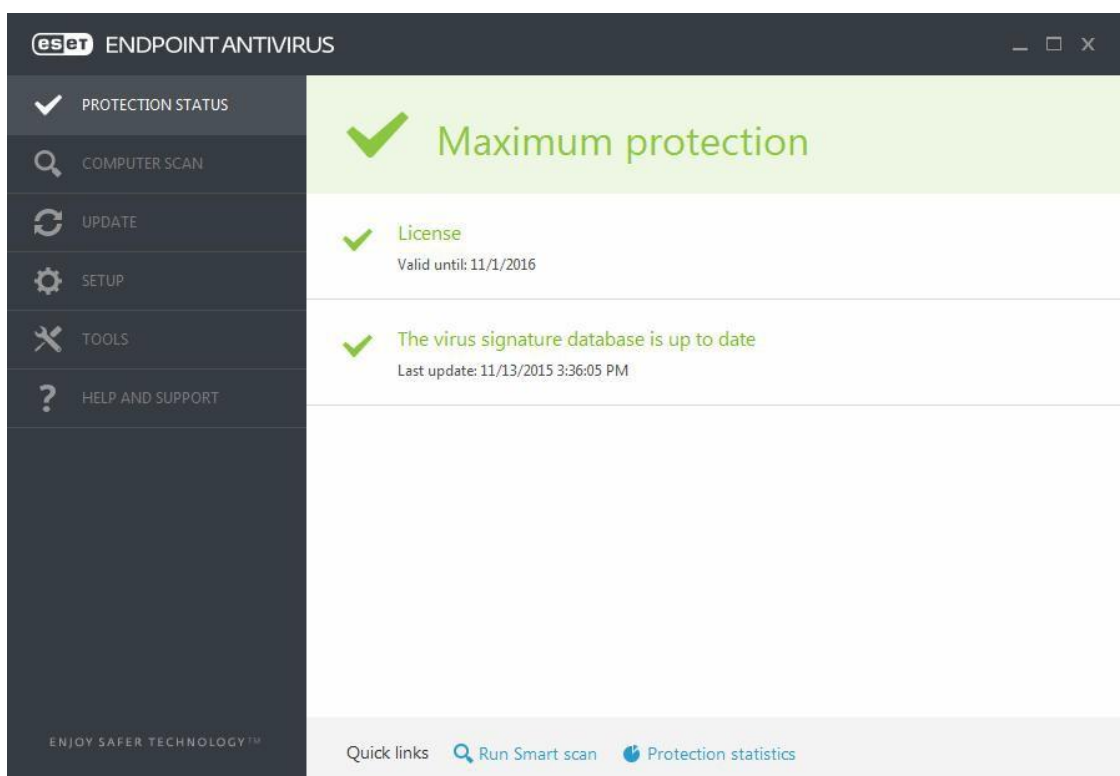


หมายเหตุ : หากไม่ได้รับใบอนุญาต ให้ติดต่อ หน่วยเทคโนโลยีสารสนเทศ

## วิธีการใช้งานโปรแกรมป้องกันไวรัส Antivirus ESET Endpoint Antivirus

### 1. คำอธิบายเมนูหน้าต่างหลักของโปรแกรม

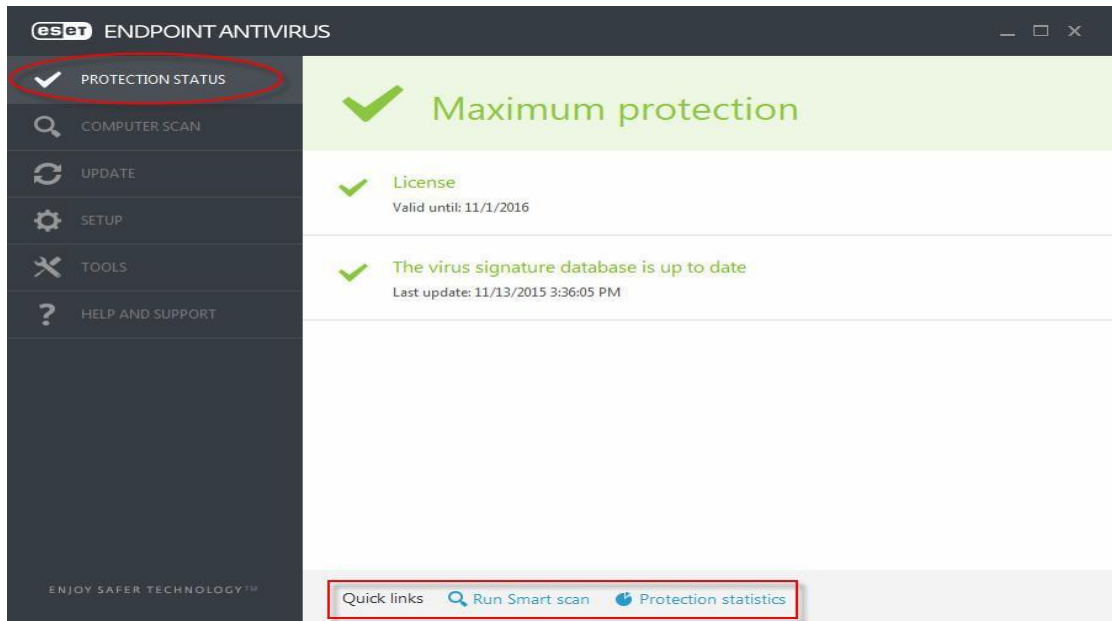
- Protection status แสดงข้อมูลเกี่ยวกับสถานะการป้องกันของ ESET Endpoint Antivirus
- Computer scan ตัวเล็อกนี้จะช่วยให้คุณสมารถกำหนดค่าและเริ่มต้นการสแกนแบบสมาร์ท การสแกนแบบกำหนดเอง หรือการสแกนสื่อที่ถอดเข้าออกได้ คุณยังสามารถทำการสแกนล่าสุดซ้ำได้
- Update แสดงข้อมูลเกี่ยวกับการอัปเดตฐานข้อมูลไวรัส
- Setup ปรับตั้งค่าการรักษาความปลอดภัยสำหรับคอมพิวเตอร์, เว็บและอีเมล
- Tools การเข้าถึงไฟล์ บันทึก, สถิติการป้องกัน, กระบวนการที่ทำงานอยู่, ติดตามการทำงาน, ตัววางกำหนดการ, กักเก็บไฟล์ไวรัส, ESET SysInspector (เครื่องมือช่วยตรวจสอบข้อมูลในเครื่อง), ESET SysRescue (สร้างซีดีกู้คืน) และการส่งไฟล์ตัวอย่างไปวิเคราะห์
- Help and support เรียกดูการเข้าถึงไฟล์วิธีใช้, ฐานความรู้ของ ESET และเว็บไซต์ของ ESET นอกจากนี้ยังมีลิงค์เพื่อเปิดคำร้องขอรับการสนับสนุนจากฝ่ายดูแลลูกค้า เครื่องมือสนับสนุนและข้อมูลเกี่ยวกับการเปิดใช้งานผลิตภัณฑ์



หน้าจอสถานะการป้องกันจะแจ้งให้คุณทราบเกี่ยวกับระดับความปลอดภัยและการป้องกันในปัจจุบันของ คอมพิวเตอร์ สถานะการป้องกันสูงสุดสีเขียว แสดงว่ามีการป้องกันสูงสุด

### 2. การทำงานของหน้าต่างหลักของโปรแกรม ESET Endpoint Antivirus

1. Protection status (สถานะการป้องกัน) เมนูนี้จะแจ้งให้ทราบเกี่ยวกับระดับการรักษาความปลอดภัยและการป้องกันในปัจจุบันของคอมพิวเตอร์, ใบอนุญาต และสถานะการอัปเดตฐานข้อมูลไวรัสหากสถานะเป็นสีเขียวแสดงว่ามีการป้องกันขั้นสูงสุดและตัวโปรแกรมทำงานปกติ นอกจากนี้หน้าต่างสถานะยังแสดงเมนูที่ใช้อยู่ในโปรแกรม ESET Endpoint Antivirus ดังภาพ



หน้าต่างสถานะยังแสดงข้อมูลเกี่ยวกับการอัปเดตล่าสุด และมีลิงก์ด่วนไปยังคุณลักษณะที่ใช้อยู่ใน ESET Endpoint Antivirus

## 2. Computer scan (การสแกนคอมพิวเตอร์)

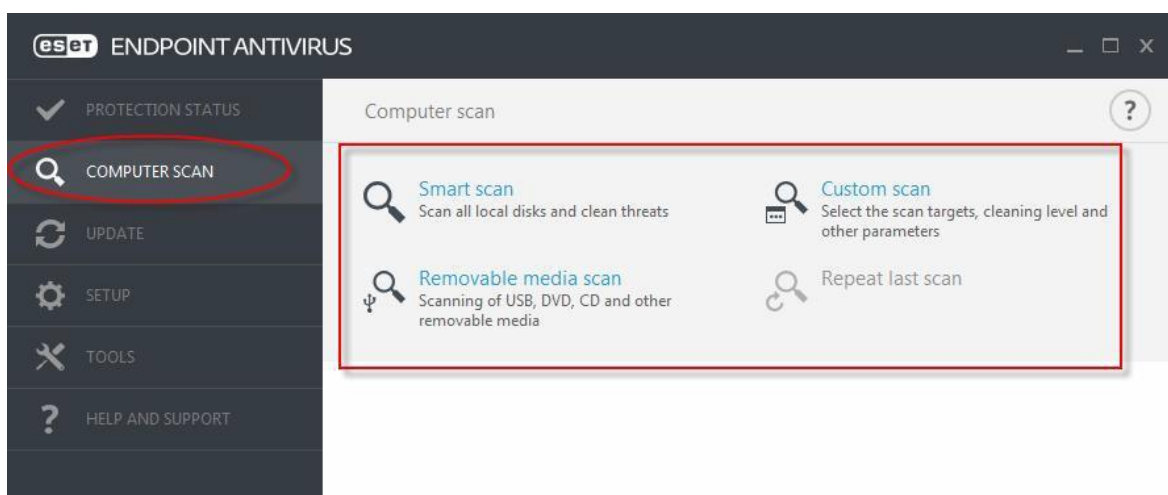
หลังจากการติดตั้งเสร็จสมบูรณ์แล้ว ESET Endpoint Antivirus จะดำเนินการสแกนคอมพิวเตอร์โดยอัตโนมัติเพื่อตรวจหาภัยคุกคาม นอกจากนี้ผู้ใช้งานยังสามารถสั่งสแกนคอมพิวเตอร์ได้ด้วยตัวเอง โดยสามารถเลือกการสแกนจาก 4 ตัวเลือกลงนี้

- **Smart scan** การสแกนแบบสมาร์ทจะช่วยให้คุณเริ่มต้นการสแกนคอมพิวเตอร์และกำจัดไฟล์ที่ติดไวรัสได้อย่างรวดเร็ว โดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ข้อดีของการสแกนแบบสมาร์ท คือ ใช้งานง่าย และไม่ต้องมีการกำหนดค่าการสแกนโดยละเอียด การสแกนแบบสมาร์ทจะตรวจสอบทุกไฟล์ในไดรฟ์ในระบบรวมทั้งกำจัดหรือลบการแฝงตัวที่ตรวจพบโดยอัตโนมัติ

- **Custom scan** การสแกนที่กำหนดเองเป็นโซลูชันที่เหมาะสม หากคุณต้องการระบุพารามิเตอร์การสแกน เช่น เป้าหมายการสแกน และวิธีการสแกน ข้อดีของการสแกนที่กำหนดเอง คือ คุณสามารถกำหนดพารามิเตอร์ในรายละเอียดได้ คุณสามารถบันทึกการกำหนดค่าไว้ไปยังโปรไฟล์การสแกนที่ผู้ใช้กำหนดซึ่งเป็นประโยชน์ถ้ามีการสแกนซ้ำโดยใช้พารามิเตอร์เดียวกัน (เป็นการสแกนโดยเลือกไดรฟ์, ไฟล์ หรืออุปกรณ์)

- **Removable media scan** การสแกนสื่อที่ถอดเข้าออกได้ เช่น ซีดี/ดีวีดี/USB เมื่อมีการเชื่อมต่อ อุปกรณ์ USB กับคอมพิวเตอร์ คุณสามารถสั่งสแกนได้ทันที

- **Repeat last scan** ทำการสแกนครั้งล่าสุดซ้ำอีกครั้ง



### 3. Update (การอัปเดต)

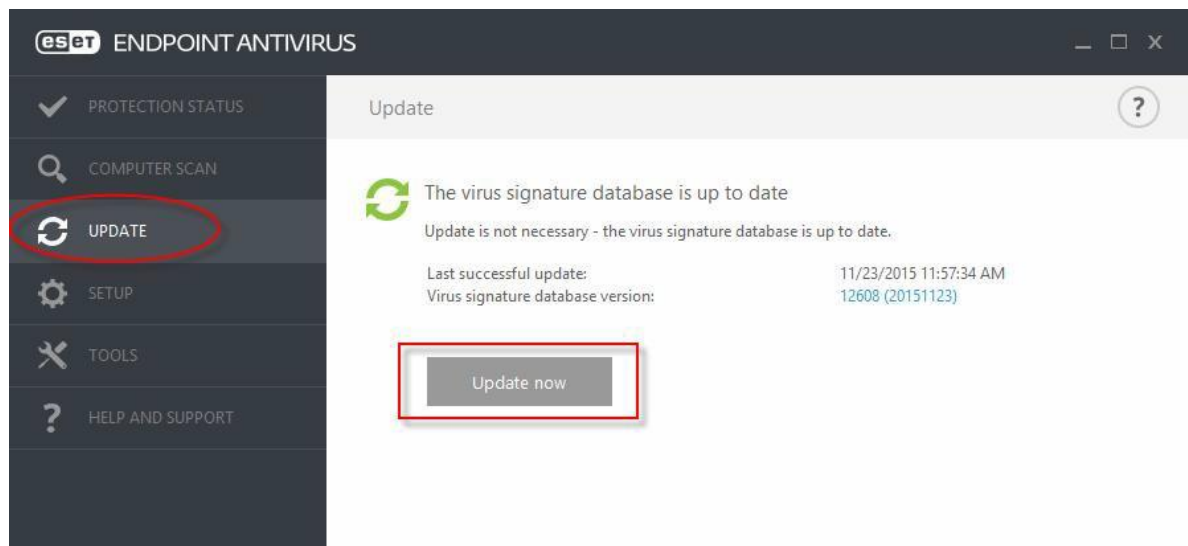
การอัปเดตเป็นประจำ เป็นวิธีการที่ดีที่สุดเพื่อให้คอมพิวเตอร์ มีระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัปเดตจะทำให้มั่นใจว่าโปรแกรม ESET Endpoint Antivirus มีความทันสมัยอยู่เสมอโดยใช้ 2 วิธี คือ

- การอัปเดตฐานข้อมูลไวรัส
- การอัปเดตองค์ประกอบของโปรแกรม

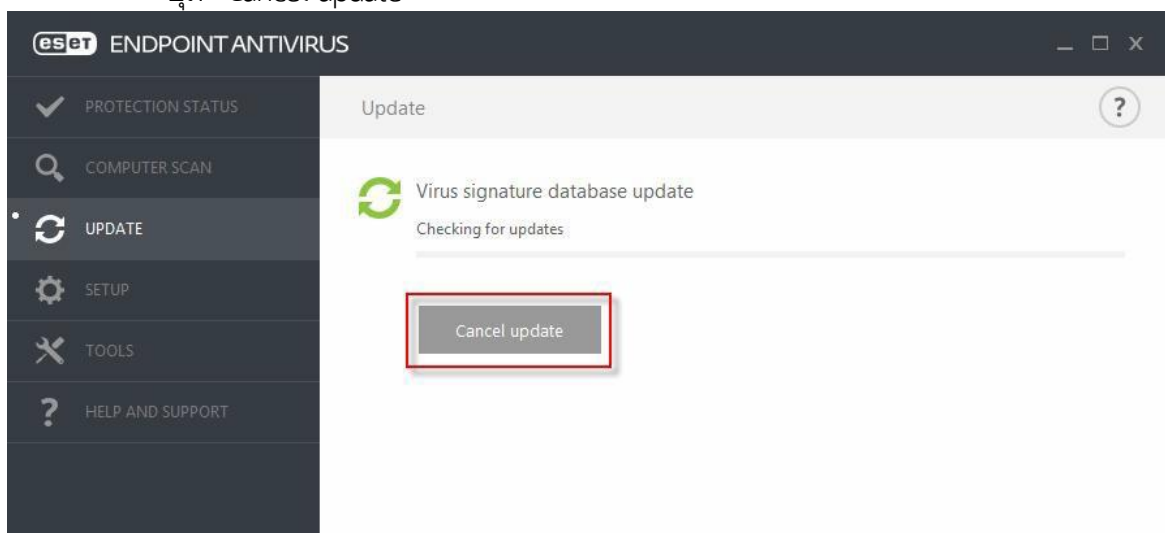
เมื่อคลิกเมนู Update ในหน้าต่างโปรแกรมหลัก จะพบสถานะการอัปเดตในปัจจุบัน รวมถึงวันที่และเวลาของการอัปเดตที่สำเร็จครั้งล่าสุด และแสดงว่าจะต้องมีการอัปเดตหรือไม่หน้าต่างหลักจะมีเวอร์ชันของ ฐานข้อมูลไวรัส เมื่อคลิกตัวเลขนี้จะลิงค์ไปยังเว็บไซต์ของ ESET ซึ่งจะแสดงฐานข้อมูลทั้งหมดที่เพิ่มขึ้นมา

- Last successful update – วันที่และเวลาล่าสุดที่อัปเดตฐานข้อมูล
- Version signature database version – หมายเลขฐานข้อมูลไวรัสที่อัปเดตไว้ล่าสุด ซึ่งเมื่อคลิกจะลิงค์ไปยังเว็บไซต์ของ ESET เพื่อดูรายการของฐานข้อมูลที่เพิ่มขึ้นมา

a. คลิกปุ่ม “Update now” เพื่อตรวจสอบการอัปเดตฐานข้อมูลไวรัสล่าสุด



b. กระบวนการอัปเดต หลังจากคลิก “Update now” กระบวนการดาวน์โหลดจะเริ่มต้น ทำงานจะแสดงแถบความคืบหน้าการดาวน์โหลด หากต้องการยกเลิกการอัปเดตให้คลิกปุ่ม “Cancel update”



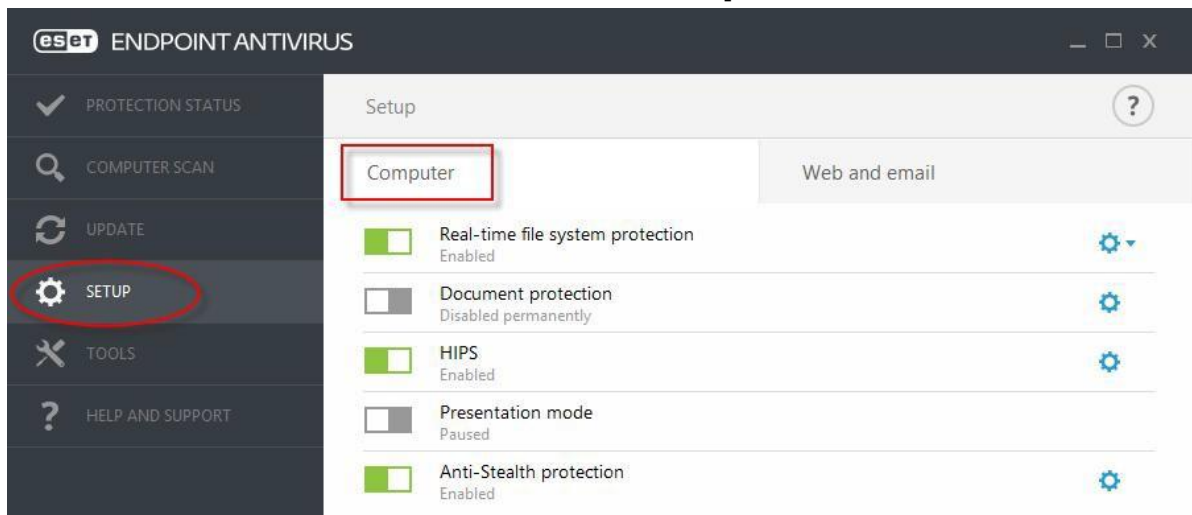
4. Setup (การตั้งค่า) เมนู Setup ประกอบด้วยส่วนต่อไปนี้ :

- **Computer**

- Web and email

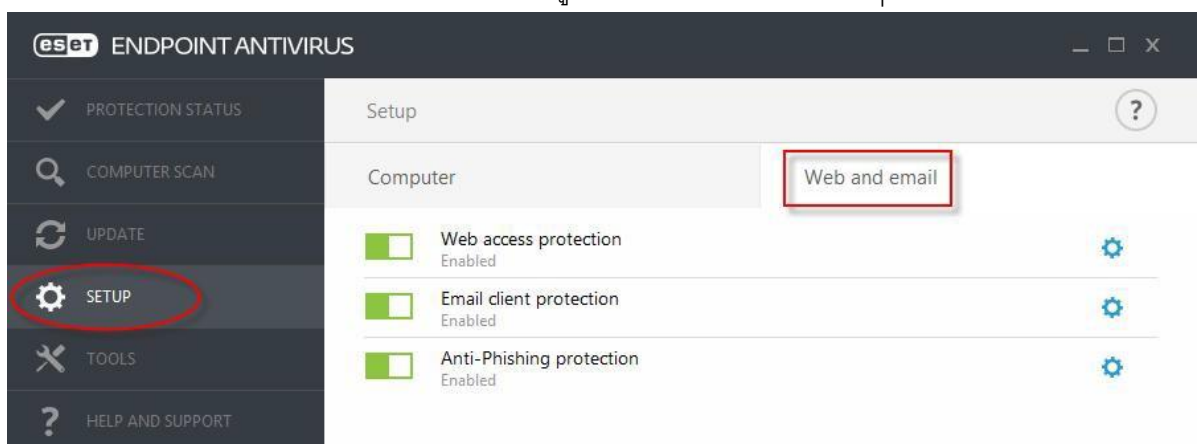
การตั้งค่าการป้องกัน Computer : จะช่วยให้คุณสามารถเปิดหรือปิดการใช้งานองค์ประกอบต่อไปนี้ :

- Real-time file system protection – การป้องกันระบบไฟล์แบบเรียลไทม์
- Document protection – การป้องกันเอกสาร Microsoft Office จะสแกนเอกสารก่อนที่จะเปิด รวมถึงไฟล์ที่ดาวน์โหลดจาก Internet Explorer โดยอัตโนมัติ เช่น องค์ประกอบ ActiveX
- HIPS – จะตรวจสอบเหตุการณ์ที่เกิดขึ้นภายในระบบปฏิบัติการและตอบสนองเหตุการณ์ตามกฎหมายที่กำหนดเอง
- Presentation mode – โหมดการนำเสนอ ช่วยให้คุณใช้ซอฟต์แวร์อย่างต่อเนื่อง ไม่ต้องการให้หน้าต่างป๊อปอัพมารบกวน และต้องการลดการใช้งาน CPU
- Anti-Stealth protection – ระบบป้องกันไวรัสประเภททูลคิทส์



การตั้งค่าการป้องกัน Web and email จะช่วยให้คุณเปิดหรือปิดใช้งานองค์ประกอบต่อไปนี้ :

- Web access protection – ระบบจะสแกนการรับส่งข้อมูลทั้งหมดผ่าน HTTP หรือ HTTPS
- Email client protection – การควบคุมการสื่อสารทางอีเมลที่ได้รับผ่านโปรโตคอล POP3 และ IMAP
- Anti-Phishing protection – การป้องกันฟิชชิ่ง จะป้องกันคุณจากความพยายามรับรหัสผ่าน ข้อมูลธนาคาร และข้อมูลที่มีความละเอียดอ่อนอื่นๆ

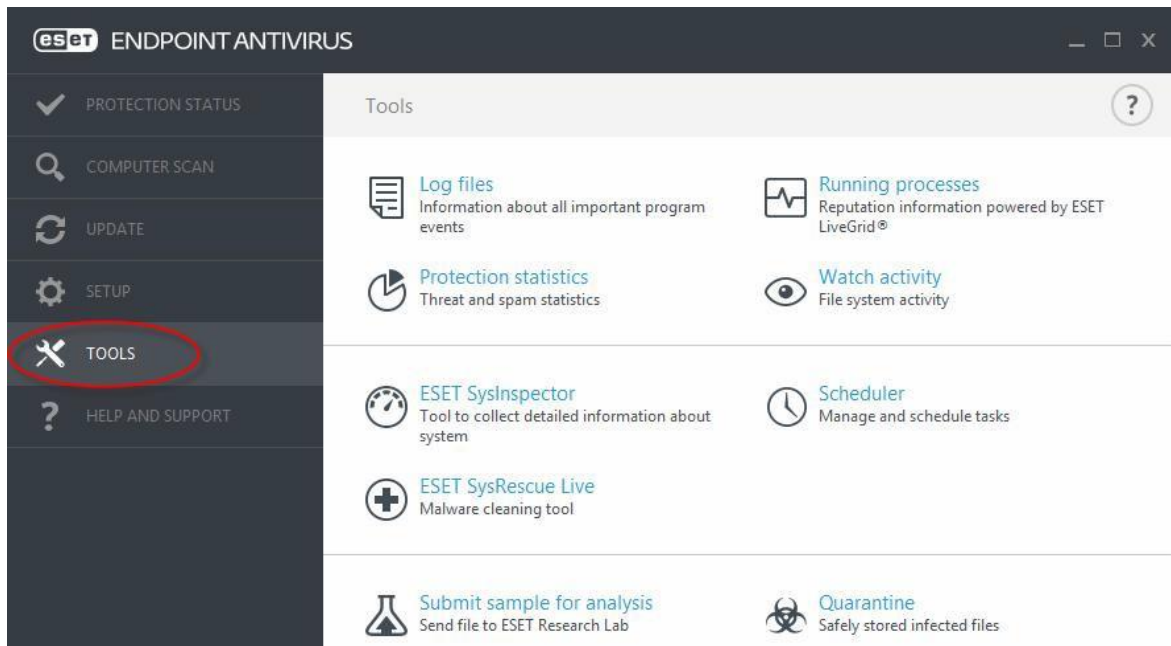


เมื่อต้องการปิดการใช้งานแต่ละโมดูลเป็นเวลาชั่วคราวให้คลิก  สวิตช์สีเขียว  
เมื่อต้องการเปิดใช้งานของโมดูลที่ถูกปิดไว้ให้คลิก  สวิตช์สีแดง



### 3. Tools (เครื่องมือ)

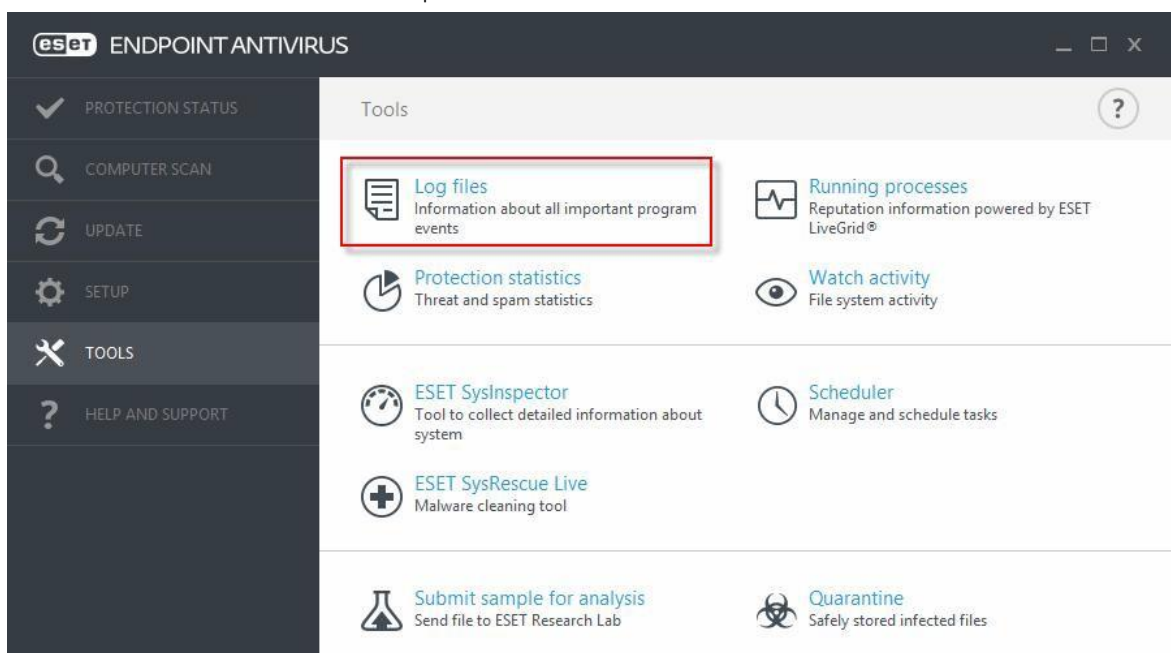
เมนูเครื่องมือ ประกอบด้วยโมดูลที่ช่วยให้การจัดการโปรแกรมง่ายขึ้นและมีตัวเลือกเพิ่มเติมสำหรับ ผู้ใช้ขั้นสูง เมนูนี้จะมีเครื่องมือต่อไปนี้



#### 1) Log files

ไฟล์บันทึกประกอบด้วยข้อมูลเกี่ยวกับเหตุการณ์ของโปรแกรมที่สำคัญที่เกิดขึ้นทั้งหมด และให้ภาพรวมของภัยคุกคามที่พบ Log files เป็นเครื่องมือที่จำเป็นในการวิเคราะห์ระบบ การตรวจหาภัยคุกคาม และการแก้ไขปัญหา การบันทึกนั้นดำเนินการในพื้นที่หลังโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ

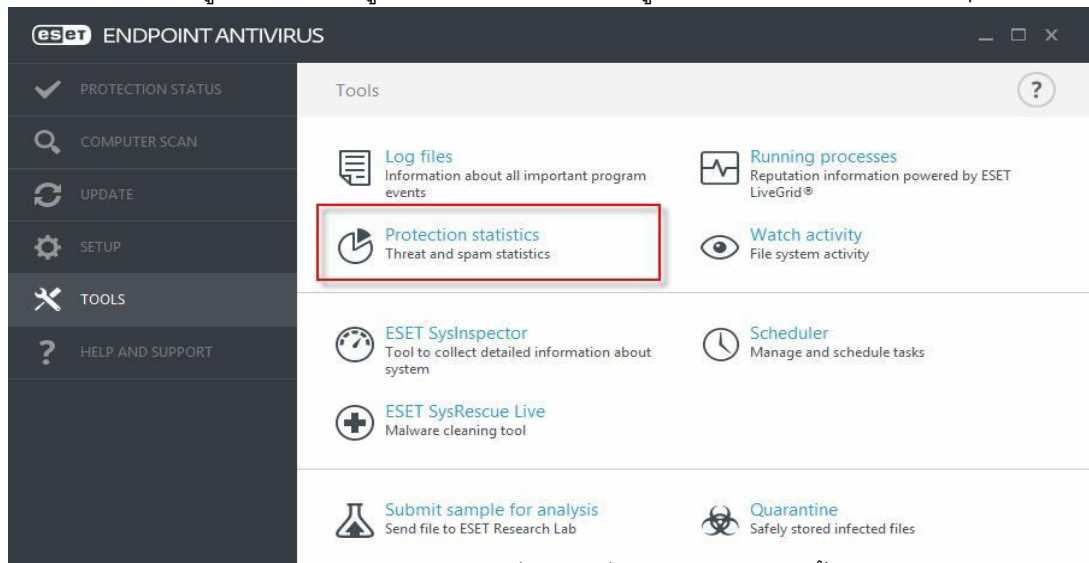
ข้อมูลจะถูกบันทึกตามการตั้งค่าความละเอียดของการบันทึกปัจจุบัน คุณสามารถดูข้อความและบันทึกได้โดยตรงจากระบบ ESET Endpoint Antivirus





## 2) Protection statistics

เมื่อต้องการดูกราฟของข้อมูลสถิติที่เกี่ยวข้องกับโมดูลการป้องกันของ ESET Endpoint Antivirus

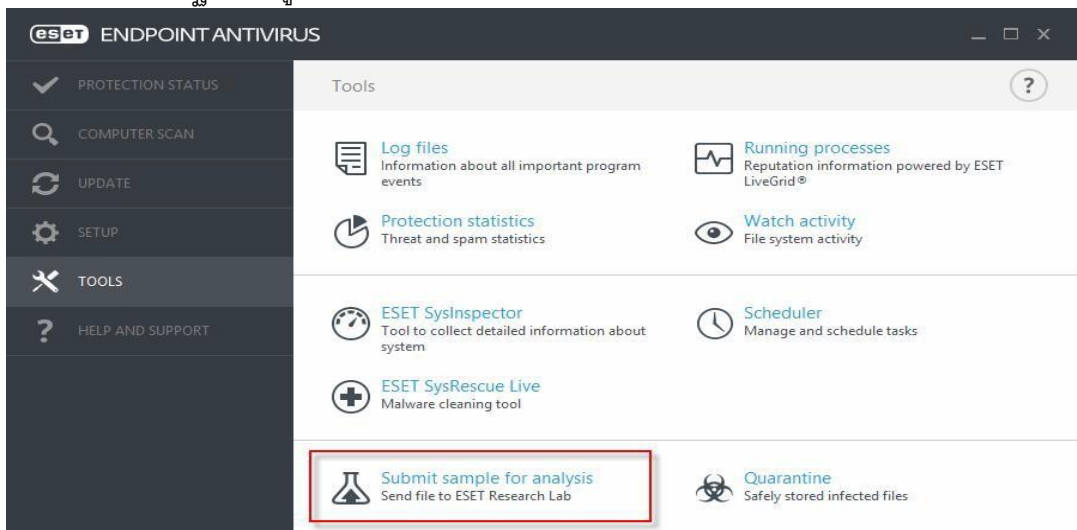


สามารถเลือกดูกราฟสถิติการป้องกัน โดยเมนูแบบเลื่อนลง ซึ่งจะมีให้เลือก ดังนี้

- Antivirus and antispymware protection - แสดงจำนวนวัตถุที่ติดไวรัสและถูกกำจัด
- File system protection - แสดงเฉพาะวัตถุที่มีการอ่านและเขียนไปยังระบบไฟล์เท่านั้น
- Email client protection - แสดงเฉพาะวัตถุที่รับหรือส่งด้วยอีเมลไคลเอ็นต์เท่านั้น
- Web access and Anti-Phishing protection - แสดงเฉพาะวัตถุที่ดาวน์โหลดโดยเว็บเบราว์เซอร์เท่านั้น

## 3) Submit sample for analysis

การส่งตัวอย่างเพื่อวิเคราะห์ หากคุณพบไฟล์ที่มีลักษณะน่าสงสัยในคอมพิวเตอร์ของคุณหรือเว็บไซต์ที่น่าสงสัยในอินเทอร์เน็ต คุณสามารถส่งไปยังห้องปฏิบัติการของไวรัสของ ESET เพื่อรับการวิเคราะห์ได้ และหากได้รับการตรวจสอบแล้วว่าตัวอย่างไฟล์ที่ส่งมาเป็นอันตราย การตรวจพบไฟล์นี้จะถูกเพิ่มในการอัปเดตฐานข้อมูลไวรัสครั้งต่อไป

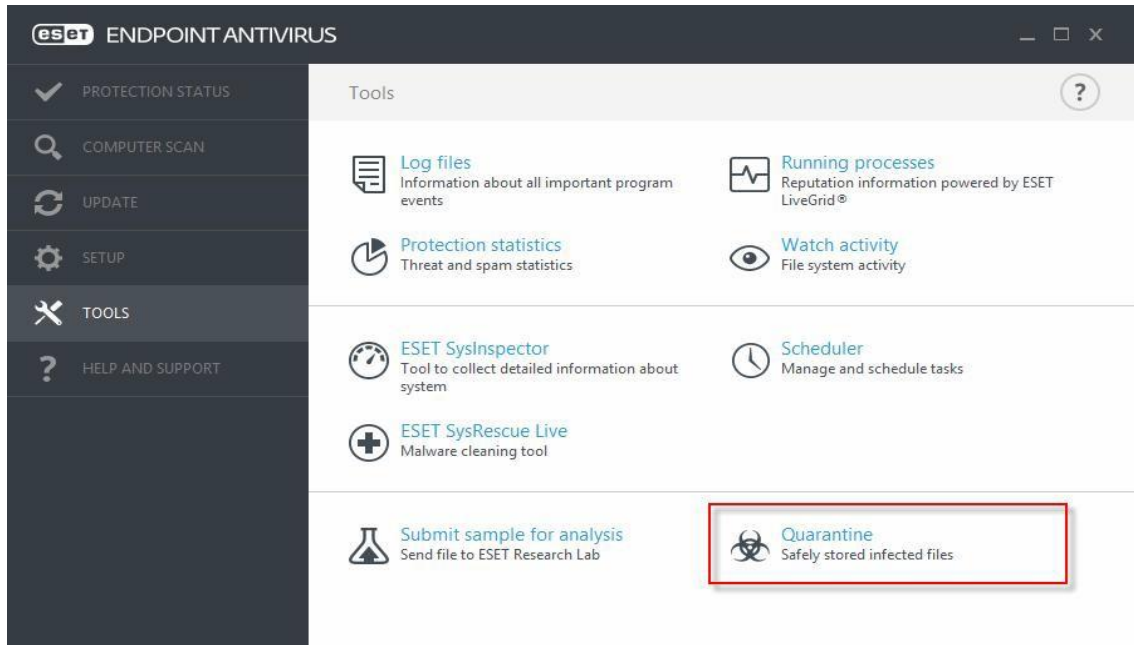


เลือกเหตุผลสำหรับการส่งตัวอย่าง โดยใช้เมนูแบบเลื่อนลง

- Suspicious file ไฟล์ที่น่าสงสัย
- Suspicious site เว็บไซต์ที่น่าสงสัย
- False positive file การตรวจพบไฟล์ที่ผิดพลาด (ไฟล์ที่ตรวจพบว่ามีไวรัส แต่จริงๆ แล้วไม่ใช่)
- False positive site การตรวจจับเว็บไซต์ที่ไม่เป็นอันตราย
- Other (อื่นๆ)

#### 4) Quarantine

หน้าที่หลักของ Quarantine ก็คือ การเก็บไฟล์ที่ติดไวรัสไว้ในที่ปลอดภัย ไฟล์ควรมีการกักเก็บถ้า ไม่สามารถล้างไวรัสได้ แต่ไม่ต้องการลบไฟล์เหล่านี้ หรือถ้าการตรวจพบด้วยความผิดพลาดโดย ESET Endpoint Antivirus ผู้ใช้สามารถเลือกที่จะกักเก็บไฟล์ ซึ่งไฟล์ที่ถูกกักเก็บจะสามารถส่งไปวิเคราะห์ที่ ห้องปฏิบัติการไวรัสของ ESET ได้



ไฟล์ที่เก็บไว้ในโฟลเดอร์กักเก็บนั้นสามารถดูได้ในตารางที่แสดงวันที่และเวลาของการกักเก็บ ตำแหน่งไฟล์ที่ ติดไวรัส ขนาดไฟล์ สาเหตุ (ตัวอย่างเช่น วัตถุที่เพิ่มโดยผู้ใช้...) และ จำนวนภัยคุกคาม

