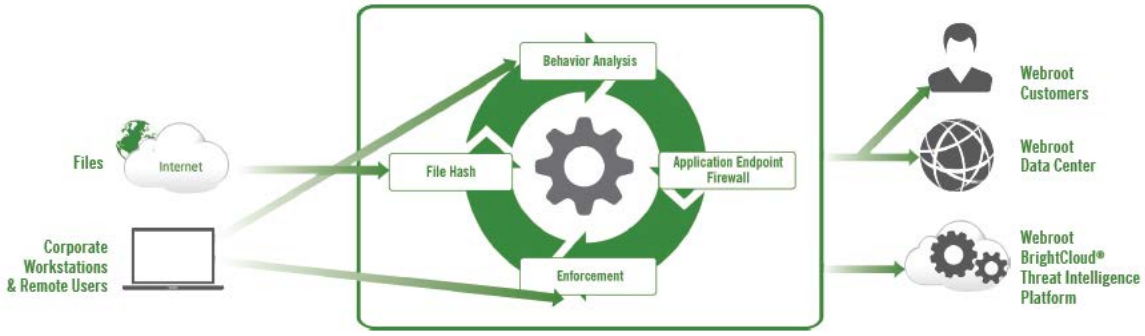
Webroot SecurityAnywhere Business Endpoint Protection (Cloud-based AntiVirus Solution)

1 Device / 1 Year



Webroot SecurityAnywhere Business Endpoint Protection โปรแกรมสแกนและป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ เครื่องเซิร์ฟเวอร์ที่รันระบบ Windows และเครื่องเซิร์ฟเวอร์แบบ เวอร์ชวลไลเซชั่น (Virtualization) เป็นระบบป้องกันภัยคุกคามในรูปแบบ Cloud-based รูปแบบใหม่ ซึ่งถือเป็นหัวใจสำคัญของระบบ Endpoint Protection ที่จะให้คุณสามารถ ปกป้องเครื่องของคุณได้อย่างดีเยี่ยมจากภัยคุกคามที่หลากหลาย อาทิ ไวรัส (Virus) มัลแวร์ (Malware) โทรจัน (Trojan) การล่อลวง (Phishing) มัลแวร์เรียกค่าไถ่ (Ransomware) สปายแวร์ (Spyware) การโจมตีผ่านเว็บเบราว์เซอร์ (Browser-based Attacks) มัลแวร์ขุดบิตคอยน์ (Cryptojacking) ด้วยการทำงานแบบ **Cloud based 100%** จึงทำให้การทำงานของ Webroot เบาและเร็ว แตกต่างจาก Antivirus แบบอื่น ที่เป็น Signature Based

นอกจากนี้ เมื่อ Webroot พบไฟล์หรือโพรเซสใหม่ที่ยังไม่สามารถชี้ชัดได้ว่าเป็นภัยคุกคาม Agent ที่ติดตั้งบนอุปกรณ์จะติดตาม และบันทึกการทำงานอย่างใกล้ชิดเพื่อคอยตรวจสอบสิ่งผิดปกติ ถ้าพบว่าไฟล์หรือโพรเซสดังกล่าวมีพฤติกรรมเป็นมัลแวร์ Agent ก็จะกำจัดมัลแวร์ทิ้งและย้อนการเปลี่ยนแปลงของระบบที่เกี่ยวข้องให้กลับไปอยู่ในสถานะก่อนที่จะติดมัลแวร์

คุณสมบัติ และ ความสามารถ (Features)

ติดตั้งง่ายและเร็ว

โปรแกรมแอนตี้ไวรัสที่ทรงพลัง และใช้เวลาเพียง 30 วินาทีในการติดตั้งโปรแกรม Agent ของ Webroot ลงในเครื่อง และสามารถทำงานร่วมกับโปรแกรมแอนตี้ไวรัสตัวอื่นๆ ที่มีติดตั้งอยู่ในเครื่องได้อย่างราบรื่น ทำให้มีความคล่องตัวทั้งในการทดลองใช้งาน การติดตั้งใหม่ หรือแม้แต่การติดตั้งทดแทนโปรแกรมแอนตี้ไวรัสตัวเดิม ได้อย่างรวดเร็วและง่ายดาย ทำให้ไม่ต้องกังวลว่าการติดตั้งโปรแกรมแอนตี้ไวรัสตัวใหม่จะส่งผลกระทบกับการทำงานของพนักงาน

จัดการเรื่องความปลอดภัยได้จากส่วนกลางผ่าน Management Console

จัดการความปลอดภัยให้กับคอมพิวเตอร์ และเซิร์ฟเวอร์ทุกเครื่องในองค์กรด้วยการควบคุมจากส่วนกลางผ่าน Management Console ที่เปิดโอกาสให้ผู้ดูแลระบบสามารถตรวจสอบสถานะ และควบคุมอุปกรณ์ใดๆ ก็ตามที่มีโปรแกรม Agent ติดตั้งอยู่ ผู้ดูแลระบบยังสามารถจัดการเรื่องความปลอดภัยให้กับอุปกรณ์ที่ติดตั้งอยู่ในสาขาต่างๆ ของธุรกิจได้ด้วย สามารถกำหนดสิทธิ์การเข้าถึงที่แตกต่างกันให้กับผู้ดูแลระบบแต่ละคนได้

การปกป้องที่ทำงานอัตโนมัติสมบูรณ์แบบ

Webroot SecurityAnywhere Business Endpoint Protection ได้ถูกออกแบบมาให้ง่ายทั้งการติดตั้ง การจัดการ และการดูแลรักษา และมีการปรับตั้งนโยบายด้านความปลอดภัยให้เลือกใช้ หรือจะกำหนดนโยบายด้านความปลอดภัยในแบบเฉพาะสำหรับธุรกิจของเราเองก็ได้ และไม่ต้องยุ่งยากกับการอัปเดตฐานข้อมูลไวรัส และการปกป้องทั้งหมดเกิดในแบบเรียลไทม์ ด้วยการทำงานบนระบบคลาวด์สมบูรณ์แบบ โดยที่ผู้ดูแลระบบสามารถจัดการเรื่องการอัปเดตโปรแกรม Agent ที่ติดตั้งอยู่ในอุปกรณ์คอมพิวเตอร์ขององค์กรได้โดยใช้เวลาเพียง 5 วินาที และมีการแจ้งเตือนเรื่องความปลอดภัย รวมถึงมีการแสดงรายงานสรุปด้านความปลอดภัยให้กับผู้ดูแลระบบอย่างเหมาะสม

เทคโนโลยีในการรับมือกับภัยคุกคามที่เหนือกว่า

Webroot ใช้เทคโลยีที่เหมาะสมในการเฝ้าระวัง และรับมือกับภัยคุกคามที่อาจเกิดขึ้นได้ แม้ในขณะที่คอมพิวเตอร์ หรืออุปกรณ์นั้นๆ อยู่ในสภาวะ Offline และมีการลดระดับการตรวจจับภัยคุกคามที่ผิดพลาด (False Detections) ให้เหลือในระดับต่ำที่สุด และแทนที่จะใช้การแบ็คอัปข้อมูลสำคัญด้วยการทำสำเนาไฟล์แบบดั่งเดิม ที่เสี่ยงต่อการโจมตีของมัลแวร์ แต่ Webroot นั้นจะใช้เทคโนโลยีที่เป็นเอกสิทธิ์เฉพาะ ที่ช่วยป้องกันการเปลี่ยนแปลงที่เกิดกับไฟล์ข้อมูลสำคัญ หรือไฟล์ของระบบ ทำให้ไฟล์ข้อมูลในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ได้รับการปกป้อง นั้นสามารถเรียกคืนสู่สภาวะปลอดภัย ได้โดยที่ไม่ต้องใช้วิธีการเรียกคืนในแบบดั่งเดิม

โปรแกรมแอนตี้ไวรัสที่ทำงานในเบื้องหลัง และไม่หน่วงเครื่อง

จุดเด่นของระบบรักษาความปลอดภัยที่ทำงานบนคลาวด์คือ กระบวนการประมวลผลอันหนักหน่วงที่เกี่ยวกับการค้นพบ และตรวจจับภัยคุกคามด้วยระบบปัญญาประดิษฐ์ นั้นทำงานบนระบบคลาวด์สมบูรณ์แบบไม่ได้เกิดขึ้นในเครื่องคอมพิวเตอร์ หรือเซิร์ฟเวอร์ของเรา นั้นหมายความว่าการสแกนเครื่องตามวงรอบการทำงาน การอัปเดตโปรแกรม Agent รวมถึงการใช้ CPU หรือหน่วยความจำ RAM ในเครื่องนั้นจะเกิดขึ้นในระดับที่ต่ำมากๆ ทำให้ไม่หน่วงเครื่อง ในขณะเดียวกัน ผู้ใช้งานเครื่องคอมพิวเตอร์ ยังได้รับการแจ้งเตือนอย่างเหมาะสมเมื่อจะเข้าถึงเว็บไซต์ที่มีภัยคุกคามแฝงอยู่

เทคโนโลยีการปกป้องที่ก้าวหน้า

ในขณะที่โปรแกรมแอนตี้ไวรัสทั่วไป มักจะมีโอกาสแค่เพียงครั้งเดียวในการตรวจจับและยับยั้งการโจมตีของภัยคุกคาม แต่ Webroot มีกระบวนการทำงานในหลายขั้นตอน โดยในขั้นแรก มันจะป้องกันไม่ให้ภัยคุกคามเล็ดลอดเข้ามาในระบบ แต่ถ้าเล็ดลอดเข้ามาได้ Webroot ก็สามารถยับยั้งมันได้ก่อนที่จะสร้างความเสียหาย และหากในกรณีที่ภัยคุกคามนั้นสามารถสร้างความเสียหายได้ (ซึ่งอาจจะเป็นภัยคุกคามตัวใหม่ที่ยังไม่เป็นที่รู้จักมาก่อน) Webroot จะทำการตรวจสอบว่ามันได้สร้างความเสียหายกับไฟล์ไหนบ้าง และจัดการซ่อมแซมความเสียหาย โดยที่ระบบจะทำความรู้จักกับภัยคุกคามตัวใหม่ เพื่อที่จะหาวิธีจัดการอย่างเหมาะสมต่อไป

ได้รับการยอมรับจากบริษัทชั้นนำด้านการรักษาความปลอดภัยบนระบบเครือข่าย

เบื้องหลังการปกป้องระดับสูงคือฐานข้อมูลด้านความปลอดภัย ที่ทำงานร่วมกับบริการ Bright Cloud ซึ่งเป็นระบบป้องกันภัยคุกคามที่ได้รับการยอมรับโดยบริษัทผู้ให้บริการด้านความปลอดภัยบนระบบเครือข่ายเกินกว่า 85 ราย โดยที่ทาง Webroot ได้ใช้ระบบสมองกลปัญญาประดิษฐ์ (AI) ในการจัดแบ่งประเภทของภัยคุกคามมาตั้งแต่ปี 2007

คุณสมบัติอื่นๆ ที่น่าสนใจของ Webroot SecurityAnywhere Business Endpoint Protection

1. มีดาต้าเซ็นเตอร์กระจายทั่วโลก เพื่อให้การปกป้องบนระบบคลาวด์อย่างเต็มประสิทธิภาพ
2. ไม่เพียงแค่ปกป้องการโจมตีที่มีเป้าหมายชัดเจน แต่ยังปกป้องการโจมตีให้กับผู้ที่ใช้งานเครื่องคอมพิวเตอร์อย่างไม่ระมัดระวังเรื่องความปลอดภัยด้วย
3. ตรวจจับ และป้องก้นระบบจาก ไวรัส มัลแวร์ โทรจัน การล่อลวง มัลแวร์เรียกค่าไถ่ สปายแวร์ การโจมตีผ่านเว็บเบราว์เซอร์ มัลแวร์ขุดบิตคอยน์ มัลแวร์ดักจับข้อมูล รวมถึงภัยคุกคามทั้งหลายทั้งปวง
4. กาารป้องกันภัยแบบหลายระดับชั้น ซึ่งมีทั้งระบบป้องกันภัยแบบตรวจดูพฤติกรรม ทำให้สามารถตรวจจับภัยคุกคามตัวใหม่ที่ยังไม่เป็นที่รู้จัก (Zero-day Threats) ภัยคุกคามบนโลกออนไลน์ รวมถึงการล่อลวง และสามารถทำงานได้แบบ Offline
5. ฟีเจอร์รักษาความเป็นส่วนตัวของข้อมูลที่มีอยู่ใน Webroot ได้รับการยอมรับจากอุตสาหกรรมธนาคารในการป้องกันการทำธุรกรรมออนไลน์ รวมถึงป้องกันภัยจากการปลอมแปลงเว็บไซต์ มัลแวร์ดักจับข้อมูล (Keyloggers) มัลแวร์แคปเจอร์หน้าจอ (Screen Grabbing) มัลแวร์ขโมยข้อมูลในคลิปบอร์ด (Clipboard Grabbing) รวมถึงการแอบลักลอบใช้โปรแกรมเบราว์เซอร์โดยมัลแวร์ (Browser Hijacking)
6. ผู้ดูแลระบบสามารถสร้าง Whitelist และ Blacklist ของรายการโปรแกรมต่างๆ ที่ อนุญาต/ไม่อนุญาต ให้ใช้ในเครื่องคอมพิวเตอร์
7. ไฟร์วอลล์แบบผสมผสานของ Webroot ตรวจสอบข้อมูลของโปรแกรมต่างๆ ที่ถูกส่งออกไปยังระบบเครือข่าย ที่ทำงานร่วมกับไฟร์วอลล์ของ Windows เพื่อป้องกันอุปกรณ์ของพนักงาน ทั้งที่เชื่อมต่อหรือไม่เชื่อมต่อกับระบบเครือข่ายขององค์กร
8. มีฟีเจอร์ที่วิเคราะห์พฤติกรรมการใช้งานคอมพิวเตอร์ของพนักงานแต่ละคน เพื่อออกแบบรูปแบบการป้องกันที่ปลอดภัยและเหมาะสมที่สุด
9. ป้องกันภัยคุกคามที่มาจากช่องทาง Offline สามารถป้องกันการรันด้วยตัวเองของโปรแกรมแฝงมัลแวร์ที่อยู่ในแฟลชไดร์ฟ รวมถึงในแผ่น CD หรือ DVD
10. รองรับการทำงานบนอุปกรณ์ที่มีหลายระบบปฏิบัติการ เครื่องที่มีระบบเวอร์ชวลไลเซชั่น รวมถึง Terminal Server และเครื่องที่รันระบบ Citrix

ความต้องการของระบบ (System Requirements)

Windows

- OS : Windows 10 32 and 64-bit , Windows 8, 8.1, 32 and 64-bit , Windows 7 32 and 64-bit , Windows Vista 32 and 64-bit , Windows XP 32 and 64-bit , Windows XP Embedded

Mac

- OS : Mac OS X 10.7 (Lion) , Mac OS X 10.8 (Mountain Lion) , OS X 10.9 (Mavericks) , OS X 10.10 (Yosemite) , OS X 10.11 (El Capitan) , macOS 10.12 (Sierra) , macOS 10.13 (High Sierra) , macOS 10.14 (Mojave) , macOS 10.15 (Catalina)

Windows Servers

- OS : Windows Server 2012 R2 Standard , R2 Essentials , Windows Server 2008 R2 Foundation , Standard , Enterprise , Windows Server 2003 Standard , Enterprise 32 and 64-bit (must support SHA-2) , Windows Small Business Server 2008 , 2011 , 2012 , Windows Server 2003 R2 for Embedded Systems , Windows Embedded Standard 2009 SP2 , Windows XP Embedded SP1 , Embedded Standard 2009 SP3 , Windows Embedded for POS Version 1.0 , Windows Server 2016 Standard, Enterprise and Datacentre , Windows Server 2019 Standard Server with Desktop Experience , Windows Server 2019 Datacenter Server with Desktop Experience

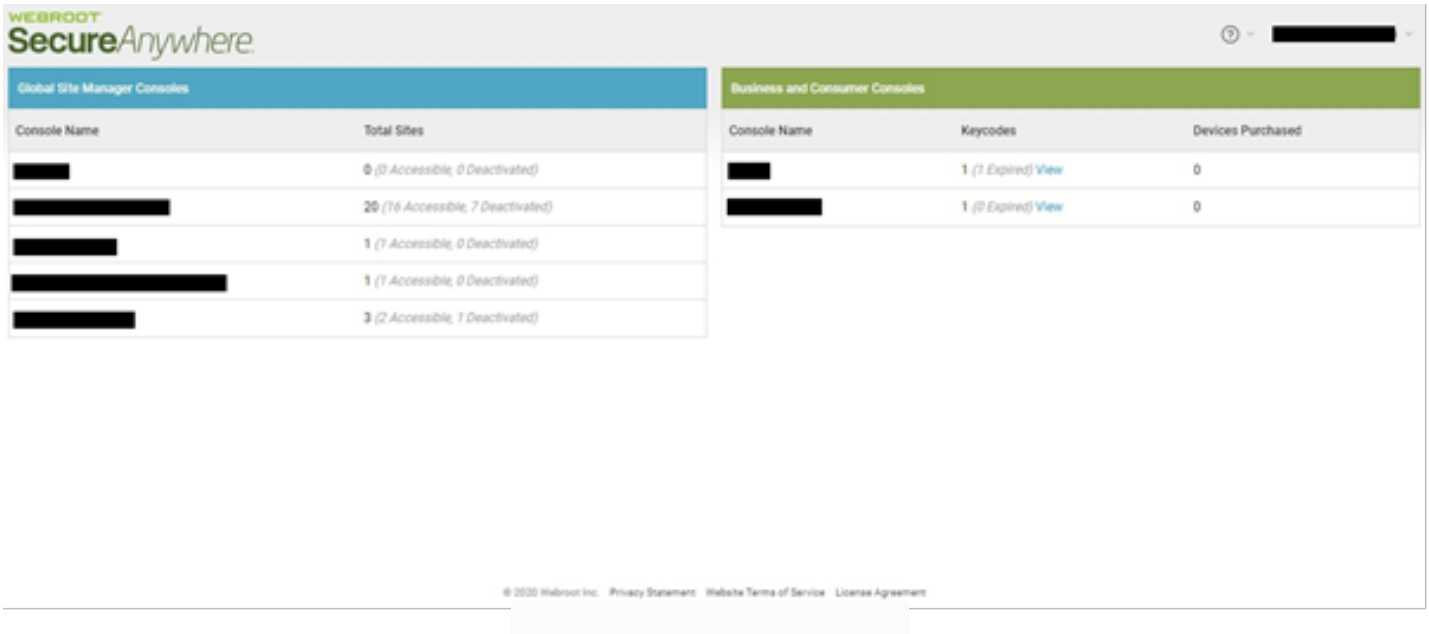
VM Platforms

- OS : VMware vSphere 5.5 and older (ESX/ESXi 5.5 and older) , Workstation 9.0 and older, Server 2.0 and older , Citrix XenDesktop 5 , XenServer 5.6 and older , XenApp 6.5 and older , Microsoft Hyper-V Server 2016 , Microsoft Hyper-V Server 2012 , 2012 R2 , Microsoft Hyper-V Server 2008 , 2008 R2 , Virtual Box

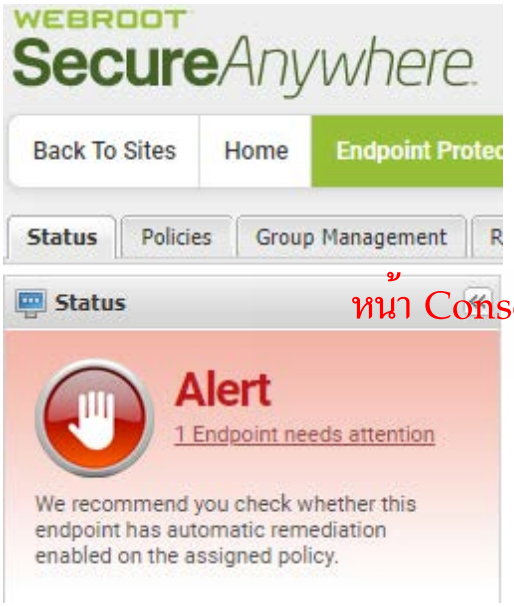
ข้อมูลเพิ่มเติมในด้านการทำงานของ Webroot

1. **Webroot** มีหน้า **Dashboard** ที่จัดการได้ง่ายและยังสามารถแสดงรายงานรูปแบบกราฟแท่งผ่าน **Web Console** ได้

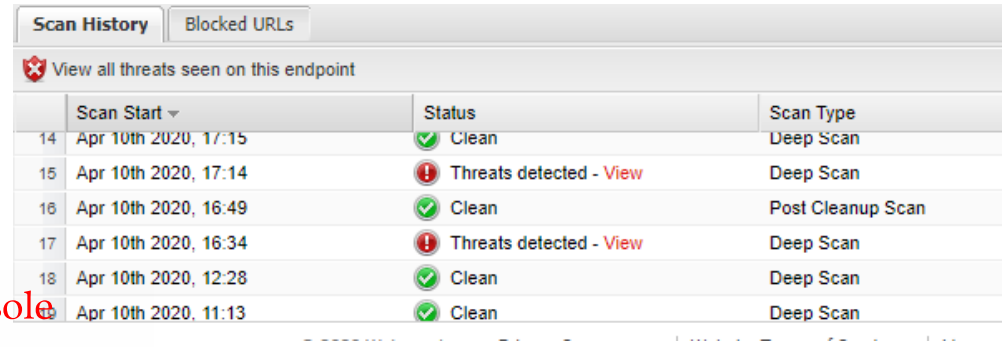
2. ในรายที่ถือ **GSM** เอง ก็สามารถเข้าไปดูและจัดการได้ง่ายๆ เช่นกัน โดยสามารถเพิ่มและกำหนดสิทธิ์ให้กับผู้ดูแลระบบได้

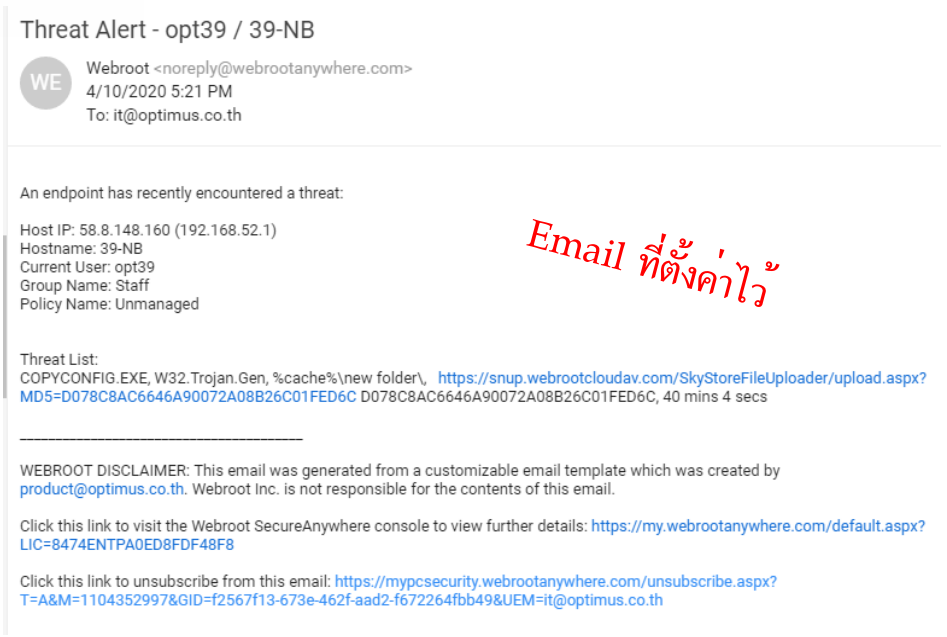


3. เมื่อ **Webroot** ตรวจเจอ ไวรัสหรือตรวจพบไฟล์ต้องสงสัยจะทำการแจ้งเตือนทันที โดยแจ้งไป **2** ทาง คือ หน้า **Console** และ ทาง **email** ที่ตั้งค่าไว้



หน้า Console





Email ที่ตั้งค่าไว้

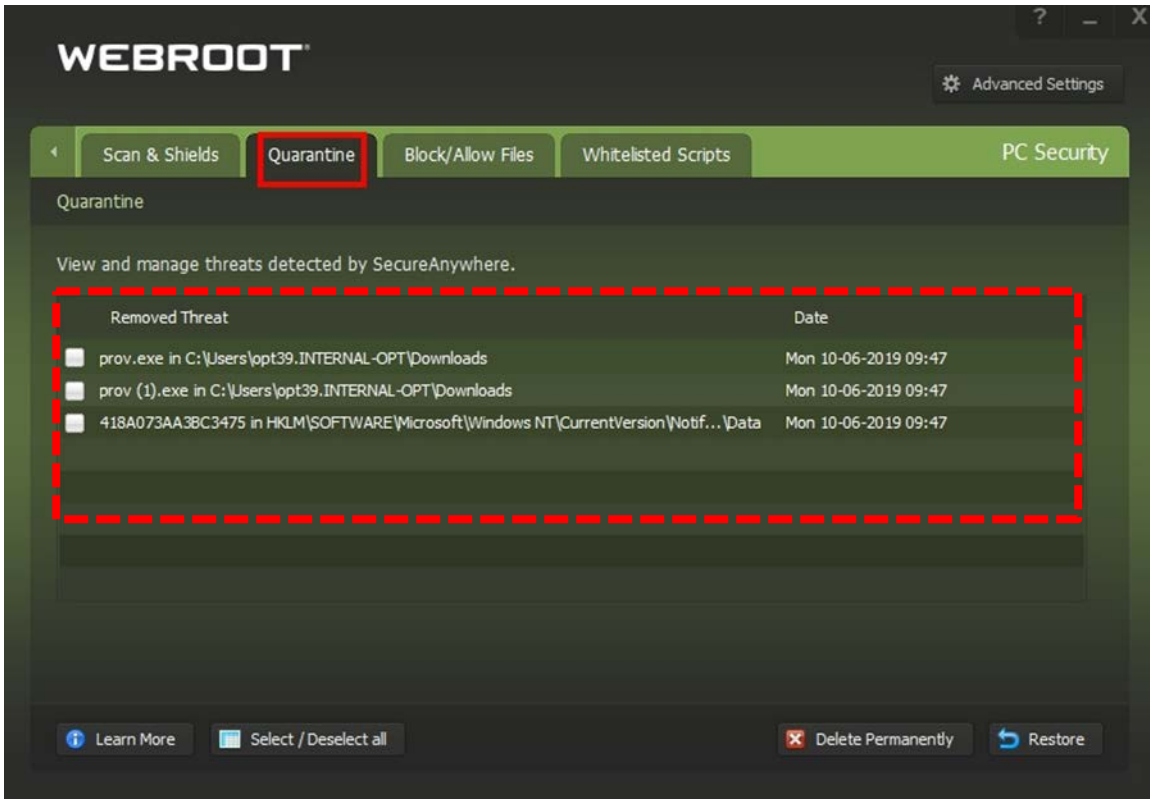
4. เมื่อ **Webroot** ตรวจเจอไวรัส หรือ ไฟล์ต้องสงสัยแล้ว **Webroot** จะมีการดำเนินการดังนี้

4.1 Create override คือการทำ Whitelist ให้ไฟล์นั้นไม่ถูก Webroot กักกันออกไป เช่นเป็นไฟล์ .exe ที่เป็นตัวลงโปรแกรม อาจจะถูกมองว่าเป็น ไวรัส Webroot จะทำการ detect และกักกันไว้ ไม่ให้มันทำงาน เป็นต้น

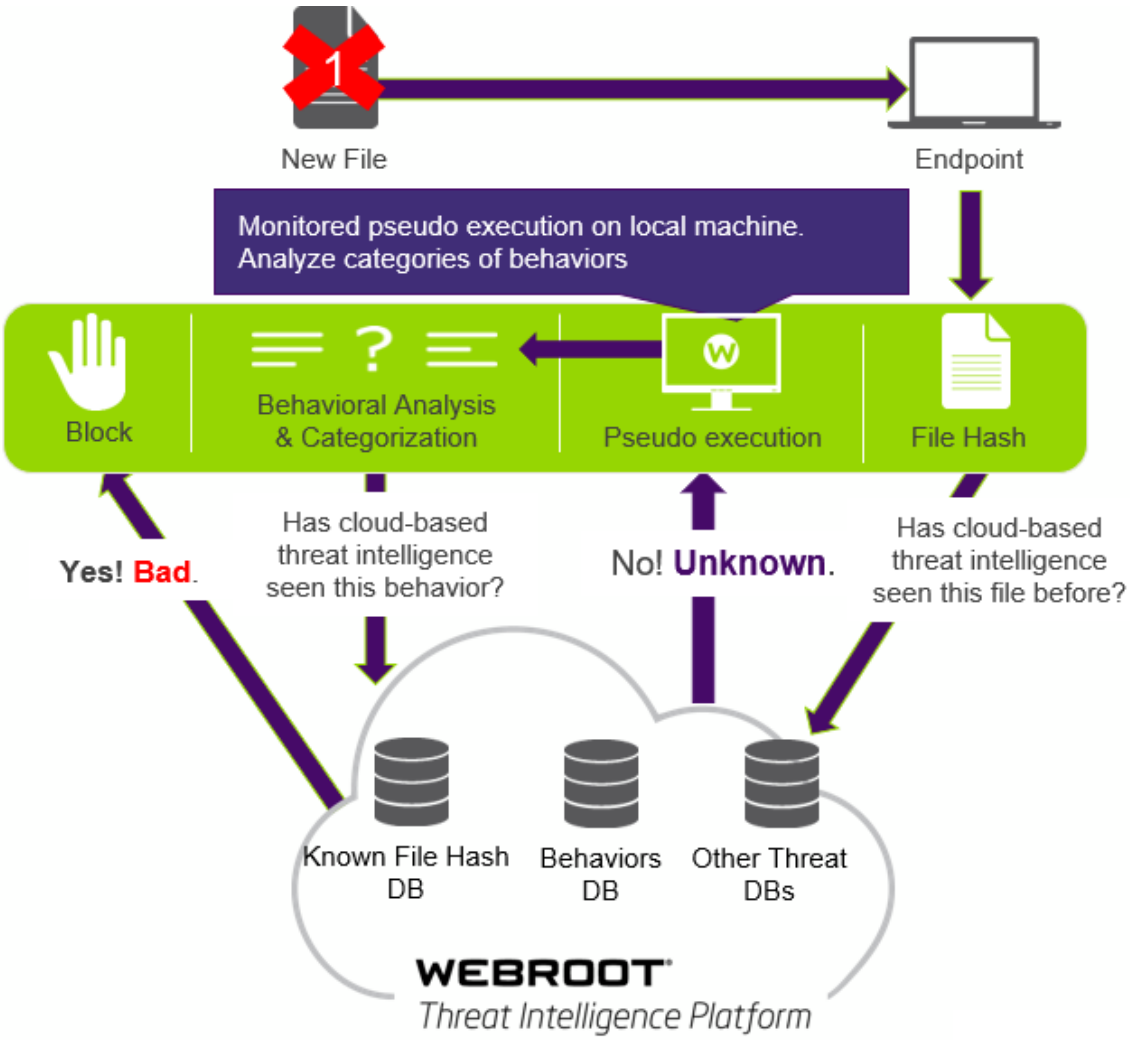
4.2 Show all PCS which have encountered this file คือโชว์ให้รู้ว่าไฟล์นี้ที่โดนกันไว้ ได้ไปอยู่บนเครื่องไหนบ้าง

4.3 Restore from Quarantine คือไฟล์ที่โดน Webroot detect ได้นั้น จะถูกกักกันไว้ในเครื่องนั้น ๆ เราจะเลือก Restore กลับมาได้เช่นกัน

ส่วนสถานที่กักกันนั้น จะต้องไปดูเครื่องที่มีไฟล์นั้น ซึ่งจะอยู่ในแท็ป **Quarantine**



5. เมื่อเกิดการติดไวรัส ที่เครื่องใด เครื่องหนึ่ง และเจอไวรัส หรือ Ransomware ร้าย ๆ อย่างพวกฝังไฟล์ และทำการถอนโปรแกรมในเครื่องได้ ซึ่งแน่นอนว่าเกิดขึ้นได้ เพราะไม่มีโปรแกรม Anti-Virus ยี่ห้อไหนที่การันตีได้ว่า จะสามารถป้องกันได้ 100% และถ้าเป็น Ransomware /Malwareระดับนี้ ก็ต้องเป็น Anti-Virus ที่สามารถทำ **Behavior Analysis** ได้ และจะต้องสามารถสร้าง **Virtual Environment** มาดัก Ransomware /Malware พวกนี้ไว้ ซึ่ง Anti-Virus ที่สามารถทำ **Behavior Analysis** ได้ในตลาดตอนนี้มีอยู่ประมาณ 2-3 ค่าย ซึ่งต้องซื้อเพิ่ม และมีราคาสูงมาก ก็ได้แก่ Sophos - intercept x แล้วก็ Trend Micro – Xgen แต่ที่พิเศษไปมากกว่านั้นคือ **Webroot มี Behavior Analysis มาด้วยอยู่แล้ว**

โดยถ้าเป็น Webroot หากเครื่องของคุณติดไวรัสประเภทนี้แล้ว จะต้องไปดูว่า ตอนนั้น Traffic มันผ่านเข้ามาทางไหน และเข้าไปเช็คได้ที่ Quarantine ซึ่งจะพบว่า มันถูกกักไว้แล้ว

หลักการทำงานของ Behavioral protection