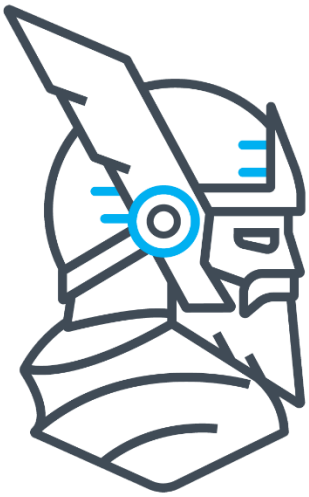


HEIMDAL™

SECURITY

คู่มือแนะนำการใช้งาน “เทพไฮมดัล” เบื้องต้น

นำเข้าและให้บริการโดย **บริษัท ไซเบอร์อัลฟ่า จำกัด**
357/60 ซอยนวมินทร์111 แขวงนวมินทร์ เขตบึงกุ่ม กรุงเทพมหานคร 10230
โทร: 02 030 1990 อีเมล: support@cybersecuritythailand.com

สารบัญ

ตรวจสอบก่อนติดตั้ง

ระบบปฏิบัติการที่รองรับ

HEIMDAL สามารถติดตั้งบนอุปกรณ์ที่ใช้ระบบปฏิบัติการต่อไปนี้

- Windows 7 (32 and 64 bit)
- Windows 8 (32 and 64 bit)
- Windows 8.1 (32 and 64 bit)
- Windows 10 (32 and 64 bit)
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- MacOS 10.13 - High Sierra, 10.14 – Mojave, 10.15 – Catalina**, 10.16 - BigSur (and above)
- Android 6.0 (and above)

ความต้องการขั้นต่ำ

- Microsoft .NET Framework 4.6.1 (or above)
- Up to 400 MB of disk space
- At least 250 MB RAM
- At least 3% of CPU usage when blocking a domain, up to 10% when opening the Heimdal™ Agent, and up to 40% during a scan
- Local administrator or domain administrator permissions (if the computer is domain-joined) during installations
- User permissions during execution
- Internet access with the following ports open to traffic: port 53 (to apply the DarkLayer Guard DNS 127.7.7.x), port 80 (to filter traffic over http), port 443 (to filter traffic over https)

สำหรับข้อมูล IP Addresses, Ports ที่ HEIMDAL ต้องใช้ และการตั้งค่า Exclusions เพื่อให้ระบบทำงานได้ตามที่ควร ไม่ถูกบล็อคโดย network firewall ขององค์กร คลิก

Recommended Browsers

HEIMDAL dashboard ใช้งานกับ internet browser ได้หลากหลาย แต่จะดีที่สุดหากใช้กับ browser ต่อไปนี้

- Google Chrome (recommended)
- Mozilla Firefox
- Microsoft Edge
- Safari

การใช้งาน module ของ HEIMDAL ร่วมกับแบรนด์อื่น ๆ

- HEIMDAL™ Threat Prevention - Endpoint (DarkLayer Guard - Endpoint) สามารถใช้ควบคู่กับโปรแกรม Antivirus แบรนด์อื่น ๆ ได้ (รวมถึง Windows Defender) แต่ไม่ควรใช้ร่วมกับโปรแกรม DNS Traffic Scanning Application ตัวอื่น เพราะอาจเกิดความขัดแย้งและทำให้ระบบทำงานได้ไม่ถูกต้อง เราแนะนำให้ปิดการทำงานของ DNS Traffic Scanning Application ตัวอื่น ๆ ก่อนที่จะเปิดการใช้งาน DarkLayer Guard
- HEIMDAL™ Patch & Asset Management และ HEIMDAL™ Ransomware Encryption Protection สามารถทำงานลักษณะ standalone หรือร่วมกับระบบ Antivirus แบรนด์อื่น ๆ ได้
- ไม่ควรใช้ HEIMDAL™ Next-Gen Endpoint ร่วมกับ antivirus ระบบฐานข้อมูลหรือ virus definition แบรนด์อื่น เพราะอาจเกิดความขัดแย้งและทำให้ระบบทำงานได้ไม่ถูกต้อง เราแนะนำให้ปิดการทำงานของ antivirus ตัวอื่น ๆ ก่อนที่จะเปิดการใช้งาน HEIMDAL™ Next-Gen Endpoint

ทำความรู้จักแต่ละ **Module** หลักแบบคร่าว ๆ

HEIMDAL™ Next-Gen Endpoint Antivirus

Cloud Antivirus ขั้นสูงที่ถูกนำมาพัฒนาและต่อยอดโดย Heimdal ด้วยเทคโนโลยี Next-Gen ต่างๆ อาทิ Real-time Cloud Scanning with Machine Learning, Active Registry Change Scanning, AI-Power Detection, Sandbox & Backdoor Inspection, Process and Behavior-Based Scanning, Brute Force Attack Blocking และฟีเจอร์พื้นฐานที่ควรต้องมีครบถ้วนสำหรับการใช้งานในองค์กร ได้แก่ Schedule Scan, Device Control, Centralized Firewall, Enforce Password for Uninstallation

HEIMDAL™ Threat Prevention – Endpoint

Advanced Protection ในลักษณะ proactive ใช้ 2-way DNS traffic filtering engine ป้องกัน Zero Hour exploits เช่น ransomware และการโจมตีขั้นสูงต่างๆ (APTs) และสามารถบล็อคเว็บไซต์ตาม Category หรือทำ blacklist/whitelist (สามารถใช้งานร่วมกันกับ antivirus ยี่ห้ออื่น รวมถึงตัวฟรีทั้งหมด)

- **DarkLayer Guard** ป้องกันภัยคุกคามที่ DNS, HTTP, HTTPS ซึ่งสามารถ ตามล่า ตรวจจับ และตอบรับได้อย่างรวดเร็วด้วยเทคโนโลยี Threat-to-Process Correlation (TTPC)
- **VectorN Detection** เพิ่มฟังก์ชั่น HIPS, HIDS และ indicator of attacks/indicator of compromise โดยใช้ Neural Network ของ AI ตรวจจับภัยคุกคามที่ซ่อนอยู่ หยุดการโจมตีที่ antivirus หรือ firewall ไม่สามารถมองเห็น

HEIMDAL™ Patch & Asset Management

ลิสต์ software ที่ติดตั้งอยู่บนทุกอุปกรณ์ อุดช่องโหว่ของระบบและ software ต่างๆ ด้วย X-Ploit Resilience อัพเดท patch ผ่านศูนย์กลาง รองรับทั้ง Windows และ 3rd party application มากกว่า 100+ software มีระบบ One Click App Installation หรือ deploy 3rd party application ข้างต้น ไปที่เครื่องปลายทางทั้งแบบ silent หรือแบบคลิก install ผ่าน HEIMDAL agent สำหรับลิสต์ software คลิก (สามารถใช้งานร่วมกันกับ antivirus ยี่ห้ออื่น รวมถึงตัวฟรีทั้งหมด)

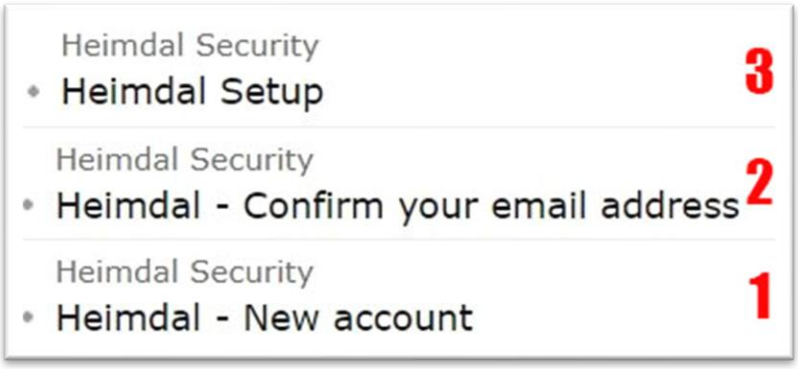
มี module ย่อยเสริมเรียกว่า Infinity Management ซึ่งสามารถนำ patch ของท่านเอง (msi, exe หรืออื่น ๆ) ไปใช้แบบ stand-alone ซึ่งสามารถ applied ตาม Group Policy ได้ optional module นี้สามารถซื้อเสริมจาก Patch & Asset Management

HEIMDAL™ Ransomware Encryption Protection

module สำหรับการวิเคราะห์ process โดยโฟกัสที่การบล็อค encryption จากพฤติกรรมที่มีพิรุธของ ransomware บนทุกเครื่องที่มีติดตั้ง module นี้ไว้ (สามารถใช้งานร่วมกันกับ antivirus ยี่ห้ออื่น รวมถึงตัวฟรีทั้งหมด)

ขั้นตอนการติดตั้ง

1. เช็ค inbox ในอีเมล



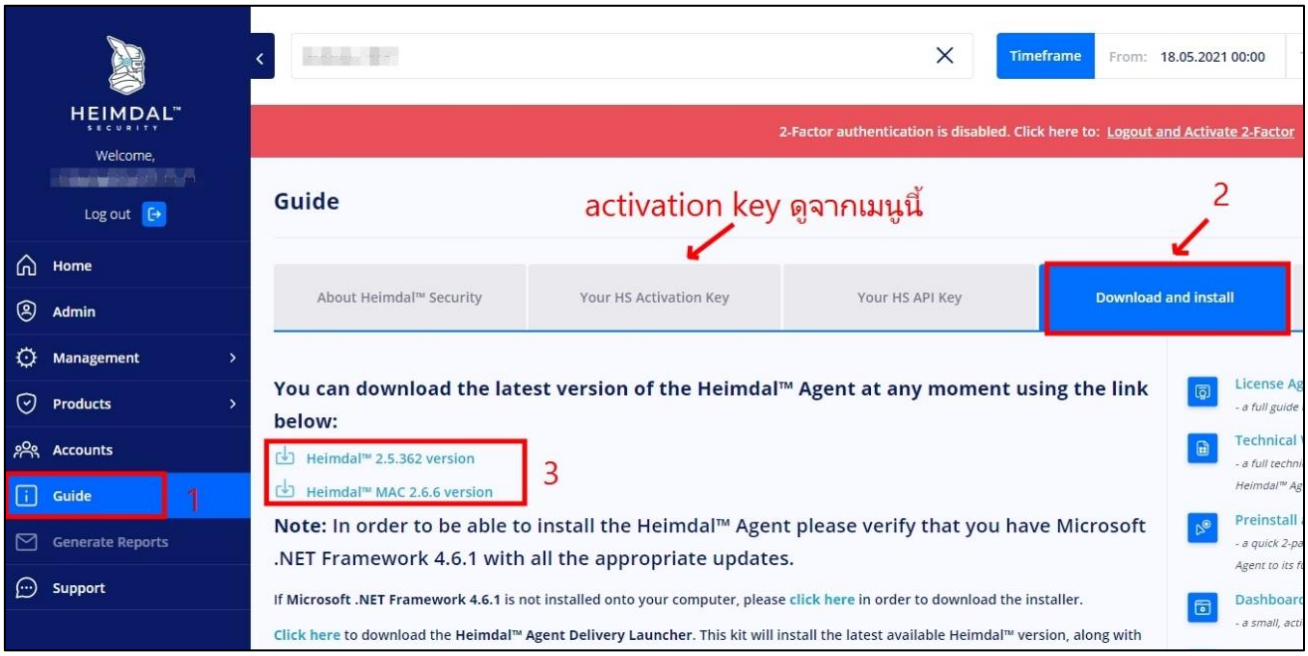
2. copy รหัสจากข้อความในอีเมลที่ 1

3. กดลิ้งค์เพื่อยืนยันอีเมลจากในอีเมลฉบับที่ 2 นำรหัสที่ copy มา paste ในช่อง current password และทำการตั้ง new password ในช่องถัดไป

4. ดาวน์โหลดตัว agent สำหรับติดตั้งได้จากอีเมลฉบับที่ 3 ติดตั้งโดยใช้ key จากเมนู Your HS Activation Key บน dashboard

5. เข้าหน้า dashboard โดย login ที่ https://rc-dashboard.heimdalsecurity.com
หมายเหตุ: การเปิด 2-factor authentication จะทำให้ account ปลอดภัยยิ่งขึ้น

   หรือท่านสามารถโหลดตัวติดตั้งได้จากหน้า dashboard ตามขั้นตอนต่อไปนี้



ข้อมูลเพิ่มเติมสำหรับการติดตั้ง

การติดตั้งแต่ละระบบปฏิบัติการ step by step

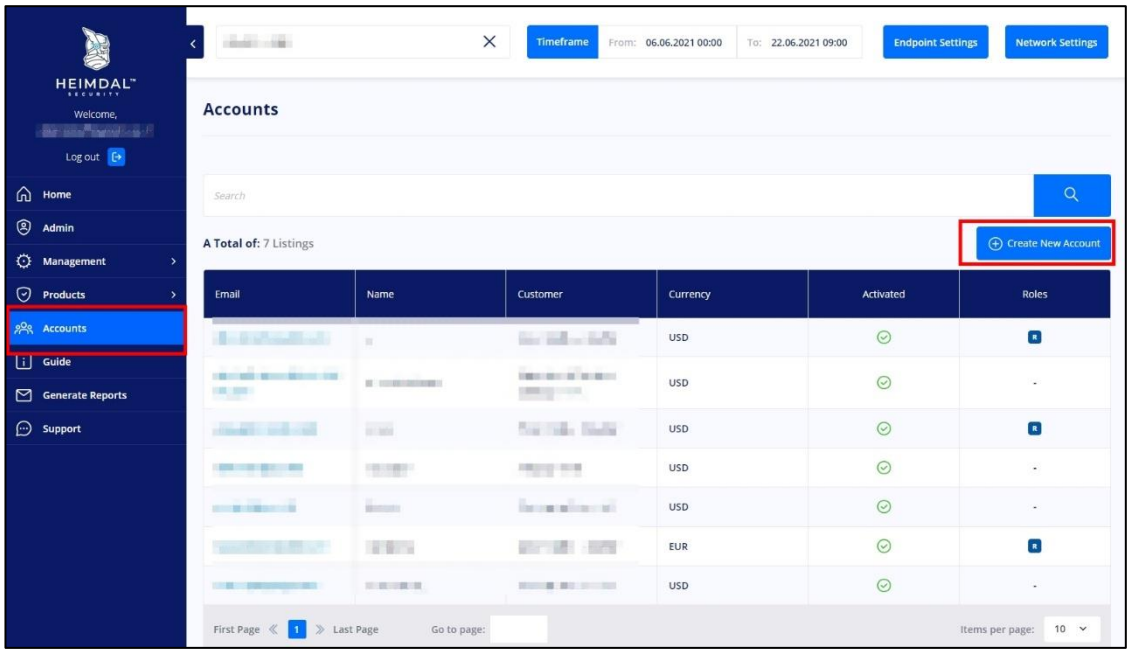
- Installing the HEIMDAL Agent (Windows)
- Installing the HEIMDAL Agent (macOS)
- Installing the HEIMDAL Agent (Android)

สำหรับขั้นตอนการติดตั้งแบบ deploy สามารถดูข้อมูลได้จากลิ้งค์ต่อไปนี้

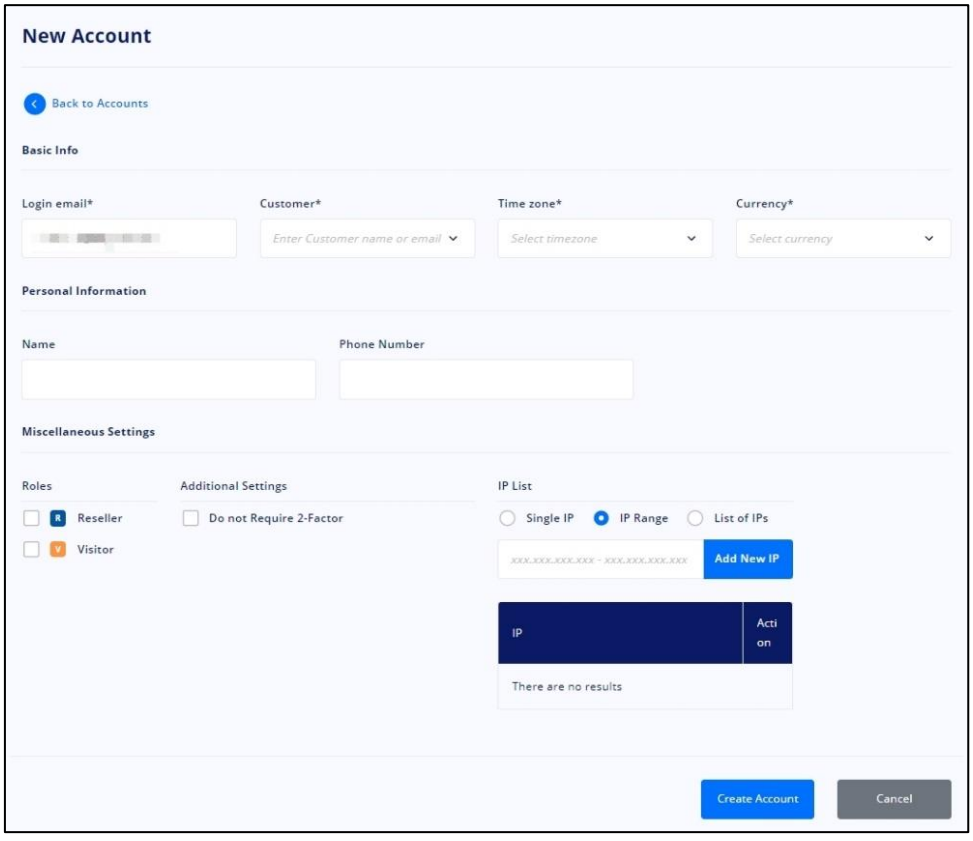
- Embedding the HEIMDAL license key into the .MSI Installer (for deployment)
- Deploying the HEIMDAL Agent through Active Directory GPO
- Deploying the HEIMDAL Agent through SCCM

การสร้าง account เพิ่ม

ท่านสามารถเพิ่ม account ให้ผู้ดูแลท่านอื่น ๆ login เข้ามายังหน้า dashboard ได้ โดยคลิกที่เมนู Account > Create New Account



กรอกข้อมูลลงในช่องให้ครบถ้วน สำหรับช่อง IP List หากไม่จำกัดการเข้าถึง สามารถกรอกเป็น 1.1.1.1-255.255.255.255 แล้วคลิก Add New IP จากนั้นคลิก Create Account



Main Dashboard

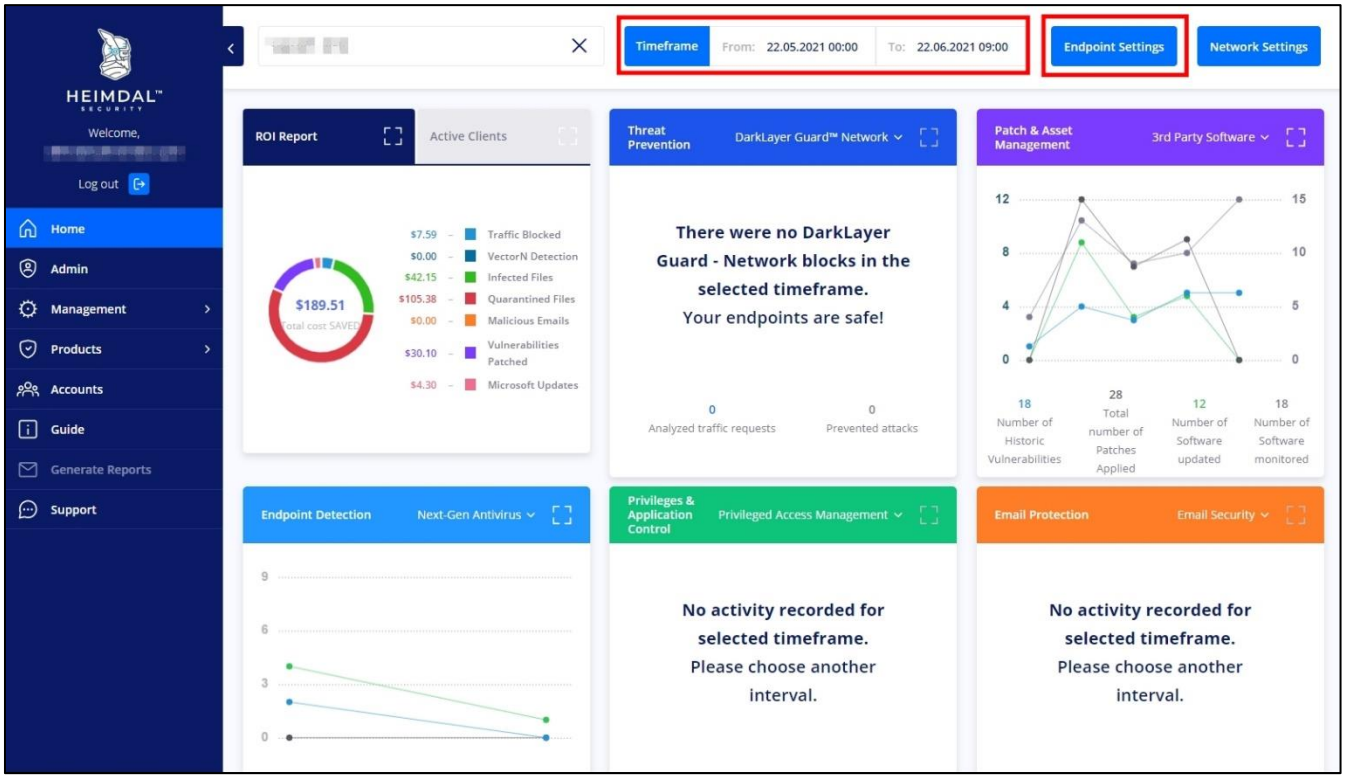
Timeframe

บริเวณด้านบนหน้าหลักของ dashboard จะมี Timeframe ให้เลือกช่วงเวลาการแสดงผลข้อมูลของบนหน้านั้น ๆ ที่กำลังเปิดอยู่

ท่านสามารถคลิกที่แต่ละช่วงเวลาของกราฟแต่ละ module เพื่อดูรายละเอียดเพิ่มเติมตามช่วงเวลาที่กำหนดได้

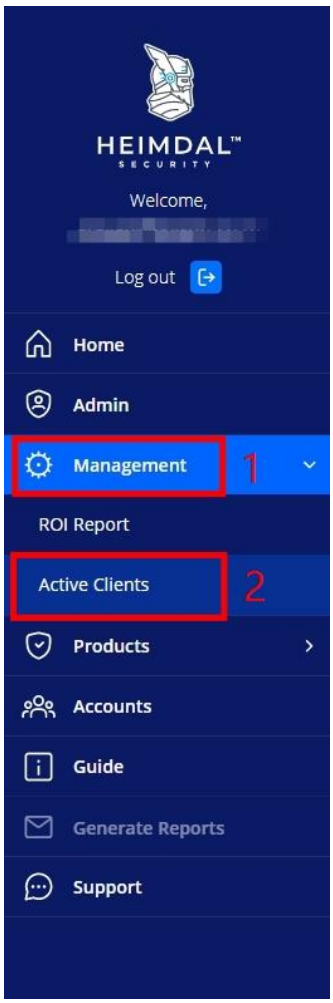
ROI Report

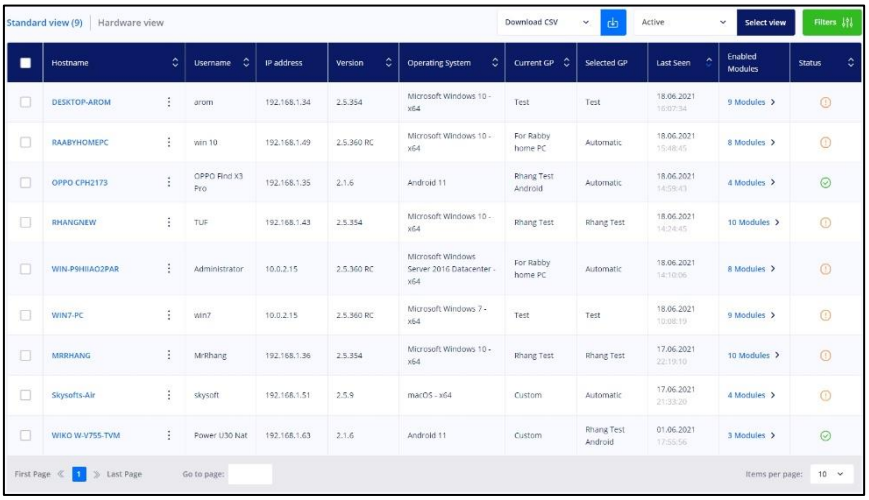
เป็นตัวเลขที่ทำให้เห็นถึงมูลค่าผลตอบแทนการลงทุนที่ HEIMDAL ได้ทำการป้องกันความเสียหายไว้ให้ ด้วยการปกป้องผู้ใช้งานและข้อมูลในระบบให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้หากไม่ได้ติดตั้ง HEIMDAL ไว้ก่อน

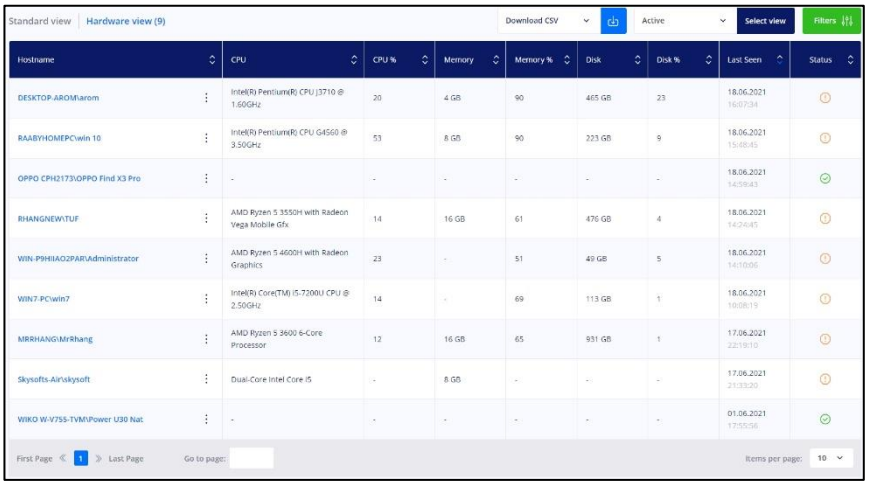


การดู Active Clients บน dashboard

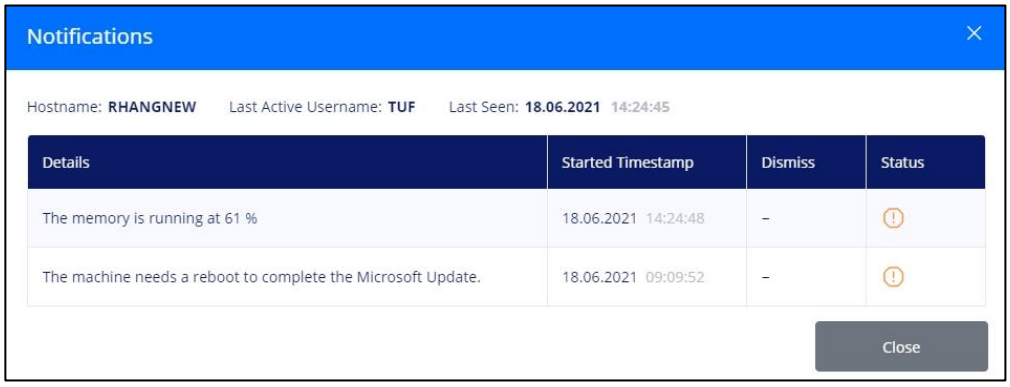
เมื่อติดตั้ง agent ที่เครื่องแล้ว ท่านสามารถดูรายชื่อเครื่องจากบน Cloud ได้จากเมนู Management > Active Clients โดยจะมีให้ดู 2 แบบคือ Standard view และ Hardware view ซึ่งให้ข้อมูลที่แสดงผลออกมาแตกต่างกัน และมี filter สำหรับกรองข้อมูลที่มุมบนขวาตาราง







column ขวาสุดของตารางรายชื่อเครื่อง จะเป็นสัญลักษณ์พร้อมเครื่องหมายสีเขียวหรือสีส้ม เมื่อคลิกจะเป็นการแสดงสถานะของเครื่องนั้น ๆ ว่าติดตั้งเรียบร้อยดีหรือมี notice สำคัญอะไรอยู่บ้าง ท่านสามารถดูรายละเอียดของข้อมูลสถานะต่าง ๆ ได้จาก คลิก



การสร้าง Group Policy (GP)

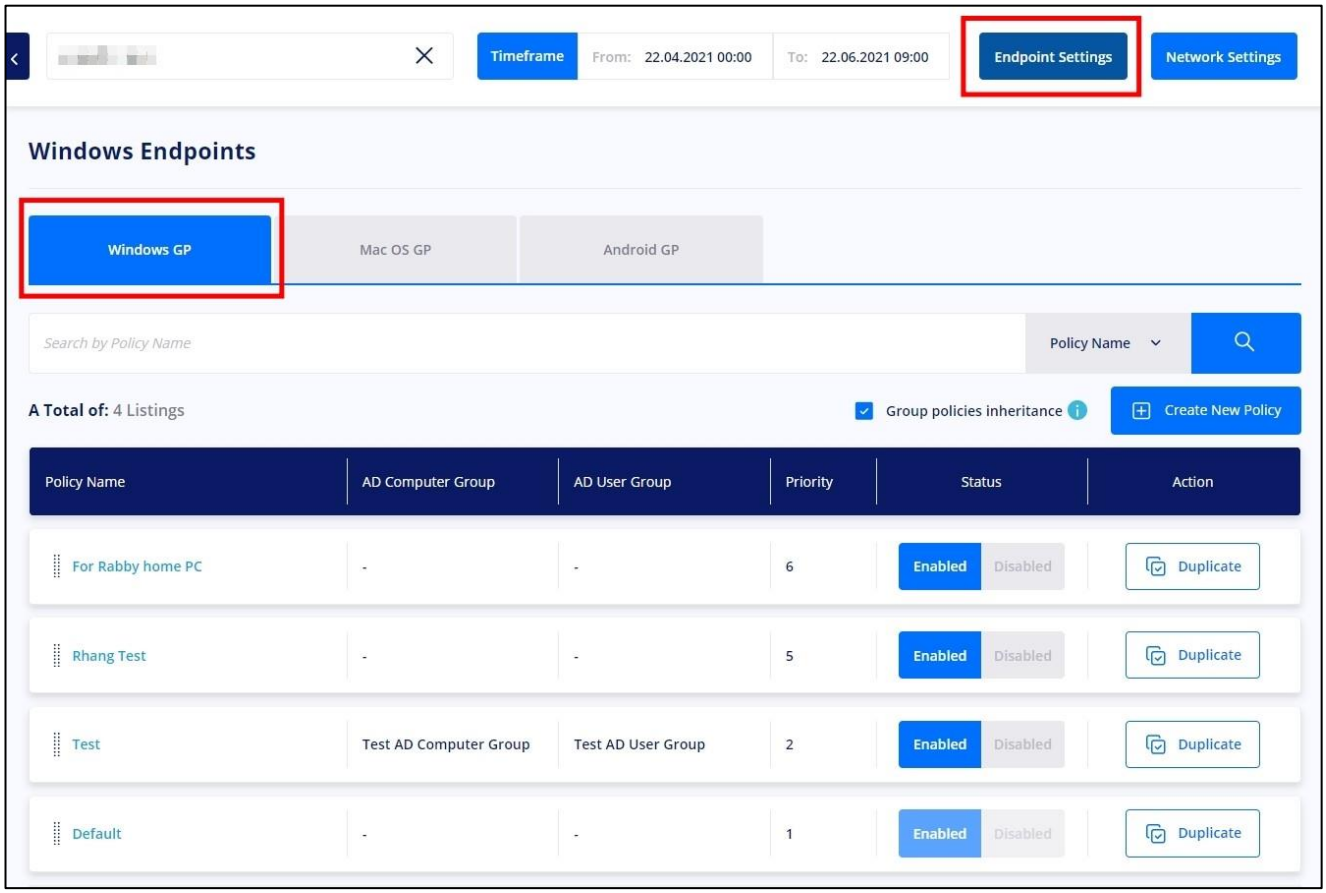
คลิกที่ Endpoint Settings ที่มุมบนขวา จากนั้นเลือก tab ระบบปฏิบัติการที่ต้องการสร้าง GP

ค่าเริ่มต้นจะมี Default ที่ไม่สามารถปรับค่าใด ๆ ได้ และ Custom ที่สามารถปรับค่าตามการใช้งานได้ โดยท่านสามารถสร้างเป็น GP ใหม่ขึ้นมาได้ด้วยการกด Duplicate

แต่ละ GP จะมีตัวเลข Priority กำกับอยู่ หากที่เมนู Management > Active Clients ท่านเลือก GP ไว้เป็น Automatic ระบบจะทำการเลือกใช้ GP ที่มี Priority สูงที่สุด (เลขมากที่สุด) โดยอัตโนมัติ

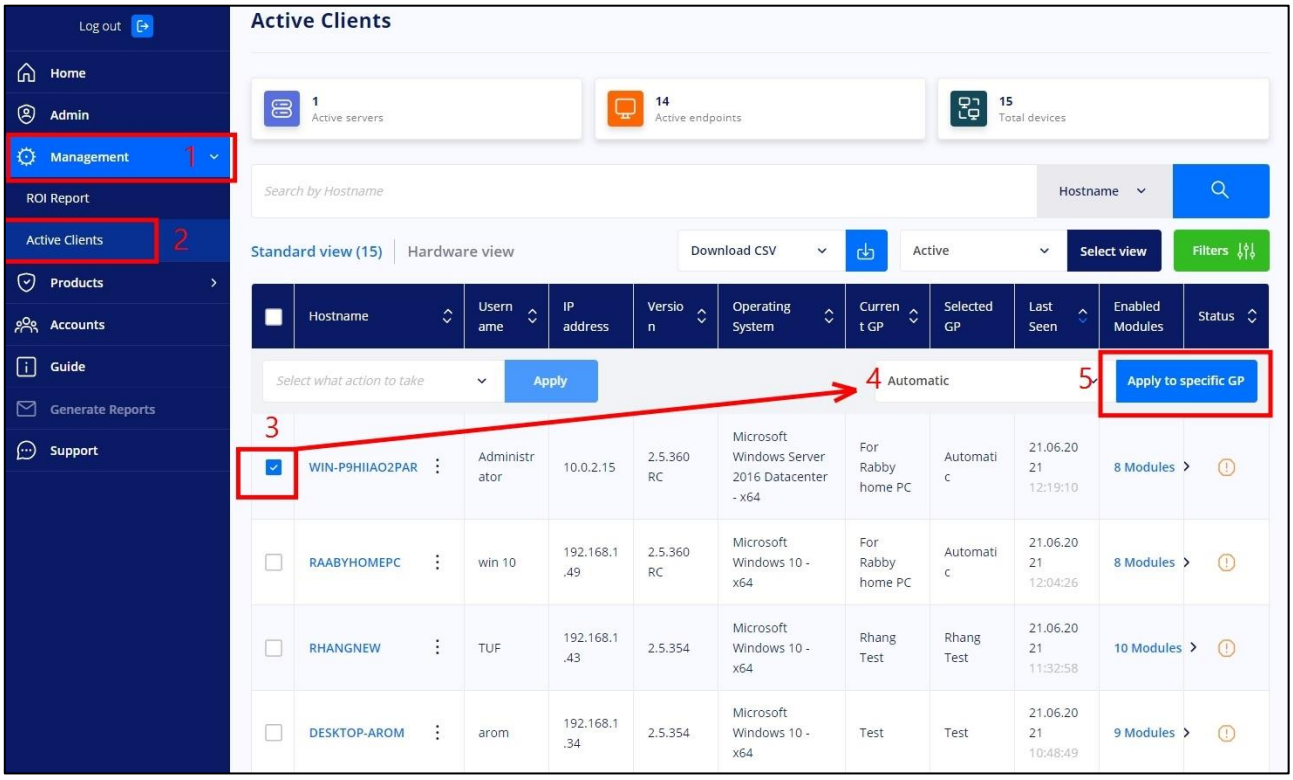
คลิกที่ชื่อ GP เพื่อเข้าสู่การตั้งค่าสำหรับ GP นั้น ๆ โดยท่านอาจจะแบ่งเป็นฝ่าย เป็นแผนก หรือแบ่งตามลักษณะการใช้งานตามแต่นโยบายขององค์กร

หลังจากตั้งค่า GP ตามที่ต้องการใช้เรียบร้อยแล้ว ต้องกำหนด Active Clients ให้มารับ GP ด้วย



การกำหนด Active Clients มารับ Group Policy (GP) ที่ตั้งไว้

ไปที่ Management > Active Clients > ติ๊กถูกที่หน้าชื่อเครื่อง > เลือก GP ตามที่ต้องการ (หากเลือกเป็น Automatic ระบบจะเลือกใช้ GP ที่มี Priority สูงสุด)

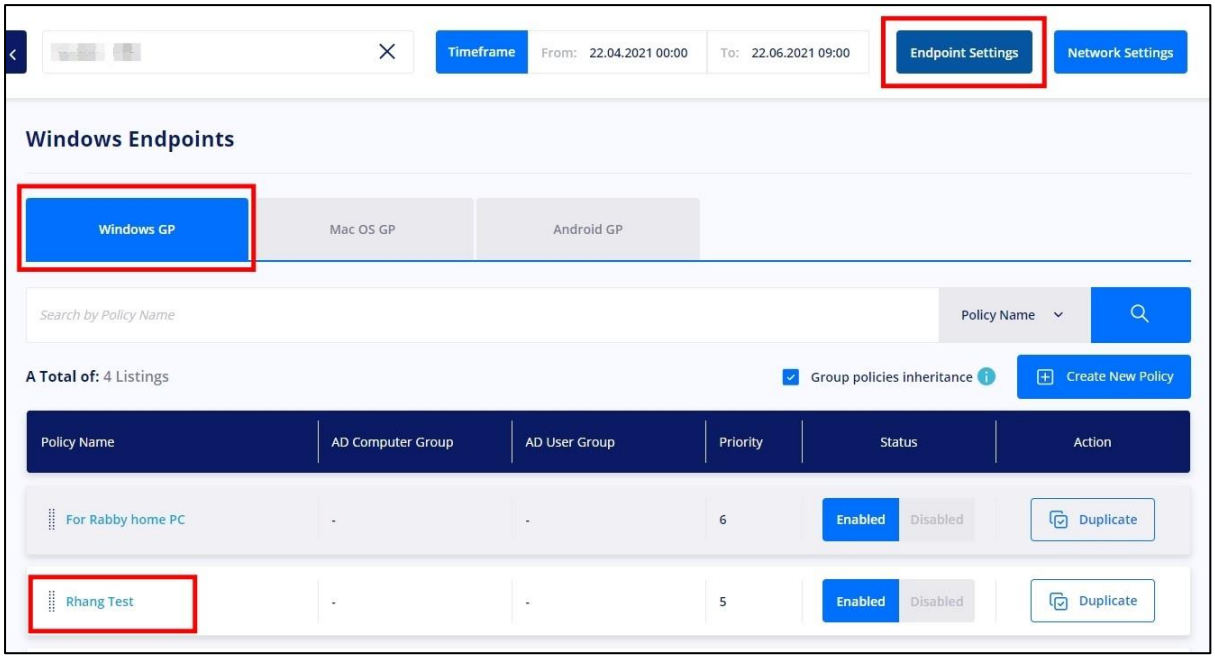


การตั้งค่า Group Policy เบื้องต้น

สำหรับข้อมูลรายละเอียดการตั้งค่าแบบละเอียด คลิก

การตั้งค่าต่าง ๆ บนหน้า dashboard แนะนำปรับให้เหมาะสมกับการใช้งานจริงในองค์กรของท่าน ภาพประกอบข้างต้นเป็นเพียงตัวอย่างเท่านั้น ซึ่งอาจไม่ใช่ค่าที่เหมาะสมที่สุดสำหรับแต่ละองค์กร

คลิกที่ Endpoint Settings ที่มุมบนขวา > เลือก tab ระบบปฏิบัติการที่ต้องการสร้าง GP > คลิกที่ชื่อ GP ที่ต้องการปรับค่า

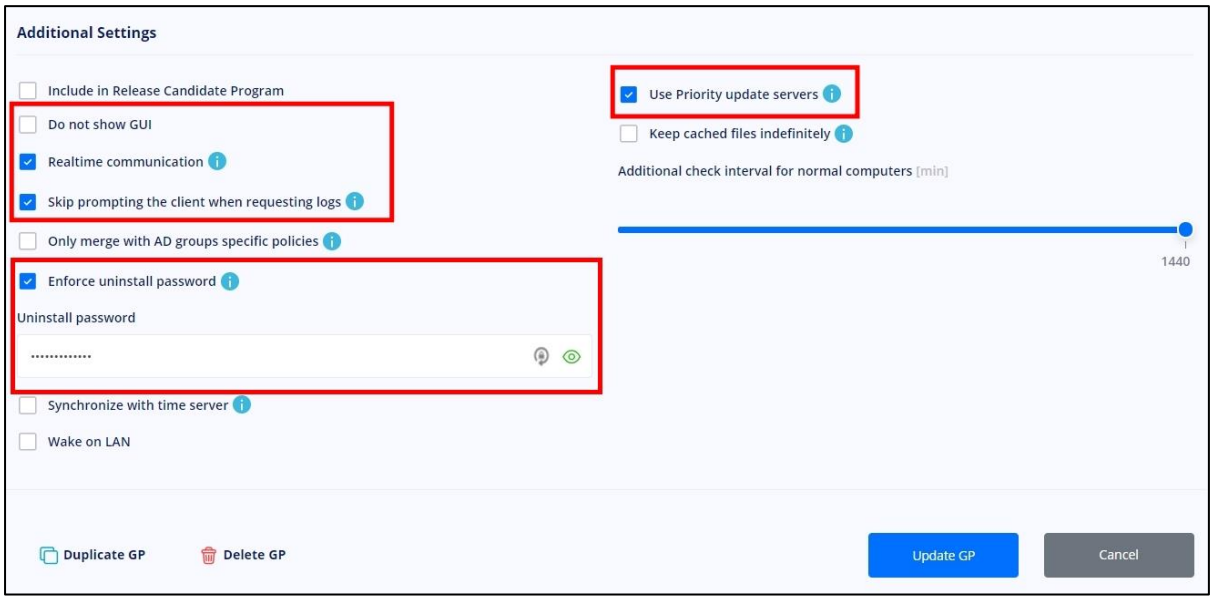


เมื่อคลิกที่ GP หนึ่งมาแล้ว จะมี tab ย่อยแตกออกมา กดที่แต่ละ tab เพื่อตั้งค่าตามหมวดหมู่ของการ setting ที่ระบบแบ่งไว้

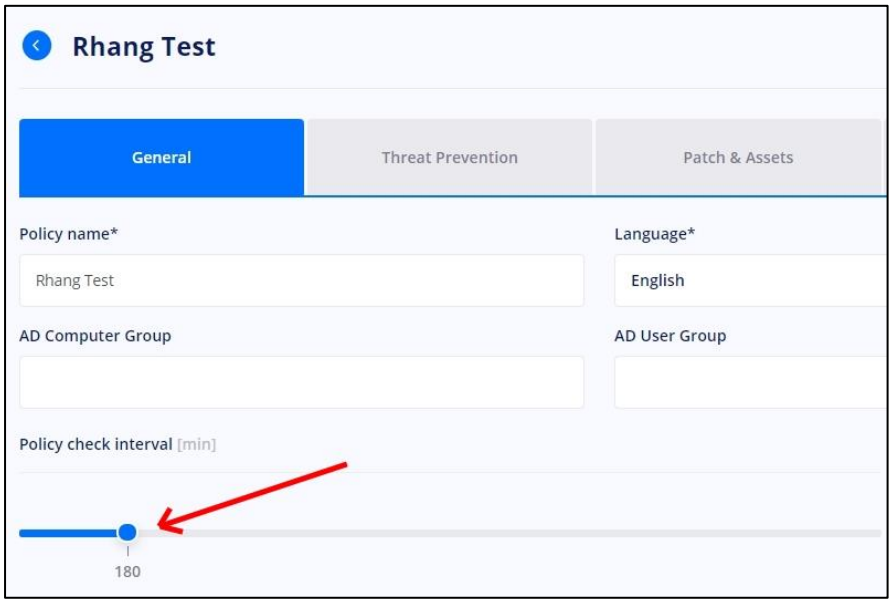
General tab มีค่าพื้นที่ฐานที่ควรต้องทราบดังนี้

- **Do not show GUI** ปิดการโชว์ icon ที่ taskbar ล่างขวาหน้าจอที่เครื่อง แนะนำสำหรับ File Servers, Citrix Servers, Terminal Servers, or RDP Servers
- **Realtime communication** ทำให้การอัพเดทค่าระหว่าง dashboard กับที่หน้าเครื่องรวดเร็วขึ้น (น้อยกว่า 1 นาที)
- **Enforce uninstall password** บังคับใช้รหัสในการ uninstall HEIMDAL ควรเปิดใช้และตั้งรหัสเฉพาะที่ผู้ดูแลทราบ เพื่อป้องกันโปรแกรมถูกถอนออกโดยไม่ได้รับอนุญาต
- **Use Priority update servers** ตั้งค่าการอัพเดท agent version และการ patch & deploy 3rd party applications ให้ผ่านเครื่องศูนย์กลางที่เข้าถึง internet เป็นประจำและอยู่ภายใน subnet เดียวกัน (P2P) โดยหลังจากติ๊กแล้วต้องไปเลือก Active Clients อย่างน้อย 1 เครื่องให้เป็น Priority Update Server

เมื่อตั้งค่าเรียบร้อยแล้ว ให้คลิก Update GP สีน้ำเงินที่มุมล่างขวา

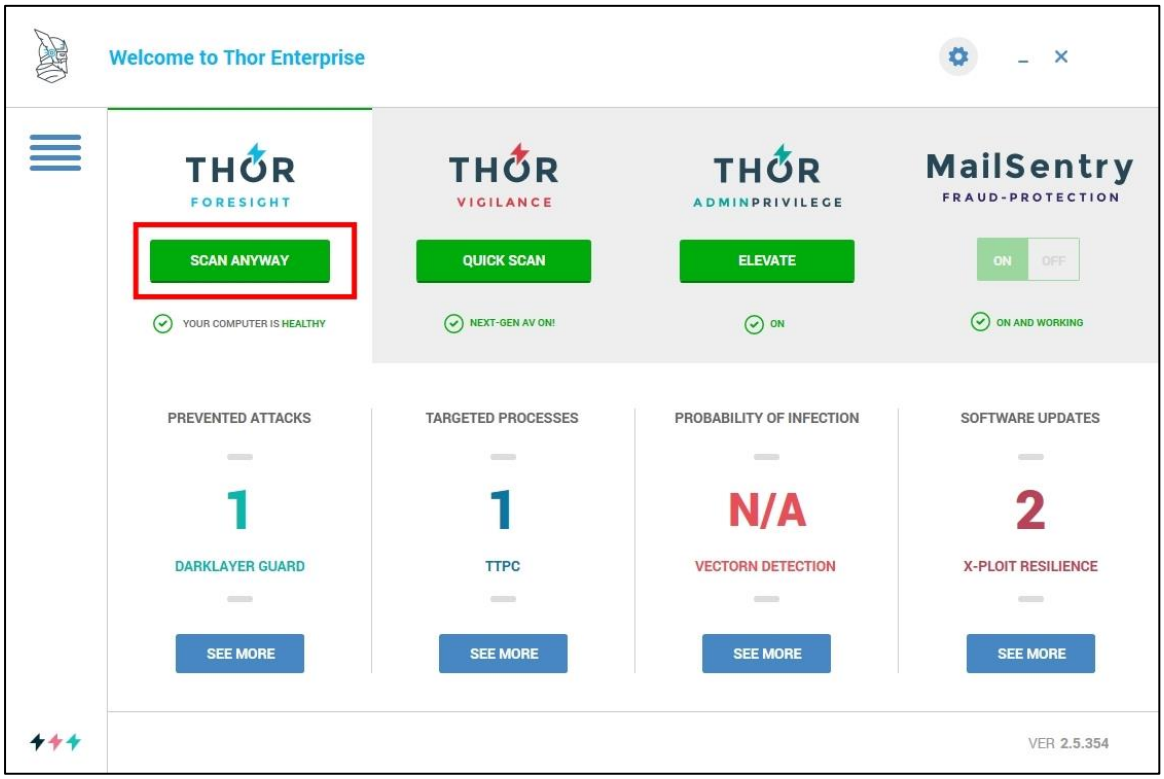


โดย default แล้ว การตั้งค่าบน dashboard จะวิ่งไปที่เครื่องปลายทางทุก 180 นาที (สามารถปรับให้ถี่สุดได้เป็นทุก 15 นาที)



หากท่านต้องการ push ค่าต่าง ๆ ที่ set ให้ไปมีผลที่เครื่องปลายทางทันที สามารถทำได้ด้วยวิธีการดังนี้

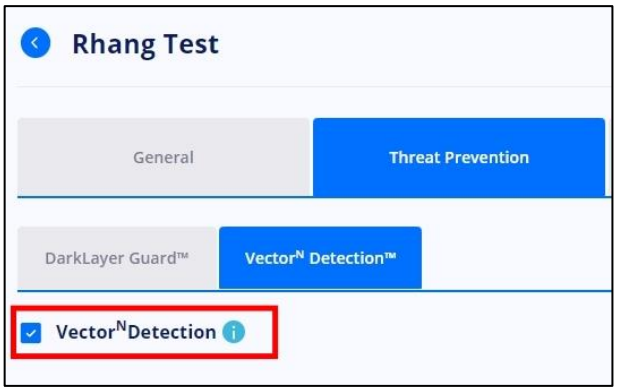
- คลิก **SCAN ANYWAY** จากตัว agent ที่หน้าเครื่องปลายทาง
- Restart HEIMDAL Client Host service
- Reboot เครื่อง



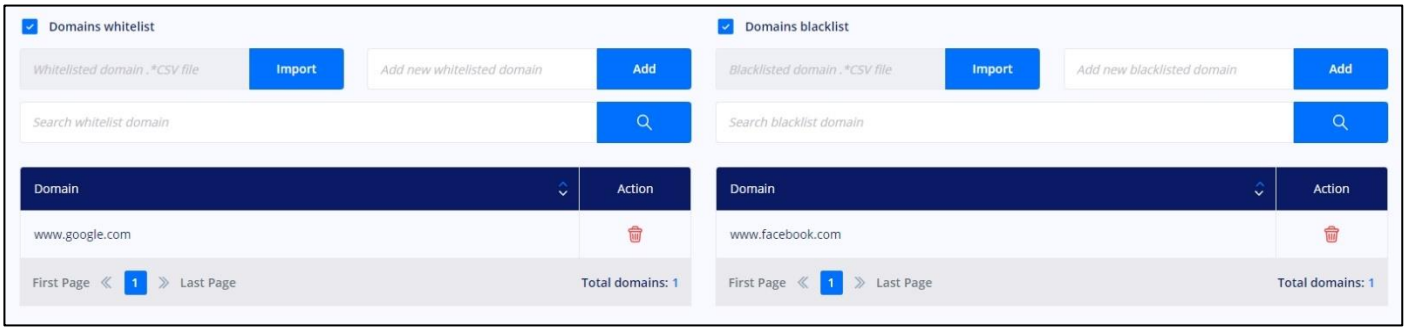
Threat Prevention tab มีค่าพื้นที่ฐานที่ควรต้องทราบดังนี้

หากท่านสั่งซื้อ Threat Prevention – Endpoint ไว้ ท่านจะสามารถคลิกที่ Threat Prevention tab ได้ หากท่านไม่ได้สั่งซื้อไว้ tab จะเป็นสีเทาอ่อนและไม่สามารถคลิกได้ (greyed out)

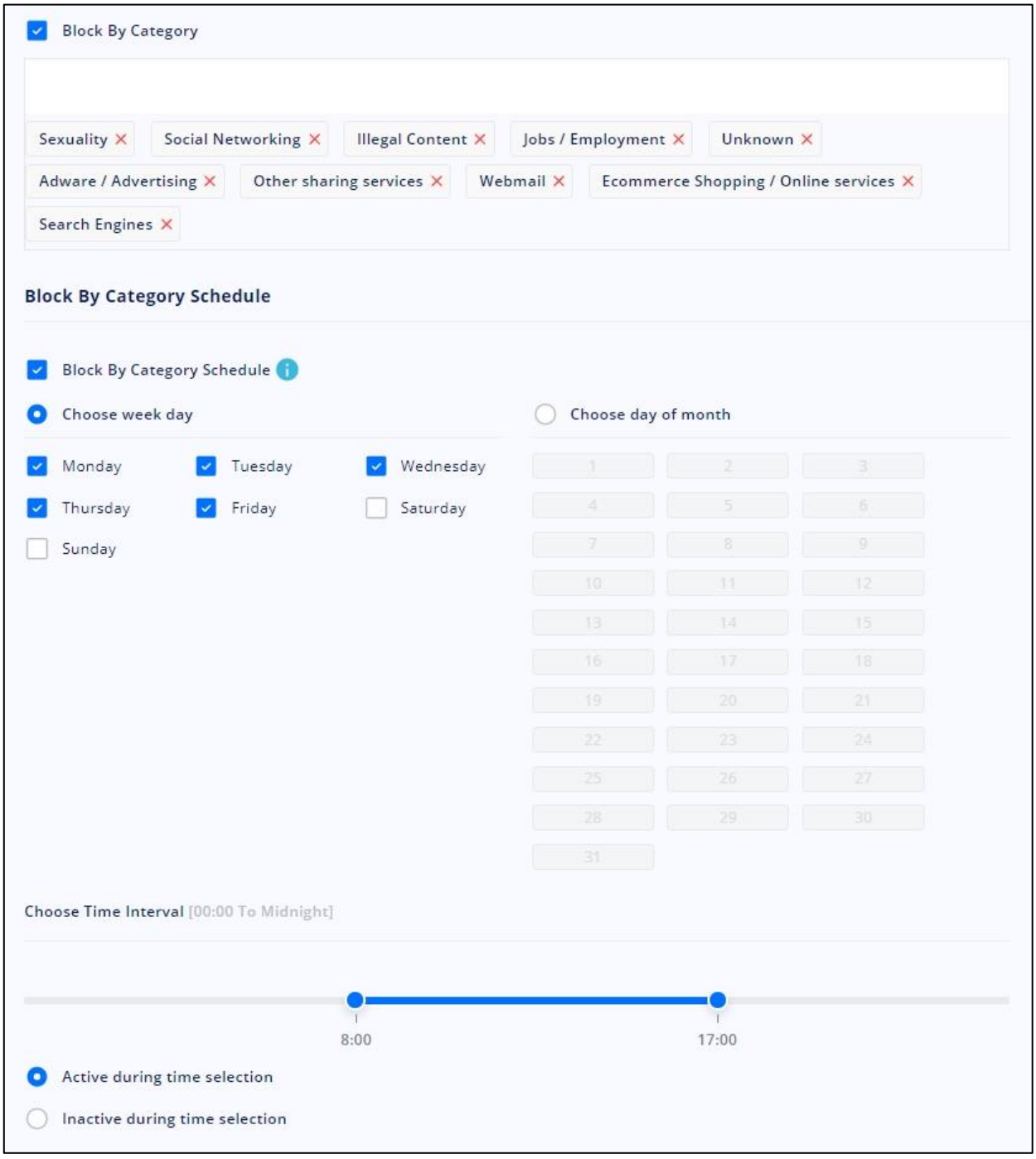
เพื่อให้ระบบทำงานและเริ่มการปกป้องระดับ Advanced Protection ท่านต้องติ๊กเปิดฟังก์ชั่นการทำงานของ DarkLayer Guard และ VectorN Detection



ท่านสามารถตั้งค่า whitelist หรือ blacklist เว็บไซต์ได้โดยติ๊กที่ Domains whitelist และ Domains blacklist ตามลำดับ



ท่านสามารถ**ตั้งค่าบล็อคเว็บไซต์ตาม Category** โดยติ๊กที่ Blocks By Category ซึ่งสามารถปรับแต่งการบล็อคได้ตามหมวดหมู่ที่มีให้สำเร็จรูป และเลือกวันตามสัปดาห์ หรือวันที่ของเดือนตามช่วงเวลาที่กำหนดปรับให้มีผล (active) หรือไม่มีผล (inactive) ได้



หากพบว่าเว็บไซต์บางเว็บไม่ตกอยู่ใน Category ที่มีอยู่ ทั้งๆที่ควรจะอยู่ใน Category นั้น ท่านสามารถ feedback ทางทีมงานเพื่อประสานต่อไปยัง HQ ที่ต่างประเทศ ให้ดำเนินการแก้ไขหรือจัดหมวดหมู่ให้เหมาะสมได้

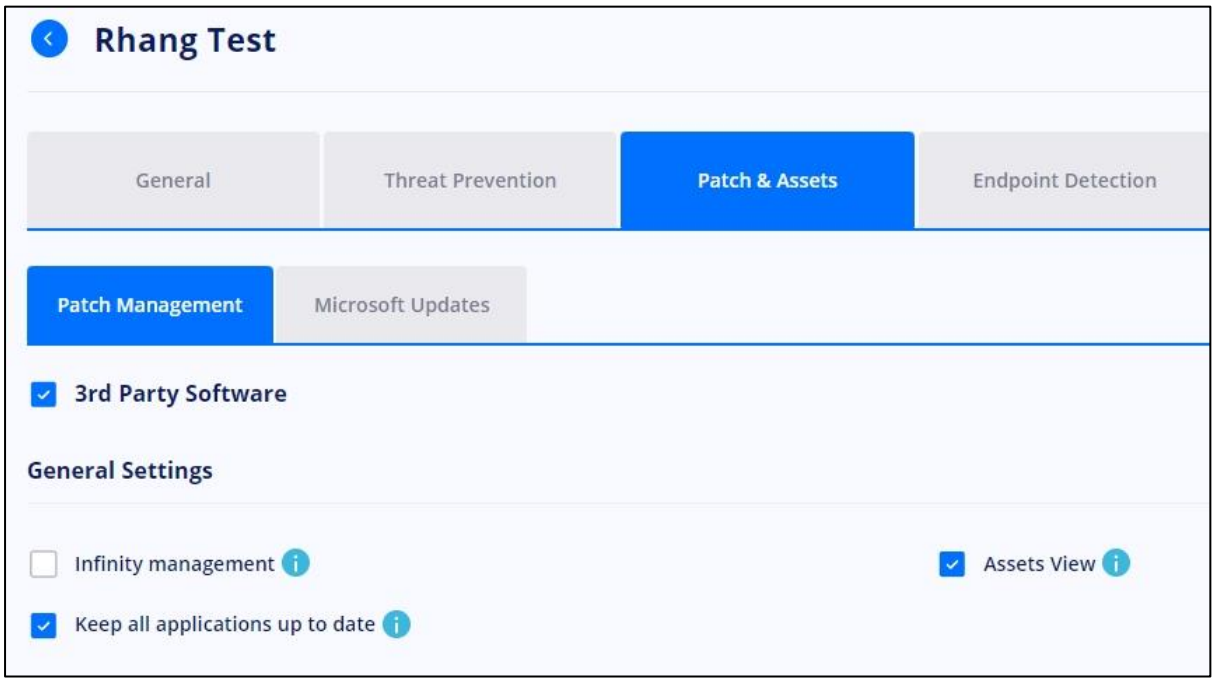
Patch & Assets tab มีค่าพื้นที่ฐานที่ควรต้องทราบดังนี้

หากท่านสั่งซื้อ Patch & Asset Management ไว้ ท่านจะสามารถคลิกที่ Patch & Asset tab ได้ หากท่านไม่ได้สั่งซื้อไว้ tab จะเป็นสีเทาอ่อนและไม่สามารถคลิกได้ (greyed out)

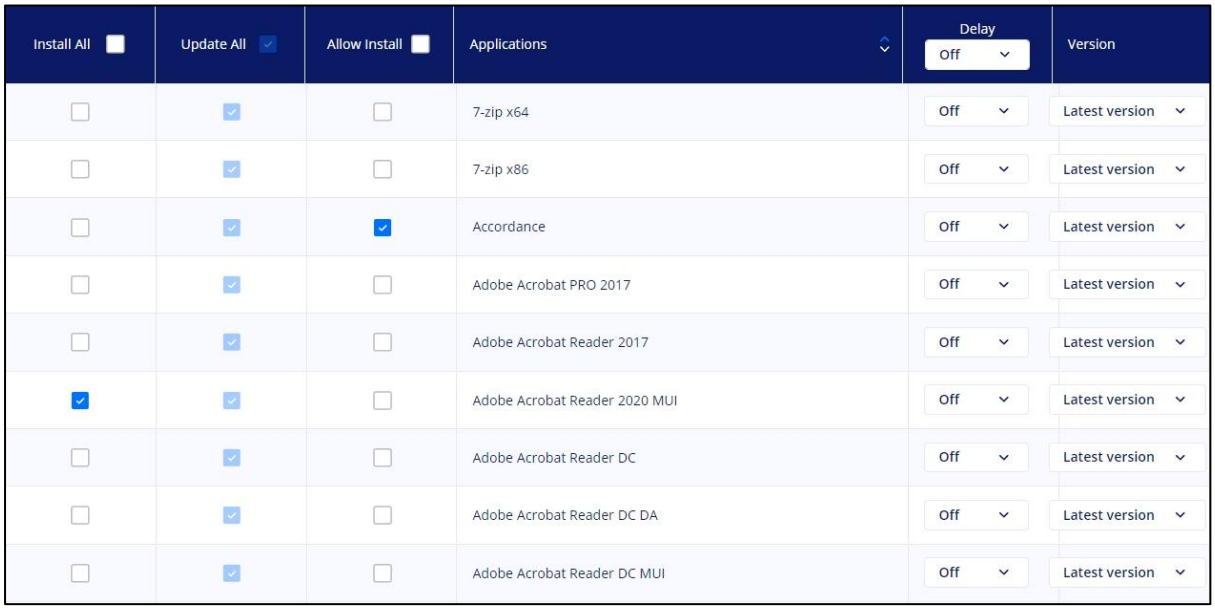
เพื่อที่องค์กรจะมีช่องโหว่ของ software น้อยที่สุด ท่านควรอัพเดท patch ของ software ที่ใช้งานภายในองค์กรอย่างสม่ำเสมอให้มากที่สุดเท่าที่จะกระทำได้ โดยเฉพาะ Patch ที่เกี่ยวข้องกับด้าน Security โดยตรง

Patch Management (tab ย่อย)

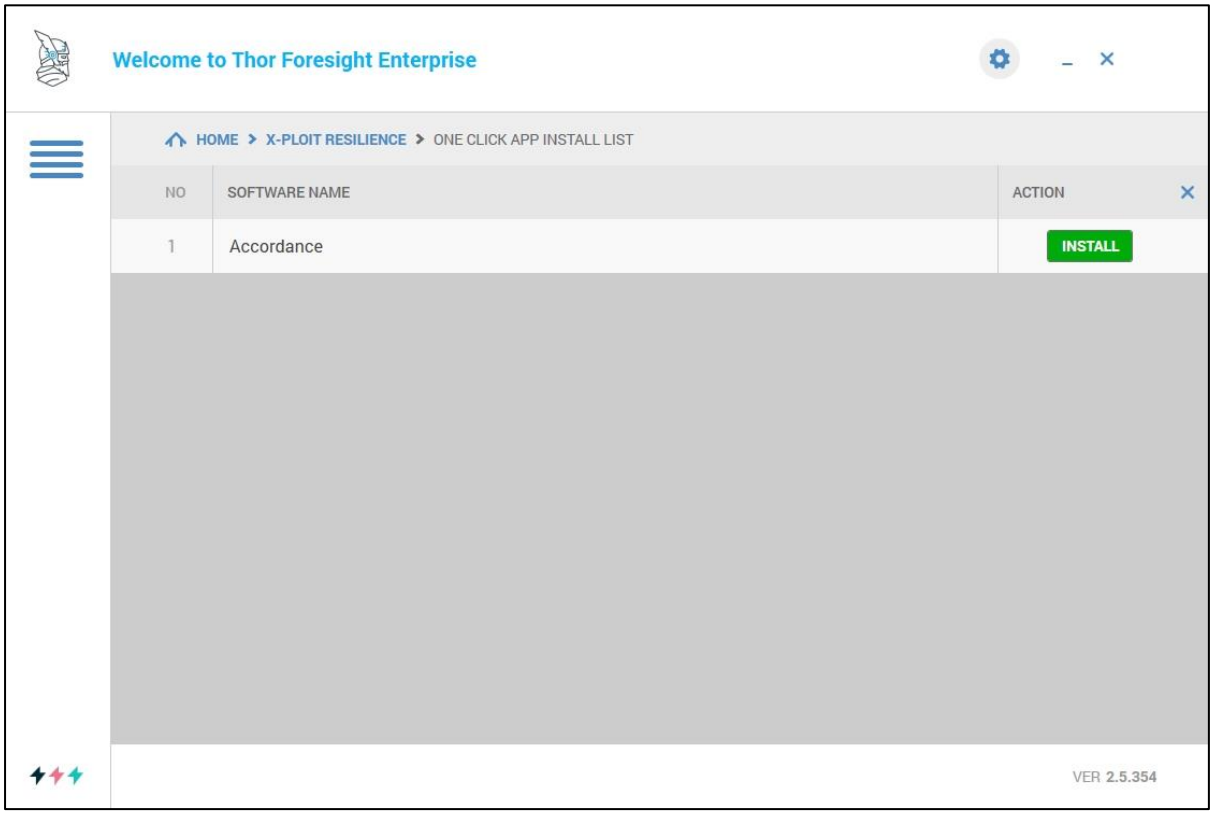
- **Infinity management** เป็นการนำ patch ของท่านเอง (msi, exe หรืออื่น ๆ) ไปใช้แบบ stand-alone ซึ่งสามารถ applied ตาม GP ได้ (เป็น optional module ย่อยที่สามารถซื้อเพิ่มได้ กรุณาติดต่อทีมงาน)
- **3rd Party Software** เปิดใช้งานฟังก์ชั่นอัพเดท patch ของ 3rd party app
- **Keep all applications up to date** อัพเดท 3rd party app ทั้งหมดที่รองรับให้เป็นเวอร์ชั่นล่าสุดโดยอัตโนมัติ สำหรับลิสต์ software คลิก
- **Assets View** เมื่อติ๊กไว้ ท่านจะสามารถ track ทุก application ที่ติดตั้งอยู่บนทุกเครื่องในองค์กรได้



ท่านสามารถกดติดตั้ง 3rd party application ไปยังเครื่องปลายทางโดยอัตโนมัติได้ โดยติ๊กที่ column **Install All** หรือจะทำเป็นลักษณะให้ที่หน้าเครื่องปลายทางคลิกติดตั้งโปรแกรมนั้น ๆ เองจาก HEIMDAL ก็ได้ โดยติ๊กที่ column **Allow Install**

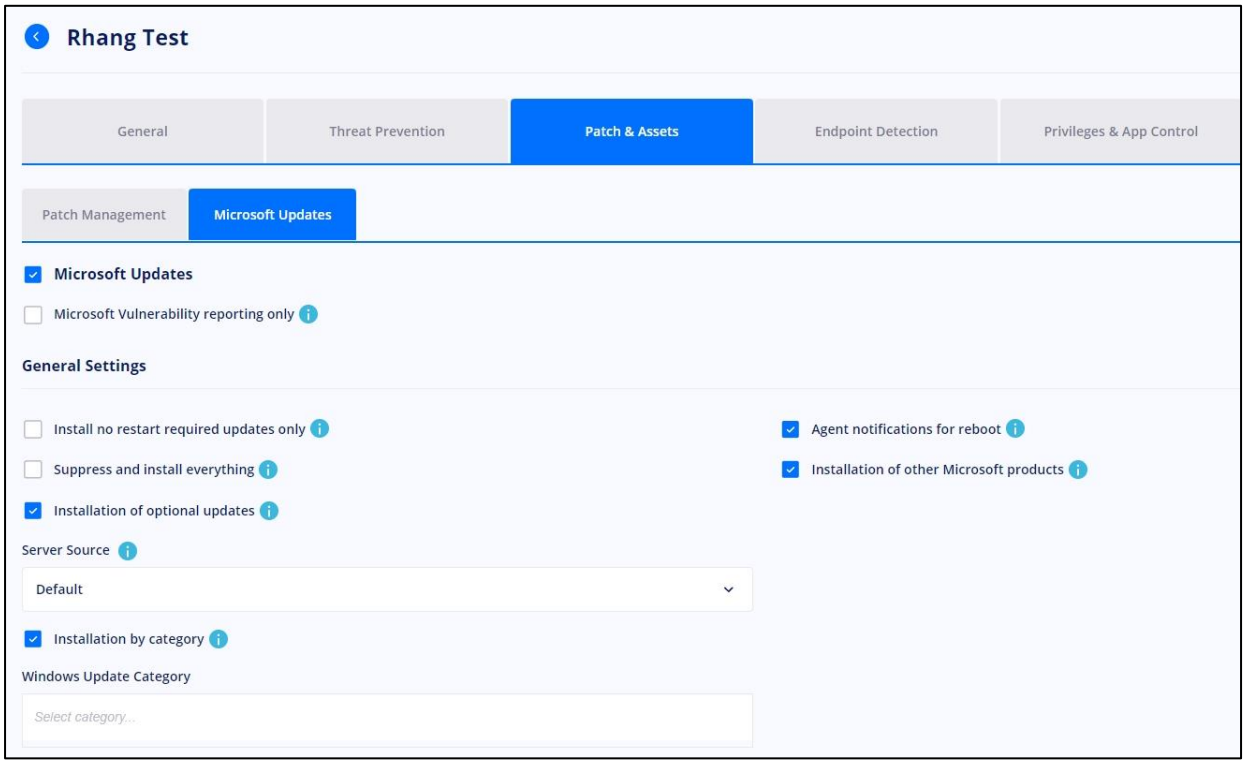


หลังจากคลิก Update GP แล้ว หากที่หน้าเครื่องปลายทางคลิกขวาที่ไอคอน HEIMDAL ที่ด้านล่างขวาหน้าจอ (System Tray) จากนั้นคลิก Show available app จะพบว่าโปรแกรมที่เลือก **Allow Install** จากหน้า dashboard ปรากฏขึ้นมา ท่านสามารถคลิก INSTALL จากหน้าต่างนี้ได้ทันที



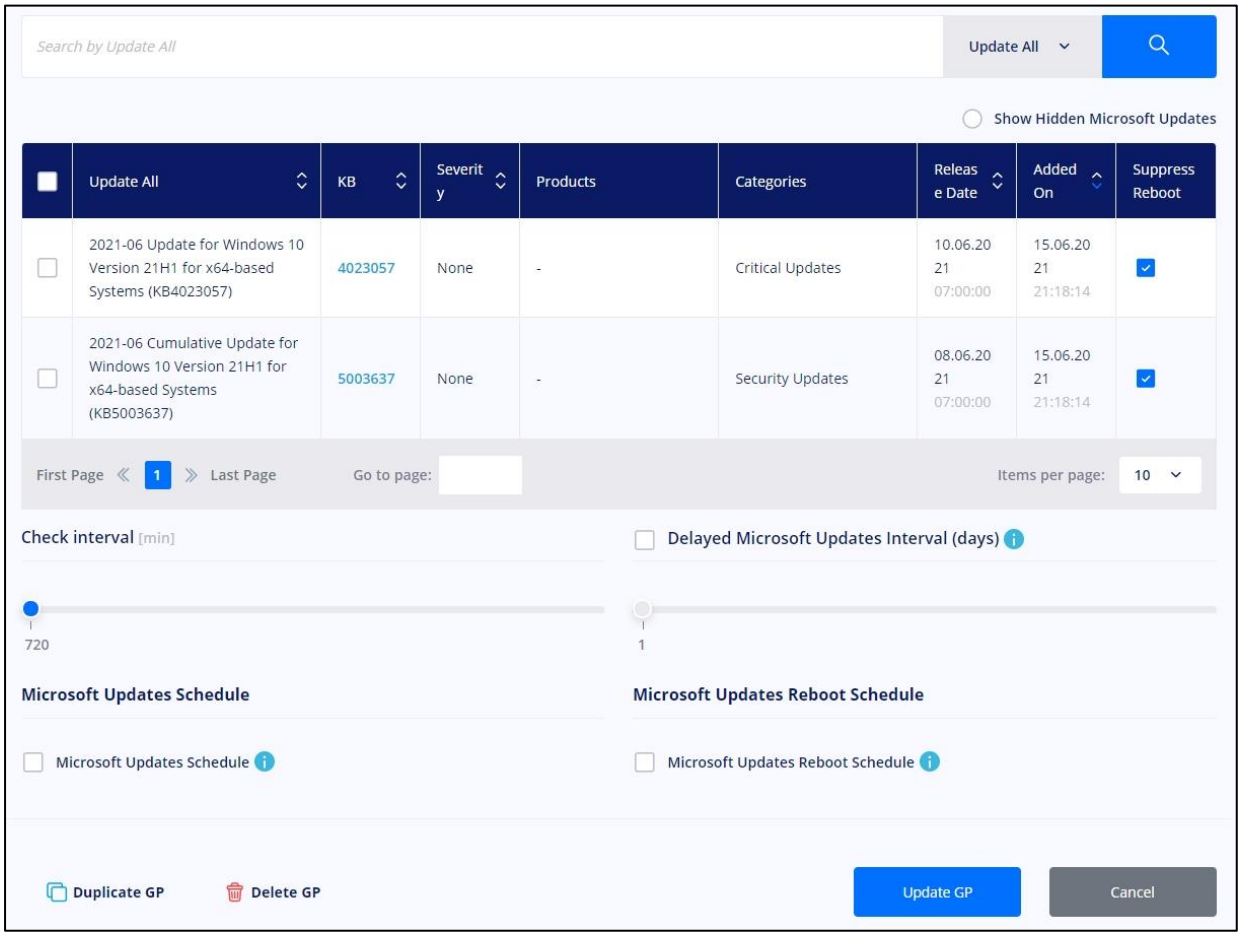
Microsoft Updates (tab ย่อย)

- **Microsoft Updates** เปิดใช้งานฟังก์ชั่น
- **Microsoft Vulnerability reporting only** หากติ๊กที่ช่องนี้จะเป็นการ report available updates เท่านั้น ไม่ทำการ install update ใด ๆ
- **Install no restart required updates only** ติดตั้งเฉพาะ update ที่ไม่ต้อง restart เท่านั้น
- **Suppress and install everything** ติดตั้งทุก update แต่จะไม่ reboot เครื่อง
- **Installation of optional updates** เปิดให้ optional updates ทำงานผ่าน module
- **Agent notifications for reboot** จะมีข้อความขึ้นที่เครื่องให้ reboot เพื่อ apply Microsoft Update ล่าสุด
- **Installation of other Microsoft** products เปิดให้ผลิตภัณฑ์อื่น ๆ ของ Microsoft อัพเดทได้ผ่าน module
- **Installation by category** เลือก install ตาม category จาก drop-down menu



- **Microsoft Update Schedule** กำหนดให้ deploy Microsoft Windows Updates ตามตารางเวลา (เดือน, สัปดาห์, วัน) หรือกำหนดให้ deploy นอกเวลาทำงาน
- **Microsoft Updates Reboot Schedule** กำหนดตารางเวลาสำหรับการ reboot มีผลเฉพาะกับโปรแกรมที่ require reboot

เมื่อตั้งค่าเรียบร้อยแล้ว ให้คลิก Update GP สีน้ำเงินที่มุมล่างขวา



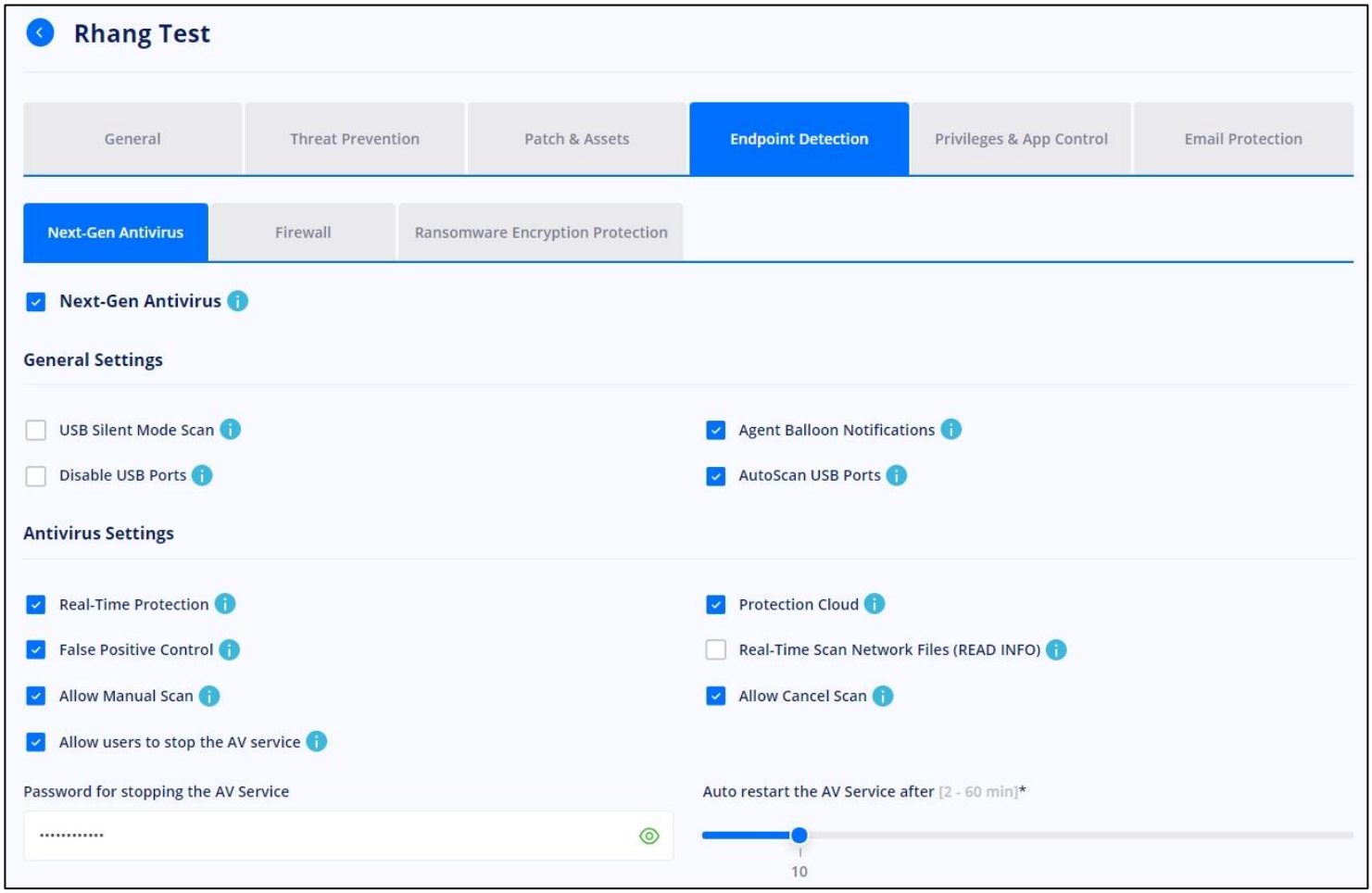
Endpoint Detection tab มีค่าพื้นที่ฐานที่ควรต้องทราบดังนี้

หากท่านสั่งซื้อใน module ของ Endpoint Detection ไว้ ท่านจะสามารถคลิกที่ Endpoint Detection tab และ module tab ย่อยนั้น ๆ ได้ หากท่านไม่ได้สั่งซื้อไว้ tab จะเป็นสีเทาอ่อนและไม่สามารถคลิกได้ (greyed out)

Next-Gen Antivirus (tab ย่อย)

- **USB Silent Mode Scan** สแกนอุปกรณ์หน่วยความจำที่เสียบผ่านช่อง USB โดยอัตโนมัติ โดยไม่มีแสดงผลการสแกนหรือข้อความใด ๆ ปรากฏที่หน้าเครื่อง
- **Disable USB Ports** ปิดการเข้าถึงอุปกรณ์หน่วยความจำทั้งหมดที่เสียบผ่านช่อง USB การจะ activate หรือ deactivate ฟังก์ชั่นนี้ จำเป็นต้อง reboot เครื่องปลายทาง
- **Agent Balloon Notification** เปิดให้มี pop up เด้งขึ้นมาที่หน้าเครื่องเมื่อมีการตรวจจับเกิดขึ้น
- **AutoScan USB Ports** สแกนอุปกรณ์หน่วยความจำที่เสียบผ่านช่อง USB โดยอัตโนมัติ
- **Real-Time Protection** สแกนอุปกรณ์แบบ real-time เพื่อดักจับภัยคุกคามทั้ง known และ unknown ถ้าปิดไว้ จะสามารถสแกนได้เฉพาะแบบ on-demand และ scheduled
- **False Positive Control** โปรแกรมจะแยกแยะการตรวจจับ false positive และป้องกันไม่ให้มีผลกับ performance การสแกน
- **Allow Manual Scan** อนุญาตให้ user สามารถกดสแกนเองได้จาก agent ที่เครื่อง
- **Allow users to stop the AV Service** อนุญาตให้ user สามารถหยุดการทำงานของ AV service ชั่วคราวได้ โดยต้องกรอกรหัสผ่านที่กำหนดในช่องด้านล่างก่อน
- **Password for stopping the AV Service** ตั้งรหัสผ่านสำหรับหยุด AV service จากที่หน้าเครื่องปลายทางชั่วคราว
- **Protection Cloud** ส่ง digital fingerprint ของไฟล์ที่มีพิรุธไปยัง real-time protection cloud เพื่อวิเคราห์ต่อและรอการแจ้งกลับว่าเป็นไฟล์ดีหรือร้าย
- **Real-Time Scan Network Files** เพิ่มประสิทธิภาพ real-time protection แต่อาจส่งผลให้ network performance ช้าลง
- **Allow Cancel Scan** อนุญาตให้ user กดยกเลิกการสแกนเองได้ ซึ่งในแง่ความปลอดภัยแล้ว ไม่แนะนำให้กดยกเลิกการสแกนบ่อยครั้ง
- **Auto restart the AV Service after** ตั้งแต่เวลาหลังจากที่หน้าเครื่องกดปิด AV service ไปแล้ว ระบบจะกลับมาทำงานต่อโดยอัตโนมัติ

(ดูข้อมูลจากหน้าที่แล้ว)



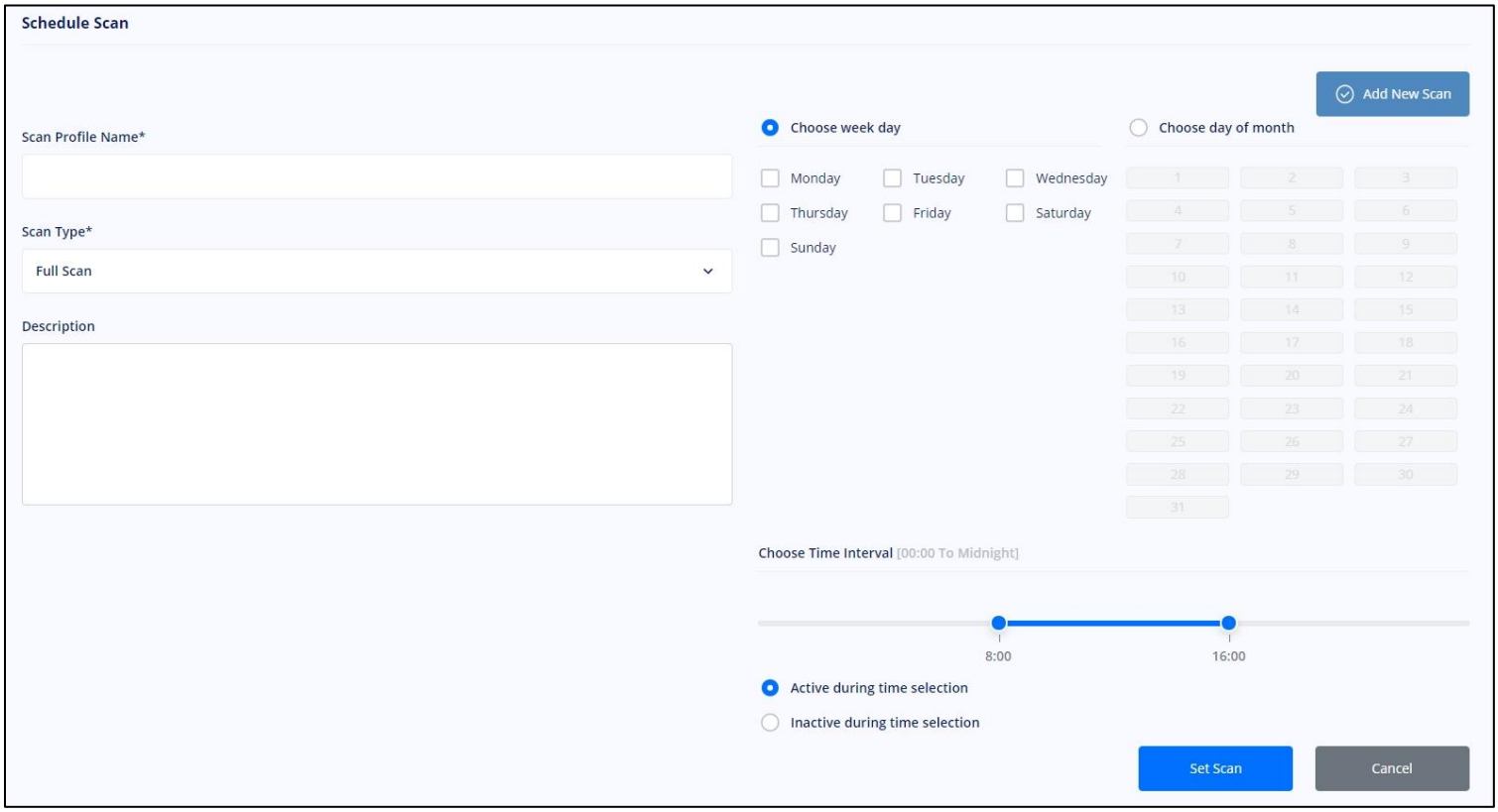
การตั้งค่า **Schedule Scan** ทำได้จากเมนูนี้ ท่านสามารถตั้งค่าให้สแกนตามวันเวลาที่กำหนดได้ โดยสามารถเลือกประเภทของการสแกน (Scan Type) ได้จาก drop-down menu ทางซ้าย ซึ่งจะแบ่งประเภทของการสแกนไว้ 8 รูปแบบ

แน่นอนว่าการ Full Scan นั้นละเอียดที่สุด แต่ใช้เวลานานกว่าการสแกนแบบอื่น ๆ ดังนั้นท่านจึงควรตั้งการสแกนให้เหมาะสมกับสภาพการใช้งานขององค์กรให้มากที่สุด

- **Full scan** – สแกน local files ทั้งหมดบน endpoints (ที่รับ GP นี้)
- **Quick scan** – สแกนเฉพาะบริเวณ critical OS location และ folder ที่มักจะถูกใช้งานจาก malware:

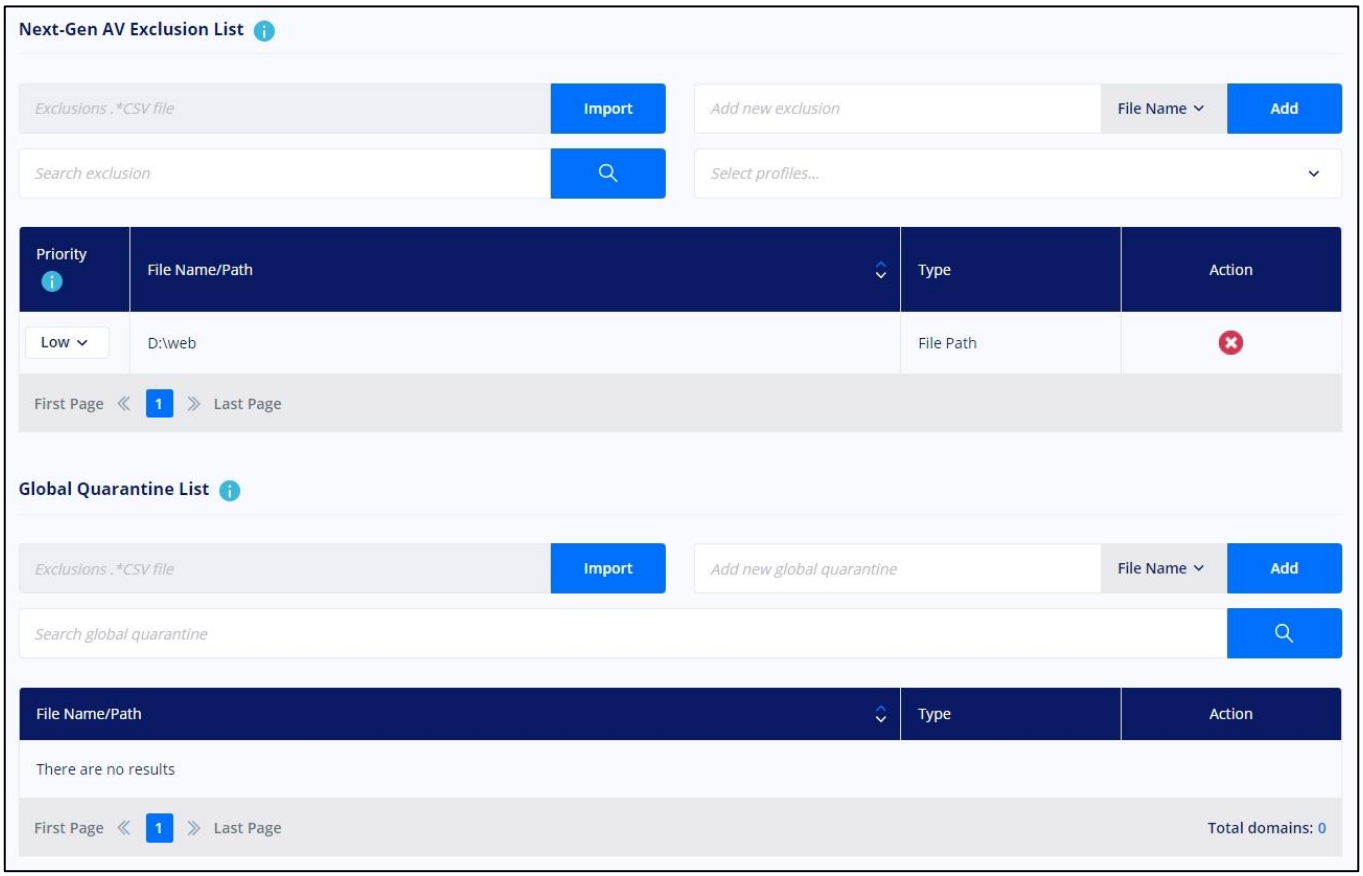
  C:\Program Files\Common Files
  C:\Program Files (x86)\Common Files
  C:\Windows
  C:\Windows\system32
  C:\Windows\SysWOW64

- **Hard Drive scan** – สแกนไฟล์ทั้งหมดบน hard drive โดยไม่สนใจไฟล์บน external media type
- **Local Drive scan** – สแกนไฟล์ทั้งหมดบน local ทั้ง hard drive, optical drive และ external storage
- **System scan** – สแกน system directory
- **Removable Drive scan** – สแกนไฟล์เฉพาะ external drive, optical drive
- **Network Drive Scan** – ทำงานได้เฉพาะกับ Mapped network drive
- **Active Processes Scan** – สแกนเฉพาะ process ที่กำลังทำงานอยู่ในเครื่อง



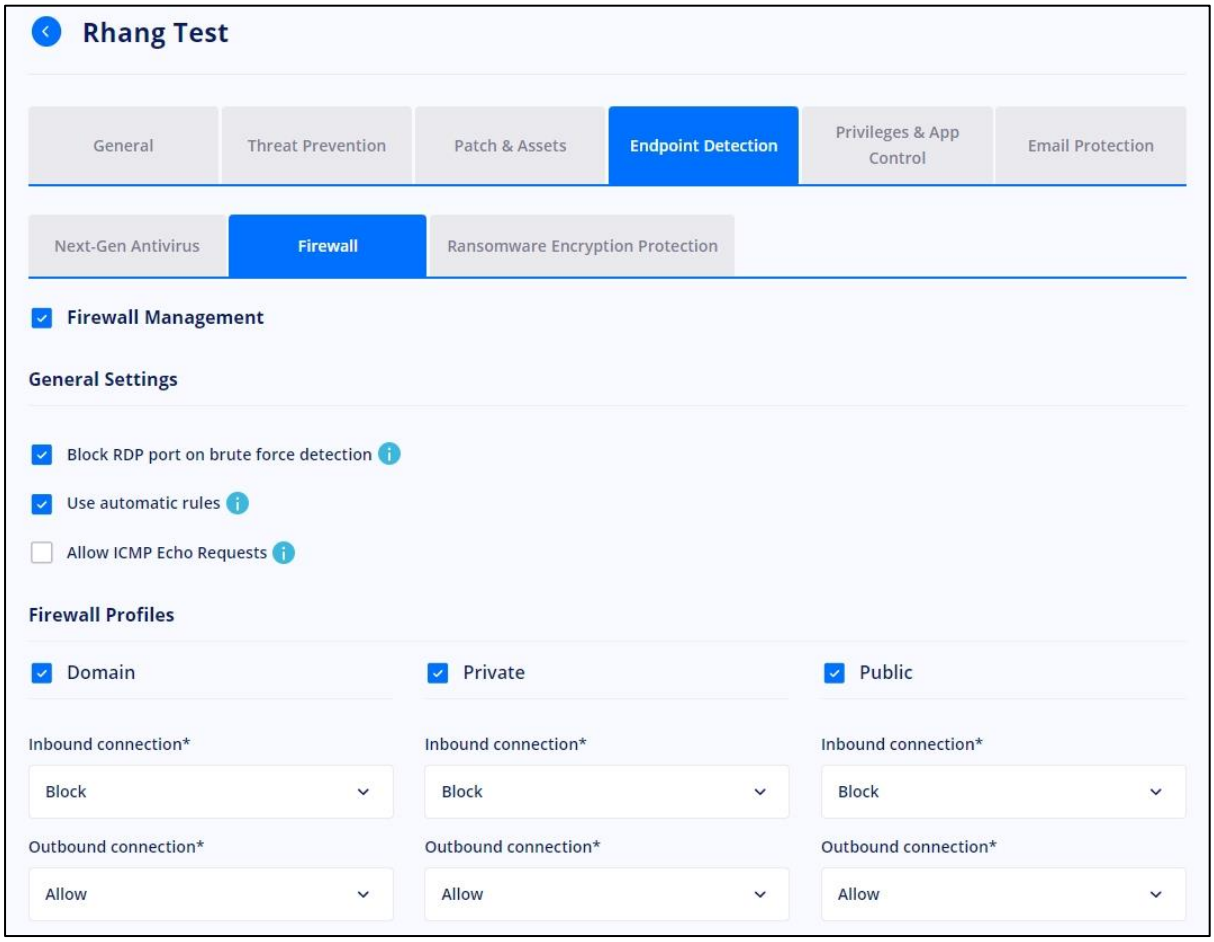
ตาราง **Next-Gen AV Exclusion List** ใช้สำหรับระบุ File Name หรือ File Path ที่เราต้องการกำหนดให้ไม่ถูก scan โดยระบบ antivirus

ตาราง **Global Quarantine List** จะเป็นการกำหนดชื่อไฟล์หรือไฟล์ที่อยู่ใน path ที่กำหนดให้ถูกส่งไปอยู่ใน quarantine ของ antivirus โดยอัตโนมัติ



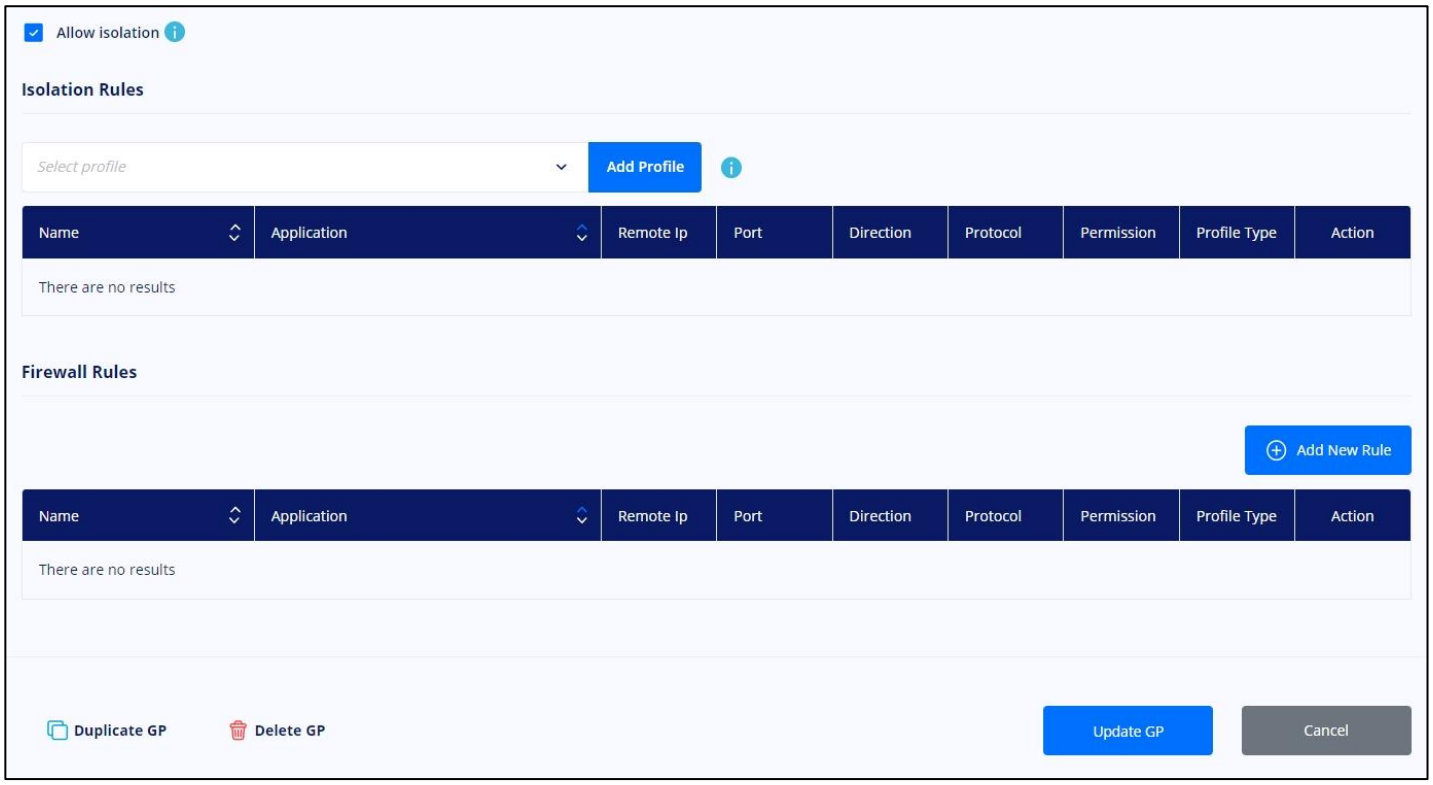
Firewall (tab ย่อย)

- **Firewall Management** เปิดการจัดการ firewall ผ่าน cloud ส่วนกลาง
- **Block RDP port on brute force detection** บล็อค RDP port 3389 เมื่อตรวจสอบเทคนิคการโจมตี brute force ถ้ามีการเปลี่ยน default RDP port ฟังก์ชั่นนี้จะไม่ active
- **Use automatic rules** สามารถตั้ง inbound/outbound connection ได้จากเมนูด้านล่าง
- **Allow ICMP Echo Requests** สร้าง firewall rule ที่อนุญาตให้ ping request ในnetwork



Allow isolation อนุญาตให้ user สามารถทำการ isolate endpoint โดยเมื่อ isolate แล้ว การเชื่อมต่อทั้งหมดสู่ภายนอกจะถูก rerouted ผ่าน service ของ HEIMDAL

สำหรับ **Firewall Rules** ท่านสามารถคลิกที่ Add New Rule แล้วปรับค่าตามที่ต้องการใช้งาน เมื่อตั้งค่าเรียบร้อยแล้ว ให้คลิก Update GP สีน้ำเงินที่มุมล่างขวา

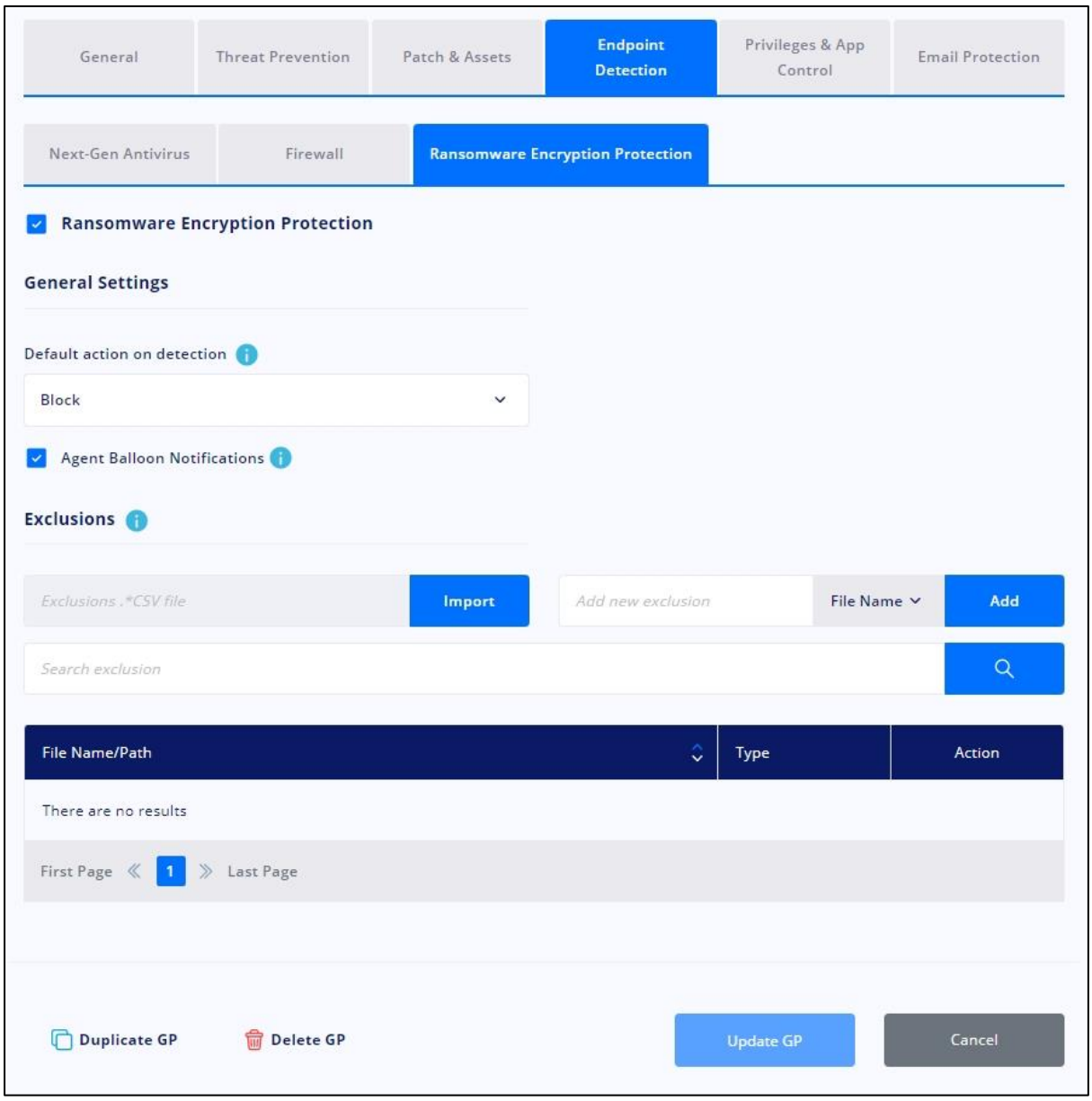


Ransomware Encryption Protection (tab ย่อย)

- **Ransomware Encryption Protection** เปิดการทำงานของ module
- **Default action on detection** ปรับเป็น block เพื่อให้ระบบทำการบล็อคการทำงานของ Encryption ที่น่าสงสัย โดยปกติแล้ว ระบบจะอนุญาตการ encrypt 1-3 ไฟล์แรก ให้ทำงานเป็นปกติไปก่อน จากนั้นจึงบล็อคเมื่อแน่ใจแล้วว่าผิดปกติ
- **Agent Balloon Notifications** เมื่อตรวจพบการ encryption ที่ผิดปกติ จะมี pop up แจ้งเตือนที่หน้าเครื่องปลายทาง

ท่านสามารถตั้งค่า exclusion หรือยกเว้นการตรวจจับจาก File Path หรือ File Name ได้จากตารางด้านล่าง

เมื่อตั้งค่าเรียบร้อยแล้ว ให้คลิก Update GP สีน้ำเงินที่มุมล่างขวา

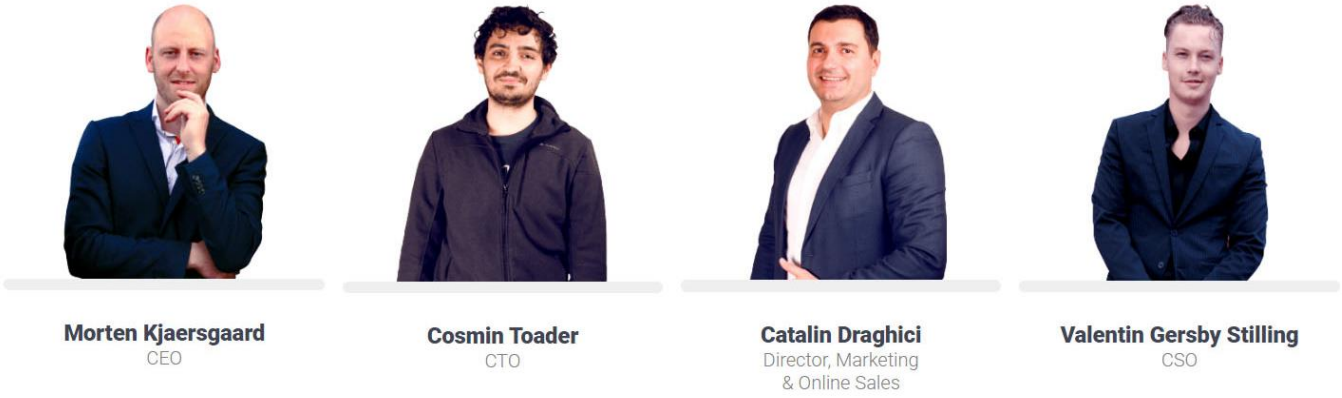


ทางทีมงานขออนุญาตแนะนำว่า **หากต้องการให้ระบบ Cyber Security องค์กรของท่านปลอดภัยสูงสุด**จาก Ransomware รวมถึง Advanced Malware ชนิดอื่นๆ ควรกระทำดังนี้

- **ให้ความรู้ security awareness กับ end user** ให้รู้จักแยกแยะ phishing มีความระมัดระวังในการกรอกข้อมูล คลิกลิ้งค์หรือดาวน์โหลดไฟล์
- **เลือกใช้ระบบ antivirus และ security ขั้นสูงเพิ่มเติม**ให้เหมาะสมกับการใช้งานขององค์กร รุ่น antivirus ระดับการป้องกันพื้นฐาน (Next-Gen Antivirus) จะเน้นป้องกัน malware ด้วยระบบฐานข้อมูลและระบบ real-time protection เป็นหลัก ซึ่งแม้จะมีความสามารถในการป้องกัน malware ทั้ง known และ unknown แต่ถ้าเป็น malware ตัวที่ใช้ pattern การโจมตีใหม่ (zero-day), fileless หรือประเภทขั้นสูง (APTs) รวมถึง ransomware ชนิดใหม่ ๆ ควรใช้การป้องกันหลายชั้นยิ่งขึ้น จึงมีความ secure ที่วางใจได้มากกว่า (Threat Prevention, Ransomware Encryption Protection)
- **ติดตั้งระบบ security บนทุกเครื่องที่เข้าถึงไฟล์แชร์กันได้** (ไม่ว่าจะ read only หรือ read & write) ไม่ควรติดตั้งเฉพาะบนเครื่อง server หรือบางเครื่องใน network ซึ่งอาจมีไฟล์แชร์ถึงกันบนเครื่อง client แต่เครื่อง client ไม่มีระบบ security ที่เพียงพอ หรือ ปิดการอัพเดท หรือใช้คนละแบรนด์กัน อาจนำมาซึ่งช่องโหว่ของระบบได้
- **ตั้งค่า Schedule Scan** สัปดาห์ละครั้งหรือเดือนละครั้งเป็นอย่างน้อย **(ดูหน้า 25)**
- **ตั้งค่าให้ระบบ security ไม่สามารถถูกปิดการทำงาน**โดย malware หรือ user ทั่วไป กรณี hacker เจาะระบบเข้ามาได้ โดยปกติจะพยายามหยุดการทำงานของ antivirus ก่อน จึงควรตั้งค่าป้องกันไว้ **(ดูหน้า 15 และ 23)**
- **ตั้งค่าให้ระบบ security ต้องใช้ password ในการถอนการติดตั้ง** และไม่จด password ทิ้งไว้ในเครื่อง **(ดูหน้า 15)**
- **ตรวจสอบการตั้งค่าของระบบ security** ว่าฟังก์ชั่นที่จำเป็นนั้นถูกเปิดใช้งานแล้ว
- **ควรอัพเดท security patch** ของ OS และ 3rd party application ที่ติดตั้งในเครื่องให้เป็นล่าสุดอยู่เสมอ (สามารถใช้ patch management ช่วยบริหารจัดการได้ **ดูหน้า 19**)
- **ปิด RDP หากไม่มีความจำเป็นต้องใช้** หรือถ้าต้องใช้ ให้ภายนอกต้องผ่าน VPN เข้ามาก่อนจะเข้าถึงเครื่อง และ user ที่ใช้ RDP ควรมีสิทธิ์เป็น user ธรรมดา ไม่ควรมีสิทธิ์เป็น Admin และเปิดฟังก์ชั่น **(ดูหน้า 27)**
- **หมั่นทำการสำรองข้อมูล (backup) ไว้เสมอ** โดยเก็บไว้ในอุปกรณ์แยกจากระบบหลัก ไม่เสียบคาไว้ที่เครื่อง หรือสามารถเข้าถึงได้ตลอดเวลา หรือใช้บริการบน cloud
- **เลี่ยงการใช้โปรแกรมที่ไม่มีลิขสิทธิ์** ไฟล์จำพวก crack, keygen, loader อาจนำมาซึ่งช่องโหว่หรือภัยคุกคามอื่น ๆ ได้ รวมถึงเลี่ยง add-on หรือ extension ต่าง ๆ ของ web browser ที่ไม่จำเป็นต้องใช้ แต่หากจำเป็นต้องใช้ สามารถตั้ง exclusion ของแต่ละ module ได้
- **ตรวจสอบโปรแกรม security ที่ติดตั้งอยู่ทุกเครื่องมีสถานะทำงานเป็นปกติและอัพเดทเป็นปัจจุบัน** โดยตรวจสอบได้จากบน dashboard หรือการแจ้งเตือนที่หน้าเครื่อง

โดยผลิตภัณฑ์ของ HEIMDAL มี solution รองรับองค์กรทุกรูปแบบ (ยกเว้น on-premise) ตามงบประมาณ ไม่ว่าจะเรื่องป้องกัน advanced malware, ransomware , patch หรือ tools เสริมในการป้องกัน

Who is HEIMDAL™ Security?



ในปี 2011 ทีมผู้ก่อตั้งได้เข้าร่วมการแข่งขัน World Hacking Championships - Def Con Capture The Flag ซึ่งมีทีมหัวกะทิเข้าร่วมแข่งขันมากมาย เช่น FBI, NSA, freelancer และบริษัทด้าน Security ขนาดใหญ่หลายแห่ง ทางทีมได้ชนะการแข่งขันในปี 2011 และ 2012 เป็น 2 ปีติดต่อกัน

ต่อมาจึงได้ได้ก่อตั้งแบรนด์ HEIMDAL ในปี 2014 โดยเน้นที่ Proactive Cloud-Based Cybersecurity Technology ที่ Copenhagen ประเทศ Denmark ปัจจุบันเป็นผู้นำด้าน proactive threat prevention ซึ่งเทคโนโลยี threat intelligence ได้รับการชื่นชมจาก FBI, ได้รับการรับรองจาก Danish Cybercrime Police และได้รับการแนะนำโดย Royal Bank of Scotland ว่าเป็น "preferred cyber security solution" ปัจจุบัน HEIMDAL ทำการปกป้องภัยคุกคามทางไซเบอร์ให้กับองค์กรมากกว่า 6,000 แห่ง รวมมากกว่า 1,000,000 endpoints และเติบโตขึ้นอย่างรวดเร็วทุกปี ข้อมูลเพิ่มเติม [คลิก]