

# HEIMDAL™

## SECURITY

**คู่มือแนะนำการใช้งาน "เทพไฮมดัล" เบื้องต้น**



## สารบัญ

หัวข้อ	เลขหน้า
ตรวจสอบก่อนติดตั้ง	3
ทำความรู้จักแต่ละ Module หลักแบบคร่าว ๆ	5
ขั้นตอนการติดตั้ง	7
การสร้าง account เพิ่ม	9
Main Dashboard	10
การดู Active Clients บน dashboard	11
การสร้าง Group Policy (GP)	12
การกำหนด Active Clients มารับ Group Policy (GP) ที่ตั้งไว้	13
การตั้งค่า Group Policy เบื้องต้น	14
General tab	15
Threat Prevention tab	17
การตั้งค่าบล็อกเว็บไซต์ตาม Category	18
Patch & Assets tab	19
Patch Management	19
Microsoft Updates	21
Endpoint Detection tab	23
Next-Gen Antivirus	23
การตั้งค่า Schedule Scan	25
Firewall	27
Ransomware Encryption Protection	29
<b>คำแนะนำให้ระบบปลอดภัยสูงสุด</b>	<b>30</b>
Who is HEIMDAL™ Security?	31



## 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 ไม่ถูกล็อคโดย 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



### 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 และฟีเจอร์พื้นฐานที่ควรต้องมีครบถ้วน สำหรับการใช้งานในองค์กร ได้แก่ Schedule Scan, Device Control, Centralized Firewall, Enforce Password for Uninstallation

**HEIMDAL™**  
Threat Prevention - Endpoint



### HEIMDAL™ Threat Prevention – Endpoint

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

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



**HEIMDAL™**  
Patch & Asset Management



## HEIMDAL™ Patch & Asset Management

ลิสต์ software ที่ติดตั้งอยู่บนทุกอุปกรณ์ อดช่องโหว่ของระบบและ software ต่างๆ ด้วย X-Ploit Resilience อัปเดต 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](#) (สามารถใช้งานร่วมกับ 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

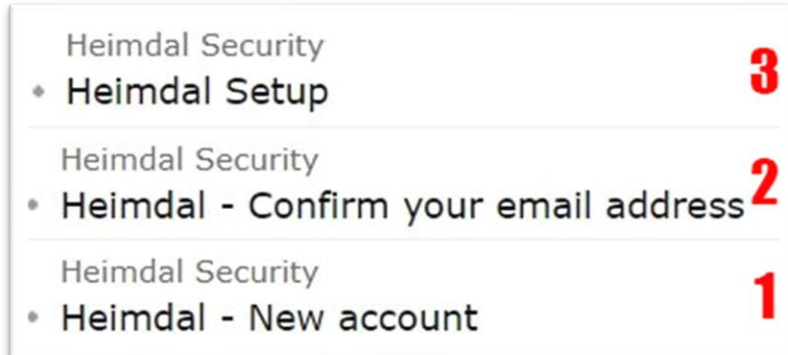
## HEIMDAL™ Ransomware Encryption Protection

module สำหรับการวิเคราะห์ process โดยโฟกัสที่การบล็อก encryption จากพฤติกรรมที่มีพิรุขของ ransomware บนทุกเครื่องที่มีติดตั้ง module นี้ไว้ (สามารถใช้งานร่วมกับ antivirus ยี่ห้ออื่น รวมถึงตัวฟรีทั้งหมด)



## ขั้นตอนการติดตั้ง

### 1. เช็ค inbox ในอีเมล



### 2. copy รหัสจากข้อความในอีเมลที่ 1

### 3. กดลิงค์เพื่อยืนยันอีเมลจากในอีเมลฉบับที่ 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 สามารถดูข้อมูลได้จากลิงค์ต่อไปนี้

- [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

The screenshot shows the Heimdal Security dashboard. On the left is a navigation menu with 'Accounts' highlighted. The main content area is titled 'Accounts' and shows a table with 7 listings. A red box highlights the 'Create New Account' button in the top right corner of the table area.

Email	Name	Customer	Currency	Activated	Roles
[blurred]	[blurred]	[blurred]	USD	✓	[blurred]
[blurred]	[blurred]	[blurred]	USD	✓	-
[blurred]	[blurred]	[blurred]	USD	✓	[blurred]
[blurred]	[blurred]	[blurred]	USD	✓	-
[blurred]	[blurred]	[blurred]	USD	✓	-
[blurred]	[blurred]	[blurred]	EUR	✓	[blurred]
[blurred]	[blurred]	[blurred]	USD	✓	-

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

The 'New Account' form is divided into several sections:

- Basic Info:** Login email\*, Customer\* (dropdown), Time zone\* (dropdown), Currency\* (dropdown).
- Personal Information:** Name, Phone Number.
- Miscellaneous Settings:**
  - Roles:** Reseller (checked), Visitor.
  - Additional Settings:** Do not Require 2-Factor.
  - IP List:** Single IP, IP Range (checked), List of IPs. Includes an 'Add New IP' button and a table with columns for IP and Action.

At the bottom, there are 'Create Account' and 'Cancel' buttons.



## Main Dashboard

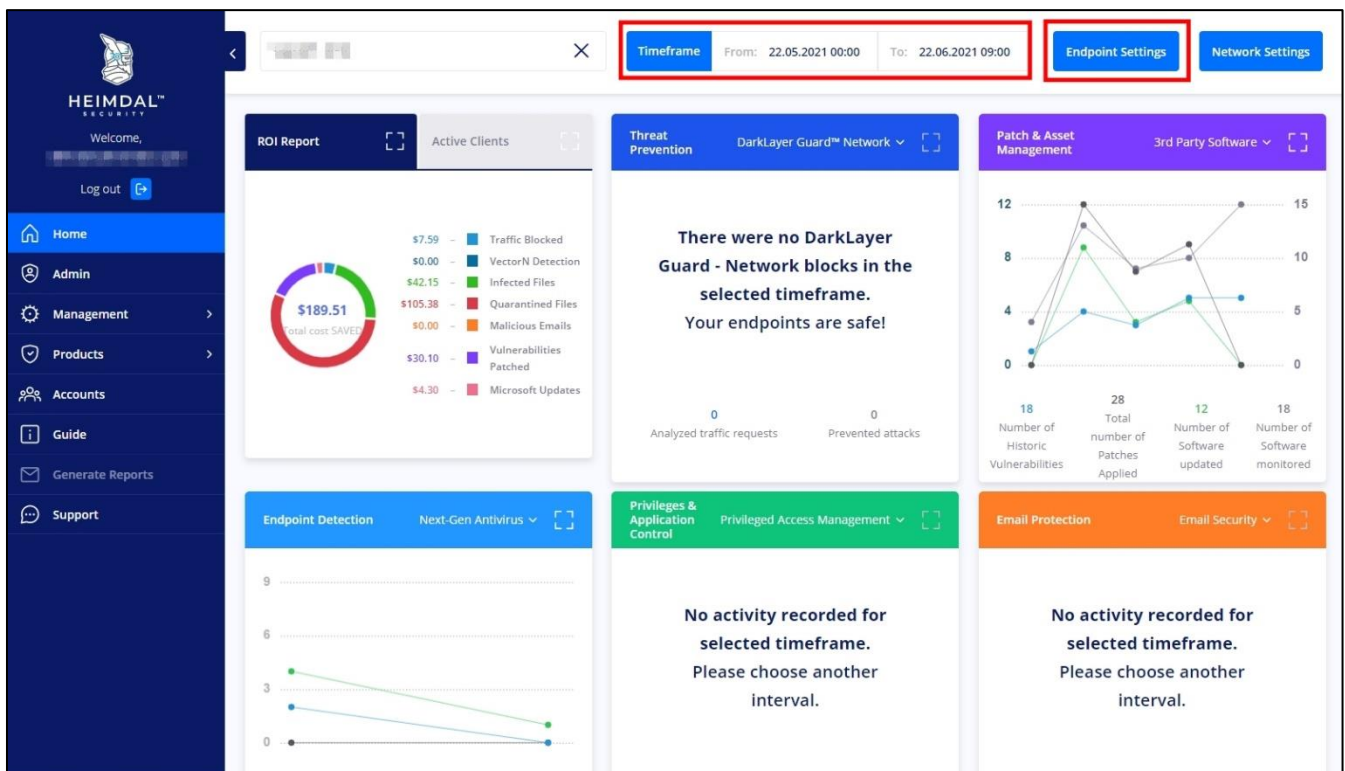
### Timeframe

บริเวณด้านบนหน้าหลักของ dashboard จะมี Timeframe ให้เลือกช่วงเวลาการแสดงผลข้อมูลของบนหน้านั้น ๆ ที่กำลังเปิดอยู่

ท่านสามารถคลิกที่แต่ละช่วงเวลาของกราฟแต่ละ module เพื่อดูรายละเอียดเพิ่มเติมตามช่วงเวลาที่กำหนดได้

### ROI Report

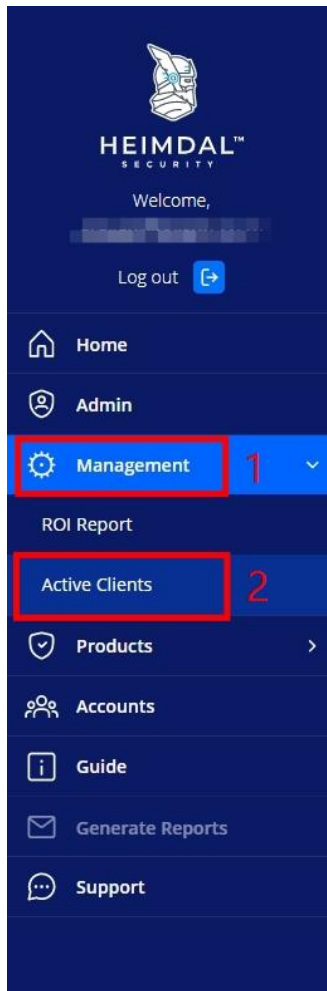
เป็นตัวเลขที่ทำให้เห็นถึงมูลค่าผลตอบแทนการลงทุนที่ HEIMDAL ได้ทำการป้องกันความเสียหายไว้ให้ ด้วยการปกป้องผู้ใช้งานและข้อมูลในระบบให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้หากไม่ได้ติดตั้ง HEIMDAL ไว้ก่อน





## 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 สำหรับกรองข้อมูลที่มบบนขวาทาราง



Hostname	Username	IP address	Version	Operating System	Current GP	Selected GP	Last Seen	Enabled Modules	Status
DESKTOP-AROM	arom	192.168.1.34	2.5.354	Microsoft Windows 10 - x64	Test	Test	18.06.2021 18:07:34	9 Modules >	🟡
RAABYHOMEPC	win 10	192.168.1.49	2.5.360 RC	Microsoft Windows 10 - x64	For Rabby home PC	Automatic	18.06.2021 15:48:45	8 Modules >	🟡
OPPO CPH2173	OPPO Find X3 Pro	192.168.1.35	2.1.6	Android 11	Rhang Test Android	Automatic	18.06.2021 14:59:43	4 Modules >	🟢
RHANGNEW	TUF	192.168.1.43	2.5.354	Microsoft Windows 10 - x64	Rhang Test	Rhang Test	18.06.2021 14:24:45	10 Modules >	🟡
WIN-PH8AQ2PAR	Administrator	10.0.2.15	2.5.300 RC	Microsoft Windows Server 2016 Datacenter - x64	For Rabby home PC	Automatic	18.06.2021 14:10:06	8 Modules >	🟡
WIN7-PC	win7	10.0.2.15	2.5.360 RC	Microsoft Windows 7 - x64	Test	Test	18.06.2021 10:08:19	9 Modules >	🟡
MRRHANG	MrRhang	192.168.1.36	2.5.354	Microsoft Windows 10 - x64	Rhang Test	Rhang Test	17.06.2021 22:19:10	10 Modules >	🟡
Skysofts-Air	skysoft	192.168.1.51	2.5.9	macOS - x64	Custom	Automatic	17.06.2021 21:33:20	4 Modules >	🟡
WIKO W-V755-TVM	Power USB Nat	192.168.1.63	2.1.6	Android 11	Custom	Rhang Test Android	01.06.2021 17:55:56	3 Modules >	🟢

Hostname	CPU	CPU %	Memory	Memory %	Disk	Disk %	Last Seen	Status
DESKTOP-AROMarom	Intel(R) Pentium(R) CPU J3710 @ 1.60GHz	20	4 GB	90	465 GB	23	18.06.2021 16:07:34	🟡
RAABYHOMEPCwin 10	Intel(R) Pentium(R) CPU G4500 @ 3.50GHz	53	8 GB	90	323 GB	9	18.06.2021 15:48:45	🟡
OPPO CPH2173OPPO Find X3 Pro	-	-	-	-	-	-	18.06.2021 14:59:43	🟢
RHANGNEWTUF	AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx	14	16 GB	61	476 GB	4	18.06.2021 14:24:45	🟡
WIN-PH8AQ2PARAdministrator	AMD Ryzen 5 4600H with Radeon Graphics	23	-	51	49 GB	5	18.06.2021 14:10:06	🟡
WIN7-PCwin7	Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz	14	-	69	113 GB	1	18.06.2021 10:08:19	🟡
MRRHANGMrRhang	AMD Ryzen 5 3600 6-Core Processor	12	16 GB	65	931 GB	1	17.06.2021 22:19:10	🟡
Skysofts-Airskysoft	Dual-Core Intel Core i5	-	8 GB	-	-	-	17.06.2021 21:33:20	🟡
WIKO W-V755-TVMPower USB Nat	-	-	-	-	-	-	01.06.2021 17:55:56	🟢

column ขวาสุดของตารางรายชื่อเครื่อง จะเป็นสัญลักษณ์พร้อมเครื่องหมายสีเขียวหรือสีส้ม เมื่อคลิกจะเป็นการแสดงสถานะของเครื่องนั้น ๆ ว่าติดตั้งเรียบร้อยดีหรือมี notice สำคัญอะไร อยู่บ้าง ท่านสามารถดูรายละเอียดของข้อมูลสถานะต่าง ๆ ได้จาก [คลิก](#)

Notifications			
Hostname: RHANGNEW    Last Active Username: TUF    Last Seen: 18.06.2021 14:24:45			
Details	Started Timestamp	Dismiss	Status
The memory is running at 61 %	18.06.2021 14:24:48	-	🟡
The machine needs a reboot to complete the Microsoft Update.	18.06.2021 09:09:52	-	🟡
Close			



## 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 ใดเป็น Automatic ระบบจะทำการเลือกใช้ GP ที่มี Priority สูงที่สุด (เลขมากที่สุด) โดยอัตโนมัติ

คลิกที่ชื่อ GP เพื่อเข้าสู่การตั้งค่าสำหรับ GP นั้น ๆ โดยท่านอาจจะแบ่งเป็นฝ่าย เป็นแผนก หรือ แบ่งตามลักษณะการใช้งานตามแต่นโยบายขององค์กร

หลังจากตั้งค่า GP ตามที่ต้องการใช้เรียบร้อยแล้ว ต้องกำหนด Active Clients ให้มารับ GP ด้วย

Search by Policy Name Policy Name

A Total of: 4 Listings  Group policies inheritance

Policy Name	AD Computer Group	AD User Group	Priority	Status	Action
For Rabby home PC	-	-	6	Enabled Disabled	<input type="button" value="Duplicate"/>
Rhang Test	-	-	5	Enabled Disabled	<input type="button" value="Duplicate"/>
Test	Test AD Computer Group	Test AD User Group	2	Enabled Disabled	<input type="button" value="Duplicate"/>
Default	-	-	1	Enabled Disabled	<input type="button" value="Duplicate"/>



## การกำหนด Active Clients มารับ Group Policy (GP) ที่ตั้งไว้

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

The screenshot displays the 'Active Clients' management page. The left sidebar contains navigation options: Home, Admin, Management (1), ROI Report, Active Clients (2), Products, Accounts, Guide, Generate Reports, and Support. The main content area shows a summary of 1 Active servers, 14 Active endpoints, and 15 Total devices. Below this is a search bar and a table of active clients. The table has columns: Hostname, Username, IP address, Version, Operating System, Current GP, Selected GP, Last Seen, Enabled Modules, and Status. A red box highlights the 'Management' menu item (1), the 'Active Clients' menu item (2), a checkbox in the first row (3), the 'Automatic' dropdown menu (4), and the 'Apply to specific GP' button (5).

Hostname	Username	IP address	Version	Operating System	Current GP	Selected GP	Last Seen	Enabled Modules	Status
<input checked="" type="checkbox"/> WIN-P9HIIAO2PAR	Administrator	10.0.2.15	2.5.360 RC	Microsoft Windows Server 2016 Datacenter - x64	For Rabby home PC	Automatic	21.06.20 21:12:19:10	8 Modules >	!
<input type="checkbox"/> RAABYHOMEPC	win 10	192.168.1.49	2.5.360 RC	Microsoft Windows 10 - x64	For Rabby home PC	Automatic	21.06.20 21:12:04:26	8 Modules >	!
<input type="checkbox"/> RHANGNEW	TUF	192.168.1.43	2.5.354	Microsoft Windows 10 - x64	Rhang Test	Rhang Test	21.06.20 21:11:32:58	10 Modules >	!
<input type="checkbox"/> DESKTOP-AROM	arom	192.168.1.34	2.5.354	Microsoft Windows 10 - x64	Test	Test	21.06.20 21:10:48:49	9 Modules >	!



## การตั้งค่า Group Policy เบื้องต้น

สำหรับข้อมูลรายละเอียดการตั้งค่าแบบละเอียด [คลิก](#)

การตั้งค่าต่าง ๆ บนหน้า dashboard แนะนำปรับให้เหมาะสมกับการใช้งานจริงในองค์กรของท่าน ภาพประกอบข้างต้นเป็นเพียงตัวอย่างเท่านั้น ซึ่งอาจไม่ใช่ค่าที่เหมาะสมที่สุดสำหรับแต่ละองค์กร

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

The screenshot shows the 'Endpoint Settings' interface. At the top, there are tabs for 'Endpoint Settings' (highlighted in red) and 'Network Settings'. Below this, there are tabs for 'Windows Endpoints', 'Mac OS GP', and 'Android GP'. The 'Windows GP' tab is highlighted in red. A search bar is present with the text 'Search by Policy Name'. Below the search bar, it says 'A Total of: 4 Listings'. There is a checkbox for 'Group policies inheritance' which is checked. A 'Create New Policy' button is also visible. The main table has the following columns: Policy Name, AD Computer Group, AD User Group, Priority, Status, and Action. The table contains two rows: 'For Rabby home PC' and 'Rhang Test' (highlighted in red). The 'Rhang Test' row has a priority of 5 and is currently 'Enabled'.

Policy Name	AD Computer Group	AD User Group	Priority	Status	Action
For Rabby home PC	-	-	6	Enabled	Disabled Duplicate
Rhang Test	-	-	5	Enabled	Disabled Duplicate

เมื่อคลิกที่ GP หนึ่งมาแล้ว จะมี tab ย่อยแตกออกมา กดที่แต่ละ tab เพื่อดังค่าตามหมวดหมู่ของการ setting ที่ระบบแบ่งไว้

The screenshot shows the configuration page for the 'Rhang Test' policy. At the top, there is a back arrow and the title 'Rhang Test'. Below this, there are several tabs: 'General' (highlighted in blue), 'Threat Prevention', 'Patch & Assets', 'Endpoint Detection', 'Privileges & App Control', and 'Email Protection'.



## General tab มีค่าพื้นฐานที่ควรต้องทราบดังนี้

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

เมื่อตั้งค่าเรียบร้อยแล้ว ให้คลิก Update GP สิ้นงานที่มุมล่างขวา

**Additional Settings**

Include in Release Candidate Program

Do not show GUI

Realtime communication ⓘ

Skip prompting the client when requesting logs ⓘ

Only merge with AD groups specific policies ⓘ

Enforce uninstall password ⓘ

Uninstall password  
 .....

Synchronize with time server ⓘ

Wake on LAN

Use Priority update servers ⓘ

Keep cached files indefinitely ⓘ

Additional check interval for normal computers [min]

1440

Duplicate GP Delete GP Update GP Cancel



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





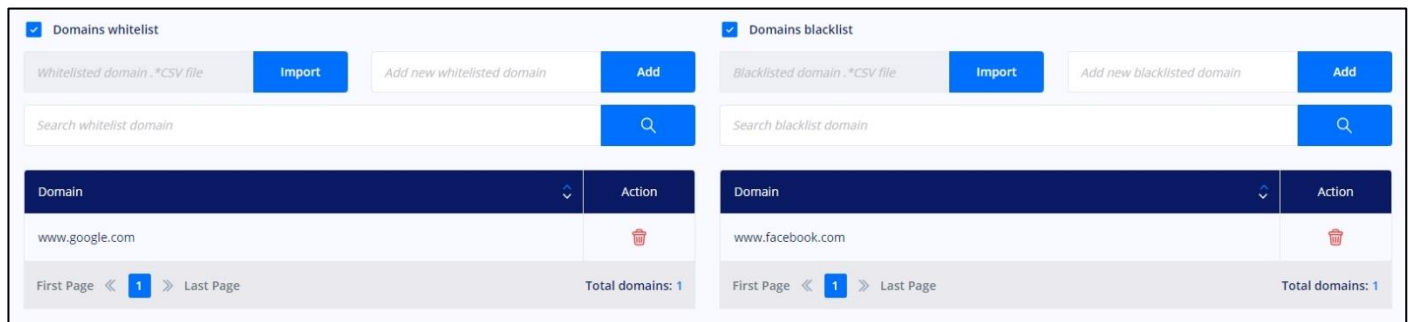
**Threat Prevention tab** มีค่าพื้นฐานที่ควรต้องทราบดังนี้

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

เพื่อให้ระบบทำงานและเริ่มการปกป้องระดับ Advanced Protection ท่านต้องตั้งเปิดฟังก์ชันการทำงานของ DarkLayer Guard และ VectorN Detection



ท่านสามารถตั้งค่า whitelist หรือ blacklist เว็บไซต์ได้โดยติ๊กที่ Domains whitelist และ Domains blacklist ตามลำดับ





ท่านสามารถตั้งค่าบล็อกเว็บไซต์ตาม **Category** โดยคลิกที่ Blocks By Category ซึ่งสามารถปรับแต่งการบล็อกได้ตามหมวดหมู่ที่มีให้สำเร็จรูป และเลือกวันตามสัปดาห์ หรือวันที่ของเดือนตามช่วงเวลาที่กำหนดปรับให้มีผล (active) หรือไม่มีผล (inactive) ได้

Block By Category

Sexuality ✕ Social Networking ✕ Illegal Content ✕ Jobs / Employment ✕ Unknown ✕

Adware / Advertising ✕ Other sharing services ✕ Webmail ✕ Ecommerce Shopping / Online services ✕

Search Engines ✕

**Block By Category Schedule**

Block By Category Schedule ⓘ

Choose week day
  Choose day of month

<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>
<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input type="checkbox"/> Saturday	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>
<input type="checkbox"/> Sunday			<input type="text" value="7"/>	<input type="text" value="8"/>	<input type="text" value="9"/>
			<input type="text" value="10"/>	<input type="text" value="11"/>	<input type="text" value="12"/>
			<input type="text" value="13"/>	<input type="text" value="14"/>	<input type="text" value="15"/>
			<input type="text" value="16"/>	<input type="text" value="17"/>	<input type="text" value="18"/>
			<input type="text" value="19"/>	<input type="text" value="20"/>	<input type="text" value="21"/>
			<input type="text" value="22"/>	<input type="text" value="23"/>	<input type="text" value="24"/>
			<input type="text" value="25"/>	<input type="text" value="26"/>	<input type="text" value="27"/>
			<input type="text" value="28"/>	<input type="text" value="29"/>	<input type="text" value="30"/>
			<input type="text" value="31"/>		

Choose Time Interval [00:00 To Midnight]

Active during time selection
  Inactive during time selection

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



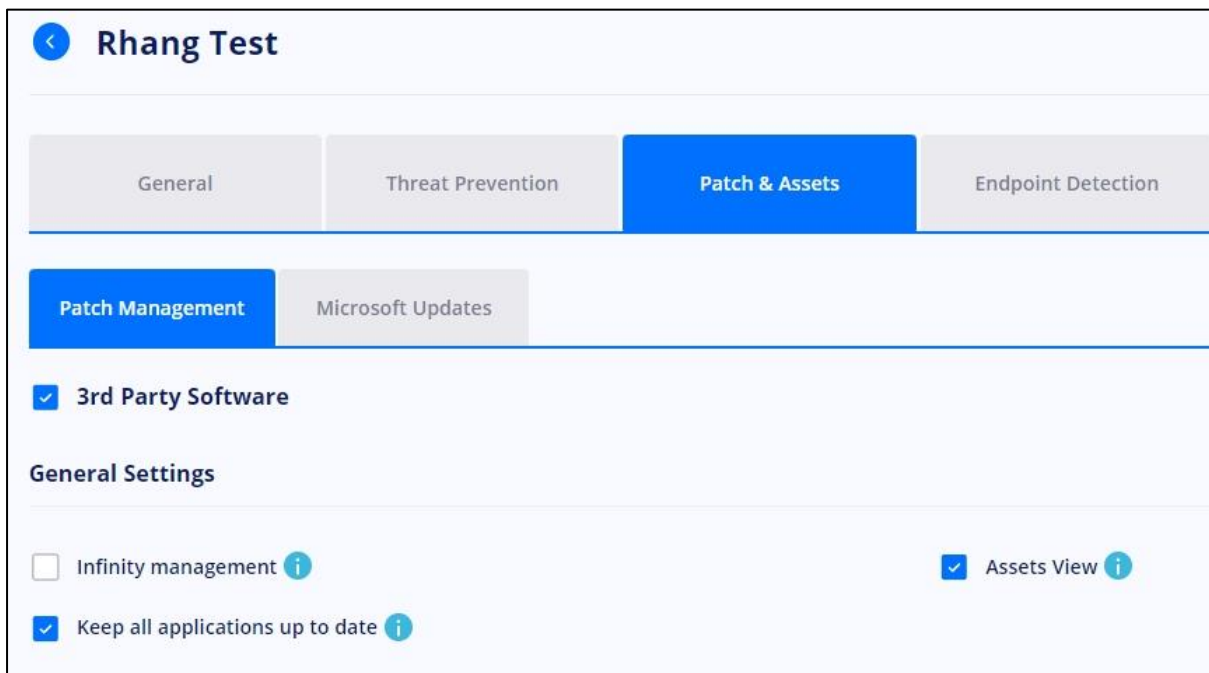
**Patch & Assets tab** มีค่าพื้นฐานที่ควรต้องทราบดังนี้

หากท่านสั่งชื่อ Patch & Asset Management ไว้ ท่านจะสามารถคลิกที่ Patch & Asset tab ได้ หากท่านไม่ได้สั่งชื่อไว้ tab จะเป็นสีเทาอ่อนและไม่สามารถคลิกได้ (greyed out)

เพื่อที่องค์กรจะมีช่องโหว่ของ software น้อยที่สุด ท่านควรอัปเดต 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 ย่อยที่สามารถชื่อเพิ่มได้ กรุณาติดต่อทีมงาน)
- **3rd Party Software** เปิดใช้งานฟังก์ชันอัปเดต patch ของ 3rd party app
- **Keep all applications up to date** อัปเดต 3rd party app ทั้งหมดที่รองรับให้เป็นเวอร์ชันล่าสุดโดยอัตโนมัติ สำหรับลิสต์ software [คลิก](#)
- **Assets View** เมื่อติ๊กไว้ ท่านจะสามารถ track ทุก application ที่ติดตั้งอยู่บนทุกเครื่องในองค์กรได้





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

Install All <input type="checkbox"/>	Update All <input checked="" type="checkbox"/>	Allow Install <input type="checkbox"/>	Applications	Delay Off	Version
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	7-zip x64	Off	Latest version
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	7-zip x86	Off	Latest version
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Accordance	Off	Latest version
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat PRO 2017	Off	Latest version
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader 2017	Off	Latest version
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader 2020 MUI	Off	Latest version
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader DC	Off	Latest version
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader DC DA	Off	Latest version
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader DC MUI	Off	Latest version

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

Welcome to Thor Foresight Enterprise

HOME > X-PLOIT RESILIENCE > ONE CLICK APP INSTALL LIST

NO	SOFTWARE NAME	ACTION
1	Accordance	<b>INSTALL</b>

VER 2.5.354



## Microsoft Updates (tab ย่อย)

- **Microsoft Updates** เปิดใช้งานฟังก์ชัน
- **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 อัปเดตได้ผ่าน module
- **Installation by category** เลือก install ตาม category จาก drop-down menu

←
Rhang Test

General

Threat Prevention

Patch & Assets

Endpoint Detection

Privileges & App Control

Patch Management

Microsoft Updates

Microsoft Updates  
 Microsoft Vulnerability reporting only i

**General Settings**

Install no restart required updates only i  
 Suppress and install everything i  
 Installation of optional updates i

Agent notifications for reboot i  
 Installation of other Microsoft products i

Server Source i

Default
▼

Installation by category i

Windows Update Category

Select category...



- **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 สิ้นน้ำเงินที่มุมล่างขวา

Search by Update All

Update All ▼
🔍

Show Hidden Microsoft Updates

	Update All	KB	Severity	Products	Categories	Release Date	Added On	Suppress Reboot
<input type="checkbox"/>	2021-06 Update for Windows 10 Version 21H1 for x64-based Systems (KB4023057)	4023057	None	-	Critical Updates	10.06.20 21 07:00:00	15.06.20 21 21:18:14	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2021-06 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5003637)	5003637	None	-	Security Updates	08.06.20 21 07:00:00	15.06.20 21 21:18:14	<input checked="" type="checkbox"/>

First Page << 1 >> Last Page
Go to page: 
Items per page: 10 ▼

Check interval [min]

720

Delayed Microsoft Updates Interval (days) ⓘ

1

**Microsoft Updates Schedule**

Microsoft Updates Schedule ⓘ

**Microsoft Updates Reboot Schedule**

Microsoft Updates Reboot Schedule ⓘ

Duplicate GP
 Delete GP

Update GP
Cancel



**Endpoint Detection tab** มีค่าพื้นฐานที่ควรต้องทราบดังนี้

หากท่านสั่งชื่อใน module ของ Endpoint Detection ไว้ ท่านจะสามารถคลิกที่ Endpoint Detection tab และ module tab ย่อยนั้น ๆ ได้ หากท่านไม่ได้สั่งชื่อไว้ tab จะเป็นสีเทาอ่อน และไม่สามารถคลิกได้ (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 ฟังก์ชันนี้ จำเป็นต้อง reboot เครื่องปลายทาง
- **Agent Balloon Notification** เปิดให้มี pop up แจ้งขึ้นมาที่หน้าเครื่องเมื่อมีการตรวจจับเกิดขึ้น
- **AutoScan USB Ports** สแกนอุปกรณ์หน่วยความจำที่เสียบผ่านช่อง USB โดยอัตโนมัติ
- **Real-Time Protection** สแกนอุปกรณ์แบบ real-time เพื่อตรวจจับภัยคุกคามทั้ง 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 ของไฟล์ที่มีพิรุศไปยัง real-time protection cloud เพื่อวิเคราะห์ต่อและรอการแจ้งกลับว่าเป็นไฟล์ดีหรือร้าย
- **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)

←

## Rhang Test

General

Threat Prevention

Patch & Assets

Endpoint Detection

Privileges & App Control

Email Protection

Next-Gen Antivirus

Firewall

Ransomware Encryption Protection

**Next-Gen Antivirus** i

**General Settings**

USB Silent Mode Scan i

Disable USB Ports i

Agent Balloon Notifications i

AutoScan USB Ports i

**Antivirus Settings**

Real-Time Protection i

False Positive Control i

Allow Manual Scan i

Allow users to stop the AV service i

Protection Cloud i

Real-Time Scan Network Files (READ INFO) i

Allow Cancel Scan i

Password for stopping the AV Service

Auto restart the AV Service after [2 - 60 min]\*

10





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

**Schedule Scan**

Add New Scan

Scan Profile Name\*

Scan Type\*

Full Scan

Description

Choose week day
  Choose day of month

<input type="checkbox"/> Monday	<input type="checkbox"/> Tuesday	<input type="checkbox"/> Wednesday	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>
<input type="checkbox"/> Thursday	<input type="checkbox"/> Friday	<input type="checkbox"/> Saturday	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>
<input type="checkbox"/> Sunday			<input type="text" value="7"/>	<input type="text" value="8"/>	<input type="text" value="9"/>
			<input type="text" value="10"/>	<input type="text" value="11"/>	<input type="text" value="12"/>
			<input type="text" value="13"/>	<input type="text" value="14"/>	<input type="text" value="15"/>
			<input type="text" value="16"/>	<input type="text" value="17"/>	<input type="text" value="18"/>
			<input type="text" value="19"/>	<input type="text" value="20"/>	<input type="text" value="21"/>
			<input type="text" value="22"/>	<input type="text" value="23"/>	<input type="text" value="24"/>
			<input type="text" value="25"/>	<input type="text" value="26"/>	<input type="text" value="27"/>
			<input type="text" value="28"/>	<input type="text" value="29"/>	<input type="text" value="30"/>
			<input type="text" value="31"/>		

Choose Time Interval [00:00 To Midnight]

8:00

16:00

Active during time selection  
 Inactive during time selection

Set Scan
Cancel



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

### Next-Gen AV Exclusion List ?

Exclusions \*.CSV file Import

Search exclusion 🔍

Add new exclusion Add

Select profiles... ▼

Priority <span style="float: right;">?</span>	File Name/Path	Type	Action
Low ▼	D:\web	File Path	✖

First Page << 1 >> Last Page

### Global Quarantine List ?

Exclusions \*.CSV file Import

Search global quarantine 🔍

Add new global quarantine Add

File Name/Path	Type	Action
There are no results		

First Page << 1 >> Last Page Total domains: 0



## Firewall (tab ย่อย)

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

←

### Rhang Test

General

Threat Prevention

Patch & Assets

Endpoint Detection

Privileges & App Control

Email Protection

Next-Gen Antivirus

Firewall

Ransomware Encryption Protection

Firewall Management

**General Settings**

Block RDP port on brute force detection i

Use automatic rules i

Allow ICMP Echo Requests i

**Firewall Profiles**

Domain

Private

Public

Inbound connection*	Inbound connection*	Inbound connection*
Block <span style="float: right;">▼</span>	Block <span style="float: right;">▼</span>	Block <span style="float: right;">▼</span>
Outbound connection*	Outbound connection*	Outbound connection*
Allow <span style="float: right;">▼</span>	Allow <span style="float: right;">▼</span>	Allow <span style="float: right;">▼</span>



**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 สิ้นงานที่มุมล่างขวา

Allow isolation ⓘ

**Isolation Rules**

Select profile

Add Profile ⓘ

Name	Application	Remote Ip	Port	Direction	Protocol	Permission	Profile Type	Action
There are no results								

**Firewall Rules**

+ Add New Rule

Name	Application	Remote Ip	Port	Direction	Protocol	Permission	Profile Type	Action
There are no results								

📄 Duplicate GP
 🗑️ Delete GP

Update GP
Cancel



## Ransomware Encryption Protection (tab ย่อย)

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

ท่านสามารถตั้งค่า exclusion หรือยกเว้นการตรวจจับจาก File Path หรือ File Name ได้จาก ตารางด้านล่าง

เมื่อตั้งค่าเรียบร้อยแล้ว ให้คลิก Update GP สิ้นน้ำเงินที่มุมล่างขวา

The screenshot shows the configuration page for Ransomware Encryption Protection. The interface includes several sections:

- Navigation Tabs:** General, Threat Prevention, Patch & Assets, **Endpoint Detection** (selected), Privileges & App Control, Email Protection.
- Sub-Tabs:** Next-Gen Antivirus, Firewall, **Ransomware Encryption Protection** (selected).
- Settings:**
  - Ransomware Encryption Protection
  - General Settings:**
    - Default action on detection: Block (dropdown menu)
    - Agent Balloon Notifications
  - Exclusions:**
    - Exclusions: \*.CSV file (with Import button)
    - Add new exclusion (with File Name dropdown and Add button)
    - Search exclusion (with search icon)
- Table:** A table with columns: File Name/Path, Type, and Action. The table is currently empty, showing "There are no results".
- Page Navigation:** First Page << 1 >> Last Page
- Bottom Actions:** Duplicate GP, Delete GP, Update GP, Cancel.



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

- **ให้ความรู้ security awareness กับ end user** ให้รู้จักแยกแยะ phishing มีความระมัดระวังในการกรอกข้อมูล คลิกลิงค์หรือดาวน์โหลดไฟล์
- **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 ปิดการอัปเดต 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** ว่าฟังก์ชันที่จำเป็นนั้นถูกเปิดใช้งานแล้ว
- **ควรอัปเดต security patch** ของ OS และ 3rd party application ที่ติดตั้งในเครื่อง ให้เป็นล่าสุดอยู่เสมอ (สามารถใช้ patch management ช่วยบริหารจัดการได้ **ดูหน้า 19**)
- **ปิด RDP หากไม่มีความจำเป็นต้องใช้** หรือถ้าต้องใช้ ให้ภายนอกต้องผ่าน VPN เข้ามาก่อนจะเข้าถึงเครื่อง และ user ที่ใช้ RDP ควรมีสิทธิ์เป็น user ธรรมดา ไม่ควรมีสิทธิ์เป็น Admin และเปิดฟังก์ชัน (**ดูหน้า 27**)
- **หมั่นทำการสำรองข้อมูล (backup) ไว้เสมอ** โดยเก็บไว้ในอุปกรณ์แยกจากระบบหลัก ไม่เสียบคาว์ที่เครื่อง หรือสามารถเข้าถึงได้ตลอดเวลา หรือใช้บริการบน cloud
- **เลี่ยงการใช้โปรแกรมที่ไม่มีลิขสิทธิ์** ไฟล์จำพวก crack, keygen, loader อาจนำมาซึ่งช่องโหว่หรือภัยคุกคามอื่น ๆ ได้ รวมถึงเสี่ยง add-on หรือ extension ต่าง ๆ ของ web browser ที่ไม่จำเป็นต้องใช้ แต่หากจำเป็นต้องใช้ สามารถตั้ง exclusion ของแต่ละ module ได้
- **ตรวจสอบโปรแกรม security ที่ติดตั้งอยู่ทุกเครื่องมีสถานะทำงานเป็นปกติและอัปเดตเป็นปัจจุบัน** โดยตรวจสอบได้จากบน dashboard หรือการแจ้งเตือนที่หน้าเครื่อง

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



## Who is HEIMDAL™ Security?



**Morten Kjaersgaard**  
CEO



**Cosmin Toader**  
CTO



**Catalin Draghici**  
Director, Marketing  
& Online Sales



**Valentin Gersby Stilling**  
CSO

ในปี 2011 ทีมผู้ก่อตั้งได้เข้าร่วมการแข่งขัน World Hacking Championships - Def Con Capture The Flag ซึ่งมีทีมหackerที่เข้าร่วมแข่งขันมากมาย เช่น FBI, NSA, freelancer และบริษัทด้าน Security ขนาดใหญ่หลายแห่ง ทางทีมได้ชนะเลิศการแข่งขันในปี 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](#)

Product of choice by:

