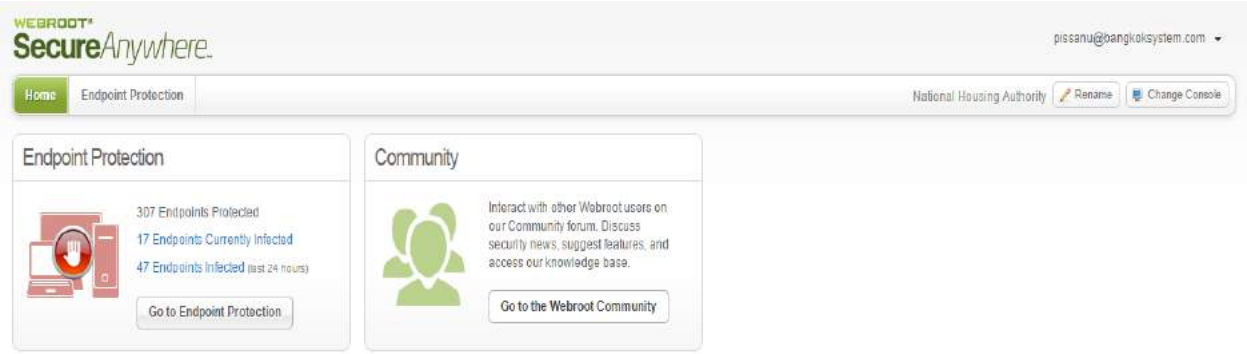
Console management



1.Home

แถบเมนูจะมี 2 เมนู ได้แก่

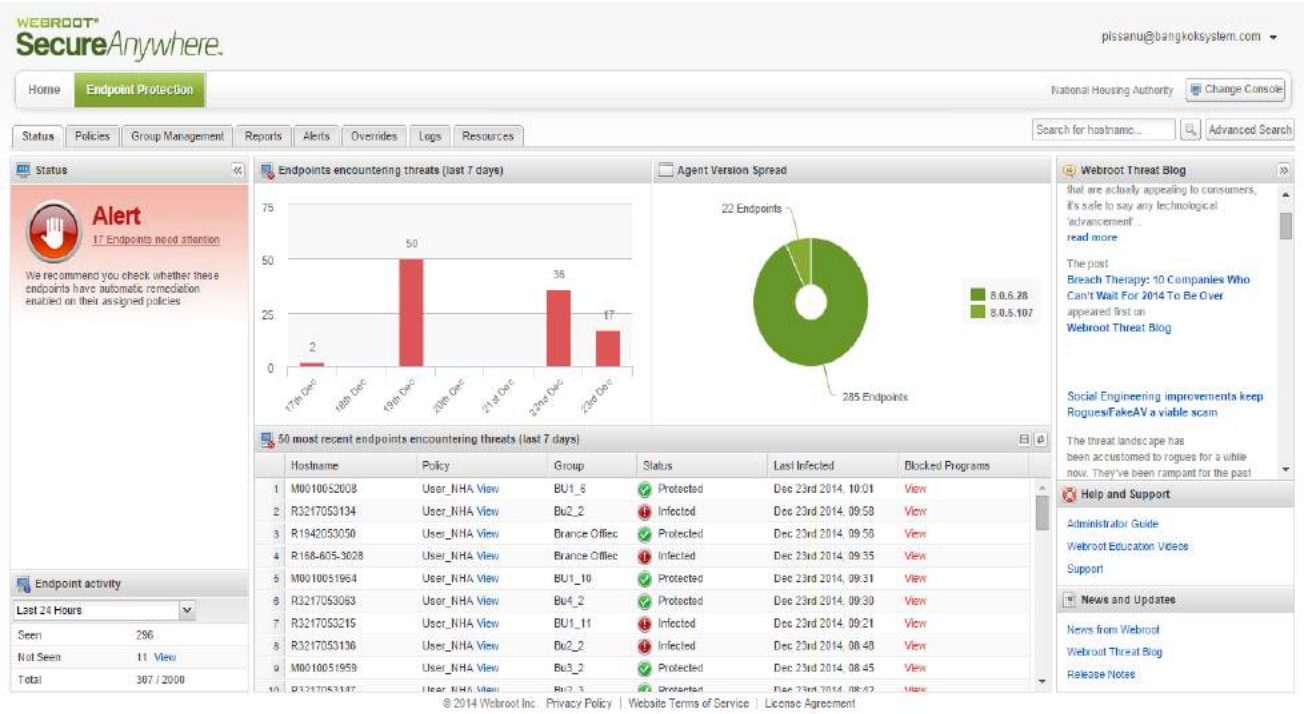
1.1 Endpoint Protection

- แสดง **Endpoints** ทั้งหมดที่ได้มีการติดตั้ง
- แสดง **Endpoints** ในปัจจุบันที่มีการตรวจเจอไฟล์ที่มีความเสี่ยง
- แสดง **Endpoints** ภายในภายใน **24** ชั่วโมงล่าสุดที่มีการตรวจสอบเจอไฟล์ที่มีความเสี่ยง

1.2 Community

กลุ่มแลกเปลี่ยนความรู้และปัญหาที่เกิดขึ้นของ **Webroot Secure AnyWhere**

2.Status



2.1 Status จะมีการแจ้งเตือน Endpoint ที่ตรวจพบไฟล์ที่มีความเสี่ยงและแนะนำให้ตรวจสอบ Endpoint ว่าจะอยู่ในกลุ่มนโยบายและรายละเอียดของไฟล์ที่มีความเสี่ยง และสามารที่คลิกเข้าไปดูรายละเอียดของการแจ้งเตือนว่า Endpoint เครื่องไหนที่แจ้งเตือน สามารถที่ทำการ Cleaup หรือ Restore และ Override ได้

1.3 Endpoint encountering threats

จะแสดงกราฟรายละเอียดการตรวจสอบเจอไฟล์ทีมีความเสี่ยงของ Endpoint ภายใน 7 วันล่าสุดและสามารถที่คลิกเข้าไปดูรายละเอียดของแต่ละกราฟ สามารถที่ทำการ Cleaup หรือ Restore และ Override ได้

1.4 **Agent Version Spread**

จะแสดงเวอร์ชั่นทั้งหมดของ Endpoint และสามารถที่จะคลิกเข้าไปดูรายละเอียดของแต่ละ Endpoint ได้

1.5 Endpoint Activity

จะแสดงสถานะการตรวจสอบ Endpoint สถานการณ์ออนไลน์และออฟไลน์และจำนวน Endpoint ทั้งหมด

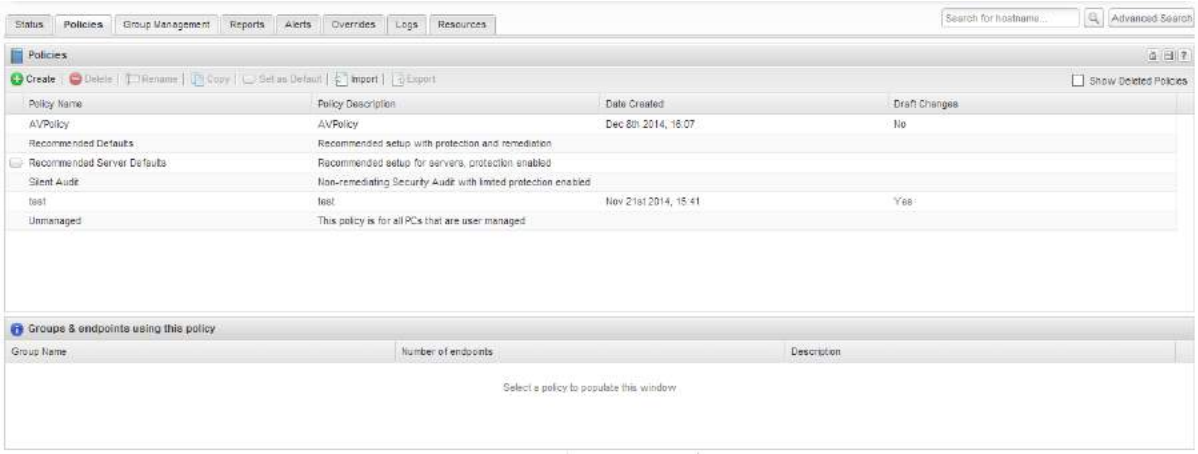
1.6 Webroot Threat Blog

จะแสดงรายละเอียดข้อมูลที่มีการปรับปรุงล่าสุด Blog ของ Webroot

1.5 Help and Support

คู่มือการใช้งานของ Webroot และ วีดิโอแนะนำการใช้งานและร่วมไปถึงข่าวในการปรับปรุงไฟล์ทีมีความเสี่ยงและภัยคุกคามต่างๆ

Polices



เมื่อกำหนดค่าการป้องกันและตรวจสอบเลือกหนึ่งในนโยบายเริ่มต้นของ กำหนดนโยบายการตั้งค่า SecureAnywhere บนอุปกรณ์ปลายทาง เช่น ตารางการสแกนและพฤติกรรมการป้องกัน สามารถใช้นโยบายเริ่มต้นหรือคุณสามารถกำหนดนโยบายมากขึ้นและกำหนดให้กับอุปกรณ์ปลายทางตัวอย่างเช่น อาจต้องการที่จะให้ผู้บริหารระบบการควบคุมมากขึ้นกว่าที่จะพนักงานคนอื่น ๆ ในกรณีที่สามารถสร้างนโยบายใหม่สำหรับผู้ดูแลระบบและให้ Endpoint

อื่น ๆ เกี่ยวกับนโยบายการเริ่มต้น

โดยจะแสดงเมนูดังนี้

- Create คือ เป็นการสร้าง Policy ขึ้นมาใหม่
- Delete คือ เป็นการลบ policy
- Rename คือ เป็นการตั้งค่าชื่อให้กับ policy นั้นๆ
- Copy คือ สามารถทำการคัดคอก policy
- Set default คือ สามรถที่จะกำหนดการตั้งค่าให้ policy เป็นค่าเริ่มต้น
- Import คือ สามารถที่จะ import ค่า configure policy
- Export คือ สามารถที่จะ export ค่า configure policy

หมายตุ Policy Unmanaged ไม่สามรถที่จะทำการแก้ไขได้ (user จะทำการจัดการเองทั้งหมด)

โดยมีการตั้งค่า Policy ดังนี้

3.1 Basic configuring

Polices Details	รายละเอียด
Show a secure Anywhere shortcut on the desktop	แสดงที่หน้าจอ
Show a system tray icon	แสดงที่แถบเมนู
Show a splash screen on bootup	แสดงตอนเริ่มต้นคอมพิวเตอร์
Show SecureAnywhere in the Start Menu	แสดงที่แถบ Star Menu
Show SecureAnywhere in Add/Remove Programs	แสดงที่ Add/Remove Programs
Show SecureAnywhere in the Windows Action Center	แสดงที่ Windows Action Center
Hide the SecureAnywhere keycode and subscription information on-screen	ซ่อน Key code ในโปรแกรม
Automatically download and apply update	ดาวน์โหลดและปรับปรุง เวอร์ชั่นโดยอัตโนมัติ
Operate background functions using fewer CPU resources	การทำงานของโปรแกรมให้ใช้ทรัพยากรน้อยจาก CPU
Favor low disk usage over verbose logging (fewer details stored in logs)	การใช้งานดิสก์ให้ต่ำ
Lower resource usage when intensive applications or games are detected	เมื่อมีการใช้งานทรัพยากรมากหรือมีการเล่นเกมส์ โปรแกรมจะใช้ทรัพยากรที่ต่ำกว่า
Allow SecureAnywhere to be shut down manually	สามารถจะปิดโปรแกรมด้วยตนเองได้
Store Execution History details	เก็บ Log การทำงานของโปรแกรมทั้งหมด
Poll interval	ช่วงเวลาในการสำรวจ
Polices details	**รายละเอียด**

Enable Scheduled Scans	เปิดการใช้สแกนตามระยะเวลาที่กำหนด
Scan Frequency	ช่วงเวลาในการสแกน
Time	เวลา
Scan on bootup if the computer is off at the scheduled time	สแกนเมื่อบูตเครื่องคอมพิวเตอร์หากเครื่องถูกปิดในเวลาที่กำหนด
Hide the scan progress window during scheduled scans	ซ่อนหน้าต่างความคืบหน้าการสแกนที่กำหนดไว้
Only notify me if an infection is found during a scheduled scan	แจ้งเตือนให้ทราบถ้าพบไวรัสในช่วงการสแกนที่กำหนดไว้เท่านั้น
Do not perform scheduled scans when on battery power	ห้ามทำการกำหนดการสแกนเมื่อใช้พลังงานจากแบตเตอรี่
Do not perform scheduled scans when a full screen application or game in open	ห้ามทำการกำหนดการสแกนเมื่อโปรแกรมประยุกต์หรือเกมส์ทำงานอยู่
Randomize the time of scheduled scans up to one hour for distributed scanning	สุ่มเวลาของการสแกนที่กำหนดไว้ถึงหนึ่งชั่วโมงสำหรับการสแกน

3.2 Scan schedule

3.3 Scan settings

Polices details	รายละเอียด
Enable Realtime Master Boot Record (MBR) Scanning	เปิดการใช้งานสแกน Master Boot Record (MBR) ตลอดเวลา
Enable Enhanced Rootkit Detection	เปิดใช้งานการตรวจหา Rookit ที่เพิ่มขึ้น
Enable “ right-click ” scanning in Windows Explorer	เปิด " คลิกขวา " สแกนใน Windows Explorer
Update the currently scanned folder immediately as scanned	อัพเดทสแกนโฟลเดอร์ปัจจุบันทันทีที่สแกน
Polices Details	**รายละเอียด**

Favor low memory usage over fast scanning	การใช้งานหน่วยความจำที่ต่ำเมื่อใช้การสแกนแบบรวดเร็ว
Favor low CPU usage over fast scanning	การใช้งาน CPU ต่ำเมื่อใช้การสแกนแบบรวดเร็ว
Save non-executable file details to scan logs	บันทึกรายละเอียดไฟล์ที่ไม่ทำงานลงในรายละเอียดการสแกน
Save the “ Authenticating File “ popup when a new file is scanned on-execution	แสดงการดำเนินการ ป๊อปอัพ "Authenticating Files" เมื่อไฟล์ใหม่ถูกสแกน
Scan archived files Automatically reboot during cleanup without prompting	สแกนไฟล์ที่เก็บไว้และรีทสตาร์เครื่องโดยอัตโนมัติโดยระหว่างการทำความสะอาดเสร็จโดยไม่ต้องแจ้งเตือน
Never reboot during malware cleanup	ไม่ต้องรีทสตาร์เครื่องใหม่โดยระหว่างการทำความสะอาดมัลแวร์เสร็จเรียบร้อย
Automatically remove threats found during background scans	ลบภัยคุกคามโดยอัตโนมัติที่พบในระหว่างการสแกน
Enable Enhanced Support	เปิดใช้งานการสนับสนุนการช่วยเหลือ
Show Infected Scan Results	แสดงผลการสแกนที่พบภัยคุกคาม
Detect Possibly Unwanted Applications (PUAs) as malicious	ตรวจจับโปรแกรมที่ไม่พึงประสงค์อาจจะเป็น (Puas) ที่เป็นอันตราย

3.4 Self Protection

Polices Details	รายละเอียด
Enable self protection response cloaking	เปิดใช้งานการป้องกันตัวเอง
Self protection Level	ระดับการป้องกันตนเอง

3.5 Heuristics

Polices Details	รายละเอียด
Enable infrared	เปิดใช้งาน
Local heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
USB heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
Internet heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
Network heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
CD/DVD heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
Offline heuristics	

Polices Details	รายละเอียด
Heuristics	
Advanced Heuristics	
Popularity heuristics	

3.6 Real Time Shield

Polices Details	รายละเอียด
Realtime Shield Enabled	เปิดการใช้งานการป้องกันตลอดเวลา
Enable Predictive Offline Protection from the central Secure-AnyWhere database	เปิดใช้งานการป้องกันแบบออฟไลน์จากฐานข้อมูลกลาง
Remember actions on blocked files	จดจำการดำเนินการไฟล์ที่ถูกปิดกั้น
Automatically quarantine previously blocked files	บล็อกไฟล์ที่มีความเสี่ยงให้เป็นไฟล์ที่ถูกปิดกั้นโดยอัตโนมัติ
Automatically block files when detected on execution	เมื่อตรวจพบไฟล์ที่มีความเสี่ยงจะดำเนินการป้องไฟล์โดยอัตโนมัติ
Scan files when written of modified	สแกนไฟล์เมื่อเขียนหรือแก้ไข
Block threats automatically if no user is logged in	บล็อกไฟล์อัตโนมัติถ้าผู้ใช้งานไม่มีการเข้าสู่ระบบ
Show real time event warnings	โชว์การแจ้งเตือนเหตุการณ์ตลอดเวลา
Show real time block modal alerts	โชว์การแจ้งเตือนการบล็อกตลอดเวลา
Show real time block notifications	โชว์การแจ้งเตือนการบล็อกตลอดเวลา

3.7 Behavior Shield

Polices Details	รายละเอียด
Behavior Shield Enabled	เปิดการป้องกันพฤติกรรม
Assess the intent of new programs before allowing them to execute	ประเมินความตั้งใจของโปรแกรมใหม่ก่อนที่จะปล่อยให้ดำเนินการต่อ
Enable advanced behavior interpretation to identify complex threats	เปิดการใช้งานการตรวจสอบพฤติกรรมชั้นสูงเมื่อระบุภัยคุกคามที่ซับซ้อน
Track the behavior of untrusted programs for advanced threat removal	ติดตามพฤติกรรมของโปรแกรมที่ไม่น่าเชื่อถือในการจัดการภัยคุกคาม
Automatically perform the recommended action instead of showing warning messages	ดำเนินการโดยอัตโนมัติในข้อความแนะนำแทนข้อความเตือน
Warn if untrusted programs attempt low-level system modifications when offline	เตือนถ้าโปรแกรมที่ไม่น่าเชื่อถือพยายามปรับเปลี่ยนในระดับต่ำเมื่อทำงานในระบบออฟไลน์

3.8 Core System Shield Enabled

Polices Details	รายละเอียด
Core System Shield Enabled	เปิดการป้องกันระบบปฏิบัติการ
Assess system modifications before they are allowed to take place	ประเมินการปรับเปลี่ยนระบบปฏิบัติการก่อนที่จะได้รับอนุญาตให้ดำเนินการ
Detect and repair broken system components	ตรวจสอบและซ่อมแซมระบบปฏิบัติการที่มีความสูญหาย
Prevent untrusted programs from modifying kernel memory	ป้องกันไม่ให้โปรแกรมที่ไม่น่าเชื่อถือจากหน่วยความจำในการปรับเปลี่ยน
Prevent untrusted programs from modifying system processes	ป้องกันไม่ให้โปรแกรมที่ไม่ได้เชื่อถือจากการปรับเปลี่ยนระบบปฏิบัติการ
Polices Details	**รายละเอียด**

Verify the integrity of the LSP chain and other system structures	ตรวจสอบความสมบูรณ์ของ LSP และโครงสร้างอื่นๆ
Prevent any program from modifying the HOSTS file	ป้องกันไม่ให้โปรแกรมใดๆมีการปรับเปลี่ยนจากไฟล์โฮสต์

3.9 Web Threat Shield

Polices Details	รายละเอียด
Web threat shield enabled	เปิดการป้องกันภัยคุกคามเว็บไซค์
Analyze search engine results and identify malicious websites before visitation	วิเคราะห์ผลการค้นหาและระบุเว็บไซค์ที่เป็นอันตราย
Automatically protect newly installed browser	ตรวจสอบอัตโนมัติเว็บไซค์ที่มีการติดตั้งใหม่
Look for malware on websites before visitation	ตรวจสอบหามัลแวร์บนเว็บไซค์ก่อนที่จะเข้าไปถึง
Look for exploits in website content before visitation	ตรวจสอบหาเนื้อหาของเว็บไซค์ก่อนที่จะเข้าไปถึง
Suppress the user's ability to make local web threat shield overrides	ป้องกันผู้ใช้งานในการใช้เว็บไซค์ที่เสี่ยงต่อภัยคุกคาม
Auto install browser addons when new browsers are installed	ติดตั้งโปรมแกรม Addon โดยอัตโมมัติเมื่อมีการติดตั้ง Web-browser ใหม่
Only install the web filtering driver (do not install the web filtering browser addons)	ให้ติดตั้งโปรแกรมควบคุมการกรองเว็บเท่านั้น (ไม่ให้ติดตั้งเบราว์เซอร์ add on กรองเว็บ)

3.10 Identity Shield

Polices Details	รายละเอียด

Identily shield Enabled	เปิดการใช้งานการป้องกันที่ระบุตัวตน
Look for identity threats online	วิเคราะห์เว็บไซค์ที่ผู้ใช้ใช้บราเซอร์และการเชื่อมโยงไปหาเว็บไซค์อื่นๆ
Analyze websites for phishing threats	วิเคราะห์เว็บไซค์สำหรับภัยคุกคามฟิชชิง
Verify websites when visited to determine legitimacy	ตรวจสอบเว็บไซค์เมื่อมีการใช้งานของเว็บไซค์ต่างๆ
Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks	ตรวจสอบความละเอียด DNS/IP ของเว็บไซค์และตรวจการโจมตี
Block websites from accessing protected credentials	บล็อกเว็บไซค์ที่มีความเสี่ยงสูง
Prevent programs from accessing protected credentials	บล็อกโปรแกรมที่มีการเข้าถึงข้อมูลประจำตัวที่ได้รับการป้องกัน
Warn before blocking untrusted programs from accessing protected data	แจ้งเตือนก่อนที่จะบล็อกโปรแกรมจาการตรวจสอบ
Allow trusted screen capture programs access to protected screen contents	อนุญาตให้โปรแกรมจับภาพหน้าจอที่เชื่อถือได้เข้าถึงเนื้อหาของหน้าจอที่มีการป้องกัน
Enable identity Shield compatibility mode	เปิดการใช้งานการป้องกัน Compatibility Mode
Enable keylogging protection in non-Latin systems	เปิดการใช้งานการบันทึกการกดคีย์บอร์ดแบบ non-Latin

3.11 Firewall

Polices Details	รายละเอียด
Enabled	เปิดการใช้งาน

Firewall level	ระดับของไฟล์วอลล์
Polices Details	**รายละเอียด**
Show firewall management warnings	แสดงคำเตือนการจัดการไฟร์วอลล์
Show firewall process warnings	แสดงคำเตือนกระบวนการไฟร์วอลล์

3.12 User interface

Polices Details	**รายละเอียด**
GUI	(Graphical user interface) สามารถแสดงการรายละเอียดการ Configure

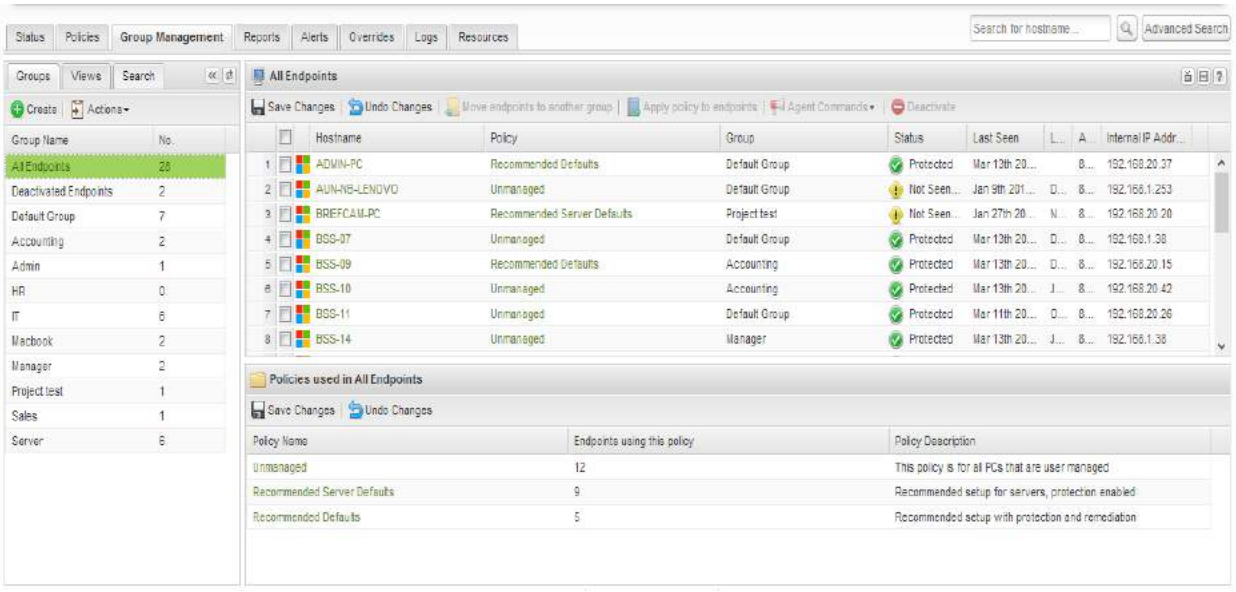
3.13 System Cleaner

Polices Details	**รายละเอียด**
Manage system cleaner centrally	จัดการทำความสะอาดระบบจากส่วนกลาง
Scheduled cleanup	กำหนดเวลาทำความสะอาด
Cleanup at specific time of day – hour	การล้างข้อมูลในช่วงเวลาที่เฉพาะเจาะจงของวัน(ชั่วโมง)
Cleanup at specific time of day - minute	การล้างข้อมูลในช่วงเวลาที่เฉพาะเจาะจงของวัน (นาที)
Enable windows explorer right click secure file erasing	เปิดใช้งาน Windows Explorer คลิกขวาลบไฟล์ที่ปลอดภัย
Windows desktop	
Recycle Bin	ถังรีไซเคิล
Recent document history	ประวัติการใช้งานเอกสารล่าสุด
Start menu click history	ประวัติการคลิก
Run history	ประวัติการเรียกใช้

Search history	ประวัติการค้นหา
Start menu order history	ประวัติการเริ่มต้นเมนู
Windows system	
Clipboard contents	เนื้อหาของคลิปบอร์ด
Windows temporary folder	โฟลเดอร์ Windows Temporary
System temporary folder	โฟลเดอร์ System Temporary
Windows update Temporary folder Windows registry streams Windows Registry	โฟลเดอร์ Windows Update Temporary Windows Registry
Default logon user history	ค่าเริ่มต้นประวัติของผู้ใช้เข้าสู่ระบบ
Memory dump files	แฟ้มการถ่ายโอนหน่วยความจำและ
CD burning storage folder	โฟลเดอร์จัดเก็บข้อมูลการเขียนซีดี
Flash cookies	คุกกี้แฟลช
Internet explorer	
Address bar history	ประวัติแถบบาร์ (Address bar)
Cookies	คุ้กกี้
Temporary internet files	
URL history	ประวัติ URL
Setup log	ประวัติการติดตั้งโปรแกม

Microsoft download folder	ไมโครซอฟท์ดาวน์โหลดโฟลเดอร์
MediaPlayer Bar history	ประวัติ Media Player Bar
Autocomplete form information	ข้อมูลรูปแบบอัตโนมัติ
Clean index.dat (cleaned on reboot)	ทำความสะอาด index.dat (ทำความสะอาดในการบูตเครื่อง)
Secure file removal	
Control the level of security to apply when removing files. Higher security levels reduce the possibility of recovering data but will require longer to clean.	ควบคุมระดับความปลอดภัยที่จะใช้เมื่อการลบไฟล์ ระดับความปลอดภัยที่สูงขึ้นลดความเป็นไปได้ของการกู้คืนข้อมูล แต่จะต้องใช้เวลานานในการทำความสะอาด

Group Management



เมื่อติดตั้ง SecureAnywhere บนอุปกรณ์ปลายทางเสร็จเรียบร้อย นโยบายเริ่มต้นจะไปอยู่ใน Default Group (Group management คือชุดของอุปกรณ์ปลายทางซึ่งจะช่วยให้จัดระเบียบอุปกรณ์ให้สามรถจัดการได้ง่าย) endpoints เมื่อรายงานลงใน Group management (หลังจากดำเนินการสแกนครั้งแรก) สามารถย้ายไปยังกลุ่มที่แตกต่างกัน ตัวอย่างเช่น อาจจะจัดระเบียบจุดสิ้นสุดตามวันและเวลาเพื่อให้สามารถกำหนดเวลาการสแกนเดียวกันสำหรับพวกเขาทั้งหมด สามารถดูทุกกลุ่มในแท็บการจัดการกลุ่ม

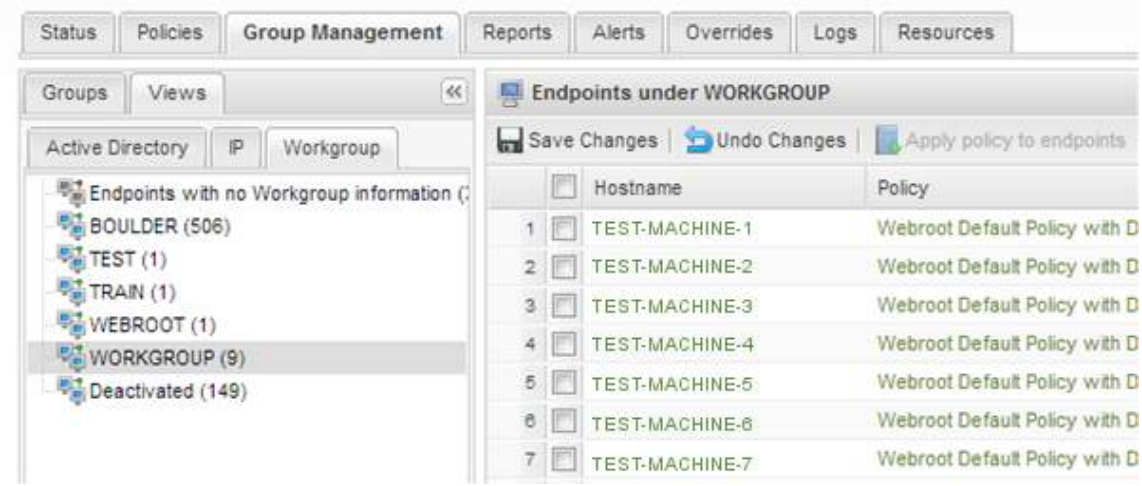
จะมีแถบเมนูทั้งหมด 5 เมนูหลักได้แก่

- Group
- Views
- Search
- All Endpoints
- Polices used in All endpoint

1.Group จะมีเมนู 3 เมนู

- Create จะเป็นการสร้าง Group เพื่อทำการ Join เข้ากับ Polices
- Actions เป็นการแก้ไขชื่อ Group ลบ และย้าย Group
- Group Name คือ เป็นเมนูที่แสดงแต่ละ Group

2.Views ดูข้อมูลที่เก็บรวบรวม Endpoint ภายใต้การบริหารจัดการกลุ่ม Domain ตามรายละเอียดตามรูปด้านล่าง



3.Search คือ เป็นการตรวจหา Endpoint โดยจะต้องการค้นหาจาก Hostname ,status, group, policy,Activec directory , keycode , operation system

4. All Endpoint จะมีเมนู 6 เมนูได้แก่

1. Save Changes เป็นการบันทึกสำหรับมีมีการเปลี่ยนแปลง กลุ่ม หรือ Polices ได้
2. Undo Changes คือเป็นการกลับไปค่าเดิม หลังจากที่ได้ทำการเปลี่ยนแปลงต่างๆ
3. Move endpoints to another group คือ เป็นการย้าย Endpoint กลุ่มหนึ่งไปยังอีกกลุ่มหนึ่ง
4. Apply policy to endpoint คือ เป็นการใช้สำหรับ เมื่อต้องการเปลี่ยนแปลง Polices ให้กับ Endpoint
5. Agent commands คือ เป็นการใช้คำสั่ง โดยมีรายละเอียดดังนี้

Agent

- Scan คือ สแกนตรวจสอบไฟล์ที่มีความเสี่ยง
- Change scan time คือเปลี่ยนแปลงเวลาการสแกน
- Scan a Folder คือเป็นการเลือกโฟลเดอร์ที่จะต้องการทำการสแกน
- Clean up คือทำการจัดการลบไฟล์ที่มีความเสี่ยงที่เก็บไว้ใน Quarantine
- System cleaner คือทำการจัดการไฟล์ที่ขยะ เช่น Temp history cookie
- Uninstall คือ ยกเลิกการติดตั้ง Endpoint
- Reset คือ การรีเซต Endpoint ให้กลับไปเป็นการตั้งค่าเริ่มต้น
- Remove Password protection คือ การลบ password ออกจาก Endpoint

Clear data

- Clear log file คือ เป็นลบไฟล์ที่เก็บ log ที่เก็บใน Endpoint
- Disable proxy setting คือ เป็นการปิดการใช้ Proxy ที่มีการตั้งค่าไว้

Keycode

- Change keycode คือเป็นการเปลี่ยน keycode ของ Endpoint
- Change keycode temporarily คือ สามารถกำหนดระยะเวลาการใช้งานของ keycode

Power & User access

- Lock endpoint คือ สามารถที่จะการ Lock windows endpoint
- Log off คือ สามารถทีจะทำการ Log off windows
- Restart คือ สามรถที่จะทำการ Restart windows
- Restart in Safe Mode with Networking คือ สามารถที่จำการ Restart เพื่อเข้า Safe Mode network

- Shutdown คือ สามารถปิดเครื่อง endpoint

Antimalware Tools

- Reset desktop คือสามารถรีเซตหน้าจอ
- Reset Screen saver คือสามารถรีเซต Screen saver
- Reset system policies คือ สามารถที่จะทำการรีเซตค่า registry ได้
- Restore file คือ สามารถที่ทำการ restore file ที่อยู่ใน Quarantine

Files &Processes

- Reverify all files and processes คือการตรวจตรวจสอบฐานข้อมูล
- Consider all items as good คือ เป็นการพิจารณารายการทั้งหมดที่ดีและทำงานอย่างปลอดภัย
- Allow processes blocked by firewall คือการอนุญาตให้การสื่อสารที่ถูกบล๊อกที่มีการตั้งค่าในไฟล์วอลล์
- Stop untrusted processes คือหยุดการทำงานทั้งหมด และสามรถทำงานงานอีกครั้งได้

Identity Shield

- Allow application คือ สามารถอนุญาต Application ทำงานได้โดยไม่ต้องตรวจสอบ
- Deny application คือ สามรถที่ทำการบล็อค Application ไม่ได้ทำงานได้
- Allow All Denied Applications คือสามารถที่อนุญาตให้ Application ทำงานได้โดยที่ยังบล็อค
- Protect an Application คือ สามรถที่ให้การตรวจสอบ Application
- Unprotect an Application คือ สามรถยกเลิกการตรวจสอบ Application

Advanced

- Run customer support script คือ สามารถ Run script เพื่อทำการ Cleanup
- Customer support Diagnostics คือสามรถทำการส่ง Lop ของ Endpoint ไปให้ Support วิเคราะห์ได้
- Download and run a file คือ สามารถทีจะให้ Endpoint ดาวห์โหลดไฟล์ด้วย Comment หรือ UR
- Run a DOS command คือสามารถที่ Run command เพื่อส่งไปยัง Endpoint
- Run a registry command คือ สามรถที่ Run command registry เพื่อส่งไปยัง Endpoint

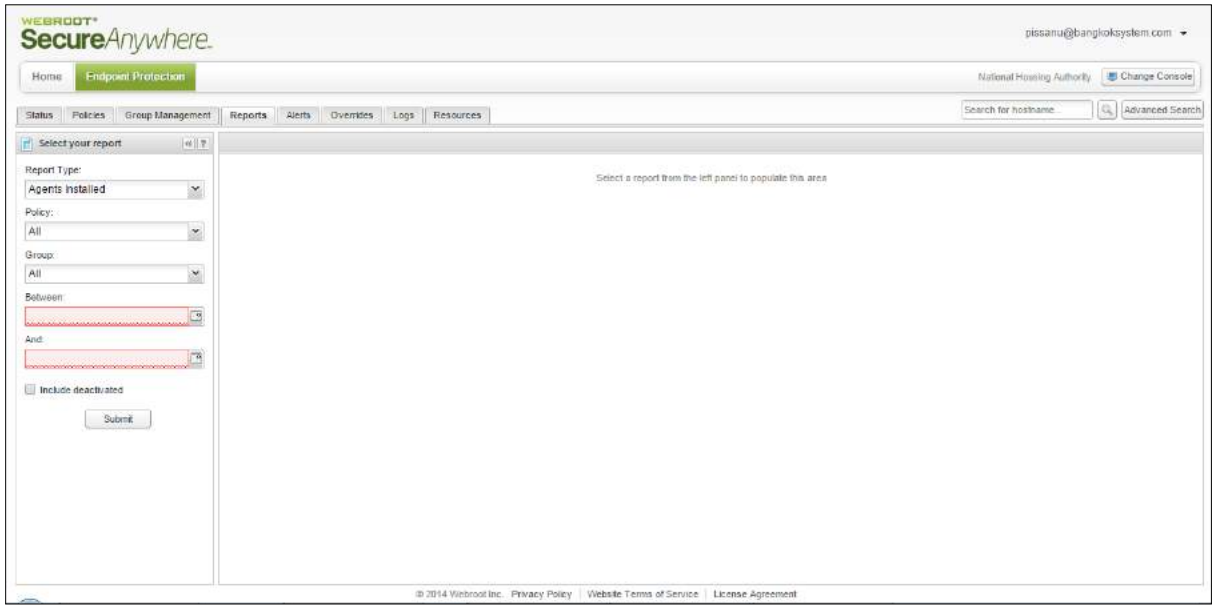
View commands for selected endpoints คือสามรถที่จะทำการตรวจสอบตรวจ คำสั่งที่มีการส่งไปให้ Endpoint ได้รับคำสั่งไปให้หรือยัง

How to use Agent commands คือ แสดงวิธีการใช้งานคำสั่งต่างๆ (วิดีโอ)

6.Deactivate คือเป็นการจัดการคืน license และรวมไปถึงไม่ได้ถูกจัดการของ Webroot อีกต่อไป หลังจาก Deactivate endpoint จะย้ายไปกลุ่ม Deactivate ทันที

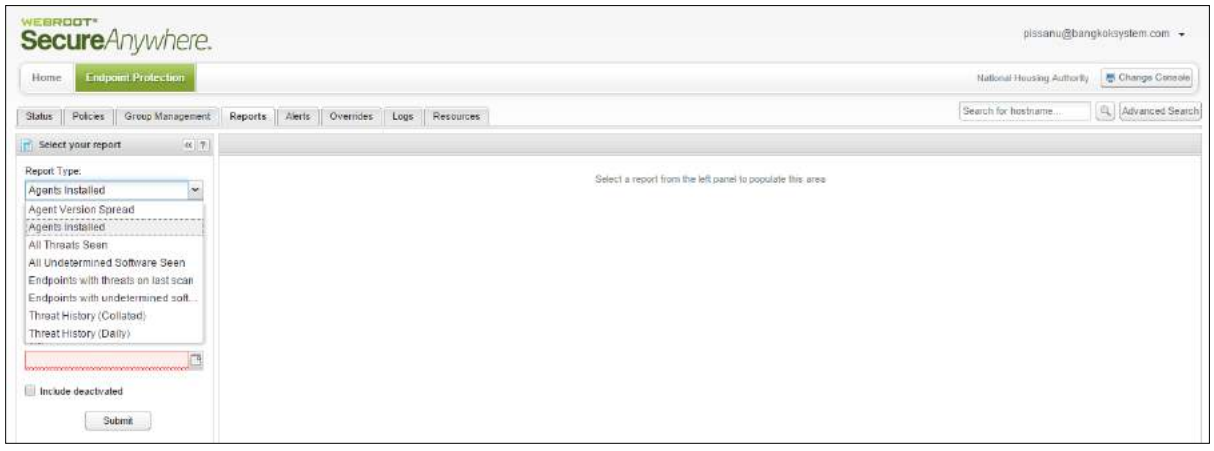
7. Polices used in All endpoint เป็นการแสดงรายละเอียดของกลุ่มและPolicy

Reports



การเรียกดูในส่วนของรายงาน (Reports) สามารถเลือก Reports ได้จากส่วนต่าง ๆ คือ

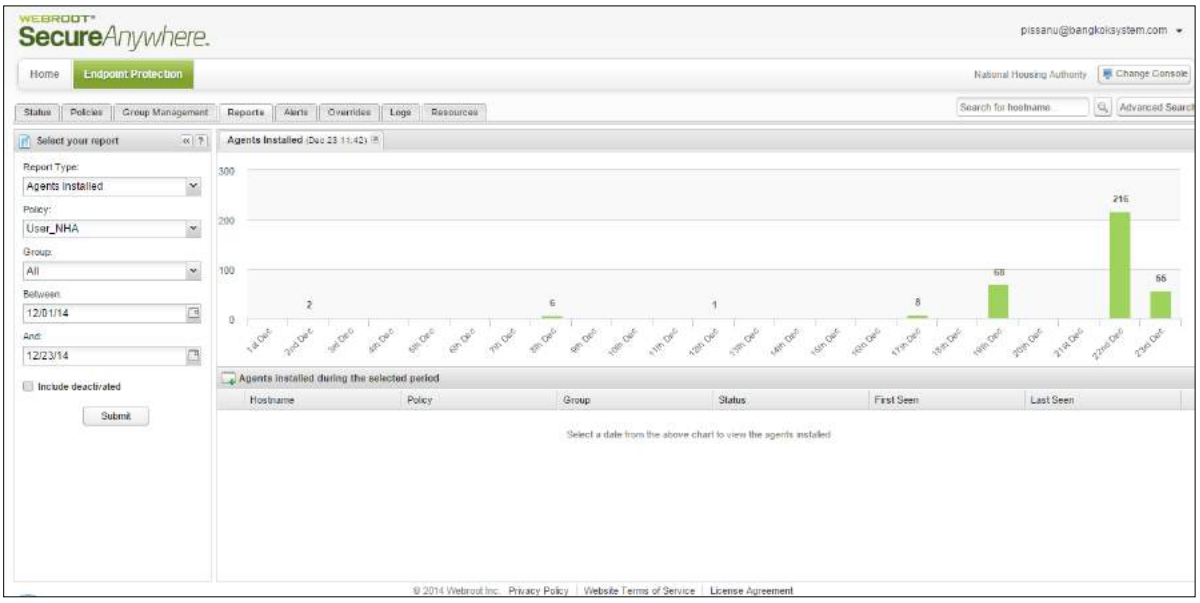
- **Report Type** แสดงรายงานตามรายการแต่ละประภท
- **Policy** แสดงรายงานแต่ละ Policy ของผู้ใช้แต่ละกลุ่มที่ได้มีการกำหนดไว้
- **Group** แสดงตามกลุ่ม
- **ระหว่างวันที่** แสดงรายงานตามวันที่ ที่ระบุระหว่างวันที่เท่าไร ถึง เท่าไร
- **ส่วน Deactivated** แสดงในส่วนของผู้ใช้ที่ได้มีการ Deactivated



Report Type

- **Agent Version Spread** เวอร์ชันของแต่ละEndpoints
- **Agents Installed** การติดตั้งโปรแกรมของ Agent
- **All Threats Seen** ไฟล์ที่มีความเสี่ยงทั้งหมด
- **All Undetermined Software Seen** ไฟล์ที่มีความเสี่ยงที่ถูกกักเก็บไว้
- **Endpoints with threats on last scan.** Endpoints ที่มีภัยคุกคามที่ตรวจพบล่าสุด
- **Endpoints with undetermined software on last scan**. Endpointsและไฟล์ที่มีความเสี่ยงที่ถูกกักเก็บไว้ ที่มีการตรวจพบล่าสุด
- **Threat History (Collated)** ประวัติไฟล์ความเสี่ยงทั้งหมด
- **Threat History (Daily)** ประวัติไฟล์ความเสี่ยง (แสดงเป็นรายวัน)

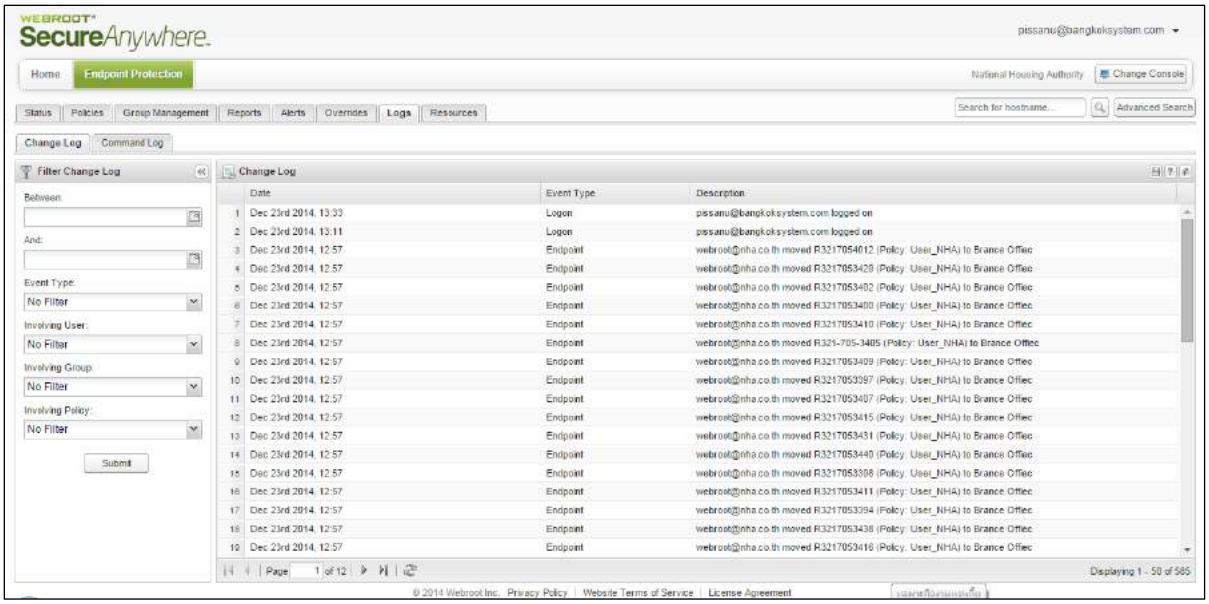
แสดงตัวอย่างรายงาน



Log

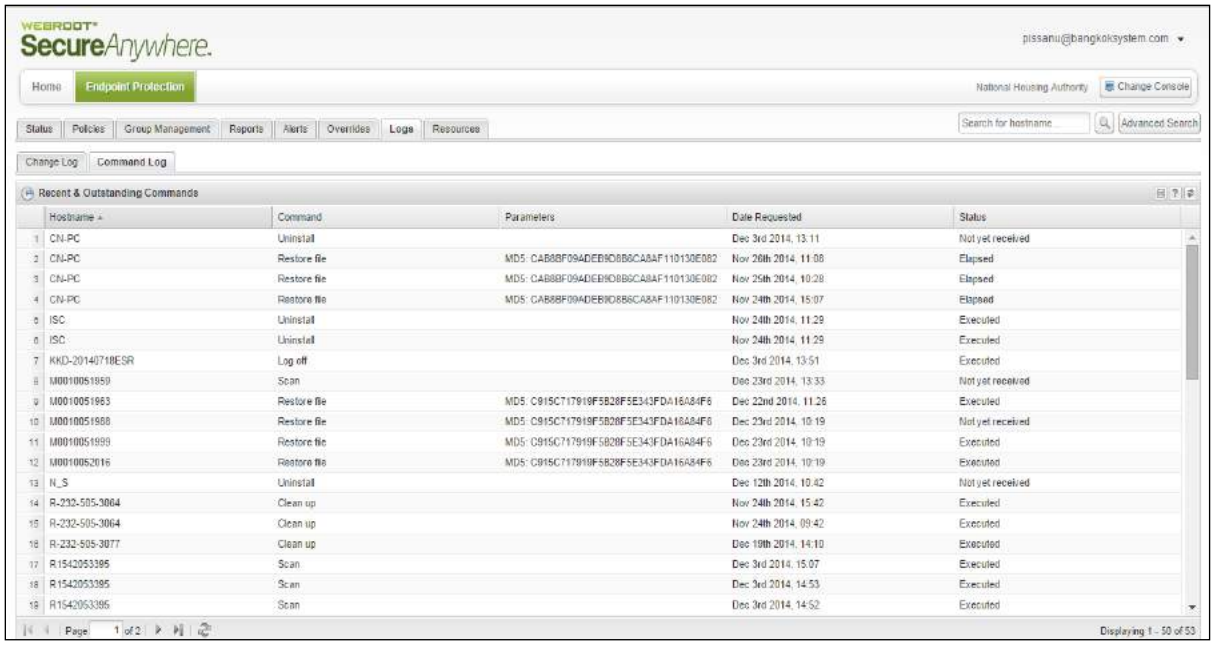
แสดงรายละเอียด 2 ส่วน คือ **Change Log** และ **Command log**

1. **Change Log**



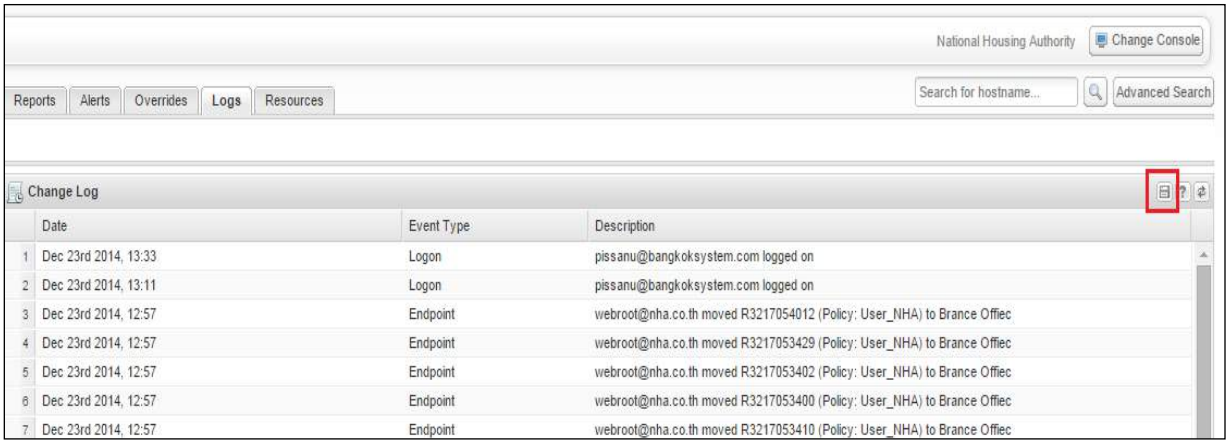
การ Filter Change log สามารถ Filter ได้โดย

- **การระบุ** ช่วงเวลาที่ต้องการ
- **Event Type** ตามประเภทเหตุการณ์ เช่น Group, Endpoint, Policy, Override และ Logon
- **Involving User** โดยผู้ที่เกี่ยวข้อง
- **Involving Group** โดยกลุ่มที่เกี่ยวข้อง
- **Involving Policy** โดยนโยบายที่เกี่ยวข้อง



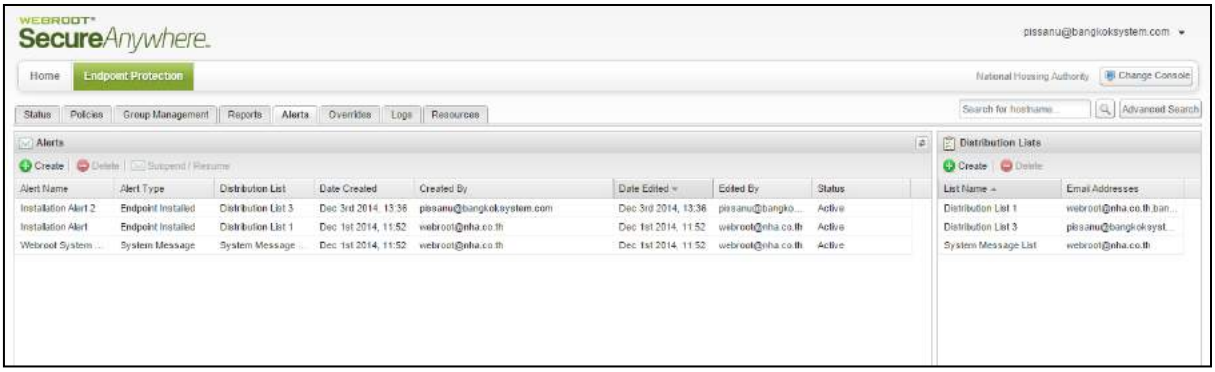
2.Command log คือ แสดงรายการ log ที่เกิดจากการ Command ที่มีการส่งคำสั่งไปที่ Endpoints

สามารถที่จะทำการ Export เป็นไฟล์ CSV.



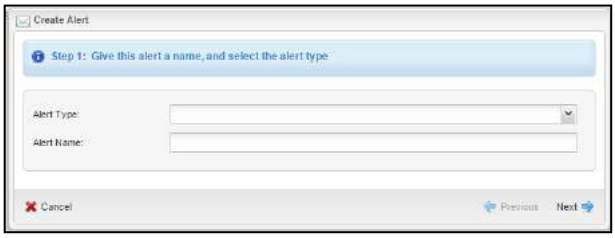
Alerts

การแสดงการแจ้งเตือน สามารถทำการสร้างการแจ้งเตือนในลักษณะต่าง ๆ ได้

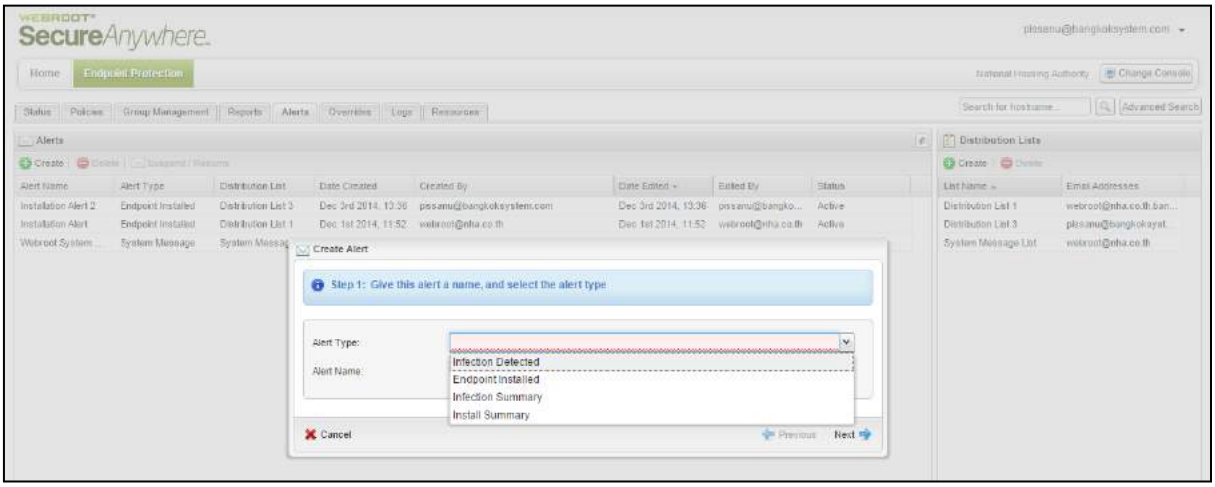


ในส่วนการ Create Alerts

Create

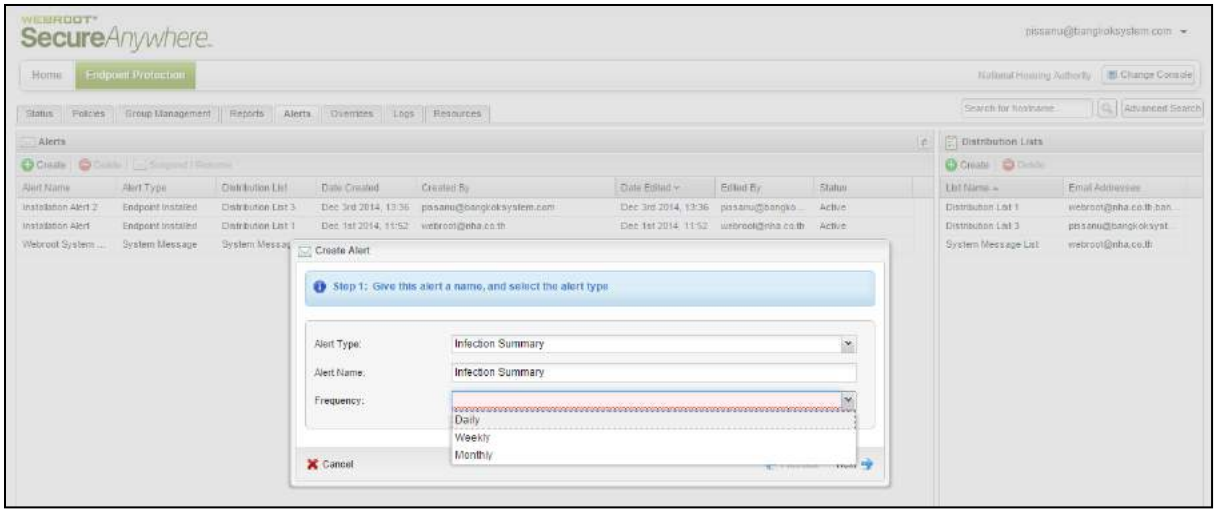


- สามารถระบุตามชนิดแสดงดังหน้าจอด้านล่าง



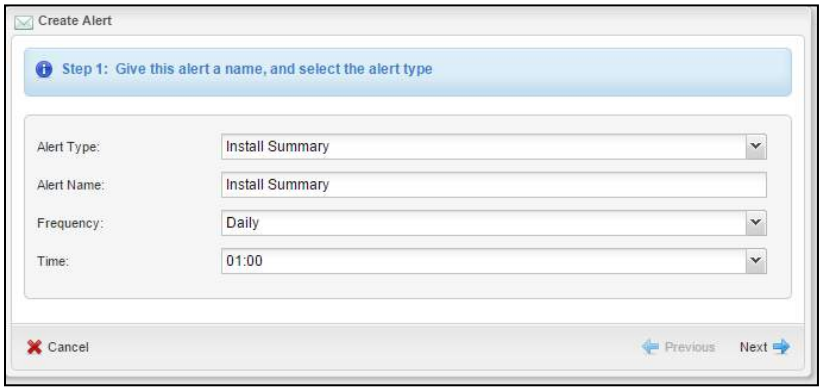
- **Infection Detected** การตรวจพบไฟล์ที่เป็นความเสี่ยงทั้งหมด
- **Endpoint Installed** การติดตั้งที่เครื่อง Endpoint
- **Infection Summary** สรุปรายการทั้งหมด
- **Install Summary** สรุปรายการที่ได้ติดตั้ง

- ในส่วนรายการ Summary จะมี Frequency ให้ระบุความถี่เป็นรายวัน สัปดาห์ หรือเดือนได้ แสดงรายละเอียดดังหน้าจอด้านล่าง

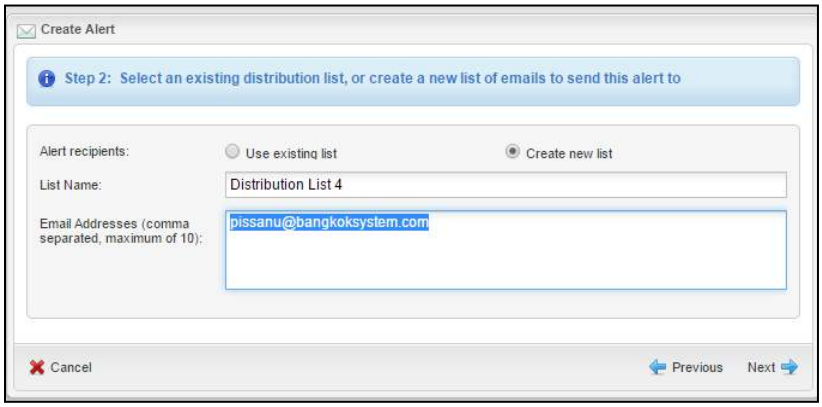


ตัวอย่างการ สร้าง Alerts

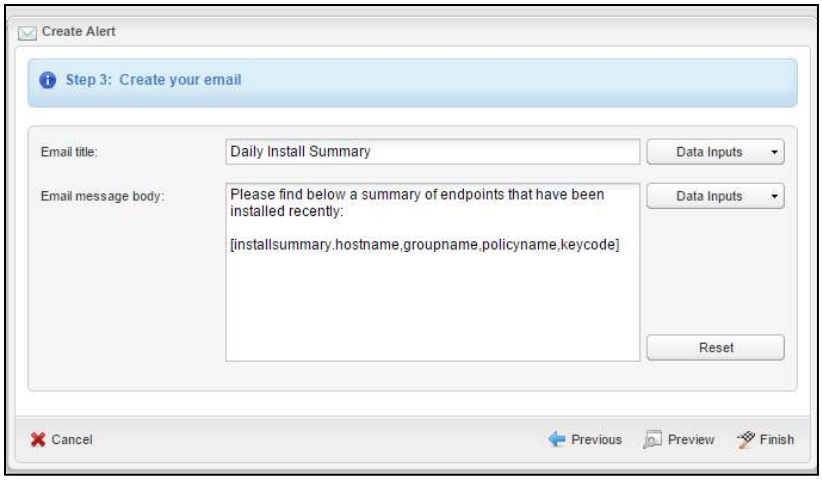
1. ระบุระเภท , ชื่อ , ระยะเวลา , เวลา



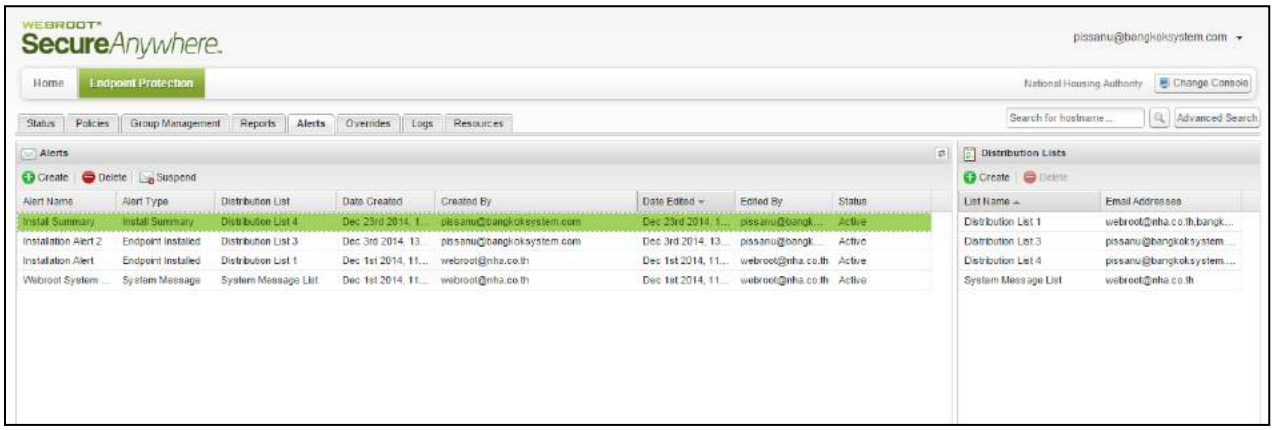
2. ทำการระบุ List Name ที่มีอยู่เดิม หรือทำการสร้างขึ้นมาใหม่เพื่อสร้าง E-mail เพื่อส่งการแจ้งเตือน



3. การสร้าง email แจ้งเตือน

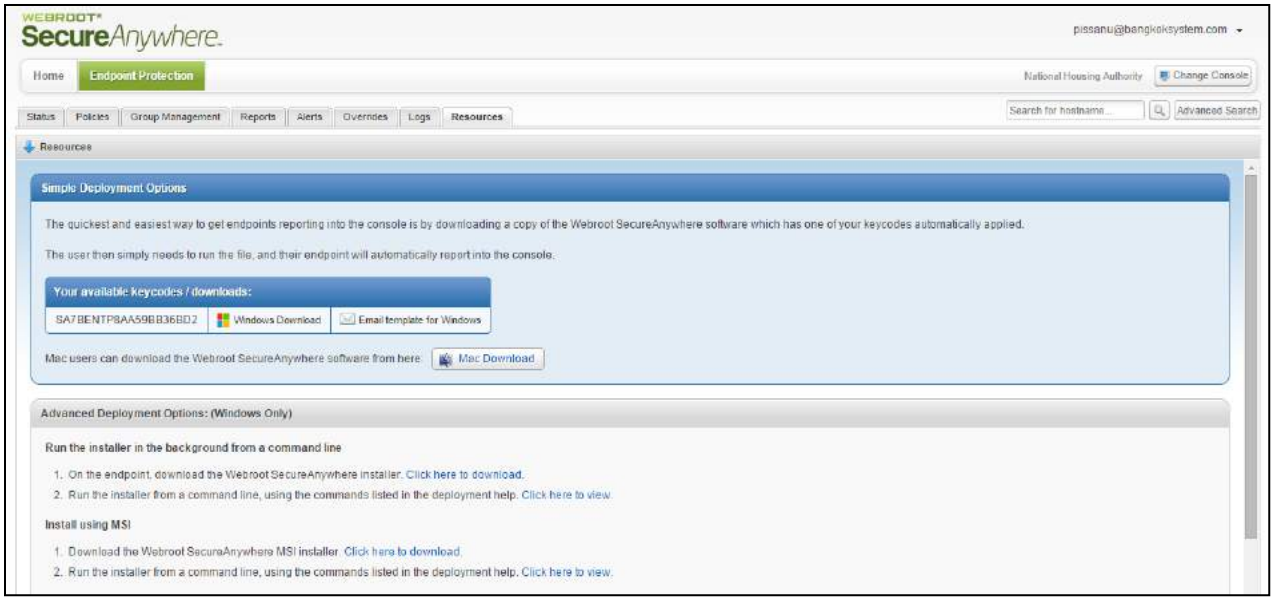


4. เมื่อมีการสร้างเรียบร้อยแล้ว ก็จะส่งการแจ้งเตือนตามเงื่อนไขที่ได้ระบุ



Resources

ส่วนแสดงทรัพยากร ที่สามารถ downloads



ประกอบด้วย 2 ส่วน คือ

- **Simple Deployment Options**

สามารถที่จะ Deploy ไฟล์.EXE ไปยังเครื่อง Agent โดยมีการ add ส่วนของ Key codes โดยเลือกที่ **Windows Download** เพื่อ download สำหรับวินโดว์ หรือส่งรายละเอียดผ่าน email ให้ผู้ใช้คลิก link เพื่อทำการติดตั้งเองได้

ในส่วนนี้รองรับใช้งานที่เป็นเครื่อง Mac ด้วย โดยเลือกที่ Mac Download

- **Advanced Deployment Options**

เป็นการจัดการไฟล์โปรแกรมที่เป็น .MSI ที่สามารถนำไปใช้ Deploy ผ่าน Group Policy User

- สามารถดูรายละเอียดขั้นตอนการติดตั้งได้ โดยคลิกที่รายละเอียดด้านล่าง

Run the installer from a command line, using the commands listed in the deployment help. Click here to view.