ENTERPRISE SECURITY

SEQRITE

20+ Glorious Years of Quick Heal Technologies

Our Brands

Quick Heal
Security Simplified

SEQRITE

Business Segments

- Home and SOHO
- SME
- Government and Enterprise

Platforms

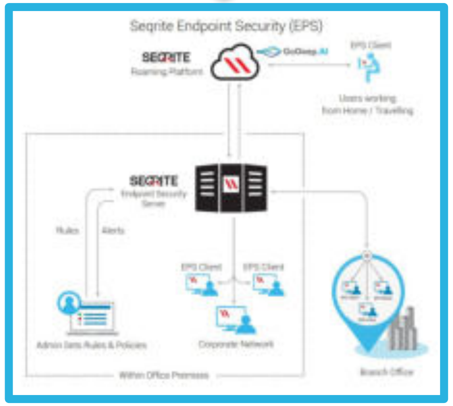
- Desktop, Laptop
- Mobile, Notepad
- Server

34% Market Share	**18.4 Mn** Active Licenses
70,000+ Enterprise Customers	**4** No. of Patents in US
80+ **Countries** Global Presence	**52,092** Number of Partners

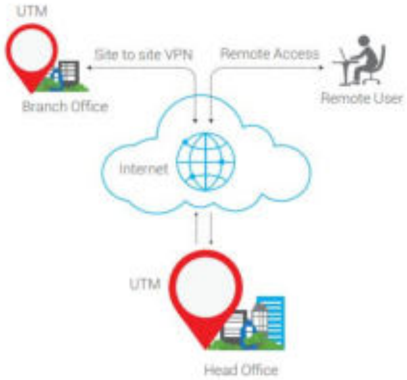
Seqrite Product

Enterprise Security and Management.

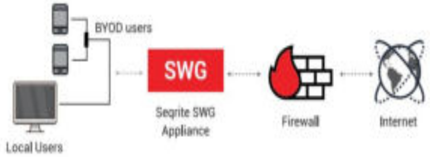
ENDPOINT SECURITY



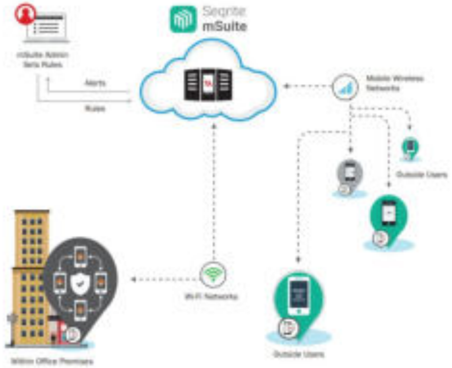
Unified Threat Management



Web Gateway Security



Enterprise Mobility Management



Workspace Management

Encryption Manager

OUR CERTIFICATE COMPLIANCE

ISO/IEC 20000-1
มาตรฐานการจัดการบริการด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับในระดับสากล

ISO 27001
มาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (ISMS)

Health Insurance Portability and Accountability Act (HIPAA)
มาตรฐานการป้องกันการเก็บรักษาข้อมูลของผู้รับบริการ

Payment Card Industry Data Security Standard (PCI DSS)
มาตรฐานความปลอดภัยสารสนเทศ

General Data Protection Regulation (General Data Protection Regulation)
มาตรฐานระเบียบการคุ้มครองข้อมูลทั่วไป

Cyber Security Act (CSA)
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

Personal Data Protection Act (PDPA)
พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

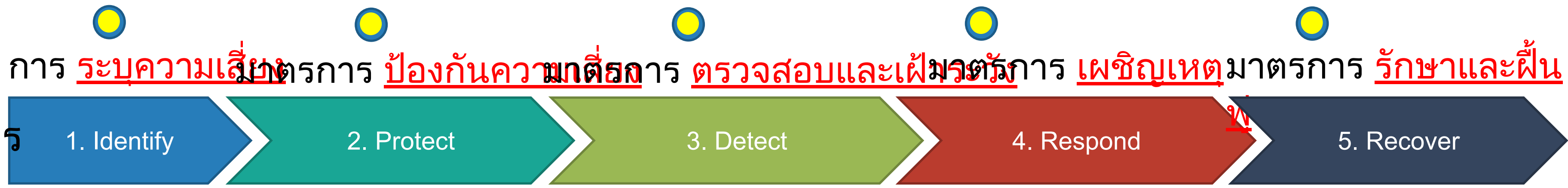
OUR CERTIFICATE COMPLIANCE

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

Cyber Security Act (CSA)

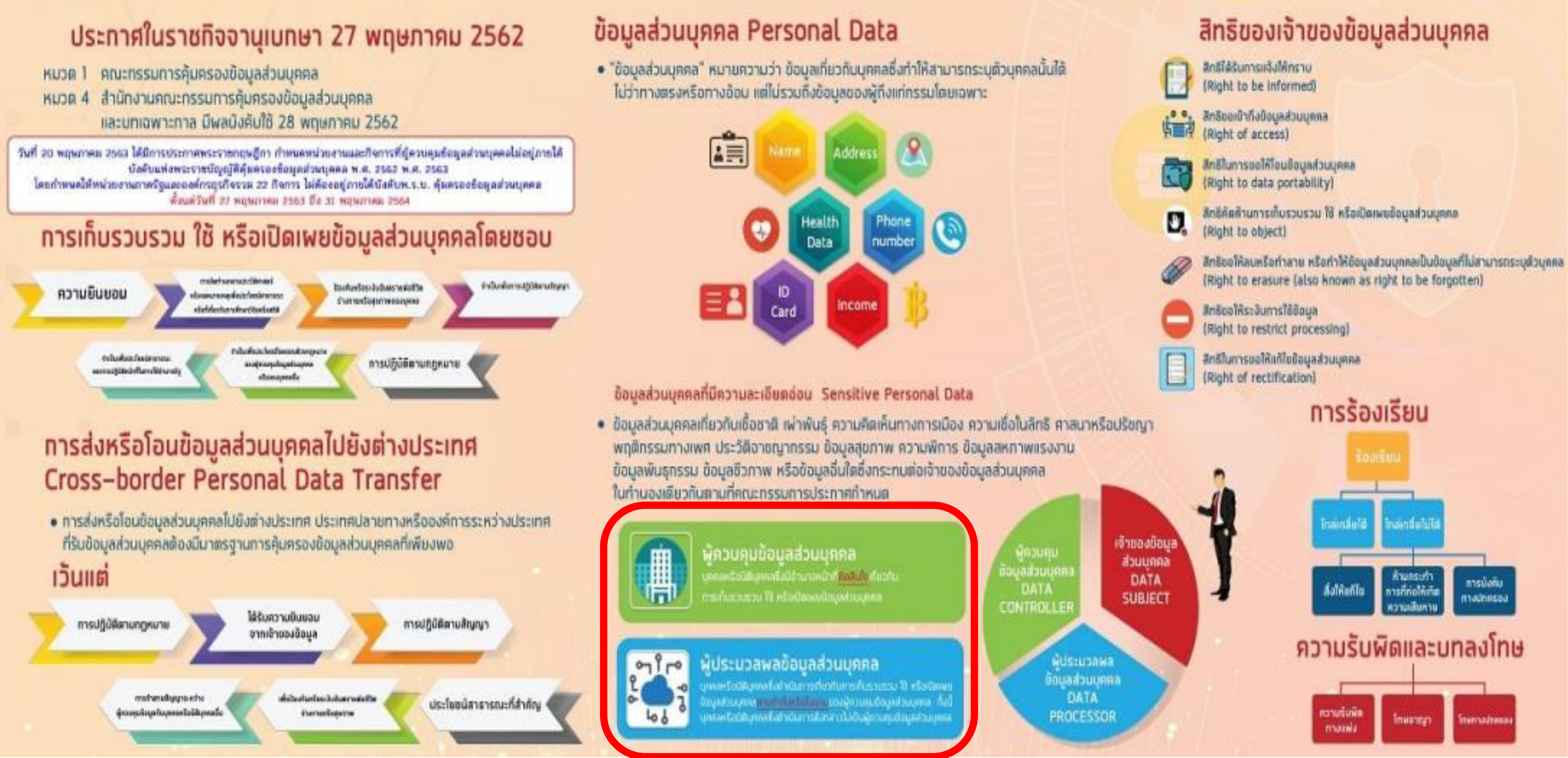
กฎหมายฉบับนี้ถูกบังคับใช้กับหน่วยงานของรัฐหรือหน่วยงานเอกชน
ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)
รวมทั้งสิ้น 6 กลุ่ม ได้แก่

- ด้านความมั่นคงของรัฐ และ บริการภาครัฐที่สำคัญ
- ด้านการเงินการธนาคาร
- ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
- ด้านการขนส่งและโลจิสติกส์
- ด้านพลังงานและสาธารณูปโภค
- ด้านสาธารณสุข



Vulnerability	Patch Management	IDS/IPS	Machine Learning	Files Backup & Restore
Asset Monitor	Web Control	Port Scan Attract Detection	Emulation Based Detection	Disk Clean-up
	Device Control	DDOSS Attract Detection	Cloud Based Deep Learning	Registry Clean-up
	Application Control	Web Gateway Protection	Cloud Based Threat Intelligence Global	Defragmentation
	Self-Protection	Mail Protection		
	Safe Mode Protection	Device Protection	Email Notification	
		Anti-virus	Dashboard & Report	
		Anti-Malware		
		Anti-Ransomware		
		Anti-Key Logger		

พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
Personal Data Protection Act (PDPA)



ประกาศในราชกิจจานุเบกษา 27 พฤษภาคม 2562

หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
และบทเฉพาะกาล มีผลบังคับใช้ 28 พฤษภาคม 2562

วันที่ 20 พฤษภาคม 2563 ได้มีการประกาศพระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้
บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563
โดยกำหนดให้หน่วยงานภาครัฐและองค์กรธุรกิจรวม 22 กิจการ ไม่ต้องอยู่ภายใต้บังคับพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
ตั้งแต่วันที่ 27 พฤษภาคม 2563 ถึง 31 พฤษภาคม 2564

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยชอบ

- ความยินยอม
- การจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ
- ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล
- จำเป็นเพื่อการปฏิบัติตามสัญญา
- จำเป็นเพื่อประโยชน์สาธารณะ และการปฏิบัติหน้าที่ในการใช้อำนาจรัฐ
- จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลอื่น
- การปฏิบัติตามกฎหมาย

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ Cross-border Personal Data Transfer

- การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

เว้นแต่

- การปฏิบัติตามกฎหมาย
- ได้รับความยินยอมจากเจ้าของข้อมูล
- การปฏิบัติตามสัญญา
- การทำตามสัญญาระหว่างผู้ควบคุมข้อมูลกับบุคคลหรือนิติบุคคลอื่น
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ
- ประโยชน์สาธารณะที่สำคัญ

ข้อมูลส่วนบุคคล Personal Data

- "ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน Sensitive Personal Data

- ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

ผู้ควบคุมข้อมูลส่วนบุคคล

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล DATA CONTROLLER
เจ้าของข้อมูลส่วนบุคคล DATA SUBJECT
ผู้ประมวลผลข้อมูลส่วนบุคคล DATA PROCESSOR

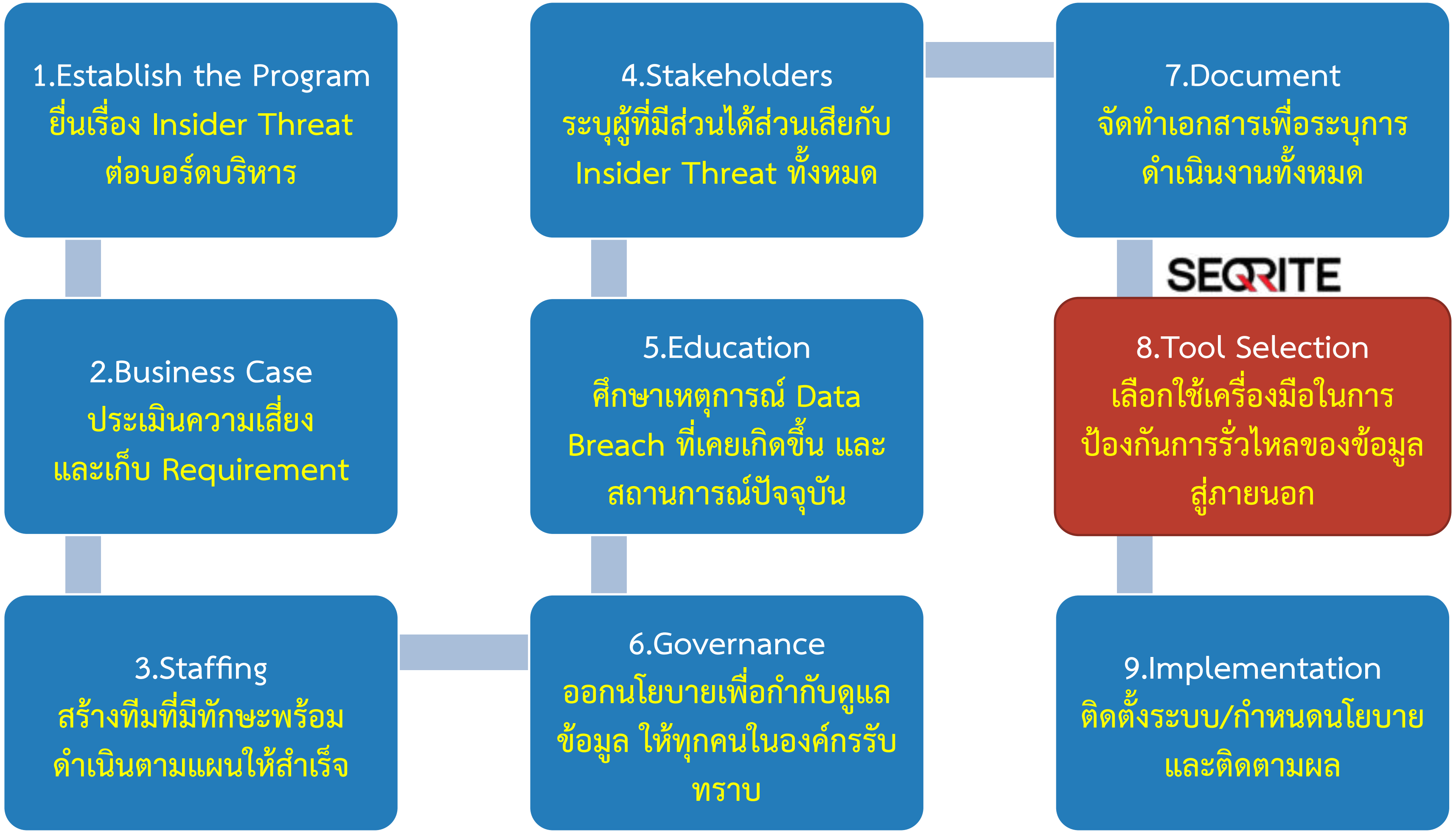
สิทธิของเจ้าของข้อมูลส่วนบุคคล

- สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)
- สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
- สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
- สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
- สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure (also known as right to be forgotten)
- สิทธิขอให้ระงับการใช้ข้อมูล (Right to restrict processing)
- สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right of rectification)

การร้องเรียน

ความรับผิดและบทลงโทษ

9 ขั้นตอนในการดำเนินแผนงาน PDPA



1.Establish the Program
ยื่นเรื่อง Insider Threat
ต่อบอร์ดบริหาร

2.Business Case
ประเมินความเสี่ยง
และเก็บ Requirement

3.Staffing
สร้างทีมที่มีทักษะพร้อม
ดำเนินตามแผนให้สำเร็จ

4.Stakeholders
ระบุผู้ที่มีส่วนได้ส่วนเสียกับ
Insider Threat ทั้งหมด

5.Education
ศึกษาเหตุการณ์ Data
Breach ที่เคยเกิดขึ้น และ
สถานการณ์ปัจจุบัน

6.Governance
ออกนโยบายเพื่อกำกับดูแล
ข้อมูล ให้ทุกคนในองค์กรรับ
ทราบ

7.Document
จัดทำเอกสารเพื่อระบุการ
ดำเนินงานทั้งหมด

8.Tool Selection
เลือกใช้เครื่องมือในการ
ป้องกันการรั่วไหลของข้อมูล
สู่ภายนอก

9.Implementation
ติดตั้งระบบ/กำหนดนโยบาย
และติดตามผล

SEQRITE PDPA COMPLIANCE

PDPA TEAM

01 Protection against theft

- ป้องกันการโจรกรรมข้อมูลโดย Hacker
- ป้องกันการโจรกรรมข้อมูลโดย Malware
- ป้องกันการทำลายข้อมูลโดย Ransomware

02 Control & Monitor

- กำหนดนโยบายในการใช้งาน เว็ปไซต์ อุปกรณ์ต่อพ่วง และ โปรแกรม
- ติดตามการเปลี่ยนแปลง Copy, Rename, Delete ของไฟล์
- ติดตามการเปลี่ยนแปลงของ อุปกรณ์ และ โปรแกรม

03 Data loss Prevention

- ป้องกันการนำข้อมูลออกจากเครื่องหรือออกจากองค์กร ในระดับ เนื้อหาในเอกสาร
- ค้นหาข้อมูลที่มีเนื้อหาตามที่ทีม PDPA แจ้งมา ว่ามีอยู่ที่ใดบ้างในองค์กร

04 Files Backup & Restore

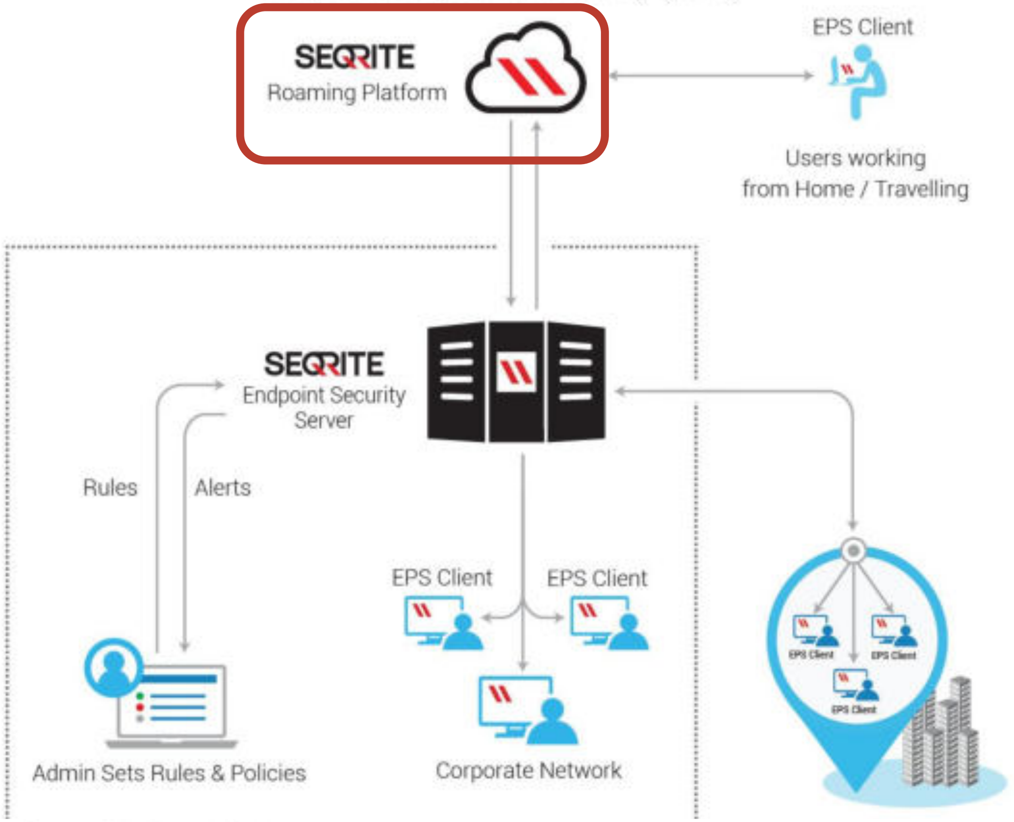
- มีระบบสำรองข้อมูลไฟล์ และสามารถนำข้อมูลกลับมาได้ ในกรณีที่ข้อมูลสูญหาย หรือถูกทำลาย

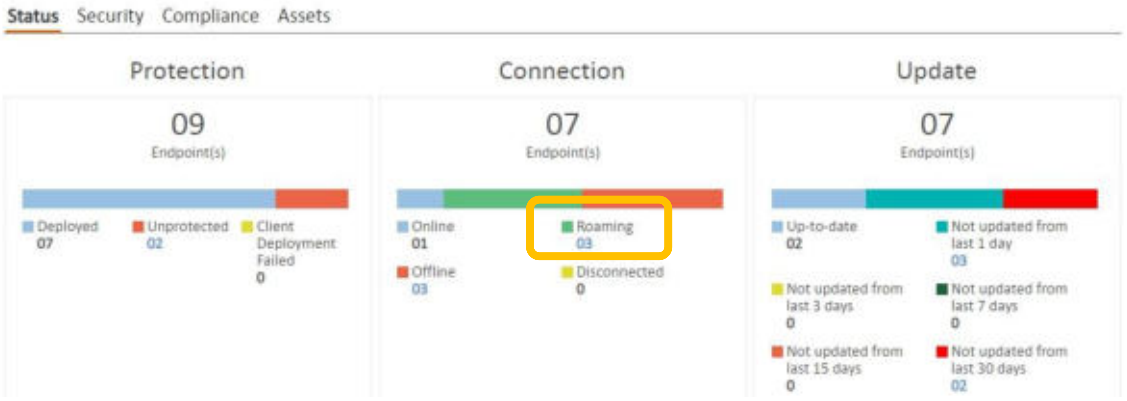
05 Notification & Report

- มีระบบแจ้งเตือนผู้ดูแลระบบ และออกรายงานได้

NEXGENERATION SEQRITE Endpoint Management (All in one endpoint Solution)

Seqrite Endpoint Security (EPS)




Status Security Compliance Assets

Protection

09
Endpoint(s)

Deployed 07
Unprotected 02
Client Deployment Failed 0

Connection

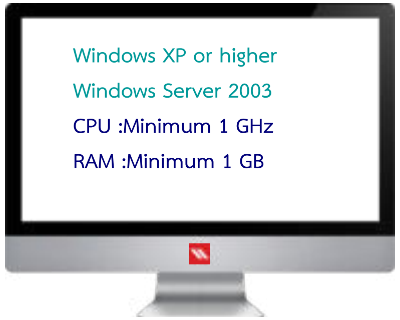
07
Endpoint(s)

Online 01
Roaming 03
Offline 03
Disconnected 0

Update

07
Endpoint(s)

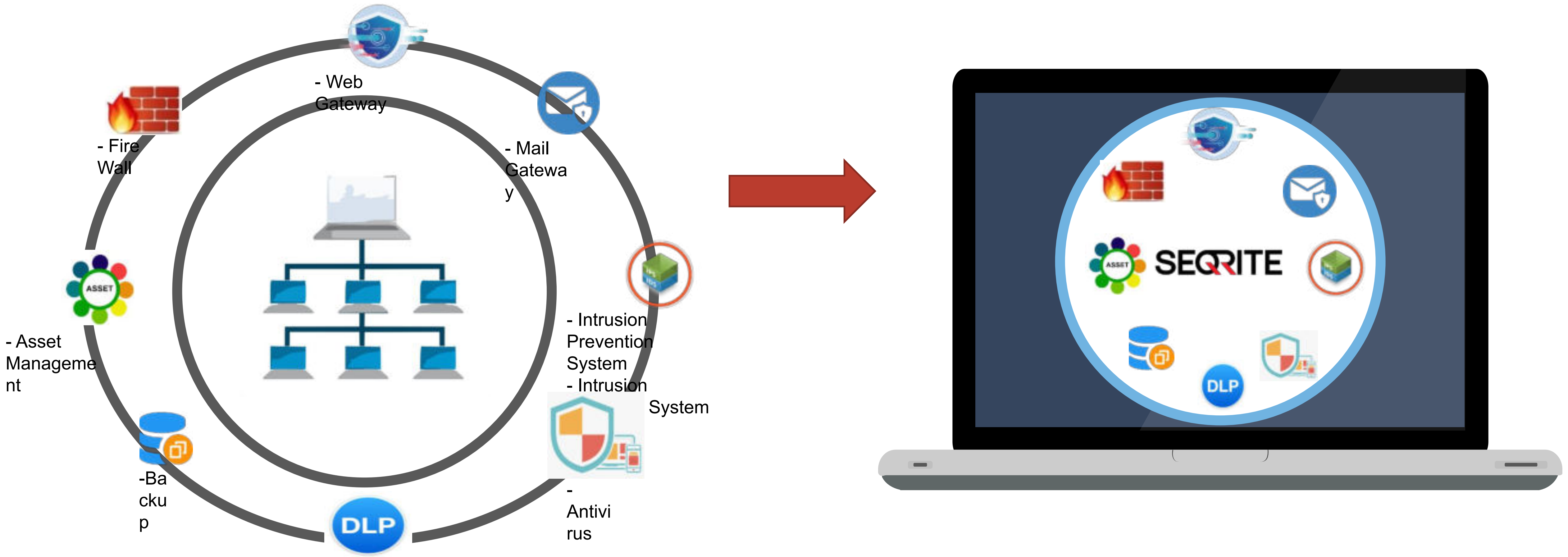
Up-to-date 02
Not updated from last 1 day 03
Not updated from last 3 days 0
Not updated from last 7 days 0
Not updated from last 15 days 0
Not updated from last 30 days 02


Windows XP or higher
Windows Server 2003
CPU :Minimum 1 GHz
RAM :Minimum 1 GB

Next generation Seqrite Endpoint Security (EPS) Multi Layer Protection.

SEQRITE

Multi Layer Protection

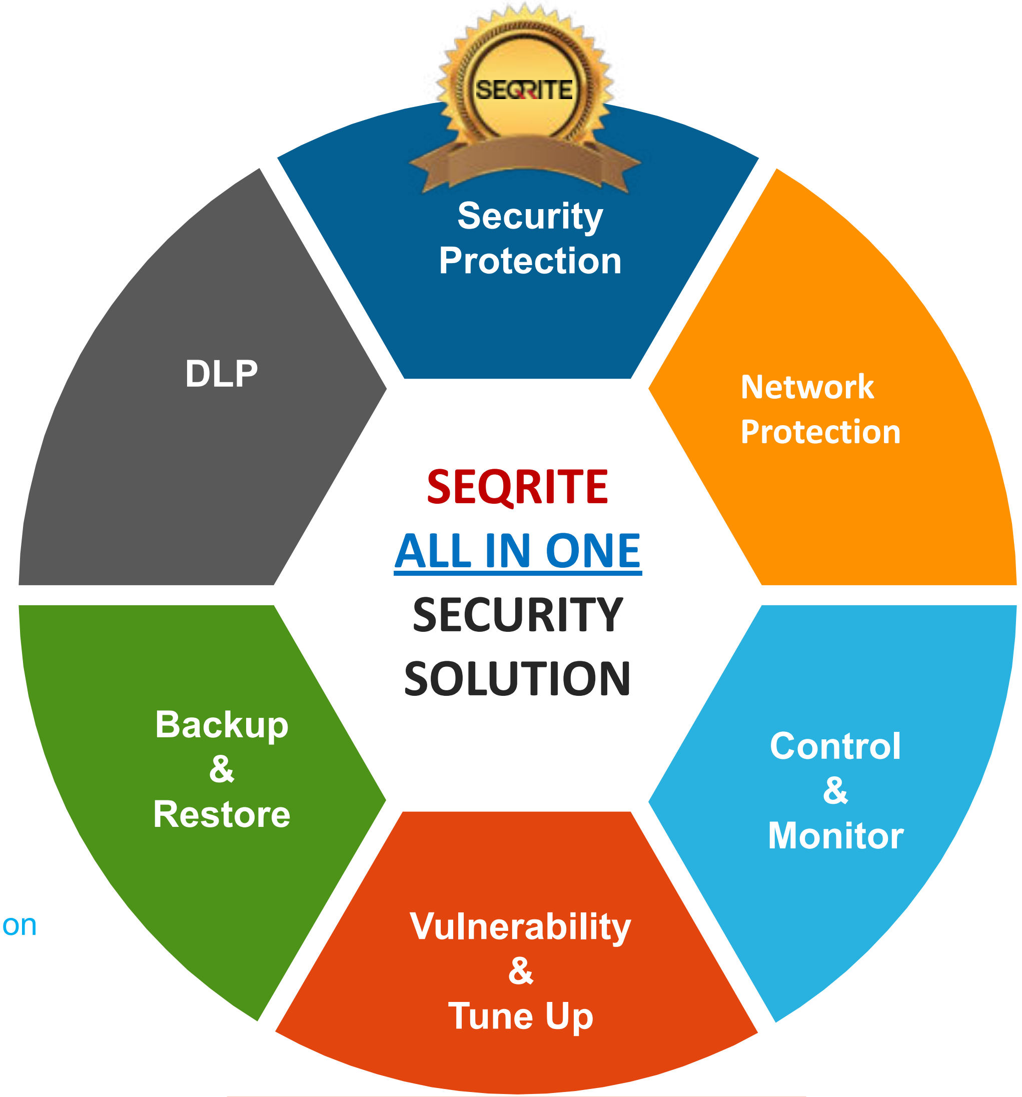


NEXGENERATION SEQRITE ENDPOINT SECURITY (All in one endpoint Solution)

- Web Protection
- Mail Protection
- Device Protection

Confidential Data Loss Prevention
- Files Type
- Pattern Data
- Key word

- Backup document files before malware and ransomware attack
- Incremental ,Compress ,Encrypt Solution
- Restore document files for malware and ransomware attack



- Anti-virus
- Anti-Malware
- Anti-Ransomware
- Anti-Key Logger
- GoDeep AI
- Safe Mode Protection

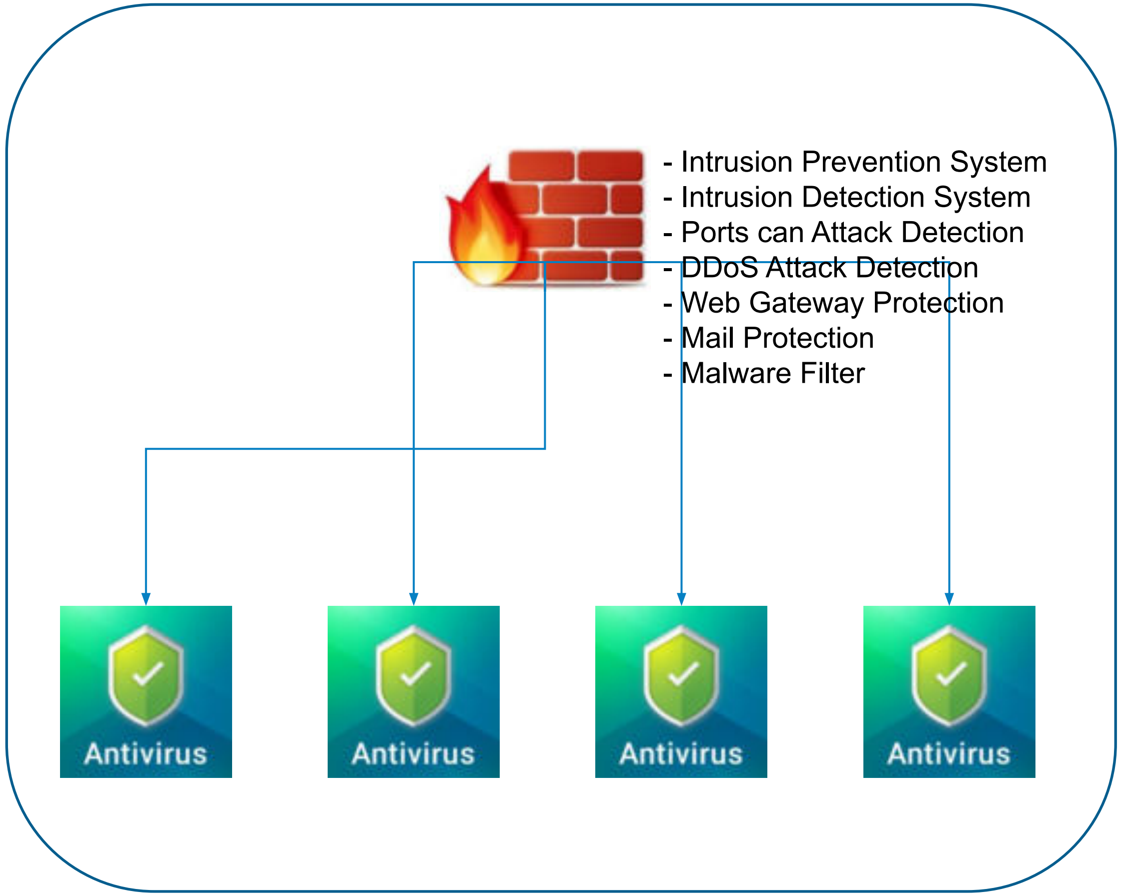
-Intrusion Detection System (IDS)
-Intrusion Prevention System (IPS)
-Port Scan Attract Detection
-DDOSS Attract Detection
- **RDP brute force attack.**

- Web Control
- Device Control
- Application Control
- Files Monitor
- Asset Monitor

- Vulnerability Scan
- **Virtual Patching**
- Patch Management

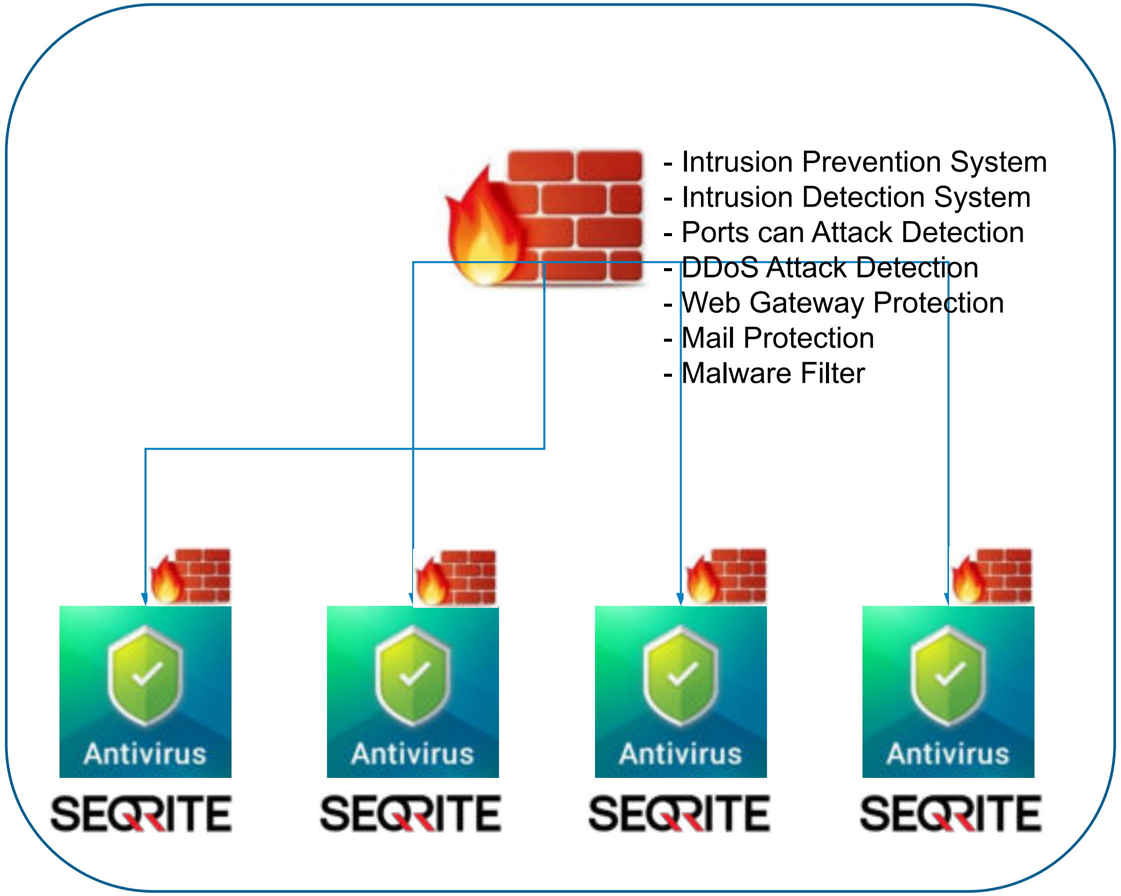
- Disk Clean-up , Register Clean-up ,Defragment

Next generation Seqrite Endpoint Security (EPS) Multi Layer Protection.



- Intrusion Prevention System
- Intrusion Detection System
- Ports can Attack Detection
- DDoS Attack Detection
- Web Gateway Protection
- Mail Protection
- Malware Filter

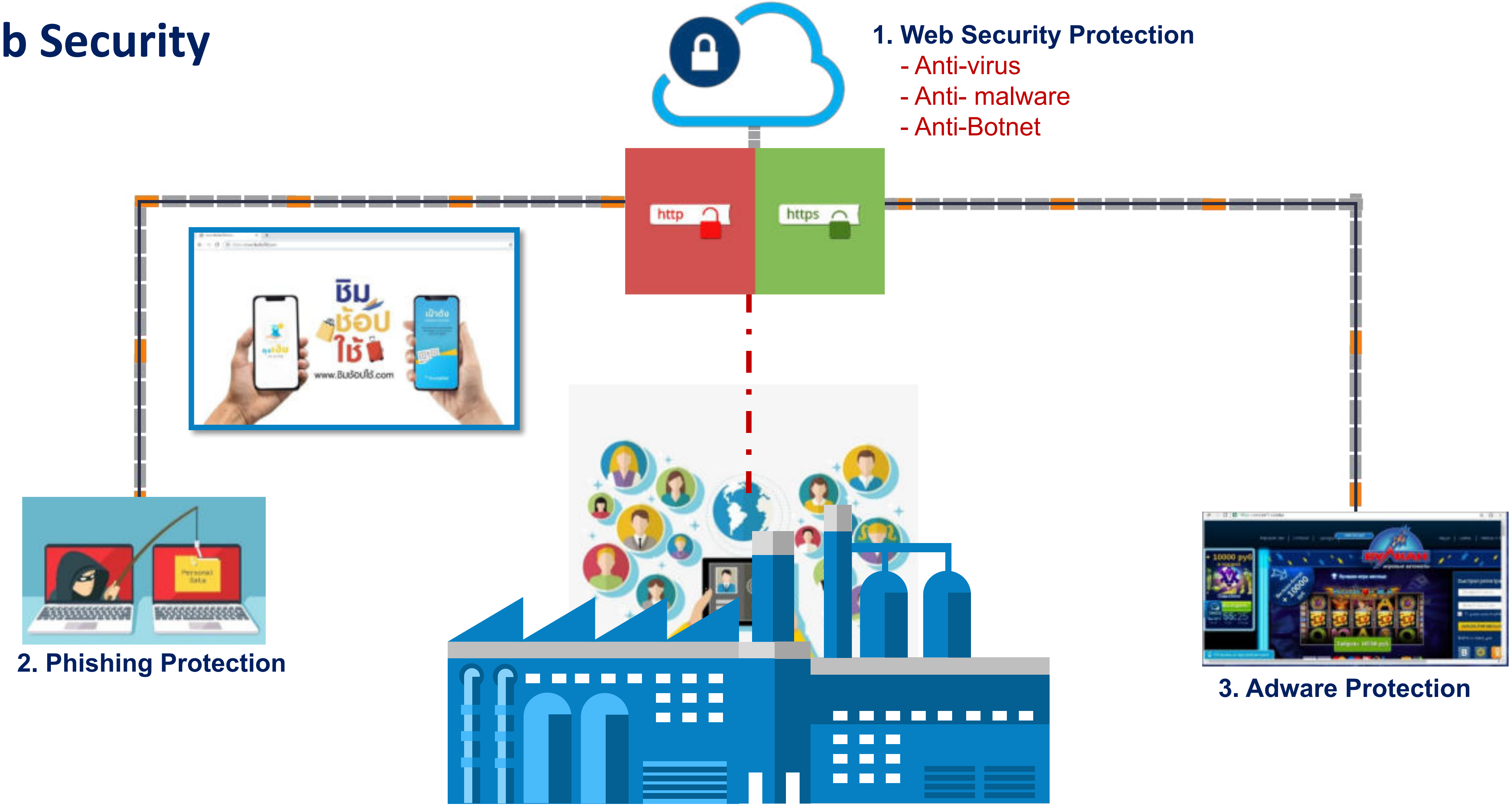
SEQRITE Multi Layer Protection



- Intrusion Prevention System
- Intrusion Detection System
- Ports can Attack Detection
- DDoS Attack Detection
- Web Gateway Protection
- Mail Protection
- Malware Filter

Next generation Seqrite Endpoint Security (EPS) Web Security Feature.

Web Security



1. Web Security Protection
   - Anti-virus
   - Anti- malware
   - Anti-Botnet

2. Phishing Protection

3. Adware Protection

Next generation Seqrite Endpoint Security (EPS) E-mail Security Feature.

E-mail Security

Email Protection

- Virus Protection
- Malware Protection

Attachment Control

Spam Protection

Whitelists and Blacklists

Next generation Seqrite Endpoint Security (EPS) Device Security Feature.

Scan External Drives

สามารถสแกนไดรฟ์ที่ใช้ USB ได้ทันทีที่เชื่อมต่อกับระบบ

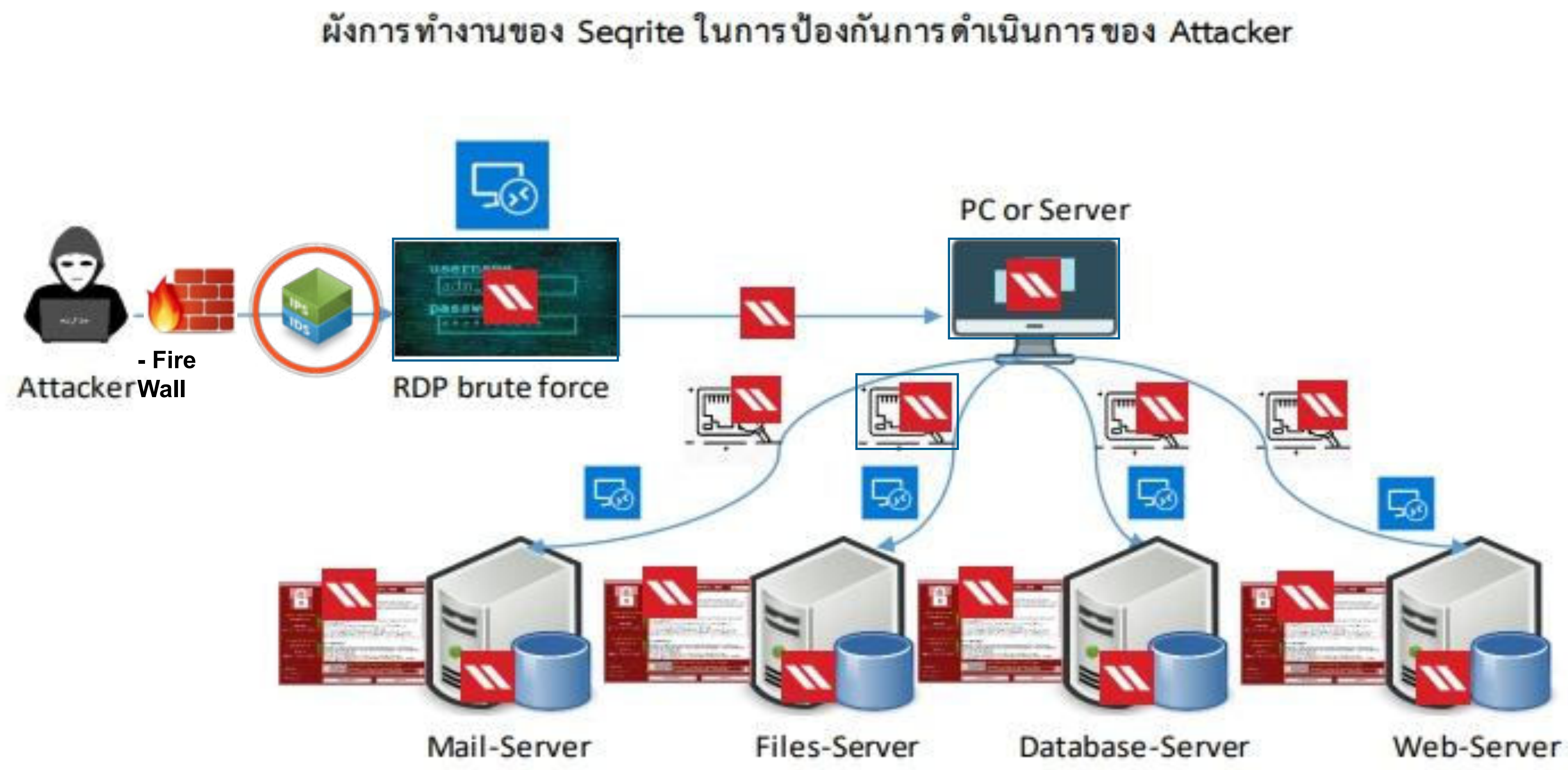
Autorun Protection

ปกป้องระบบของ จากมัลแวร์ที่ทำงานอัตโนมัติ จากอุปกรณ์USB หรือ ซีดี / ดีวีดี

Mobile Scan

สแกนหาไวรัสสปายแวร์และมัลแวร์อื่น ๆ ในโทรศัพท์มือถือ ในกรณีที่เชื่อมต่อจากสาย USB หรือ Bluetooth

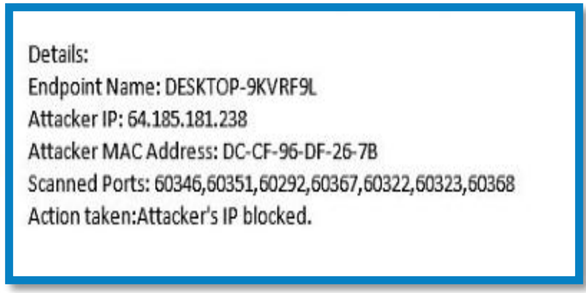
Next generation Seqrite Endpoint Security (EPS) Network Protection Feature.



Network Protection

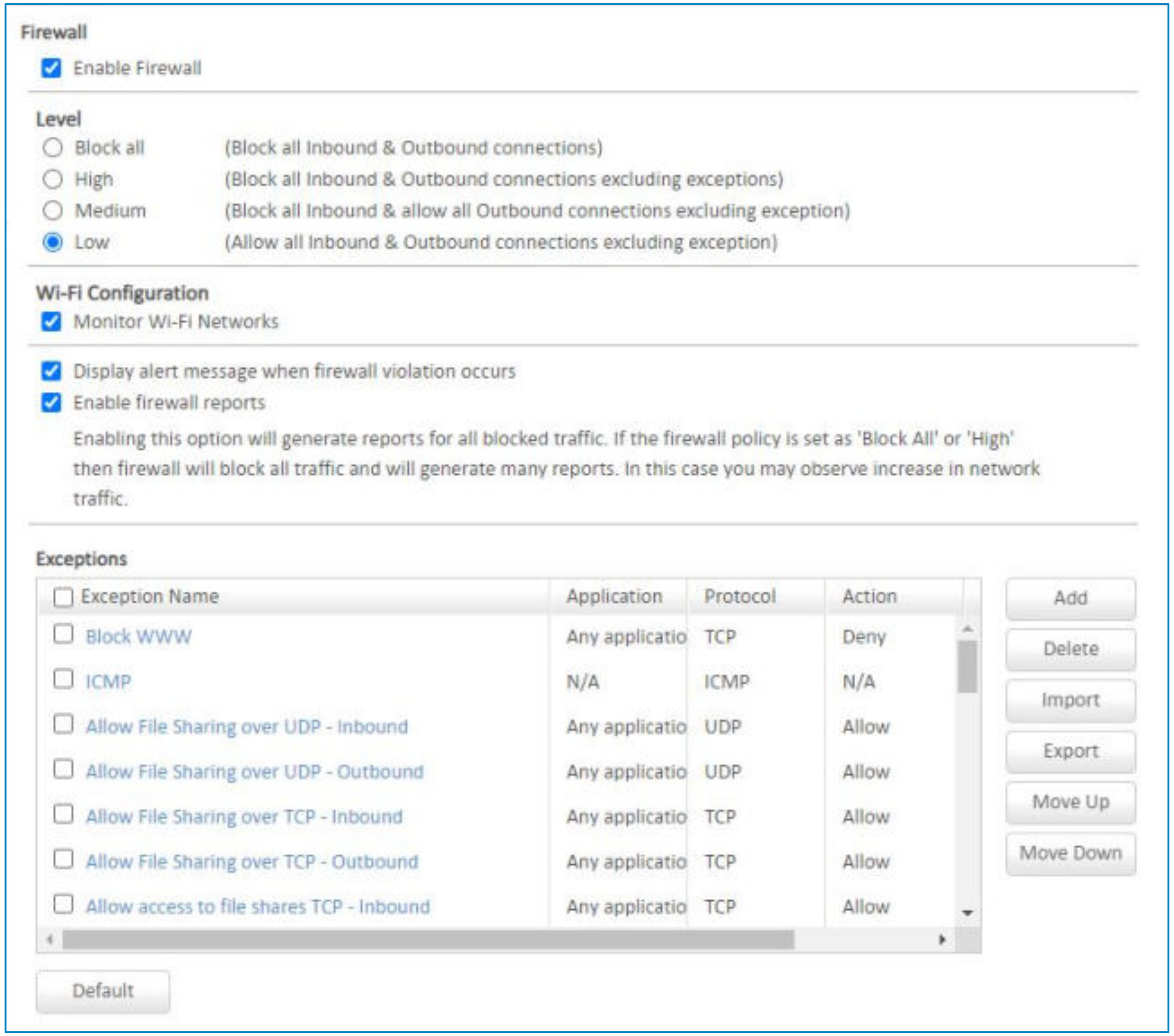
Multilayered Protection

- Anti-Virus
- Firewall
- IDS/IPS
- Port Scan Attack Detection
- DDOS Attack Detection (*)
- Source of Infection



Details:
Endpoint Name: DESKTOP-9KVRF9L
Attacker IP: 64.185.181.238
Attacker MAC Address: DC-CF-96-DF-26-7B
Scanned Ports: 60346,60351,60292,60367,60322,60323,60368
Action taken:Attacker's IP blocked.

Next generation Seqrite Endpoint Security (EPS) Network Protection Feature.



Firewall

☑ Enable Firewall

Level

○ Block all (Block all Inbound & Outbound connections)
○ High (Block all Inbound & Outbound connections excluding exceptions)
○ Medium (Block all Inbound & allow all Outbound connections excluding exception)
● Low (Allow all Inbound & Outbound connections excluding exception)

Wi-Fi Configuration

☑ Monitor Wi-Fi Networks

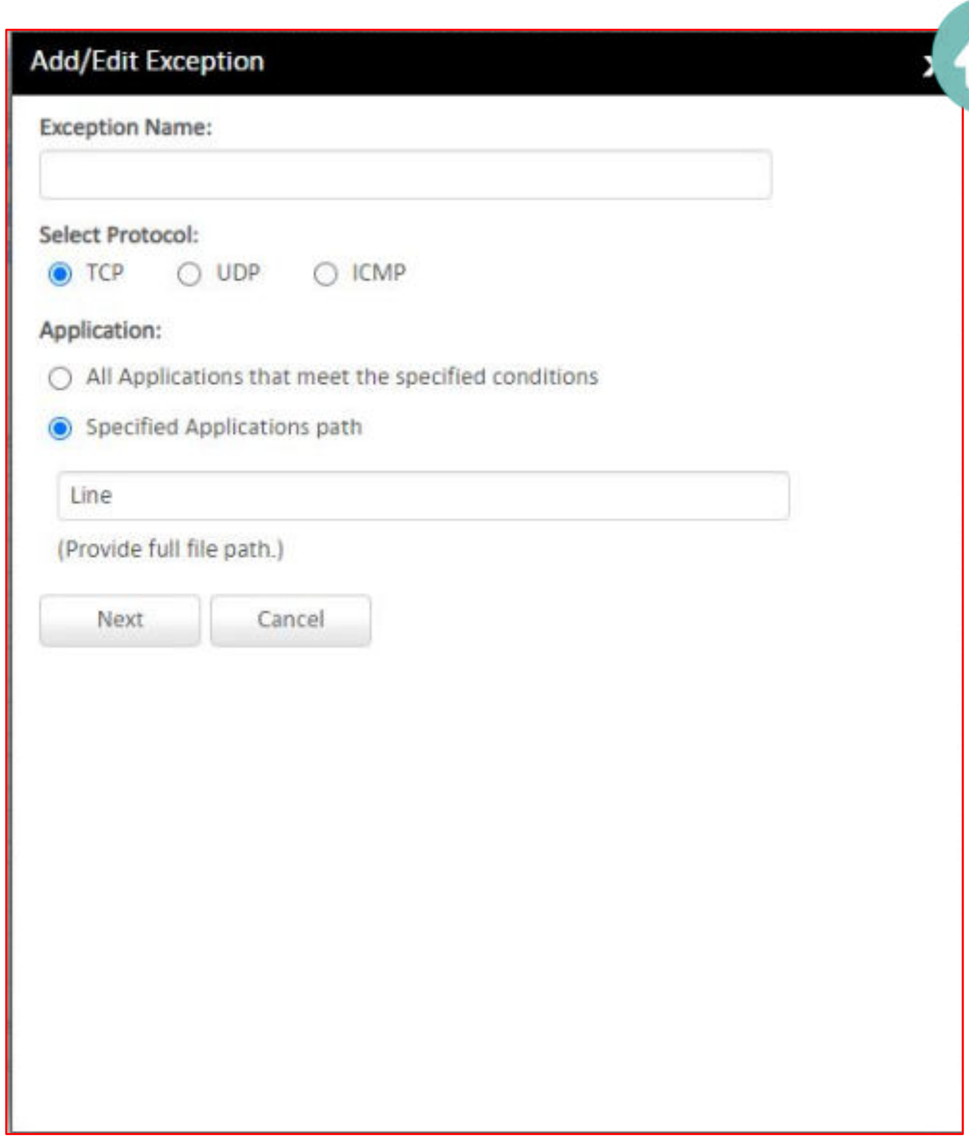
☑ Display alert message when firewall violation occurs

☑ Enable firewall reports

Enabling this option will generate reports for all blocked traffic. If the firewall policy is set as 'Block All' or 'High' then firewall will block all traffic and will generate many reports. In this case you may observe increase in network traffic.

Exceptions

□ Exception Name	Application	Protocol	Action
□ Block WWW	Any applicatio	TCP	Deny
□ ICMP	N/A	ICMP	N/A
□ Allow File Sharing over UDP - Inbound	Any applicatio	UDP	Allow
□ Allow File Sharing over UDP - Outbound	Any applicatio	UDP	Allow
□ Allow File Sharing over TCP - Inbound	Any applicatio	TCP	Allow
□ Allow File Sharing over TCP - Outbound	Any applicatio	TCP	Allow
□ Allow access to file shares TCP - Inbound	Any applicatio	TCP	Allow



Add/Edit Exception

Exception Name:

Select Protocol:

● TCP ○ UDP ○ ICMP

Application:

○ All Applications that meet the specified conditions

● Specified Applications path

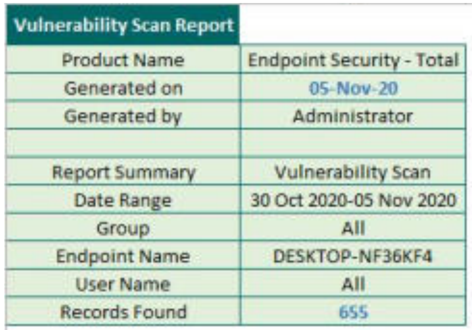
Line

(Provide full file path.)

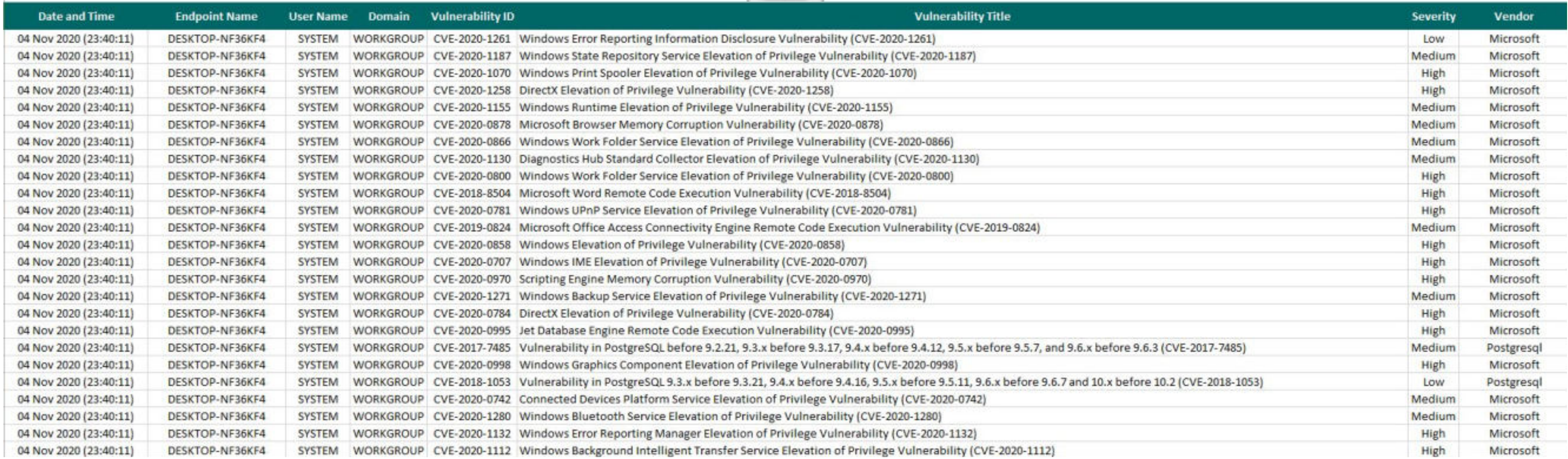
Next generation Seqrite Endpoint Security (EPS) Network Protection Feature.

IDS/I
S

Virtual Patching

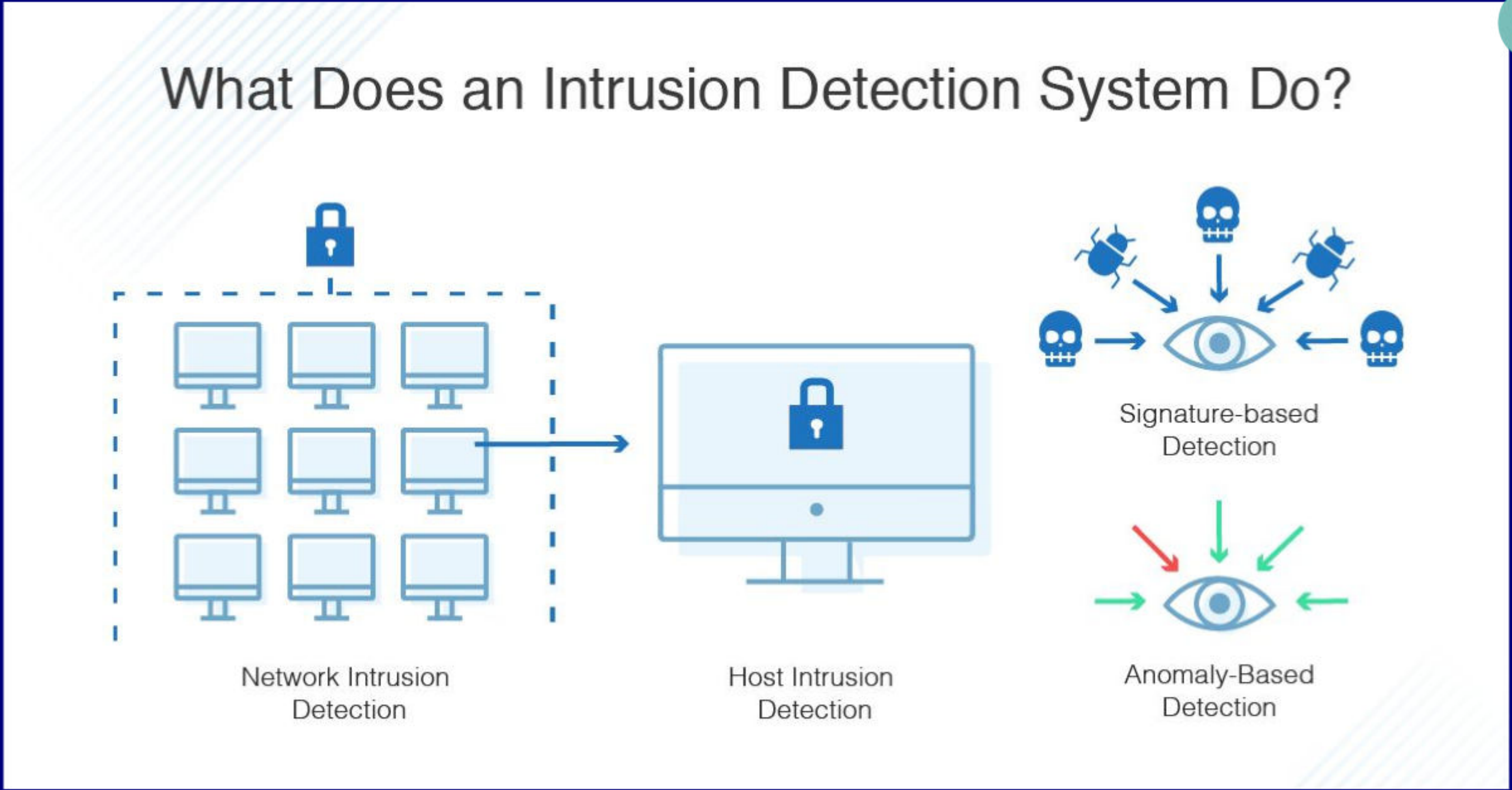


Vulnerability Scan Report	
Product Name	Endpoint Security - Total
Generated on	05-Nov-20
Generated by	Administrator
Report Summary	Vulnerability Scan
Date Range	30 Oct 2020-05 Nov 2020
Group	All
Endpoint Name	DESKTOP-NF36KF4
User Name	All
Records Found	655



Date and Time	Endpoint Name	User Name	Domain	Vulnerability ID	Vulnerability Title	Severity	Vendor
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1261	Windows Error Reporting Information Disclosure Vulnerability (CVE-2020-1261)	Low	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1187	Windows State Repository Service Elevation of Privilege Vulnerability (CVE-2020-1187)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1070	Windows Print Spooler Elevation of Privilege Vulnerability (CVE-2020-1070)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1258	DirectX Elevation of Privilege Vulnerability (CVE-2020-1258)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1155	Windows Runtime Elevation of Privilege Vulnerability (CVE-2020-1155)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0878	Microsoft Browser Memory Corruption Vulnerability (CVE-2020-0878)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0866	Windows Work Folder Service Elevation of Privilege Vulnerability (CVE-2020-0866)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1130	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability (CVE-2020-1130)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0800	Windows Work Folder Service Elevation of Privilege Vulnerability (CVE-2020-0800)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2018-8504	Microsoft Word Remote Code Execution Vulnerability (CVE-2018-8504)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0781	Windows UPnP Service Elevation of Privilege Vulnerability (CVE-2020-0781)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2019-0824	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability (CVE-2019-0824)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0858	Windows Elevation of Privilege Vulnerability (CVE-2020-0858)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0707	Windows IME Elevation of Privilege Vulnerability (CVE-2020-0707)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0970	Scripting Engine Memory Corruption Vulnerability (CVE-2020-0970)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1271	Windows Backup Service Elevation of Privilege Vulnerability (CVE-2020-1271)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0784	DirectX Elevation of Privilege Vulnerability (CVE-2020-0784)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0995	Jet Database Engine Remote Code Execution Vulnerability (CVE-2020-0995)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2017-7485	Vulnerability in PostgreSQL before 9.2.21, 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3 (CVE-2017-7485)	Medium	Postgresql
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0998	Windows Graphics Component Elevation of Privilege Vulnerability (CVE-2020-0998)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2018-1053	Vulnerability in PostgreSQL 9.3.x before 9.3.21, 9.4.x before 9.4.16, 9.5.x before 9.5.11, 9.6.x before 9.6.7 and 10.x before 10.2 (CVE-2018-1053)	Low	Postgresql
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0742	Connected Devices Platform Service Elevation of Privilege Vulnerability (CVE-2020-0742)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1280	Windows Bluetooth Service Elevation of Privilege Vulnerability (CVE-2020-1280)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1132	Windows Error Reporting Manager Elevation of Privilege Vulnerability (CVE-2020-1132)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1112	Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability (CVE-2020-1112)	High	Microsoft

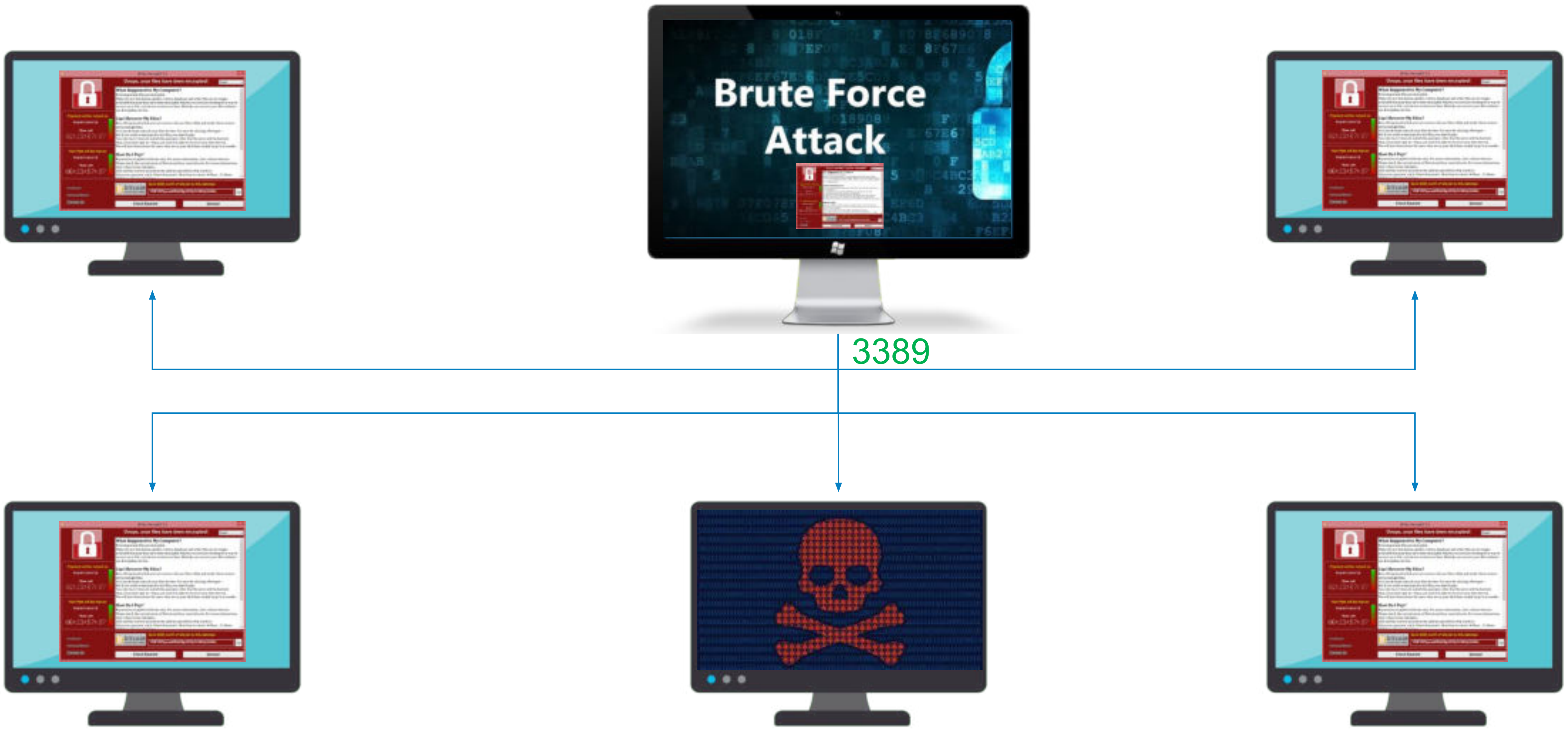
Next generation Seqrite Endpoint Security (EPS) IDS /IPS Feature.



What Does an Intrusion Detection System Do?

Next generation Seqrite Endpoint Security (EPS)

RDP brute force



Next generation Seqrite Endpoint Security (EPS)

Report For - Seqrite Endpoint Security Intrusion Detection & Prevention

Friday, 11 October, 2019, Time 09:59:10

Seqrite Endpoint Security Version - 18.00

Virus database - 09 October 2019

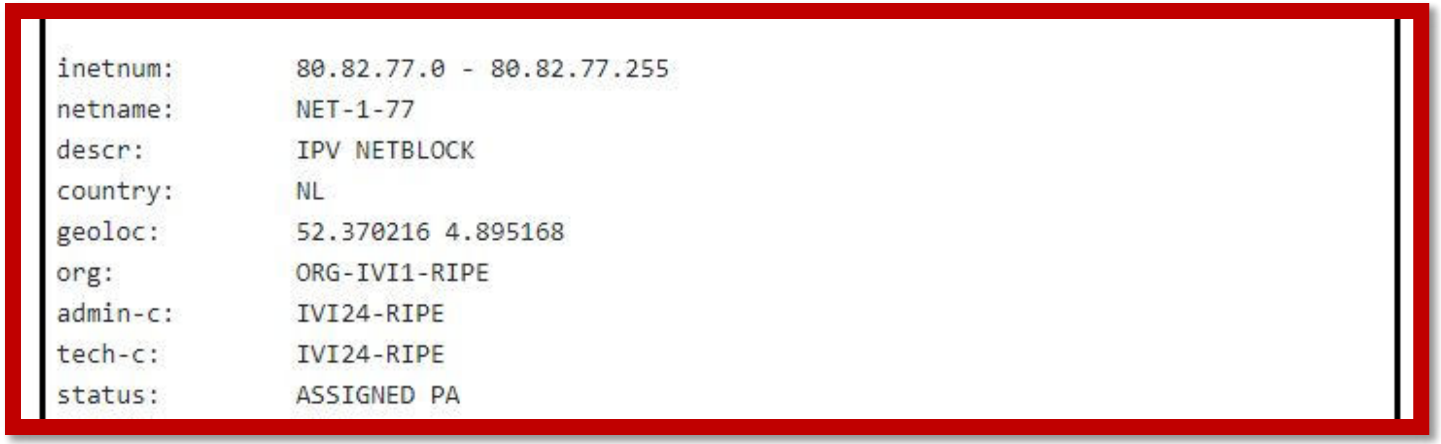
Action Taken: Attacker's IP blocked.

Vulnerability detected: **RDP brute force attack.**

Description: Brute force attack on remote desktop protocol.

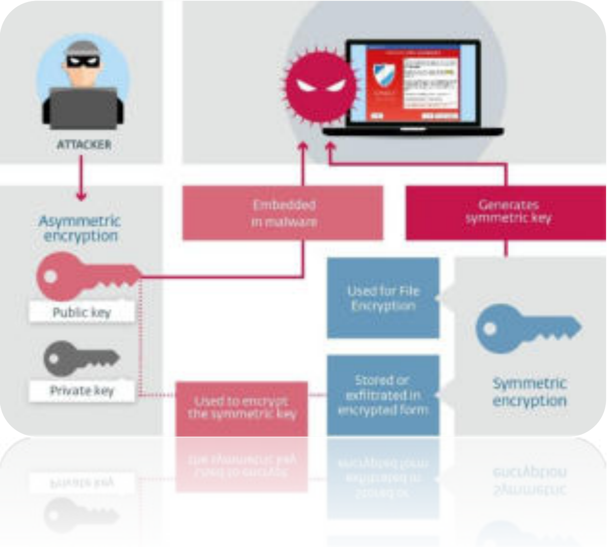
References: RDP brute force attack detected.

Attacker IP: **80.82.77.33**



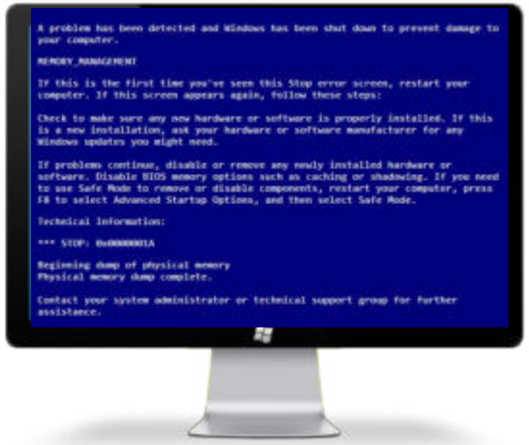
```
inetnum:        80.82.77.0 - 80.82.77.255
netname:        NET-1-77
descr:          IPV NETBLOCK
country:        NL
geoloc:         52.370216 4.895168
org:            ORG-IVI1-RIPE
admin-c:        IVI24-RIPE
tech-c:         IVI24-RIPE
status:         ASSIGNED PA
```

Next generation Seqrite Endpoint Security (EPS)



SMB/EternalBlue.UN!SP.31780

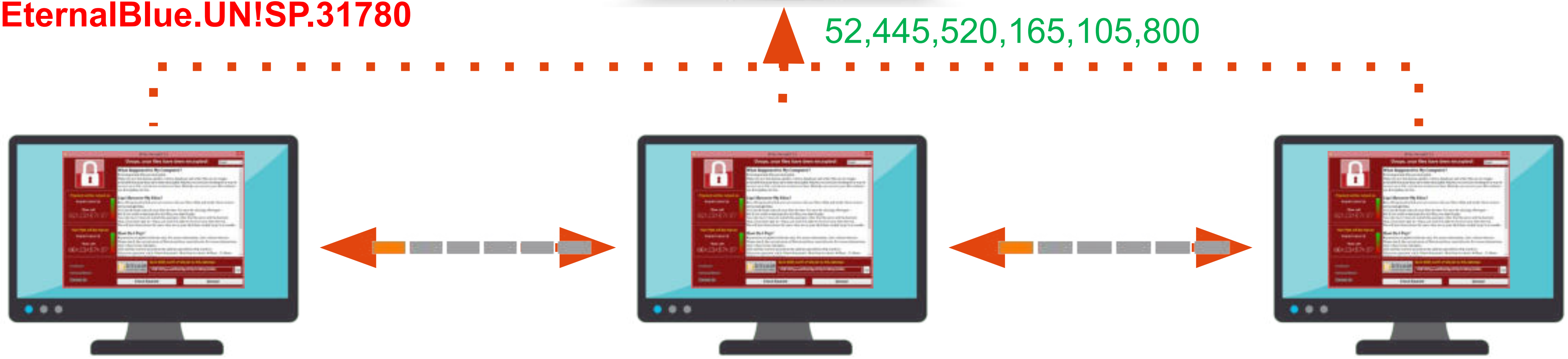
Server



```
A problem has been detected and Windows has been shut down to prevent damage to
your computer.

MEMORY_MANAGEMENT

If this is the first time you've seen this Stop error screen, restart your
computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this
is a new installation, ask your hardware or software manufacturer for any
Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or
software. Disable BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your computer, press
F8 to select Advanced Startup Options, and then select Safe Mode.

Technical Information:

*** STOP: 0x0000001A

Beginning dump of physical memory
Physical memory dump complete.

Contact your system administrator or technical support group for further
assistance.
```

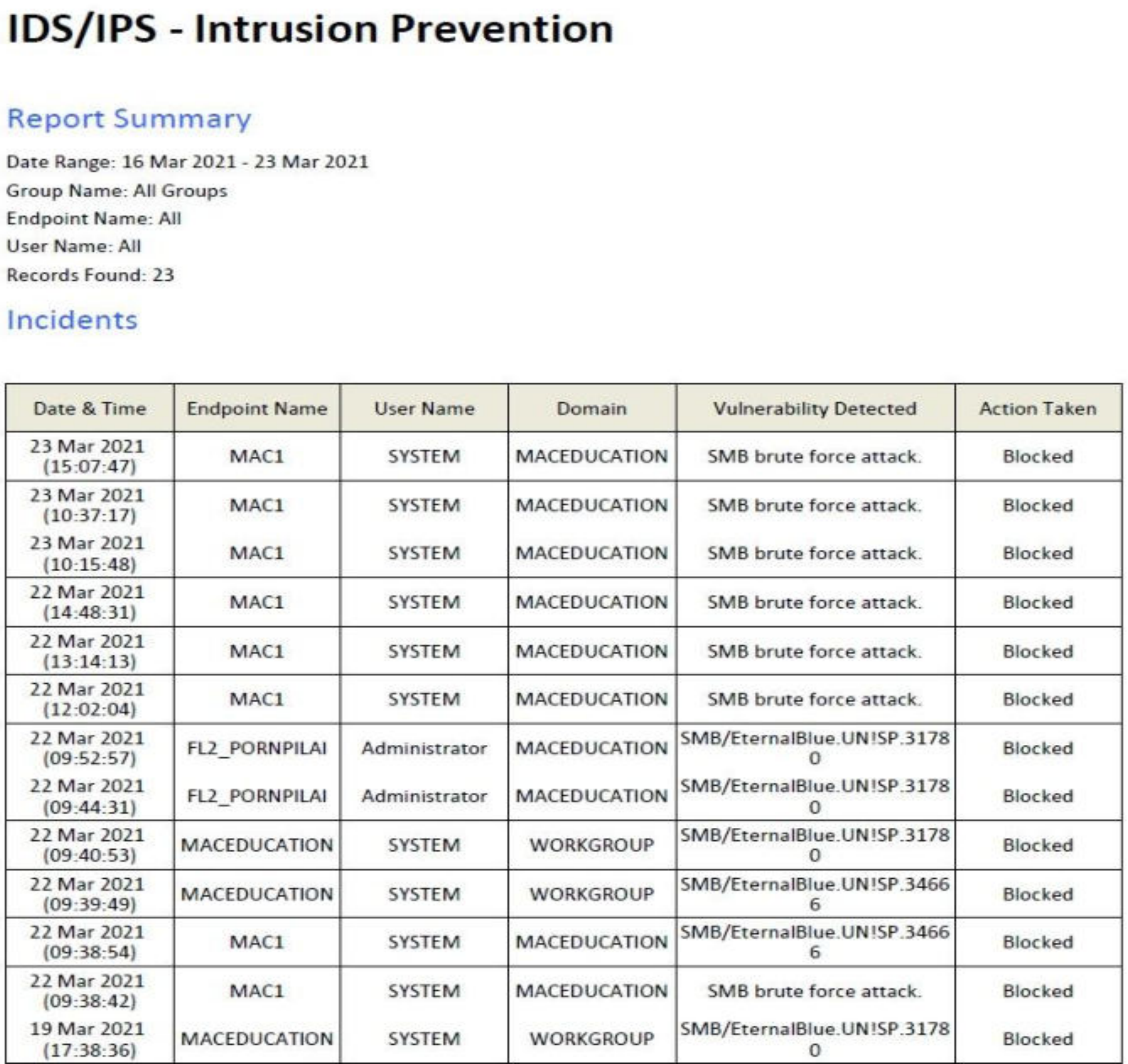
“ EternalBlue ”
is currently being used in a massive ransomware outbreak. The ransomware used in this campaign is ‘WannaCrypt

52,445,520,165,105,800



การทำงานของ ไวรัสเรียกค่าไถ่

Next generation Seqrite Endpoint Security (EPS)



IDS/IPS - Intrusion Prevention

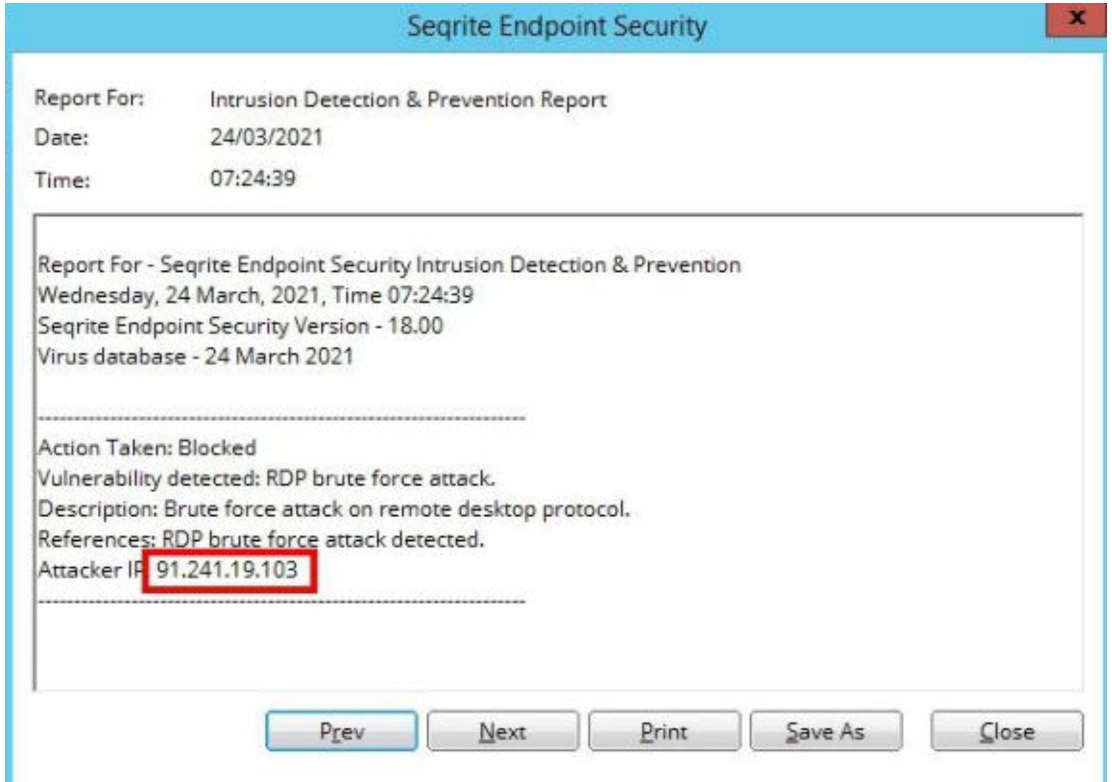
Report Summary

Date Range: 16 Mar 2021 - 23 Mar 2021
Group Name: All Groups
Endpoint Name: All
User Name: All
Records Found: 23

Incidents

Date & Time	Endpoint Name	User Name	Domain	Vulnerability Detected	Action Taken
23 Mar 2021 (15:07:47)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
23 Mar 2021 (10:37:17)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
23 Mar 2021 (10:15:48)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
22 Mar 2021 (14:48:31)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
22 Mar 2021 (13:14:13)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
22 Mar 2021 (12:02:04)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
22 Mar 2021 (09:52:57)	FL2_PORNPILAI	Administrator	MACEDUCATION	SMB/EternalBlue.UN!SP.31780	Blocked
22 Mar 2021 (09:44:31)	FL2_PORNPILAI	Administrator	MACEDUCATION	SMB/EternalBlue.UN!SP.31780	Blocked
22 Mar 2021 (09:40:53)	MACEDUCATION	SYSTEM	WORKGROUP	SMB/EternalBlue.UN!SP.31780	Blocked
22 Mar 2021 (09:39:49)	MACEDUCATION	SYSTEM	WORKGROUP	SMB/EternalBlue.UN!SP.34666	Blocked
22 Mar 2021 (09:38:54)	MAC1	SYSTEM	MACEDUCATION	SMB/EternalBlue.UN!SP.34666	Blocked
22 Mar 2021 (09:38:42)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
19 Mar 2021 (17:38:36)	MACEDUCATION	SYSTEM	WORKGROUP	SMB/EternalBlue.UN!SP.31780	Blocked

“ EternalBlue ”
is currently being used in a massive ransomware outbreak. The ransomware used in this campaign is ‘WannaCrypt



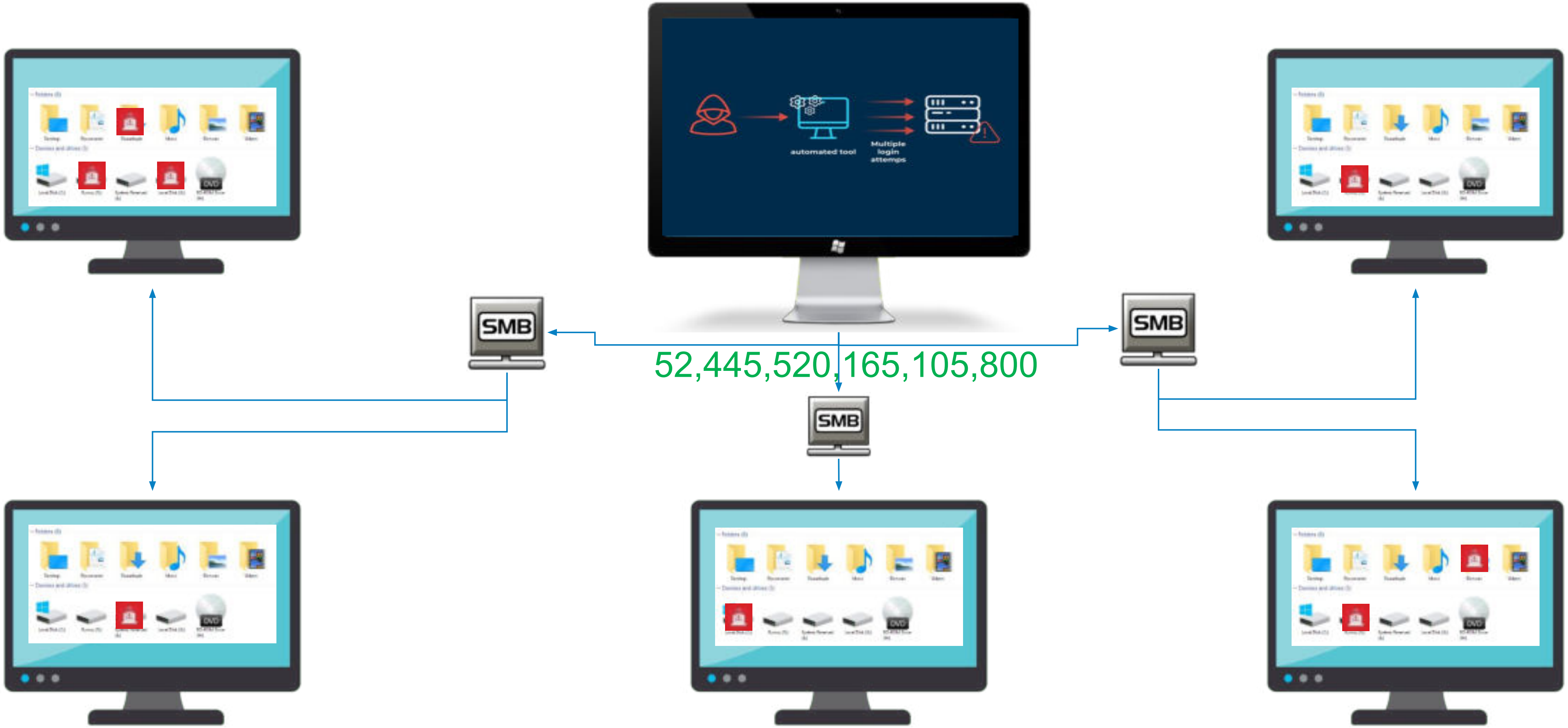
Report For: Intrusion Detection & Prevention Report
Date: 24/03/2021
Time: 07:24:39

Report For - Seqrite Endpoint Security Intrusion Detection & Prevention
Wednesday, 24 March, 2021, Time 07:24:39
Seqrite Endpoint Security Version - 18.00
Virus database - 24 March 2021

Action Taken: Blocked
Vulnerability detected: RDP brute force attack.
Description: Brute force attack on remote desktop protocol.
References: RDP brute force attack detected.
Attacker IP 91.241.19.103

Next generation Seqrite Endpoint Security (EPS)

smb brute force



52,445,520,165,105,800

Next generation Seqrite Endpoint Security (EPS)

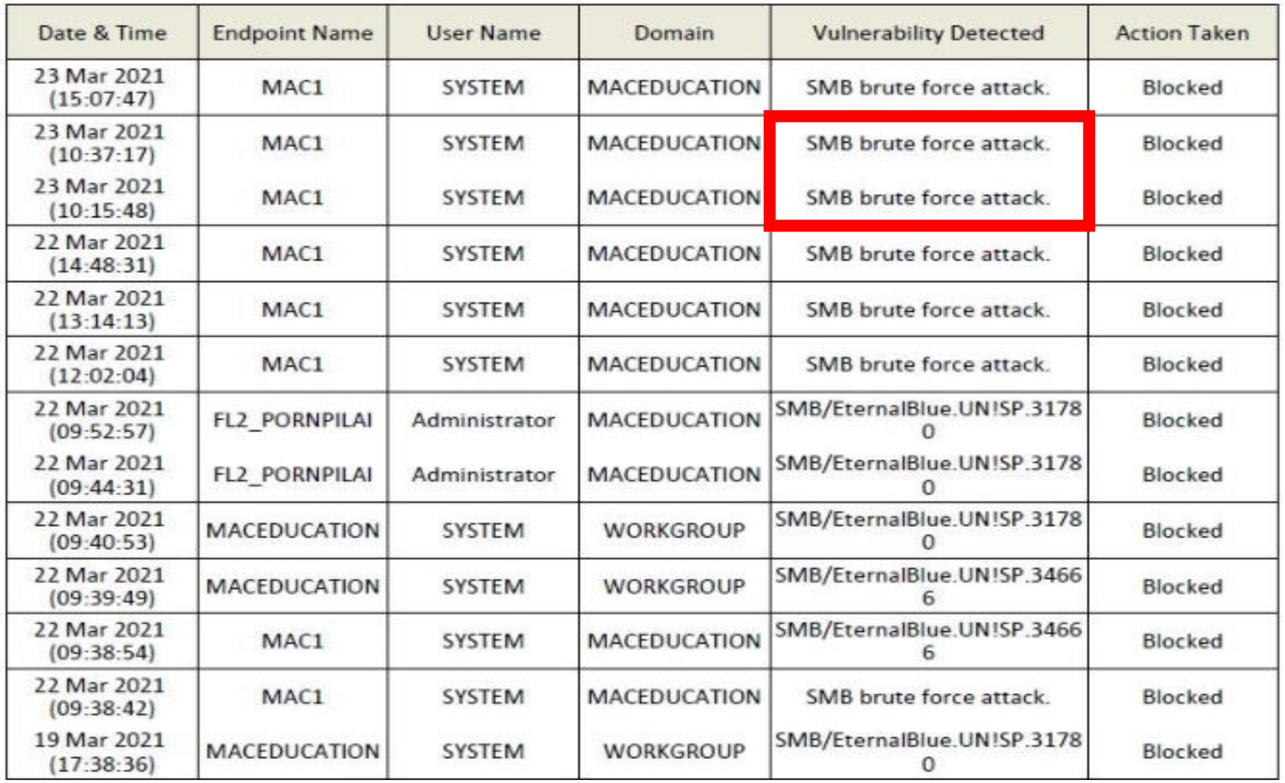
smb brute force

IDS/IPS - Intrusion Prevention

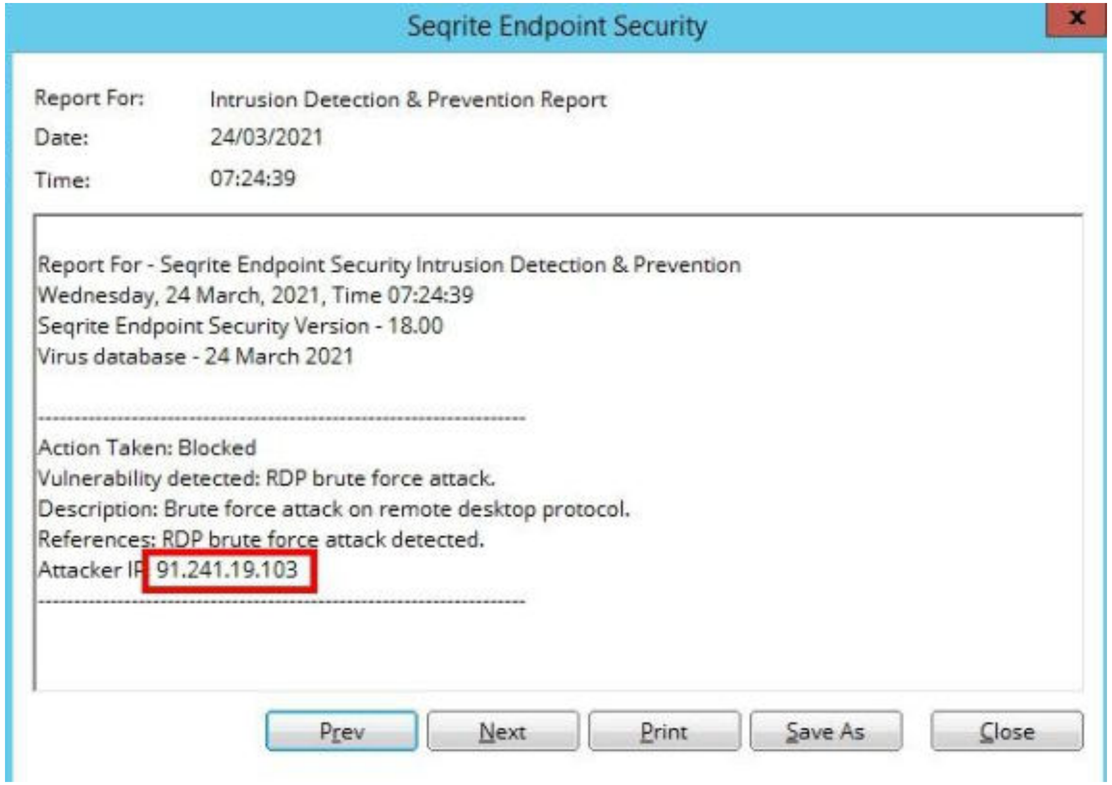
Report Summary

Date Range: 16 Mar 2021 - 23 Mar 2021
Group Name: All Groups
Endpoint Name: All
User Name: All
Records Found: 23

Incidents



Date & Time	Endpoint Name	User Name	Domain	Vulnerability Detected	Action Taken
23 Mar 2021 (15:07:47)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
23 Mar 2021 (10:37:17)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
23 Mar 2021 (10:15:48)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
22 Mar 2021 (14:48:31)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
22 Mar 2021 (13:14:13)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
22 Mar 2021 (12:02:04)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
22 Mar 2021 (09:52:57)	FL2_PORNPILAI	Administrator	MACEDUCATION	SMB/EternalBlue.UN!SP.31780	Blocked
22 Mar 2021 (09:44:31)	FL2_PORNPILAI	Administrator	MACEDUCATION	SMB/EternalBlue.UN!SP.31780	Blocked
22 Mar 2021 (09:40:53)	MACEDUCATION	SYSTEM	WORKGROUP	SMB/EternalBlue.UN!SP.31780	Blocked
22 Mar 2021 (09:39:49)	MACEDUCATION	SYSTEM	WORKGROUP	SMB/EternalBlue.UN!SP.34666	Blocked
22 Mar 2021 (09:38:54)	MAC1	SYSTEM	MACEDUCATION	SMB/EternalBlue.UN!SP.34666	Blocked
22 Mar 2021 (09:38:42)	MAC1	SYSTEM	MACEDUCATION	SMB brute force attack.	Blocked
19 Mar 2021 (17:38:36)	MACEDUCATION	SYSTEM	WORKGROUP	SMB/EternalBlue.UN!SP.31780	Blocked



Seqrite Endpoint Security

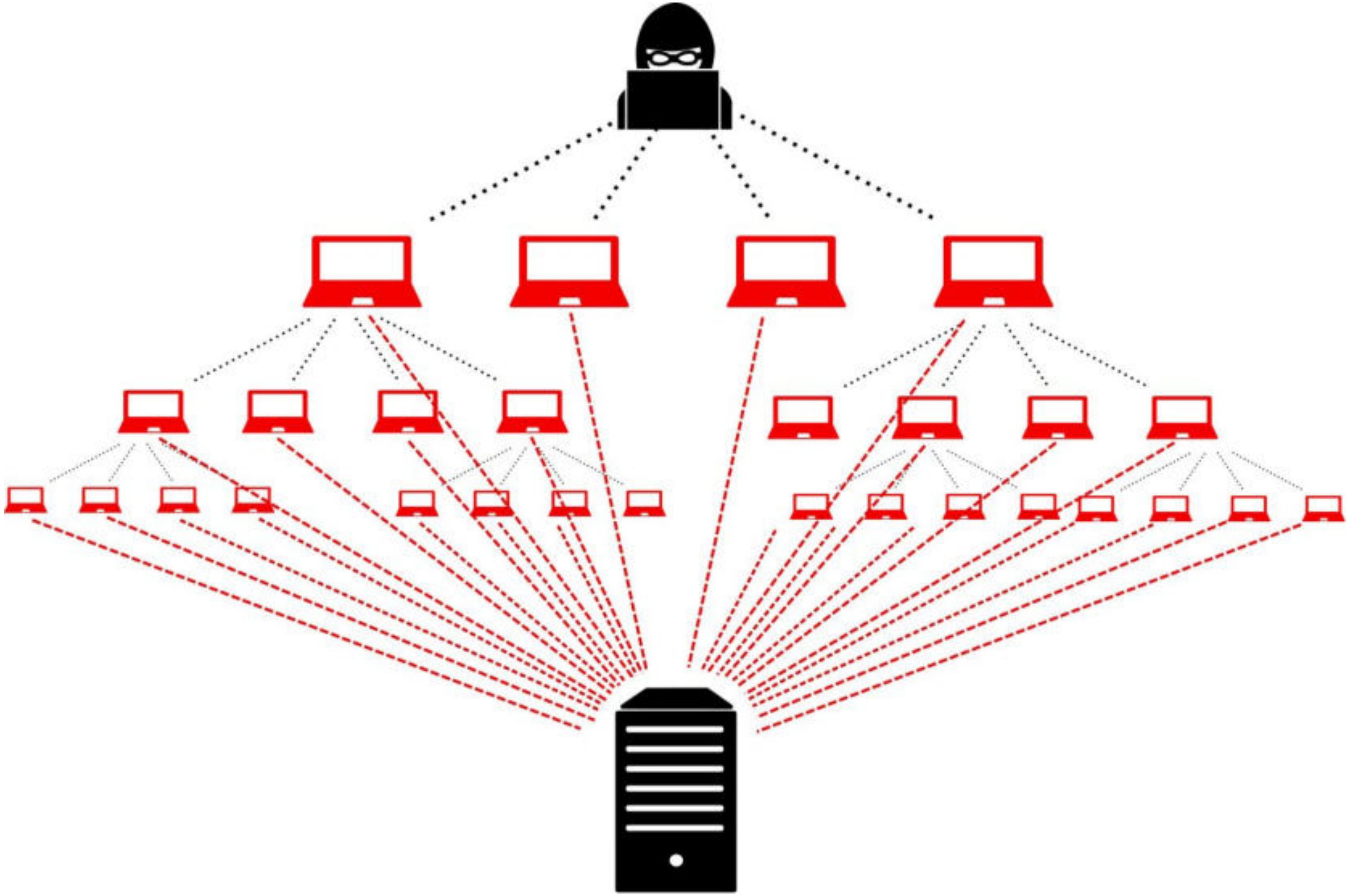
Report For: Intrusion Detection & Prevention Report
Date: 24/03/2021
Time: 07:24:39

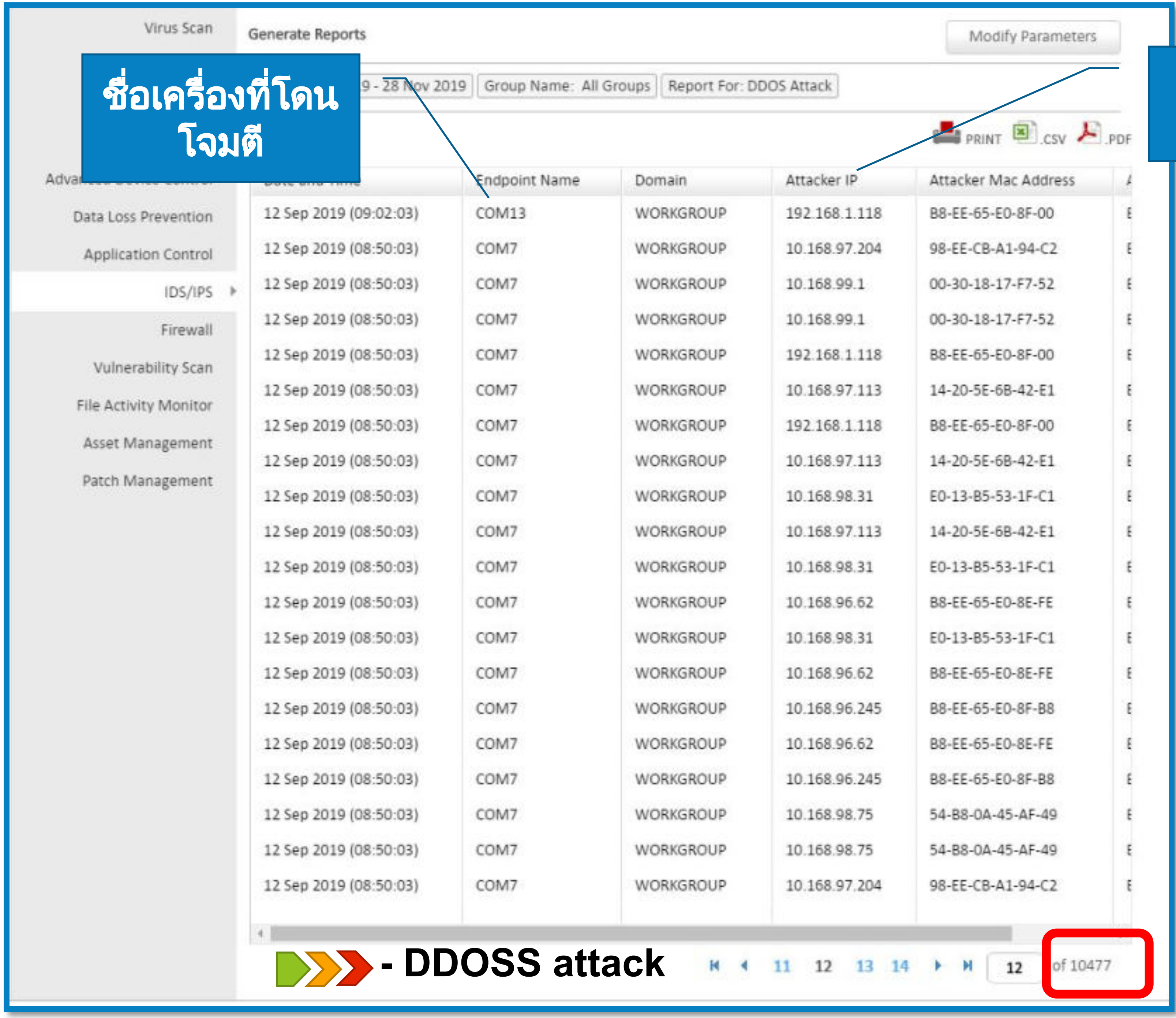
Report For - Seqrite Endpoint Security Intrusion Detection & Prevention
Wednesday, 24 March, 2021, Time 07:24:39
Seqrite Endpoint Security Version - 18.00
Virus database - 24 March 2021

Action Taken: Blocked
Vulnerability detected: RDP brute force attack.
Description: Brute force attack on remote desktop protocol.
References: RDP brute force attack detected.
Attacker IP 91.241.19.103

Next generation Seqrite Endpoint Security (EPS)

- DDOSS attack





Generate Reports

9 - 28 Nov 2019 | Group Name: All Groups | Report For: DDOS Attack

Date and Time	Endpoint Name	Domain	Attacker IP	Attacker Mac Address	A
12 Sep 2019 (09:02:03)	COM13	WORKGROUP	192.168.1.118	B8-EE-65-E0-8F-00	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.97.204	98-EE-CB-A1-94-C2	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.99.1	00-30-18-17-F7-52	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.99.1	00-30-18-17-F7-52	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	192.168.1.118	B8-EE-65-E0-8F-00	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.97.113	14-20-5E-6B-42-E1	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	192.168.1.118	B8-EE-65-E0-8F-00	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.97.113	14-20-5E-6B-42-E1	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.98.31	E0-13-B5-53-1F-C1	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.97.113	14-20-5E-6B-42-E1	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.98.31	E0-13-B5-53-1F-C1	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.96.62	B8-EE-65-E0-8E-FE	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.98.31	E0-13-B5-53-1F-C1	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.96.62	B8-EE-65-E0-8E-FE	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.96.245	B8-EE-65-E0-8F-B8	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.96.62	B8-EE-65-E0-8E-FE	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.96.245	B8-EE-65-E0-8F-B8	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.98.75	54-B8-0A-45-AF-49	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.98.75	54-B8-0A-45-AF-49	E
12 Sep 2019 (08:50:03)	COM7	WORKGROUP	10.168.97.204	98-EE-CB-A1-94-C2	E

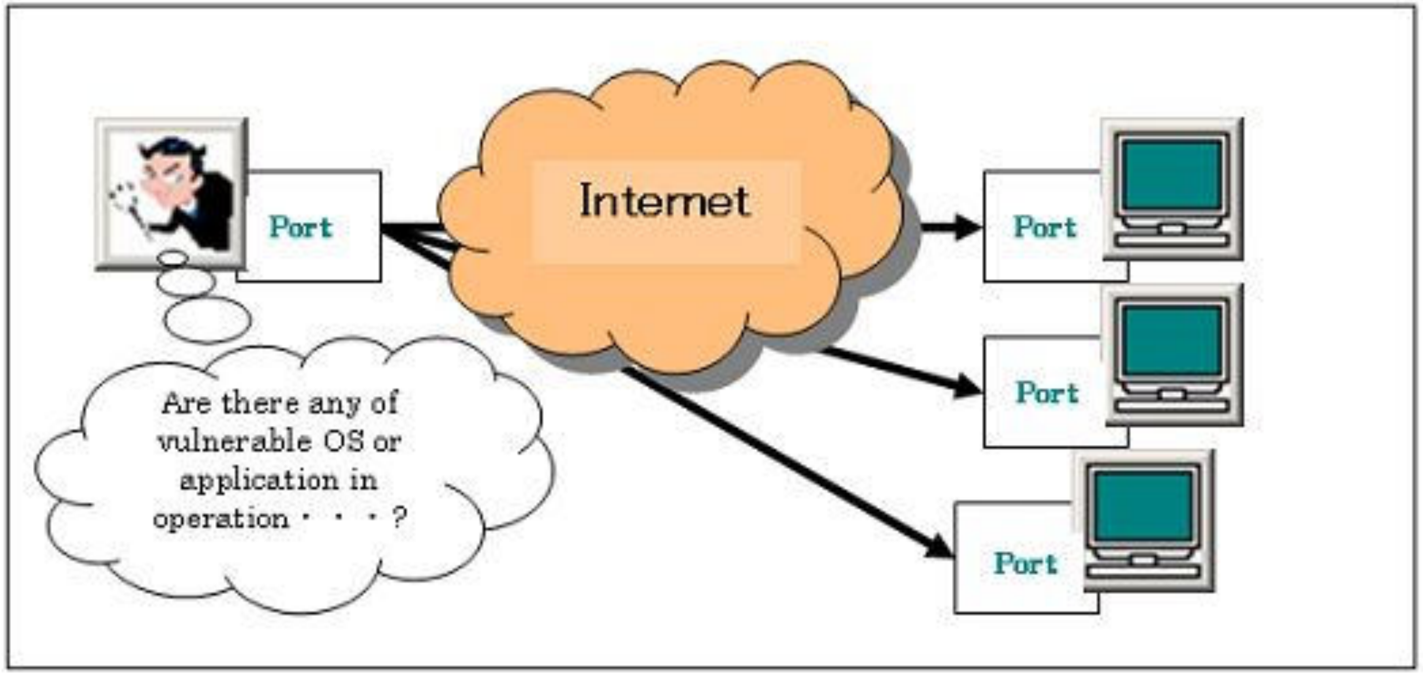
⏮ ◀ 11 12 13 14 ▶ ⏭ 12 of 10477

ชื่อเครื่องที่โดนโจมตี

IP ที่โจมตี DDOSS

- DDOSS attack

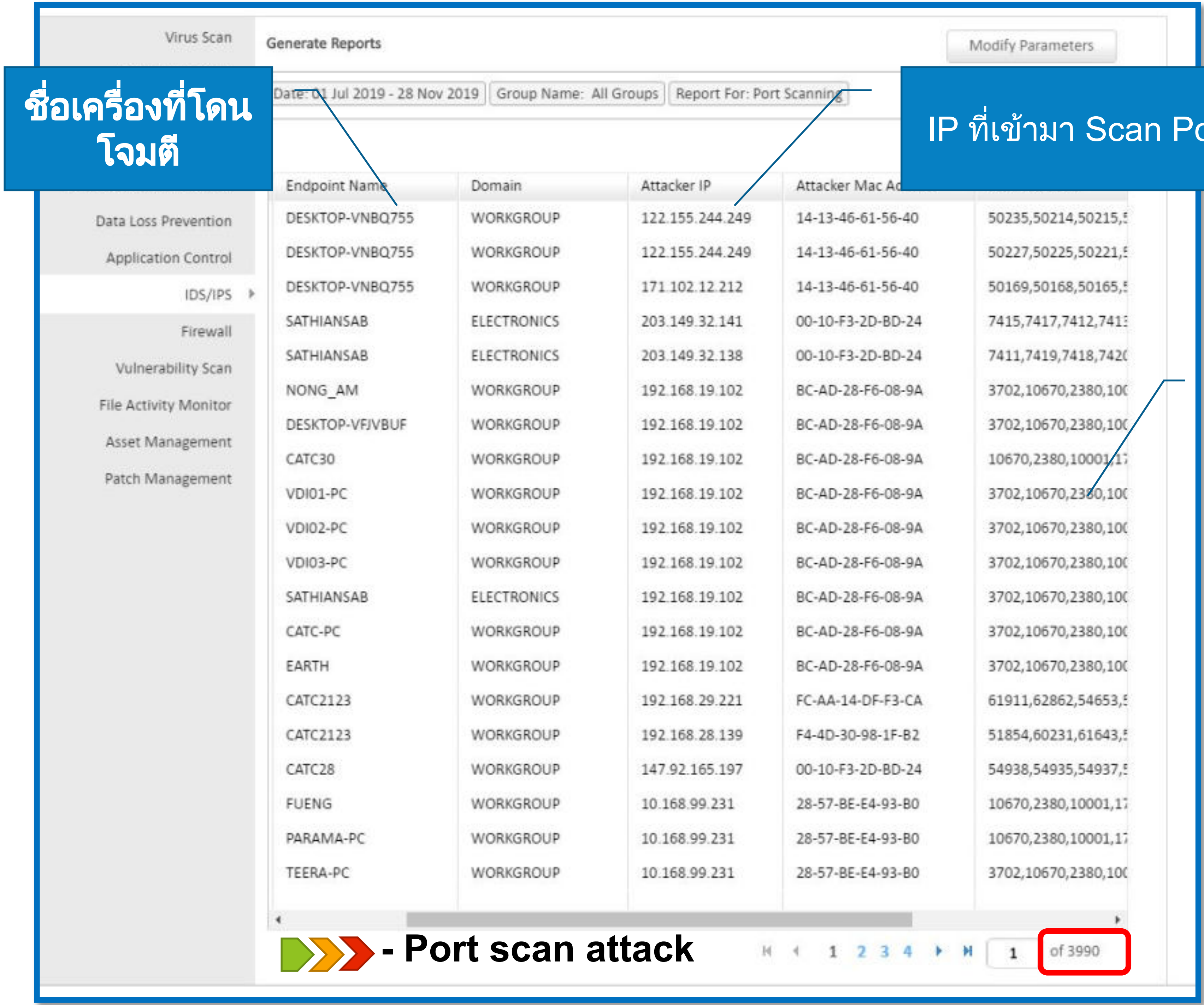
- Port scan attack


Port
Internet
Port
Port
Port
Are there any of vulnerable OS or application in operation · · · ?

ชื่อเครื่องที่โดนโจมตี

IP ที่เข้ามา Scan Port

Port ที่ถูก Scan



Generate Reports

Date: 01 Jul 2019 - 28 Nov 2019 | Group Name: All Groups | Report For: Port Scanning

Endpoint Name	Domain	Attacker IP	Attacker Mac Ad	
DESKTOP-VNBQ755	WORKGROUP	122.155.244.249	14-13-46-61-56-40	50235,50214,50215,5
DESKTOP-VNBQ755	WORKGROUP	122.155.244.249	14-13-46-61-56-40	50227,50225,50221,5
DESKTOP-VNBQ755	WORKGROUP	171.102.12.212	14-13-46-61-56-40	50169,50168,50165,5
SATHIANSAB	ELECTRONICS	203.149.32.141	00-10-F3-2D-BD-24	7415,7417,7412,741
SATHIANSAB	ELECTRONICS	203.149.32.138	00-10-F3-2D-BD-24	7411,7419,7418,742
NONG_AM	WORKGROUP	192.168.19.102	BC-AD-28-F6-08-9A	3702,10670,2380,10
DESKTOP-VFJVBUF	WORKGROUP	192.168.19.102	BC-AD-28-F6-08-9A	3702,10670,2380,10
CATC30	WORKGROUP	192.168.19.102	BC-AD-28-F6-08-9A	10670,2380,10001,17
VDI01-PC	WORKGROUP	192.168.19.102	BC-AD-28-F6-08-9A	3702,10670,2380,10
VDI02-PC	WORKGROUP	192.168.19.102	BC-AD-28-F6-08-9A	3702,10670,2380,10
VDI03-PC	WORKGROUP	192.168.19.102	BC-AD-28-F6-08-9A	3702,10670,2380,10
SATHIANSAB	ELECTRONICS	192.168.19.102	BC-AD-28-F6-08-9A	3702,10670,2380,10
CATC-PC	WORKGROUP	192.168.19.102	BC-AD-28-F6-08-9A	3702,10670,2380,10
EARTH	WORKGROUP	192.168.19.102	BC-AD-28-F6-08-9A	3702,10670,2380,10
CATC2123	WORKGROUP	192.168.29.221	FC-AA-14-DF-F3-CA	61911,62862,54653,5
CATC2123	WORKGROUP	192.168.28.139	F4-4D-30-98-1F-B2	51854,60231,61643,5
CATC28	WORKGROUP	147.92.165.197	00-10-F3-2D-BD-24	54938,54935,54937,5
FUENG	WORKGROUP	10.168.99.231	28-57-BE-E4-93-B0	10670,2380,10001,17
PARAMA-PC	WORKGROUP	10.168.99.231	28-57-BE-E4-93-B0	10670,2380,10001,17
TEERA-PC	WORKGROUP	10.168.99.231	28-57-BE-E4-93-B0	3702,10670,2380,10

1 of 3990

- Port scan attack

Next generation Seqrite Endpoint Security (EPS)

Report For - Seqrite Endpoint Security Intrusion Detection & Prevention

Friday, 11 October, 2019, Time 09:59:10

Seqrite Endpoint Security Version - 18.00

Virus database - 09 October 2019

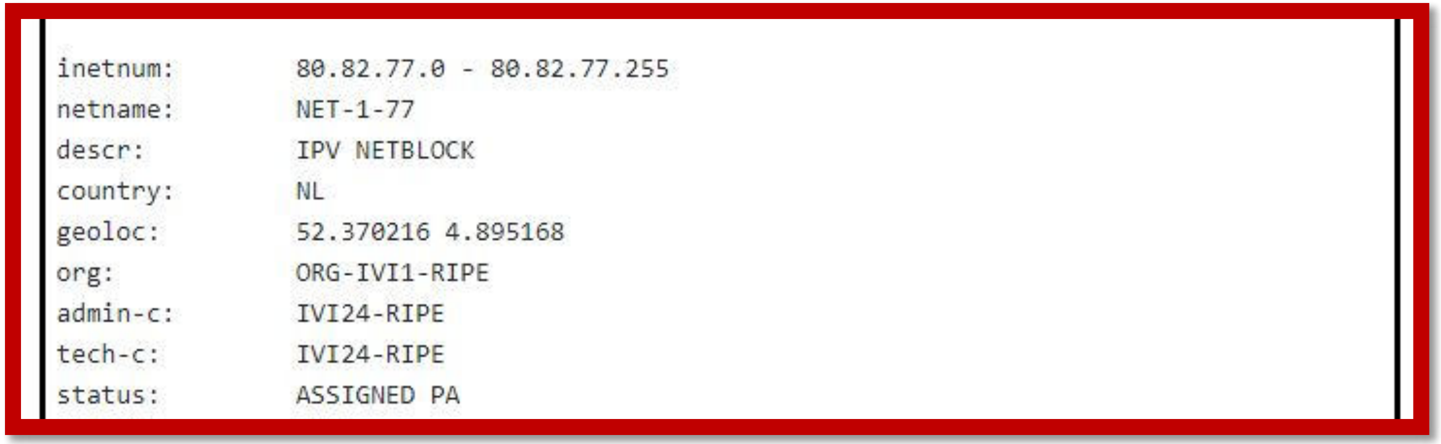
Action Taken: Attacker's IP blocked.

Vulnerability detected: **RDP brute force attack.**

Description: Brute force attack on remote desktop protocol.

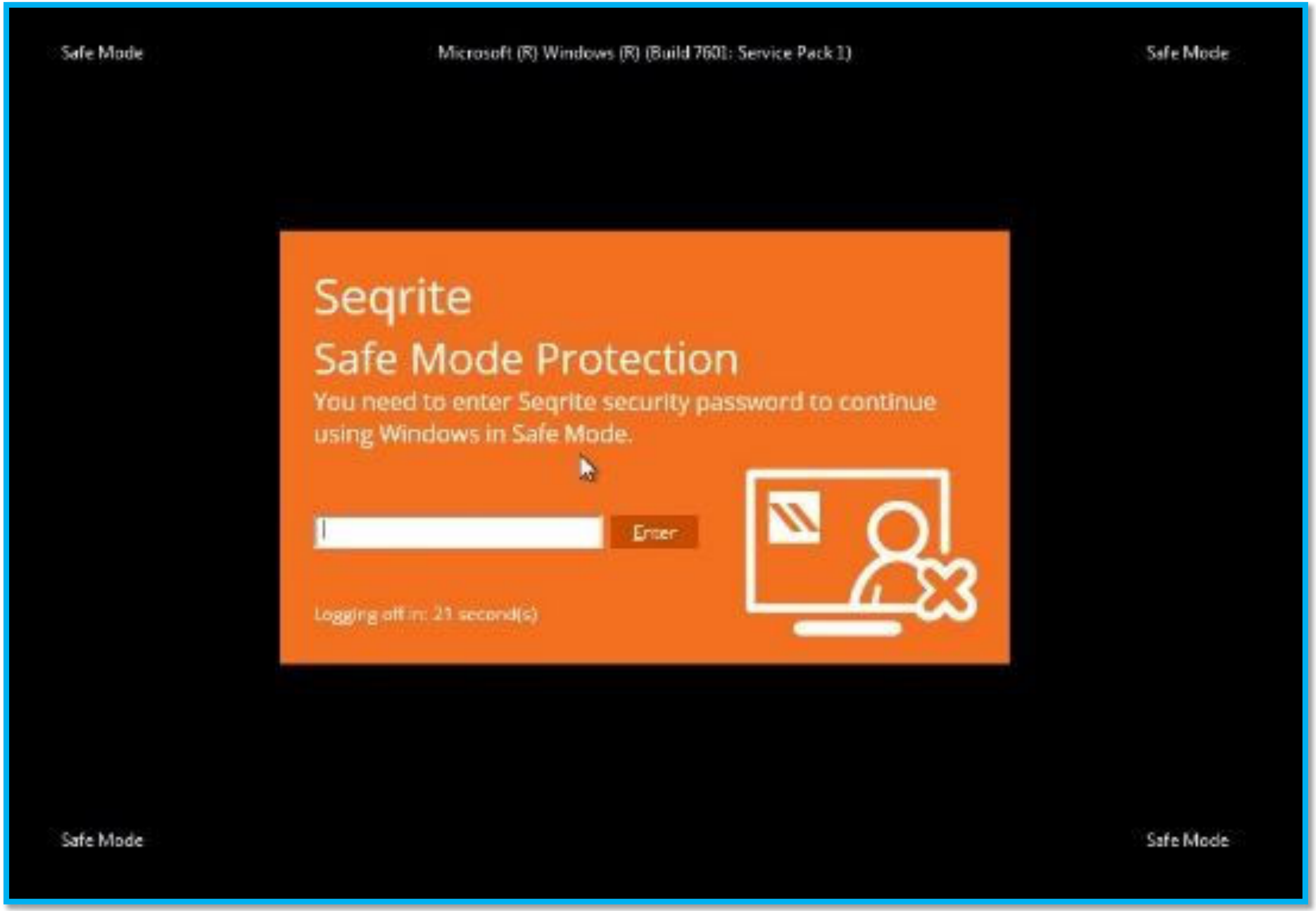
References: RDP brute force attack detected.

Attacker IP: **80.82.77.33**



```
inetnum:        80.82.77.0 - 80.82.77.255
netname:        NET-1-77
descr:          IPV NETBLOCK
country:        NL
geoloc:         52.370216 4.895168
org:            ORG-IVI1-RIPE
admin-c:        IVI24-RIPE
tech-c:         IVI24-RIPE
status:         ASSIGNED PA
```

Next generation Seqrite Endpoint Security (EPS)



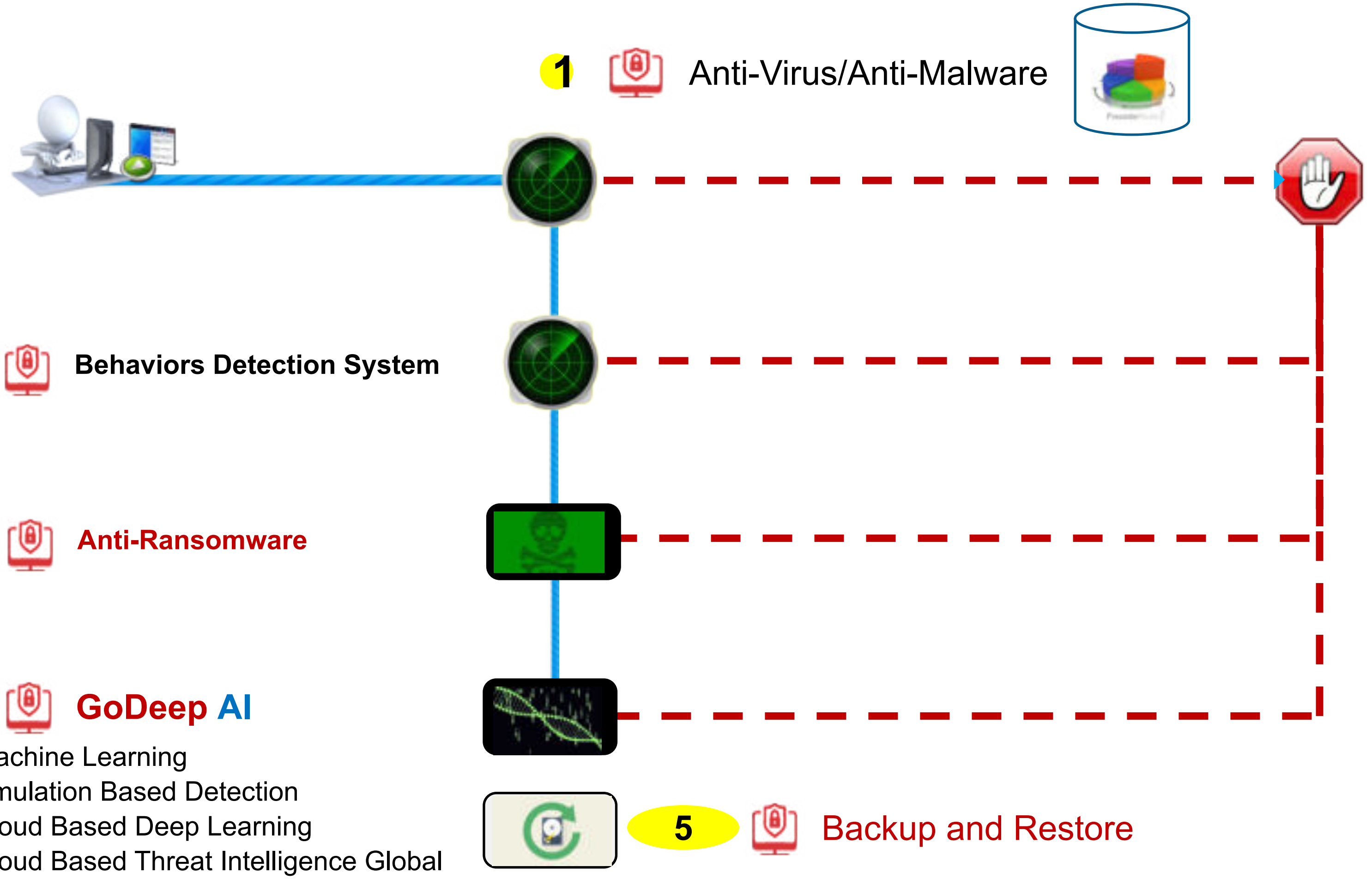
Seqrite

Safe Mode Protection

You need to enter Seqrite security password to continue using Windows in Safe Mode.

Logging off in: 21 second(s)

Next generation Seqrite Endpoint Security (EPS) Core Protection Feature.



1 Anti-Virus/Anti-Malware

2 Behaviors Detection System

3 Anti-Ransomware

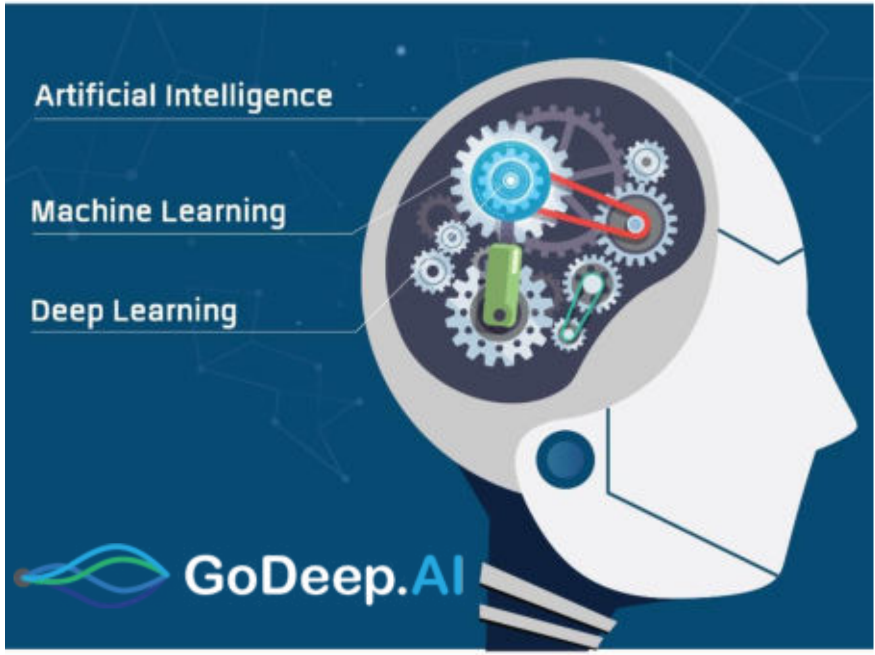
4 GoDeep AI

- Machine Learning
- Emulation Based Detection
- Cloud Based Deep Learning
- Cloud Based Threat Intelligence Global

5 Backup and Restore

Core Protection

Multilayered Protection



Block Suspicious Packed

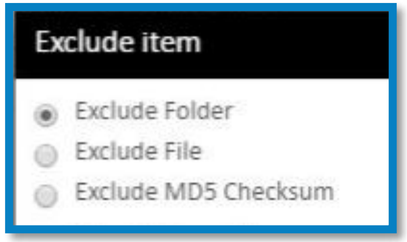
Anti-Rogueware

Anti-Key Locker

Auto run Protection

Automatic Boot Time Scan

Self-Protection



Exclude item

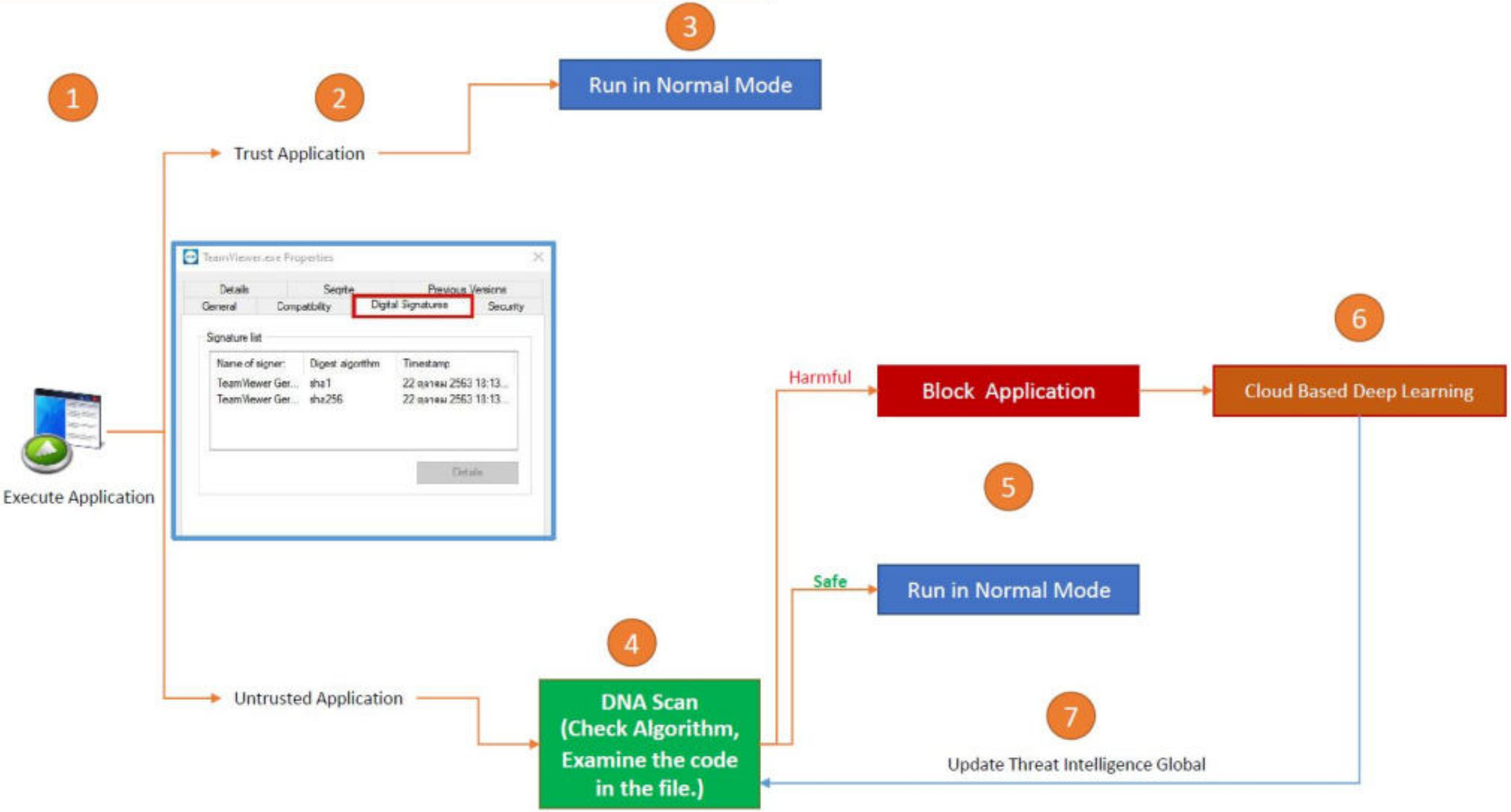
● Exclude Folder

○ Exclude File

○ Exclude MD5 Checksum

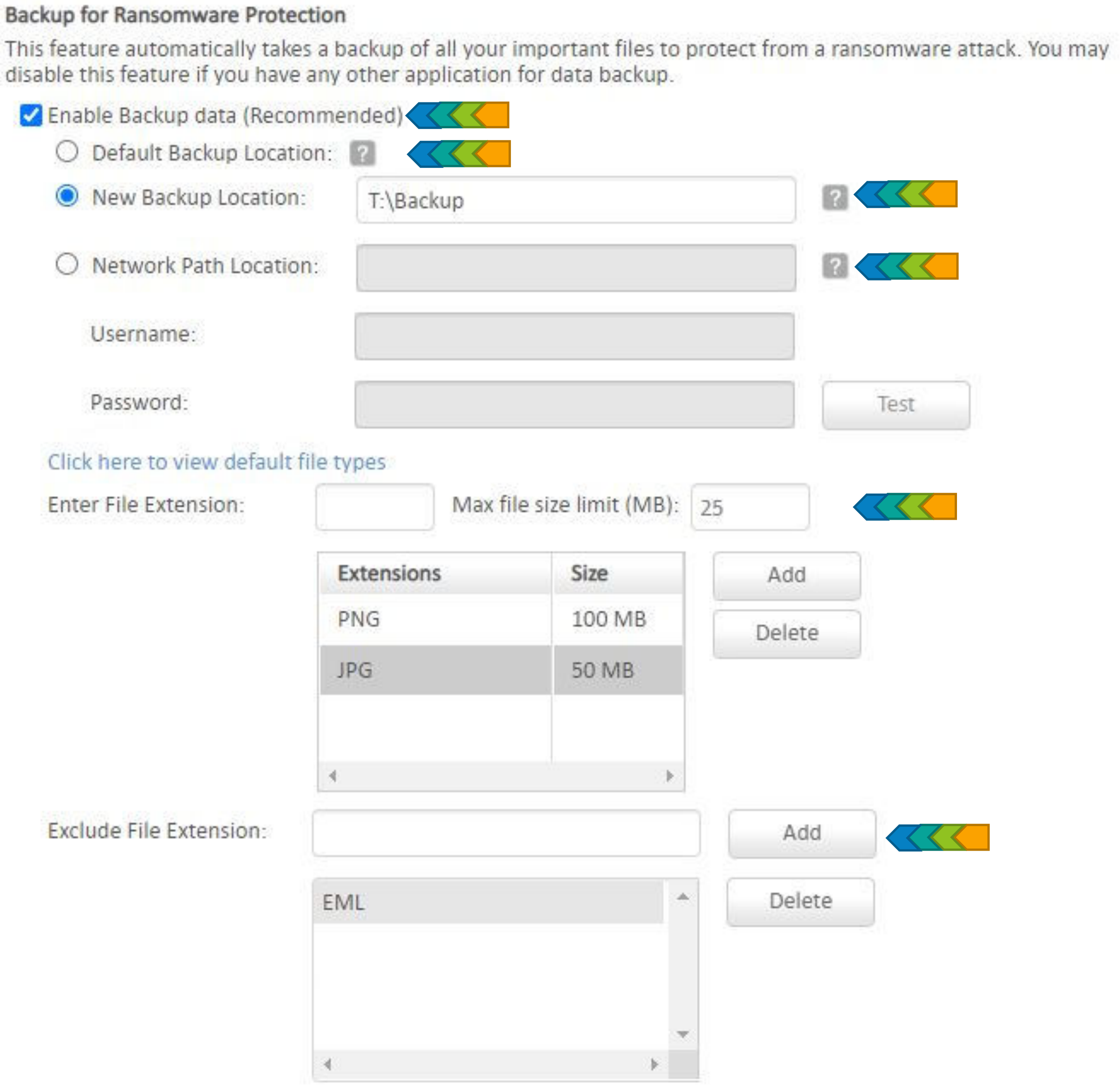
Next generation Seqrite Endpoint Security (EPS) GoDeep.AI Feature.

AI Technology



Name of signer:	Digest algorithm	Timestamp
TeamViewer Ger...	sha1	22 ตุลาคม 2563 18:13...
TeamViewer Ger...	sha256	22 ตุลาคม 2563 18:13...

Next generation Seqrite Endpoint Security (EPS) Backup & Restore Feature.



Backup for Ransomware Protection

This feature automatically takes a backup of all your important files to protect from a ransomware attack. You may disable this feature if you have any other application for data backup.

☑ Enable Backup data (Recommended)

○ Default Backup Location:

● New Backup Location: T:\Backup

○ Network Path Location:

Username:

Password:

Click here to view default file types

Enter File Extension: Max file size limit (MB): 25

Extensions	Size
PNG	100 MB
JPG	50 MB

Exclude File Extension:

EML

เปิด-ปิด Feature Backup

เลือก Path ที่เก็บ ไฟล์ Backup อัตโนมัติ

กำหนด Path ที่เก็บ ไฟล์ Backup

กำหนด Virtual Path ที่เก็บ ไฟล์ Backup

เพิ่ม ประเภทไฟล์ Backup

ยกเว้น ประเภทไฟล์ Backup

Next generation Seqrite Endpoint Security (EPS) Backup & Restore Feature.

Backup & Restore

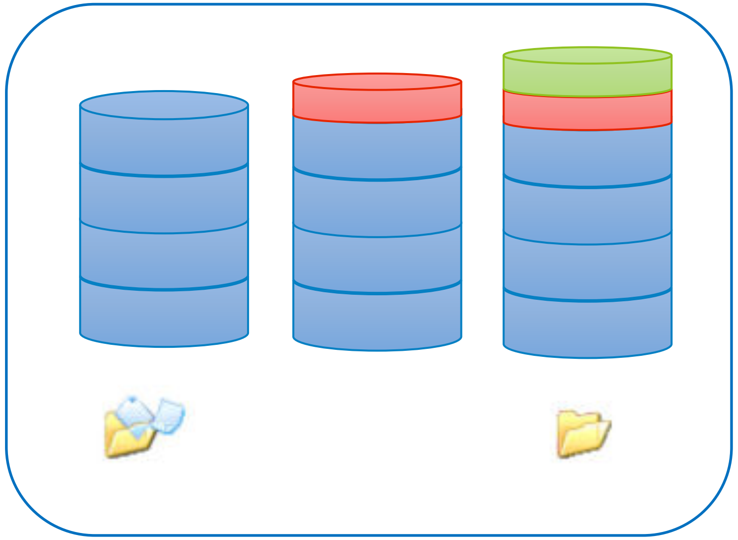
- Backup is taken based on file extensions specified. Currently

Text Files	: txt
Email Files	: eml
Document Files	: doc, docx, xls, xlsx, ppt, pptx, pdf, wps, wpt, rtf, et, docm, xlsm, pptm, ett, dpt, dps, ods, odp, odg, odt
Accounting Files	: tcp, 900, tsf, 001, 247, 500, 989, tsm

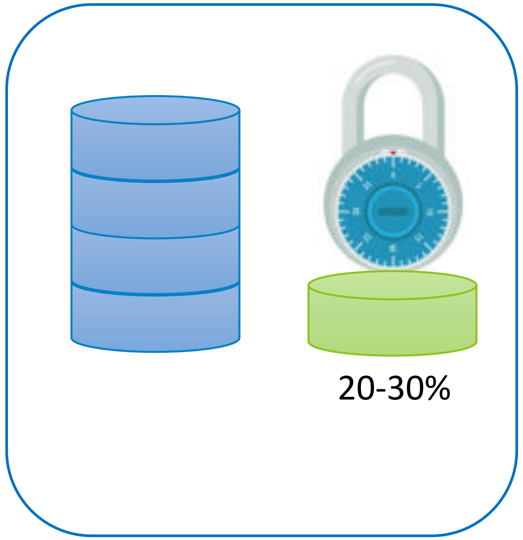
- **Automatic Backup** is initiated silently.(Virus/Malware/Ransomware/Unknown is edit file tools)

- **Schedule Backup** is launched first after 30 minutes of Core Scanning Server service (sapissvc.exe)start. Later, the tool is launched after every 4 hours.

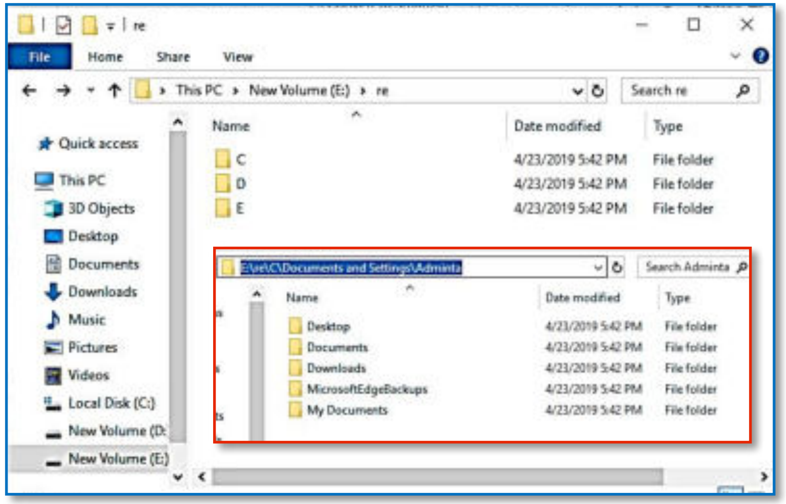
Incremental backup



Compressed /Encrypted/Self-Protection



Restore backup Files



Name	Date modified	Type
C	4/23/2019 5:42 PM	File folder
D	4/23/2019 5:42 PM	File folder
E	4/23/2019 5:42 PM	File folder

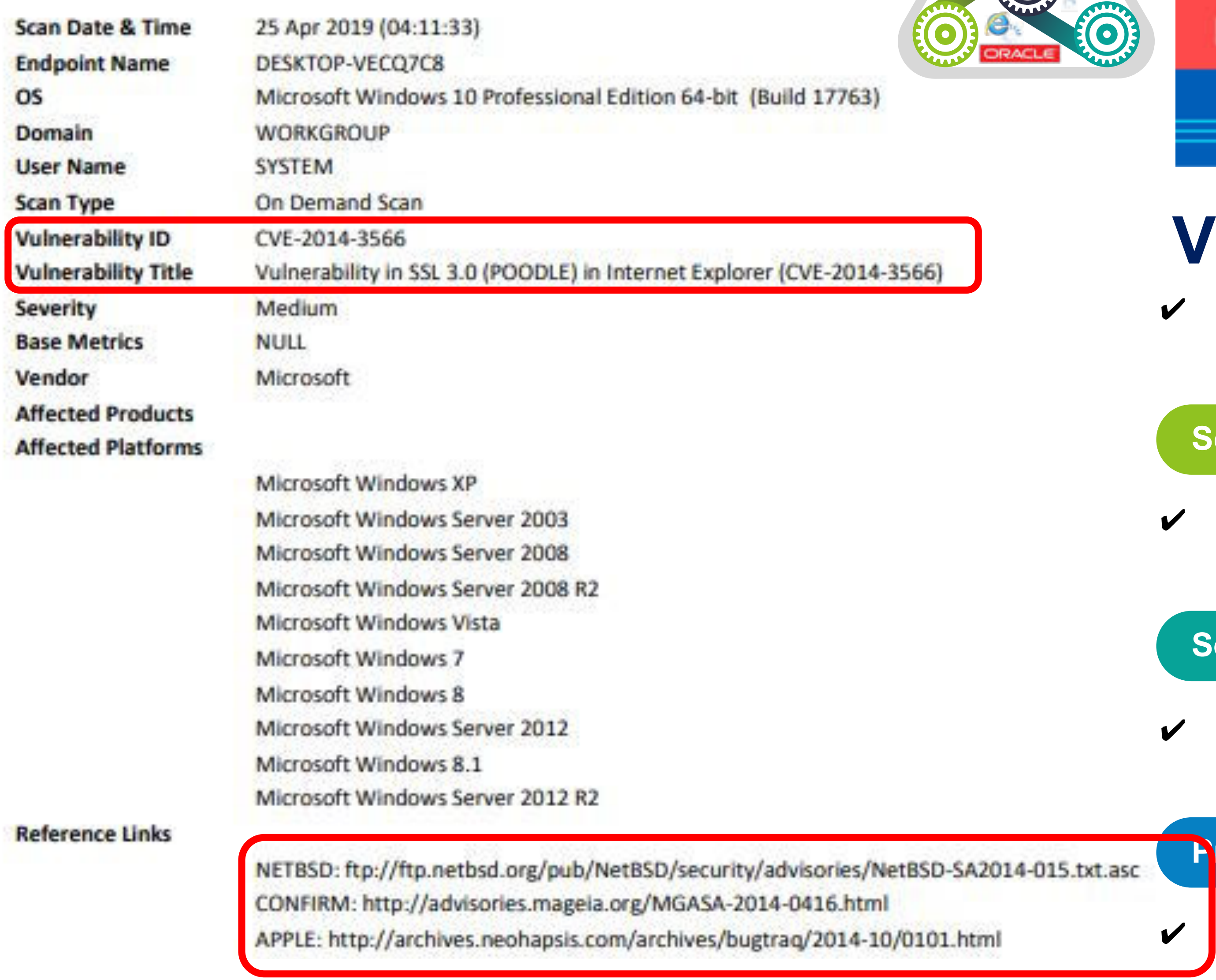
E:\re\C\Documents and Settings\Adminta

Search Adminta

Name	Date modified	Type
Desktop	4/23/2019 5:42 PM	File folder
Documents	4/23/2019 5:42 PM	File folder
Downloads	4/23/2019 5:42 PM	File folder
MicrosoftEdgeBackups	4/23/2019 5:42 PM	File folder
My Documents	4/23/2019 5:42 PM	File folder

Next generation Seqrite Endpoint Security (EPS) Vulnerability Scan Feature.

Vulnerability Scan Detailed Report



Scan Date & Time	25 Apr 2019 (04:11:33)
Endpoint Name	DESKTOP-VECQ7C8
OS	Microsoft Windows 10 Professional Edition 64-bit (Build 17763)
Domain	WORKGROUP
User Name	SYSTEM
Scan Type	On Demand Scan
Vulnerability ID	CVE-2014-3566
Vulnerability Title	Vulnerability in SSL 3.0 (POODLE) in Internet Explorer (CVE-2014-3566)
Severity	Medium
Base Metrics	NULL
Vendor	Microsoft
Affected Products	
Affected Platforms	
	Microsoft Windows XP Microsoft Windows Server 2003 Microsoft Windows Server 2008 Microsoft Windows Server 2008 R2 Microsoft Windows Vista Microsoft Windows 7 Microsoft Windows 8 Microsoft Windows Server 2012 Microsoft Windows 8.1 Microsoft Windows Server 2012 R2
Reference Links	
	NETBSD: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2014-015.txt.asc CONFIRM: http://advisories.mageia.org/MGASA-2014-0416.html APPLE: http://archives.neohapsis.com/archives/bugtraq/2014-10/0101.html

Vulnerability

✔ Scans vulnerabilities in applications such as Adobe, Safari, Mozilla, Oracle, etc.

Schedule Scan

✔ Schedule Scans vulnerabilities in applications such as Adobe, Safari, Mozilla, Oracle, etc.

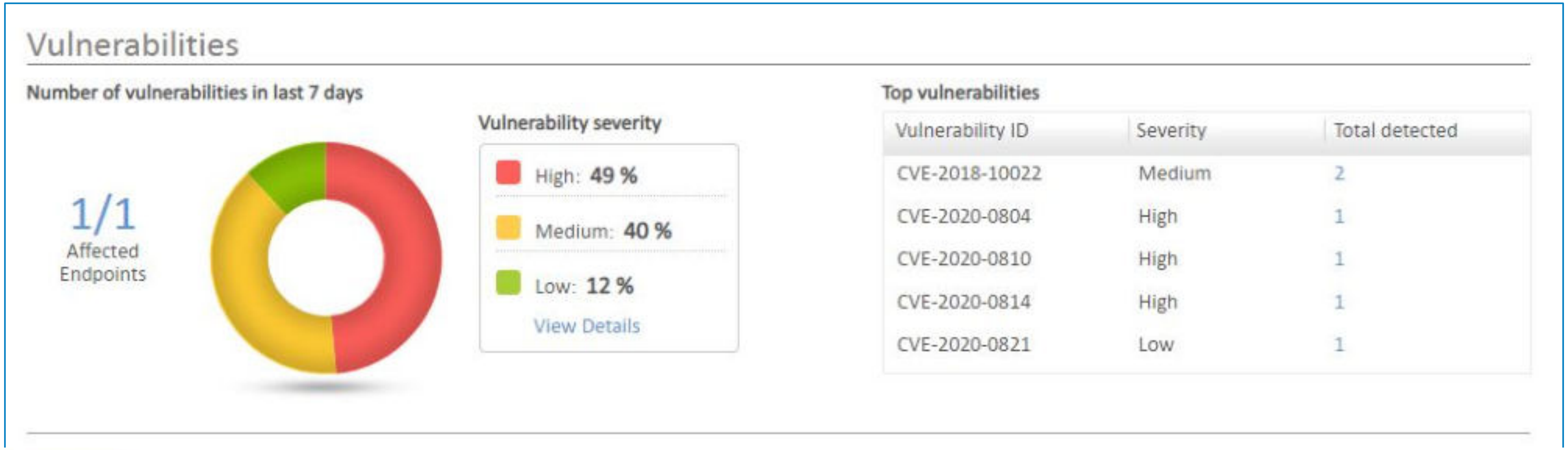
Sends notifications

✔ Sends notifications regarding unpatched operating systems working on computers within the network.

Provides summarized

✔ Provides summarized view of vulnerabilities as per severity.

Next generation Seqrite Endpoint Security (EPS) Vulnerability Scan Feature.



Vulnerabilities

Number of vulnerabilities in last 7 days

1/1
Affected
Endpoints

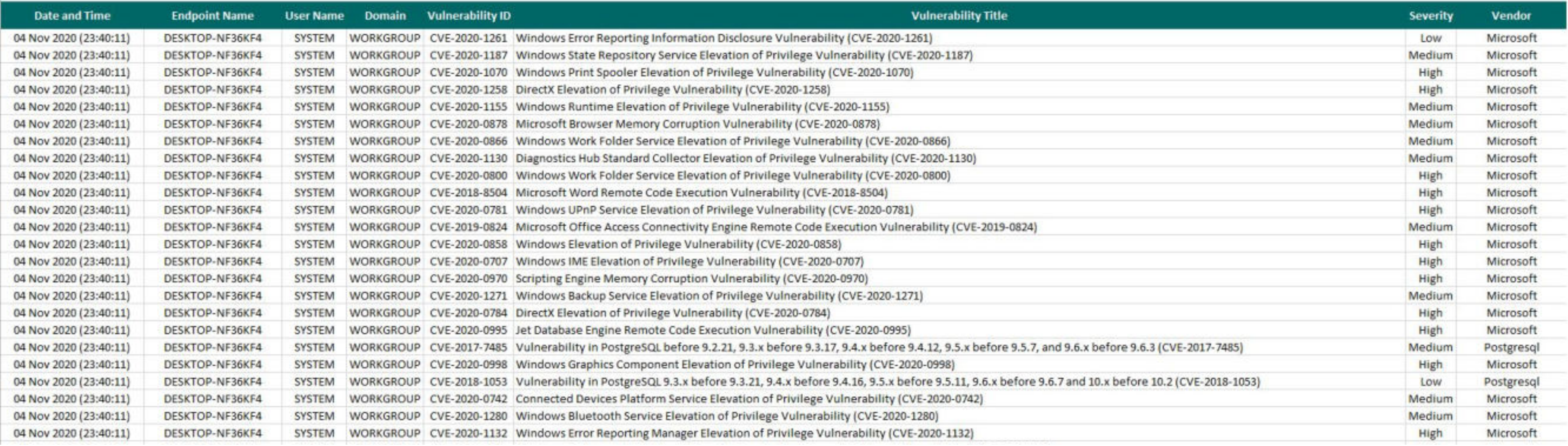
Vulnerability severity

- 🟥 High: **49 %**
- 🟨 Medium: **40 %**
- 🟩 Low: **12 %**

View Details

Top vulnerabilities

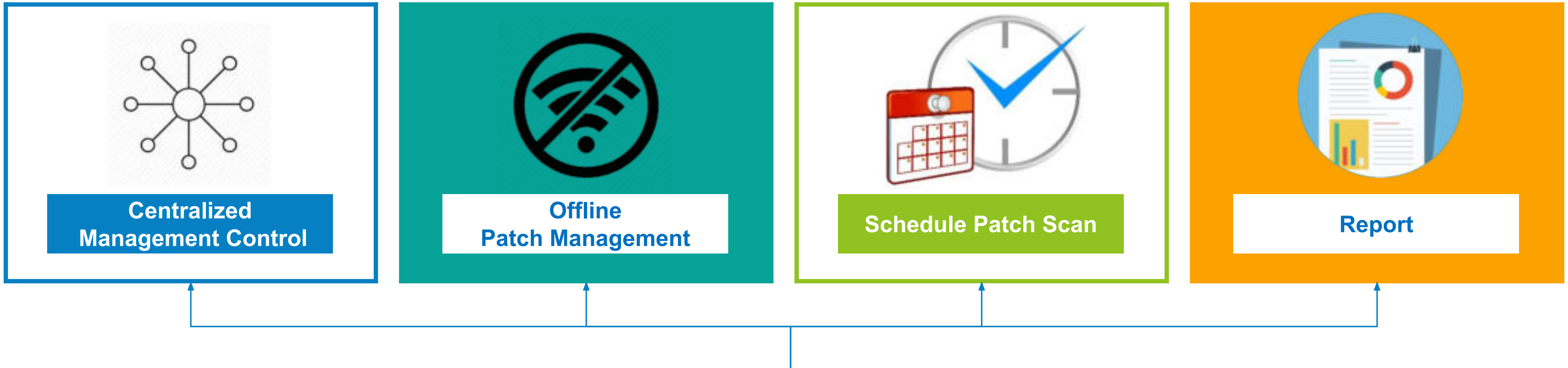
Vulnerability ID	Severity	Total detected
CVE-2018-10022	Medium	2
CVE-2020-0804	High	1
CVE-2020-0810	High	1
CVE-2020-0814	High	1
CVE-2020-0821	Low	1



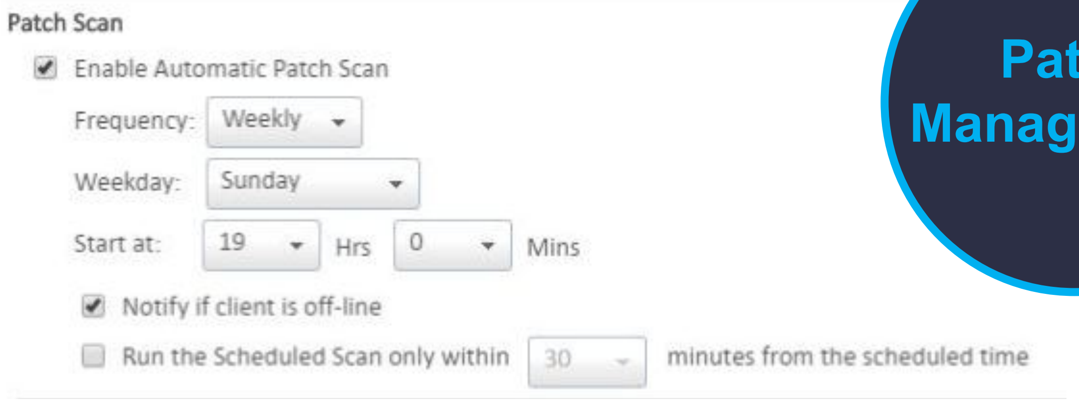
Date and Time	Endpoint Name	User Name	Domain	Vulnerability ID	Vulnerability Title	Severity	Vendor
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1261	Windows Error Reporting Information Disclosure Vulnerability (CVE-2020-1261)	Low	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1187	Windows State Repository Service Elevation of Privilege Vulnerability (CVE-2020-1187)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1070	Windows Print Spooler Elevation of Privilege Vulnerability (CVE-2020-1070)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1258	DirectX Elevation of Privilege Vulnerability (CVE-2020-1258)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1155	Windows Runtime Elevation of Privilege Vulnerability (CVE-2020-1155)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0878	Microsoft Browser Memory Corruption Vulnerability (CVE-2020-0878)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0866	Windows Work Folder Service Elevation of Privilege Vulnerability (CVE-2020-0866)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1130	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability (CVE-2020-1130)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0800	Windows Work Folder Service Elevation of Privilege Vulnerability (CVE-2020-0800)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2018-8504	Microsoft Word Remote Code Execution Vulnerability (CVE-2018-8504)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0781	Windows UPnP Service Elevation of Privilege Vulnerability (CVE-2020-0781)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2019-0824	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability (CVE-2019-0824)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0858	Windows Elevation of Privilege Vulnerability (CVE-2020-0858)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0707	Windows IME Elevation of Privilege Vulnerability (CVE-2020-0707)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0970	Scripting Engine Memory Corruption Vulnerability (CVE-2020-0970)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1271	Windows Backup Service Elevation of Privilege Vulnerability (CVE-2020-1271)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0784	DirectX Elevation of Privilege Vulnerability (CVE-2020-0784)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0995	Jet Database Engine Remote Code Execution Vulnerability (CVE-2020-0995)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2017-7485	Vulnerability in PostgreSQL before 9.2.21, 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3 (CVE-2017-7485)	Medium	Postgresql
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0998	Windows Graphics Component Elevation of Privilege Vulnerability (CVE-2020-0998)	High	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2018-1053	Vulnerability in PostgreSQL 9.3.x before 9.3.21, 9.4.x before 9.4.16, 9.5.x before 9.5.11, 9.6.x before 9.6.7 and 10.x before 10.2 (CVE-2018-1053)	Low	Postgresql
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-0742	Connected Devices Platform Service Elevation of Privilege Vulnerability (CVE-2020-0742)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1280	Windows Bluetooth Service Elevation of Privilege Vulnerability (CVE-2020-1280)	Medium	Microsoft
04 Nov 2020 (23:40:11)	DESKTOP-NF36KF4	SYSTEM	WORKGROUP	CVE-2020-1132	Windows Error Reporting Manager Elevation of Privilege Vulnerability (CVE-2020-1132)	High	Microsoft

Next generation Seqrite Endpoint Security (EPS) Patch Management Feature.

Centralized patch management solution to patch vulnerabilities of Microsoft and Non-Microsoft application.



Patch Management



Patch Scan

☑ Enable Automatic Patch Scan

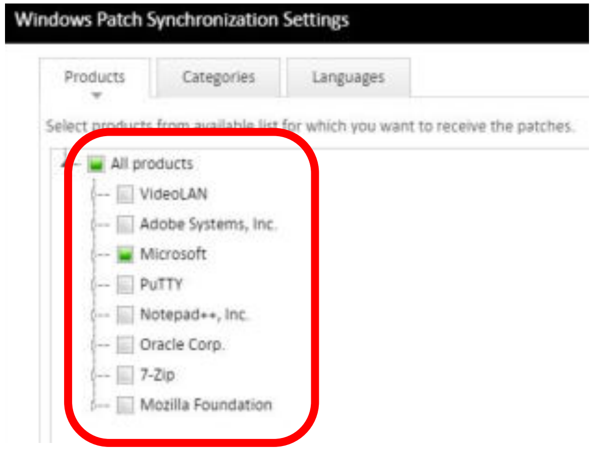
Frequency: Weekly

Weekday: Sunday

Start at: 19 Hrs 0 Mins

☑ Notify if client is off-line

□ Run the Scheduled Scan only within 30 minutes from the scheduled time

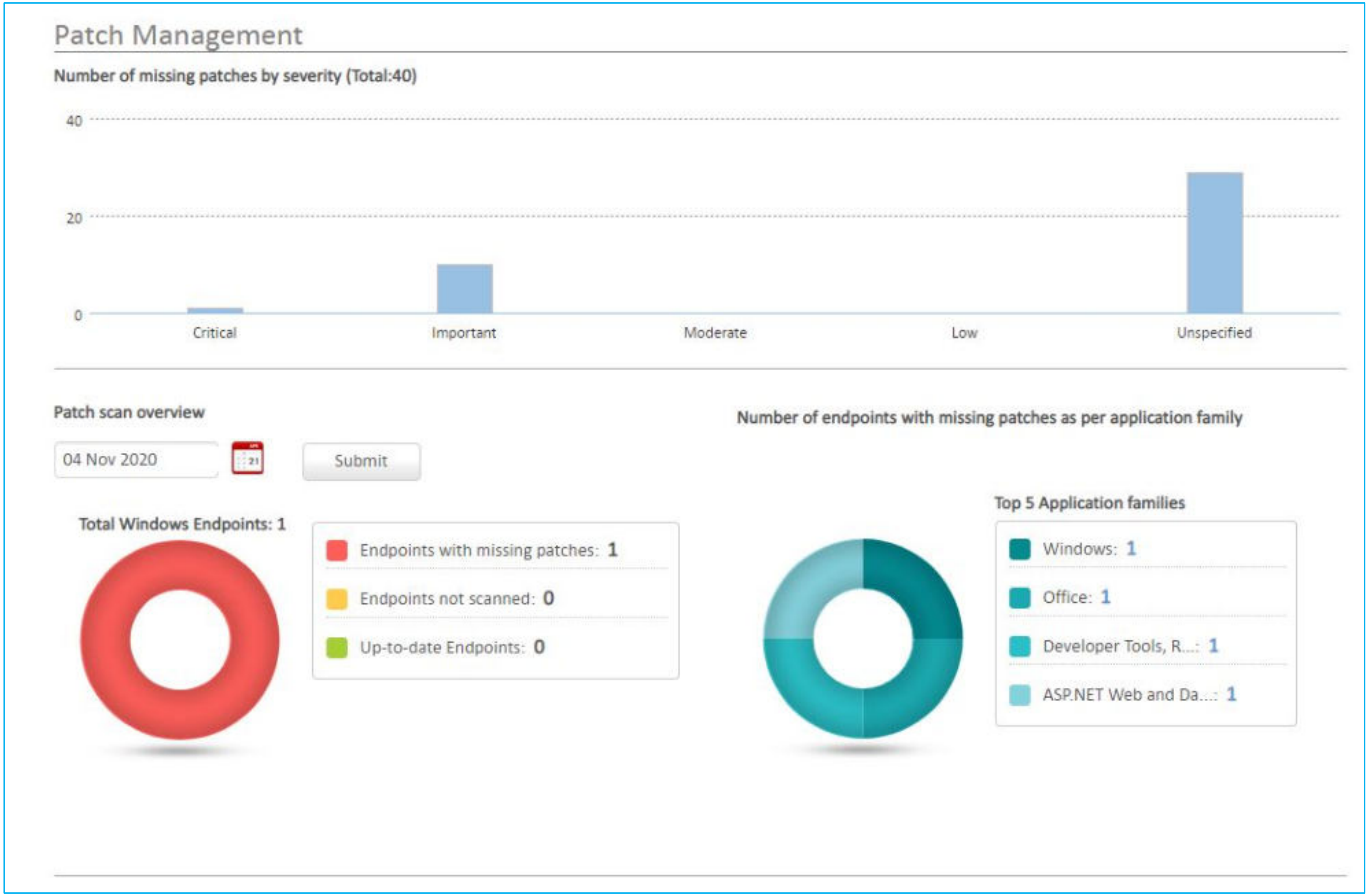


Windows Patch Synchronization Settings

Select products from available list for which you want to receive the patches.

- 🟩 All products
  - □ VideoLAN
  - □ Adobe Systems, Inc.
  - 🟩 Microsoft
  - □ PuTTY
  - □ Notepad++, Inc.
  - □ Oracle Corp.
  - □ 7-Zip
  - □ Mozilla Foundation

Next generation Seqrite Endpoint Security (EPS) Patch Management Feature.



Patch Management

Number of missing patches by severity (Total:40)

Patch scan overview

04 Nov 2020

Total Windows Endpoints: 1

🟥 Endpoints with missing patches: 1

🟨 Endpoints not scanned: 0

🟩 Up-to-date Endpoints: 0

Number of endpoints with missing patches as per application family

Top 5 Application families

■ Windows: 1

■ Office: 1

■ Developer Tools, R...: 1

■ ASP.NET Web and Da...: 1

Next generation Seqrite Endpoint Security (EPS) Asset Management Feature.

System Information

- Operating System
- Application Name
- System Manufacturer
- Memory
- Processor
- Last Shutdown time

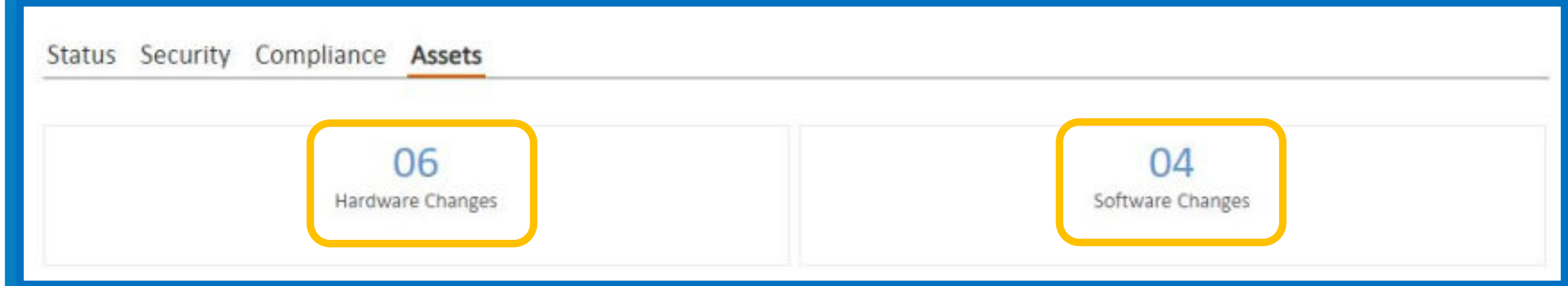
Asset Tracking

- Track Hardware changes
- Track Software changes

Customized Reports

PRINT .CSV .PDF

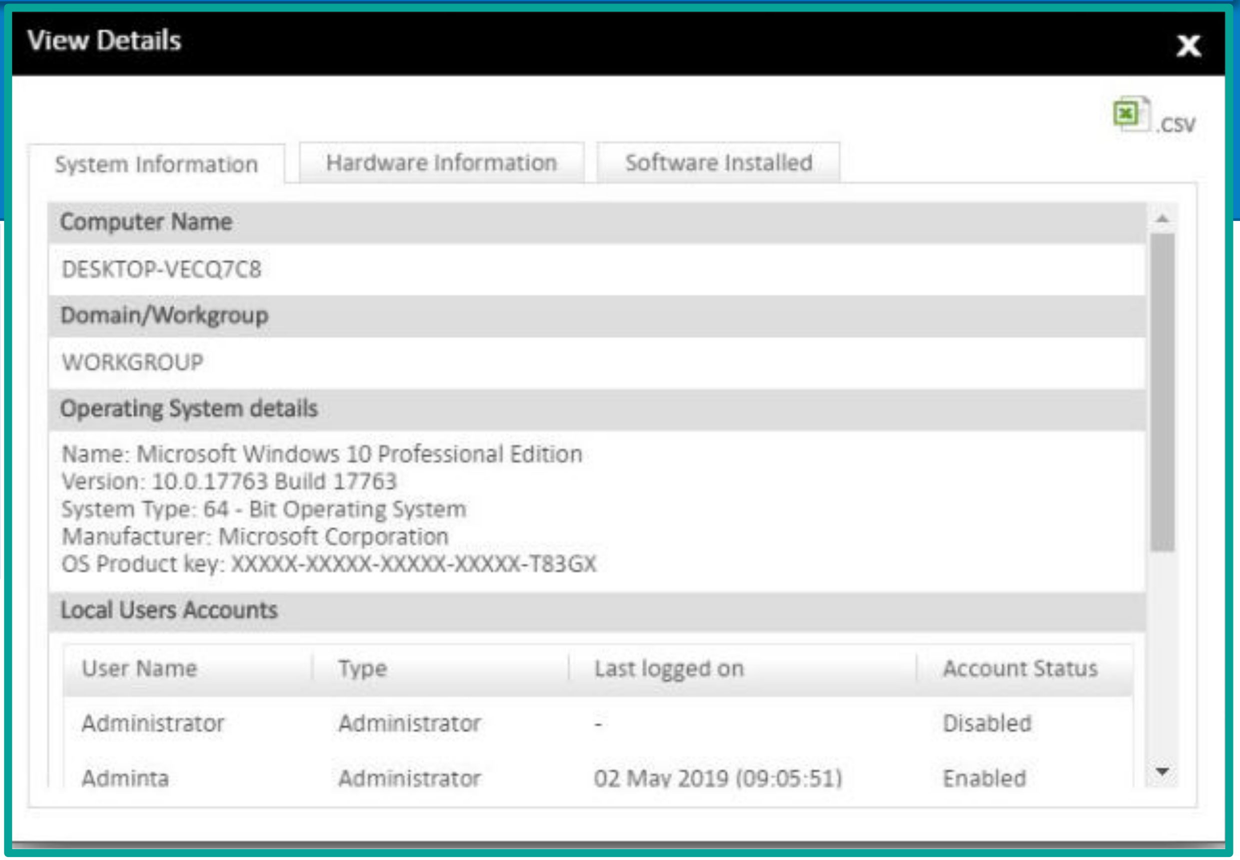
Asset Management



06 Hardware Changes

04 Software Changes

Office



Computer Name

DESKTOP-VECQ7C8

Domain/Workgroup

WORKGROUP

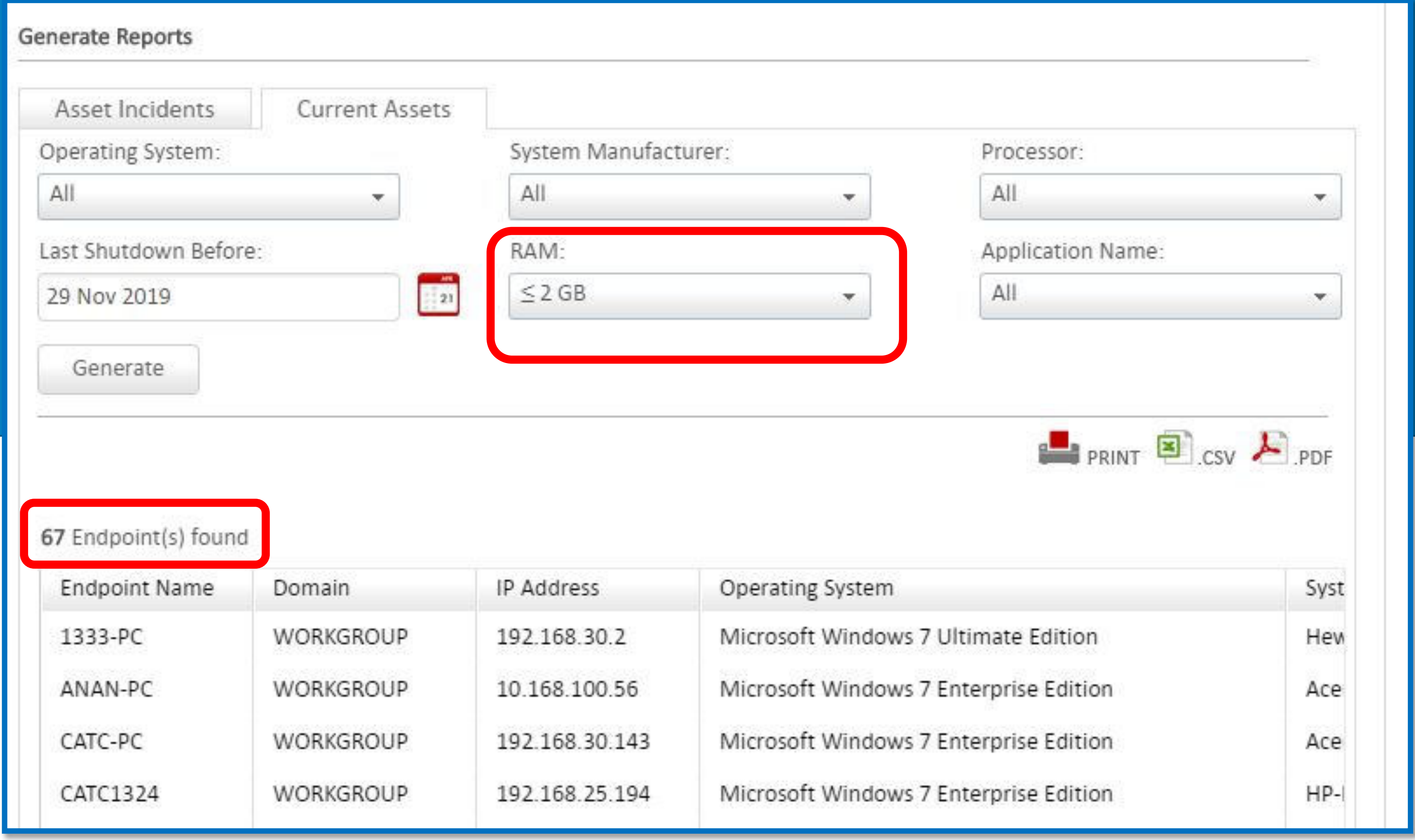
Operating System details

Name: Microsoft Windows 10 Professional Edition
Version: 10.0.17763 Build 17763
System Type: 64 - Bit Operating System
Manufacturer: Microsoft Corporation
OS Product key: XXXXX-XXXXX-XXXXX-XXXXX-T83GX

Local Users Accounts

User Name	Type	Last logged on	Account Status
Administrator	Administrator	-	Disabled
Adminta	Administrator	02 May 2019 (09:05:51)	Enabled

Next generation Seqrite Endpoint Security (EPS) Asset Management Feature.



Generate Reports

Operating System: All

System Manufacturer: All

Processor: All

Last Shutdown Before: 29 Nov 2019

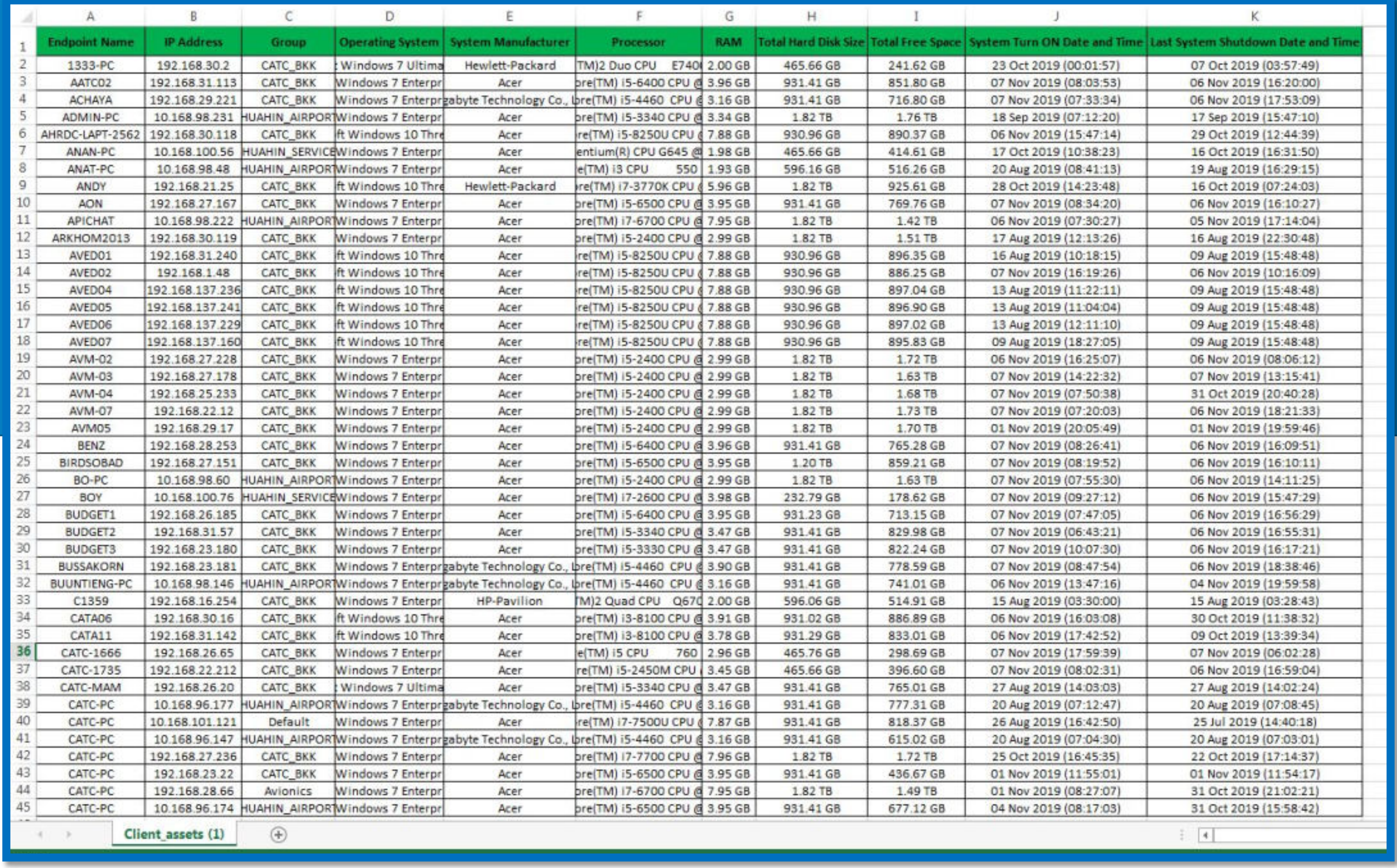
RAM: ≤ 2 GB

Application Name: All

67 Endpoint(s) found

Endpoint Name	Domain	IP Address	Operating System	Syst
1333-PC	WORKGROUP	192.168.30.2	Microsoft Windows 7 Ultimate Edition	Hew
ANAN-PC	WORKGROUP	10.168.100.56	Microsoft Windows 7 Enterprise Edition	Ace
CATC-PC	WORKGROUP	192.168.30.143	Microsoft Windows 7 Enterprise Edition	Ace
CATC1324	WORKGROUP	192.168.25.194	Microsoft Windows 7 Enterprise Edition	HP-I

Next generation Seqrite Endpoint Security (EPS) Asset Management Feature.

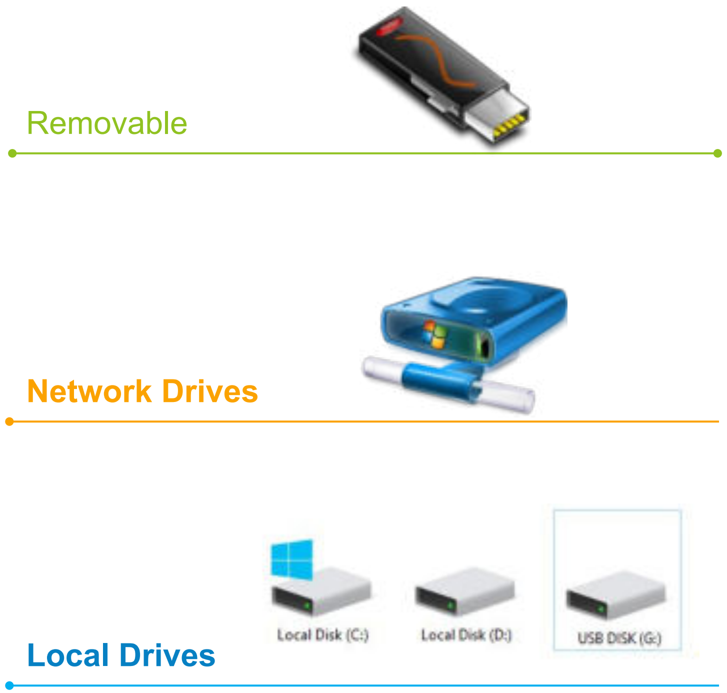


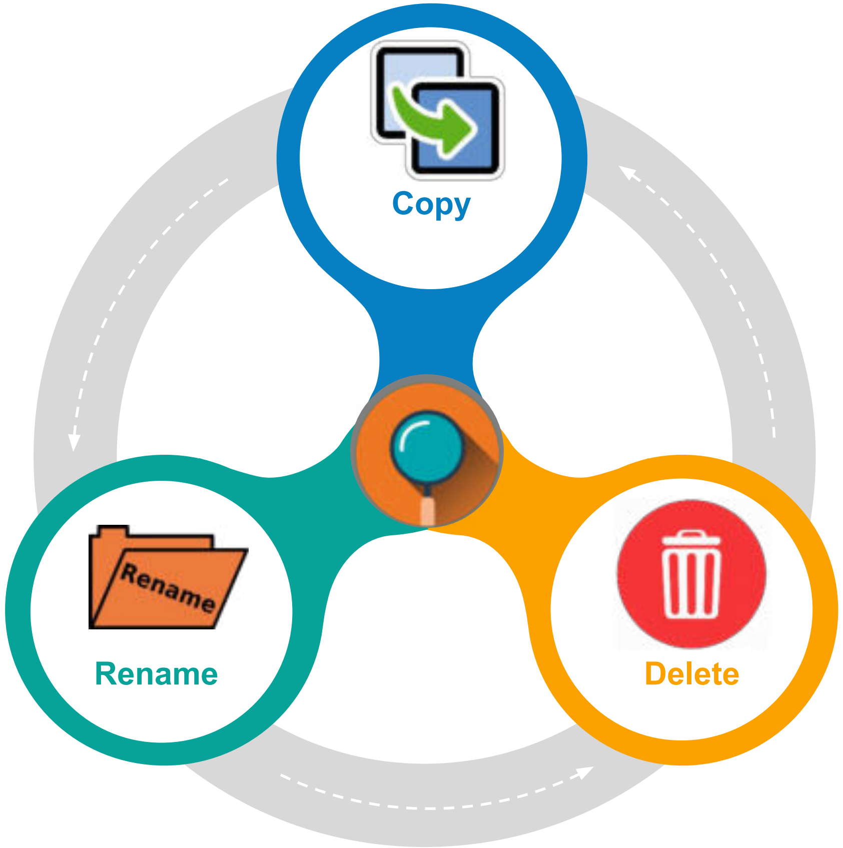
	A	B	C	D	E	F	G	H	I	J	K
1	Endpoint Name	IP Address	Group	Operating System	System Manufacturer	Processor	RAM	Total Hard Disk Size	Total Free Space	System Turn ON Date and Time	Last System Shutdown Date and Time
2	1333-PC	192.168.30.2	CATC_BKK	t Windows 7 Ultima	Hewlett-Packard	TM)2 Duo CPU E740	2.00 GB	465.66 GB	241.62 GB	23 Oct 2019 (00:01:57)	07 Oct 2019 (03:57:49)
3	AATC02	192.168.31.113	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-6400 CPU @	3.96 GB	931.41 GB	851.80 GB	07 Nov 2019 (08:03:53)	06 Nov 2019 (16:20:00)
4	ACHAYA	192.168.29.221	CATC_BKK	Windows 7 Enterpr	gabyte Technology Co., L	ore(TM) i5-4460 CPU @	3.16 GB	931.41 GB	716.80 GB	07 Nov 2019 (07:33:34)	06 Nov 2019 (17:53:09)
5	ADMIN-PC	10.168.98.231	HUAHIN_AIRPORT	Windows 7 Enterpr	Acer	ore(TM) i5-3340 CPU @	3.34 GB	1.82 TB	1.76 TB	18 Sep 2019 (07:12:20)	17 Sep 2019 (15:47:10)
6	AHRDC-LAPT-2562	192.168.30.118	CATC_BKK	ft Windows 10 Thre	Acer	re(TM) i5-8250U CPU @	7.88 GB	930.96 GB	890.37 GB	06 Nov 2019 (15:47:14)	29 Oct 2019 (12:44:39)
7	ANAN-PC	10.168.100.56	HUAHIN_SERVICE	Windows 7 Enterpr	Acer	entium(R) CPU G645 @	1.98 GB	465.66 GB	414.61 GB	17 Oct 2019 (10:38:23)	16 Oct 2019 (16:31:50)
8	ANAT-PC	10.168.98.48	HUAHIN_AIRPORT	Windows 7 Enterpr	Acer	e(TM) i3 CPU 550	1.93 GB	596.16 GB	516.26 GB	20 Aug 2019 (08:41:13)	19 Aug 2019 (16:29:15)
9	ANDY	192.168.21.25	CATC_BKK	ft Windows 10 Thre	Hewlett-Packard	re(TM) i7-3770K CPU @	5.96 GB	1.82 TB	925.61 GB	28 Oct 2019 (14:23:48)	16 Oct 2019 (07:24:03)
10	AON	192.168.27.167	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-6500 CPU @	3.95 GB	931.41 GB	769.76 GB	07 Nov 2019 (08:34:20)	06 Nov 2019 (16:10:27)
11	APICHAT	10.168.98.222	HUAHIN_AIRPORT	Windows 7 Enterpr	Acer	ore(TM) i7-6700 CPU @	7.95 GB	1.82 TB	1.42 TB	06 Nov 2019 (07:30:27)	05 Nov 2019 (17:14:04)
12	ARKHOM2013	192.168.30.119	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-2400 CPU @	2.99 GB	1.82 TB	1.51 TB	17 Aug 2019 (12:13:26)	16 Aug 2019 (22:30:48)
13	AVED01	192.168.31.240	CATC_BKK	ft Windows 10 Thre	Acer	re(TM) i5-8250U CPU @	7.88 GB	930.96 GB	896.35 GB	16 Aug 2019 (10:18:15)	09 Aug 2019 (15:48:48)
14	AVED02	192.168.1.48	CATC_BKK	ft Windows 10 Thre	Acer	re(TM) i5-8250U CPU @	7.88 GB	930.96 GB	886.25 GB	07 Nov 2019 (16:19:26)	06 Nov 2019 (10:16:09)
15	AVED04	192.168.137.236	CATC_BKK	ft Windows 10 Thre	Acer	re(TM) i5-8250U CPU @	7.88 GB	930.96 GB	897.04 GB	13 Aug 2019 (11:22:11)	09 Aug 2019 (15:48:48)
16	AVED05	192.168.137.241	CATC_BKK	ft Windows 10 Thre	Acer	re(TM) i5-8250U CPU @	7.88 GB	930.96 GB	896.90 GB	13 Aug 2019 (11:04:04)	09 Aug 2019 (15:48:48)
17	AVED06	192.168.137.229	CATC_BKK	ft Windows 10 Thre	Acer	re(TM) i5-8250U CPU @	7.88 GB	930.96 GB	897.02 GB	13 Aug 2019 (12:11:10)	09 Aug 2019 (15:48:48)
18	AVED07	192.168.137.160	CATC_BKK	ft Windows 10 Thre	Acer	re(TM) i5-8250U CPU @	7.88 GB	930.96 GB	895.83 GB	09 Aug 2019 (18:27:05)	09 Aug 2019 (15:48:48)
19	AVM-02	192.168.27.228	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-2400 CPU @	2.99 GB	1.82 TB	1.72 TB	06 Nov 2019 (16:25:07)	06 Nov 2019 (08:06:12)
20	AVM-03	192.168.27.178	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-2400 CPU @	2.99 GB	1.82 TB	1.63 TB	07 Nov 2019 (14:22:32)	07 Nov 2019 (13:15:41)
21	AVM-04	192.168.25.233	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-2400 CPU @	2.99 GB	1.82 TB	1.68 TB	07 Nov 2019 (07:50:38)	31 Oct 2019 (20:40:28)
22	AVM-07	192.168.22.12	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-2400 CPU @	2.99 GB	1.82 TB	1.73 TB	07 Nov 2019 (07:20:03)	06 Nov 2019 (18:21:33)
23	AVM05	192.168.29.17	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-2400 CPU @	2.99 GB	1.82 TB	1.70 TB	01 Nov 2019 (20:05:49)	01 Nov 2019 (19:59:46)
24	BENZ	192.168.28.253	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-6400 CPU @	3.96 GB	931.41 GB	765.28 GB	07 Nov 2019 (08:26:41)	06 Nov 2019 (16:09:51)
25	BIRDSOBAD	192.168.27.151	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-6500 CPU @	3.95 GB	1.20 TB	859.21 GB	07 Nov 2019 (08:19:52)	06 Nov 2019 (16:10:11)
26	BO-PC	10.168.98.60	HUAHIN_AIRPORT	Windows 7 Enterpr	Acer	ore(TM) i5-2400 CPU @	2.99 GB	1.82 TB	1.63 TB	07 Nov 2019 (07:55:30)	06 Nov 2019 (14:11:25)
27	BOY	10.168.100.76	HUAHIN_SERVICE	Windows 7 Enterpr	Acer	ore(TM) i7-2600 CPU @	3.98 GB	232.79 GB	178.62 GB	07 Nov 2019 (09:27:12)	06 Nov 2019 (15:47:29)
28	BUDGET1	192.168.26.185	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-6400 CPU @	3.95 GB	931.23 GB	713.15 GB	07 Nov 2019 (07:47:05)	06 Nov 2019 (16:56:29)
29	BUDGET2	192.168.31.57	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-3340 CPU @	3.47 GB	931.41 GB	829.98 GB	07 Nov 2019 (06:43:21)	06 Nov 2019 (16:55:31)
30	BUDGET3	192.168.23.180	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-3330 CPU @	3.47 GB	931.41 GB	822.24 GB	07 Nov 2019 (10:07:30)	06 Nov 2019 (16:17:21)
31	BUSSAKORN	192.168.23.181	CATC_BKK	Windows 7 Enterpr	gabyte Technology Co., L	ore(TM) i5-4460 CPU @	3.90 GB	931.41 GB	778.59 GB	07 Nov 2019 (08:47:54)	06 Nov 2019 (18:38:46)
32	BUUNTIENG-PC	10.168.98.146	HUAHIN_AIRPORT	Windows 7 Enterpr	gabyte Technology Co., L	ore(TM) i5-4460 CPU @	3.16 GB	931.41 GB	741.01 GB	06 Nov 2019 (13:47:16)	04 Nov 2019 (19:59:58)
33	C1359	192.168.16.254	CATC_BKK	Windows 7 Enterpr	HP-Pavilion	TM)2 Quad CPU Q670	2.00 GB	596.06 GB	514.91 GB	15 Aug 2019 (03:30:00)	15 Aug 2019 (03:28:43)
34	CATA06	192.168.30.16	CATC_BKK	ft Windows 10 Thre	Acer	ore(TM) i3-8100 CPU @	3.91 GB	931.02 GB	886.89 GB	06 Nov 2019 (16:03:08)	30 Oct 2019 (11:38:32)
35	CATA11	192.168.31.142	CATC_BKK	ft Windows 10 Thre	Acer	ore(TM) i3-8100 CPU @	3.78 GB	931.29 GB	833.01 GB	06 Nov 2019 (17:42:52)	09 Oct 2019 (13:39:34)
36	CATC-1666	192.168.26.65	CATC_BKK	Windows 7 Enterpr	Acer	e(TM) i5 CPU 760	2.96 GB	465.76 GB	298.69 GB	07 Nov 2019 (17:59:39)	07 Nov 2019 (06:02:28)
37	CATC-1735	192.168.22.212	CATC_BKK	Windows 7 Enterpr	Acer	re(TM) i5-2450M CPU @	3.45 GB	465.66 GB	396.60 GB	07 Nov 2019 (08:02:31)	06 Nov 2019 (16:59:04)
38	CATC-MAM	192.168.26.20	CATC_BKK	t Windows 7 Ultima	Acer	ore(TM) i5-3340 CPU @	3.47 GB	931.41 GB	765.01 GB	27 Aug 2019 (14:03:03)	27 Aug 2019 (14:02:24)
39	CATC-PC	10.168.96.177	HUAHIN_AIRPORT	Windows 7 Enterpr	gabyte Technology Co., L	ore(TM) i5-4460 CPU @	3.16 GB	931.41 GB	777.31 GB	20 Aug 2019 (07:12:47)	20 Aug 2019 (07:08:45)
40	CATC-PC	10.168.101.121	Default	Windows 7 Enterpr	Acer	re(TM) i7-7500U CPU @	7.87 GB	931.41 GB	818.37 GB	26 Aug 2019 (16:42:50)	25 Jul 2019 (14:40:18)
41	CATC-PC	10.168.96.147	HUAHIN_AIRPORT	Windows 7 Enterpr	gabyte Technology Co., L	ore(TM) i5-4460 CPU @	3.16 GB	931.41 GB	615.02 GB	20 Aug 2019 (07:04:30)	20 Aug 2019 (07:03:01)
42	CATC-PC	192.168.27.236	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i7-7700 CPU @	7.96 GB	1.82 TB	1.72 TB	25 Oct 2019 (16:45:35)	22 Oct 2019 (17:14:37)
43	CATC-PC	192.168.23.22	CATC_BKK	Windows 7 Enterpr	Acer	ore(TM) i5-6500 CPU @	3.95 GB	931.41 GB	436.67 GB	01 Nov 2019 (11:55:01)	01 Nov 2019 (11:54:17)
44	CATC-PC	192.168.28.66	Avionics	Windows 7 Enterpr	Acer	ore(TM) i7-6700 CPU @	7.95 GB	1.82 TB	1.49 TB	01 Nov 2019 (08:27:07)	31 Oct 2019 (21:02:21)
45	CATC-PC	10.168.96.174	HUAHIN_AIRPORT	Windows 7 Enterpr	Acer	ore(TM) i5-6500 CPU @	3.95 GB	931.41 GB	677.12 GB	04 Nov 2019 (08:17:03)	31 Oct 2019 (15:58:42)

File Activity Monitor

Monitor (Copy, Rename, Delete)

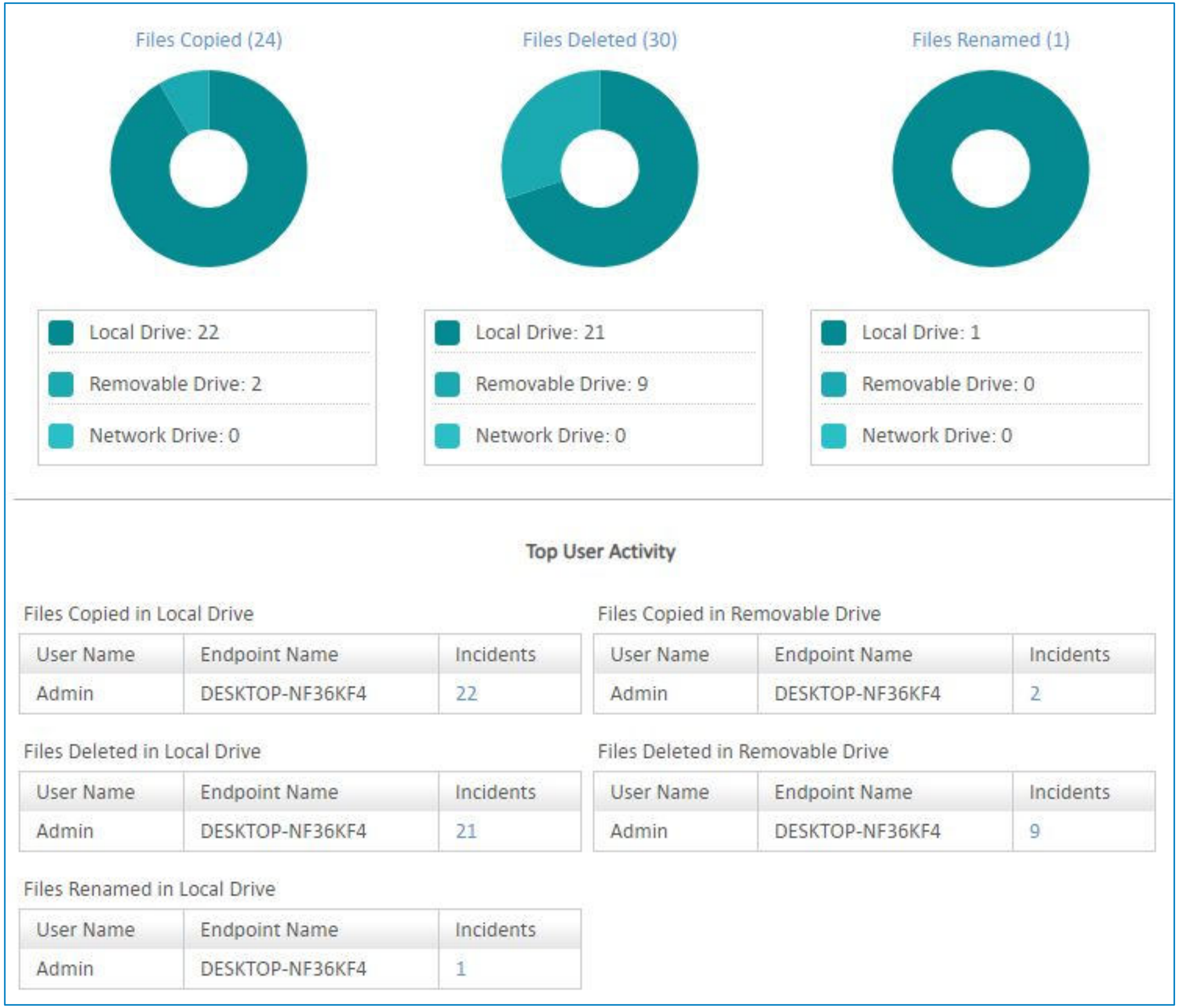
Removable /Network Drives/Local Drives





- Text Files
- Data Files
- Audio Files
- Video Files
- Image Files
- Database Files
- Executable Files
- Custom Files
- Monitor Only Delete Activity

Next generation Seqrite Endpoint Security (EPS) File Activity Monitor Feature.



Files Copied (24)

■ Local Drive: 22

■ Removable Drive: 2

■ Network Drive: 0

Files Deleted (30)

■ Local Drive: 21

■ Removable Drive: 9

■ Network Drive: 0

Files Renamed (1)

■ Local Drive: 1

■ Removable Drive: 0

■ Network Drive: 0

Top User Activity

Files Copied in Local Drive

User Name	Endpoint Name	Incidents
Admin	DESKTOP-NF36KF4	22

Files Copied in Removable Drive

User Name	Endpoint Name	Incidents
Admin	DESKTOP-NF36KF4	2

Files Deleted in Local Drive

User Name	Endpoint Name	Incidents
Admin	DESKTOP-NF36KF4	21

Files Deleted in Removable Drive

User Name	Endpoint Name	Incidents
Admin	DESKTOP-NF36KF4	9

Files Renamed in Local Drive

User Name	Endpoint Name	Incidents
Admin	DESKTOP-NF36KF4	1

Web Control

1. Web Filtering

- Custom Web Block
- Block Web Categories
- Block All Web

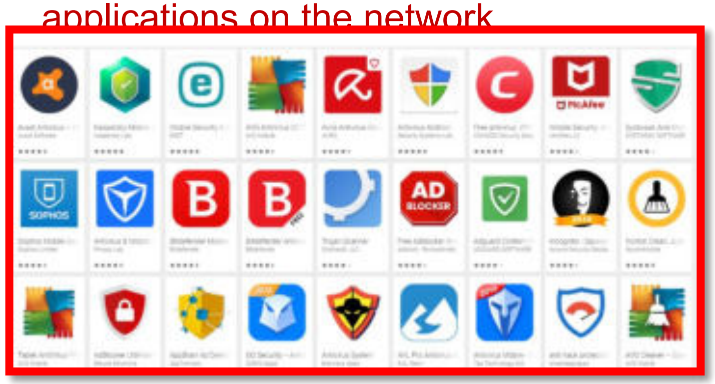
2. Internet Access Control

- Schedule Internet Access

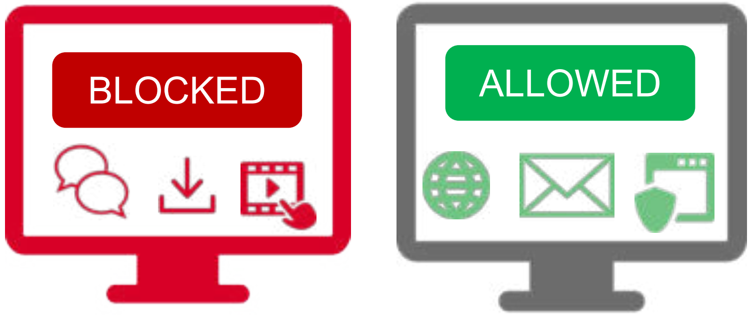
Next generation Seqrite Endpoint Security (EPS) Application Control Feature.

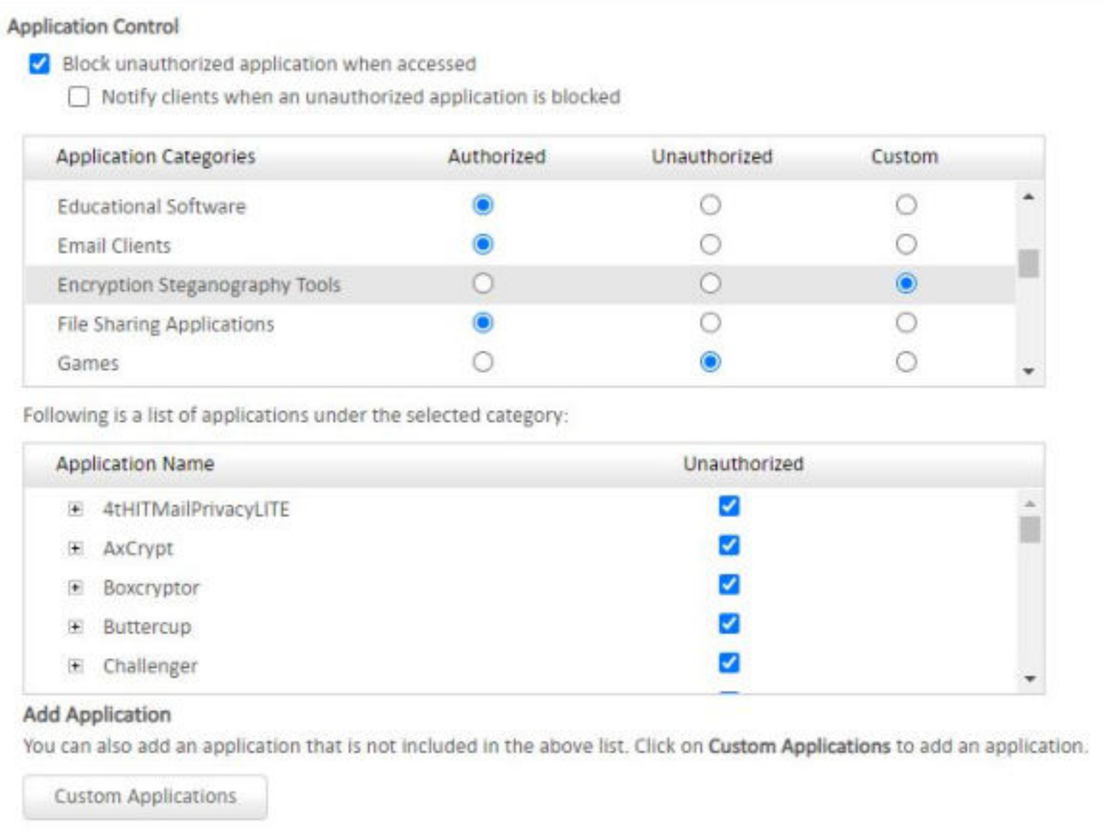
Application Control

Blocks the use of unauthorized applications on the network



- **Application Categories**
- Add Application List
- Schedule Scan





Application Control

☑ Block unauthorized application when accessed

□ Notify clients when an unauthorized application is blocked

Application Categories	Authorized	Unauthorized	Custom
Educational Software	●	○	○
Email Clients	●	○	○
Encryption Steganography Tools	○	○	●
File Sharing Applications	●	○	○
Games	○	●	○

Following is a list of applications under the selected category:

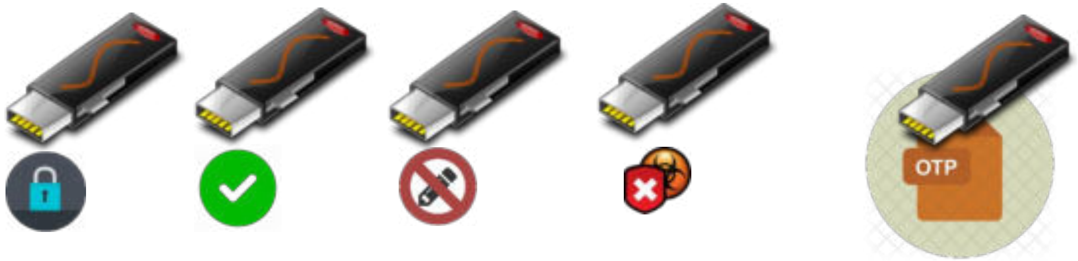
Application Name	Unauthorized
⊞ 4tHITMailPrivacyLITE	☑
⊞ AxCrypt	☑
⊞ Boxcryptor	☑
⊞ Buttercup	☑
⊞ Challenger	☑

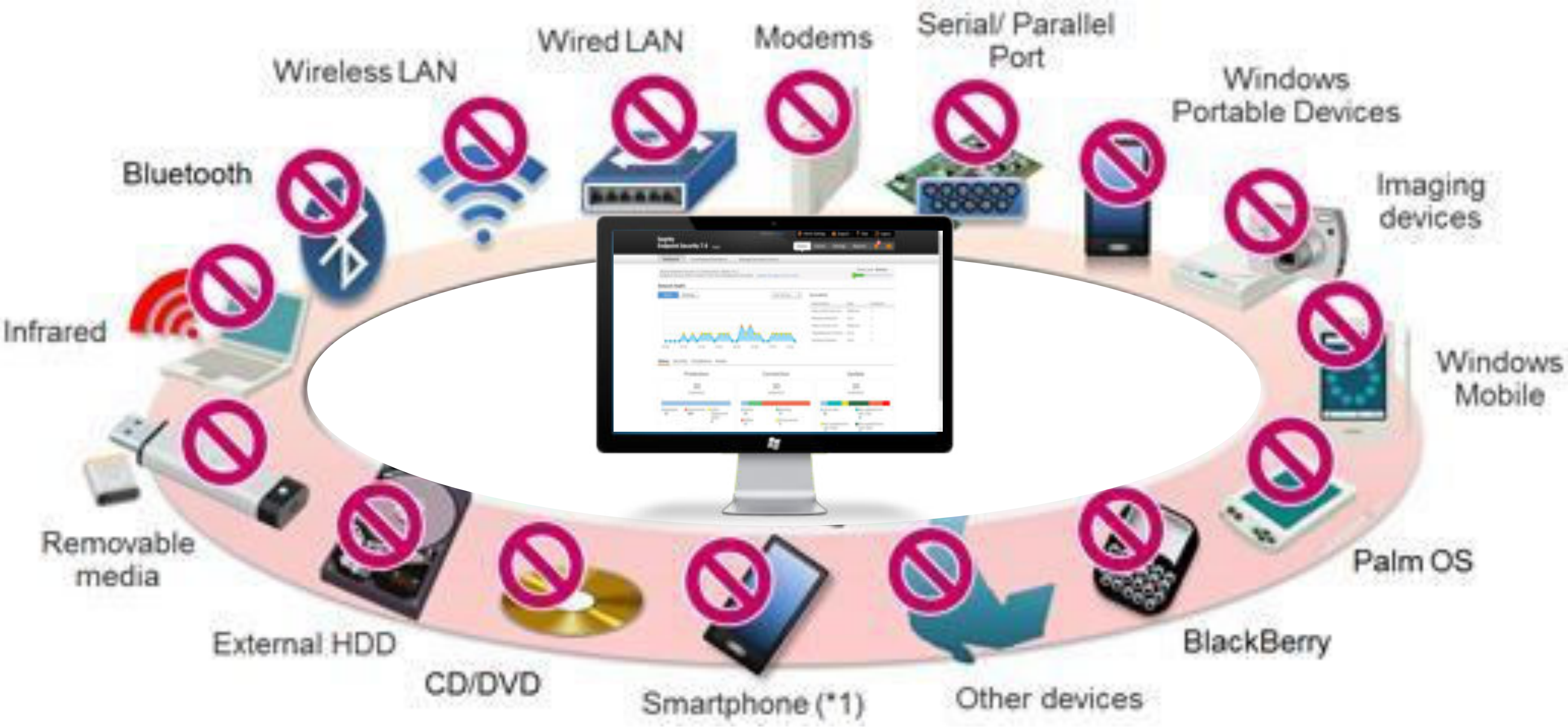
Add Application

You can also add an application that is not included in the above list. Click on **Custom Applications** to add an application.

Custom Applications

Next generation Seqrite Endpoint Security (EPS) Advance Device Control Feature.





Device Control

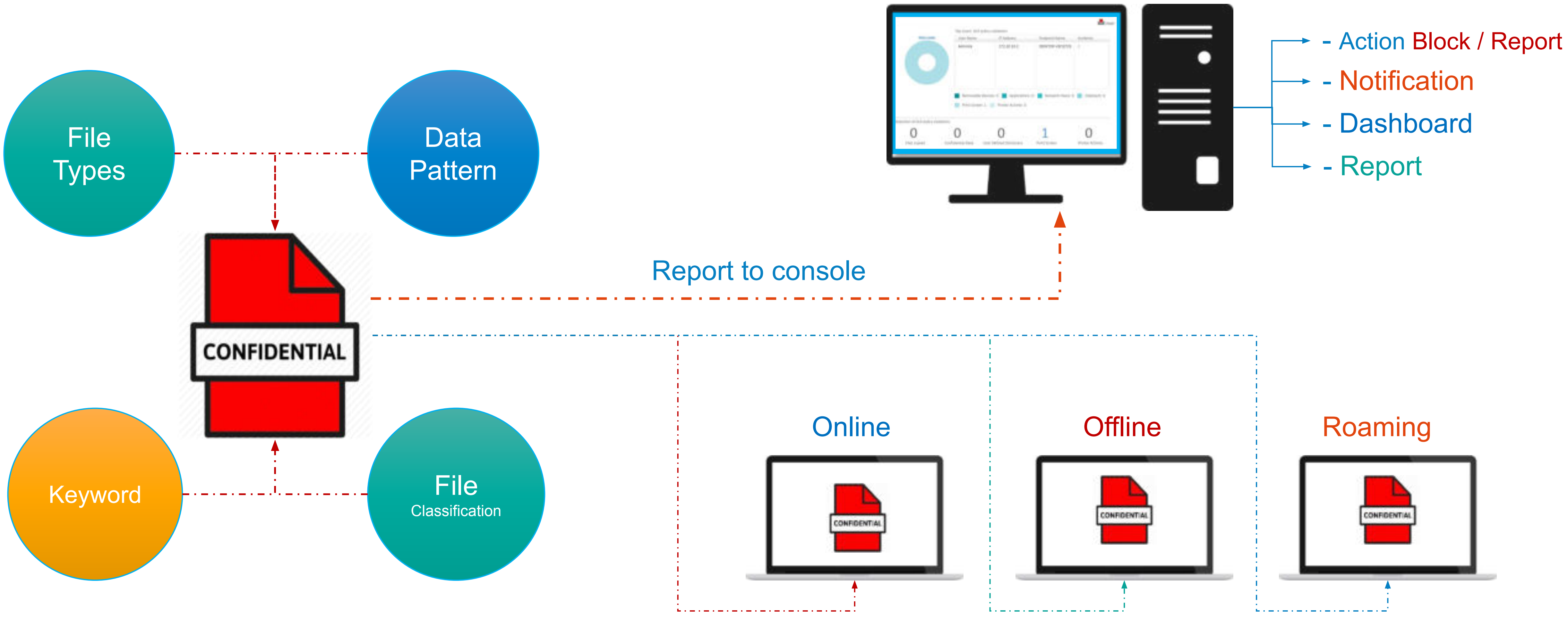
-Restrict use of unauthorized devices in the network.
(Block, Allow, Read Only, Exceptions Device)

i. USB Storage Device
ii. CD/DVD
iii. Internal Card Reader (SD Cards, Memory Cards)
iv. Floppy Drive
v. Wi-Fi
vi. Bluetooth
vii. Firewire Bus
viii. Serial Port
ix. SATA Controller
x. Thunderbolt
xi. PCMCIA
xii. Card Reader Device (MTD/SCSI)
xiii. Windows Portable Device (Digicams, Smartphones)
xiv. iPhone/iPad/iPod xv. Blackberry
xvi. Scanner & Imaging Devices
xvii. Webcam
xviii. Local Printers
xix. Teensy Board
xx. Network Share

Next generation Seqrite Endpoint Security (EPS) Data Loss Prevention Feature.

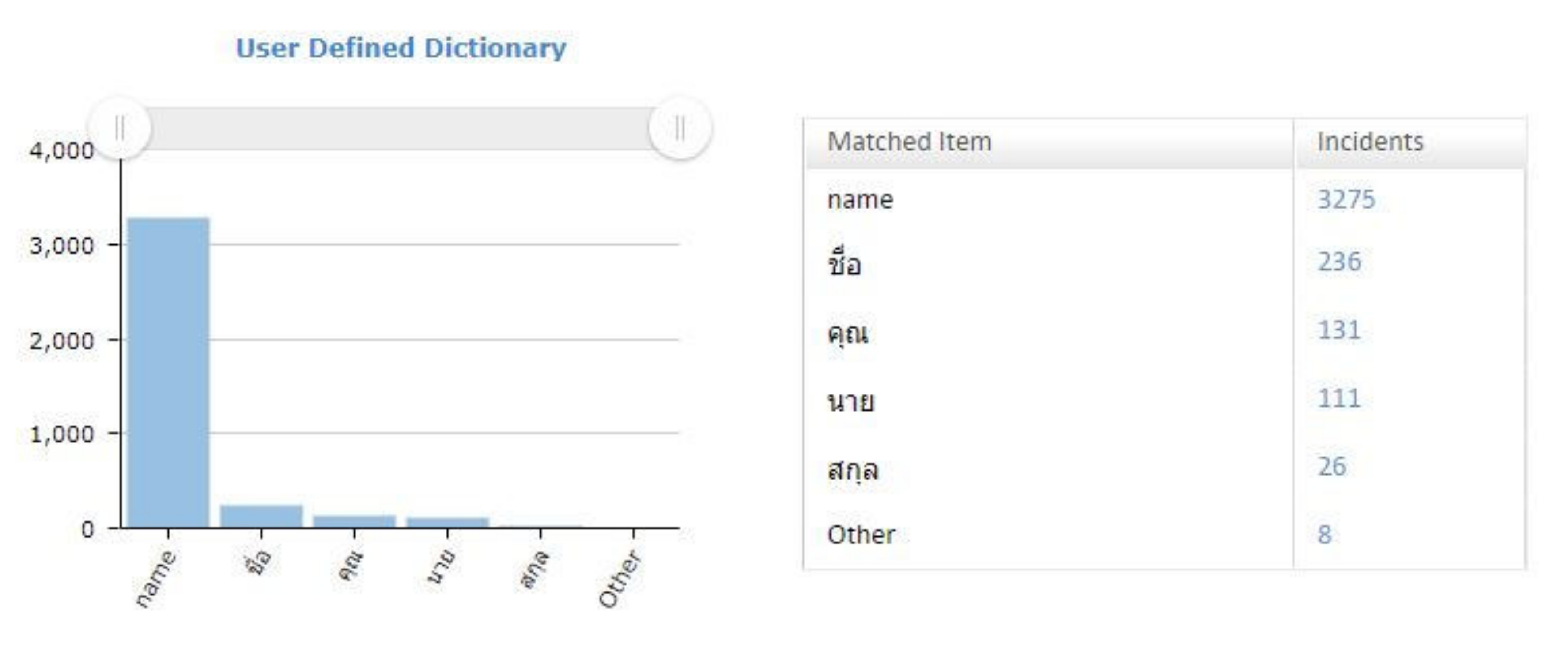
Data loss Prevention

DLP prevents data theft and leakage of confidential data, by monitoring various data transfer channels.



Next generation Seqrite Endpoint Security (EPS) Data Loss Prevention Feature.

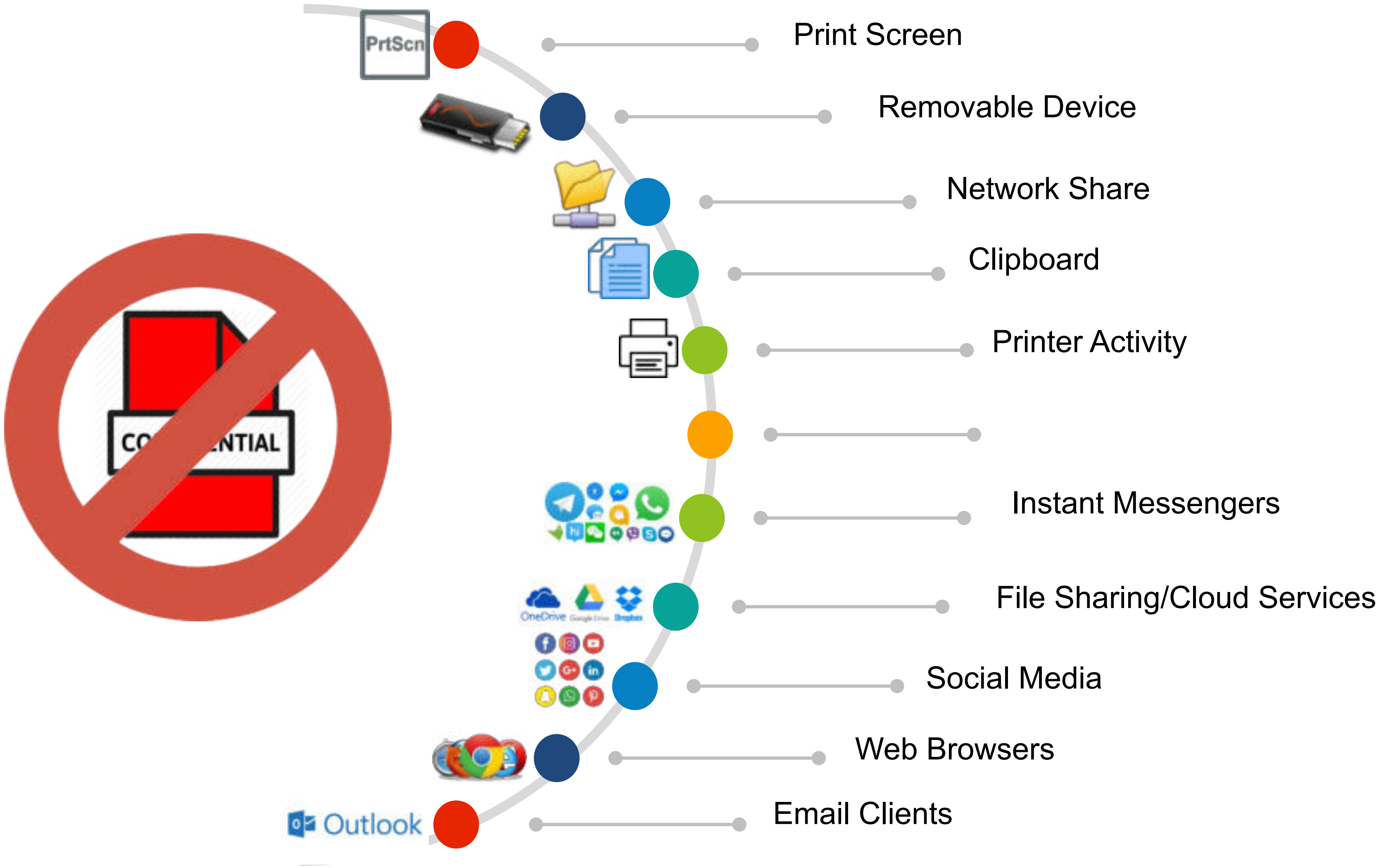
Data-At-Rest Scan



Matched Item	Incidents
name	3275
ชื่อ	236
คุณ	131
นาย	111
สกุล	26
Other	8

Next generation Seqrite Endpoint Security (EPS) Data Loss Prevention Feature.

Channel of DLP protection.



Print Screen

Removable Device

Network Share

Clipboard

Printer Activity

Instant Messengers

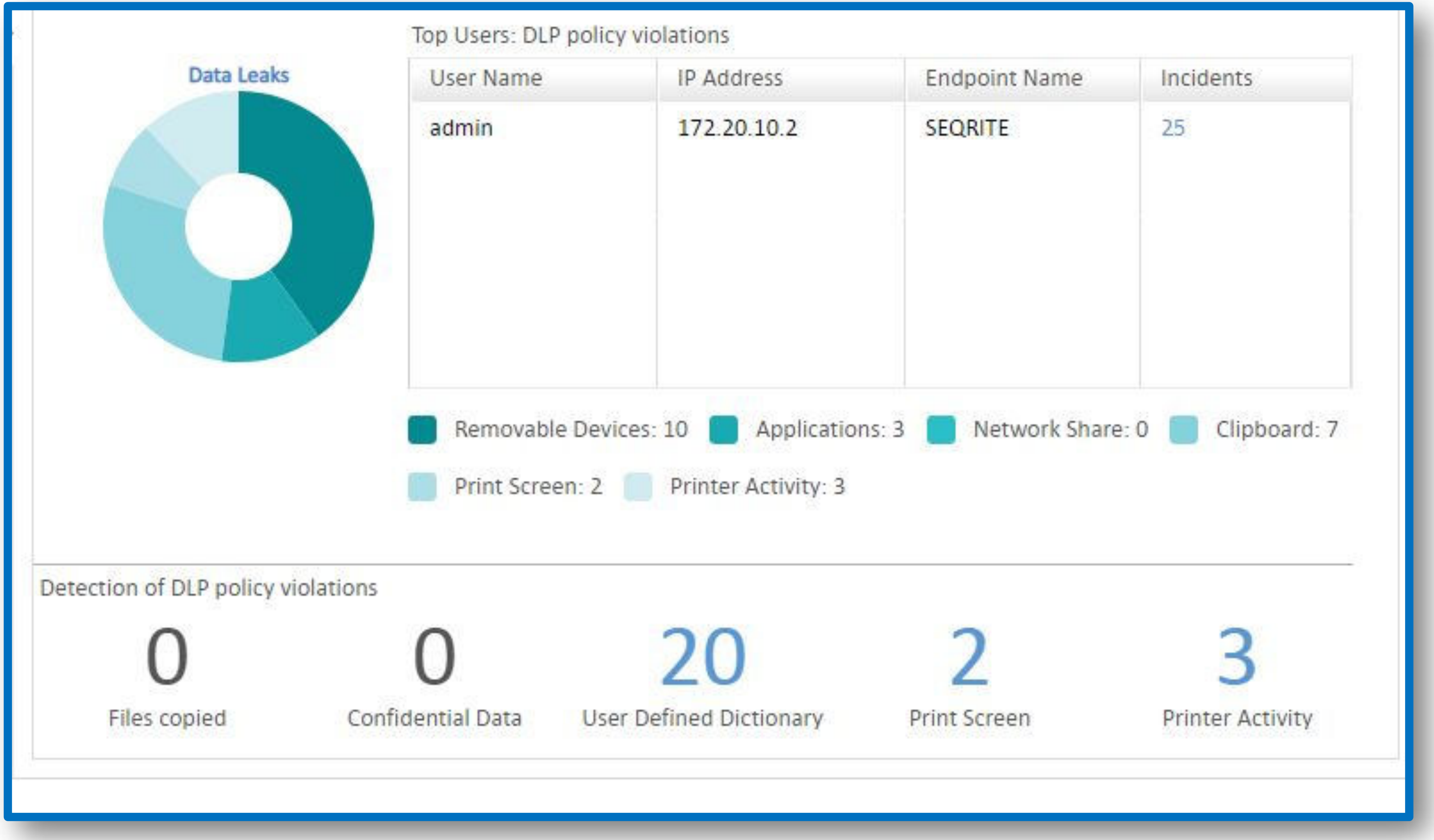
File Sharing/Cloud Services

Social Media

Web Browsers

Email Clients

Next generation Seqrite Endpoint Security (EPS) Data Loss Prevention Feature.



Top Users: DLP policy violations

User Name	IP Address	Endpoint Name	Incidents
admin	172.20.10.2	SEQRITE	25

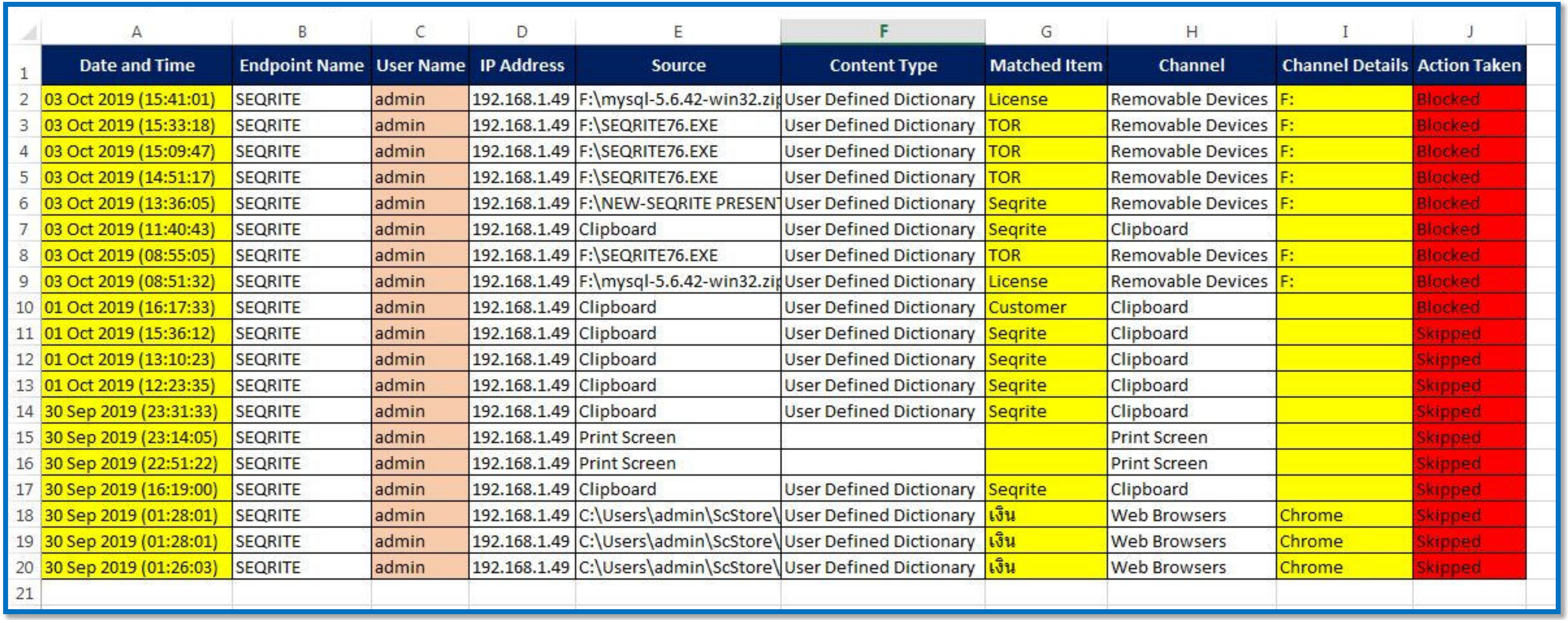
■ Removable Devices: 10 ■ Applications: 3 ■ Network Share: 0 ■ Clipboard: 7

■ Print Screen: 2 ■ Printer Activity: 3

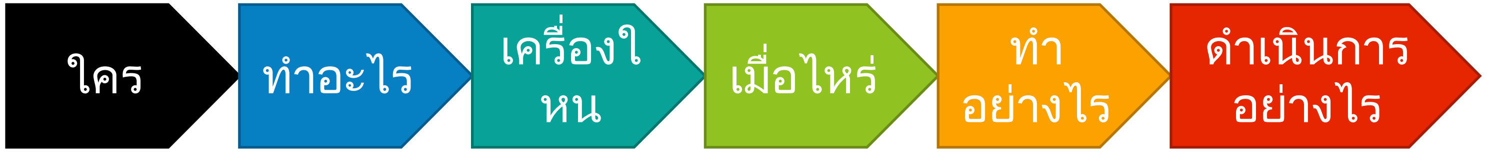
Detection of DLP policy violations

Files copied	Confidential Data	User Defined Dictionary	Print Screen	Printer Activity
0	0	20	2	3

Next generation Seqrite Endpoint Security (EPS) Data Loss Prevention Feature.



	A	B	C	D	E	F	G	H	I	J
1	Date and Time	Endpoint Name	User Name	IP Address	Source	Content Type	Matched Item	Channel	Channel Details	Action Taken
2	03 Oct 2019 (15:41:01)	SEQRITE	admin	192.168.1.49	F:\mysql-5.6.42-win32.zip	User Defined Dictionary	License	Removable Devices	F:	Blocked
3	03 Oct 2019 (15:33:18)	SEQRITE	admin	192.168.1.49	F:\SEQRITE76.EXE	User Defined Dictionary	TOR	Removable Devices	F:	Blocked
4	03 Oct 2019 (15:09:47)	SEQRITE	admin	192.168.1.49	F:\SEQRITE76.EXE	User Defined Dictionary	TOR	Removable Devices	F:	Blocked
5	03 Oct 2019 (14:51:17)	SEQRITE	admin	192.168.1.49	F:\SEQRITE76.EXE	User Defined Dictionary	TOR	Removable Devices	F:	Blocked
6	03 Oct 2019 (13:36:05)	SEQRITE	admin	192.168.1.49	F:\NEW-SEQRITE PRESENT	User Defined Dictionary	Seqrite	Removable Devices	F:	Blocked
7	03 Oct 2019 (11:40:43)	SEQRITE	admin	192.168.1.49	Clipboard	User Defined Dictionary	Seqrite	Clipboard		Blocked
8	03 Oct 2019 (08:55:05)	SEQRITE	admin	192.168.1.49	F:\SEQRITE76.EXE	User Defined Dictionary	TOR	Removable Devices	F:	Blocked
9	03 Oct 2019 (08:51:32)	SEQRITE	admin	192.168.1.49	F:\mysql-5.6.42-win32.zip	User Defined Dictionary	License	Removable Devices	F:	Blocked
10	01 Oct 2019 (16:17:33)	SEQRITE	admin	192.168.1.49	Clipboard	User Defined Dictionary	Customer	Clipboard		Blocked
11	01 Oct 2019 (15:36:12)	SEQRITE	admin	192.168.1.49	Clipboard	User Defined Dictionary	Seqrite	Clipboard		Skipped
12	01 Oct 2019 (13:10:23)	SEQRITE	admin	192.168.1.49	Clipboard	User Defined Dictionary	Seqrite	Clipboard		Skipped
13	01 Oct 2019 (12:23:35)	SEQRITE	admin	192.168.1.49	Clipboard	User Defined Dictionary	Seqrite	Clipboard		Skipped
14	30 Sep 2019 (23:31:33)	SEQRITE	admin	192.168.1.49	Clipboard	User Defined Dictionary	Seqrite	Clipboard		Skipped
15	30 Sep 2019 (23:14:05)	SEQRITE	admin	192.168.1.49	Print Screen			Print Screen		Skipped
16	30 Sep 2019 (22:51:22)	SEQRITE	admin	192.168.1.49	Print Screen			Print Screen		Skipped
17	30 Sep 2019 (16:19:00)	SEQRITE	admin	192.168.1.49	Clipboard	User Defined Dictionary	Seqrite	Clipboard		Skipped
18	30 Sep 2019 (01:28:01)	SEQRITE	admin	192.168.1.49	C:\Users\admin\ScStore\	User Defined Dictionary	เงิน	Web Browsers	Chrome	Skipped
19	30 Sep 2019 (01:28:01)	SEQRITE	admin	192.168.1.49	C:\Users\admin\ScStore\	User Defined Dictionary	เงิน	Web Browsers	Chrome	Skipped
20	30 Sep 2019 (01:26:03)	SEQRITE	admin	192.168.1.49	C:\Users\admin\ScStore\	User Defined Dictionary	เงิน	Web Browsers	Chrome	Skipped
21										



ใคร

ทำอะไร

เครื่องไหน

เมื่อไหร่

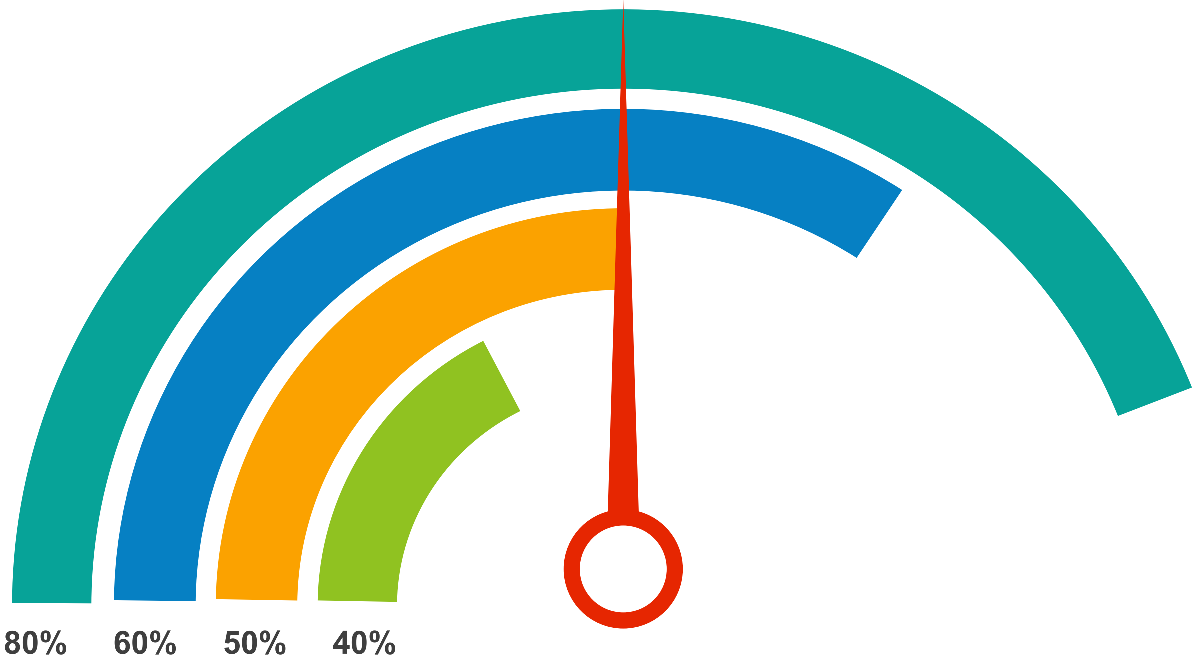
ทำอย่างไร

ดำเนินการอย่างไร

Next generation Seqrite Endpoint Security (EPS) System Tune Up Feature.

System Tune Up

Helps to improve system performance.



1 **Disk Clean-up**

2 **Registry Clean-up**

3 **Defragmentation**

4 **Report**

Next generation Seqrite Endpoint Security (EPS) Report

Report

Reports and logs for various protection modules can be fetched manually or scheduled to be emailed at periodic intervals.

Print Report

Export Report to CSV File

Export Report to PDF File

Scheduled Reports

Customize Report Parameters

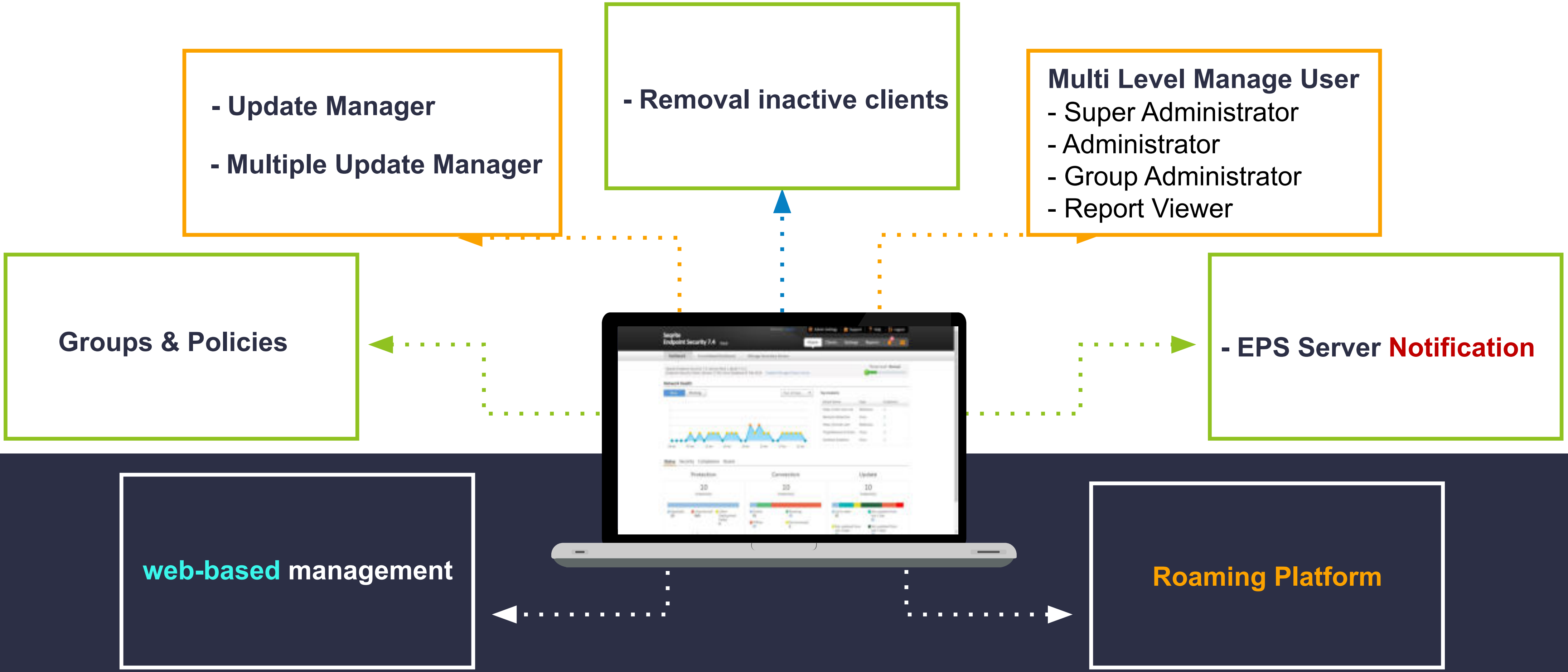
Management Server Event Logs Report

CSV
PDF
Adobe
LOG

Next generation Seqrite Endpoint Security (EPS) Management Console.

Management Console

User friendly interface for monitoring configuring and managing systems in the network with detailed report and graphical dashboard. Primary and Secondary Server architecture to manage distributed network effectively.



- Update Manager
- Multiple Update Manager

- Removal inactive clients

Multi Level Manage User
- Super Administrator
- Administrator
- Group Administrator
- Report Viewer

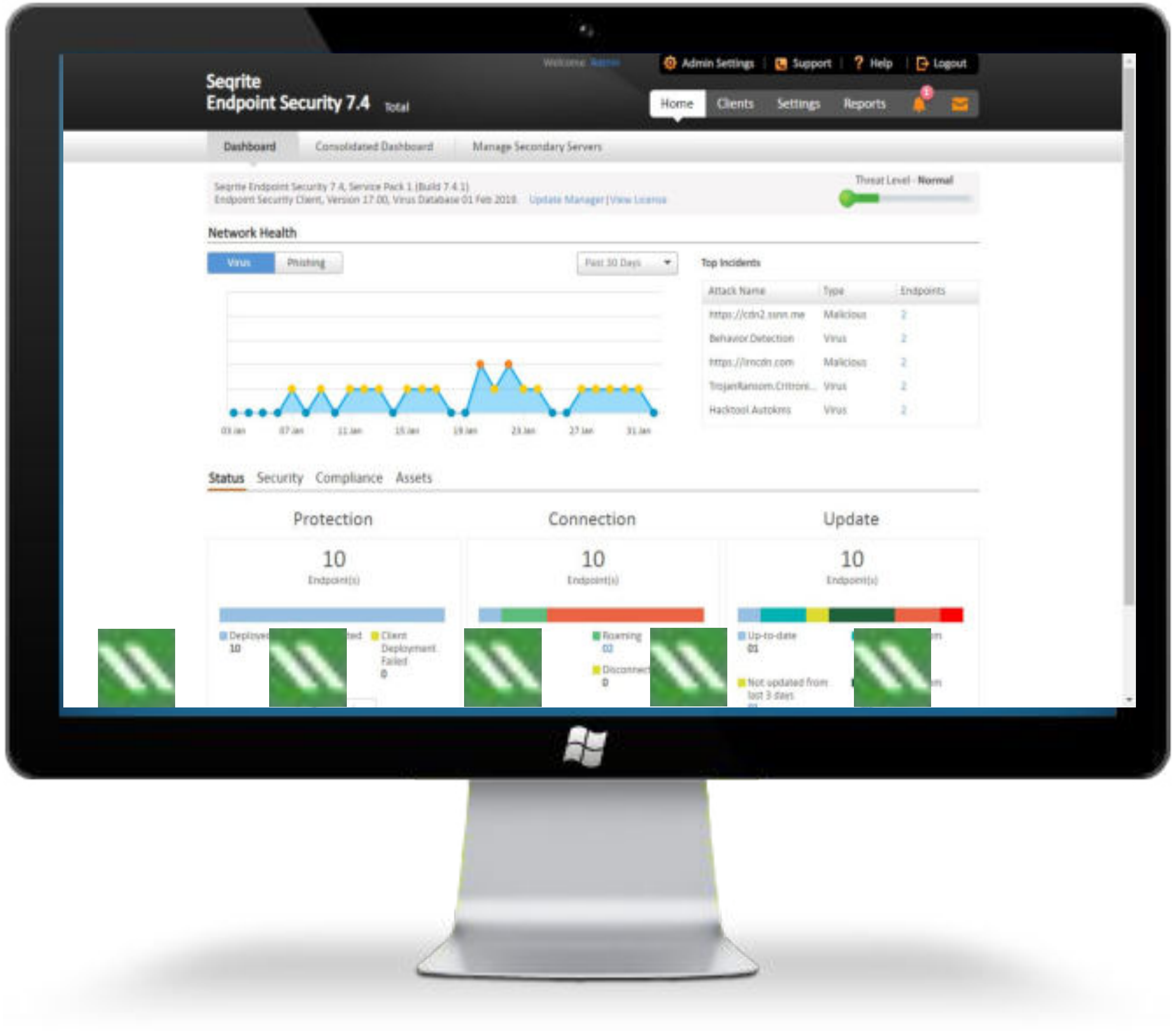
Groups & Policies

- EPS Server Notification

web-based management

Roaming Platform

Next generation Seqrite Endpoint Security (EPS) Client Deployment.



Seqrite
Endpoint Security 7.4 Total

Welcome Admin | Admin Settings | Support | ? Help | Logout

Home | Clients | Settings | Reports

Dashboard | Consolidated Dashboard | Manage Secondary Servers

Seqrite Endpoint Security 7.4, Service Pack 1 (Build 7.4.1)
Endpoint Security Client, Version 17.00, Virus Database 01 Feb 2018 Update Manager | View License

Threat Level - Normal

Network Health

Virus | Phishing | Past 30 Days

Top Incidents

Attack Name	Type	Endpoints
https://cdn2.ssnn.me	Malicious	2
Behavior Detection	Virus	2
https://lmcdn.com	Malicious	2
TrojanRansom.Crittoni...	Virus	2
Hacktool Autokms	Virus	2

Status | Security | Compliance | Assets

Protection	Connection	Update
10 Endpoint(s)	10 Endpoint(s)	10 Endpoint(s)
Deployed 10 Client Deployment Failed 0	Roaming 02 Disconnect 0	Up-to-date 01 Not updated from last 3 days

Through Active Directory
Sync with Active Directory groups to deploy Endpoint Security Client.

Remote Install
Install Endpoint Security Client remotely.

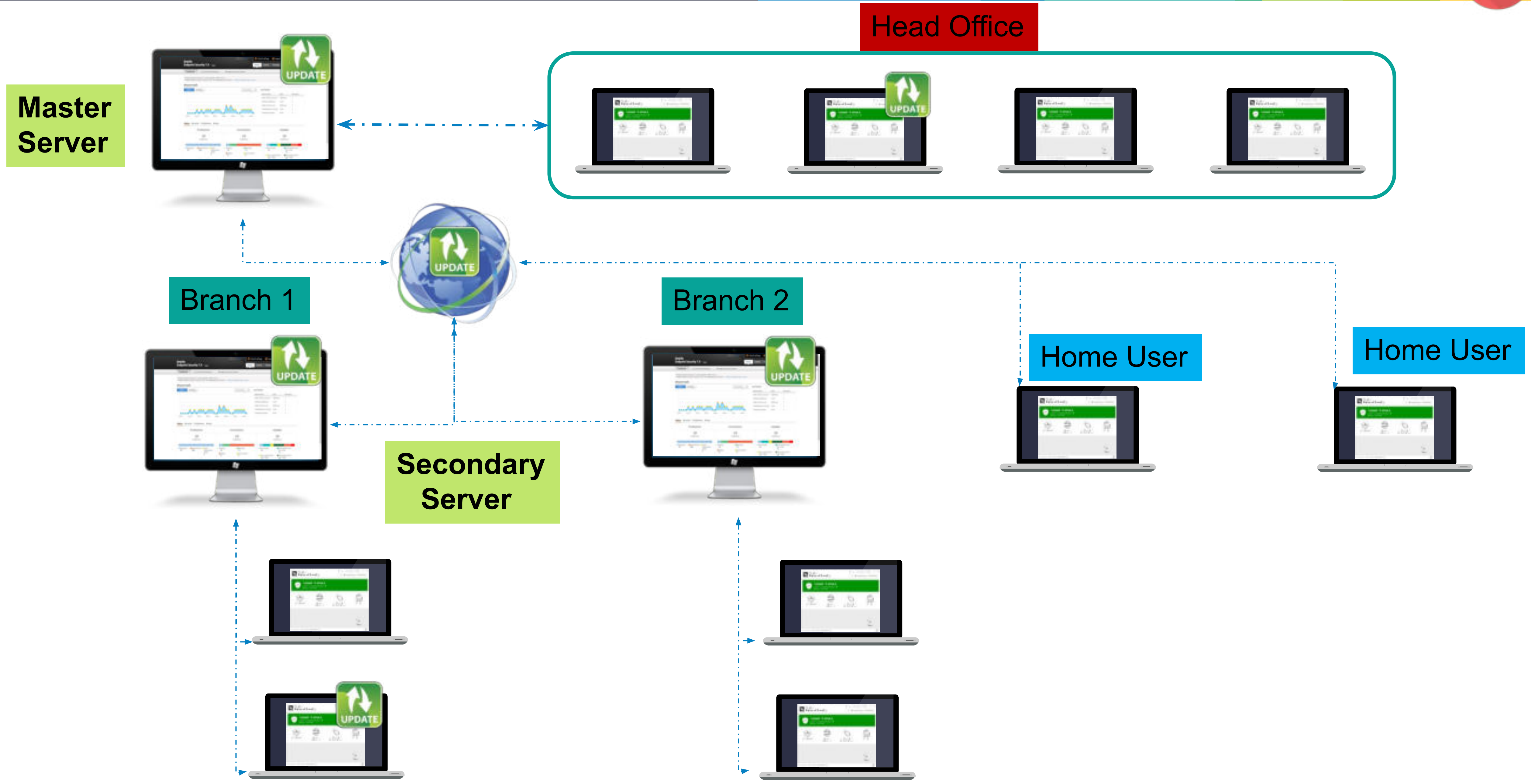
Notify Install
Send e-mail notification containing URL to Client Installation.

Client Packager
Create client installer for manual installation.

Login Script
Assign login script for client installation.

Remote Uninstall
Uninstall Client remotely.

Next generation Seqrite Endpoint Security (EPS) Management System.



Head Office

Master Server

Branch 1

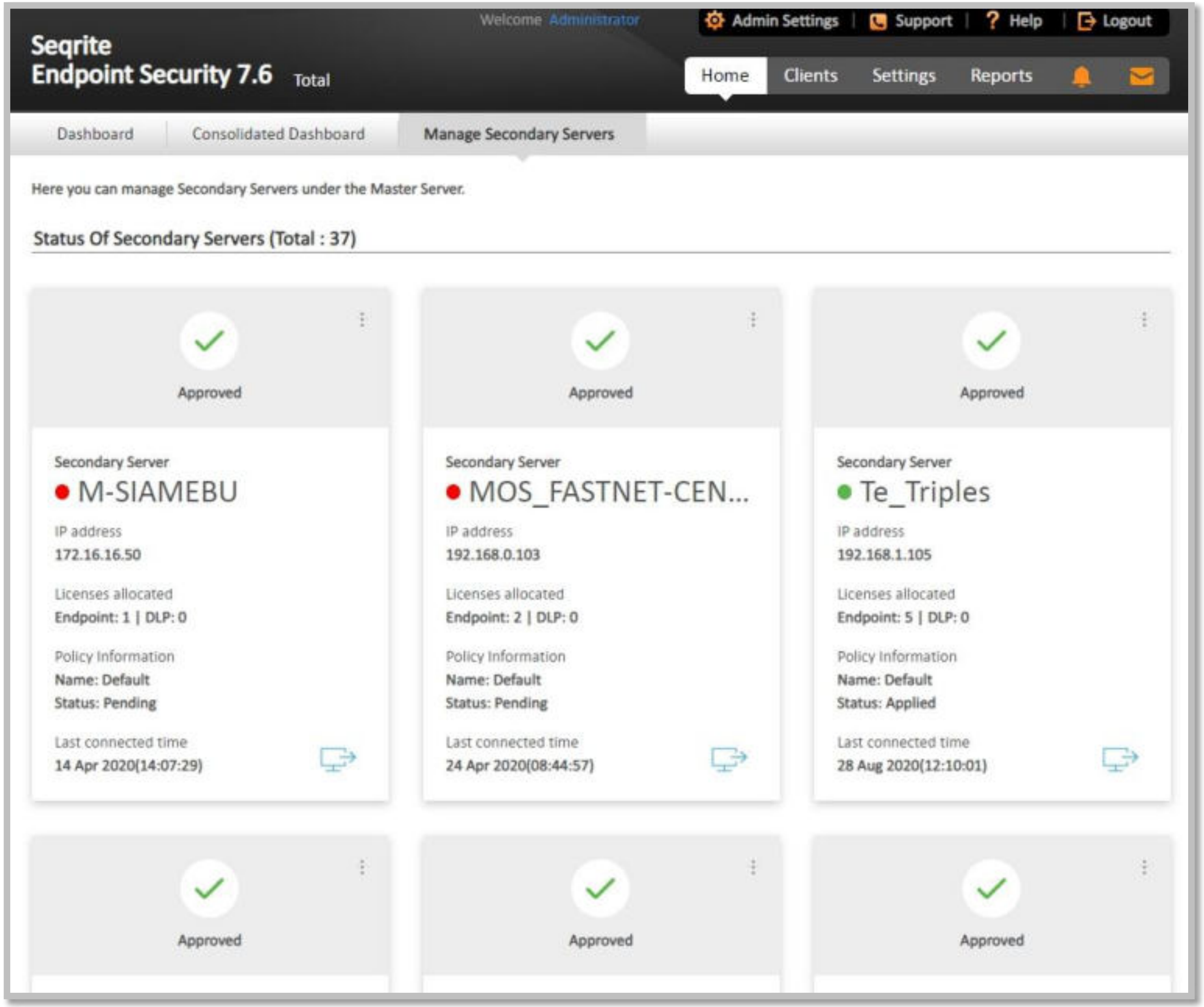
Branch 2

Secondary Server

Home User

Home User

Next generation Seqrite Endpoint Security (EPS) Manage Secondary Servers.



Here you can manage Secondary Servers under the Master Server.

Status Of Secondary Servers (Total : 37)

Approved

Secondary Server
● M-SIAMEBU
IP address
172.16.16.50
Licenses allocated
Endpoint: 1 | DLP: 0
Policy Information
Name: Default
Status: Pending
Last connected time
14 Apr 2020(14:07:29)

Approved

Secondary Server
● MOS_FASTNET-CEN...
IP address
192.168.0.103
Licenses allocated
Endpoint: 2 | DLP: 0
Policy Information
Name: Default
Status: Pending
Last connected time
24 Apr 2020(08:44:57)

Approved

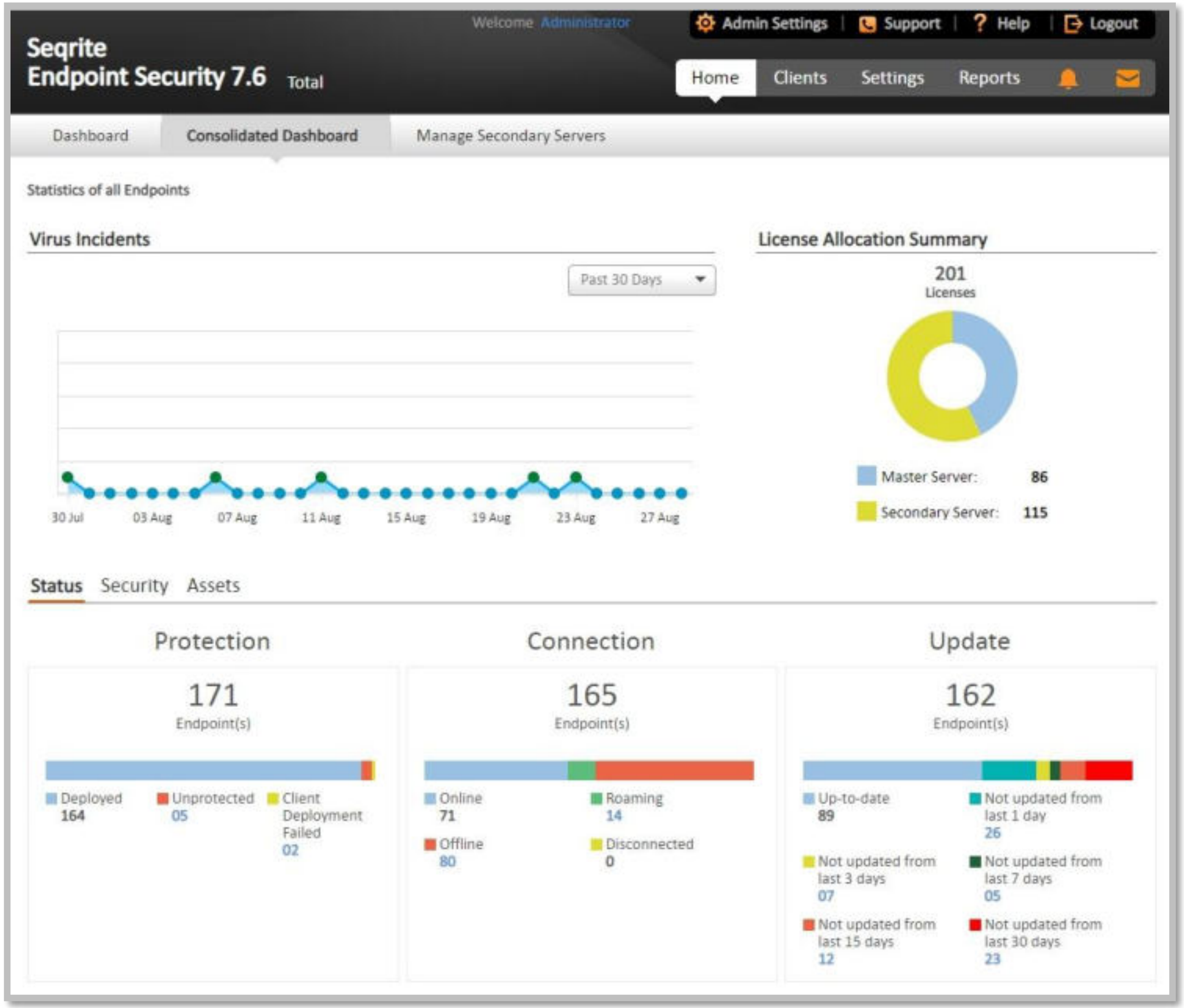
Secondary Server
● Te_Triples
IP address
192.168.1.105
Licenses allocated
Endpoint: 5 | DLP: 0
Policy Information
Name: Default
Status: Applied
Last connected time
28 Aug 2020(12:10:01)

Approved

Approved

Approved

Next generation Seqrite Endpoint Security (EPS) Consolidated Dashboard.



Statistics of all Endpoints

Virus Incidents

License Allocation Summary

201 Licenses

🟦 Master Server:	86
🟨 Secondary Server:	115

Protection

171 Endpoint(s)

🟦 Deployed	164
🟥 Unprotected	05
🟨 Client Deployment Failed	02

Connection

165 Endpoint(s)

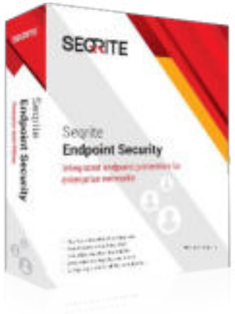
🟦 Online	71
🟩 Roaming	14
🟥 Offline	80
🟨 Disconnected	0

Update

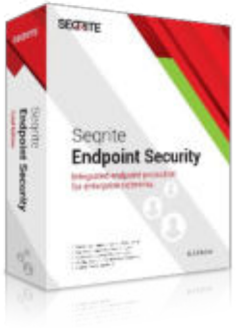
162 Endpoint(s)

🟦 Up-to-date	89
🟩 Not updated from last 1 day	26
🟨 Not updated from last 3 days	07
🟩 Not updated from last 7 days	05
🟥 Not updated from last 15 days	12
🟥 Not updated from last 30 days	23

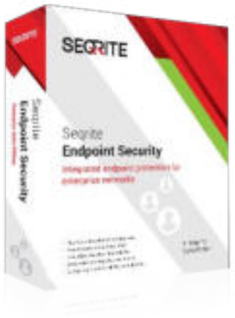
Next generation Seqrite Endpoint Security (EPS) Product Editions.



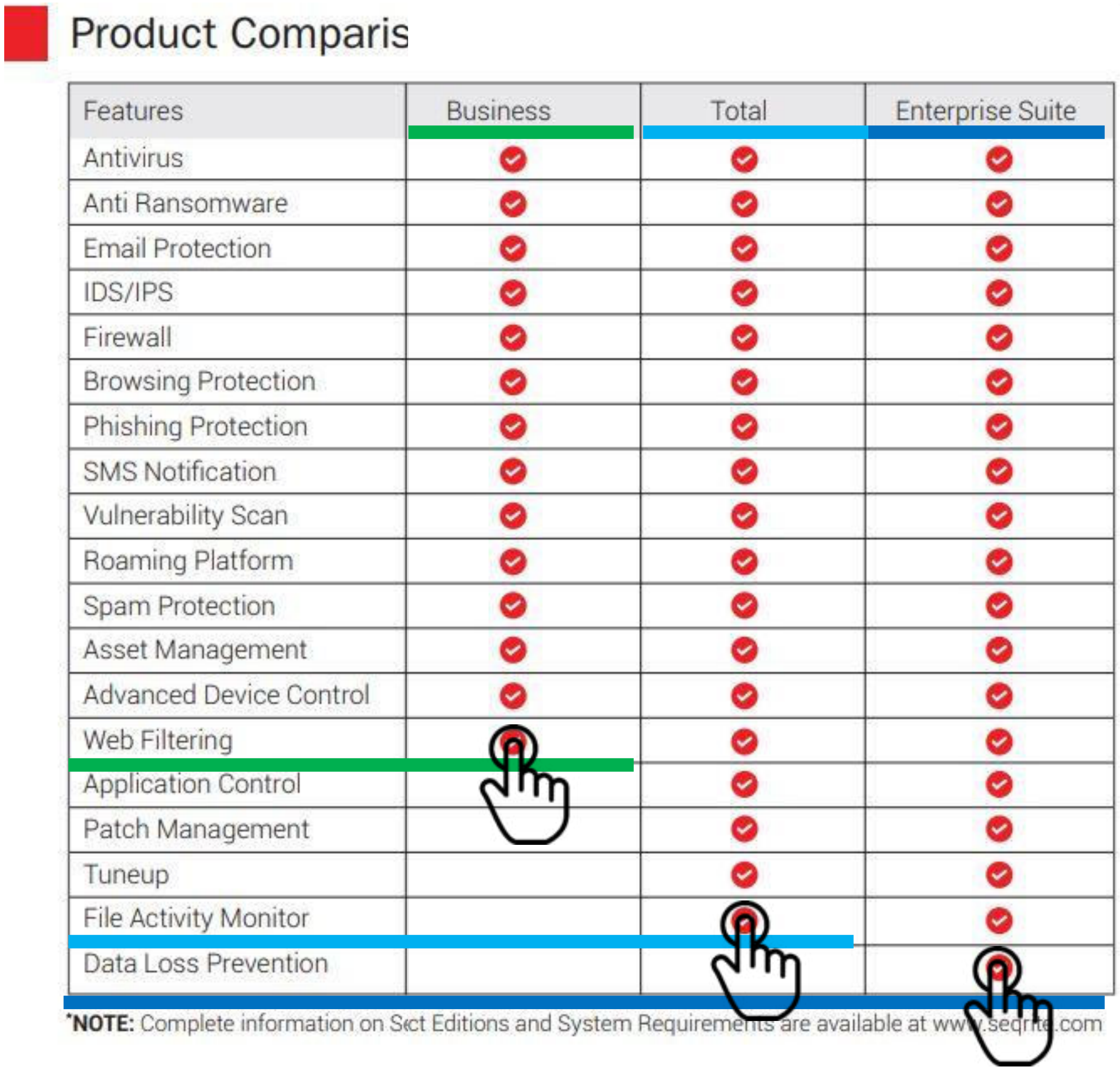
Business Edition: Endpoint protection with Advanced Device Control gives that ‘extra’ protection to enterprises.



Total Edition: Complete endpoint protection against sophisticated and targeted attacks.



Enterprise Suit Edition: Total endpoint protection and Data Loss Prevention (DLP) in one license.



Product Comparis

Features	Business	Total	Enterprise Suite
Antivirus	✓	✓	✓
Anti Ransomware	✓	✓	✓
Email Protection	✓	✓	✓
IDS/IPS	✓	✓	✓
Firewall	✓	✓	✓
Browsing Protection	✓	✓	✓
Phishing Protection	✓	✓	✓
SMS Notification	✓	✓	✓
Vulnerability Scan	✓	✓	✓
Roaming Platform	✓	✓	✓
Spam Protection	✓	✓	✓
Asset Management	✓	✓	✓
Advanced Device Control	✓	✓	✓
Web Filtering	✓	✓	✓
Application Control		✓	✓
Patch Management		✓	✓
Tuneup		✓	✓
File Activity Monitor		✓	✓
Data Loss Prevention			✓

*NOTE: Complete information on Sct Editions and System Requirements are available at www.seqrite.com

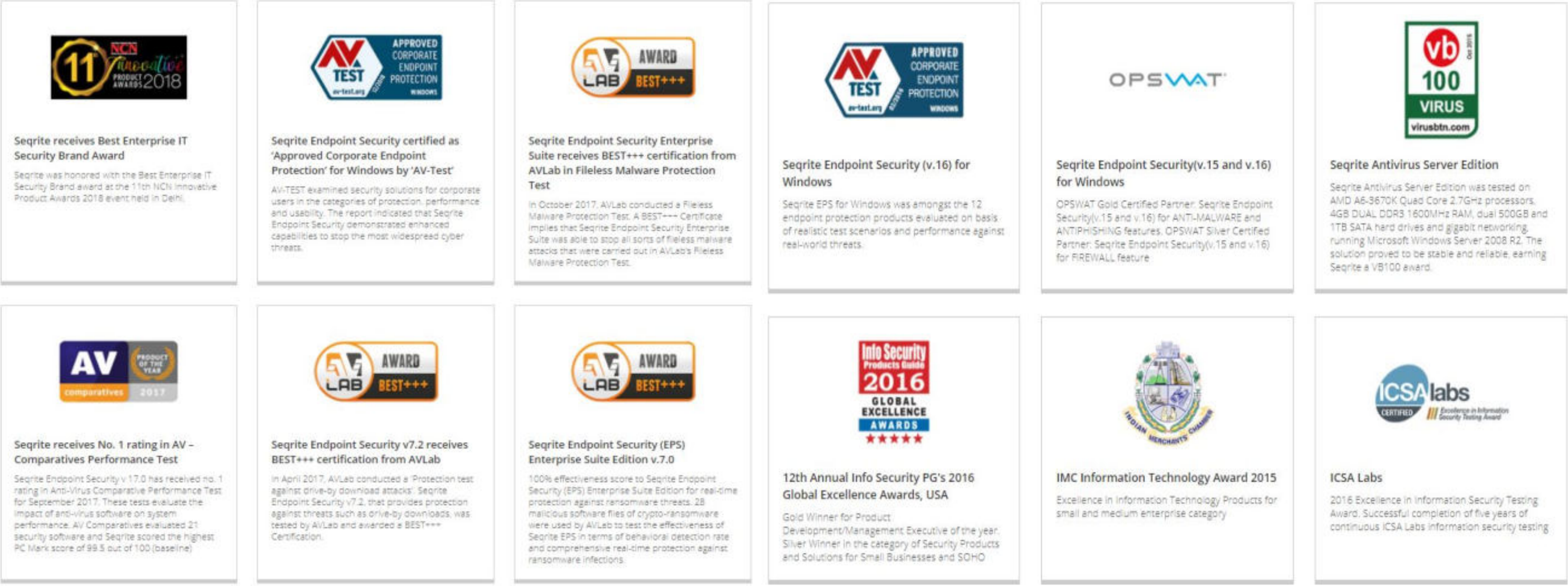
SEQRITE THAILAND

Nextech Distribution Company Limited.

47/315 อาคารไคตัค ชั้นที่ 5 ถนนป๊อปปูล่า ต.บ้านใหม่ อ.ปากเกร็ด จ.นนทบุรี 11120
เบอร์โทร 02-0563663 , 062-1919663

Next generation Seqrite Endpoint Security (EPS)

Awards & Certifications



NCN
11 Innovative
PRODUCT AWARDS 2018
AV TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS av-test.org
AVLAB AWARD BEST+++
OPSWAT
vb 100 VIRUS virusbtn.com
AV comparatives PRODUCT OF THE YEAR 2017
Info Security Products Guide 2016 GLOBAL EXCELLENCE AWARDS
INDIAN MERCHANTS' CHAMBER
ICSA labs CERTIFIED Excellence in Information Security Testing Award

Seqrite receives Best Enterprise IT Security Brand Award

Seqrite was honored with the Best Enterprise IT Security Brand award at the 11th NCN Innovative Product Awards 2018 event held in Delhi.

Seqrite Endpoint Security certified as 'Approved Corporate Endpoint Protection' for Windows by 'AV-Test'

AV-TEST examined security solutions for corporate users in the categories of protection, performance and usability. The report indicated that Seqrite Endpoint Security demonstrated enhanced capabilities to stop the most widespread cyber threats.

Seqrite Endpoint Security Enterprise Suite receives BEST+++ certification from AVLab in Fileless Malware Protection Test

In October 2017, AVLab conducted a Fileless Malware Protection Test. A BEST+++ Certificate implies that Seqrite Endpoint Security Enterprise Suite was able to stop all sorts of fileless malware attacks that were carried out in AVLab's Fileless Malware Protection Test.

Seqrite Endpoint Security (v.16) for Windows

Seqrite EPS for Windows was amongst the 12 endpoint protection products evaluated on basis of realistic test scenarios and performance against real-world threats.

Seqrite Endpoint Security(v.15 and v.16) for Windows

OPSWAT Gold Certified Partner: Seqrite Endpoint Security(v.15 and v.16) for ANTI-MALWARE and ANTIPHISHING features. OPSWAT Silver Certified Partner: Seqrite Endpoint Security(v.15 and v.16) for FIREWALL feature

Seqrite Antivirus Server Edition

Seqrite Antivirus Server Edition was tested on AMD A6-3670K Quad Core 2.7GHz processors, 4GB DUAL DDR3 1600MHz RAM, dual 500GB and 1TB SATA hard drives and gigabit networking, running Microsoft Windows Server 2008 R2. The solution proved to be stable and reliable, earning Seqrite a VB100 award.

Seqrite receives No. 1 rating in AV – Comparatives Performance Test

Seqrite Endpoint Security v 17.0 has received no. 1 rating in Anti-Virus Comparative Performance Test for September 2017. These tests evaluate the impact of anti-virus software on system performance. AV Comparatives evaluated 21 security software and Seqrite scored the highest PC Mark score of 99.5 out of 100 (baseline)

Seqrite Endpoint Security v7.2 receives BEST+++ certification from AVLab

In April 2017, AVLab conducted a 'Protection test against drive-by download attacks'. Seqrite Endpoint Security v7.2, that provides protection against threats such as drive-by downloads, was tested by AVLab and awarded a BEST+++ Certification.

Seqrite Endpoint Security (EPS) Enterprise Suite Edition v.7.0

100% effectiveness score to Seqrite Endpoint Security (EPS) Enterprise Suite Edition for real-time protection against ransomware threats. 28 malicious software files of crypto-ransomware were used by AVLab to test the effectiveness of Seqrite EPS in terms of behavioral detection rate and comprehensive real-time protection against ransomware infections.

12th Annual Info Security PG's 2016 Global Excellence Awards, USA

Gold Winner for Product Development/Management Executive of the year. Silver Winner in the category of Security Products and Solutions for Small Businesses and SOHO

IMC Information Technology Award 2015

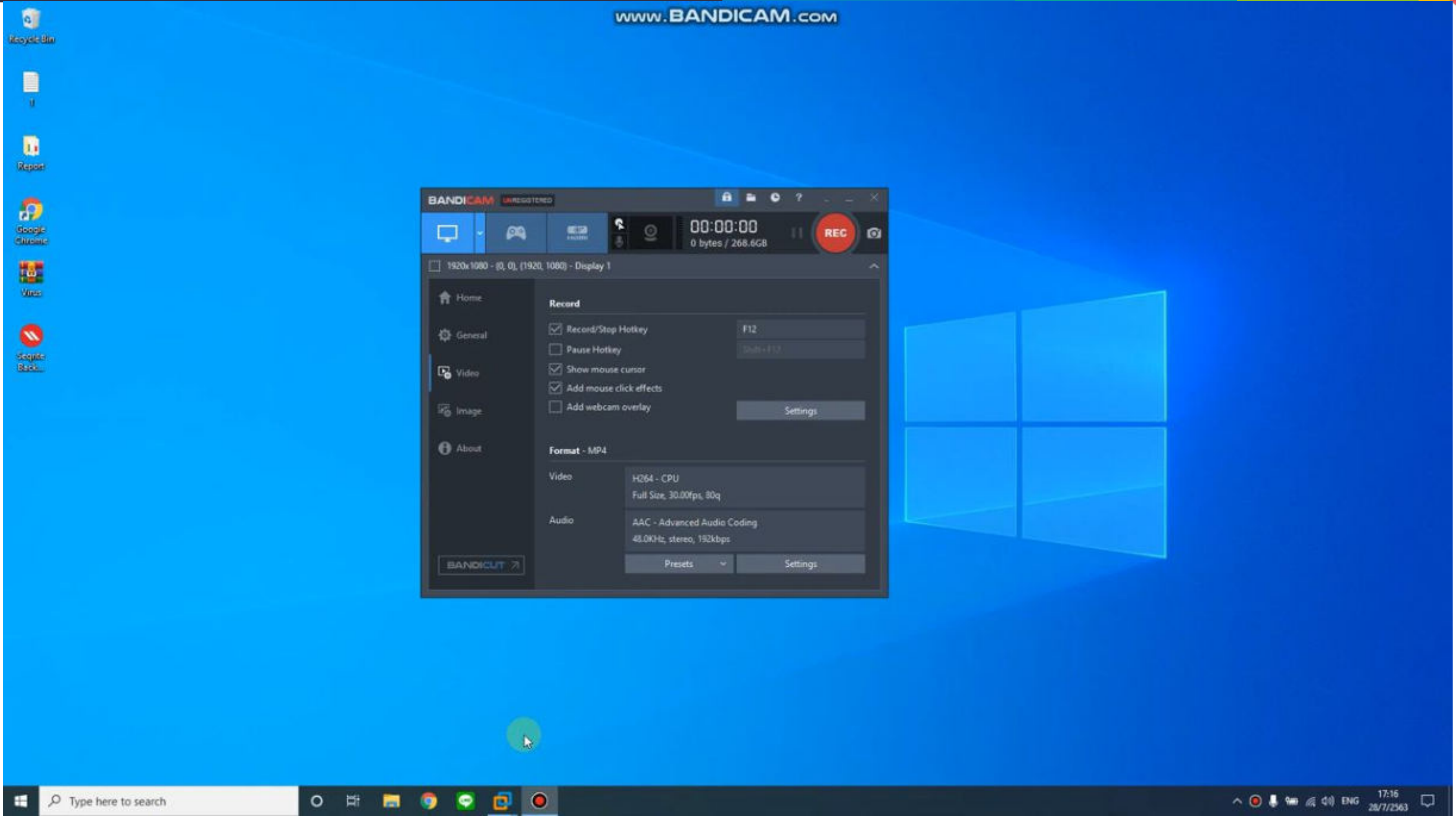
Excellence in Information Technology Products for small and medium enterprise category

ICSA Labs

2016 Excellence in Information Security Testing Award. Successful completion of five years of continuous ICSA Labs information security testing

Next generation Seqrite Endpoint Security (EPS)

Backup & Restore



00:00:00
0 bytes / 268.6GB

1920x1080 - (0, 0), (1920, 1080) - Display 1

Record

☑ Record/Stop Hotkey F12
□ Pause Hotkey Shift+F12
☑ Show mouse cursor
☑ Add mouse click effects
□ Add webcam overlay Settings

Format - MP4

Video: H264 - CPU
Full Size, 30.00fps, 80q

Audio: AAC - Advanced Audio Coding
48.0KHz, stereo, 192kbps

Presets Settings