SEQRITE

Enterprise Security Solutions by Quick Heal

Seqrite
Endpoint Security

Integrated enterprise security and unified endpoint management console

Enterprise Suite Edition

www.seqrite.com

Product Highlights

Innovative endpoint security that prevents data leakage, monitors assets, file transfers and provides robust web security and antivirus features.

- Integrates malware protection, web protection, browser and data protection (DLP)-all in one license.
- Centralized patch management solution for all Microsoft application vulnerability patching needs.
- Comprehensive and cumulative information of Windows, Mac and Linux endpoints with enhanced Asset Management feature.
- Administrators can specify device names and time-based access ensuring complete control of USB interface.
- Strong endpoint protection for Windows, Mac and Linux platforms from one management console.

Features

ADVANCED DEVICE CONTROL

Allows you to manage various external devices that your employees use. It enables organizations to control, configure and define separate access policies for various device types on Windows and Mac platforms. With the help of this feature, IT administrators can grant,

- Permit temporary access to a device for specific client for configured duration.
- Specified access to USB mass storage devices based on its model name.
- Blocking of USB interface is possible for all USB devices except mass storage and input devices.
- Full device encryption for all file systems.

In addition to these enhancements, each external storage device can be granted the following access types:

- **Allow** – Data can be transferred to and from the device.
- **Block** – Data cannot be transferred to or from the device.
- **Read Only** – Data can only be read from the device

WEB FILTERING

Allows the blocking of particular categories of websites (e.g. Social Networking, Games, etc.) or individual user-specified websites to limit web access and increase productivity.

APPLICATION CONTROL

Categories of applications can be either authorized or unauthorized from being executed within the network. This feature also gives the flexibility to add custom applications to an existing blocked list.

- Allows entire categories of applications to be either authorized or unauthorized.
- Custom applications that do not exist in the predefined blocked list can be added.
- Gives an extensive overview of all applications (authorized or unauthorized) installed within the network.

ASSET MANAGEMENT

Gives comprehensive and cumulative information about the hardware and software configuration of every endpoint. The administrators can easily view details such as hardware configuration, system information, updates installed and hardware/software changes pertinent for each system. Notifications are sent to the configured email addresses whenever any alteration to the hardware or software takes place on any system. For instance, if there is a change in RAM a notification is sent to the administrators with all details of the change.

VULNERABILITY SCAN

This feature scans known vulnerabilities of installed applications and operating systems in the network in real-time. It helps frame security measures against known vulnerabilities and protects against security breaches by threat agents.

- Scans vulnerabilities in applications such as Adobe, Safari, Mozilla, Oracle, etc.
- Sends notifications regarding unpatched operating systems working on computers within the network.

PATCH MANAGEMENT

Centralized patch management strategy to successfully remediate security vulnerabilities. It enables IT administrators to check and install missing patches for Microsoft applications installed in enterprise endpoints. A simplified and centralized approach to ensure that all required patches are successfully deployed for reduced security risks and optimal network productivity.

DATA LOSS PREVENTION

Stops data leakage within or outside the organization by regulating data transfer channels such as removable devices, network sharing, web apps, online services, print screen and system clipboard. DLP also provides the ability to scan data-at-rest on end-points and removable devices. The following channels can be regulated by DLP:

- Office files, graphic files, programming files and others.
- Confidential data like credit/debit card details and personal files.
- Customized user-defined dictionary can be implemented, and instant alerts or cumulative reports can be gained to preside over data leakage.

FILE ACTIVITY MONITOR

Audits confidential files to monitor suspicious actions such as file copy, file rename or file delete. In this manner, internal and external threats can be blocked and confidential data leakage can be monitored. All files that are transferred to local drives, removable drives or network drives can also be policed.

File activity monitor is an invaluable tool for auditing all the files that move in and out of the network and also for receiving a bird's eye view of all actions against confidential files of all formats within an organization. Administrator can specify folder paths to be excluded from being monitored by this feature.

IDS / IPS

Advanced defense detects attacks from various sources such as port scanning attack, Distributed Denial of Service (DDoS) and more. This detection implements a security layer to all communications and cordons your system from unwanted intrusions or attacks.

- **Intrusion Prevention** – Blocks malicious network activities that attempt to exploit software vulnerabilities of the applications.
- **Port Scanning Attack Prevention** – Essentially, a port scan attack consists of sending a message to each port in the network, one at a time. Depending on the response received the attacker determines if the port is being used and can be probed further for vulnerabilities. This feature blocks intruder attempts aimed at attacking any open port in the network.
- **DDoS Attack Prevention** – DDoS (Distributed Denial of Service) is a type of DoS attack where multiple compromised systems which are usually infected with malware – are used to target a single system, resulting in denial of service.
  Seqrite Endpoint Security successfully blocks any attempt to initiate any DDoS attack to any system in the network.

GROUP POLICY MANAGEMENT

Different user groups within the network can be defined and flexible policies can be set accordingly for each group.

SPAM PROTECTION

Scans your endpoint inboxes for spam, phishing attacks and unsolicited emails that sneak through network defenses.

THIRD-PARTY ANTIVIRUS REMOVAL

During the EPS client installation, if another antivirus solution is detected its uninstaller will be launched, or it will automatically be uninstalled. The Seqrite EPS installation will not proceed unless the previously installed antivirus is uninstalled from the system.

BROWSING PROTECTION

Endpoint clients can be safeguarded against attacks originating from malicious websites accessed from within the network.

PHISHING PROTECTION

Phishing attacks that originate from malicious codes over the Internet are thwarted before they can enter the network and spread.

FIREWALL PROTECTION

Blocks unauthorized access to the business network. Allows customization rules to be set to Low, Medium, High or Block All based on observed network traffic. Administrators can also configure exceptions for specific IP addresses or ports to be allowed or blocked. The three Firewall customization levels are:

- **Low** – Firewall configured at Low allow access to all incoming and outgoing traffic excluding added exceptions.
- **Medium** – Allows all outgoing traffic but blocks incoming traffic excluding added exceptions.
- **High** – Blocks all incoming and outgoing traffic excluding added exceptions.
- **Block all** – Blocks all incoming and outgoing traffic.

  This feature also gives the flexibility to configure exceptions to the Firewall rules. For instance, if the Firewall configuration has been set on 'High', an exception to allow all connections for a specific IP address or port can be added.

TUNEUP

This feature enhances the performance of computer systems in the network by cleaning junk files and deleting invalid registry/disk entries.

- Tuneup can be carried out for all endpoints from the Endpoint Security Server.
- Maintenance can also be scheduled at a specific time and date.

ROAMING PLATFORM

Seqrite Roaming Platform is a cloud-based solution that allows enterprises to stay connected with and manage endpoints at all times, even when the endpoints are out of the local enterprise network. With the help of this feature, network administrators can rest assured as they can view the latest endpoint status, and easily perform the following activities on endpoints not connected to the network:

- Check the compliance status
- Apply security policies
- Scan for security threats
- Perform tune-ups to improve performance
- Redirection of roaming clients
- Apply service packs
- View reports and notifications

EMAIL AND SMS NOTIFICATIONS

This feature sends notifications to preconfigured email addresses and phone numbers.

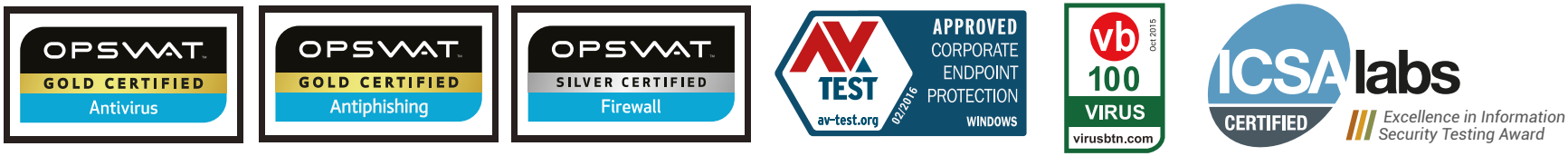
- These notifications alert the network administrator about critical network events such as detection of viruses, virus out breaks, attempts to access an unauthorized device, license expiry date etc.

OTHERS

Seqrite Windows client builds and features are also integrated into Endpoint Security. The following Windows client settings can also be configured from EPS server:

- **Behavior Detection System settings** – These settings detect unknown viruses and malware and other threats in real- time by inspecting application behavior via heuristic scanning techniques.
- **Safe Mode Protection settings** – These settings help avoid unauthorized access to computers when they are in safe

Certifications



Product Comparison

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

***NOTE:** Data Loss Prevention is not available in EPS Business or EPS Total by default. The feature is only available as an additional pack.

System Requirements

System requirements for Seqrite Endpoint Security server are as follows:

General Requirements

Component	Requirements
Processor	1 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium or higher RAM 2 GB – 4 GB
Hard disk space	5200 MB
Web browser	• Internet Explorer 7, 8, 9, 10, or 11 • Google Chrome 45, 46, or 47 • Mozilla Firefox 38, 39, or 40
Display	1024 x 768

- For more than 25 clients, Seqrite recommends to install EPS Server and Patch Management server on the Windows server operating system.

For more than 500 clients, Seqrite recommends:

- A dedicated Web server (IIS).
- Minimum 2 GHz processor or higher.
- 4 GB RAM or higher

Operating system requirements:

- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 7 Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows Vista Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows XP 32-bit SP3, 64-bit SP1 and SP2 / Professional Edition (32-bit / 64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)

Additional software required for SEPS server

Seqrite EPS server needs to have Microsoft IIS Web server as well as Microsoft. NET Framework 4.0 on your computer system.

Web server	Requirements
IIS	IIS Version 10 on Windows 10
	IIS Version 8.5 on Windows 8.1 and Windows Server 2012 R2
	IIS Version 8.0 on Windows 8 and Windows Server 2012
	IIS Version 7.5 on Windows 7 and Windows Server 2008 R2
	IIS Version 7.0 on Windows Vista and Windows Server 2008
	IIS Version 6.0 on Windows Server 2003
	IIS Version 5.1 on Windows XP SP3

The EPS installer will install required IIS Components.

Java Runtime Environment (JRE) Requirements

Java Runtime Environment (JRE) required to perform installation through Web page and Add Device functionalities are as follows:

OS versions	Requirements	JRE
32-bit	32-bit	JRE 7, JRE 8
64-bit	32-bit	32-bit JRE 7, 32-bit JRE 8
	64-bit	64-bit JRE 7, 64-bit JRE 8

System requirements for Seqrite EPS clients

System requirements for Seqrite Endpoint Security clients are as follows:

Component	Requirements
Processor	1 GHz 32-bit (x86) or 64-bit (x64) for Windows Vista or later
RAM	1 GB
Hard disk space	3200 MB
Web Browser	Internet Explorer 5.5 or later

Seqrite Endpoint Security client can be installed on a computer system with any one of the following operating systems:

- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit / 64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)

- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- Microsoft Windows 2000 SP 4 Professional / Server / Advanced Server

System requirements for Mac OS

Software and hardware requirements for Seqrite EPS clients on Mac OS are as follows:

Component	Requirements
MAC OS	Mac OS OS X, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11
Processor	Intel or compatible
RAM	512 MB
Hard disk space	1200 MB

System requirements for Linux OS

Seqrite
Endpoint Security

Software and hardware requirements for Seqrite EPS clients on Linux OS are as follows:

Component	Linux OS versions	Requirements
Linux OS	32-bit	• BOSS 6 • Fedora 14, 18, 19, 20, 21 • openSUSE 11.4, 12.2, 12.3 • Linux Mint 13, 14, 15, 16, 17.3 • Ubuntu 10.10, 12.04 LTS, 12.04.3 LTS, 13.04, 13.10, 14.04, 14.10, and 15.04 • CentOS 6.3, 6.4, 6.5
	64-bit	• Fedora 14, 18, 19, 20, 21 • openSUSE 11.4, 12.2, 12.2 • Linux Mint 13, 14, 15, 16, 17.3 • Ubuntu 10.10, 11.4, 12.04.2 LTS, 13.04, 13.10, 14.04, 14.10, and 15.04 • CentOS 6.3, 6.4, 6.5
Processor		Intel or compatible
RAM		512 MB
Memory		300 MHz or higher
Hard disk space		1200 MB

Corporate Office

Quick Heal Technologies Limited

Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune - 411014, Maharashtra, India

Email: info@seqrite.com | Website: www.seqrite.com