SEQRITE

Enterprise Security Solutions by Quick Heal

Seqrite
Endpoint Security

Integrated enterprise security and unified endpoint management console

Total 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.

- Reduced security risks with Application Control and Advanced Device Control.
- Prevents data leakage with easily configurable Data Loss Prevention and File Activity Monitor.
- Maintains transparency of endpoints through in-depth Asset Management.
- Combines threat-centric intrusion prevention and other protection technologies.
- Simplified maintenance with flexible Group Redirection, Tuneup and Multiple Update Manager.

Features

ADVANCED DEVICE CONTROL

Controls and configures various device types for Windows and Mac platforms. Separate access policies can be configured for storage devices, mobile phones, cameras, other wireless devices, card readers and many more.

With the help of this feature, your network remains protected against unverified devices. Advaced Device control also allows you to manage the various devices that your employees use. The administrator can also create exception lists for specific devices. Each 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 administrators comprehensive knowledge about the hardware and software configuration of every endpoint. Administrators can garner information such as hardware configuration, system information, updates installation and hardware/software changes pertinent for every system. Notifications are sent to the configured email addresses whenever any alteration to the hardware on any system takes place.

- For instance, if an endpoint updates its RAM a notification is sent. Similarly, notifications are received for new devices, hardware added/removed and hardware changes. This allows administrators to know all there is to know about every endpoint at all times.

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.

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

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

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.

MULTIPLE UPDATE MANAGERS

This feature allows multiple update managers to be deployed across the network. This helps in load balancing and in avoiding network congestion as is usually the case for a single update manager.

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 mode.

Certifications

Product Comparison

Feature	Business	Total
Antivirus	✓	✓
Email Protection	✓	✓
IDS/IPS Protection	✓	✓
Firewall Protection	✓	✓
Phishing Protection	✓	✓
Browsing Protection	✓	✓
SMS Notification	✓	✓
Vulnerability Scan	✓	✓
Asset Management	✓	✓
Spam Protection		✓
Web Filtering		✓
Application Control		✓
Advanced Device Control		✓
Tuneup		✓
File Activity Monitor		✓
Roaming Platform		✓

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

Feature Pack

Get additional Feature Packs for Total Edition at an extra cost.

Feature Pack	Features
DLP	Data Loss Prevention

System Requirements

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

- Microsoft Windows 2000 SP 4 Professional / Server / Advanced Server
- Microsoft Windows XP Professional (32-bit/64-bit)
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials

- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)

Minimum System Requirement for Console System

- 1 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium processor or equivalent
- 1 GB of RAM
- 2200 MB of free disk space
- Internet Explorer 6 or later
- Monitor that supports 1024 x 768 resolution in 256-color mode

Additional Software Required for Console System

Console needs to have Web server services of either Microsoft IIS or Apache Web server on the system. If Microsoft IIS is to be configured as Web server, the version requirements are as follows:

- IIS Version 5.0 on Windows 2000
- IIS Version 5.1 on Windows XP
- IIS Version 6.0 on Windows Server 2003
- IIS Version 7.0 on Windows Vista and Windows Server 2008
- IIS Version 7.5 on Windows 7 and Windows Server 2008 R2

- IIS Version 8.0 on Windows 8 and Windows Server 2012
- IIS Version 8.5 on Windows 8.1 and Windows Server 2012 R2

If Apache is to be configured as Web server, the version requirement is as follows:

- Apache Web Server 2.0 or later

Ensure that the IIS components shown below are configuered. Unavailability of these components may result in inaccesability of the EPS website.

- IIS Management Console
- Default Document
- Static Content
- CGI

Other Essential Configuration on Console System

- Administrator or Domain Administrator access on the console system.
- File and printer sharing for Microsoft Networks installed.
- Transmission Control Protocol/Internet Protocol (TCP/IP) support installed.
- Internet Explorer Version 7, 8, 9, 10, or 11.
- EPS website is also best viewed in Google Chrome version 39,40 or 41 or Mozilla Firefox version 34,35 or 36

Network Deployment Scenarios

- If the network is configured using DHCP, the Endpoint Security server system on which EPS will be installed and the DHCP server system should be configured using a static IP address.
- If EPS is to be installed on a server with two network cards and Seqrite client agents are to be deployed on both the networks, then during installation of EPS the administrator has to configure Domain Name based communication.

Java Runtime Environment (JRE) requirements:

Requirements to perform installation through webpage, notify install, and add device functionality are as follows:

- On 32-bit Windows operating system
  - To perform above operations, JRE 7 or JRE 8 should be installed
- On 64-bit Windows operating system
  - To perform above operations from 32-bit browsers, 32-bit JRE 7 or JRE 8 should be installed
  - To perform above operations from 64-bit browsers, 64-bit JRE 7 or JRE 8 should be installed

Endpoint requirements

Windows workstations supported:

- Microsoft Windows 2000 SP 4 Professional / Server / Advanced Server
- Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit/64-bit)
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Vista Home Basic / Home Premium / Ultimate / Business / Enterprise (32-bit/64-bit)
- Microsoft Windows Server 2008 Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows Server 2008 R2 Web / Standard / Enterprise / Datacenter (64-bit)
- Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)

- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)

Minimum System Requirements for Windows Endpoint

- 1 GB of RAM
- 1800 MB of free disk space
- 1 GHz 32-bit (x86) or 64-bit (x64) processor for Windows Vista, Windows 2008 Server and Windows 7
- For Windows 2000 – Service Pack 4 or later
- Internet Explorer 5.5 or later
- Administrative privilege is required for installation

Supported Mac Endpoints:

- Mac OS X 10.6, 10.7, 10.8, 10.9, and 10.10
- Mac computer with Intel processor

Minimum system requirements for Mac endpoints:

- 512 MB of RAM
- 1200 MB free hard disk space

Supported Linux Endpoints:

32- Bit:

- Fedora 14, 19
- openSUSE 11.4, 12.2, 12.3
- Ubuntu 10.10, 12.04 LTS, 12.04.3 LTS, 13.04, and 13.10

64-Bit:

- Fedora 14, 18, 19
- openSUSE 12.1
- Ubuntu 12.04.2 LTS, 13.04, 13.10
- CentOS 6.3

Minimum system requirements for Linux endpoints:

- 512 MB of RAM or higher
- 1 GB free hard disk space
- Intel-based processor (or compatible), 300 MHz or higher

Headquarters

Quick Heal Technologies Ltd.

Marvel Edge, Office No. 7010 C & D, 7th Floor, Viman Nagar, Pune 411 014

Email: info@seqrite.com, For more details visit: www.seqrite.com