REVE EPS Features
(Ver 3.0.0.32)

REVE™
a n t i v i r u s
Secured Digital Experience

REVE ENDPOINT SECURITY: KEY FEATURES

REVE Endpoint Security provides robust network security solution from highest malware detection to device and application control. Facilitates admin to perform various management tasks remotely without needing any personal visit to the node. Provides a flexible licensing solution, no of protected endpoints can be scaled up as per the requirements anytime with zero license management efforts.

Interactive local console

A user-friendly dashboard helping you to manage your entire network efficiently from a single control panel. Report generation, license management, device management via remote login.

Robust & Smart LAN Server

1 single server can serve 1000+ clients depending on server architecture

Installation for Client

- ✓ Push Installation along with client's IP Address.
- ✓ Client packager (86 KB) easy installation Via Email or any sharing media
- ✓ Individual Installation via client exe.

Installation Protection/ Trusted IP

Unauthorized installation in the same IP address can be prevented by installation blocking from server console. Admin can define a trusted/restricted IP range where EPS clients will be installed/blocked.

Installation Status

- ✓ Admin can check installation status along with IP address.
- ✓ User Rename- Admin can give alias name to user(s)
- ✓ Total License status.

Isolated Client Management

Support clients that are completely disconnected from LAN. Also, have option for
- ✓ Code generation & management
- ✓ Group, policy & report management

Asset Management

Asset information (OS name, No. of Processor, OS install date, Total Memory, Total HDD Size, Available HDD Size, BIOS Serial, Processor info, motherboard/CPU Manufacturer etc.) for every deployed client can be fetched from central console system.

Installed Software list- The installed software details of every deployed client like software name, version, size, installation date, etc., can be get from here.

Graphs Report- graphical representation of RAM, HDD is also available in this section.

Activation Information

- Admin can check individual client license status.
- **User Deletion:** Now admin can remove a user (License count will be decreased after complete uninstallation)

Vulnerability Scan

Vulnerability scan is an automated technology that attempts to identify vulnerabilities in client system. This scan can be performed remotely on client system from central EPS Console.

Group- Policy Management

Grouping policy management for different hierarchy client to create different group to implement various policy to manage

- ✓ Group- Scan / Update
- ✓ Anti- Ransomware
- ✓ Scan Settings
- ✓ Email Security
- ✓ Web control
- ✓ Device control
- ✓ Application control
- ✓ Firewall
- ✓ IPS/IDS
- ✓ File Monitoring
- ✓ Data Loss Prevention
- ✓ Activity Monitoring
- ✓ Uninstallation Protection
- ✓ Data Backup

Scan Settings: Following options under the category.
- ✓ AV Protection settings
- ✓ Exclusion settings
- ✓ Signature update settings
- ✓ Scan action settings
- ✓ Update Manager

Anti- Ransomware: Anti-Ransomware feature will protect your important folder from being attacked by Ransomware. Once you add a folder/path, Ransomware protection will protect that path from any violations, if any process trying to write or encrypt that folder REVE will block automatically. REVE Client Has an option to unblock a process from client UI.

Email- Security control: Following options under the category.
- ✓ Email protections with attachment
- ✓ Blacklist/Whitelist/Subject list options

Web Control (Block/Surveillance)

Websites can be filtered from around 50 defined web site categories & also can add website via URL. The surveillance mode provides a real-time monitoring on website access.

- ✓ Category wise Blocking
- ✓ Whitelist/Blacklist

Device Control

The below device types can be controlled (Allowed/Restricted) by EPS admin console for different group of clients remotely:

- ✓ USB Blocking
- ✓ CD/DVD Blocking
- ✓ Card Reader Blocking
- ✓ Bluetooth Blocking
- ✓ Windows Portable Device
- ✓ Block All Storage Device
- ✓ Read-only option given in Device Control (USB)
- ✓ USB whitelisting option. This can be done either manually or previously used USB (in the LAN network)
- ✓ Vendor wise whitelisting is also available
- ✓ User can also request admin to grant access (if USB is not allowed for the user)
- ✓ Pending task option for admin (To grant USB access for a particular user)

Smart Application Control

Admin can put control over installed applications by configuring app usage restrictions on Client PC's. Even Admin can add more application with pre-defined list as per his choice. Admin can create different policy for different group of people.

Uninstallation Protection

Unauthorized/accidental uninstallation can be prevented by enabling

- ✓ Password protection on REVE Clients
- ✓ Alert to admin via E-mail & Local Console.

Firewall

Protocol based (TCP/UDP/ICMP), Port based, Application based. Option to manage port scan & stealth mode.

- ✓ Port Scan- Keeps the system ports concealed from hacking or intrusion tools.
- ✓ Stealth Mode- This makes the system unreachable in network and keeps protected from any kind of intruding activities.
- ✓ Rules (Protocol, Port, Application and Custom) - Enables to create firewall rules using different parameters to deny/permit the inbound/outbound network traffic/request.

IPS/IDS

REVE EPS is now detecting these 5 mentioned attacks along with Automatic Prevention:

- ✓ DDOS Attack- **Distributed Denial of services** (**DDOS**), in this attack if attacker manage to find open ports and IP of any Sever/pc/website/web application. He can target that IP and port to send multiple request at a single time causing Sever/pc/website/web application to stop working.
- ✓ ICMP Attack- **ICMP** stands for **Internet Control Message Protocol** most of the two-way communication are based on ICMP.
- ✓ RDP Attack- **Remote Desktop** Protocol (**RDP**) is used for remotely connecting to Windows systems. In an **RDP attack**, criminals look for unsecured **RDP** services to exploit and access enterprise networks. It's frighteningly easy to do so because many organizations fail to secure **RDP** services against improper access.
- ✓ SMB Attack- **Server Message Block** (**SMB**) this attack exploits a bug present in SMB version 1.0, SMB is also used for remote code execution which may ransomware and malware uses SMB to spared in a same network. Hence the IDS will be detected if any activity happens through SMB port.
- ✓ Syn-Floyd Attack- **SYN flood** is a form of DOS attack in which an attacker sends a succession of **SYN** requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic

Deep packet inspection - REVE scan content inside any packet.

File Access Monitoring

Admin can monitor files (what user is accessing) based on the extension on local or removal drive. Even Admin can add more extension with pre-defined list as per his choice. Admin can also get details report (Last modify/removed time) of the accessed files.

Data Loss Prevention (DLP)

Admin can block the following channel to prevent data loss. Admin can also get details report on access violation-
- ✓ Print Screen control
- ✓ Printer control
- ✓ Removal Drive data control – restrict user to copy files (extensions based)
- ✓ Clipboard control – monitor sensitive data like email/credit card (country wise)
- ✓ Private IP restriction
- ✓ Public IP restriction
- ✓ Mail client restriction
- ✓ FTP clients restriction
- ✓ Block standard SSH/Telnet services
- ✓ Block web services

Activity Monitoring

Automatic Screenshotter which can take period snapshots of the screen without any user input in the background. Admin can set this policy according to Working Times (working hours & working days) to monitor all the user. Admin also can check Active screen time of User's.

Data Backup

With REVE Antivirus in your PC, you are safe from any kind of data loss. You can keep your data safe which can be restored any time. REVE Antivirus Data backup feature allows you to safeguard your data in your PC and in any internal network location.

Local backup: The local backup option allows you to store your important data in any physical location in your PC. So, if any of your files gets deleted by mistake or becomes corrupt, you can restore them from the PC itself. All file formats are supported such as jpg, pdf, xls, rtf, ppt, zip, csv etc. You also have the flexibility to choose how many versions of any particular file, you want to backup. For example, backup can be created for up to 4 versions of an xls or pptx.

Internal network backup: You can use the internal backup option to store files securely in any internal network location. So, if there is hard disk failure or loss of device, you can restore your files easily from network location.

**You can configure Local Data Backup & Network data backup option from REVE EPS console, so no need to configure from individual client pc.

Admin Control
- ✓ Ultimate control for admin to prevent Personal Information, support for change password & Activation key.
- ✓ Admin can allow Multi user login.
- ✓ Admin can generate activation code according to his Isolated installation.
- ✓ If anyone try to login admin console with wrong password admin will be notified via E-mail.

Data syncing option
In case of server uninstallation, all user's data will be restored from server at REVE EPS Console.

Extra Privileges
- ✓ Support for active directory.
- ✓ Email notification for Policy creation, Group creation, client uninstallation, and Rule violation etc.
- ✓ Daily/ Weekly Reporting by Email according to specific policy features.
- ✓ Graphical representation of report. Advanced Date wise searching option are available.
- ✓ Admin can Export each report in Excel Sheet.
- ✓ Server Console Migration facility.
- ✓ Client Migration facility.
- ** **Web Dashboard**

System Requirement (EPS Server)

Component	Requirements
Processor	1.6 ghz Intel Pentium/Equivalent with HT or higher
Memory	Minimum 4GB Recommended 8GB or more
Storage (Free Space on System Drive)	Minimum 5GB Recommended 10GB or more
Operating System	Windows 7 Onwards
.Net Framework	4.5.2 or higher

Recommend Platforms:
- Windows 7 onwards.
- Windows Server 2008 onwards.

REVE EPS Client Features

Fastest Scan Engine: Combination of traditional signature-based detection with industry-leading behavioral detection that give advanced protection against viruses, spyware, adware, dialers and other malicious application. Multiple type of scan supported: -

- ✓ Scan File
- ✓ Scan Folder
- ✓ Scan system
- ✓ Scan running process
- ✓ Scan Registry
- ✓ Cookies scanning

Anti –Rootkit

Detects and removes any rootkit that is hidden on your computer using advanced rootkit detection technology.

Advanced Real-Time Protection

Advanced real time monitoring system monitor your systems behavior in real time to maintain the system clean and threat free.

Web Security / Anti Phishing

Web Security/ Anti Phishing Constantly monitors online activities, REVE Antivirus intercepts and blocks malicious websites preventing various scams or phishing attempts.

Anti-spyware

- ✓ Able to totally protect from spyware, adware, Trojans, key loggers, P2P Threats, Hackers tools, DDOS Attack Agents in real time.
- ✓ Centralized update/download mechanism to download details of latest Spywares and push the same across all the desktops from console.
- ✓ Auto-quarantine or auto-delete spyware without end-user interaction.

Anti-Malware

Continuously monitors the network and to protect from any type of virus attacks on your server. REVE Endpoint Security protects Windows server from rootkits, worms and other hidden malware through constant scanning.

Patch Management and Vulnerability Scanner

Vulnerability scanner detect and fix operating systems vulnerability. Patch Management help to install the missing patch in operating systems.

Smart Data Restore

A proactive safety measure for ransom ware attacks. Provides the dynamic data backup feature for client PC, backed up data can be restored to the desired location anytime by the permission of IT Admin.

High Performance

It will not slow down your system to get smooth PC experience.

USB Scanner

Scans external storage devices and protects USB drives from auto-run infections.

Email security & Anti-spam

Detects infected E-mail attachments. Anti-Spam engine filter your E-mail from spam and it also protects you from phishing scams.

- ✓ Black list / white list E-mail Address
- ✓ Spam Folder
- ✓ Support for all Outlook versions.

Self-Protection

Protects REVE Antivirus for Windows against malware attempting to block the application or remove it from PC.

PC Tune-up

You can tune-up & optimize your PC performance

1. Start-up manager/optimizer.
2. Disk de-fragmentation tool.
3. Registry cleaner/defragment/Restore.
4. Shortcut cleaner.
5. Browser Cleaner.

6. Duplicate finder
7. File Shredder
8. Settings/Scheduler
9. Auto Cleaning

Rescue Disk: Secure your data in case of system crash.

Password Protected AV Settings
Client is able to create password protection for his AV settings.

System Requirements (Client)

Component	Requirements
Processor	1.6 GHz Intel Pentium/Equivalent with HT or higher
Memory	Minimum 1.5GB Recommended 2GB or more
Storage (Free Space on System Drive)	Minimum 800 MB Recommended 2GB or more
.Net Framework	4.5.2or higher

** Supported Platforms: Windows XP SP3 onwards along with Windows Server

Awards & Certifications

ABOUT REVE ANTIVIRUS

REVE Antivirus is a vertical of REVE Group with its headquarters in Singapore and software Development centers in India and Bangladesh. It has an active presence across 10 countries and currently services customers in more than 80 nations. A Microsoft approved product, REVE Antivirus are now listed in **Gartner** for EPS & also received certification from VB100, a security information portal, testing and certification body and OPSWAT, a San Francisco-based software company.