Safeguard your Organization's Data
with the Most Comprehensive

REVE EndpOint Cloud

REVE
antivirus
Secured Digital Experience

REVE EPS CLOUD: KEY FEATURES

From the highest malware detection to device and application control, REVE Endpoint Security Cloud provides comprehensive network security solutions. It allows the administrator to do numerous management operations without having to physically visit the node. It also offers a flexible licensing approach, allowing the number of protected endpoints to be scaled up as needed at any moment with no additional license management effort.

Interactive Cloud Dashboard

From a single control panel, a user-friendly dashboard allows you to efficiently manage your whole network. Cloud login allows you to view reports, manage licenses, and control devices from anywhere in the world.

Robust & Smart Cloud Server

Clients using Cloud EPS can get the most recent virus signature update from any location with an internet connection.

Installation for Client

✓ Single installer file for any version of Windows.

Installation Protection

It is impossible to install and activate any client without the permission of the admin, as the admin has to generate a license key. As a result, any unauthorized installation of the license can be prevented.

Installation Status

✓ Admin can check installation status along with Name, IP address & MAC.
✓ User Rename- Admin can give alias name to users.
✓ Admin can check Total License status.

Asset Management

The central Cloud console system may retrieve asset information (OS name, number of processors, OS install date, total memory, total HDD size, available HDD size, BIOS Serial, Processor data, motherboard/CPU Manufacturer, and so on) for each deployed client.

Activation Information

• Admin can check individual client license status.
• **User Deletion:** Admin can remove a user (License count will be decreased aftercomplete uninstallation)

Vulnerability Scan

Vulnerability scan is a type of automated technology that looks for flaws in a client's system. This scan can be carried out by the client.

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
- ✓ Cloud Backup

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

Anti- Ransomware: Your essential folder will be protected from Ransomware attacks thanks to the anti-Ransomware feature. Once you add a folder/path to Ransomware Protection, it will be protected from any violations. If any process tries to write or encrypt that folder, REVE will instantly block it. The REVE Client includes a feature that allows you to unblock a process from the client UI.

Email- Security control: Following options under the category.
- ✓ Email protections with attachment
- ✓ Blacklisting/Whitelisting Email
- ✓ Subject Blacklisting option
- ✓ Domain Whitelisting option

Web Control (Block/Surveillance)
Websites can be filtered by one of about 50 predefined categories, and they can also be added by URL. The surveillance mode allows you to monitor website access in real-time.
- ✓ Category wise Blocking
- ✓ Whitelist/Blacklist

Device Control
Admins can control (Allow/Restrict) the following device kinds remotely from the EPS Cloud Dashboard for different groups or individual clients:
- ✓ USB Blocking
- ✓ CD/DVD Blocking
- ✓ Card Reader Blocking
- ✓ Bluetooth Blocking
- ✓ Windows Portable Device
- ✓ Block All Storage Device
- ✓ A read-only option is given in Device Control (USB)

Smart Application Control
On Client PCs, the Admin can exert control over installed applications by defining app usage limitations based on a pre-defined list. Distinct policies can be created by the administrator for different categories of users.

Uninstallation Protection
Unauthorized/accidental uninstallation can be prevented by enabling
- ✓ Password protection on REVE Clients
- ✓ Alert to admin via E-mail & Web Dashboard.

Firewall
Option to regulate port scan and stealth mode based on protocol (TCP/UDP/ICMP), port, and application.
- ✓ Port Scan - Protects system ports from hacking and intrusion tools.
- ✓ Stealth Mode - renders the machine unavailable in the network, keeping it safe from invading actions.
- ✓ Rules (Protocol, Port, Application, and Custom) - Allows you to create firewall rules that refuse or allow inbound/outbound network traffic/requests based on various factors.

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 an attacker manages to find open ports and IP of any Sever/PC/website/web application. He can target that IP and port to send multiple requests 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 is 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 spare in the same network. Hence the IDS will be detected if any activity happens through the 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 removaldrive. 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 detailsreport 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 client's 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 cloud location.

Cloud backup: Cloud backup option allows you to take backup your important data in Cloud location. So, if any of your files gets deleted by mistake or becomes corrupt, Cloud Console Administrator can restore those from the Cloud. If there is hard disk failure or loss of device, you can also restore your files easily from Cloud location. All backup will happen according to extension base & as per allocated space of each systems.

Admin Control
- ✓ Ultimate control for admin to prevent Personal Information, support for change password & Activation key.
- ✓ Admin can allow Multi user login.
- ✓ Only Admin can generate activation code according to installation.

Extra Privileges
- ✓ 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 areavailable.
- ✓ Admin can Export each report in Excel Sheet.
- ✓ Client Migration facility.
- ✓ There is no way to loss Cloud Console user's data.

REVE EPS Cloud Requirement
- ✓ Only Uninterrupted Internet require to access cloud console.
- ✓ By Any browser Cloud console can be accessible.

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.

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

Password Protected AV Settings

Client UI is password protected. This Password Protection is only Maintain by Administrator.

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

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

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.