

## eScan Enterprise EDR (with MDM & Hybrid Network Support)

More and more employees today access corporate data via mobile devices. This has brought in a new set of security risk for organizations who will now have to protect the mobile devices in the network along with the virtual or physical desktops and servers. eScan provides solutions to all these issues with its new product, eScan Enterprise EDR (with MDM & Hybrid Network Support).

eScan Enterprise EDR (with MDM & Hybrid Network Support) is a comprehensive Anti-Virus and Information Security Solution that allows you to manage risk and protect your critical infrastructure efficiently. The new eScan Management Console (EMC) module includes a Secure Web Interface that facilitates dynamic security management of the server, endpoints, and mobile devices in the corporate network. It is an excellent combination of advanced and futuristic technologies that provides protection to Windows, Mac, Linux, iOS and Android based devices and endpoints in the corporate network. eScan Enterprise EDR includes Mobile Device Management (MDM) module which is specifically designed with an aim to facilitate administrator to remotely monitor, secure, and manage all Android-based devices in the network.

### Key Features - eScan Management Console



#### New Secure Web Interface with Summarized Dashboard

The new Secure Web Interface uses SSL technology to encrypt all communications. eScan's summarized dashboard provides administrators the status of the managed endpoints in graphical format like deployment status, protection status and statistics.



#### Asset Management

eScan's Asset Management module provides the entire hardware configuration and list of software installed on endpoints. This helps administrators to keep track of all the hardware and software resources installed on all endpoints connected to the network.



#### Role Based Administration

Role based Administration through EMC enables the administrator to share the configuration and monitor responsibilities of the organization among several administrators.



#### Mobile Device Management

eScan facilitates effective MDM that allows administrators to create different groups for different locations, add devices, move devices from one group to another group, define rules / policies for Anti-Virus, setting Call & SMS Filter, Web Protection, Anti-Theft, Password and Device Oriented policy.



#### Active Directory Synchronization

With this feature, the administrators can synchronize eScan Centralized Console groups with Active Directory containers. New computers and containers discovered in Active Directory are copied into EMC automatically and the notification of the same can be sent to the system administrators.

### Key Features - eScan EDR



#### Event Collector (Security Events) and Co-relation

All Windows security events (unauthorized login attempts, RDP connections, and Policy changes) are monitored for behavioral changes, policy violations, and exceeding granted rights. These events are then forwarded to the server with secure protocols for threat analysis and storage. Besides, all the OS and app logs are collected which also improves real-time visibility, network safety, and time management.



#### Threat Analysis

All event logs are stored at a secured server and analyzed further for threats-based on the malware type and corruption. They are checked against rule-based policies and regulations, then identified and categorized for security threat nature and level.



#### Historical Investigation - RCA

With Windows events and Threat Analysis, a deep RCA is carried out against detected and potential threats to identify its root cause. The RCA helps you identify the loose ends in your network and take appropriate action to mitigate threats before the threat takes over the network.



#### EDR Violation events from endpoints

eScan EDR solution is equipped with advanced technologies that gathers the information from all the endpoints which are categorized as known and unknown zero-day attacks. eScan

### Other Highlights

- ▣ State-of-the-art Anti-Malware with signature & behavior based protection.
- ▣ Unified Console for Windows, Mac, Linux, iOS and Android
- ▣ License Management
- ▣ Import & Export of Settings
- ▣ Update Agent / Task Deployment
- ▣ Outbreak Prevention (Improvised) ■
- ▣ On Demand Scanning for Windows, Mac, and Linux
- ▣ File Reputation Services for Windows and Linux
- ▣ Sophisticated File Blocking and Folder Protection ■
- ▣ Rescue Mode for Windows and Linux
- ▣ Auto Backup and Restore of Critical System files ■
- ▣ Malware URL Filter ■
- ▣ Send Message ■
- ▣ Policy Templates / Auto Grouping / Client Live Updater ■
- ▣ Schedule Scan ■ ▲ ■ ■
- ▣ One-Time Password / Privacy Control ■
- ▣ Inbuilt eScan Remote Support ■
- ▣ 24x7 FREE Online Technical Support through e-mail, Chat and Forums

endpoints automatically detects and send the log & events to eScan EDR solution. Attacks includes credential stealing, malignant JavaScript or VBScript, potentially obfuscated scripts, untrusted or unsigned executable files from removable devices, creation of WMI and PsExec commands, Office and Adobe apps from creating child processes, injecting codes, creating executable content, and Win32 API calls from macros. eScan endpoints also prevents malware from abusing WMI to attain persistence on a device.



#### EDR Violation events from Advanced Ransomware

eScan EDR gather the log & events from endpoints protecting and blocking of executables (.exe, .dll, or .src) and script (.ps, .vbs, .js) files that autorun quickly after opening an email. eScan EDR uses its heuristic PBAE technologies to monitor and block all the apps that are suspected as ransomware through their activity or behavior. Along with this, it also terminates the network session, if any infected system tries to gain access of protected system.



### Key Features - eScan Endpoints (Windows)

#### Data Leak Prevention (DLP) - Attachment Control

eScan empowers enterprises to minimize the risk of data theft with its advanced features like Attachment Control and Device Control. Through Attachment control the admin can block/allow all attachments the user tries to send through specific processes as well as trusted websites that you define. It is a pay and use feature.



### Session Activity Report

EMC monitors and logs the session activity of the managed computers. It will display a report of the endpoint startup / shutdown / logon / logoff / remote session connect / disconnect. With this report the administrators can trace the user logon and logoff activity along with remote sessions that took place on all managed computers.



### eBackup

eScan allows you to take a backup of your files on a scheduled basis, and is stored in an encrypted and compressed file format. It takes backup of all Office documents & many more. The backup will be taken on the drive with the largest free storage available. The backup can also be taken on network drive which is a pay and use feature.



### Print Activity Monitoring

eScan comprises of Print Activity module that efficiently monitors and logs printing tasks done by all the managed endpoints. It also provides a detailed report in PDF, Excel or HTML formats of all printing jobs done by managed endpoints through any printer connected to any computer locally or to the network.



### Proactive Behavioral Analysis Engine (PBAE)

PBAE provides real-time protection for organizations and users against Ransomware attacks. It monitors the activity of all processes and blocks the one whose behavior matches to a Ransomware.



### Terminal Services Protection (TSPM)

TSPM module by eScan not just detects the brute force attempts but also heuristically identifies suspicious IP Addresses/Hosts. It blocks any attempts to access the system.



### Two-Factor Authentication (2FA)

The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your basic system logon. The 2FA feature requires personnel to enter an additional passcode/password after entering the system login password. It is a pay and use feature.



### Remote Monitoring Management (RMM)

Remote monitoring and management (RMM) is a type of remote IT management software used by Managed IT Service Providers (MSPs) to remotely monitor client endpoints, networks, and computers. It is a pay and use feature.



### Advanced Anti-Spam

With its advanced Anti-Spam facility, eScan prevents you from receiving spams. It checks the content of outgoing and incoming mails as well as quarantines advertisement mails. Moreover, eScan scans all the emails in real-time for malicious content using Dual Anti-Virus Engine.



### Data Encryption

Data Encryption lets you protect sensitive and confidential data from unauthorized access and data leak. With this module, the user can create a Vault that stores data in encrypted format.



## Key Features - eScan Endpoints (Hybrid OS)



### Advanced Web Protection

eScan comes with an advanced Web Protection feature that allows administrators to define the list of sites to block or whitelist on endpoints connected to the network where eScan is installed. For Windows endpoints eScan also provides the facility for time-based access restriction.



### Enhanced Two-way Firewall

The two-way Firewall with predefined rule sets will help you in putting up a restriction to incoming and outgoing traffic and hacking. It provides the facility to define the firewall settings as well as define the IP range, permitted applications, trusted MAC addresses and local IP addresses.



### Anti-Theft

eScan helps you in image capture, screen shots, lock down of device, Alerts, scream, Data wipe, SIM watching, and locating your devices. eScan ensures complete protection from any unauthorized access on the event if your device is lost or stolen. It is a pay and use feature on the Windows endpoints.



### Device Control

The Advanced Device feature enables you to, allow or block access to USB devices connected to Windows, Mac and Linux endpoints in the network. On Windows, access can be restricted for Webcam, SD cards, Imaging, Bluetooth and Composite devices. Access to thumb drives can be restricted on Windows, Mac and Linux. Access to CD-ROM can be restricted on Windows and Linux.



### Application Control

eScan's effective Application Control module allows you to block/whitelist and define time restrictions for allowing or blocking execution of applications on Windows endpoints. It helps in accessing only the whitelisted applications, while all other third-party applications are blocked. On Android by default, all downloaded applications are blocked. On iOS devices you can apply restriction policies for various applications such as Siri, Youtube, Safari, iTunes, and more.

## Key Features - Mobile Device Management Android

- Kiosk Mode
- Privacy Advisor / Web Control
- Device Oriented Policy
- Wi-Fi and App specific Network Blocking
- Content Library
- Fencing Locations and more

## iOS

- Device Restriction Policy
- Web Clip and Email Protection
- Wi-Fi Protection
- Content Library and more

## Minimum System Requirements

### Windows

#### (Windows Server and Workstations)

#### Platforms Supported

Microsoft® Windows® 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1 (For 32-bit and 64-bit edition)

#### For Server

- CPU - 3.0 GHz Intel™ Core™ Duo processor or equivalent.
- Memory - 4 GB and above
- Disk Space (Free) - 8 GB and above

#### For Endpoints (Windows)

- CPU - 2.0 GHz recommended Intel Pentium or equivalent
- Memory - 1 GB and above
- Disk Space (Free) - 1 GB and above

#### eScan Console can be accessed by using below browsers:

- Google Chrome & all chromium-based browsers
- Firefox 14 and above
- Internet Explorer 9 and above

### Linux

#### (Linux Endpoints)

#### Platforms Supported

RHEL 4 and above ( 32 and 64 bit )  
CentOS 5.10 and above ( 32 and 64 bit )  
SLES 10 SP3 and above ( 32 and 64 bit )  
Debian 4.0 and above ( 32 and 64 bit )  
openSuSe 10.1 and above ( 32 and 64 bit )  
Fedora 5.0 and above ( 32 and 64 bit )  
Ubuntu 6.06 and above ( 32 and 64 bit )  
Mint 12 and above (32 and 64 bit)

#### Hardware Requirements (Endpoints)

- CPU - Intel® Pentium or compatible or equivalent.
- Memory - 1 GB and above
- Disk Space - 1 GB free hard drive space for installation of the application and storage of temporary files

### Mac

#### (Mac Endpoints)

#### Platforms Supported

OS X Snow Leopard ( 10.6 or later )  
OS X Lion ( 10.7 or later )  
OS X Mountain Lion ( 10.8 or later )  
OS X Mavericks ( 10.9 or later )  
OS X Yosemite ( 10.10 or later )  
OS X El Capitan ( 10.11 or later )  
macOS Sierra ( 10.12 or later )  
macOS High Sierra ( 10.13 or later )  
macOS Mojave ( 10.14 or later )  
macOS Catalina ( 10.15 or later )

#### Hardware Requirements (Endpoints)

- CPU - Intel based Macintosh
- Memory - 1 GB and above
- Disk Space (Free) - 1 GB and above

### Android

#### (Android Endpoints)

#### Platforms Supported

- Operating System: Android 4.4 and above
- Others: Internet Connection

#### iPhone & iPad

#### (iPhone & iPad Endpoints) Platforms Supported

Compatible OS: iOS 10.3 or later  
Device Space: 40-50 MB space  
Memory: 20-50 MB (varies by device)

Other:  
3G/4G (LTE) or Wi-Fi Internet connection required for download.