eScan™
Enterprise Security

eScan Enterprise EDR (Hybrid Network & Mobile Device Support)

eScan Endpoint Detection and Response (EDR) is a comprehensive, integrated, and layered endpoint protection solution that delivers real-time visibility, analysis, protection, and remediation for endpoints. This helps to gain deep insights and alerts admin about the malicious activity that allows fast investigation, and restricts the attacks on endpoints as soon as detected. It supports automated and manual actions to restrict the potential threats on the endpoint. It proactively reduces the attack, prevents malware infection, detects and defuses potential threats in real-time.

eScan EDR 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. It allows you to scan your mobile devices from same management platform.

eScan
Enterprise EDR
(Hybrid Network & Mobile Device Support)

eScan™
Enterprise Security

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.

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.

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 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.

eScan
Enterprise EDR
(Hybrid Network & Mobile Device Support)

eScan™
Enterprise Security

Why eScan Enterprise EDR ?

Uniform Management

- **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, Top 10 summary, Asset Changes, EDR Dashboard, and Live Status.

- **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 as well as software resources installed on all the endpoints connected to the network.

Enhanced Endpoint Protection

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

With the additional capabilities like Attachment Control and Device Control, eScan protects organizations from the risk associated with unauthorized transfer of sensitive content. Attachment Control allows to control the users' attempt in the distribution of sensitive information via specific processes as well as trusted websites that you define. It is a pay and use feature.

- **Two-Factor Authentication (2FA)**

eScan provides an extra layer of protection to the log-in process that authenticates and prevents any hackers from accessing the computer and personal data. This offers an additional step of security as cyberthieves require more than a username and password for authentication.

Powered By Futuristic Technology

- **Proactive Behavioral Analysis Engine (PBAE)**

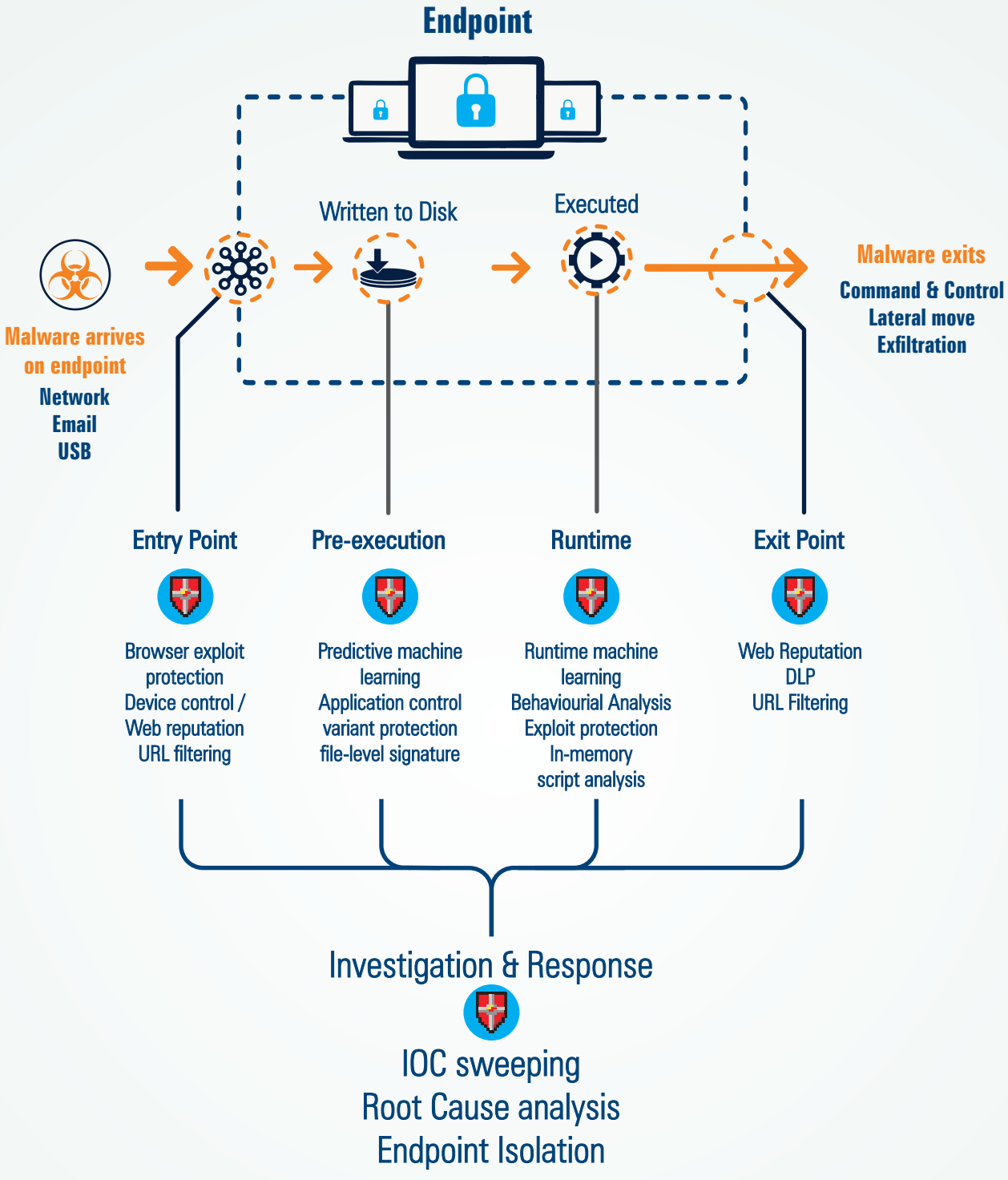
PBAE provides real-time protection for organizations and users against Ransomware attacks. It monitors the activity of all processes and blocks the one whose behavior matches to Ransomware.

- **Terminal Services Protection Module (TSPM)**

eScan is equipped with improvised TSPM that not only detects and blocks the brute force and suspicious IP addresses but also allows to whitelist the IP addresses for secured RDP connections.

eScan
Enterprise EDR
(Hybrid Network & Mobile Device Support)

eScan™
Enterprise Security



eScan
Enterprise EDR
(Hybrid Network & Mobile Device Support)

eScan™
Enterprise Security

Key Features: eScan (Management Console)

EDR Dashboard

eScan provides the summarized dashboard of the incidents that allows admins to gain deeper insights and taken quicker actions as and when detected. It gives overview of incidents such as eScan, Windows, Endpoints, and Network in graphical as well as in detailed form.

Role Based Administration

Role based Administration through eScan Management Console allows administrators to create level-based admin groups with a set of predefined privileges for more secured access.

Active Directory Synchronization

Administrators can synchronize eScan Centralized Console groups with Active Directory containers. All the new computers and containers found in Active Directory are automatically copied into eScan Centralized Console and the system admin will be notified.

Client Live Updater

With the help of eScan's Client Live Updater, events related to eScan and security status of all endpoints are captured, recorded, and can be monitored in real-time. It can also export events in excel file.

Enhanced Setting

eScan provides various advanced setting such as Roaming Clients, 2FA for Terminal users, Password Policy Settings, creating report with customized logo, Auto-isolation Setting, Advanced security setting, and more.

Policy Templates

Policy template makes policy deployment simple; it allows the admin to create policies for security and compliance and enforce these policies on designated managed groups.

Advance Security

eScan has included Advanced Security policy that alerts admin about the malicious activities that helps organizations to identify and stop breaches in real-time automatically and efficiently, without overwhelming the security team with false alarms or affecting business operations.

eScan
Enterprise EDR
(Hybrid Network & Mobile Device Support)

eScan™ Enterprise Security

Key Features: eScan Endpoints (Windows)

eBackup

eScan enables admin to take a backup of all the files manually or automatically (scheduled basis) and stored it in an encrypted and compressed format. It also allows you to take backup on local drive, network drive, or on cloud (pay and use feature). eScan allows admin to import/export the server data that can be restored in case of any system failure or disaster.

Session Activity Report

eScan Management Console 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. Admins can use this report to track users' logon and logoff activities, as well as remote sessions, on all managed computers.

Remote Monitoring Management*

Remote monitoring and management (RMM) is a type of remote IT management software used by Managed IT Service Providers (MSPs) allow admins to remotely track issues and monitor IT assets. It helps organizations to gain insights into performance, health, and status of their endpoints. It is a pay and use feature.

Windows Patch Management

eScan's Patch Management Module auto-updates Windows OS security patch from Cloud or from EMC Console, on PC's those are part of DMZ/Air-Gapped Networks. The module also reports patching availability for Critical Apps like Adobe, Java, etc.

Offline updates

eScan addresses the need for offline updates of isolated networks by allowing the admin to use an internet-connected computer to pre-download all updates that are required by computers on the air gap network so that he/she can then copy the update files to the isolated network.

Update Agent

The administrators can add computers as Update Agents. As a result, the traffic between the eScan Corporate Server and the client is reduced. The signature updates and policies will be downloaded from the eScan EDR Server and distributed to the other managed computers in the group via Update Agent. It save all bandwidth and improve the performance.

eScan
Enterprise EDR
(Hybrid Network & Mobile Device Support)

eScan™
Enterprise Security

Key Features: eScan Endpoints (Windows)

Print Activity Monitoring

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

Privacy Control

Privacy control allows scheduling the auto erase of your cache, ActiveX, cookies, plugins, and history. It also helps to permanently delete files and folders without the fear of them being recovered by third-party applications, thus preventing data exploitation.

Advanced Anti-Spam

eScan provides protection against spam mails with its powerful Anti-Spam Technology. It checks the content of outgoing and incoming emails and quarantines commercial mails. Furthermore, eScan uses powerful, heuristic driven Dual Anti-Virus engines to scan all emails for virus, worms, Trojans, spyware, adware, and hidden malicious content on real-time basis.

Key Features: eScan Endpoints (Hybrid OS)

Device Control

eScan is equipped with Advanced Device Control feature that allows/blocks the access to USB devices on endpoints in the network. Access to Webcam, SD cards, Imaging, Bluetooth and Composite devices are restricted on Windows endpoints. Access to thumb drives can be restricted on Windows, Mac, and Linux. Access to CD-ROM can be restricted on Windows and Linux.

Schedule Scanning

eScan offers you an option for scheduled scanning, which will run seamlessly in the background without interrupting your current working environment. It performs scheduled scans for selected files / folders or the entire system for the scheduled period, thus providing you the best protection against cyber threats.

eScan
Enterprise EDR
(Hybrid Network & Mobile Device Support)

eScan™
Enterprise Security

Key Features: eScan Endpoints (Hybrid OS)

Advanced Web Protection

eScan is equipped with Advanced Web Protection that protects from accessing dangerous, phishing and fraudulent pages. It allows admin to define the list of sites to restrict or whitelist on endpoints connected to the network. As a result, when an URL points to a known phishing or fraudulent website, or to malicious content such as spyware or viruses, the webpage is blocked and an alert is displayed. eScan also provides time-based access restrictions in the Windows endpoints.

Enhanced Two-way Firewall

eScan Two-way Firewall filters all the incoming and outgoing network requests, which enables you to monitor every inbound and outbound connection that is being established. This locks out hackers from connecting to the system and defends the connection of undesired apps to the internet. 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 for the Windows endpoints.

One-Time Password

The administrator can use One-Time Password option to enable or disable any eScan module on any endpoint for a desired time. This allows admin to assign privileges to certain users without violating a networks' security policy.

Application Control

eScan's Application Control helps you outsmart cybercriminals and keeps your business secure and productive. It prevents zero-day and ATP attacks by blocking the execution of unauthorized applications. Using whitelisting, admins can prevents attacks from unknown malware by allowing only known whitelisted applications. 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.

eScan
Enterprise EDR
(Hybrid Network & Mobile Device Support)

eScan™
Enterprise Security

Other Highlights

- State-of-the-art Anti-Malware with signature & behavior based protection.
- Unified Console for Windows, Mac, Linux, iOS and Android
- On Demand Scanning for Windows, Mac, and Linux
- Sophisticated File Blocking and Folder Protection
- Auto Back-up and Restore of Critical System files
- Inbuilt eScan Remote Support
- Outbreak Prevention (Improvised)
- Rescue Mode for Windows and Linux
- License Management
- Import & Export of Settings
- Task Deployment
- Auto Grouping
- Malware URL Filter
- Send Message
- Forensic Report
- Roaming Client
- 24x7 FREE Online Technical Support through e-mail, Chat and Forums

eScan™

Enterprise Security

An ISO 27001 Certified Company **Toll Free No.: 1800 267 2900** **www.escanav.com**

MicroWorld Software Services Pvt. Ltd.
CIN No.: U72200MH2000PTC127055
Tel.: +91 22 6772 2900
email: sales@escanav.com

Awards

Partnerships

Comprehensive Protection for
SOHO • BUSINESS • CORPORATE • ENTERPRISE