eScan Enterprise EDR - Cloud

eScan Enterprise EDR - Cloud is SaaS platform based Premier cybersecurity solution designed for corporate networks. eScan EDR (Endpoint Detection and Response) provides comprehensive, integrated, and layered endpoint protection that delivers real-time visibility, analysis, protection, and remediation for connected computers in a network system. This helps to gain deep insights and alerts the 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 futuristic technologies that provides protection to Windows, Mac, and Linux based endpoints in the corporate network.

eScan
Enterprise EDR - Cloud

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, and EDR Dashboard.

• Asset Management

eScan's Asset Management module helps admin to keep track of hardware information and a list of software installed on the endpoints. Besides, it allows to view the hardware changes that have been made to the configuration of the systems in the network. It also allows to export the detailed report of the same to have deeper knowledge.

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.

• Non- Intrusive Learning Pattern (NILP)

eScan uses Non- Intrusive Learning Pattern (NILP), a revolutionary technology that uses Bayesian Filtering and works on the principles of Artificial Intelligence (AI) to analyze each email and prevents spam and phishing emails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each email and categorize it as spam or ham based on the behavioral pattern of the user.

• MicroWorld Winsock Layer (MWL)

eScan's "MicroWorld-WinSock Layer" (MWL) is a revolutionary concept in scanning Internet traffic on a real-time basis. It has changed the way the world deals with Content Security threats. Unlike the other products and technologies, MWL tackles a threat before it reaches your applications. MWL is technically placed above the WinSock layer and acts as a "Transparent Gatekeeper" on the WinSock layer of the operating system.

eScan
Enterprise EDR - Cloud

eScan™ Enterprise Security

Key Features - eScan Management Console

• Exclusive 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.

• Excluded Clients

This feature will allow administrator to restrict the client endpoints from unmanaged computers being auto added in any group(s). The admin needs to add the computers using host name, host name with wildcard, IP address, or IP range in the list. Now, the listed computers will not be auto added in the managed group(s).

• Enhanced Settings

eScan provides various advanced setting such as SIEM, creating report with customized logo, Advance security policy, and many 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.

• 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.

eScan
Enterprise EDR - Cloud

eScan™
Enterprise Security

Key Features - eScan EDR

• 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.

• 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.

• 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.

• 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 - Cloud

eScan™ Enterprise Security

Key Features: eScan Endpoints (Windows)

• 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.

• 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.

• 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 eScan EDR Server and distributed to the other managed computers in the group via Update Agent. It save all bandwidth and improve the performance.

• 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.

eScan
Enterprise EDR - Cloud

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.

• Schedule Scan

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.

• 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.

• Reverse Shell

eScan's Reverse Shell feature for Linux based endpoints, restricts reverse shell attack from remote machine. Thus preventing attackers from exploiting a remote command execution vulnerability using a reverse shell session.

• File Integrity Monitor

eScan's File Integrity Monitoring validates the integrity of the files and folders value between the current and the original file state to detect potential compromises for Linux based endpoints.

• 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.

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