eScan Vision Core XDR

eScan Vision Core XDR (eXtended Detection and Response) is a broader and layered endpoint security solution that delivers real-time visibility, analysis, protection, and remediation for endpoints. This provides deeper insights and alerts the admin about malicious activity, which facilitates quicker investigation and restricts the attacks on endpoints as soon as detected.

The Vision Core XDR consists of the latest modules like Phishing simulation and IP Radar. Additionally, a MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is included to give your network an expanded cybersecurity coverage. As an enterprise-grade security solution, it supports automated and manual actions to restrict the potential threats on the endpoint. It proactively reduces the attack, prevents malware infection, and neutralizes potential threats by detecting them in real-time. eScan Vision Core XDR is designed using in-demand and futuristic technologies available for Windows, Mac, and Linux based endpoints across the enterprise.

Why eScan Vision Core XDR?

Uniform Management

- **Web-based Console 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, Live Status, and IP Radar.

- **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.

Extended Endpoint Protection

- **Data Leak Prevention (DLP)**

  With the additional capabilities like Attachment control, Content control, Sensitive file/folder protection, File activity monitoring, Workspace apps, and several other features, eScan protects organizations from the risk associated with unauthorized transfer of sensitive content. It is an Add-on feature.
  *This feature requires additional license.

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

  eScan provides an extra layer of protection to the log-in process that authenticates and prevents any criminals from accessing the computer and personal data. This offers an additional step of security as cyber thieves require more than a username and password for authentication. It is an Add-on feature.
  *This feature requires additional license.

Powered By Futuristic Technologies

- **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-Learning Intrusive 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.

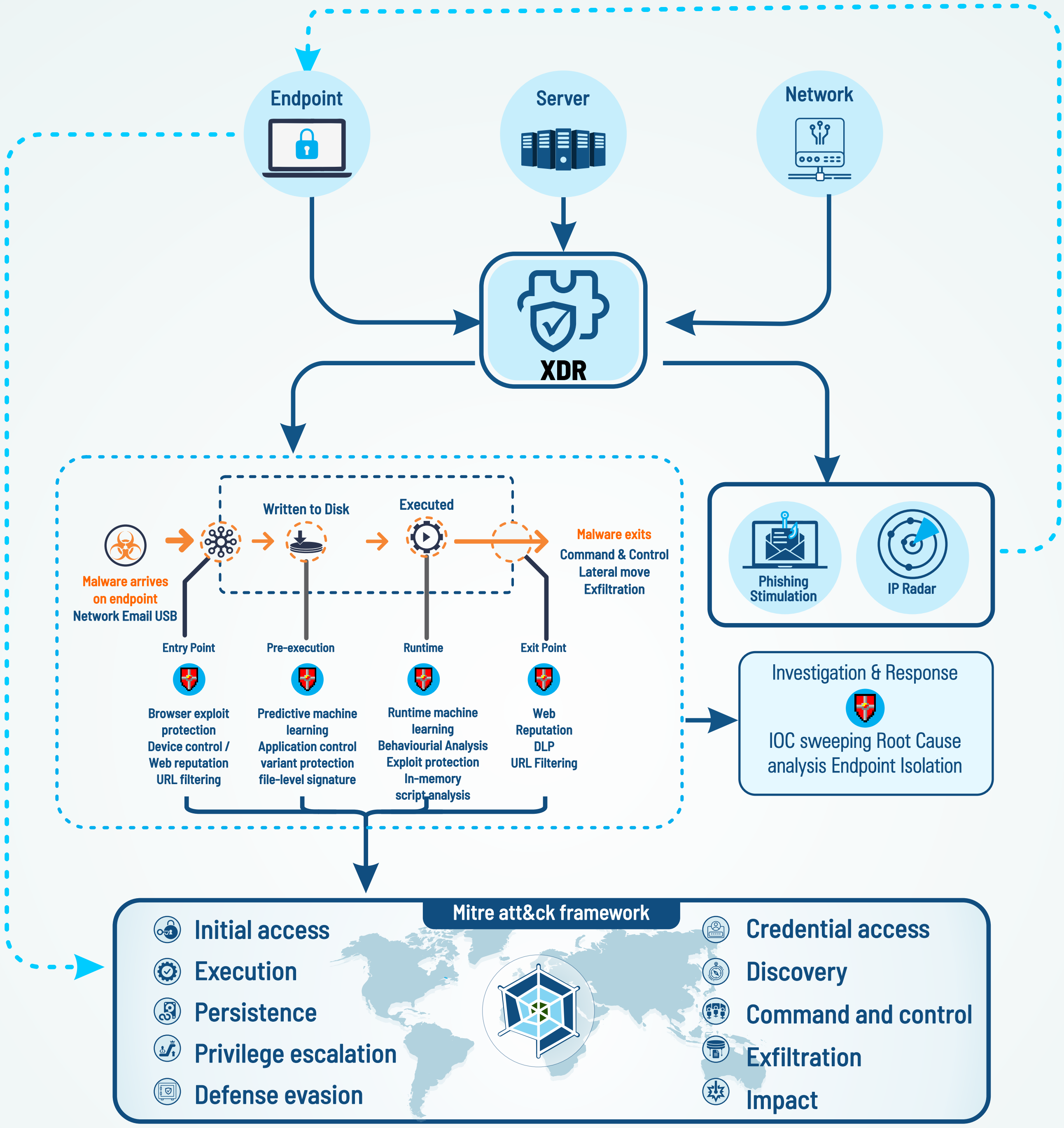
eScan
Vision Core XDR

eScan™
Enterprise Security

Powered By Futuristic Technologies

- **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.



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.

Anti-Theft

eScan helps you in locking down the device, alerts, scream, data wipe, and locating the devices. eScan ensures complete protection from any unauthorized access on the event if your device is lost or stolen. It is an Add-on feature for the Windows endpoints.
*This feature requires additional license.

Auto Grouping

This feature allows admin to automatically add clients to appropriate subgroups. Here, admins will need to create groups and then add client criteria based on host / hostname with wildcard / IP address / IP range.

Enhanced Setting

eScan provides various advanced setting such as roaming clients, outbreak prevention, SIEM, creating report with customized logo, policy criteria templates, and many more.

ADS (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 eScan Centralized Console automatically and the notification of the same can be sent to the system administrators.

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).

Outbreak Prevention

If the virus count exceeds the limits set by administrator, an outbreak email notification will be sent to the user-specified recipient. This will simultaneously trigger an Auto Isolation of infected endpoints in order to restrict the infection in a network.

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.

Key Features: eScan (Management Console)

Phishing Simulation

eScan's new functionality called Phishing Simulation enables organization's threat intelligence team to assess employees' understanding of email phishing threats widely used by attackers. In simple terms, phishing simulation is an internal activity where a mock phishing email is sent to employees to assess whether they click on embedded links or ignore the email. These phishing mails are created by mimicking the actual phishing emails. If the employees respond to the mail by clicking the email links, the action gets stored for further analysis of conducting Phishing awareness program.

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.

IP Radar

eScan added IP Radar in its web console dashboard which is a global map where you can view all the active and established IP connections initiated and connected to eScan server. This feature allows you to trace all the connections that are currently running via eScan server. In simple terms, when IP communication is initiated between XDR sensor and other resources globally, it will be marked on the map with colored lines depending on the type of connection. Also, you can easily choose domestic, foreign, or all the connections for specific view on the map.

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.

Key Features: eScan Vision Core XDR

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.

EDR Violation events from endpoints

eScan Vision Core XDR 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 the 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 Vision Core XDR gather the log & events from endpoints protecting and blocking of executables (.exe, .dll, or .src) and script (.ps, .vbs, .js) files that auto-run quickly after opening an email. It 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.

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.

MITRE ATT&CK Framework

eScan has included MITRE ATT&CK framework to analyze every threat incident detected by eScan XDR. It displays the details of the TTPs (tactics, techniques, and procedures) involved in the attack. The framework shows information related to the TTPs used by the attackers to break into the systems. Organization's threat intelligence team can use this framework to detect adversarial behavior and to map observed activity to specific ATT&CK techniques to understand what stage of attack they faced. This information of TTPs can also be used to share intelligence on emerging threats, helping organizations stay up-to-date with evolving attack methods.

Key Features: eScan Endpoints (Windows)

eBackup & Restore

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 (Add-on feature). eScan allows admin to import/export the server data that can be restored in case of any system failure or disaster.

*This feature requires additional license for allowing the usage of cloud storages.

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.

Patch Management and Patch Reports

eScan looks up the OS information and provides critical security patches along with updates automatically. The eScan server downloads the patches for different versions of Windows OS and distributes the same to the various endpoints. The Patch Report displays the number of Windows security patches installed and not installed on Managed Computers. This will help an admin to identify the number of vulnerable systems in the network and install the critical patches quickly. It is also an Add-on feature.

*The Patch Management feature requires additional license.

Remote Monitoring & Management (RMM)

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 an Add-on feature.

*This feature requires additional license.

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.

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.

Key Features: eScan Endpoints (Windows)

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.

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.

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

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.

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 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.

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.

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.

Enhanced Firewall

eScan 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.

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.

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.

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

Microsoft Partner

Intel Software Partner

Comprehensive Protection for
SOHO • BUSINESS • CORPORATE • ENTERPRISE