eScan Endpoint Detection & Response (EDR) Solution

An ISO 27001 Certified Company

www.escanav.com

Table of Contents

Technologies ______ **2**

Proactive Behavioral Analysis Engine (PBAE) Technology **2**

Host Intrusion Prevention System (HIPS) **2**

Non-Intrusive Learning Pattern (NILP) Technology **3**

Domain & IP Reputation Check (DIRC) Technology **3**

Adaptive Security Architecture ______ **4**

Critical Capabilities ______ **6**

Infrastructure **6**

Architecture **6**

Detection **7**

Investigation **7**

Prevention and Remediation **8**

eScan's Endpoint Detection and Response (EDR) Solution offers detection mechanisms with combinations of behavioral indicators that are able to detect and block attackers' tools, techniques and procedures. It is capable of alleviating fileless malicious activities that use memory exploits and take advantage of Windows utilities such as MSTSC, CMD, and PowerShell.

Technologies

Proactive Behavioral Analysis Engine (PBAE) Technology

eScan's R&D team has developed an algorithm based on the behavior of Ransomware program that protects the IT assets of an organization. The Proactive Behavioral Analysis Engine (PBAE) is a breakthrough technology that mollifies ransomware attacks on all systems protected with eScan Security Suite.

PBAE monitors the activity of all processes on endpoints and when it encounters any behavior that matches to ransomware, a red flag is raised and the process is blocked. PBAE will invalidate the network session, if an infected system tries to access or modify the files of the network share of a protected system.

PBAE is successfully blocking ransomware attacks such as Locky, Zepto, Crysis, and many more. Moreover, by analyzing the events from our Cloud (ESN) we are successfully detecting and mitigating thousands of Ransomware attacks since the rollout of PBAE.

Host Intrusion Prevention System (HIPS)

eScan's Host Intrusion Prevention System (HIPS) technology comes with an array of Intrusion Detection and Intrusion Prevention capabilities. This technology helps in detecting when a rootkit, keylogger, spyware, or Trojan is installed on the system. HIPS technology not only warns the user about any intrusion, but, also blocks it.

HIPS monitors and verifies the behavior, state, and the stored data on a computer. It maintains a database of system objects, which contains information about the attributes of each object. Here are the benefits of the HIPS technology:

- It helps you block behavior-based attacks by malware or attackers on a real-time basis.
- It helps eliminate zero-day attacks.
- It provides protection against buffer-overflows.
- It provides protection from attacks that bypass the security provided by firewall and content security programs.
- It protects OS files and registry keys from modification by malware.
- It prevents unauthorized code from executing on the computer.

When eScan detects a potential threat, HIPS alerts the user, blocks the suspicious activities based on user’s input, and stores the report of the activity in a log file.

Non-Intrusive Learning Pattern (NILP) Technology

eScan's Non-Intrusive Learning Pattern (NILP) technology uses Bayesian Filtering and works on the principles of Artificial Intelligence (AI). It has self-learning capabilities and uses an adaptive mechanism to categorize emails-based on the behavioral pattern of the user.

NILP updates itself by using regular research feeds from MicroWorld servers. Whenever a new email arrives, NILP analyzes it based on the collected information and then classifies it as ham or spam.

NILP also maintains a database containing the DNA imprints of millions of spam emails, which it updates continuously. It uses the existing DNA imprints in the database to reverse its learning and determine whether the email is ham or spam. In this way, the NILP technology protects the user’s inbox from spam and phishing emails.

Domain & IP Reputation Check (DIRC) Technology

eScan's Domain & IP Reputation Check (DIRC) technology verifies the credibility of web domains by tracking suspicious activities on the web pages. ISPs usually follow authentication standards like Sender Policy Framework (SPF), Sender ID, Domain Keys, and Domain Keys Identified Mail (DKIM).

DIRC verifies the integrity of the IP addresses using following criteria:

- By comparing them with a list of known email senders (Real-time Blacklist Servers [RBL servers] and Auto-Spam Whitelist).
- By using Dynamic service that assesses the reputation of email senders on real-time basis.

Adaptive Security Architecture

eScan EDR solution provides scalable data management, analytics capability and data mining (displaying summary of Top 10 threats detected) which gives you detailed understanding of the prevailing threat landscape in your organization. eScan EDR is a feature of eScan Endpoint Protection Platform (EPP) solutions to enhance monitoring and Critical Incidence Response.

eScan EDR solution identifies, responds to threats & provides defense in real-time. eScan integrates the events with SIEM and feeds them to Security Operation Center (SOC) to provide advance workflow capabilities and scalable data management.

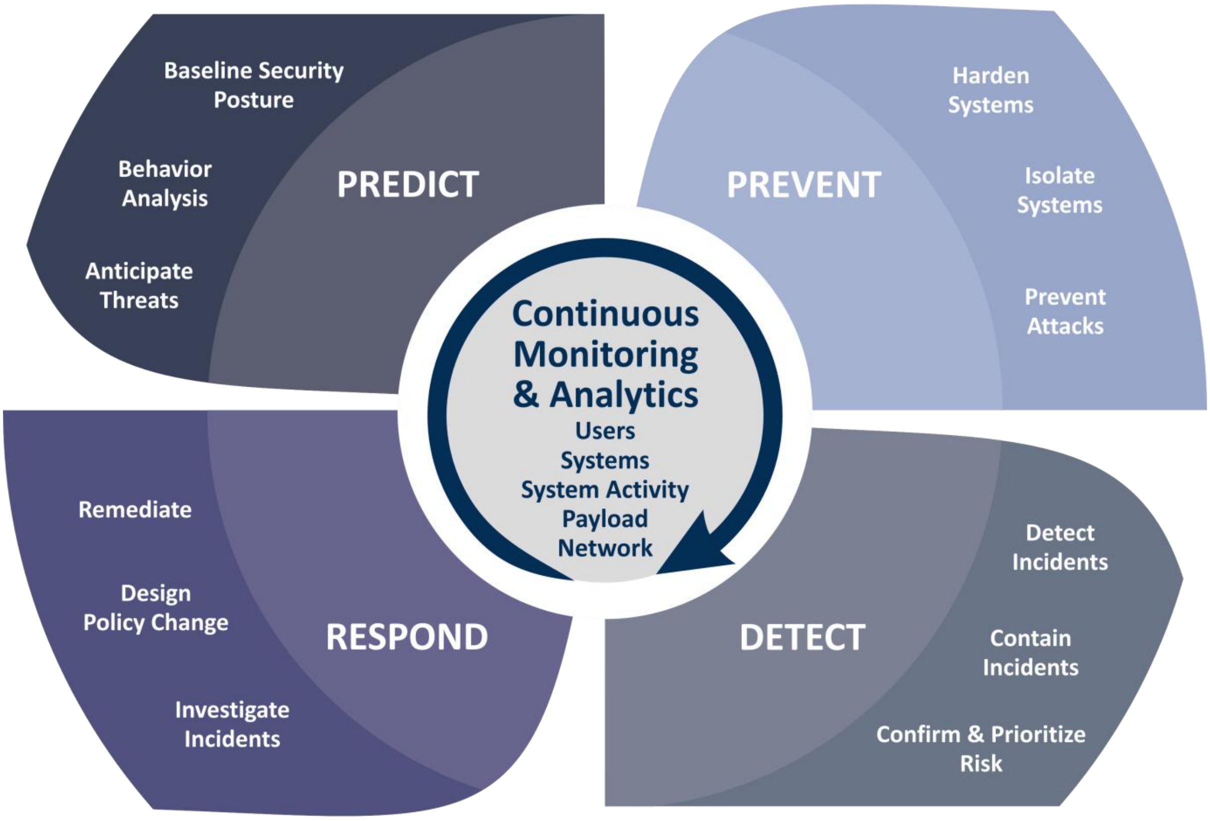

Figure 1: Adaptive Security Architecture

eScan's EDR solution provides the following primary features:

- **Detect security incidents**: Normally, security incidents are self-detected via monitoring of endpoint and application behavior violations, or by validating internally or externally discovered Indicator of Compromises (IOCs). eScan EDR solution will prioritize the detected security incidents, for the security analyst, based on confidence, severity, and risk, in order to prioritize the response activities. Incidents will be shown in SIEM module of either a third-party or eScan Suite.
- **Contain the incident at the endpoint**: eScan ensures that the network traffic or process execution can be remotely controlled, while quarantining the system from rest of the Enterprise network.
- **Investigate security incidents**: The investigate feature consists of historical timeline of all primary endpoint events across all monitored endpoints to determine both the technical changes and business effects.
  Technical changes: File, Registry, Network, Driver, and Execution Activities.
  Business effects: Possible loss of customer data, Transaction fraud, and so on.

- **Remediate endpoints to a pre-infection state**: eScan suite will remove malicious files, rollback and repair other changes. eScan EDR solution creates remediation instructions for other groups to implement with its own toolsets.

Along with all the primary capabilities, eScan EDR also provides the following new innovative and emerging capabilities:

- eScan provides File & Folder access, Network execution, and USB block execution features that blocks execution of threats instead of reporting them.
- eScan provides advanced threat hunting dashboard and automation for enhanced SOCs.
- eScan not only supports Windows-based endpoints but also supports Mac, Linux, iOS and Android OS, which includes advanced event collection capabilities.
- eScan's R&D team has come up with of advanced technologies based on artificial intelligence and machine learning for detection of files.
- eScan provides continuous update for improvement of solutions for both on-premises and cloud.
- eScan's Support and Level 3 Engineers provide Root Cause Analysis (RCA) with recommended action plans and proactive configuration and assessments of security to reduce the attack surface and therefore the infection rate.
- eScan provides risk-based prioritization (Top 10 Summary of threats) on dashboard so that SOC heads can focus on them and remediate them.
- eScan Support team provide scalability and advanced performance to reduce the impact on network and endpoints, and to scale the back-end database.

Critical Capabilities

Infrastructure

eScan solution consists of endpoint agent data collector with a centralized data repository and a management server (either cloud-based or on-premises). As mentioned earlier, eScan EDR solution supports various platforms such as Windows, Linux, Mac, and Android. The detection capabilities of threats vary based on the platform used. The number of endpoints supported by a single management server ranges from 10,000 to 40,000.

Architecture

eScan EDR solution mainly focuses on monitoring and visibility of a wide range of endpoint behaviors and state changes. This is significant where data is stored (distributed or centrally) and when stored centrally, whether it is stored on-premises or on cloud.

On the endpoint themselves, distributed storage of endpoint logs makes it easier to scale. However, in a global organization, a large number of endpoints will create a load that will slow down or not respond to the queries at given time. Centralizing endpoint log data storage is more responsive and allows for more intensive and continuous data mining, but also requires a large data repository to be created.

eScan's cloud instance data storage addresses deployment and scalability problems and also allows EDR to provide cross-company event correlation. eScan's cloud-based storage of EDR data, however, introduces data privacy and potential regulatory issues as data is moved off-premises.

Detection

The most critical feature of eScan EDR solution is the ability to detect advanced hidden threats, without the use of externally fed IOCs. eScan uses funnel detection method that switches from low-cost, but highly deterministic technique, to less deterministic techniques to detect unknown attacks. eScan EDR provides layered security with artificial intelligence, machine learning, and sandbox. It also inspects the portable executable files which includes Java, PowerShell, Office documents, and Perl. This is achieved in various ways that are as follows:

- **Signatures**: eScan scans the files based on signature database which includes both good and bad files. This is low-overhead detection method.
- **Algorithms**: eScan uses machine learning detection methods that are accurate at detecting variants of known bad files.
- **Emulated**: eScan EDR solution searches for partial matches to know the bad code snippets to inspect the file code in real-time.
- **Sandbox**: eScan sandbox technique detects the files using behavior detection methods that are executed in virtual environment.

Investigation

eScan EDR solution helps security analyst to investigate suspicious events through the available forensic information (log & event files), which helps to determine both technical and business-level of impacts. eScan records all the changes, both malicious and non-malicious, that allows the security team to easily search and pivot.

Following features are provided by the eScan EDR solution:

- Prioritize the risk according to the severity of the incident depending upon change in the configuration of the assets. It not only alerts the users when there is change in the configuration but also when changes are observed in physical security such as low disk space, and more.
- eScan EDR generates DEBUG folder which includes the detailed information about the particular system which helps to fetch the information about the suspect files or memory and disk dumps.
- As mentioned earlier, eScan provides real-time forensic information of endpoints state and artifacts.
- eScan EDR solution provides sandbox integration along with cloud and on-premises support.

eScan provides alert management that allows easy assignment, transition, annotation, and resolution of incident.

Prevention and Remediation

eScan provides actions that can be taken from the administration console to block suspicious incidents while being investigated. The critical action taken by eScan is to quarantine a suspected malicious file and to isolate the suspected endpoints from rest of the network while investigation is going on. eScan also kills or blocks the process or files right at the initial stage.

eScan EDR solution has detailed event history information so that one can roll back the recorded malicious activity. eScan EDR solution provides simple application control that blocks any further execution of the file until a signature is obtained.