SOLUTION OVERVIEW

ENTERPRISE INSPECTOR

Uncover the unknown in your network with this EDR solution from the cybersecurity insiders

CYBERSECURITY
EXPERTS ON YOUR SIDE

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ESET Enterprise Inspector is a sophisticated Endpoint Detection & Response tool for identification of anomalous behavior and breaches, risk assessment, incident response, investigations and remediation.
It monitors and evaluates all the activities happening in the network (for example, user, file, process, registry, memory and network events) in real time and allows you to take immediate action if needed.

ESET's Endpoint Protection Platform
Multilayered endpoint security where every single layer sends data to ESET Enterprise Inspector.

+

ESET Enterprise Inspector
Sophisticated EDR tool that analyzes vast amounts of data in real time so no threat goes undetected.

=

Complete prevention, detection and response solution that allows quick analyzes and remediation of any security issues in the network.

The ESET difference

HISTORIC THREAT HUNTING

Not only does ESET Enterprise Inspector offer fully customized threat hunting but also historic threat hunting. Easily adjust behavior rules, then "rescan" the entire events database. This allows you to then identify any new alerts triggered by the adjusted detection rules. No longer are you searching for a static IOC but for dynamic behavior with multiple parameters.

IN CLOUD OR ON-PREMISE

Taking advantage of flexible and secure architecture, ESET Enterprise Inspector allows on-premise as well as cloud deployment for better scalability based on the company size and needs.

OPEN ARCHITECTURE

Provides a unique behavior and reputation-based detection that is fully transparent to security teams. All rules are easily editable via XML to allow fine-tuning or easily created to match the needs of specific enterprise environments, including SIEM integrations.

ADJUSTABLE SENSITIVITY

Easily suppress false alarms by adjusting the sensitivity of detection rules for different computer groups or users. Combine criteria such as file name / path / hash / command line / signer to fine-tune the trigger conditions.

REPUTATION SYSTEM

ESET's extensive filtering enables security engineers to filter out every known-good application using ESET's robust reputation system. Our reputation system contains a database of hundreds of millions of good files to ensure security teams spend their time on the unknown, not on false positives.

SYNCHRONIZED RESPONSE

Built on top of existing ESET endpoint security offering, creating a consistent ecosystem that allows cross-linking of all relevant objects and synchronized remediation of incidents. Security teams can kill processes, download the file that triggered an alert, or simply initiate a computer shutdown or reboot directly from the console.

Recommended Managed Security Services

ESET Threat Monitoring

ESET Threat Monitoring operators constantly monitor your network and endpoint security, alerting you in real time when something suspicious needs your attention.

ESET Threat Hunting

ESET experts help customers investigate data, events and alarms generated by ESET Enterprise Inspector including root cause analyses, forensic investigation and actionable mitigation advice.

The possibilities

THREAT HUNTING

Apply filters to data to sort based on file popularity, reputation, digital signature, behavior or contextual information. Setting up multiple filters allows automated threat hunting which can be customized to each company's environment. Allows for easy threat hunting including APTs and targeted attacks.

INCIDENT DETECTION (ROOT CAUSE ANALYSIS)

Quickly and easily view all security incidents in the alarms section. With a few clicks security teams can see a full root cause analysis that includes: what was affected, where, and when the executable, script or action was performed.

INVESTIGATION AND REMEDIATION

Use a built-in set of rules or create your own rules to respond to detected incidents. Each triggered alarm features a proposed next step to be performed for remediation. Quick response functionality enables specific files to be blocked by hash, processes to be killed and quarantined, and selected machines to be isolated or turned off remotely. This quick response functionality helps to ensure that any single incident will not fall through the cracks.

DATA COLLECTION

View comprehensive data about a newly executed module including: time of execution, user who executed, dwell time and attacked devices.

INDICATORS OF COMPROMISE DETECTION

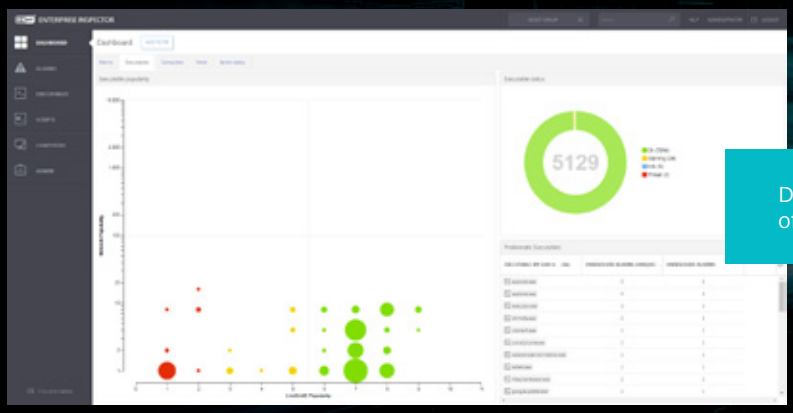
View and block modules based on over 30 different indicators, including hash, registry modifications, file modifications and network connections.

ANOMALY AND BEHAVIOR DETECTION

Check actions that were carried out by an executable and utilize ESET's LiveGrid® Reputation system to quickly assess if executed processes are safe or suspicious. Grouping of computers by user or department allows security teams to identify if the user is entitled to perform a specific action or not.

COMPANY POLICY VIOLATION

Block malicious modules from being executed in your network. Detect violations of policies about using specific software like torrent applications, cloud storages, Tor browsing or other unwanted software.



Dashboard
of ESET Enterprise Inspector

ESET IN NUMBERS

110m+
users worldwide

400k+
business customers

200+
countries & territories

13
global R&D centers