PRODUCT OVERVIEW

ENTERPRISE INSPECTOR

Ensure outstanding visibility and synchronised remediation with ESET EDR

CYBERSECURITY
EXPERTS ON YOUR SIDE

ESET Enterprise Inspector is a sophisticated Endpoint Detection & Response tool for identification of anomalous behaviour 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 users to take immediate action if needed.

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

+

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

=

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

Solution Capabilities

Threat Hunting

Apply data filters to sort based on file popularity, reputation, digital signature, behavior or contextual information. Setting up multiple filters allows automated easy threat hunting, including APTs and targeted attacks which is customisable to each company's environment. By adjusting behavior rules, ESET Enterprise Inspector can be customised also for Historic Threat Hunting and "rescan" the entire events database.

Incident Detection (Root Cause Analysis)

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

Investigation and Remediation

Use a built-in set of rules and create your own rules to respond to detected incidents. Each triggered detection 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.

One-click Isolation

Define network access policies to quickly stop malware's lateral movements. Isolate a compromised device from the network by just one click in the EEI interface. Also, easily remove the devices from the containment state.

Scoring

Prioritise the severity of alarms with scoring functionality that attributes a severity value to incidents and allows the admin to easily identify computers with a higher probability of a potential incident.

Tagging

Assign and unassign tags for fast filtering to EEI objects such as computers, alarms, exclusions, tasks, executables, processes and scripts. Tags are shared among users, and once created, they can be assigned within seconds.

Data Collection

View comprehensive data about a newly executed process, including time of execution, user who executed it, dwell time and affected devices.

Secure Log-in

Enable two-factor authentication - an extra layer of security for your administrator account to prevent an adversary from logging in, even if they have your password.

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 utilise ESET's LiveGrid® Reputation system to quickly assess if executed processes are safe or suspicious. Monitoring anomalous user-related incidents are possible due to specific rules written to be triggered by behavior, not simple malware or signature detections. 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 Detection

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.

Key Benefits

Synchronised Response

Built on top of existing ESET endpoint security offering, it creates 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 a detection, or simply initiate a computer reboot, shutdown, scan, or isolate the device from the network directly from the console.

Open Architecture

Provides a unique behavior and reputation-based detection that is fully transparent to security teams. All rules are written in a common XML format and can be easily customized and created to match the needs of specific enterprise environments, including SIEM integrations.

Remote Access

ESET Enterprise Inspector features remote PowerShell capabilities that allow Security Engineers to remotely inspect and configure their organization's computers, so a sophisticated response can be achieved without breaking the user's workflow.

Public API

ESET Enterprise Inspector features an API that enables accessing and exporting of detections, and their remediation to allow effective integration with tools such as SIEM, SOAR, ticketing tools and many others.

Adjustable Sensitivity

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

MITRE ATT&CK™

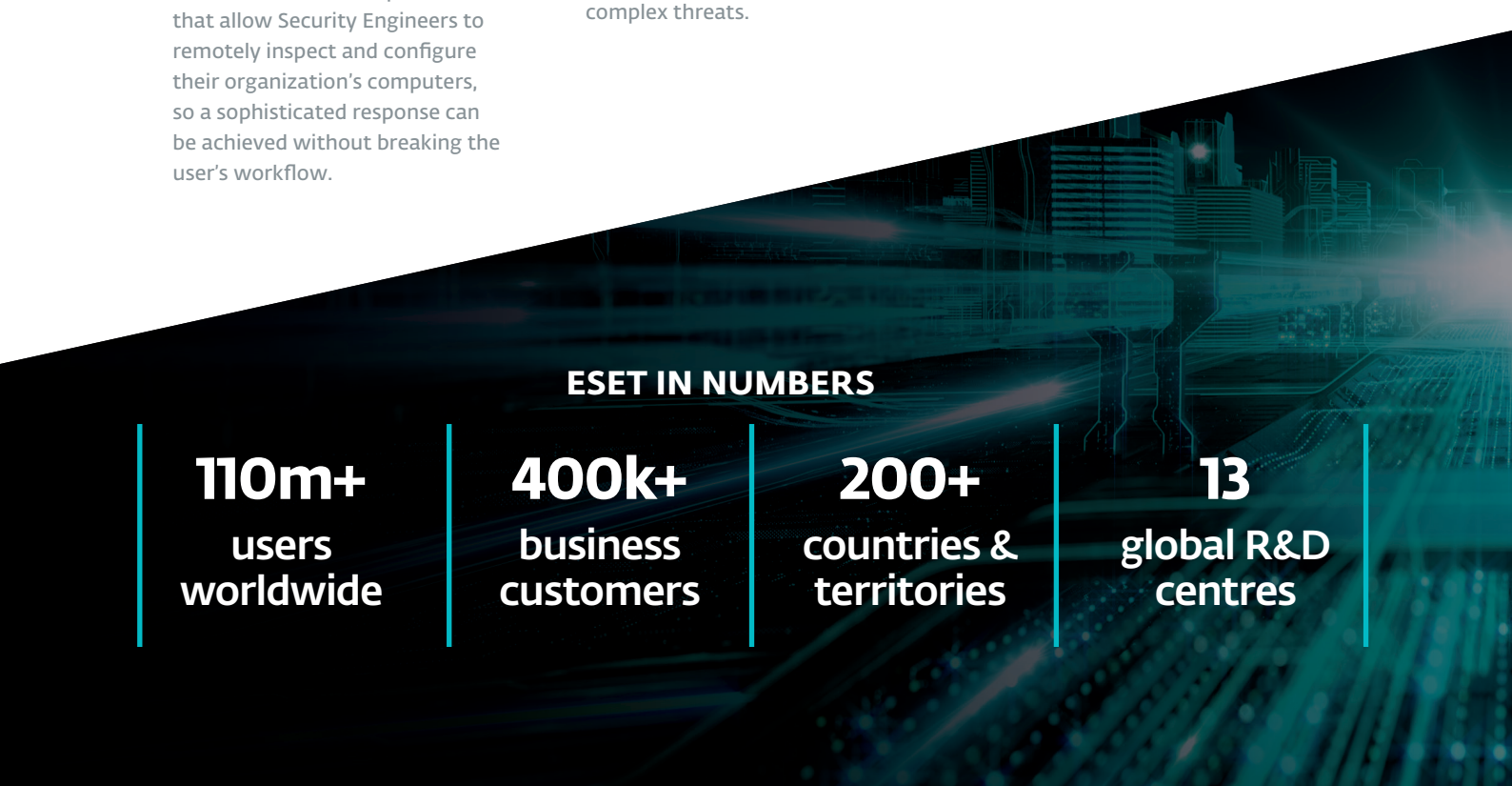
ESET Enterprise Inspector references its detections to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework, which in one click provides you with comprehensive information even about the most complex threats.

Multi-Platform

ESET Enterprise Inspector supports Windows and MacOS, which makes it a perfect choice for multiplatform environments.

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 benign files to ensure security teams spend their time on the unknown, and potentially malicious, not on false positives.



ESET IN NUMBERS

110m+ users worldwide

400k+ business customers

200+ countries & territories

13 global R&D centres