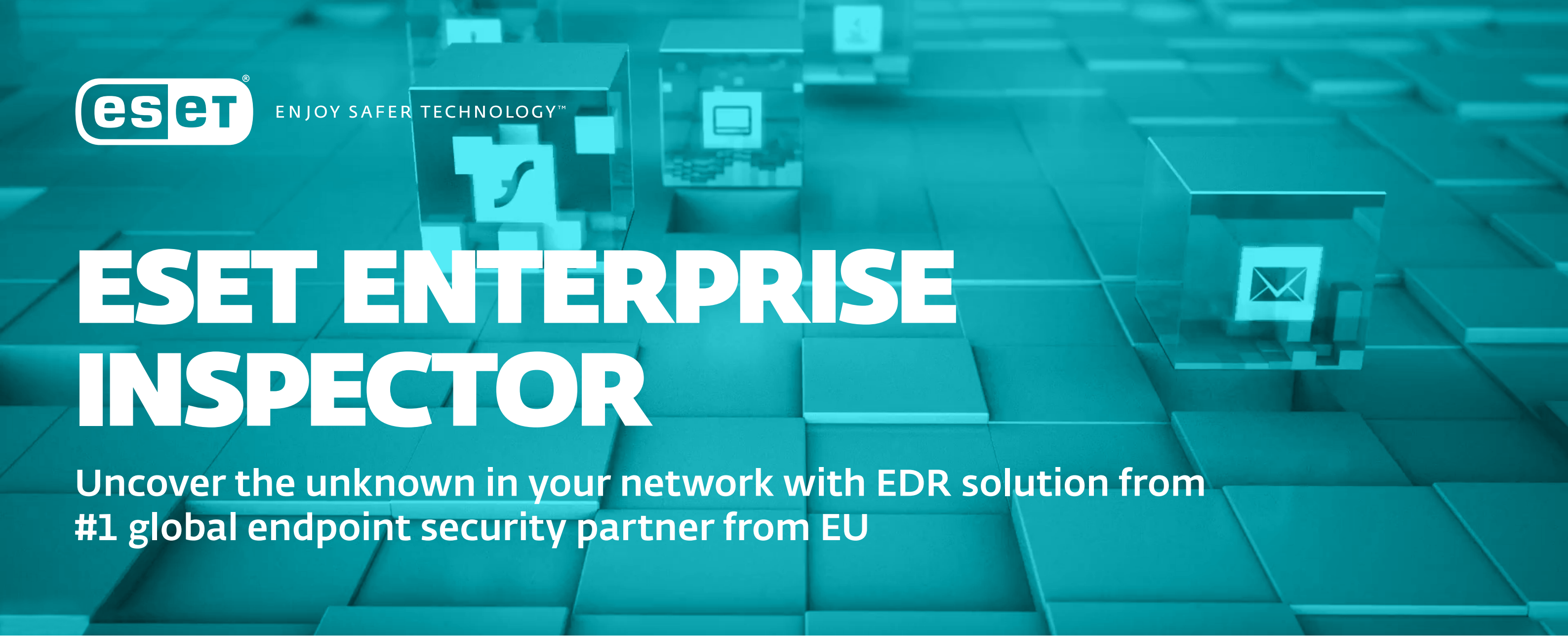


ENJOY SAFER TECHNOLOGY™

ESET ENTERPRISE INSPECTOR

Uncover the unknown in your network with EDR solution from #1 global endpoint security partner from EU

ESET Enterprise Inspector is ESET's Endpoint Detection and Response (EDR) tool for identification of anomalous behavior, identification of breaches, risk assessment, and further forensic investigation that features response capabilities to mitigate the discovered threats.

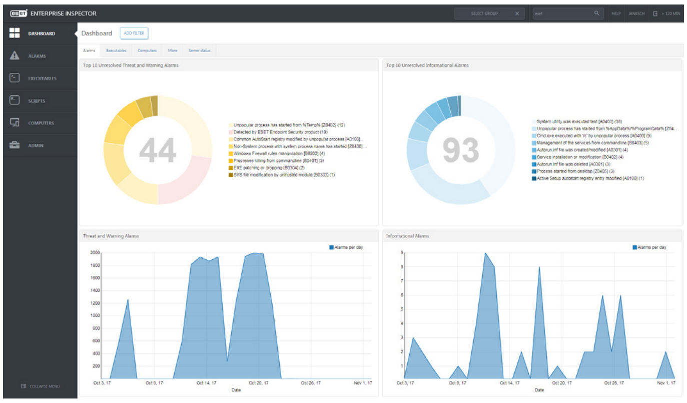
Problem: Invisible threats

The real danger is not what is detected, but what is hidden in the grey zone: APTs silently running in the network or undetected security incidents or breaches that happened in the past. This additional forensic visibility into security incidents is indispensable. Security teams need improved security monitoring, more sensitive threat detection, enhanced response, and both automatic and manual remediation capabilities.

Solution: Personalized EDR

ESET Enterprise Inspector lets security teams intuitively hunt for APTs, file less attacks and other type of malicious activity by applying behavioral and machine learning algorithms over low-level system data collected from endpoints. They can easily configure their own indicators of attack, perform threat hunting, forensic analysis, and root cause analysis.

ESET Enterprise Inspector Dashboard



Unpopular process has started from %Temp% [Z0402] (12)
Detected by ESET Endpoint Security product (10)
Common AutoStart registry modified by unpopular process [A0103]...
Non-System process with system process name has started [Z0400] ...
Windows Firewall rules manipulation [B0202] (4)
Processes killing from commandline [B0401] (3)
EXE patching or dropping [B0304] (2)
SYS file modification by untrusted module [B0303] (1)

System utility was executed test [A0403] (38)
Unpopular process has started from %AppData%/%ProgramData% [Z04...
Cmd.exe executed with "/c" by unpopular process [A0400] (9)
Management of the services from commandline [B0403] (5)
Autorun.inf file was created/modified [A0301] (4)
Service installation or modification [B0402] (4)
Autorun.inf file was deleted [A0301] (3)
Process started from desktop [Z0405] (3)
Active Setup autostart registry entry modified [A0100] (1)

Utilization scenarios and possibilities

Suspicious activity detection and triage

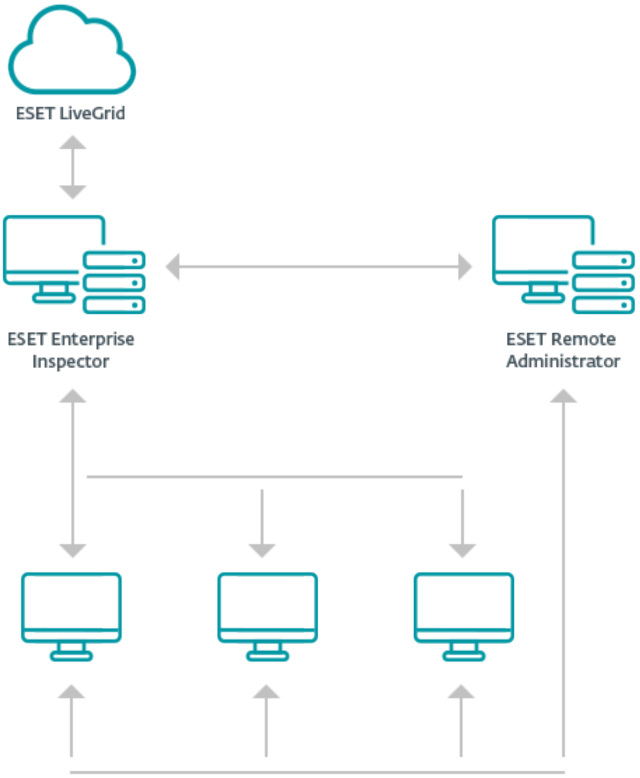
The weakest point in security is often a person sitting by the keyboard, even without any bad intentions. Enterprise Inspector easily identifies these weak elements by sorting the computers by number of unique alarms triggered. If a user triggers multiple alarms, it is a clear indicator that his activity should be validated.

Threat Hunting

The distinctive strength of ESET Enterprise Inspector is in Threat Hunting by "finding a needle in a haystack" approach. By applying filters to data that sorts based on file popularity or reputation, digital signature, behavior, and contextual information, any malicious activity can be easily identified and investigated. Setting up multiple filters allows automated threat-hunting task and can adjust the detection threshold to company specific environment.

Security Ecosystem

ESET Enterprise Inspector is not a standalone product. It is an EDR tool built on top of existing ESET Endpoint Security solutions. The ecosystem is consistent. ESET Enterprise Inspector and ESET Remote Administrator share the same concepts, flows, journeys, and design language with a high level of interactivity, simple contextual navigation, and drill down capabilities that allow cross-linking of all relevant objects.



Context defines structure

“Maliciousness” of an activity depends on the context. Activities performed on computers of network administrators are very different from the ones in the finance department. With proper grouping of computers, security teams can easily identify, if this user is entitled to perform a specific activity on this machine. Synchronization of ESET Remote Administrator endpoint groups and ESET Enterprise Inspector rules provides outstanding results of contextual information.

Open and flexible solution

ESET Enterprise Inspector is an open architecture solution, which means that security team can adjust detection rules describing attack techniques to specific environment of the organization. Open architecture also gives flexibility to configure ESET Enterprise Inspector to detect violations of organization policies about using specific software like torrent applications, Cloud storages (e.g. Dropbox), Tor browsing, starting own servers, and other unwanted software.

Description of alarms and next steps

It’s usually difficult for security teams to quickly prioritize and decide the next step among all the triggered alarms. Therefore, for each triggered alarm there is a proposed next step to be performed for remediation. This helps to ensure that any single important incident will not fall through the cracks.

Incident data search and investigation

With a few clicks security team can see what was affected, where and when specific executable, script, or action was performed, and analyze the cause of it “back to the root”. Each file created on devices monitored by ESET Enterprise Inspector can be tracked by its origin, which process and what user created it. Due to the nature of ESET Enterprise inspector working in conjunction with our endpoint products, it allows us to trace incidents back further than just to a file. For instance, if the endpoint has email protection module active, security team can also see the information about the email, to which the file was attached.

Quick response

When ESET Enterprise Inspector identifies a threat, it provides a quick response functionality. Specific file can be blocked by hash, processes can be killed and quarantined, and selected machines can be isolated or turned off remotely. This helps administrators to quickly make decisions without getting bogged down with excessive amounts of alerts, notifications, and other remediation steps.

As ESET Enterprise Inspector agent extends functionality of ESET endpoint security solutions, all of ESET’s malware removal features are active and allow ESET to remove detected malware, be it Trojans, backdoors, viruses, rootkits, potentially unwanted software, malicious browser extensions and other.

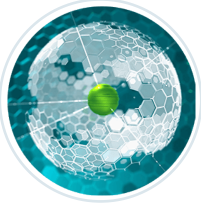
Assets for security teams

Upgraded network visibility

ESET Enterprise Inspector enriches prevention capabilities providing granular visibility into all scripts and processes executed within the company. Its extensive filtering enables security engineers to filter out every known-good application using ESET reputation system and file properties to narrow down the search and focus on what is relevant or needs further investigation. Data is presented in an easily understandable form to further streamline flows and prevent wasted time identifying information that matters.

Customized threat hunting capabilities

ESET Enterprise Inspector allows sub-string search among computers, executables, processes, and even individual modifications and provides extensive options for customization of views and data filtering and mining. Threat hunting has never been easier and faster.

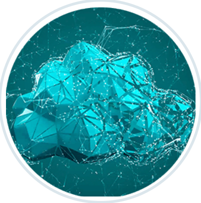


Safe security communication

Both ESET Enterprise Inspector and ESET Remote Administrator databases are deployed on premise, which prevents sensitive data leakage outside company environment, greatly lowers bandwidth overhaul, and allows near real-time synchronization of ESET Enterprise Inspector events with ESET Remote Administrator.

Tailored monitoring system

Unlike competitive solutions, ESET Enterprise Inspector provides a uniques behavior and reputation based detection that is fully transparent to security teams. All rules are easily editable via XML to allow fine-tuning or creation of new ones to match the needs of specific enterprise environments.



Synchronized response

ESET Enterprise Inspector is built on top of existing ESET security Endpoint offering, creating a consistent ecosystem that allows cross-linking of all relevant objects, as well as synchronized remediation of incidents. Security teams can kill the process, download the file that triggered it, or simply initiate a remote computer shutdown or reboot either through ESET Enterprise Inspector or ESET Remote Administrator console.

Who we are

ESET is a multinational software security partner, we protect more than 100 million users around the world and we are #1 global endpoint security partner from EU. ESET is privately held, with no need for quick ROI for investors. That allows us to focus solely on security. This year we are celebrating 30 years of constant technology evolution.

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ENJOY SAFER TECHNOLOGY™

ESET is a EU-based IT security company founded in 1992 and headquartered in Bratislava, Slovakia. The company has a global presence, with regional distribution centers in San Diego, Buenos Aires and Singapore, and office worldwide. **www.eset.com**