ENJOY SAFER TECHNOLOGY™

ESET ENTERPRISE INSPECTOR

Discover and eliminate APTs and Targeted Attacks

Endpoints are the most used entry point for Advanced Persistent Threats and Targeted Attacks. In order to reflect the changing landscape of attacks, it is necessary to monitor and evaluate all the activities happening in the network in real time and take immediate action if needed. ESET Enterprise Inspector is an Endpoint Detection and Response tool which uses advanced techniques to monitor and evaluate suspicious processes and behavior, policy violations, and anomalies, and provides detailed information and response options in the event of security incidents.

Gathering the data

ESET Enterprise Inspector gathers detailed data about activities on the endpoint – from low level system data through security data and network data to endpoint information and statistics. The data is aggregated and stored in a searchable format with extensive filtering possibilities on the server and evaluated in real time.

Understanding the data

All collected data is evaluated to detect anomalies and incidents in real time. In combination with ESET's unique detection and protection technologies and its threat intelligence and cloud malware protection system based on 100 million of sensor worldwide – **ESET LiveGrid®** – it is possible to identify Advanced Persistent Threats and Targeted Attacks never seen before and take immediate action. ESET Enterprise Inspector is able to connect the dots – to discover correlations of otherwise safe processes, files or activities, evaluate them in a complex relationship manner and thus detect hidden threats or weak points of the security.

Remediation

ESET Enterprise Inspector provides multiple options to respond to an incident or suspicious activities. Any suspicious process can be blocked and the object can be sent to ESET for an immediate full threat intelligence report. Any suspected infected endpoint can be quarantined from the rest of the network and its communication isolated to only internal systems or ESET Enterprise Inspector management server.

Usability

The ESET Enterprise Inspector dashboard provides "look and see" information about the activities in the network. Drill-down visualization of the data helps to uncover attack vectors, affected endpoints and users, files used in the attacks, how all of these were connected, where the process started first and other information important for incident investigation.

Network Attack Protection

This extension of firewall technology improves detection of known vulnerabilities, for which a patch has not yet been deployed. It also allows for faster and more flexible detection of malicious traffic.

Network Attack Protection adds an extra layer of protection against known network vulnerabilities for which a patch has not been released or deployed yet.

Our technology looks for exploits by analyzing the content of network protocols.

Any detected attack attempts are then blocked and reported to the user.

Exploit Blocker

While ESET's scanning engine covers exploits that appear in malformed document files, and Network Attack Protection targets the communication level, our Exploit Blocker technology blocks the exploitation process itself. Exploit Blocker monitors typically exploitable applications (browsers, email clients, Flash, Java, and more) and focuses on exploitation techniques.

Exploit Blocker is designed to fortify applications on users' systems that are often exploited.

It keeps a constant lookout over processes for any signs of suspicious activity or behavior.

It blocks any threat, sending its fingerprint to ESET LiveGrid to ward off future attacks.

Cloud Malware Protection System

The ESET Cloud Malware Protection System is one of several technologies based on ESET's LiveGrid cloud system. Possible threats are monitored and submitted to the ESET cloud via the ESET LiveGrid Feedback System for automatic sandboxing and behavioral analysis.

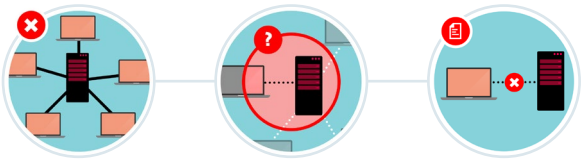
Suspicious unknown applications and potential threats are monitored and submitted to ESET cloud via the **ESET LiveGrid feedback system**.

Collected samples are subjected to **automatic sandboxing and behavioral analysis**, which results in the creation of automated signatures where malicious activity is confirmed.

ESET clients learn about these automated detections via the **ESET LiveGrid Reputation system** without the need to wait for the next signature database update.

Enhanced Botnet Protection

ESET Botnet Protection detects malicious communication used by botnets, and at the same time identifies the offending processes. Malicious communications are blocked and reported to the user.



Botnet Protection provides another layer of network-based detection to reveal possible running threats.

It searches outgoing network communication for known malicious patterns, and matches the remote site against a blacklist of malicious ones.

Any **detected malicious communication is blocked** and reported to the user.

ESET received the most "Advanced+" awards in Proactive Tests by AV-Comparatives

ESET received the "Advanced+" award in the AV-Comparatives Real-World Protection Test

ESET has the longest unbroken run of VB100 awards for malware detection of any IT security vendor. We've been excelling at VB100 tests since 2003.

ESET holds the top mark for spam detection, as awarded by Virus Bulletin.

About ESET: Since 1987, ESET® has been developing award-winning security software that now helps over 100 million users to Enjoy Safer Technology. Its broad security product portfolio covers all popular platforms and provides businesses and consumers around the world with the perfect balance of performance and proactive protection. The company has a global sales network covering 180 countries, and regional offices in Bratislava, San Diego, Singapore and Buenos Aires.
www.eset.com