PRODUCT OVERVIEW

ENDPOINT SOLUTIONS

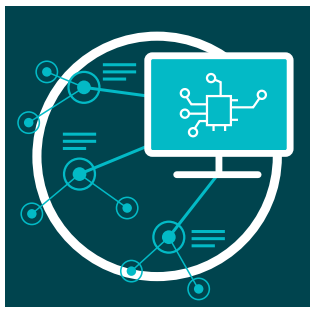
CYBERSECURITY
EXPERTS ON YOUR SIDE

The Technology

Our products and technologies stand on 3 pillars:

ESET LIVEGRID®

Whenever a zero day threat such as ransomware is seen, the file is sent to our cloud-based malware protection system – LiveGrid®, where the threat is detonated and behaviour is monitored. Results of this system are provided to all endpoints globally within minutes without requiring any updates.



MACHINE LEARNING

Uses the combined power of neural networks and handpicked algorithms to correctly label incoming samples as clean, potentially unwanted or malicious.

HUMAN EXPERTISE

World-class security researchers sharing elite know-how and intelligence to ensure the best round-the-clock threat intelligence.

A single layer of defence is not enough for the constantly evolving threat landscape. All ESET Endpoint security products have the ability to detect malware pre-execution, during execution and post-execution. Focusing on more than a specific part of the malware lifecycle allows us to provide the highest level of protection possible.

The ESET Difference

Multi-layered Protection

ESET combines multi-layered technology, machine learning and human expertise to provide our customers with the best level of protection possible. ESET's technology is constantly adjusting and changing to provide the best balance of detection, false positives and performance.

Cross-platform Support

ESET Endpoint protection products support all Operating Systems including Windows, Mac OS, Linux and Android. From a single pane of glass, all endpoint products can be fully managed; Mobile Device Management for iOS and Android is fully integrated.

Unparalleled Performance

Countless times, an organisation's biggest concern is the performance impact of an endpoint protection solution. ESET products continue to excel in the performance arena and win third-party tests that prove how lightweight the endpoints are on systems.

Worldwide Presence

ESET has offices in 22 countries worldwide, R&D labs in 13 and presence in over 200 countries and territories. This helps to provide data to stop malware prior to it spreading across the globe, as well as prioritise new technologies based on the most recent threats or possible new vectors.

ESET's Endpoint Protection Solutions

ESET Endpoint Security for Windows/Mac/Android

ESET Endpoint Antivirus for Windows/Mac/Linux

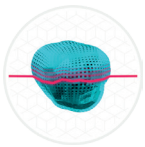
ESET File Security for Windows Server/Linux/FreeBSD/Azure

ESET Mobile Device Management for Apple iOS

ESET Endpoint Solutions technical features

RANSOMWARE SHIELD

ESET Ransomware Shield is an additional layer protecting users from ransomware. This technology monitors and evaluates all executed applications based on their behavior and reputation. It is designed to detect and block processes that resemble the behavior of ransomware.

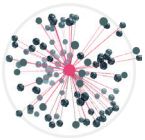


ADVANCED MEMORY SCANNER

ESET Advanced Memory Scanner monitors the behavior of a malicious process and scans it once it decloaks in memory. Fileless malware operates without needing persistent components in the file system that can be detected conventionally. Only memory scanning can successfully discover and stop such malicious attacks.

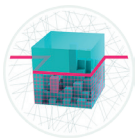
EXPLOIT BLOCKER

ESET Exploit Blocker monitors typically exploitable applications (browsers, document readers, email clients, Flash, Java and more), and instead of just aiming at particular CVE identifiers, it focuses on exploitation techniques. When triggered, the threat is blocked immediately on the machine.



BOTNET PROTECTION

ESET Botnet Protection detects malicious communication used by botnets, and at the same time it identifies the offending processes. Any detected malicious communication is blocked and reported to the user.



UEFI SCANNER

ESET is the first endpoint security provider to add a dedicated layer into its solution that protects the Unified Extensible Firmware Interface (UEFI). ESET UEFI Scanner checks and enforces the security of the preboot environment and is designed to monitor the integrity of the firmware.

HIPS

ESET's Host-Based Intrusion Prevention System monitors system activity and uses a predefined set of rules to recognise suspicious system behavior. Moreover, the HIPS self-defense mechanism stops the offending process from carrying out the harmful activity.