ENJOY SAFER TECHNOLOGY™

ESET'S MULTI-LAYERED APPROACH TO SECURITY

The fight against modern malware, which is dynamic and often targeted, requires a multi-layered approach. **The more multi-layered your security, the fewer incidents you'll need to resolve.** ESET began incorporating proactive and smart technology into its scanning engine more than 20 years ago, and — thanks to the efforts of our global research labs — continues to add extra layers of protection.

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.

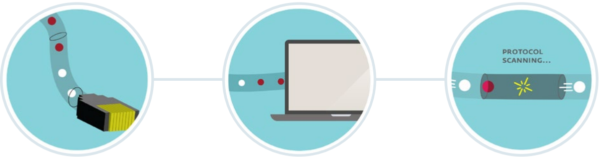
Suspicious unknown applications and potential threats are monitored and submitted to ESET cloud via the **ESET LiveGrid feedback system**.

Collected samples are subjected to **automatic sandboxing and behavioral analysis**, which results in the creation of automated detections 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 module update.

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 toward off future attacks.

ENJOY SAFER TECHNOLOGY™

Advanced Memory Scanner

Advanced Memory Scanner is a unique ESET technology which effectively addresses an important issue of modern malware — heavy use of obfuscation and/or encryption. To tackle these issues, Advanced Memory Scanner monitors the behavior of a malicious process, and scans it once it decloaks in memory.

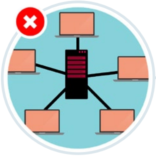
Advanced Memory Scanner uncovers malware which employs sophisticated obfuscation and encryption tricks to avoid detection by conventional means.

Our technology monitors the behavior of a malicious process and scans it once it decloaks in the system memory.

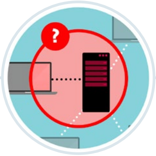
Any identified malware is flagged and subsequently eliminated by this additional layer of protection.

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.

Reputation & Cache

When inspecting a file or URL our products first check the local cache for known malicious or white-listed benign objects. This improves scanning performance. Afterwards, our ESET LiveGrid® Reputation System is queried for the object's reputation.

ESET LiveGrid cloud system collects threat-related information from millions of ESET users to determine file age and prevalence.

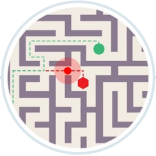
Unkown, previously unseen threats are submitted to ESET for further analysis and processing.

Our cloud server logic automatically evaluates this data and provides rapid response via black- and white-listing.

DNA Detections

DNA Detections are complex definitions of malicious behavior and malware characteristics. While malicious code can be easily modified or obfuscated, object behavior cannot be changed so easily. Therefore DNA Detection can identify even previously unseen malware which contains genes that indicate malicious behavior.

Our **Advanced Heuristics** approach proactively detects malware we haven't come across before.



We detect malware based on its functionality by uncovering the way it behaves.

Advanced techniques, such as DNA-based scanning, identify threats based on the code structure.

AV ADVANCED+ ★★★ HEURISTIC / BEHAVIOURAL TEST comparatives MAR 2015

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

AV ADVANCED+ ★★★ -REAL WORLD- PROTECTION TEST comparatives DEC 2015

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

vb 100 VIRUS virusbtn.com

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.

vb March 2016 VERIFIED SPAM + virusbtn.com

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