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.

Machine learning

ESET has its own in-house machine learning engine, called ESET Augur. It monitors and evaluates all executed applications using behavioral heuristics.

ESET Augur uses the combined power of neural networks (such as deep learning and long short-term memory) and a group of six classification algorithms.

Generates a consolidated output and helps correctly label the incoming sample as clean, potentially unwanted or malicious.

Works in conjunction with other protective technologies such as DNA, sandbox and memory analysis.

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.

ESET ransomware shield

This technology monitors and evaluates all executed applications based on their behavior and reputation.

Designed to detect and block processes that resemble the behaviors of ransomware.

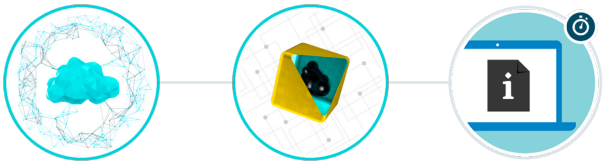
If ESET Ransomware Shield is triggered by a suspicious action, the user will be prompted to approve or deny a blocking action.

Offers the highest possible level of ransomware protection, in conjunction with other ESET technologies such as Cloud Malware Protection System.

ENJOY SAFER TECHNOLOGY®

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.

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.

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.

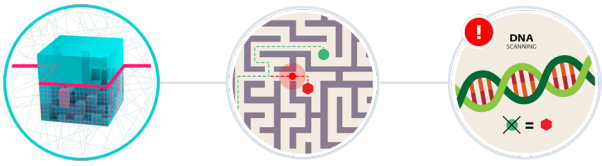
Exploit Blocker is designed to fortify applications on users' systems that are often exploited.

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.

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.

For comprehensive information on ESET technology, visit eset.com/us/technology

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: For 30 years, ESET® has been developing industry-leading IT security software and services for businesses and consumers worldwide.
www.eset.com