ESET

ENDPOINT PROTECTION PLATFORM

Multilayered technology, machine learning and human expertise working together in dynamic equilibrium provided by the #1 global endpoint security partner from the EU.

ESET
ENJOY SAFER TECHNOLOGY®

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

What is an **endpoint protection platform?**

An endpoint protection platform (EPP) is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

ESET's Endpoint Security solutions leverage a multilayered approach that utilizes multiple technologies working in a dynamic equilibrium, which has the ability to constantly balance performance, detection and false positives.

Why **endpoint protection solutions?**

RANSOMWARE

Ransomware has been a constant concern for industries across the world ever since Cryptolocker in 2013. Despite ransomware existing for far longer, it was never a major threat that businesses were concerned about. However, now a single incidence of ransomware can easily render a business inoperable by encrypting important or necessary files. When a business experiences a ransomware attack, it quickly realizes that the backups it has are not recent enough, so the business feels as though it must pay the ransom.

ESET Endpoint Security provides layers of defense to not just prevent ransomware but to detect it if it ever exists within an organization. It is important to prevent and detect ransomware, as every time someone pays a ransom, it convinces the criminals to continue to utilize this attack.

TARGETED ATTACKS AND DATA BREACHES

Today's cybersecurity landscape is constantly evolving with new attack methods and never-before-seen threats. When an attack or data breach occurs, organizations are typically surprised that their defenses were compromised or are completely unaware that the attack even happened. After the attack is finally discovered, organizations then reactively implement mitigations to stop this attack from being repeated. However, this does not protect them from the next attack that may use another brand-new vector.

ESET Endpoint Security solutions use threat intelligence information based on our global presence to prioritize and effectively block the newest threats prior to their delivery anywhere else in the world. In addition, most endpoint protection platforms feature cloud-based updating to respond quickly in the case of a missed detection without having to wait for a normal update.

FILELESS ATTACKS

Newer threats, called fileless malware, exist exclusively in computer memory, making it impossible for file scanning-based protections to detect it. Furthermore, some fileless attacks will leverage currently installed applications that are built into the OS to make it even harder to detect a malicious payload. For example, the use of PowerShell in these attacks is very common.

ESET Endpoint protection platforms have mitigations in place to detect malformed or hijacked applications to protect against fileless attacks. ESET has also created dedicated scanners to constantly check memory for anything that is suspicious. By utilizing this multi-layered approach, we make sure we always stay one step ahead of the newest malware.

ESET Endpoint Security provides layers of defense to not just prevent malware but to detect it if it ever exists within an organization.

When an attack or data breach occurs, organizations are typically surprised that their defenses were compromised or are completely unaware that the attack even happened.

Newer threats, called fileless malware, exist exclusively in computer memory, making it impossible for file scanning-based protections to detect it.

"ESET has been our reliable security solution for years. It does what it has to do; you do not have to worry. In short, ESET stands for: reliability, quality and service."

—Jos Savelkoul, Team Leader ICT-Department; Zuyderland Hospital, Netherlands; 10,000+ seats

ESET's endpoint protection solutions

ESET Endpoint Security for Windows/macOS/Android

ESET Endpoint Antivirus for Windows/macOS/Linux Desktop

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

ESET Mobile Device Management for Apple iOS

The ESET difference

MULTILAYERED PROTECTION

ESET combines multilayered technology, machine learning and human expertise to provide our customers with the best level of protection possible. Our technology is constantly adjusting and changing to provide the best balance of detection, false positives and performance.
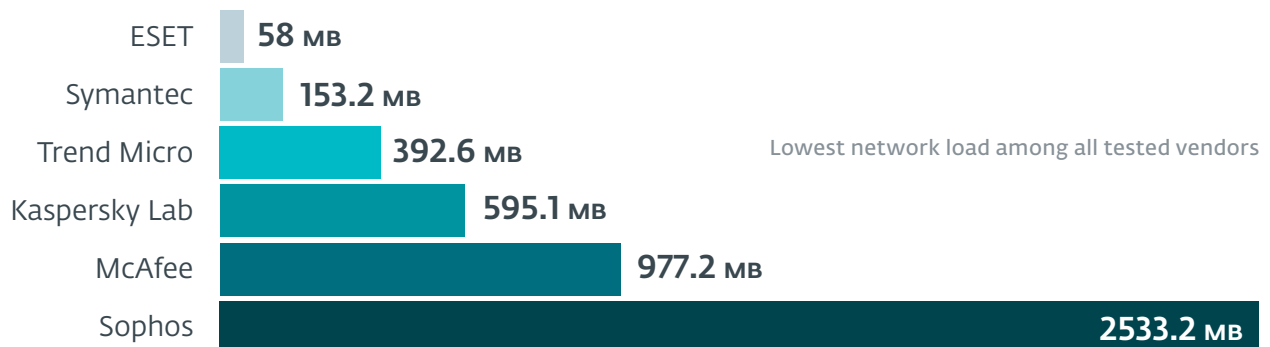
UNPARALLELED PERFORMANCE

Countless times, an organization'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 light-weight our endpoints are on systems.

CROSS PLATFORM SUPPORT

ESET Endpoint products support all OSes 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 built in as well.

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 us with data to stop malware prior to it spreading across the globe, as well as prioritize new technologies based on the most recent threats or possible new vectors.

Vendor	Network load
ESET	58 MB
Symantec	153.2 MB
Trend Micro	392.6 MB
Kaspersky Lab	595.1 MB
McAfee	977.2 MB
Sophos	2533.2 MB

Lowest network load among all tested vendors

Source: AV-Comparatives: Network Performance Test, Business Security Software

"...the best testimony? The stats from our helpdesk: after we introduced ESET, our support guys don't log any calls—they don't have to deal with any antivirus or malware-related issues!"

— Adam Hoffman, IT Infrastructure Manager;
Mercury Engineering, Ireland; 1,300 seats

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 behavior is monitored. Results of this system are provided to all endpoints globally within minutes without requiring any updates.
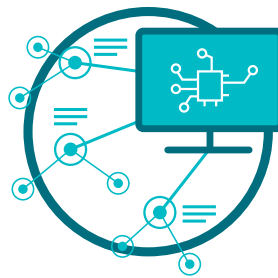
MACHINE LEARNING

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 defense 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.

MACHINE LEARNING

All ESET Endpoint products have been using machine learning in addition to all other layers of defense since 1997. ESET currently uses machine learning in conjunction with all of our other layers of defense. Specifically, machine learning is used in the form of consolidated output and neural networks.
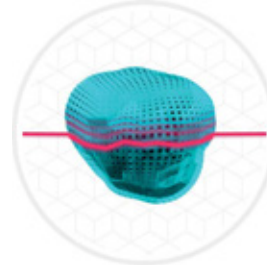
ADVANCED MEMORY SCANNER

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.

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.

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.
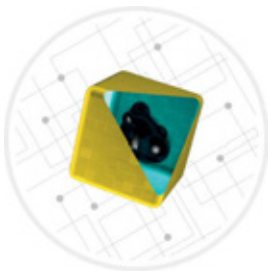
IN-PRODUCT SANDBOX

Today's malware is often heavily obfuscated and tries to evade detection as much as possible. To see through this and identify the real behavior hidden underneath the surface, we use in-product sandboxing. With the help of this technology, ESET solutions emulate different components of computer hardware and software to execute a suspicious sample in an isolated virtualized environment.

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.

NETWORK ATTACK PROTECTION

This technology improves detection of known vulnerabilities on the network level. It constitutes another important layer of protection against spreading malware, network-conducted attacks, and exploitation of vulnerabilities for which a patch has not yet been released or deployed.

DNA DETECTIONS

Detection types range from very specific hashes to ESET DNA Detections, which are complex definitions of malicious behavior and malware characteristics. While the malicious code can be easily modified or obfuscated by attackers, the behavior of objects cannot be changed so easily and ESET DNA Detections are designed to take advantage of this principle.

HIPS

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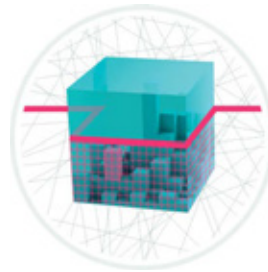
UEFI SCANNER

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. If modification is detected, it notifies the user.

"The biggest thing that stands out is its strong technical advantage over other products in the marketplace. ESET offers us reliable security, meaning that I can work on any project at any time knowing our computers are protected 100%."

— Fiona Garland, Business Analyst Group IT; Mercury Engineering, Ireland; 1,300 seats
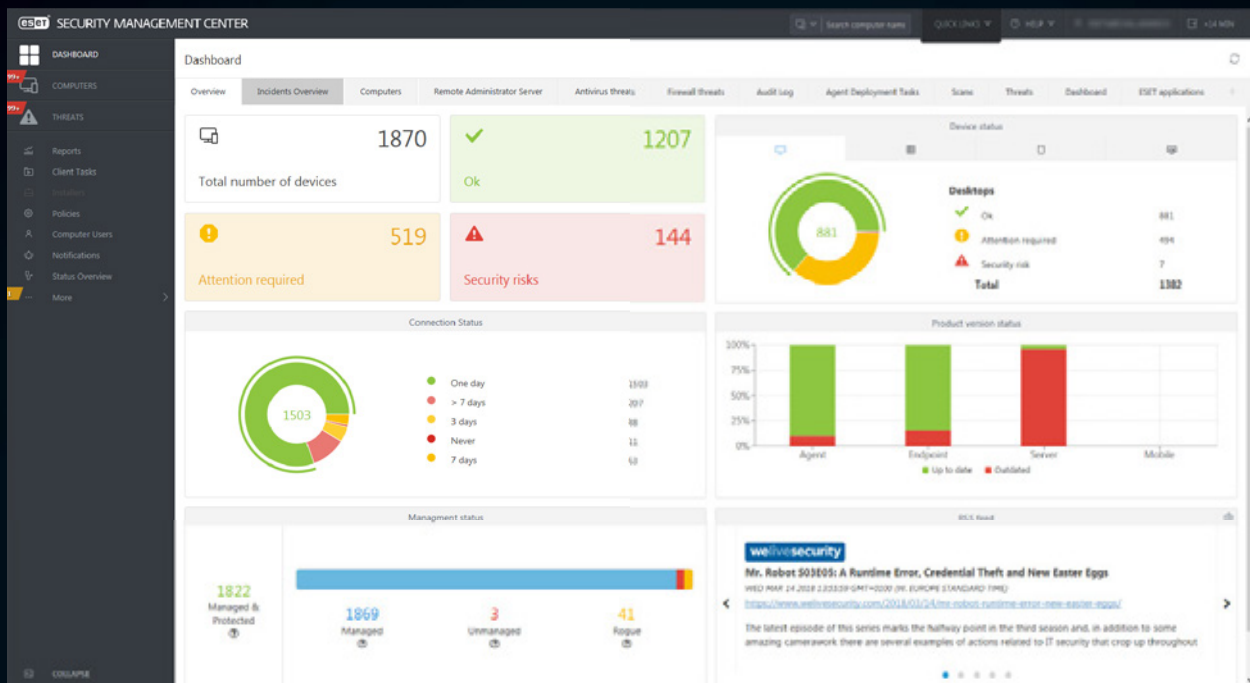
ESET Security Management Center

All ESET endpoint solutions are managed from a single pane of glass—ESET Security Management Center— that can be installed on Windows or Linux. In addition to installing, ESET has a virtual appliance that you can simply import in for quick and easy setup.
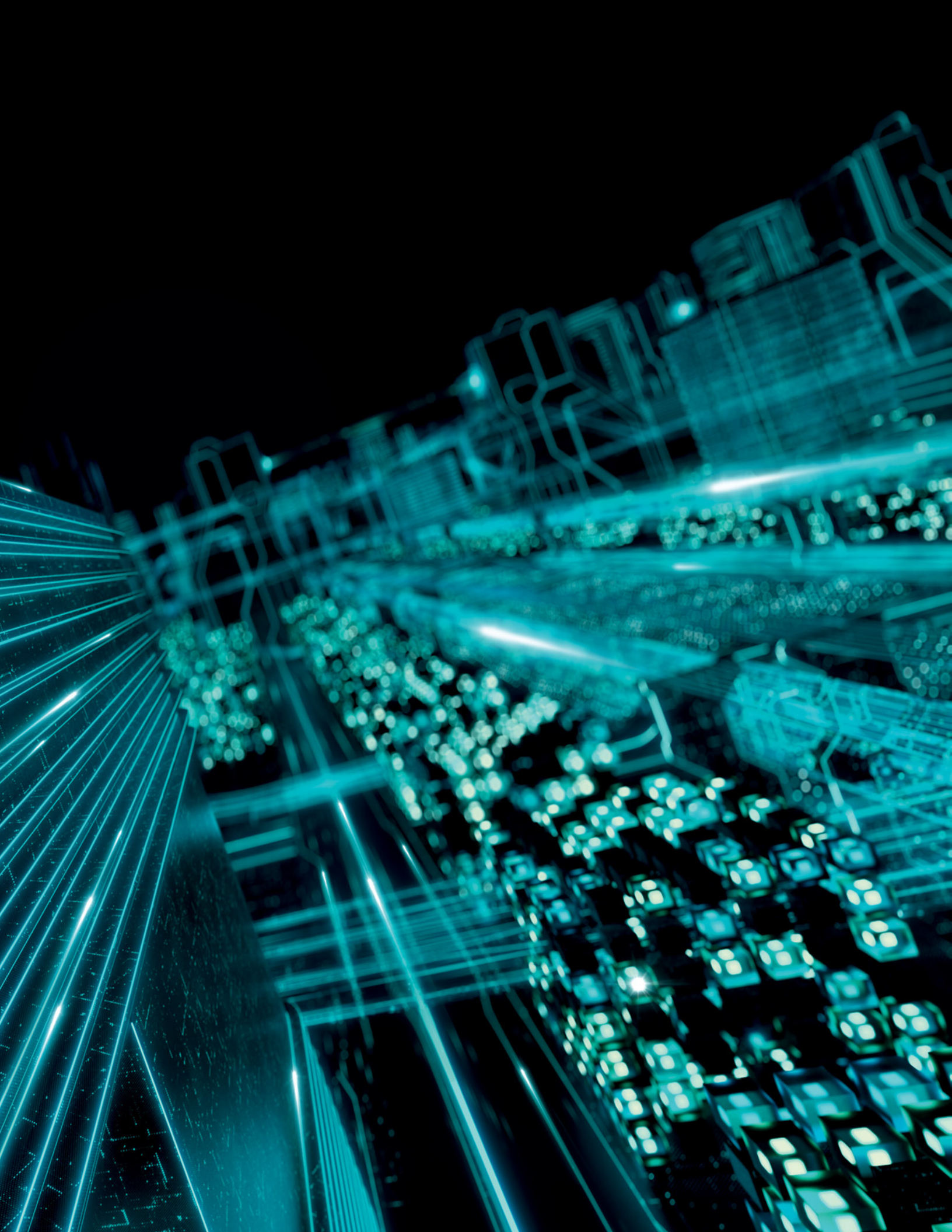
Use cases

Ransomware

Some businesses want extra insurances that they will be protected from Ransomware attacks.

SOLUTION

✓ Network Attack Protection has the ability to prevent ransomware from ever infecting a system by stopping exploits at the network level.

✓ Our multilayered defense features an in-product sandbox that has the ability to detect malware that attempts to evade detection by using obfuscation.

✓ Leverage ESET's cloud malware protection system to automatically protect against new threats without the need to wait for the next detection update.

✓ All products contain protection in the form of Ransomware Shield to ensure that businesses are protected from malicious file encryption.

Zero-day threats

Zero-day threats are a major concern for businesses because they do not know how to protect against something that they have never seen before.

SOLUTION

✓ ESET endpoint products leverage heuristics and machine learning as part of our multilayered approach to prevent and protect against never-before-seen malware.

✓ 13 global R&D labs help to quickly respond to malware at first incidence anywhere across the globe.

✓ ESET's cloud malware protection system automatically protects against new threats without the need to wait for the next detection update.

Fileless malware

Fileless malware is a relatively new threat and due to it only existing in memory requires a different approach then traditional file-based malware.

SOLUTION

✓ A unique ESET technology, Advanced Memory Scanner, protects against this type of threat by monitoring the behavior of malicious processes and scanning them once they decloak in memory.

✓ Reduce data gathering and investigation time by uploading threat into ESET Threat Intelligence to provide information on how the threat functions.

✓ Multilayered technology, machine learning and human expertise provide our customers with the best level of protection possible.

"When we found ESET, we knew it was the right choice: reliable technology, robust detection, local presence and excellent technical support, everything that we needed."

— Ernesto Bonhoure,
IT Infrastructure Manager,
Hospital Alemán,
Argentina, 1,500+ seats

About ESET

ESET—a global player in information security—has been named as the only challenger in the 2018 Gartner Magic Quadrant for Endpoint Protection Platforms.*

For more than 30 years, ESET® has been developing industry-leading IT security software and services, delivering instant, comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide.

ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.

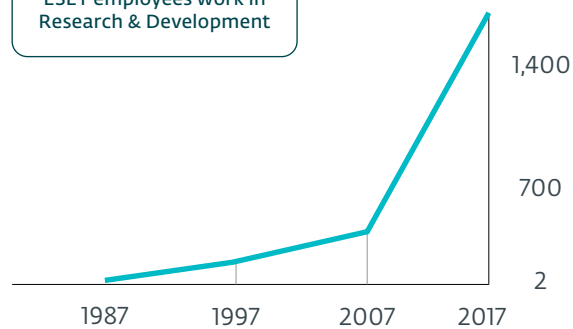## ESET IN NUMBERS

110M +
users worldwide

400k+
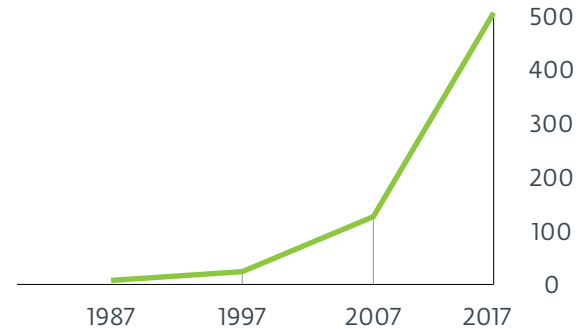business customers

200+
countries & territories

13
global R&D centers

ESET EMPLOYEES

More than one-third of all ESET employees work in Research & Development

1,400

700

2

1987   1997   2007   2017

ESET REVENUE

in million €

500
400
300
200
100
0

1987   1997   2007   2017

*Gartner does not endorse any vendor, product or service depicted in its research publications. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

HONDA

protected by ESET since 2011

license prolonged 3x, enlarged 2x

GREENPEACE

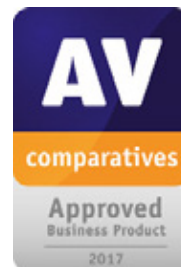protected by ESET since 2008

license prolonged/enlarged 10x

Canon

protected by ESET since 2016

more than 14,000 endpoints

T ··

ISP security partner since 2008

2 million customer base

SOME OF OUR TOP AWARDS

SE Labs
AAA
OCT-DEC 2016
ENTERPRISE ENDPOINT

THE CHANNEL CO.
CRN
★★★★★
PARTNER PROGRAM GUIDE
WINNER 2017

AV comparatives
Approved
Business Product
2017

SC MEDIA
RECOMMENDED

"Given the good features for both anti-malware and manageability, and the global reach of customers and support, ESET should be on the shortlist for consideration in enterprise RFPs for anti-malware solutions."

KuppingerCole Leadership Compass
Enterprise Endpoint Security: Anti-Malware Solutions, 2018