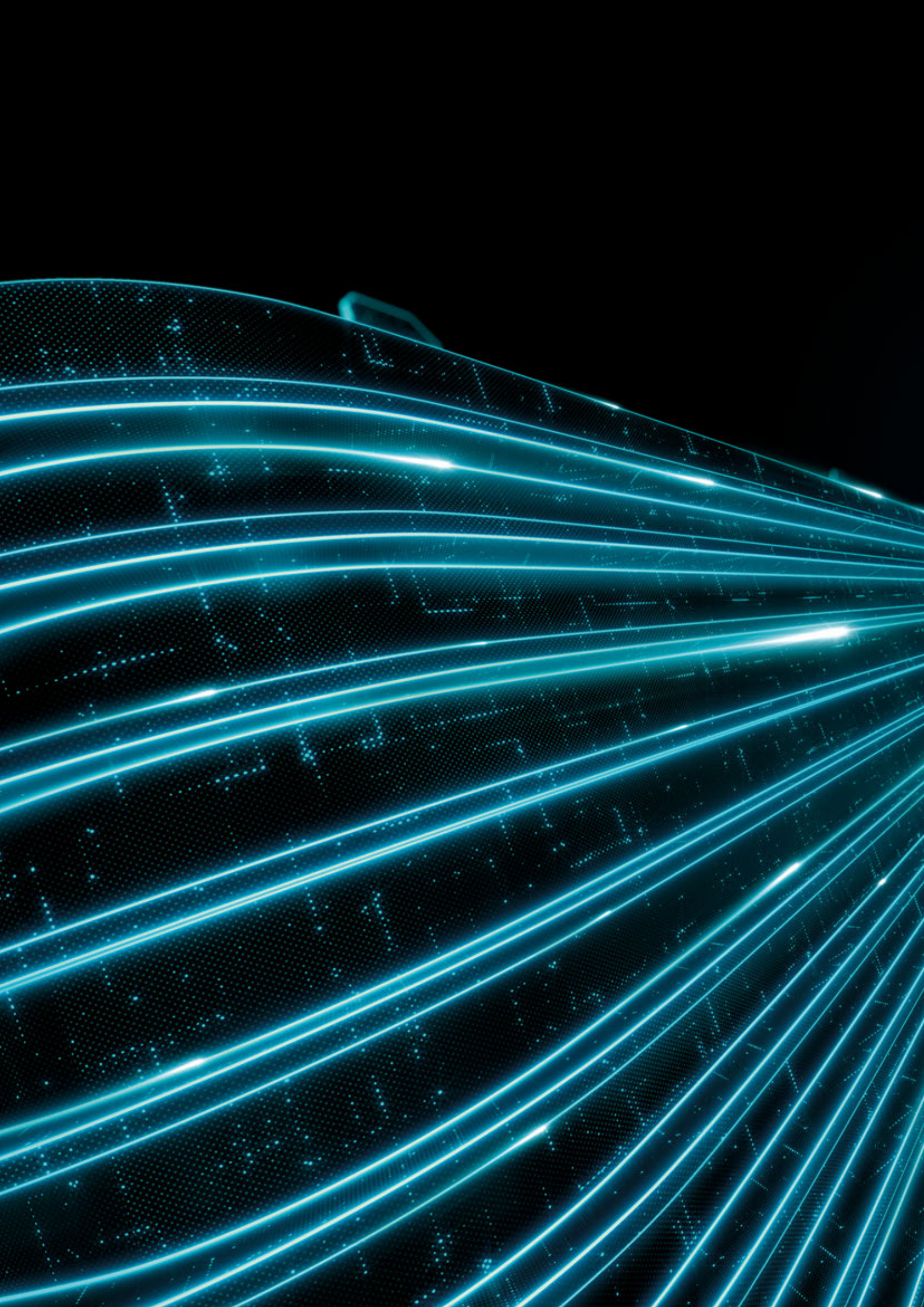# (eset)®

SERVER SECURITY

Protect servers using reliable multilayered solution without compromise

Progress. Protected.

What is a file security solution?

A file security product is designed to protect the central servers of an organization from threats. This product should be installed on any non-specialized server to ensure that organizational resources are not infected. Companies nowadays put their organization at risk by allowing users to save files to a company network share, without adequately protecting their network shares from malicious files. A single user saving a malicious file to a network drive can instantly cause a cascade effect that renders your organization's files inaccessible.

ESET Server Security provides advanced protection to all general servers, network file storage, and multi-purpose servers. It pays special attention to ensure the servers are stable and conflict-free to keep maintenance windows and restarts at a minimum level in order to not disrupt business continuity.

Why **file security 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, they quickly realize that the backups they have are not recent enough, so the business feels as though they must pay the ransom.

With servers, ransomware can be an even bigger problem due to a users' ability to save ransomware to a network drive. ESET Server Security solutions provides layers of defense to not just prevent ransomware, but to detect it if it ever exists within an organization. It is important to try and 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 Server Security solutions use Threat Intelligence information based on their global presence to prioritize and effectively block the newest threats prior to their delivery anywhere else in the world. Servers are typically a more sought after target due to them usually containing sensitive or confidential data. To better protect against these increase attempts ESET Server Security solutions 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. Further, 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 Server Security solutions have mitigations in place to detect malformed or hijacked applications to protect against fileless attacks. Others have created dedicated scanners to constantly check memory for anything that is suspicious. Either way, File Security products have always been challenged to try and stay one step ahead of the newest malware.

ESET's solutions provide 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 Server Security solutions

ESET Server Security for Microsoft Windows Server

ESET Server Security for Linux

ESET Server Security for Microsoft Azure

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.
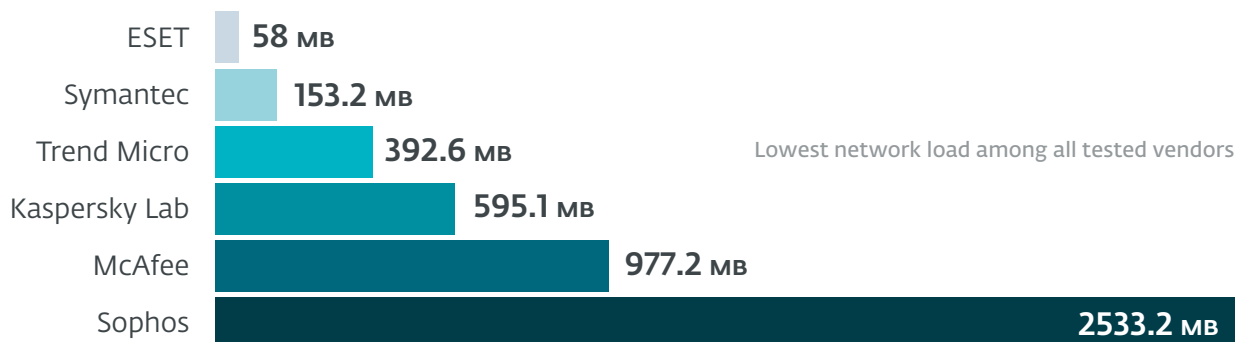
CROSS PLATFORM SUPPORT

ESET Server Security solutions support multiple OSes and platforms including Windows Server, Office365 OneDrive, Linux/FreeBSD and Microsoft Azure. From a single pane of glass, all ESET solutions can be fully managed.

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.

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.
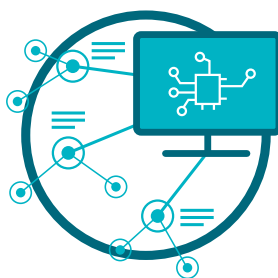
MACHINE LEARNING

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 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.
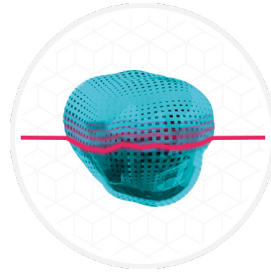
ADVANCED MEMORY SCANNER

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.
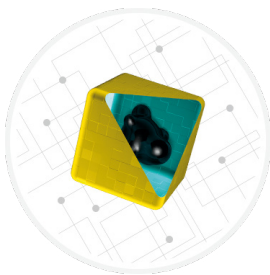
IN-PRODUCT SANDBOX

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.
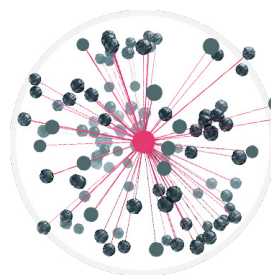
BOTNET PROTECTION

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.
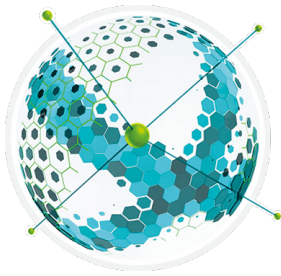
NETWORK ATTACK PROTECTION

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.
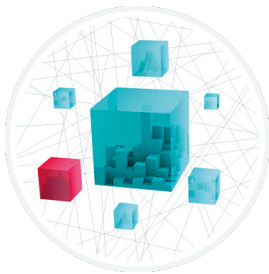
BEHAVIORAL DETECTION - HIPS

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.
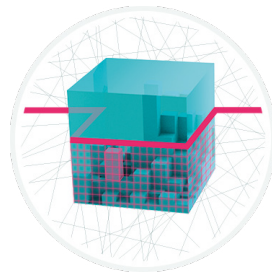
AMSI/SCRIPT SCANNING

ESET solutions leverage the Antimalware Scan Interface (AMSI) to provide enhanced malware protection for users, data, applications, and workload. In addition, it utilizes the protected service interface that is a new security module built into Windows that only allows trusted, signed code to load and better protect against code injection attacks.

"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
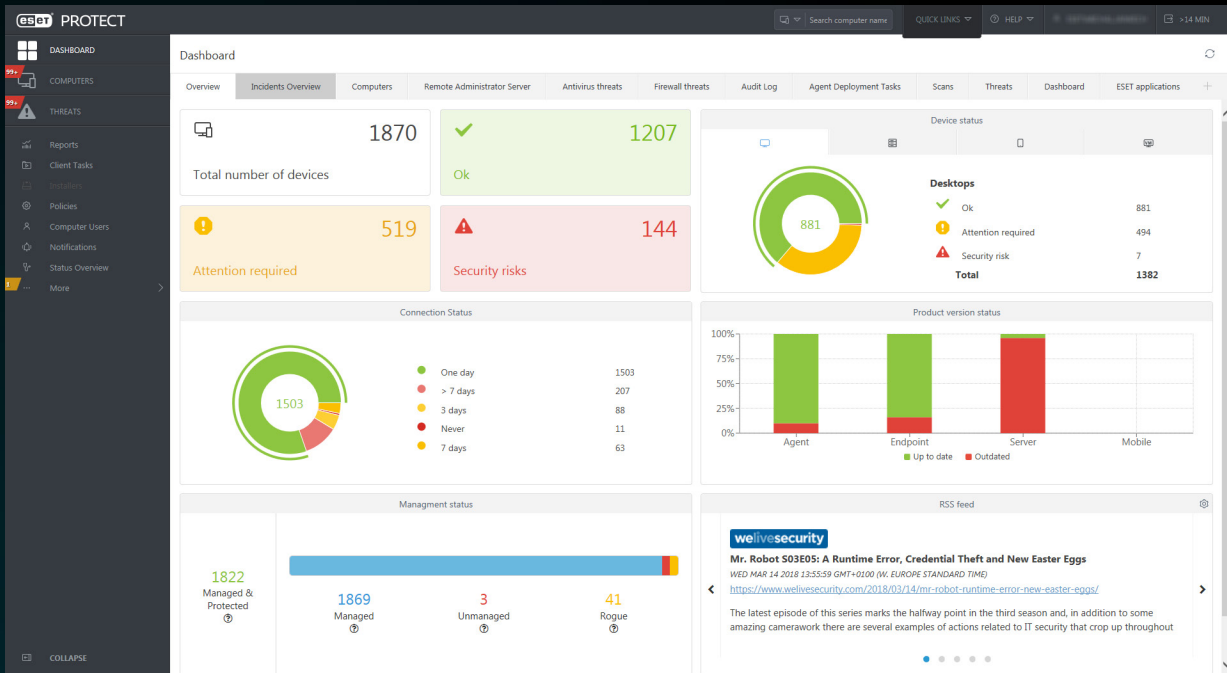
ESET PROTECT

All ESET endpoint solutions are managed from
a single-pane-of-glass cloud console, ESET PROTECT,
ensuring the complete overview of your network.

"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

Use cases

Fileless malware

Use Case: File-less malware is a relatively new threat and due to it only existing in memory requires a different approach than 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.

✓ If ESET Server Security is unsure of a potential threat, it has the ability to upload the sample to ESET's Advanced Threat Defense, ESET LiveGuard Advanced, to make the highest quality decision on whether something is malicious.

✓ If a threat is confirmed, reduce data gathering and investigation time by uploading threat into ESET Threat intelligence to provide information on how the threat functions.

Zero-day threats

Use Case: Zero-day threats are a major concern for businesses due to them not knowing how to protect against something that they have never seen before.

SOLUTION

✓ ESET Threat Intelligence provides data on the newest threats and trends as well as targeted attacks to help businesses predict and prevent the newest threats.

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

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

Ransomware

Use Case: Some Businesses want extra insurances that they will be protected from Ransomware attacks. In addition, they want to ensure their network drives are safe from being encrypted.

SOLUTION

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

✓ Our multi-layered 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 post-execution protection in the form of Ransomware Shield to ensure that businesses are protected from malicious file encryption.

✓ If ESET Server Security is unsure of a potential threat, it has the ability to upload the sample to ESET's Advanced Threat Defense, ESET LiveGuard Advanced, to make the highest quality decision on whether something is malicious.
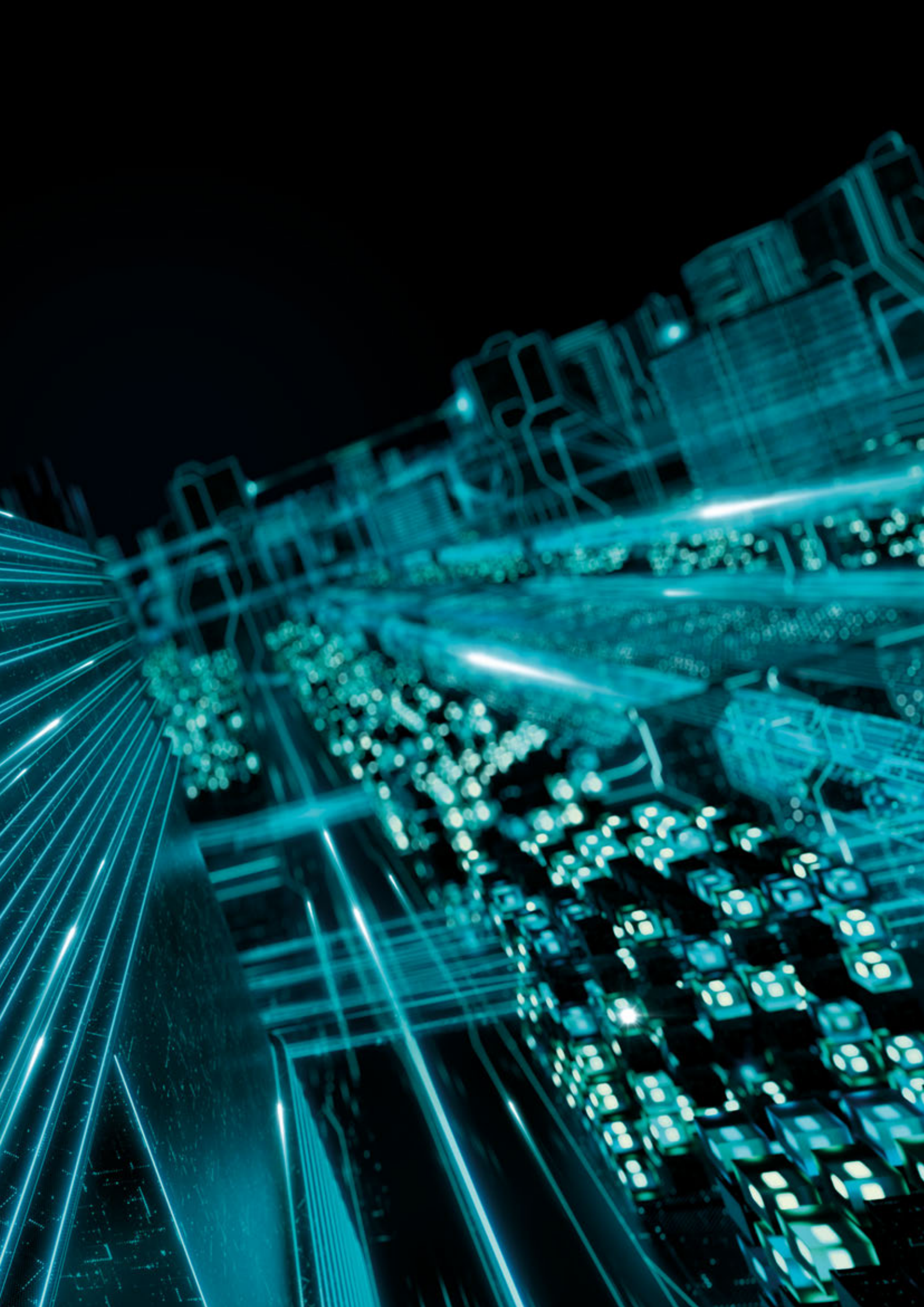
About ESET

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

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

ESET IN NUMBERS

1bn+
internet users protected

400k+
business customers

200+
countries & territories

13
global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition

protected by ESET since 2017 more than 9,000 endpoints

Allianz Suisse

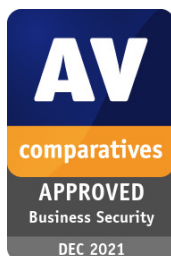protected by ESET since 2016 more than 4,000 mailboxes

Canon Marketing Japan Group

protected by ESET since 2016 more than 32,000 endpoints

T··

ISP security partner since 2008 2 million customer base

COMMITTED TO THE HIGHEST INDUSTRY STANDARDS

AV comparatives APPROVED Business Security DEC 2021

ESET received the Business Security APPROVED award from AV - Comparatives in the Business Security Test in December 2021.

G2 Leader WINTER 2022

ESET consistently achieves top rankings on the global G2 user review platform and its solutions are appreciated by customers worldwide.

FORRESTER®

ESET solutions are regularly recognized by leading analyst firms, including in "The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" as a sample vendor.