

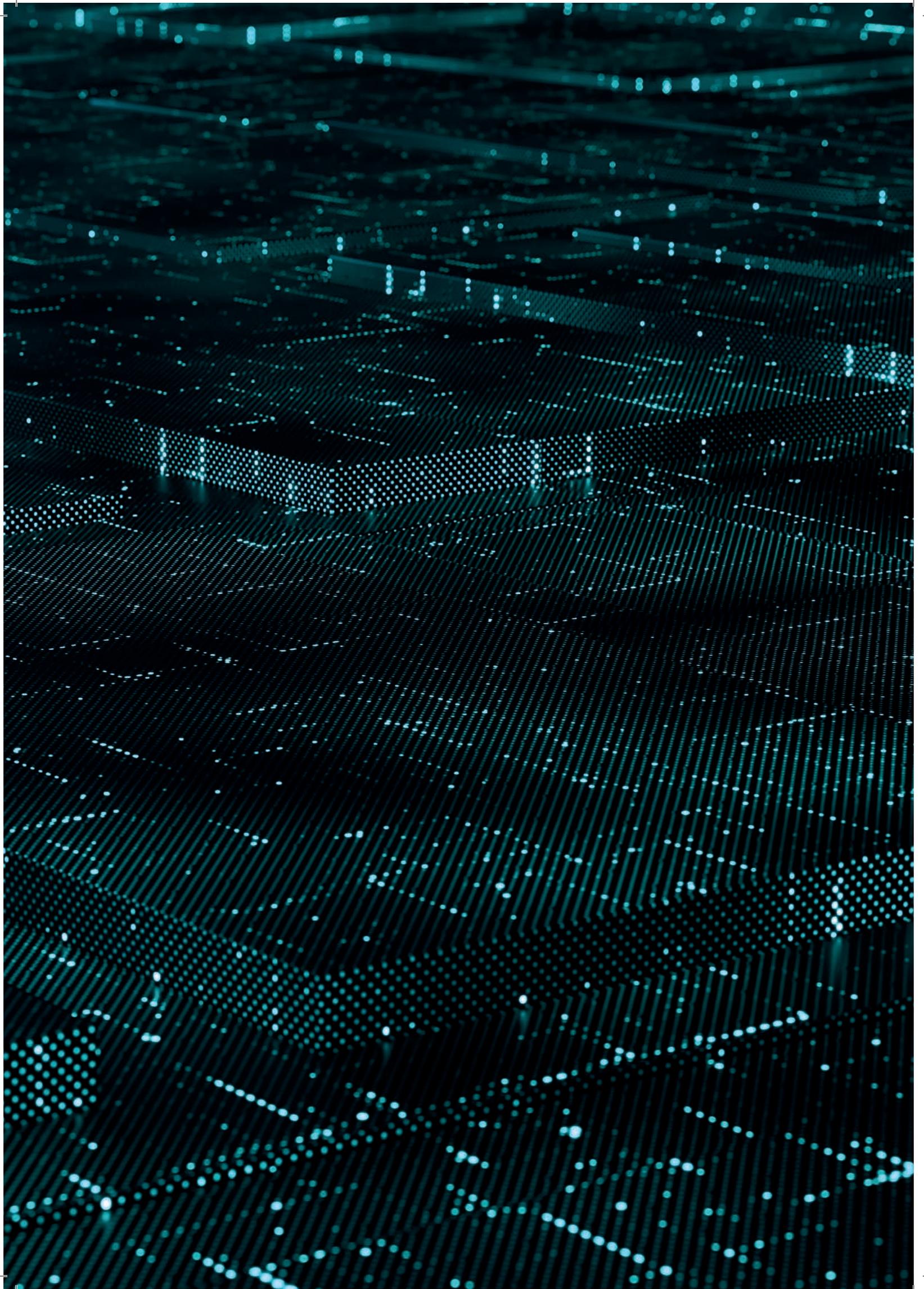
SOLUTION OVERVIEW



# ENDPOINT SOLUTIONS

Powerful multilayered protection for  
desktops, laptops and smartphones

Progress. Protected.





# 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 protection solutions leverage a multilayered approach that utilises multiple technologies working together, with 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 having existed for far longer, it was never previously seen as a major threat by businesses. However, now a single incidence of ransomware can easily render a business inoperable by encrypting important or essential files. When a business experiences a ransomware attack, it can quickly realise that the backups it has are not recent enough, thus tempting it to pay the ransom.

ESET's endpoint protection solutions provide multiple layers of defence to not just prevent ransomware but to detect it if it ever appears within an organisation. It is important to prevent and detect ransomware, as every time someone pays a ransom, it encourages the criminals to continue to utilise this mode of 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, organisations are typically surprised that their defences were compromised or are completely unaware that the attack even happened. After the attack is finally discovered, organisations then reactively implement measures to block any similar attack from being repeated. However, this does not protect them from the next attack, which may use another brand-new vector.

ESET's endpoint protection solutions use threat intelligence information based on their global presence to prioritise and effectively block the newest threats prior to their delivery anywhere else in the world. In addition, our 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 them. Furthermore, some fileless attacks will leverage currently installed applications that are built into the operating system 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 utilising this multilayered approach, we make sure we always stay one step ahead of the newest malware.



ESET's endpoint protection solutions provide multiple layers of defence to not just prevent malware but to detect it if it ever appears within an organisation.

When an attack or data breach occurs, organisations are typically surprised that their defences 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 them.

*"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



vmware®

# ESET's endpoint protection solutions

ESET Endpoint Security for Windows/macOS/Android  
ESET Endpoint Antivirus for Windows/macOS/Linux  
ESET Server Security for Windows Server/Linux/Azure  
ESET MDM for iOS and iPadOS

Product features and functionality may differ, depending on operating system.

# 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 endpoint protection products support all OSes - Windows (including Windows on ARM), macOS, Linux and Android. All our endpoint products can be fully managed from a single pane of glass; mobile device management for iOS and Android is fully built in as well.

## UNPARALLELED PERFORMANCE

A major concern for many organisations is the performance impact of their 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 a 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 to prioritise new technologies based on the most recent threats or possible new vectors.

*“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

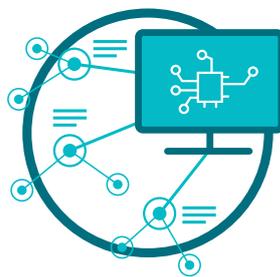
# The Technology

Our products and technologies rest on three 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 its behaviour is monitored. The 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

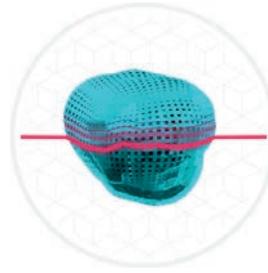
ESET's world-class security researchers share elite know-how and intelligence to ensure our users benefit from optimum, round-the-clock threat intelligence.

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.



## MACHINE LEARNING

All ESET endpoint products have been using machine learning in addition to our other layers of defence since 1997. Specifically, machine learning is used in the form of consolidated output and neural networks. For a deep inspection of the network, admins can turn on a special aggressive machine learning mode that works even without internet connection.



## ADVANCED MEMORY SCANNER

ESET Advanced Memory Scanner monitors the behaviour 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.



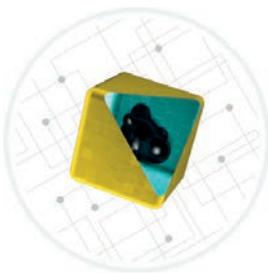
## RANSOMWARE SHIELD

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



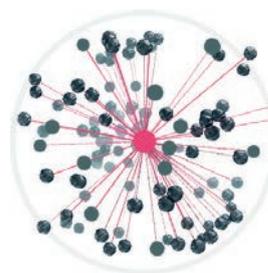
## EXPLOIT BLOCKER

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.



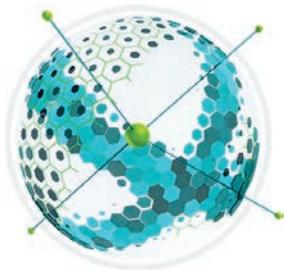
## IN-PRODUCT SANDBOX

Today's malware is often heavily obfuscated and tries to evade detection as much as possible. To see through this and identify the real behaviour 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 virtualised environment.



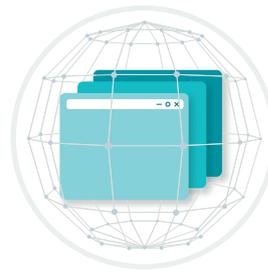
## BOTNET PROTECTION

ESET Botnet Protection detects malicious communication used by botnets, and at the same time 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 the spread of malware, network-conducted attacks, and exploitation of vulnerabilities for which a patch has not yet been released or deployed.



## SECURE BROWSER

Designed to protect organisation's assets with a special layer of protection that focuses on the browser, as the main tool used to access critical data inside the intranet perimeter and in the cloud. Secure Browser provides enhanced memory protection for the browser process, coupled with keyboard protection, and lets admins add URLs to be protected by it.



## HIPS

ESET's Host-Based Intrusion Prevention System monitors system activity and uses a predefined set of rules to recognize suspicious system behaviour. Moreover, the HIPS self-defence 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.

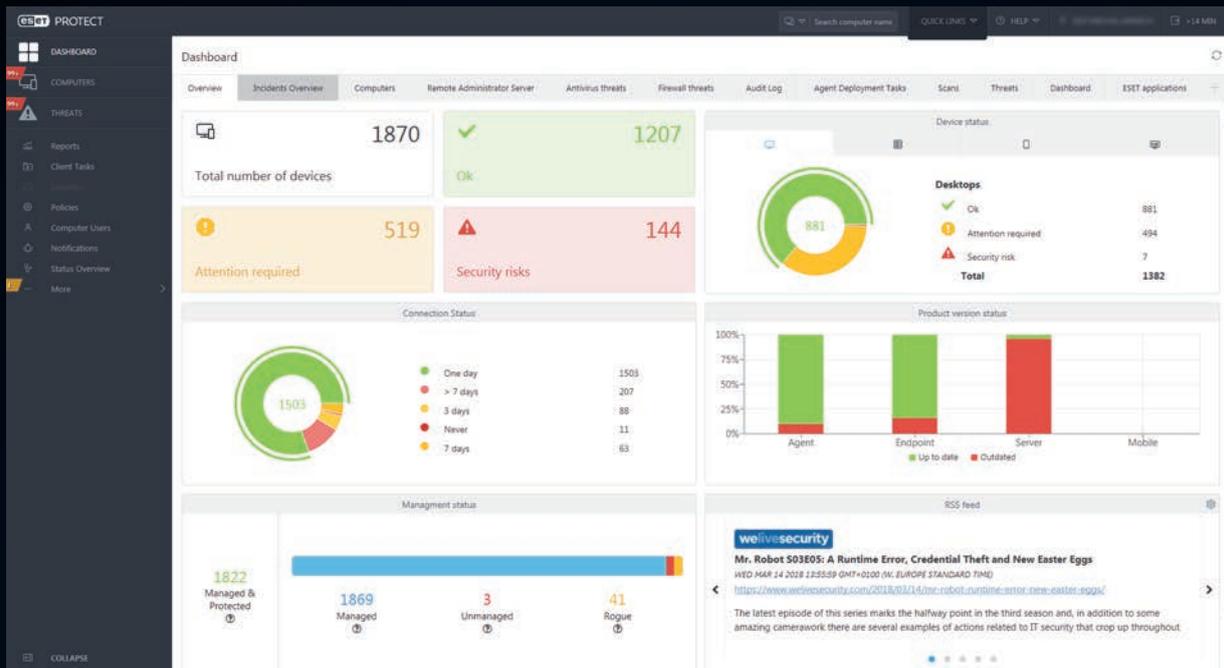


## BRUTE FORCE ATTACK PROTECTION

A security feature that protects devices against potential guessing of credentials and illegitimate establishment of a remote connection. Protection can be easily configured through a policy directly from the console, and exclusions can be created when something is blocked but shouldn't be.

*"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 ESET PROTECT console – which can be cloud-based or on-premises - ensuring a complete overview of your network.

# Use cases

## Ransomware

Some businesses want extra assurance 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 defence 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 ESET users are protected from malicious file encryption.

## Fileless malware

Fileless malware is a relatively new threat and, as it exists only in memory, requires a different approach compared to traditional file-based malware.

### SOLUTION

- ✓ A unique ESET technology, Advanced Memory Scanner, protects against this type of threat by monitoring the behaviour of malicious processes and scanning them once they decloak in memory.
- ✓ Reduce data gathering and investigation time by uploading the threat to ESET Threat Intelligence in order to provide information about how it functions.
- ✓ Multilayered technology, machine learning and human expertise provide our customers with the best level of protection possible.

## Stolen credentials

Phishing attacks and fake websites mimicking real organizations to steal login credentials and financial data are on the rise.

### SOLUTION

- ✓ ESET endpoint products are designed to protect an organisation's assets with a unique layer of protection, focusing on the browser as the primary tool to access critical data inside the intranet perimeter and in the cloud.
- ✓ Secure Browser feature protects sensitive data while browsing online.
- ✓ With a single click, administrators can choose to include all banking and payment portals and decide to protect the browser for specific websites or not.

## Password-guessing attacks

Remote Desktop Protocol (RDP) and Server Message Block (SMB) are attractive attack vectors that can allow an attacker to obtain full remote control of a system.

### SOLUTION

- ✓ Brute Force Attack Protection provides an effective defence against frontal attacks on password-protected remote access points.
- ✓ Protects devices against potential guessing of credentials and illegitimate establishment of remote connections.
- ✓ Can be easily configured through a policy directly from the console; exclusions can be created when something is blocked but shouldn't be.
- ✓ Versatile: users can add their own rules or modify existing ones.



*“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

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



protected by ESET  
since 2017 more than  
9,000 endpoints



protected by ESET  
since 2016 more than  
4,000 mailboxes



Canon Marketing Japan Group

protected by ESET  
since 2016 more than  
32,000 endpoints



ISP security partner  
since 2008 2 million  
customer base

## COMMITTED TO THE HIGHEST INDUSTRY STANDARDS



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



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



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.



**eset**<sup>®</sup> Digital Security  
Progress. Protected.