ESET®

ENDPOINT SECURITY

Powerful multilayered protection
for desktops and laptops

Progress. Protected.

What is **Modern Endpoint Protection?**

Modern endpoint protection 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.

ESET's endpoint protection solutions

✓ **ESET Endpoint Security for Windows**

✓ **ESET Endpoint Security for macOS**

✓ **ESET Endpoint Antivirus for Windows**

✓ **ESET Endpoint Antivirus for macOS**

✓ **ESET Endpoint Antivirus for Linux**

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

ESET Digital Security
Progress. Protected.

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

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 lightweight our endpoints are on systems.

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.

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.

All ESET endpoint protection solutions are managed from a single ESET PROTECT console—which can be cloud-based or on-premises—ensuring that you have a complete overview of your network.

Our unique, multilayered approach to security

ESET LiveSense technology, combined with our machine learning expertise, cloud reputation system, and our people, together power the world's most formidable cyber threat prevention, detection and response platform.

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.
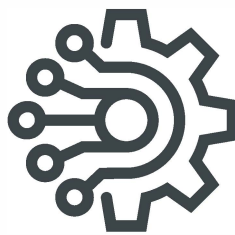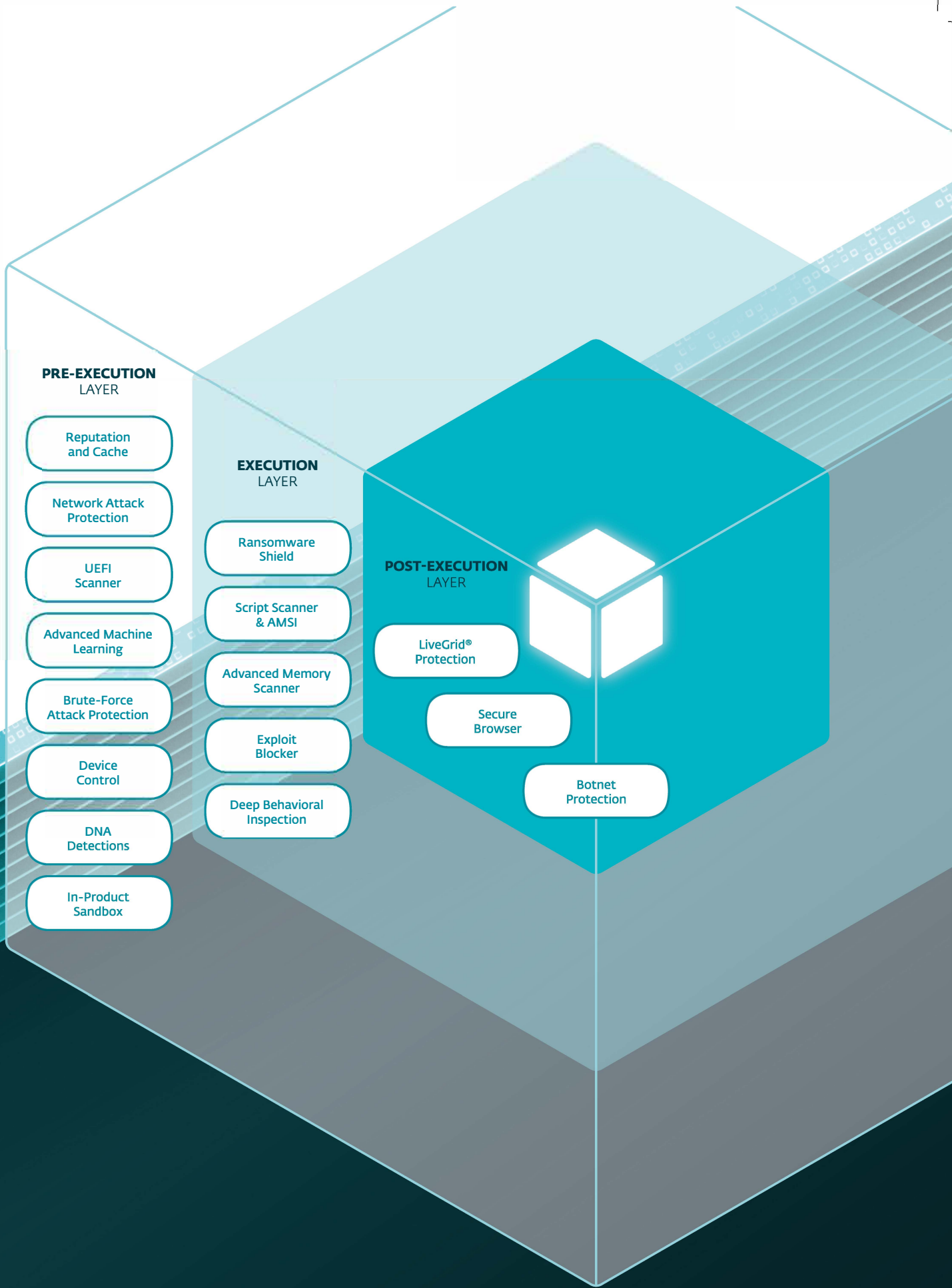
MACHINE LEARNING

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.

ESET® Digital Security **Progress. Protected.**

PRE-EXECUTION
LAYER

Reputation
and Cache

Network Attack
Protection

UEFI
Scanner

Advanced Machine
Learning

Brute-Force
Attack Protection

Device
Control

DNA
Detections

In-Product
Sandbox

EXECUTION
LAYER

Ransomware
Shield

Script Scanner
& AMSI

Advanced Memory
Scanner

Exploit
Blocker

Deep Behavioral
Inspection

POST-EXECUTION
LAYER

LiveGrid®
Protection

Secure
Browser

Botnet
Protection

These are some of ESET LiveSense core technologies and indicate approximately when and where they detect and block threats, covering the entire threat lifecycle in the system—from its pre-boot to resting state. Learn more

eseT ®
Digital Security
Progress. Protected.

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.

SECURE BROWSER

Designed to protect an 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.

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.

RANSOMWARE SHIELD

The 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.
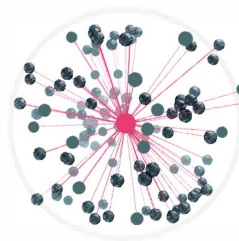
BOTNET PROTECTION

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.

HIPS

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

★ ★ ★ ★ ★

"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 for Group IT,
Mercury Engineering (Ireland), 1300 seats

(eset) ® Digital Security
Progress. Protected.

Use Cases

Ransomware

PROBLEM

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 a Ransomware Shield to ensure that ESET users are protected from malicious file encryption.

Password-guessing attacks

PROBLEM

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.

Stolen credentials

PROBLEM

Phishing attacks and fake websites mimicking real organisations 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.

Fileless malware

PROBLEM

Fileless malware is a relatively new threat and, as it exists only 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 behaviour of malicious processes and scanning them once they decloak in memory.

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

About ESET

WHEN TECHNOLOGY ENABLES PROGRESS, ESET® IS HERE TO PROTECT IT.

ESET brings over 30 years of technology-driven innovation and provides the most advanced cybersecurity solutions on the market. Our modern endpoint protection is powered by unique ESET LiveSense® multilayered security technologies, combined with the continuous use of machine learning and cloud computing. Backed by the world's best threat intelligence and research, ESET products offer the perfect balance of prevention, detection and response capabilities. With high usability and unparalleled speed, we are dedicated to protecting the progress of our customers, ensuring maximum protection.

ESET IN NUMBERS

1bn+
protected
internet users

400k+
business
customers

195
countries and
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
Canon Marketing Japan Group

protected by ESET since 2016
more than 32,000 endpoints

T · ·

ISP security partner since 2008
2 million customer base

RECOGNITION

AV comparatives
APPROVED
Business Security
DEC 2022

ESET received the Business Security APPROVED award from AV - Comparatives in the Business Security Test in December 2022.

Leader
SPRING
2023

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

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET has been recognised as a 'Top Player' for the fourth year in a row in Radicati's 2023 Advanced Persistent Threat Market Quadrant.