TUDORVALE

OVERVIEW

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 Linux**

Product features and functionality may differ depending on operating system and purchased subscription tier.

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 13 countries worldwide, 11 R&D labs and a presence in 178 countries. 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.

Windows Mac iOS Android vmware

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.

★★★★★

"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

Industry-leading technology from ESET

AI-native, multilayered approach to digital security

Our proprietary technology, ESET LiveSense®, features several layers of protection. It works alongside ESET LiveGrid®, our cloud-powered threat hunting technology, which collects and analyses a vast array of suspicious samples. Combined with AI and our human expertise, ESET's security solutions offer real-time protection against everevolving cyber threats.

ARTIFICIAL INTELLIGENCE

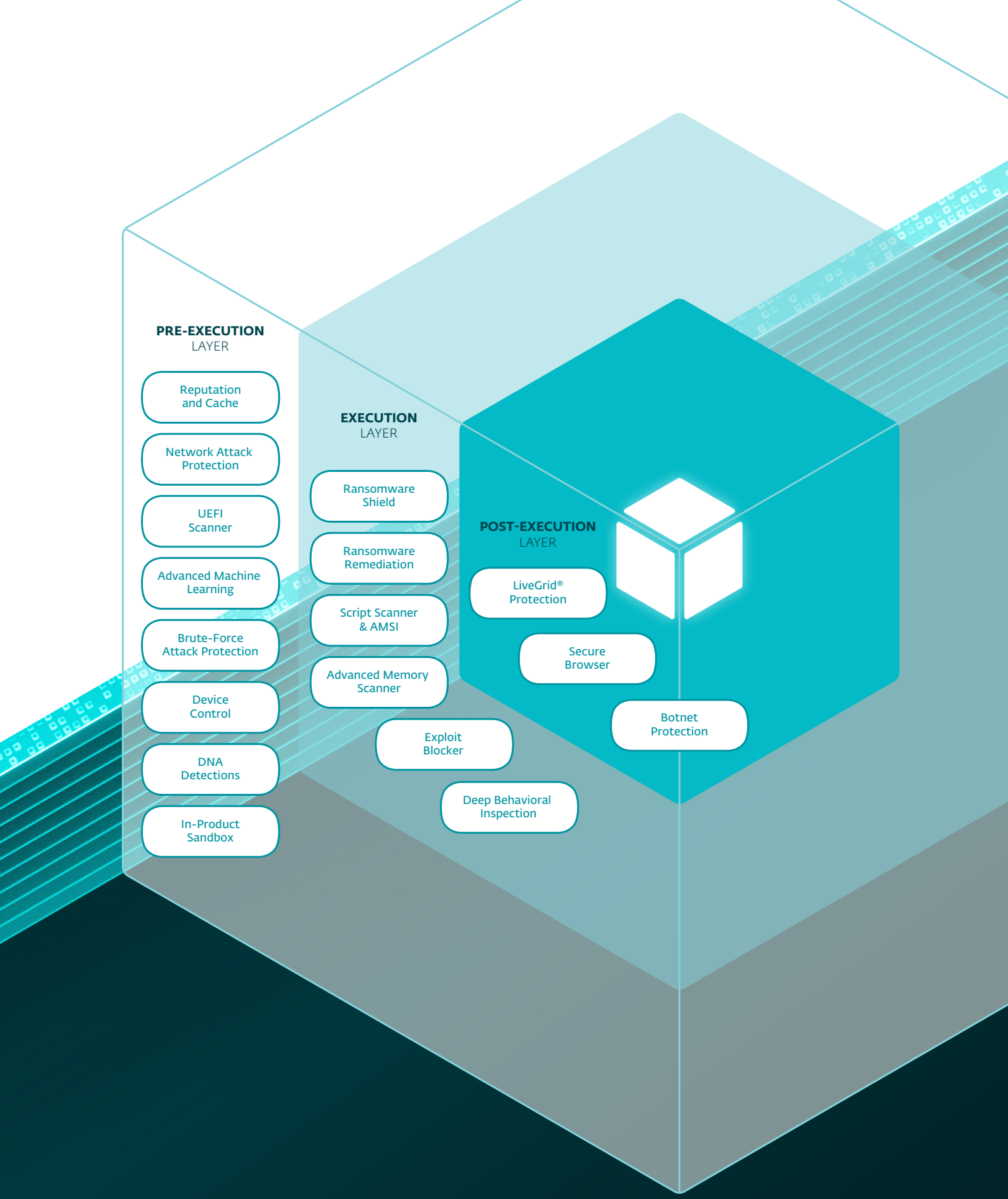
Uses the combined power of neural networks and handpicked algorithms to correctly label incoming samples as clean, potentially unwanted or malicious. To offer the best detection rates and lowest possible number of false positives, ESET Augur, our machine-learning engine, is fine tuned to cooperate with other protective technologies such as DNA, sandbox and memory analysis, to extract behavioural features.

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.

HUMAN EXPERTISE

It's not all about technology. ESET invests heavily in its people to ensure we have an educated and trained workforce that wants to stay with the company. Worldclass security researchers share their knowledge to ensure the best roundtheclock global threat intelligence.



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

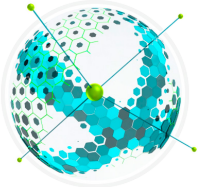
Cybersecurity
Progress. Protected.

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.

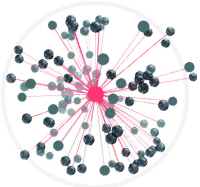
RANSOMWARE SHIELD

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 behaviour of ransomware.

RANSOMWARE REMEDIATION NEW

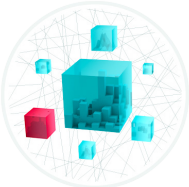
Comprehensive rollback through seamless, automated file restoration from secure backups, minimising the impact of ransomware attacks. This proprietary feature complements Ransomware Shield protection with advanced detection and remediation technologies, surpassing the Volume Shadow Copy Service by other vendors.

Note: Included in ESET PROTECT Advanced and higher subscription tiers.



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.

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.
- ✓ Automatically restore any compromised files with the Ransomware Remediation feature (included in ESET PROTECT Advanced and higher subscription tiers).

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.

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.

This is ESET

Proactive defence. Minimise risks with prevention.

Stay one step ahead of known and emerging cyber threats—targeted attacks, zero-day threats, ransomware, phishing, and more—with our AI-Native, prevention-first approach. ESET combines the power of AI and human expertise to deliver easy and effective protection.

Experience best-in-class, science-driven security, backed by over 30 years of in-house global cyber threat intelligence. Our extensive R&D network, led by industry-acclaimed researchers, powers our award-winning, cloud-first cybersecurity platform. ESET solutions are highly customizable, include local support, and have minimal impact on performance.

ESET protects your business so you can unlock the full potential of technology.

ESET IN NUMBERS

1bn+
protected internet users

500k+
business customers

178
countries

11
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

ISP security partner since 2008
2 million customer base

RECOGNITION

AV comparatives APPROVED Business Security JUL 2024

ESET is a consistent **top-performer in independent tests** by AV-Comparatives and achieves best detection rates with no or minimal false positives.

SUMMER 2025 Grid Leader

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

IDC ANALYZE THE FUTURE

ESET has been recognised as a Leader in endpoint security in the IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses 2024 Vendor Assessment.

For more information please contact,
Andrew Jones | CEO | Tudorvale Limited
Phone: +447802287738
Email: aj@tudorvale.com