OVERVIEW

LIVEGUARD ADVANCED

Proactive cloud-based threat prevention with autonomous remediation

Progress. Protected.

What is **advanced threat defence?**

A proactive technology that uses advanced adaptive scanning, cutting-edge artificial intelligence, cloud sandboxing and in-depth behavioural analysis to prevent targeted attacks as well as new, never-before-seen threat types, especially ransomware. ESET provides cloud-based advanced threat prevention with autonomous remediation capabilities and cloud-driven threat hunting. A detailed overview of the global malware landscape enables real-time protection against ever-evolving cyber threats.

ESET LiveGuard Advanced provides another layer of security for ESET Mail Security, ESET Endpoint Security and ESET Cloud Office Security. Its cloud-based advanced technology consists of multiple types of sensors that complete static analysis of code, deep inspection of the sample with machine learning, in-memory introspection and behaviour-based detection.

Why use **proactive cloud-based threat defence?**

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 not previously 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 realises that the backups it has are not recent enough, so it may feel compelled to pay the ransom.

Proactive cloud-based threat detection with autonomous remediation provides an additional layer of defence outside of a company's network, to prevent ransomware from ever executing in a production environment.

TARGETED ATTACKS AND DATA BREACHES

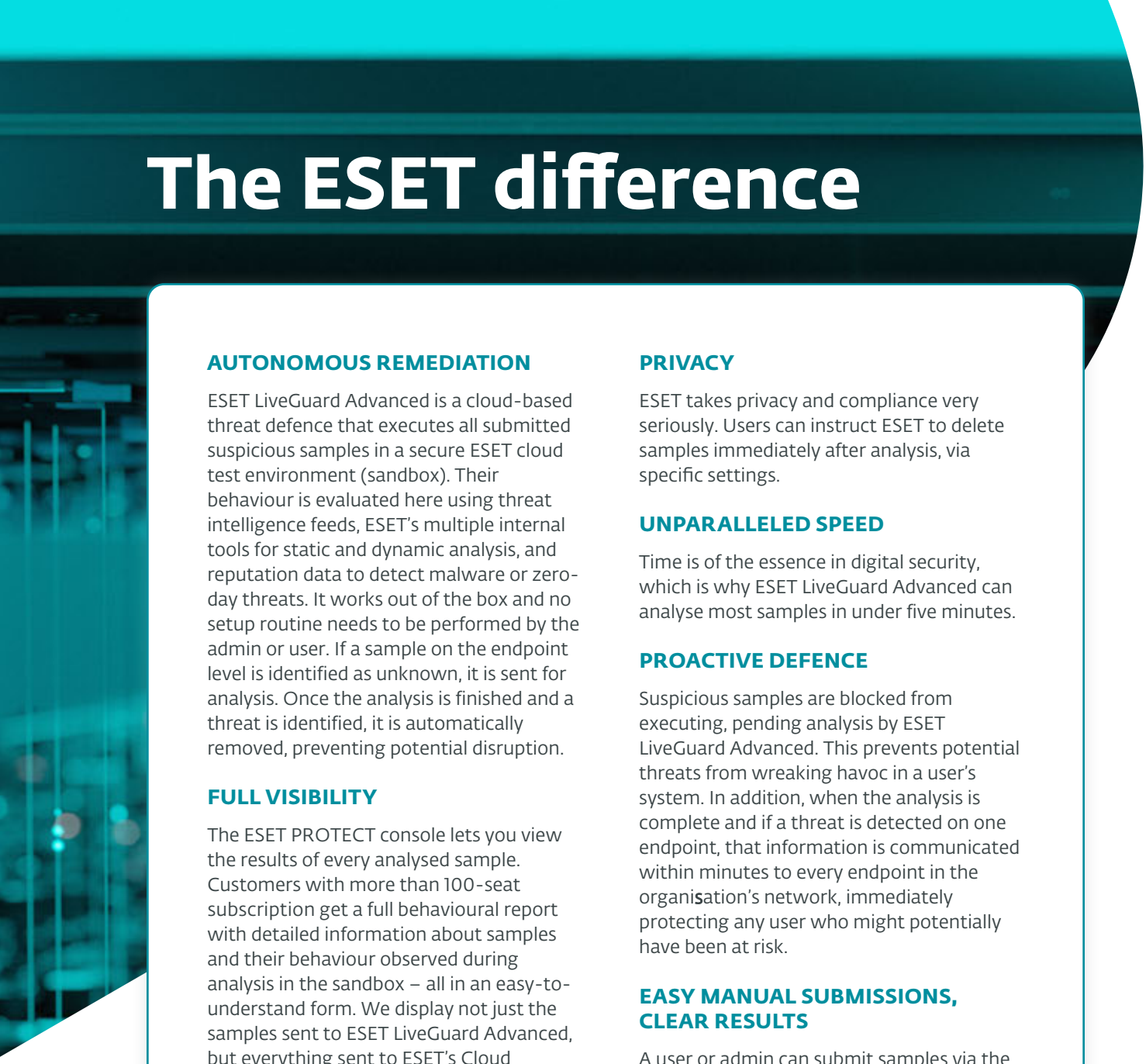
Today's cybersecurity landscape is constantly evolving with new attack methods and never-before-seen threats. When an attack or data breach occurs, organisations are typically surprised that their defences were compromised or are completely unaware that the attack even happened. After the attack is finally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

A cloud security sandbox's approach is much more effective than just looking at the appearance of the potential threat, because it goes beyond just the mere form and instead observes what the potential threat does. This helps it to be much more conclusive when determining if something is a targeted attack, an advanced persistent threat, or benign.

Static and dynamic analysis is performed by an array of machine-learning algorithms, using techniques including deep learning.

A cloud security sandbox outside the user's network can go beyond just analysing appearance, and instead observe what the potential threat actually does.

The ESET difference



AUTONOMOUS REMEDIATION

ESET LiveGuard Advanced is a cloud-based threat defence that executes all submitted suspicious samples in a secure ESET cloud test environment (sandbox). Their behaviour is evaluated here using threat intelligence feeds, ESET's multiple internal tools for static and dynamic analysis, and reputation data to detect malware or zero-day threats. It works out of the box and no setup routine needs to be performed by the admin or user. If a sample on the endpoint level is identified as unknown, it is sent for analysis. Once the analysis is finished and a threat is identified, it is automatically removed, preventing potential disruption.

FULL VISIBILITY

The ESET PROTECT console lets you view the results of every analysed sample. Customers with more than 100-seat subscription get a full behavioural report with detailed information about samples and their behaviour observed during analysis in the sandbox – all in an easy-to-understand form. We display not just the samples sent to ESET LiveGuard Advanced, but everything sent to ESET's Cloud Malware Protection System – ESET LiveGrid®.

OMNIPRESENT PROTECTION

ESET technology supports your organisation's working practices. ESET LiveGuard Advanced can analyse files wherever users are located – a remote or hybrid workforce gets the same protection as office-based employees. If anything malicious is detected, the whole company is immediately protected.

PRIVACY

ESET takes privacy and compliance very seriously. Users can instruct ESET to delete samples immediately after analysis, via specific settings.

UNPARALLELED SPEED

Time is of the essence in digital security, which is why ESET LiveGuard Advanced can analyse most samples in under five minutes.

PROACTIVE DEFENCE

Suspicious samples are blocked from executing, pending analysis by ESET LiveGuard Advanced. This prevents potential threats from wreaking havoc in a user's system. In addition, when the analysis is complete and if a threat is detected on one endpoint, that information is communicated within minutes to every endpoint in the organisation's network, immediately protecting any user who might potentially have been at risk.

EASY MANUAL SUBMISSIONS, CLEAR RESULTS

A user or admin can submit samples via the ESET PROTECT console for analysis and get the complete results at any time. Admins will see who sent what and what the result was.

ENHANCED EMAIL PROTECTION

ESET LiveGuard Advanced goes beyond file analysis – it works directly with ESET Mail Security or ESET Cloud Office Security to prevent the delivery of malicious emails to your organisation. To support business continuity, only external emails can be sent to ESET LiveGuard Advanced for inspection.

Use cases

Ransomware

PROBLEM

Ransomware tends to enter unsuspecting users' mailboxes through email.

SOLUTION

- ✓ ESET Mail Security automatically submits suspicious email attachments to ESET LiveGuard Advanced.
- ✓ ESET LiveGuard Advanced analyses the sample, then submits the result back to ESET Mail Security, usually within 5 minutes.
- ✓ ESET Mail Security detects and automatically remediates attachments that contain the malicious content.
- ✓ The malicious attachment never reaches the recipient.

Unknown or questionable files

PROBLEM

Sometimes employees or IT might receive a file that they want to double-check is safe.

SOLUTION

- ✓ Any user can submit a sample for analysis directly within all ESET products.
- ✓ The sample is quickly analysed by ESET LiveGuard Advanced.
- ✓ If a file is determined to be malicious, all computers in the organisation are protected.
- ✓ IT admin has full visibility into the user who submitted the sample, and whether the file was clean or malicious.

Granular protection for different company roles

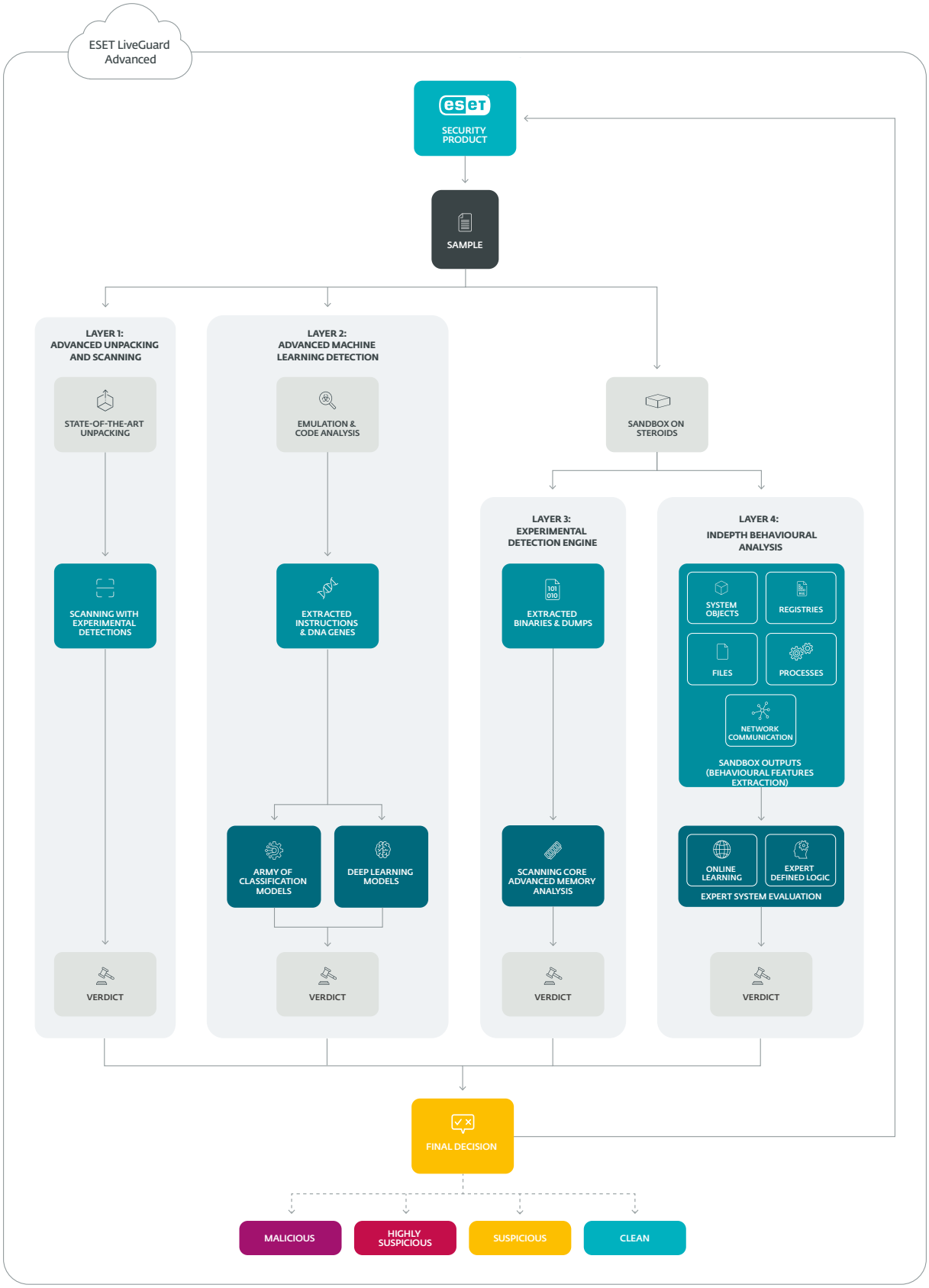
PROBLEM

Every role in the company requires different levels of protection. Developers or IT employees require different security restrictions than the office manager or CEO.

SOLUTION

- ✓ Configure a unique policy per computer or per server in ESET LiveGuard Advanced.
- ✓ Automatically apply a different policy based off a different static user group or Active Directory group.
- ✓ Automatically change configuration settings simply by moving a user from one group to another.

How our advanced analysis works



ESET LiveGuard Advanced uses 4 separate detection layers to ensure the highest detection rate. Each layer uses a different approach and delivers a verdict on the sample. The final assessment comprises the results of all information about the sample.

LAYER 1

Advanced unpacking and scanning

Samples undergo static analysis and state-of-the-art unpacking and are then matched against an enriched threat database.

LAYER 2

Advanced machine learning detection

Static and dynamic analysis is performed by an array of machine learning algorithms, using techniques including deep learning.

LAYER 3

Experimental detection engine

Samples are inserted into "sandboxes on steroids" that closely resemble full-scale user devices. They are subsequently monitored for any sign of malicious behaviour.

LAYER 4

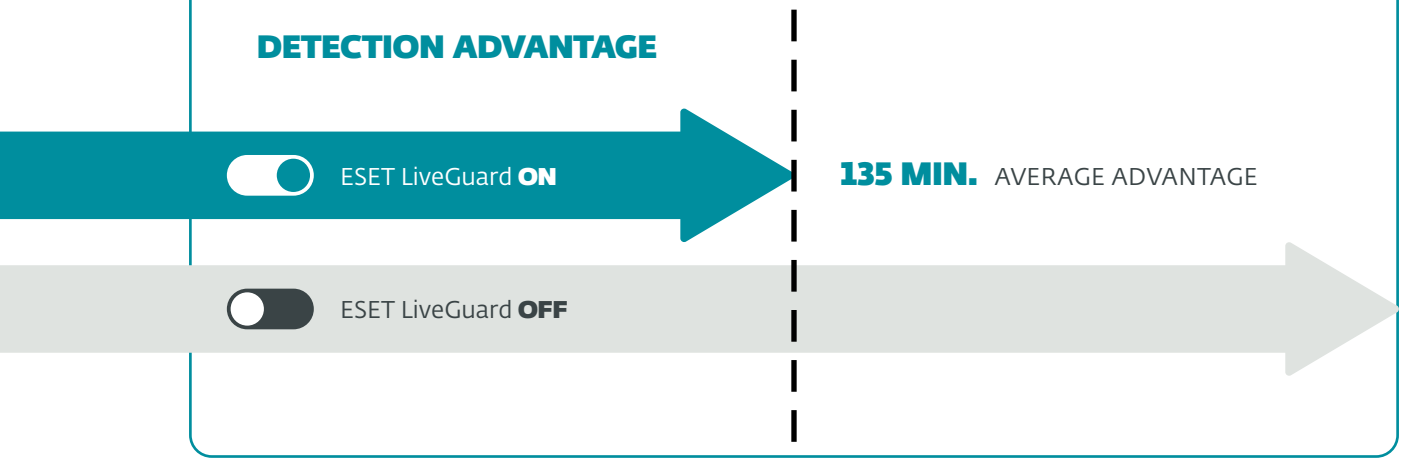
In-depth behavioural analysis

All sandbox outputs are subject to an in-depth behavioural analysis that identifies known malicious patterns and chains of actions.

THE SOLUTION COMBINES ALL AVAILABLE VERDICTS FROM THE DETECTION LAYERS AND EVALUATES EACH SAMPLE'S STATUS. THE RESULTS ARE DELIVERED TO THE USER'S ESET SECURITY APPLICATION AND COMPANY INFRASTRUCTURE FIRST, AND RESPECTIVE MITIGATION IS APPLIED AUTOMATICALLY.

UNPARALLELED SPEED

Dedicated cloud sandbox analysis in under 5 minutes



eset Digital Security
Progress. Protected.

This is ESET

Proactive defence. Minimise risks with prevention.

Stay one step ahead of known and emerging cyber threats with our AI-native, prevention-first approach. We combine the power of AI and human expertise to make protection easy and effective.

Experience best-in-class protection thanks to our in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers.

ESET PROTECT, our cloud-first XDR cybersecurity platform, combines next-gen prevention, detection, and proactive threat hunting capabilities with a broad variety of security services, including managed detection and response.

Our highly customisable solutions include local support and have minimal impact on performance, identify and neutralise known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

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

ESET IN NUMBERS

1bn+
protected internet users

400k+
business customers

200
countries and territories

13
global R&D centres

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 DEC 2023

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

G2 Leader WINTER 2024

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

kuppingercole ANALYSTS

ESET is **recognised as a Market Leader** and an Overall Leader in MDR, according to the KuppingerCole Leadership Compass 2023.