SOLUTION OVERVIEW

LIVEGUARD ADVANCED

Proactive defence against zero-day and never-before-seen threat types

Progress. Protected.

What is **advanced threat defence?**

A proactive cloud-based technology that uses advanced adaptive scanning, cutting-edge machine learning, cloud sandboxing and in-depth behavioural analysis to prevent targeted attacks as well as new, never-before-seen threat types, especially ransomware.

ESET LiveGuard Advanced provides another layer of security for ESET products like Mail Security, Endpoint products and 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 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, it quickly realises that the backups it has are not recent enough, so the business feels as though it must pay the ransom.

A proactive cloud-based threat detection product 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, organizations 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 that 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 appearance and instead observes what the potential threat does. This helps it be much more conclusive when determining if something is a targeted attack, advanced persistent threat, or benign.

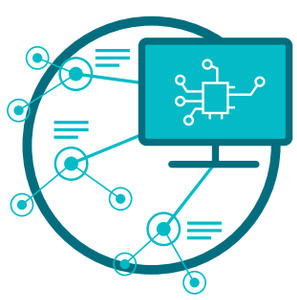
Static and dynamic analysis is performed by an array of machine-learning algorithms, using techniques including deep learning.

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

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 behaviour 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.

The ESET difference

MULTILAYERED PROTECTION

ESET LiveGuard Advanced is a cloud-based threat defence solution that executes all submitted suspicious samples to a secure test environment at ESET HQ, where their behaviour is evaluated using threat intelligence feeds, ESET's multiple internal tools for static and dynamic analysis, and reputation data to detect zero-day threats. Four layers are used to analyse samples, which can be deployed dynamically depending on the results that emerge. ESET LiveGuard Advanced combines all verdicts from the detection layers and evaluates each sample's status. The results are delivered first to the user's ESET security product and their company's infrastructure.

FULL VISIBILITY

For every analysed sample, you can view the final result in the ESET PROTECT console. On top of that, customers with more than 100-seat licence 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. Not only do we simply display samples that were sent to ESET LiveGuard Advanced but everything that is sent to ESET's Cloud Malware Protection System – ESET LiveGrid®.

MOBILITY

Nowadays, employees in organisations are increasingly working remotely and not on-premises. That is why ESET LiveGuard Advanced can analyse files no matter where users are. The best part is that if anything malicious is detected, the whole company is immediately protected.

PRIVACY

ESET takes privacy and compliance very seriously. Via specific settings, the user can instruct ESET to delete samples immediately after analysis.

UNPARALLELED SPEED

Every minute counts, which is why ESET LiveGuard Advanced is able to analyse the majority of samples in under 5 minutes. If a sample was previously analyzed, it is simply a few seconds until all devices at your organization are protected.

PROVEN AND TRUSTED

ESET has been in the security industry for over 30 years, and we continue to evolve our technology to stay one step ahead of the newest threats. As a result, 1 billion internet users worldwide are now protected by ESET. Our technology is constantly scrutinised and validated by third-party testers who show how effective our approach is at stopping the latest threats.

PROACTIVE DEFENCE

If a sample is found to be suspicious it is 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.

Use cases

Ransomware

USE CASE

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 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.

Granular protection for different company roles

USE CASE

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.

Unknown or questionable files

USE CASE

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.

ESET LiveGuard Advanced features

AUTOMATIC PROTECTION

Once everything is set up, there is no action needed by the admin or the user. The endpoint or server product automatically decides whether a sample is good, bad or unknown. If the sample is unknown, it is sent to ESET LiveGuard Advanced for analysing. Once analysis is finished, the result is shared and the endpoint products respond accordingly.

TAILORED CUSTOMISATION

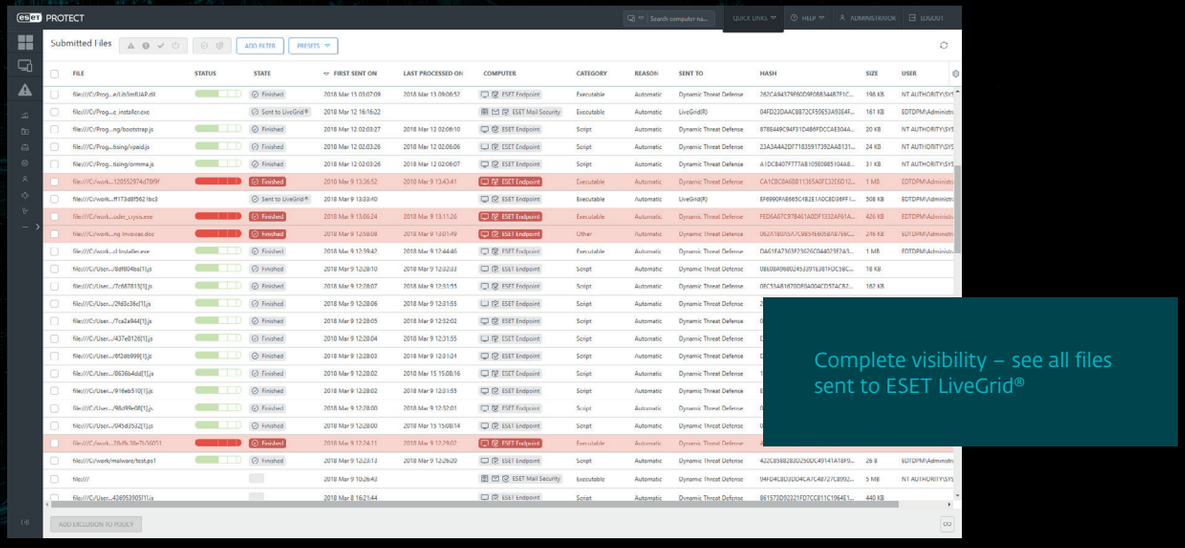
ESET allows per-computer detailed policy configuration for ESET LiveGuard Advanced so the admin can control what is sent and what should happen based on the result received. In addition, settings can be applied not just per computer, but also per computer group.

MANUAL SUBMISSION

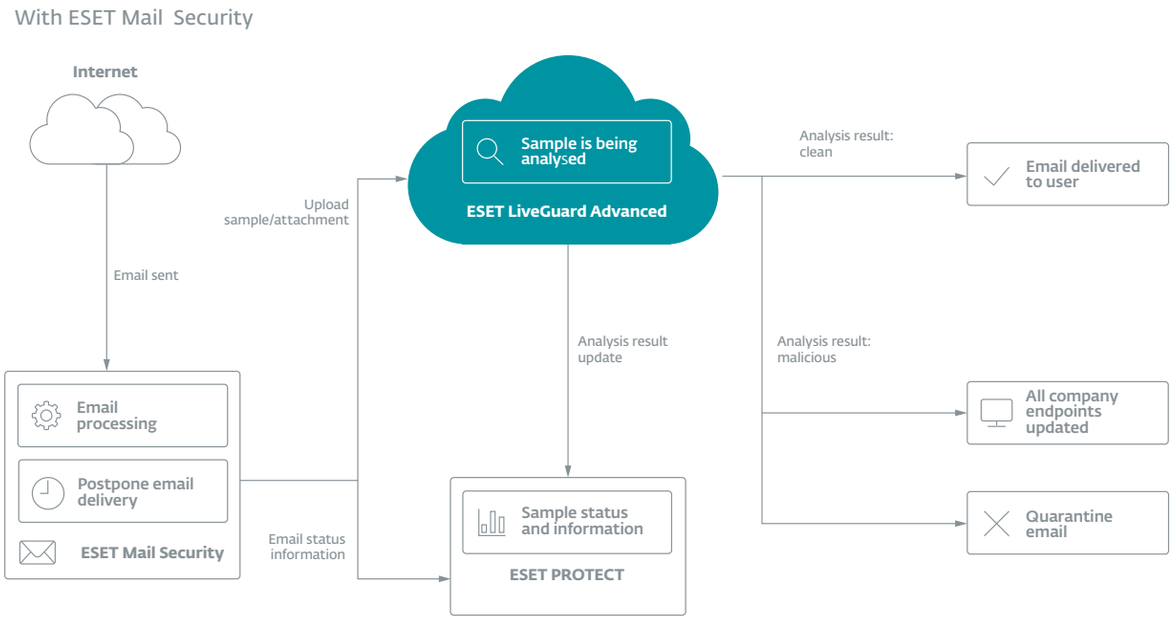
At any time, a user or admin can submit samples via an ESET compatible product for analysis and get the full result. Admins will see who sent what and what the result was directly in the ESET PROTECT console.

MAIL SECURITY PROTECTION

Not only does ESET LiveGuard Advanced work with files, but it also works directly with ESET Mail Security to ensure that malicious emails are not delivered to your organisation. To ensure business continuity, only emails coming from outside of the organisation can be sent to ESET LiveGuard Advanced for inspection.



How **ESET LiveGuard Advanced works**



ESET LiveGuard Advanced is compatible with ESET Endpoint, Server and Cloud app security (Microsoft 365) products, and is fully integrated into ESET management consoles.

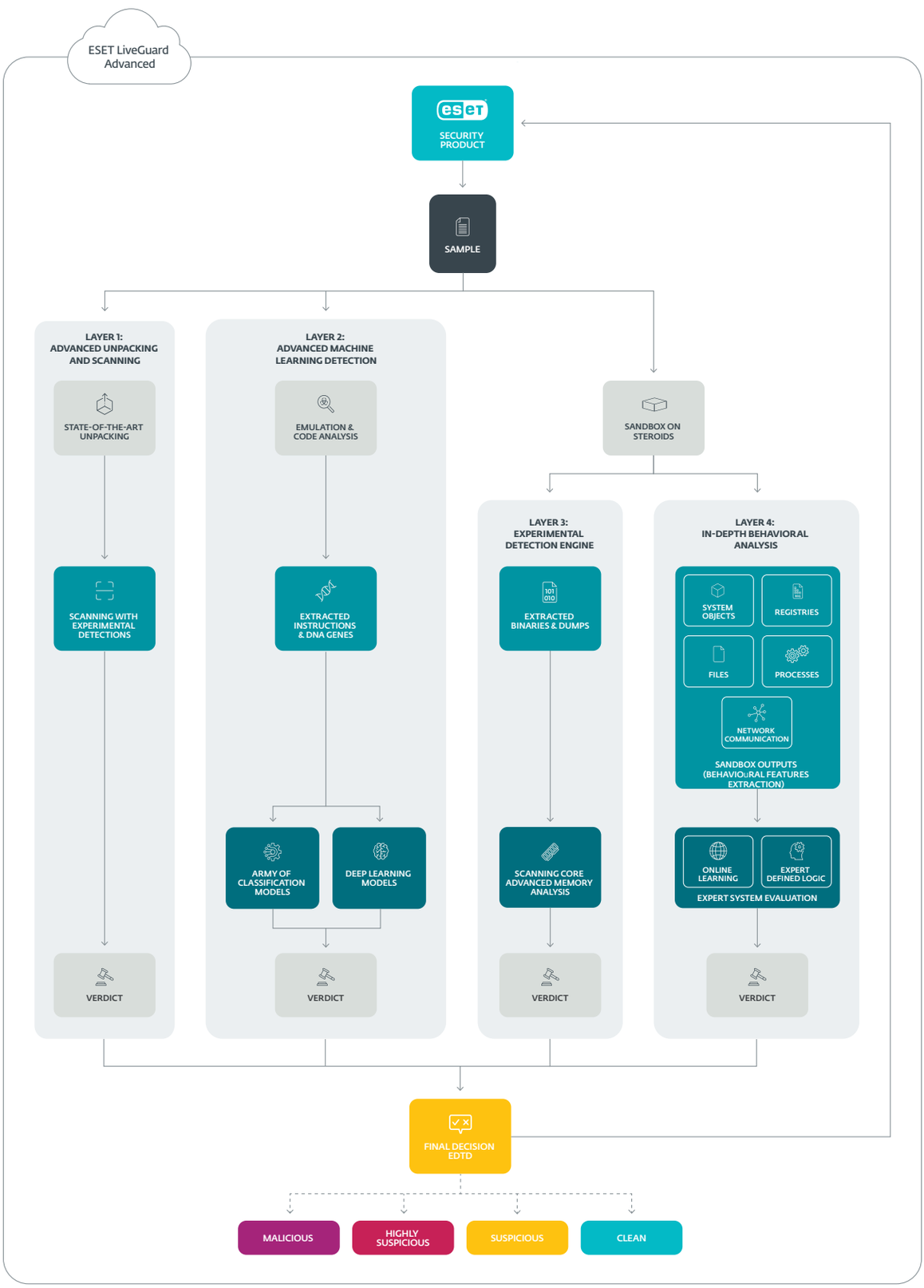
"Amazing Product!"

What do you like best?

"I like how easy it was to roll out to all my workstations and how quickly it secured my network. I have found unwanted software and see daily emails of it stopping network bugs from becoming a pain. I sleep better knowing my network is protected by ESET."

— Michael P. / Network manager / Mid-market (51-1,000 emp.)

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

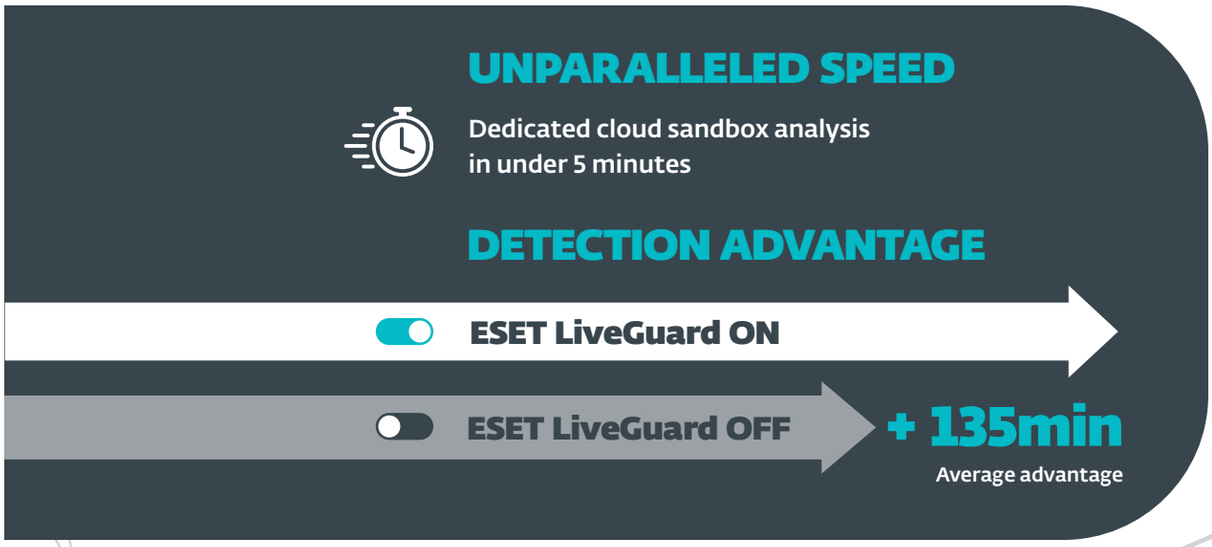
Samples are inserted into "sandboxes on steroids" that closely resemble full-scale user devices. They are subsequently monitored for any sign of malicious behaviour.

LAYER 4

In-depth behavioral 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 PRODUCT AND COMPANY INFRASTRUCTURE FIRST.



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
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.

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.

eset® Digital Security
Progress. Protected.