OVERVIEW

LIVEGUARD ADVANCED

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

Progress. Protected.

What is **advanced threat defense?**

A proactive technology that uses advanced adaptive scanning, cutting-edge machine learning, cloud sandboxing and in-depth behavioral 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 behavior-based detection.

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

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 realizes 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 defense 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 defenses were compromised or are completely unaware that the attack even happened. After the attack is finally discovered, organizations 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 THREAT HUNTING

ESET LiveGuard Advanced is a cloud-based threat defense that executes all submitted suspicious samples in a secure ESET cloud test environment (sandbox). Their behavior 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 analyzed sample. Customers with more than 100-seat licenses get a full behavioral report with detailed information about samples and their behavior 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 organization's working practices. ESET LiveGuard Advanced can analyze 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 analyze most samples in under five minutes.

PROACTIVE DEFENSE

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 organization'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 organization. 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 analyzes 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 analyzed by ESET LiveGuard Advanced.
- ✓ If a file is determined to be malicious, all computers in the organization 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

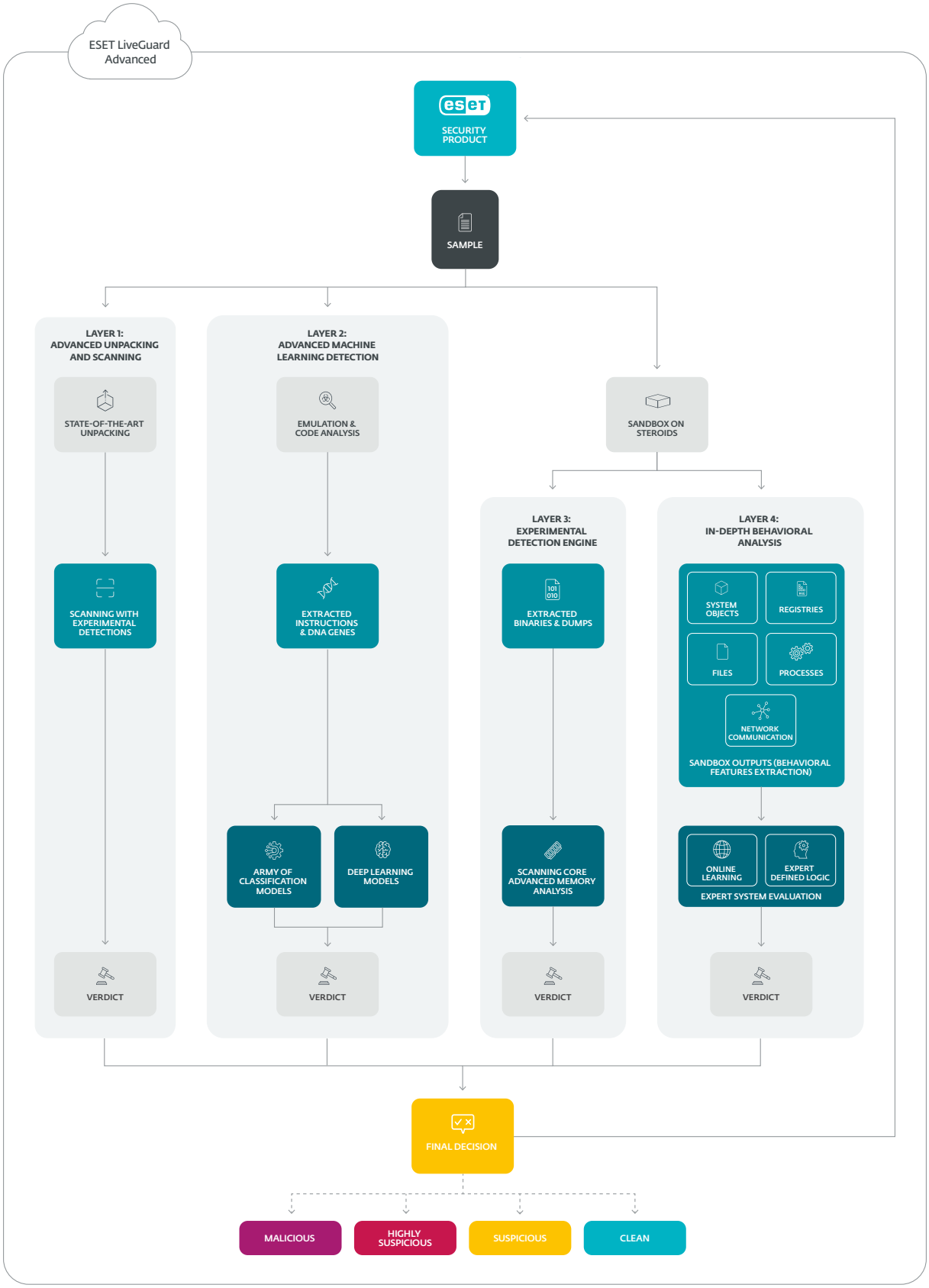
PROBLEM

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 behavior.

LAYER 4

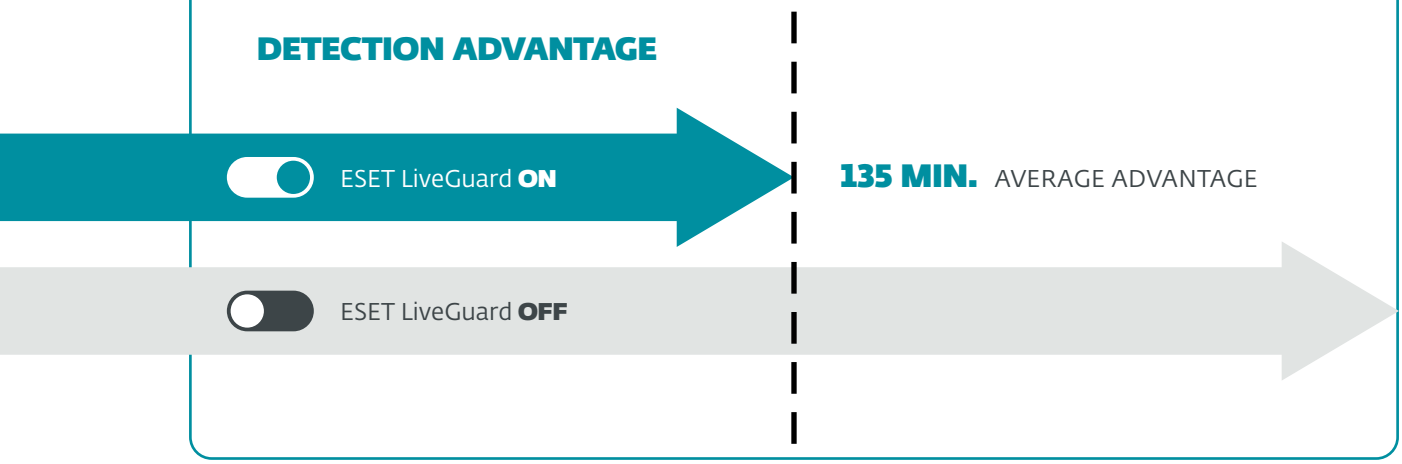
In-depth behavioral analysis

All sandbox outputs are subject to an in-depth behavioral 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.

About ESET

Next-gen digital security for business

WE DON'T JUST STOP BREACHES—WE PREVENT THEM

Unlike conventional solutions that focus on reacting to threats after they've been executed, ESET offers an unmatched AI-powered prevention-first approach backed by human expertise, renowned global Threat Intelligence, and an extensive R&D network led by industry-acclaimed researchers—all for the continuous innovation of our multilayered security technology.

Experience unparalleled protection from ransomware, phishing, zero-day threats and targeted attacks with our award-winning, cloud-first XDR cybersecurity platform that combines next-gen prevention, detection, and proactive threat hunting capabilities. Our highly customizable solutions include hyperlocal support. They offer minimal impact on endpoint performance, identify and neutralize emerging threats before they can be executed, ensure business continuity, and reduce the cost of implementation and management.

In a world where technology enables progress, protect your business with ESET.

ESET IN NUMBERS

1bn+
protected internet users

400k+
business customers

200
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
JUL 2023

ESET received the Business Security APPROVED award from AV - Comparatives in the Business Security Test in July 2023.

G2
Leader
SUMMER
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 recognized as a 'Top Player' for the fourth year in a row in Radicati's 2023 Advanced Persistent Threat Market Quadrant.