



DYNAMIC THREAT DEFENSE

Prevent zero-day threats and ransomware
with powerful cloud-based sandboxing

CYBERSECURITY
EXPERTS ON YOUR SIDE



What is a **Cloud security sandbox product?**

A cloud security sandbox is an isolated test environment in which a suspicious program is executed and its behavior is observed, noted and then analyzed in an automated manner.

ESET Dynamic Threat Defense provides another layer of security for ESET products like Mail Security and Endpoint products by utilizing a cloud-based sandboxing technology to detect new, never-before-seen types of threats, especially ransomware. This sandbox 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 a Cloud Security Sandbox?

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 realizes that the backups it has are not recent enough, so the business feels as though it must pay the ransom.

A cloud security sandbox product provides an additional layer of defense outside of a company's network to prevent ransomware from ever executing in a production environment.

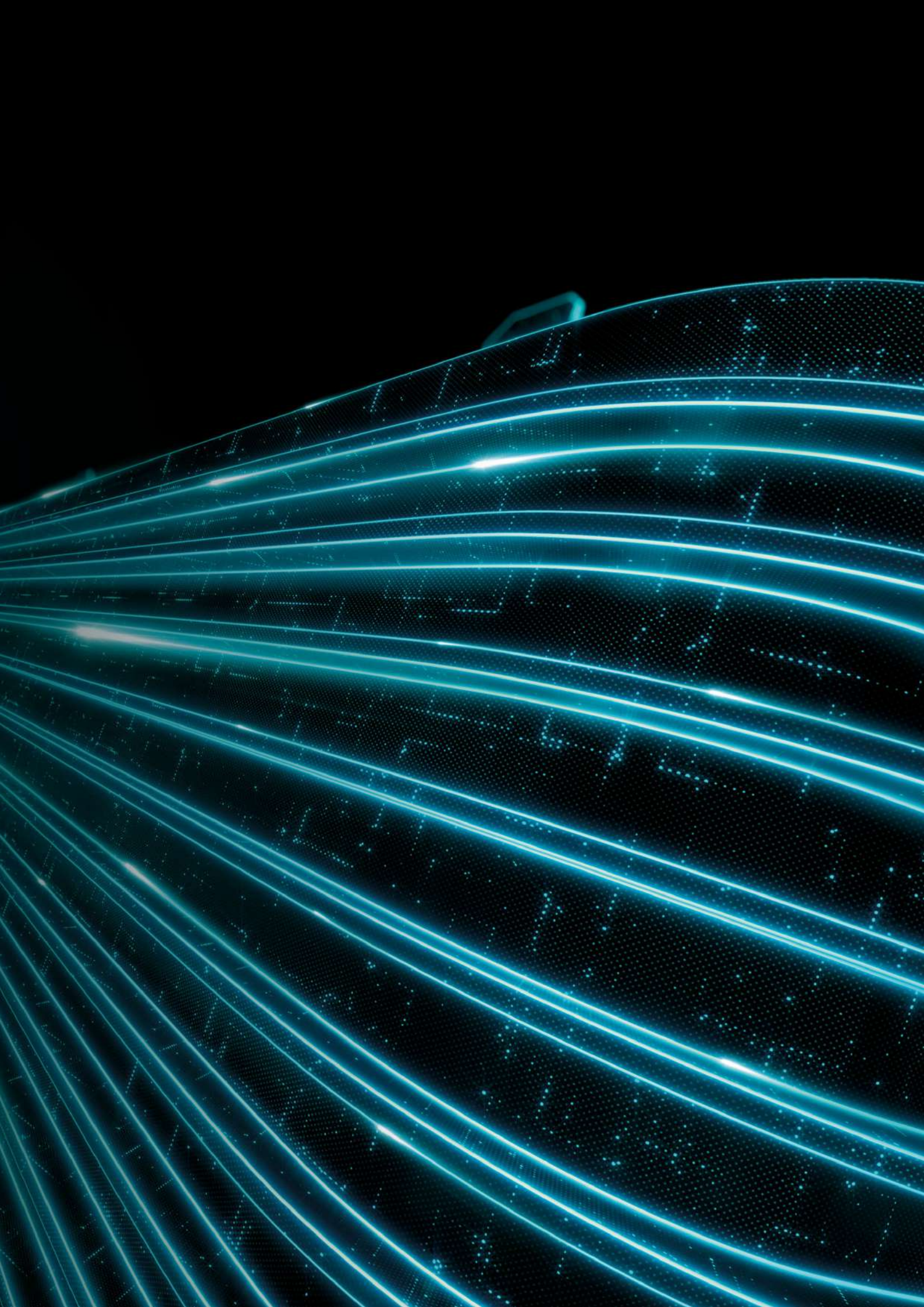
TARGETED ATTACKS AND DATA BREACHES

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 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.

A cloud security sandbox product provides an additional layer of defense outside of a company's network.

A cloud security sandbox goes beyond just the mere appearance and instead observes what the potential threat does.

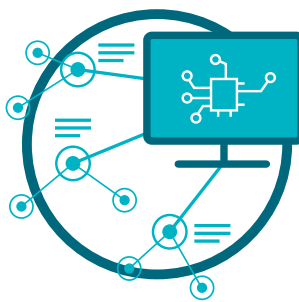


Our products and technologies stand on 3 pillars



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 behavior 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

Within Dynamic Threat Defense, ESET utilizes 3 different machine learning models once a file is submitted. After that, it runs the sample through a full sandbox which simulates user behavior to trick anti-evasive techniques. Next, a deep learning neural network is used to compare the behavior seen versus historical behavioral data. Last but not least, the latest version of ESET's scanning engine is used to take everything apart and analyzed for anything unusual.

FULL VISIBILITY

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

MOBILITY

Nowadays, customers are increasingly working remotely and not on-premise. That is why ESET Dynamic Threat Defense can analyze files no matter where users are. The best part is that if anything malicious is detected, the whole company is immediately protected.

UNPARALLELED SPEED

Every minute counts, which is why ESET Dynamic Threat Defense is able to analyze 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. This has led us to be trusted by over 110 million users worldwide. Our technology is constantly scrutinized and validated by third-party testers who show how effective our approach is at stopping the latest threats.

FILE	REMOVE	STATE	FIRST SENT ON	LAST PROCESSED ON	COMPUTER	CATEGORY	REASON	SENT TO	HASH	SIZE	USAGE
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 11 03:07:06	2018 Mar 11 03:08:10	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	167234478E0D9F9834A87E1C...	198 KB	NT AUTHORITY\SYSTEM
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 12 16:56:22		ESET PROTECT	File/Executable	Automatic	LiveGrid®	04F032A48B71C2F9E34358F4...	191 KB	ESET\PROTECT\ADMINISTRATOR
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 12 00:09:27	2018 Mar 12 00:09:10	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	E78246C4F51C489F00C4E3D4...	20 KB	NT AUTHORITY\SYSTEM
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 12 00:09:29	2018 Mar 12 00:09:08	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	E3A3A42D771E20817305A421...	24 KB	NT AUTHORITY\SYSTEM
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 12 00:09:30	2018 Mar 12 00:09:07	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	A1D3C487771A1E500451846...	31 KB	NT AUTHORITY\SYSTEM
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 13:43:12	2018 Mar 9 13:43:11	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	C41D2C3A8811182427C381D...	1 KB	ESET\PROTECT\ADMINISTRATOR
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:25:49	2018 Mar 9 10:25:49	ESET PROTECT	File/Executable	Automatic	LiveGrid®	0F808F1880C492145C208FF...	908 KB	ESET\PROTECT\ADMINISTRATOR
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:25:24	2018 Mar 9 10:25:23	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	F0A8C7C7B1A102D73320F0A...	622 KB	ESET\PROTECT\ADMINISTRATOR
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:25:08	2018 Mar 9 10:25:08	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	18C7F8C351F02A4883810234...	248 KB	ESET\PROTECT\ADMINISTRATOR
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 17:48:21	2018 Mar 9 17:48:20	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	12461824787876702A87102...	1 KB	ESET\PROTECT\ADMINISTRATOR
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:18	2018 Mar 9 10:28:18	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	10826A90C0410E1070102A...	18 KB	
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:07	2018 Mar 9 10:28:07	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense	08C7A81870F0A4C052A07...	167 KB	
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:08	2018 Mar 9 10:28:05	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:08	2018 Mar 9 10:28:02	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:04	2018 Mar 9 10:28:04	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:09	2018 Mar 9 10:28:09	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:02	2018 Mar 9 10:28:02	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:02	2018 Mar 9 10:28:05	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:05	2018 Mar 9 10:28:05	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:08	2018 Mar 9 10:28:04	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:11	2018 Mar 9 10:28:11	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:12	2018 Mar 9 10:28:12	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:40	2018 Mar 9 10:28:40	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			
file\ProgramData\ESET\Setup.exe		Finalized	2018 Mar 9 10:28:44	2018 Mar 9 10:28:44	ESET PROTECT	File/Executable	Automatic	Dynamic Threat Defense			

Complete visibility – see all files sent to ESET LiveGrid®

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 Dynamic Threat Defense.
- ✓ ESET Dynamic Threat Defense analyzes 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.

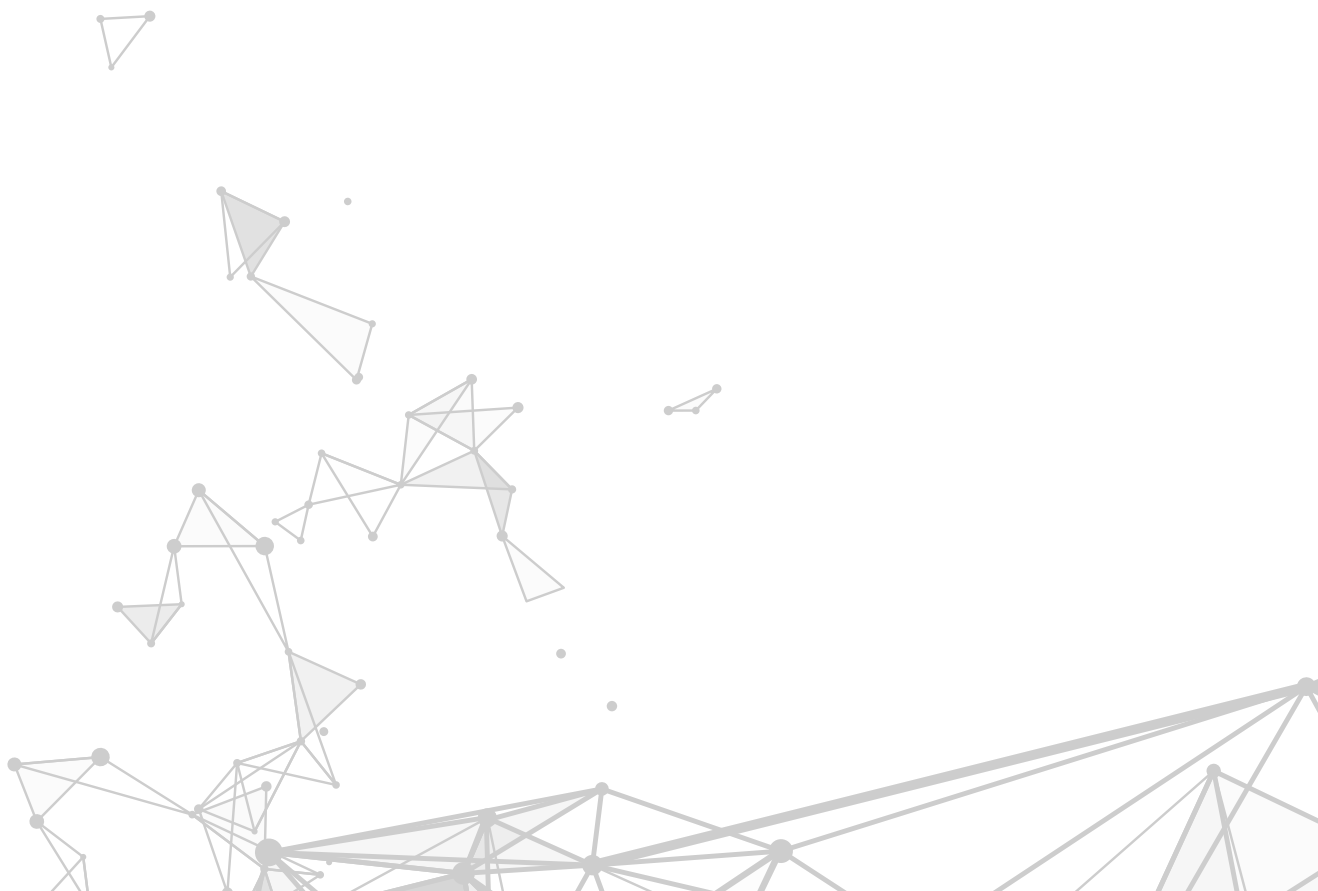
Granular protection for different company roles

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 Dynamic Threat Defense.
- ✓ 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 analyzed by ESET Dynamic Threat Defense.
- ✓ 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.



FILE BEHAVIOR REPORT ESET

STATUS	Malware
SHA-1	FD36A7C70B4E42DF1E324F1A848D9F6C40F
SIZE	430748
CATEGORY	Executable

Detected Behaviors

BEHAVIOR	Malware detected after execution
EXPLANATION	Sample has been detected as malicious after execution
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware disabled with ESET scanning engine after execution

BEHAVIOR	New file created in the Windows folder
EXPLANATION	Sample has created new files in the Windows folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence

BEHAVIOR	Analysed sample copied
EXPLANATION	Sample has been copied to a different location
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence

BEHAVIOR	Startup list modified
EXPLANATION	Sample has added a new entry to the Windows Startup applications list
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware wants to run after a system reboot

BEHAVIOR	Machine Learning detection
EXPLANATION	Sample behaves very similarly to known malware
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware has been detected by Neural network Machine Learning

BEHAVIOR	New files in Program Files folder created
EXPLANATION	Sample has created new files in the Windows Program Files folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Sample may be a Potentially Unwanted Application

ESET DYNAMIC THREAT DEFENSE





ESET Dynamic Threat Defense technical 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 Dynamic Threat Defense for analyzing. Once analysis is finished, the result is shared and the endpoint products respond accordingly.

TAILORED CUSTOMIZATION

ESET allows per-computer detailed policy configuration for ESET Dynamic Threat Defense so the admin can control what is sent and what should happen based off the receiving result.

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

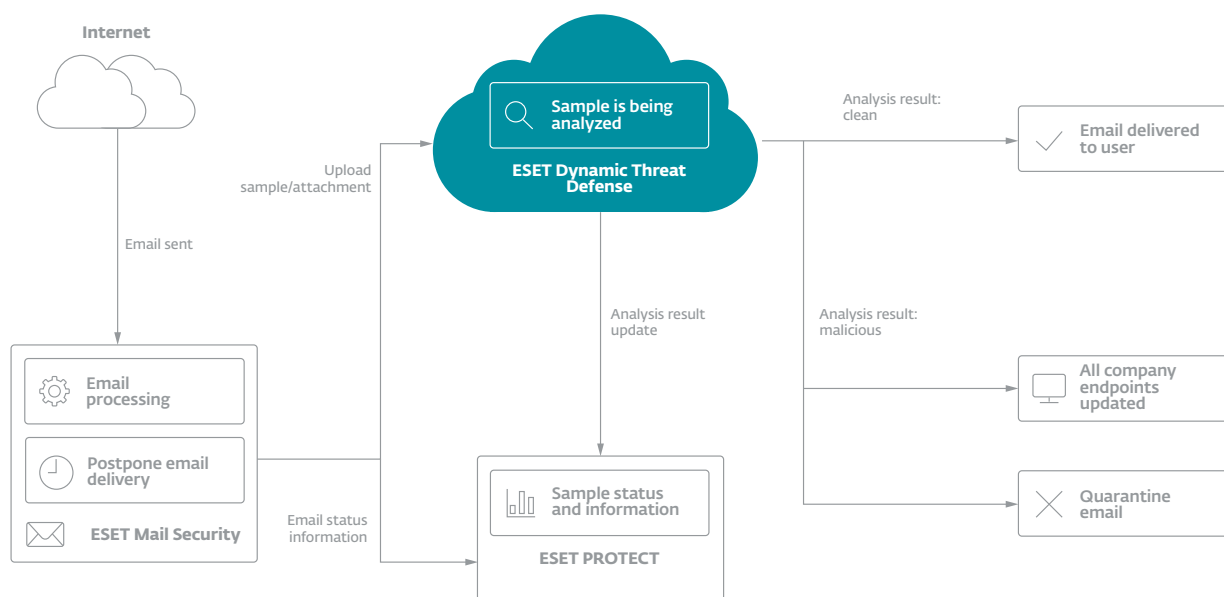
Not only does ESET Dynamic Threat Defense work with files, but it also works directly with ESET Mail Security to ensure that malicious emails are not delivered to your organization. To ensure business continuity, only emails coming from outside of the organization can be sent to ESET Dynamic Threat Defense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

“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 Group IT;
Mercury Engineering, Ireland; 1.300 seats

How ESET Dynamic Threat Defense works

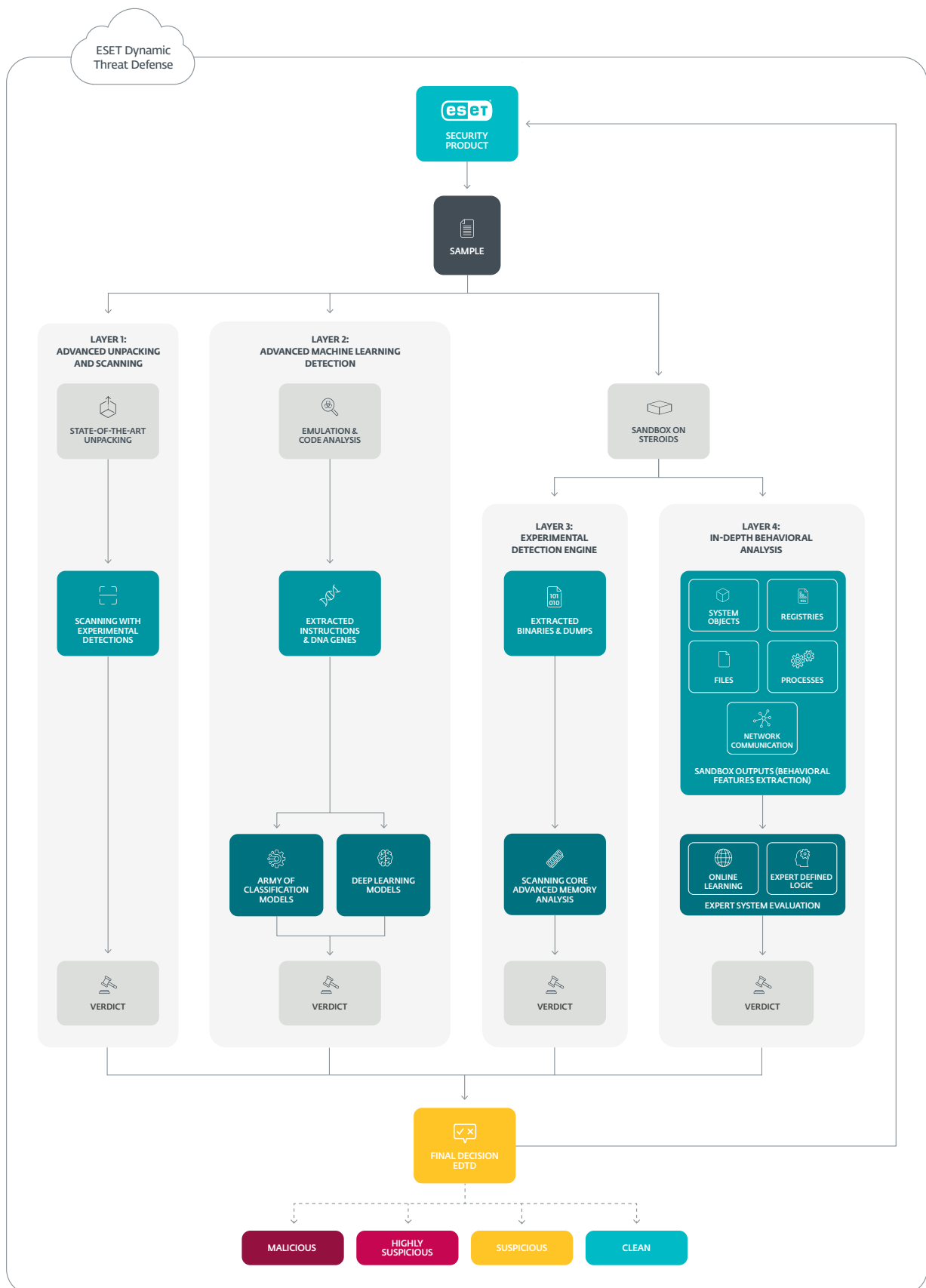
With ESET Mail Security



“Our experience with ESET has been more than satisfactory, so much so that we have renewed our licenses for three more years. So, without a doubt, we recommend ESET solutions to all companies that want to increase their levels of security.”

— Ernesto Bonhoure, IT Infrastructure Manager;
Hospital Alemán, Argentina, 1.500+ seats

How our advanced analysis works



About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services, delivering instant, comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide.

ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.

ESET IN NUMBERS

110m+
users
worldwide

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 14,000 endpoints

Canon

Canon Marketing Japan Group

protected by ESET since 2016
more than 9,000 endpoints

Allianz 
Suisse

protected by ESET since 2016
more than 4,000 mailboxes



ISP security partner since 2008
2 million customer base

Why choose ESET



ESET is compliant with **ISO/IEC 27001:2013**, an internationally recognized and applicable security standard in implementing and managing information security. The certification is granted by the third-party accredited certification body **SGS** and demonstrates ESET's full compliance with industry-leading best practices.

ESET RECOGNITIONS



ANALYST VOICES

Gartner

ESET was named the only Challenger in 2019 Gartner Magic Quadrant for Endpoint Protection Platforms, for the second year running.

FORRESTER

ESET has been recognized as a sample vendor in **The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2020**, namely in the endpoint security suite and mobile security suite categories.

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

ESET recognized as a 'Top Player' for the third year in a row in **Radicati's 2020 Endpoint Security Market Quadrant**.

Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019. Gartner does not endorse any vendor, product or service depicted in its research publications. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner Peer Insights is a free peer review and ratings platform designed for enterprise software and services decision makers. Reviews go through a strict validation and moderation process to ensure information is authentic. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences, and do not represent the views of Gartner or its affiliates.



CYBERSECURITY
EXPERTS ON YOUR SIDE

