

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

Progress. Protected.

### What is advanced threat defense? A proactive cloud-based technol uses advanced adaptive scappi

A proactive cloud-based technology that uses advanced adaptive scanning, cuttingedge 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 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 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 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 proactive cloud-based threat detection 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.

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 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 roundthe-clock threat intelligence.



# The ESET difference

#### **MULTILAYERED PROTECTION**

ESET LiveGuard Advanced is a cloud-based threat defense solution that executes all submitted suspicious samples to a secure test environment at ESET HQ, where their behavior 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 analyze 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 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 LiveGuard Advanced but everything that is sent to ESET's Cloud Malware Protection System – ESET LiveGrid<sup>®</sup>.

#### MOBILITY

Nowadays, employees in organizations are increasingly working remotely and not on-premises. That is why ESET LiveGuard Advanced can analyze 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 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. As a result, 1 billion internet users worldwide are now protected by ESET. Our technology is constantly scrutinized and validated by third-party testers who show how effective our approach is at stopping the latest threats.

#### **PROACTIVE DEFENSE**

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 organization'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 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 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 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.





# 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 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 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 organization. To ensure business continuity, only emails coming from outside of the organization can be sent to ESET LiveGuard Advanced for inspection.

PROTECT						Q V Search	computer na			A VOWINELING	ON 3 1000	UT		
Sub	mitted Files 🔺 🛛 🤟 🛇	0 2	ADD FILTER	5 V						_	_			0
0	FILE	STATUS	STATE	· FIRST SUNT ON	LAST PROCESSED ON	COMPUTER	CATLGORY	REASON	SONT TO		HASH	5425	USER	ф
0	Relot/Prog.athbadulut.dl	CONT I D	@ Reished	2018 Mar 13 00:07:00	2018 Mar 13 08 06 52	CD @ (SfT Endpoint	Everytable	Automatic	Dynamic Thread I	Deleme	26224843797602970883448	W1C. 19838	NTAUTHOR	PUM*
0	Seccorrigue_installerate		C Sent to UveGrid*	2010 Mer 12 16:16:22		III C Q LLL Mel Security	Decutable	Automatic	LANGING RD		SHEDE3DAACBEF2CF5HES3A	0647	LOTOPIN AN	-
0	field/C/Prog. rephoststrap (s		@ Rinished	2018 Mar 12 02:09:27	2018 Mar 12 02:0610	C @ ISIT Endpoint	Script	Automatic	Dynamic Thread I	Defence	ETBEAHPCHIPS ID486PDCCA	1004A. 20 KB	NT AUTHOR	TV:SVS
0	Second Prog. KningSepaid ja		@ Reished	2018 Mar 12 02:03 26	2018 May 12 02:06:06	C 12 150 Endpoint	Script	Automatic	Dynamic Thread I	Delesse	23434443077163591736244	18131. 34 KD	NT AUTHOR	PU.SHS
0	Sie.i/CuProgtringlorminaja	CID.	© limited	2018 Mer 12 020325	2018 May 12 02:06:07	CD (© ESET Endpoint	Seriet	Automatic	Dynamic Thread I	Detense	A10C3407F771A8101605051	0448	NTAUTHOR	PV.94
0	file:///Cy/work120552974d70991		C Related	2018 Mar 9 13 3652	2018 Mar 9 104041	C C ISIT Endpoint	Decutable	Automatic	Dynamic Throat I	Defense	CATCHCHARDERTONSACTED	8012. 1MB	EDTD/M/Ad	niniste.
0	Eie.005/work, #1736856215x3		Sent to Usefeid #	2018 Mar 6 13 35 40		CD 12 1517 Endpoint	Executable	Automatic	Lied-ic(R)		IFSINGRAFINGCARDENADCED	55FP1. 508 KB	ROTOPINE AN	
0	Real/Clivaria.ader_nytiseve		© finished	2018 Mar 9 13 06 24	2018 May 9 13/126	C C R STENSION	Executable	Automatic	Dynamic Thread I	Delesse	FED64670975461400F10328	664. 456B	EDIDPM AN	
0	Resil/Culvers, ing Invelops.doc	-	C Reizhed	2018 Mar 9 12:58:08	2018 Mar 9 130149	C Q ISIT Endpoint	Other	Automatic	Dynamic Throat I	Defense	DRUK/BUASACCRISHURCHIA	FIEC. 24518	EDIDRM/Ad	niniste.
0	fie.000/workd installer and		© Riskel	2018 Mar 9 12 39-42	2018 Mar 9 12:41-45	D @ ESET Endpoint	Everytable	Automatic	Dynamic Thread I	Defense	DA41637363F236260044023	E243 1 MB	SOLDINE VIE	
0	NextCluer_10104pd0(p	<b>.</b> ID	© finished	01.05.51 P ieM 8705	2018 Mar 9 123239	C) @ 15(1 Extpoint)	Script	Automatic	Dynamic Thread I	Delesse	08086496803453091(38/9D	CSBC- 18 KD		
0	SiecologyUser_/7e887813(10,p	<b>.</b> I.D	Ø Reiched	2018 Mar 9 12:28:07	2018 Mar 9 12(3105	C (2 ISIT Encipcent	Script	Automatic	Dynamic Thread I	Defense	DECSGARTSTODROADO4CD57	4CB2. 182.48		
0	flexcol/user_/260406ct036	-	© Rripes	2018 Mar 9 12/28/06	2018 Mar 9 12/31/55	C @ ISIT Endpoint	Script	Automatic	Dynamic Thread I	Detense	3			
0	64000,044	-	© Trided	2018 Mar 9 12:28:05	2018 Mar 9 12:32:02	C (2 1517 Endpoint	Script	Automatic	Dynamic Thread I	Delessa	4			
0	file.000/User.u/407e8126(1)jp		@ Rinahed	2018 Mer 9 12:28:04	2018 May 9 12:31:55	C (2 LSLT Endpoint	Script	Automatic	Dynamic Thread I	Detense				
0	fie.col/User/90(#9900.8	<b>CONT</b>	© Rrides	2018 Mar 9 12:25:03	2018 Mar 9 123124	C @ ISI7 Entpoint	Script	Automatic	Dynamic Thread I	Defense	Co	mple	te vis	ibil
0	fiex/00/User_/9638bilds[1]js	CTD.	@ Rnished	2018 Mar 9 12:28:02	2018 Mar 15 15 0816	C) @ ISIT Exclosien	Script	<b>Automatic</b>	Dynamic Thread I	Defense				
0	6ieu000/Useru/916eb510[1](a	COLUMN TO	@ finished	2018 Mar 0 12:26/2	2018 May 9 12/31/55	C) (2) ISIT Endpoint	Script	Automatic	Dynamic Thread I	Determe	se	nt to I	ESEI	LIV
0	fie.cod/User_/98499e0815ja		C Anisted	2018 Mar 9 12/25/00	2018 Mar 9 12/32/01	C @ ISIT Endpoint	Soriet	Automatic	Dynamic Thread I	Defense				
0	\$94000;User_/545c1532[1](a	-	© Reished	2018 Mar 9 12 28:00	2018 Mar 15 15 68 14	C 😨 ISIT Exclosier	Script	<b>Automatic</b>	Dynamic Thread I	Defense				
0	Sieu000/work28/9k/38e7b/98991		@ finished	2018 Mar 9 12:24:11	2018 May 9 12/2962	C C 12 CST Exclosed	Everatable	Automatic	Dynamic Thread I	Delesse				
0	field/work/matkato/testps3	<b>—</b> 1 D	C Anabel	2018 Mar 9 12/28/18	2118 Mar 9 120620	C @ 1517 Endpoint	Script	Automatic	Dynamic Thread I	Defense	4220358828302500049141	1991 268	SOLDIM VIE	ningto
0	\$e.07			2018 Mar 9 10:25:43		E C 2 DE Mai Security	Deputable	Automatic	Dynamic Thread I	Detense	SHIDHCEEUDD4CATCHETZY	2912	NEAUTHOR	TY SYS
0	Emmed. Uner_4500000001115			2018 Mar 8 16 21 44		CD IP ESET Endecient	Societ	Automatic	Dunarie Thread	Delenar	161571042321F07C0815C1	6411. 445 KB		
1.00														-
A	DELUSION TO POUCY													00

## How ESET LiveGuard Advanced works

With ESET Mail Security Internet Analysis result: clean Sample is being analyzed Email delivered to use Upload ESET LiveGuard Advanced sample/attachmen Email sent Analysis result: malicious Analysis result update All company endpoints updated Email processing Postpone email deliverv Sample status and information Quarantine 600 email Email status ESET Mail Security informatio ESET PROTECT

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

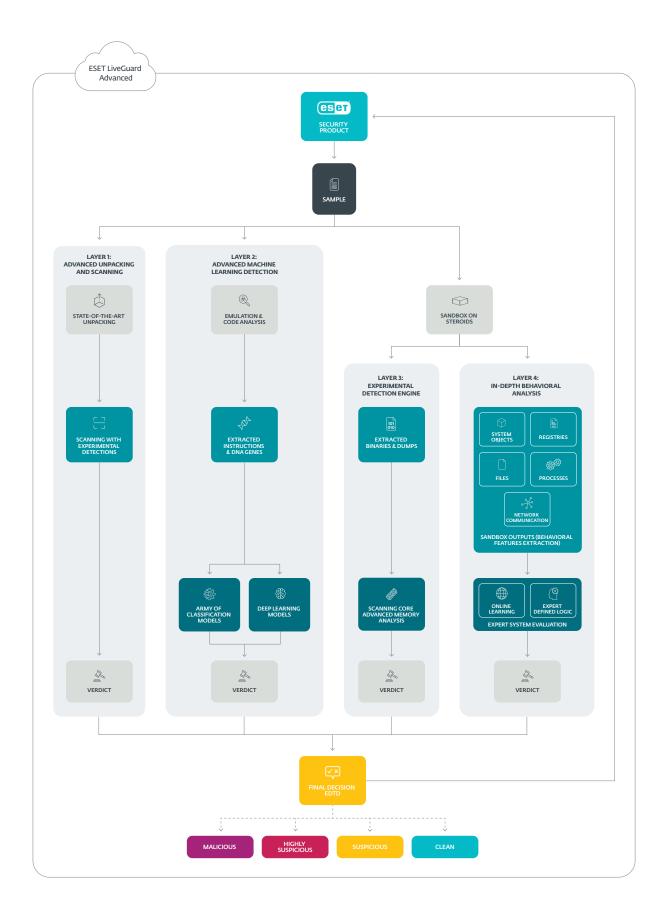
#### "Amazing Product!"

#### 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 stateof-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**

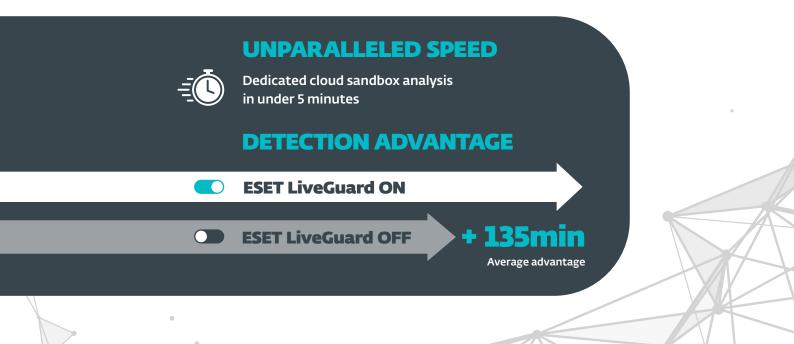
Samples are inserted into "sandboxes on steroids" that closely resemble full-scale user devices. They are subsequently monitored for any sign of malicious behavior.

#### 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 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.

#### 200+ 400k+ 1bn+ 13 business countries & global R&D internet users protected territories customers centers SOME OF OUR CUSTOMERS Allianz (II) Canon TSUBISHI Canon Marketing Japan Group Suisse Drive your Ambition protected by ESET protected by ESET protected by ESET ISP security partner since 2008 2 million since 2017 more than since 2016 more than since 2016 more than 9,000 endpoints 4.000 mailboxes 32,000 endpoints customer base

**ESET IN NUMBERS** 

#### 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.



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.



Digital Security **Progress. Protected.**