

## DYNAMIC THREAT DEFENSE

### Prevent zero-day threats with powerful

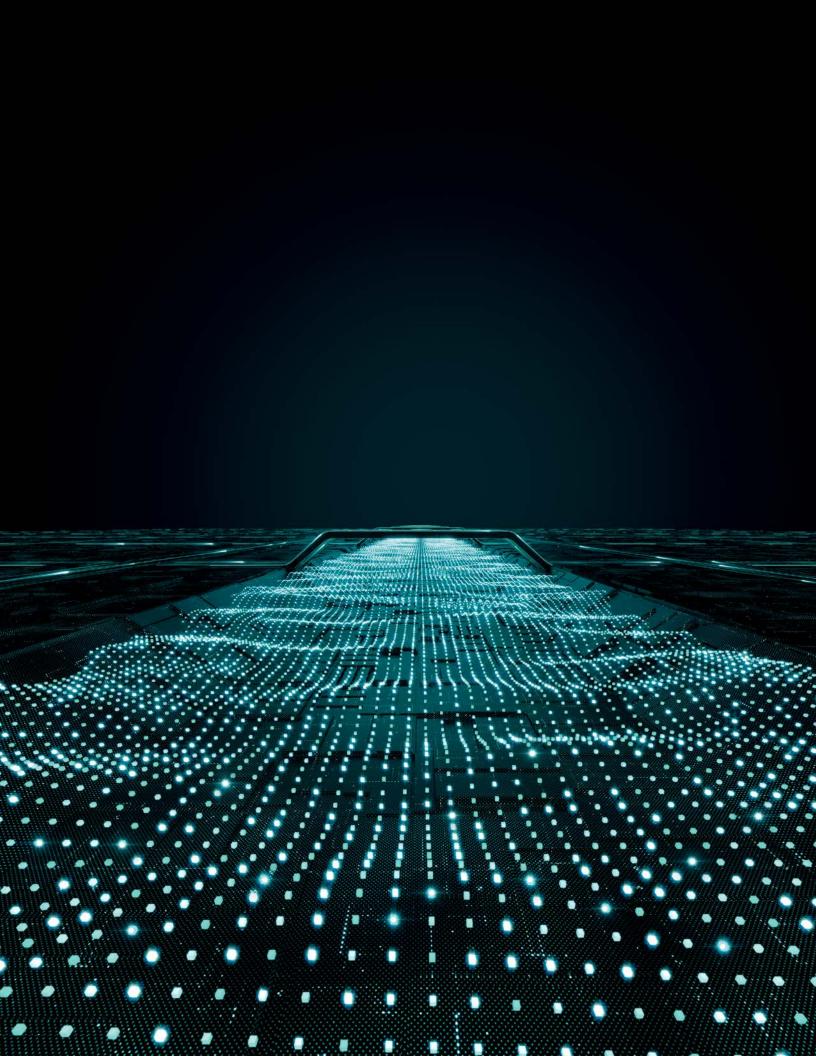
cloud-based sandboxing



THE WY M



30 YEARS OF CONTINUOUS IT SECURITY INNOVATION



### 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

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 a new, never-before-seen type of threat. 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.

automated manner.

# 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.

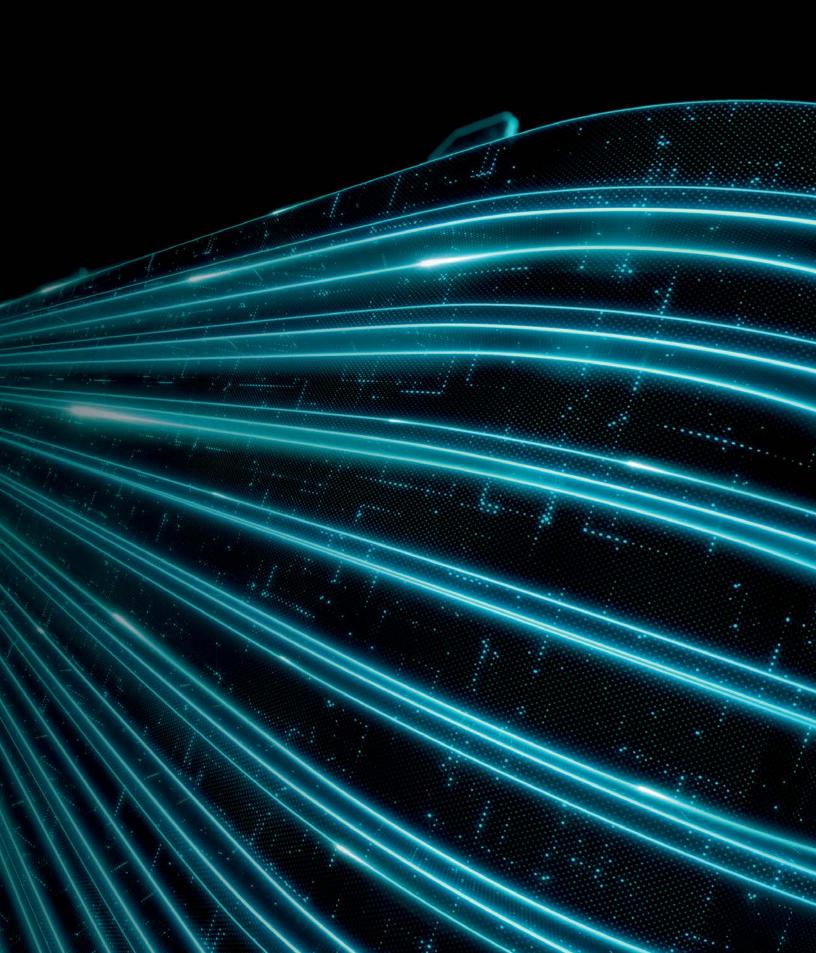
A cloud security sandbox product provides an additional layer of defense outside of a company's network to prevent ransomware from ever executing in a production environment.

#### TARGETED ATTACKS AND DATA BREACHES

Today's cybersecurity landscape is constantly evolving with new attack methods and neverbefore-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.



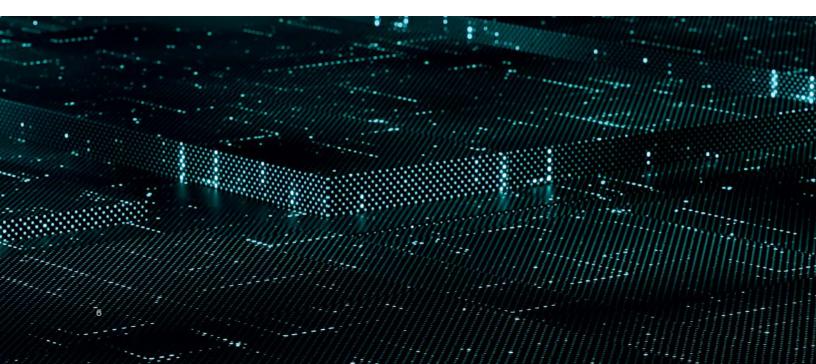
#### **MACHINE LEARNING**

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**

Every analyzed sample is listed in ESET Security Management Center console with various information about the sample itself and its origin. All information is displayed 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<sup>®</sup>.

### MOBILITY

Nowadays, customers are constantly traveling and not on premise, that is why ESET Dynamic Threat Defense is able to 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.

	Million         A         O         Image: A the A t		000 NUTRE   PEOPT 12200   (0) Sectors Uniquest? (0) Sectors Uniquest? (0) Sectors Uniquest? (0) Sectors (0)   (0) Sectors		LAST PROCESSION ON 2018 New 13 05/05/32 2018 New 17 05/05/32 2018 New 17 05/05/33 2018 New 17 05/05/37 2018 New 17 05/05/37	COMPUTER C S Stituter S S S Stituter S S S Stituter S	CATHOLIN Servicible Social Social Social Social	MASON Actomatic Actomatic Actomatic Actomatic	SHIFT TO Dynamic Thread Orlemon LowScraffi, Dynamic Thread Orlemon Dynamic Thread Orlemon	ники зассаноти поряоналитеть очтороженихочикалитеть споряоналитеталисталия заканото порогодитеть	20.×8	О ини 0 илиполтизе кладнолтизе кладнолтизе кладнолтизе	
Playof     Playof	۲۵۵٬۹۰۰ پر ۱۹۹۵ ۱۵۵٬۹۰۰ پر ۱۹۹۹ ۱۵۵٬۹۰۰ پر ۱۹۹۹ ۱۵۵٬۹۰۰ پر ۱۹۹۹ ۱۵۵٬۹۰۰ پر ۱۹۹۹ ۱۵۵٬۹۰۰ پر ۱۹۹۹ ۱۵۵٬۹۰۰ پر ۱۹۹۹		Finite	2018 May 13 054740 2018 May 12 061822 2018 May 12 061822 2018 May 12 054829 2018 May 12 054829 2018 May 12 054829 2018 May 12 054829	2216 Mar 13 06/05/2 2216 Mar 17 05/05/13 2219 Mar 12 05/06/09 2218 Mar 12 05/06/07	이 및 Eff Enfanier 월 전 및 Eff Enfanier 이 및 Eff Enfanier 이 및 Eff Enfanier 이 및 Eff Enfanier	Secular becalar Sour Sour	Automatic Automatic Automatic Automatic	Opraerie Treast Onleiner Livelsraft) Opraerie Treast Onleiner Opraerie Treast Onleine	зассанатическиональнитис. очисальновитестикальным. спасановитесновогосальна.	794.83 741.84 20.84	NT AUTHOR THUSE * EDTURMARINAR NT AUTHOR THUSE	
Record     Record	IC:/Pape_cystationisme IC:/Pape_cystationisme IC:/Pape_transportune IC:/Pape_transportune IC:/Pape_transportune IC:/Pape_transportune IC:/Pape_transportune IC:/Pape_transportune IC:/Pape_transportune		Serre United     Trodel     Oriveted     Privated     Privated     Trodel     Serreted     Serreted     Serreted     Serreted	2018 Mar 12 16/19/22 2018 Mar 12 00/03/7 2018 Mar 12 00/03/8 2018 Mar 12 00/08/29 2018 Mar 12 00/08/29	2218 Mer 42 4246 10 2218 Mer 42 4246 00 2218 Mer 42 42460	<ul> <li>B 2 2 cut the source</li> <li>D 2 cut feature</li> <li>D 2 cut feature</li> <li>D 3 cut feature</li> <li>D 3 cut feature</li> </ul>	berutahir Soriat Soriat	Aconace Aconacie Actonacie	LiveGrid(R) Dynamic Trinell Celevia Dynamic Trinal Celevia	сиссосносносоносоновальным спісановитисногосонова	141.KJ 20.XB	EDEPMAdministr NT AUDIOR/76345	
Record     Record	UCCPsgglowstwigs UCCPsgtorsprend (J UCCPsgtorsprend) UCCPsgtorsprend) UCCPsgtorsprend) UCCPsgtorsprend) UCCPsgtorsprend) UCCPsgtorsprend)		C Traine) C Frainet Frainet C Trainet C Trainet	2018 Mar 12 024027 2018 Mar 12 024028 2018 Mar 12 024028 2018 Mar 11 024025	2218 Mar 12 030909 2018 Mar 12 030909	C 2 Different	Sour. Sour	Actonacie Actonacie	Dynamic Trend Onlesse Dynamic Thread Onlesse	етисьносонгліськигосськловых.	20.×8	AT AUDIOR TYSIC	
Heavy     Heavy     Heavy     Heavy     Heavy     Heavy     Heavy	05/1494-33193/1984(p 05.51493-35193/149799 05.51493-31730952145199 05.51493-3487,1995444 05.51493-3495,1995444		C Rested Fridad D Rested O Sec 5: Livelaid®	2018 Mar 12 0208428 2018 Mar 12 0208428 2018 Mar 11 020852	2218 Mar 12 030909 2018 Mar 12 030909	© © Bill Induseri © © ISII Enduseri	Serge	Avtenance	Dynamic Thread Defense				
Report     Report     Nector     Nector     Nector     Nector     Nector     Nector     Nector     Nector     Nector	urtelleng, songsonmanja ottomene, 1225209447879 urtelmene, 417740502163 utelmene, ander gynstand utelmene, ang konstanting		C Fridad Control C Sector L Sector	2216 Mar 12-03-8825 2216 Mar 9 (12)-852	2018 Mar 12 050507	D & BIT Enborr				2048443067182817902448101	34.48	AT AUTHORITY DVI	
Allerian	of Share R., 122222014 (1979) NCAwak, H1716M1216(1 NCAwak, asile pystam NCAwak, asile pystam		() Terc to Live Did #	2216 Mar 9 123452			Sorpr	Delonary.					
Record     Record	WC/week#17768/19216c3 WC/week	-	⊖ terrativetid≉		2218 Mar 9 1343-41	Contra Million Contractory			Dyrams: Treast Defence	A10034077771AB10350883104Ab.	31.68	NT AUTHORITY SHE	
C Hall	of Courts and Sources			2218 May 9 151540		Carl Contract Conditional	bendatu	Puternatic	Dynamic Phreat Delence	саласания пленинализаци.	1.845	1000 Mildrenstr	
C Held	Wheek, og konstande		(C) Freehand			C 2 Internation	Desistable	Accord	(set all)	EN090943925C402E140C803091	204.65	EDERMAINING	
C Held		-	the second se	2212 Mar 9 1209-24	2018 146 9 121129	C 2 Uit Indusire	Descutative	Automatic	Dynamic Press Defense	PEDBARTOR/SHETADETUZZEFETAL	4113	101014August	
	of shareh of installer our		(2) Residuel	1010 Mar # 1218.04	2210 344 8 13,0148	C 2 furthetert	Other.	Sales and Sales	Dynamic Treast Daleman	0424180432709854F8018267980	24148	Internation	
C Ne.U	the second second second	0001100	(i) Revolution	2018 Mar 9 123942	2216 Mar 9 124446	C (2 1587 Bridgeort	Exercitable	Automatic	Dynamic Proof Defence	DARTEA/16/F216260440231243	1 MB	LODIMAdministr	
	ACTORN CRIMINAL AND A CONTRACTOR	C	(i) Printed	2018 May 9 12 28 10	2218 Mar 9 12 32 33	C 2 Eff behave	Sage	duro natic	Dynamic Treat Delense	CREDINARIZZASTINITALICE SRC	15.68		
E 66.07	0.CPUses_7066785211La	000	(i) finished	2018 Mar 9 12/28/07	2218 Mar 9 123155	D @ Hill Endowed	Seat	Automatic	Dynamic Trisot Defense	GECSEARINETECHDAGOACDIS/WCR2	162.63		
() (les)	WOYCheel. (Mails/Her(1))e	0000	(C) Finished	3018.Mar 8 1228.06	2218 Mar 9 17 31 55	C 2 Fift foduint	Serge	Actoriatie	Dynamic Treast Gelence	28083900			
- feat	//C/Gen.//tes2e944[1].js	C	() Tennet	2318 Mar 9 122809	2216 May 9 123202	C 2 BITEstoort	Serget	Automatic	Dynamic Proof Defonce	0402846			
El Nega	0107/1041-/48748128[3]js	1000	(i) firinted	2218 Mar 9 12 28 84	2258.8Aur 8 12 31 55	CI (P. 1587 Rodport)	Seepe	hennes	Dynamic Threat Defense	Bic23P			
C. New	1/C/Qeex/9/200999111a	CHILD T I	C linined	2018 May # 122843	2218 Mar 9 1231 24	CO CE LIST Graduaries	Sept	Automatic	Dynamic Threat Defense	CO	mnl	ete vis	ibility—see all file
<ol> <li>test</li> </ol>	UCVUMe_18854646(1)(e		@ Frishet	3018 Mar # 1238.02	2218 Mar 15 1548118	C Q ISH Magning	Serge	Actomatic	Dynamic Trynat Dafance	Marketter.			
<ul> <li>(b)//</li> </ul>	VC/Lien./996eb510(1),#		(). Frontes	2018 Mar 9 122800	2216 Mar 9 123135	🖵 😰 Lill Endesirt	Serpt	Automatic	Dynamic Threat Defense	sei Sei	nt to	) ESET	LiveGrid®
C) Yest	//Cr/men_/98/99e08(11)#	1000	@ Reiner	2018 Mar 9 1228-00	2018 Mar 9 12:12:01	🗇 🖗 Kill Belgeler	Serge.	<i>Automatic</i>	Dynamic Threat Deleture	0401785			
D Ne.17	WEAUser-1946/82201La	C 1 1	() Finished	2218 May 9 1228-00	2218 Mar 15 15:00.14	D. 12 List Externet	Siret	Automatic	Dynamic Threat Defense	6047801			
The Period	interventurated and states states		C freiher	2010 Mar # 122411	2216,7464 8 12,29 62	C 2 CHI Industri	Dervision	Patronette	Dynamic Press Datasce	APPARTA			
C field	1/C/www.www.com/cont.com	CHARTER TO D	(i) Frished	2016 Mar 9 122313	2010 Mar 9 122620	D 12 LSET Endsoirt	Selec	Automatic	Dynamic Threat Defense	422025882830259004614141010	26.0	LD1D1MAdministri	
D . 19=///	W)			2018 Mar 9 182643		1 C 2 SET Mail Serverty	Gesistable	Automatic	Dynamic Threat Defense	94/0408030040474872708981	5.102	NTAUTHORITYLES	
C. New	Collect@09580915a		111	2018 Mer # 192144		C (2 EBT Indexed	Seciel	Antenda	Diramic Treast Defense	enteroscientoriconconent.	440.12		

## Use cases

### Ransomware

### **USE CASE**

Ransomware tends to enter unsuspecting users' mailboxes through email.

### **SOLUTION**

- ESET Mail Security automatically submits emails that contain unknown files to ESET Dynamic Threat Defense.
- ESET Dynamic Threat Defense analyzes the sample, then submits the result back to Mail Security usually within 5 minutes.
- If the file was found to be malicious, ESET Mail Security automatically destroys the email that contained the malicious content.
- The malicious email 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.

#### A FILE BEHAVIOR REPORT eser A STATUS SHA-1 SIZE CATEGORY 4367368 Detected Behaviors BEHAVIOR EXPLANATION BENION CAUSES Malware detected after execution Sample hal been detected as malice Clean applications should not do the MALICIOUS Malasare detected with ESET scanning BEHAVIOR New files created in the Windows folder Sample has created new files in the Window EXPLANATION BENIGN CAUSES MALICIOUS Malazara tried to hide its presence Analyzed sample cepied Sample has been copied to a other entit This is standard between im--BEHAVIOR EXPLANATION BENION CAUSES MALICIOUS CAUSES Malazzre tried to hide its present BEHAVIOR EXPLANATION BENION CAUSE MALICIOUS CAUSES wants to run after a system reboot BEHAVIOR EXPLANATION BENION CAUSES MALICIOUS REMAYIOR. BEHAVIOR New Riss in Program Files felder created EXPLANATION Sample has created new files in the Window BENION CAUSES This is standard behavior for some installers MALICIOUS



## 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 Security Management Center.

### MAIL SECURITY PROTECTION

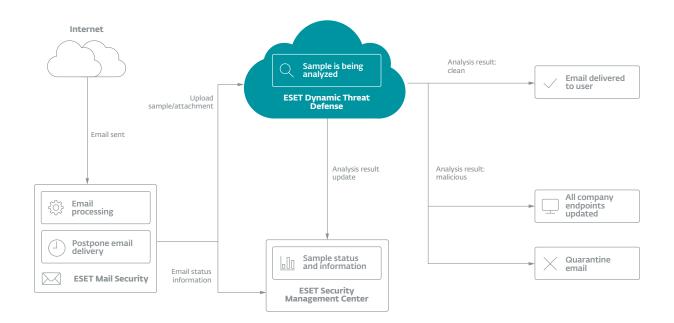
Not only does ESET Dynamic Threat Defense work with files, but it also works directly with ESET Mail Security to ensure that malicious emails are not delivered to your organization. To ensure business continuity, only emails coming from outside of the organization can be sent to ESET Dynamic Threat Defense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

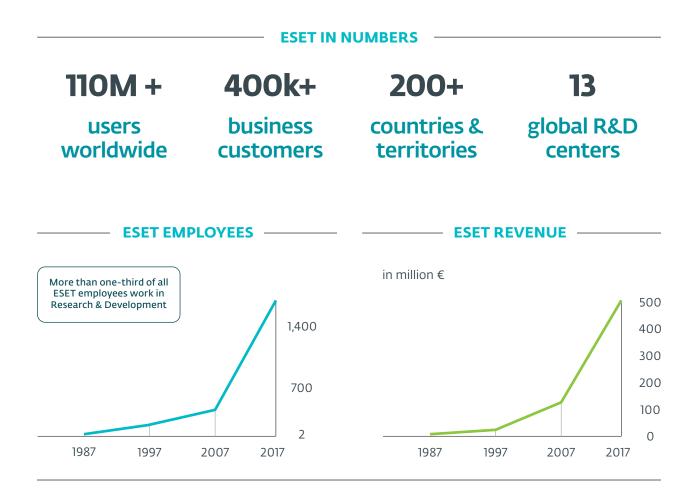


## **About ESET**

ESET—a global player in information security—has been named as the only challenger in the 2018 Gartner Magic Quadrant for Endpoint Protection Platforms.\*

For more than 30 years, ESET<sup>®</sup> 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.



\*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.

### SOME OF OUR CUSTOMERS



protected by ESET since 2011 license prolonged 3x, enlarged 2x



protected by ESET since 2016 more than 14.000 endpoints

### GREENPEACE

protected by ESET since 2008 license prolonged/enlarged 10x



ISP security partner since 2008 2 million customer base



### SOME OF OUR TOP AWARDS







"Given the good features for both anti-malware and manageability, and the global reach of customers and support, ESET should be on the shortlist for consideration in enterprise RFPs for anti-malware solutions."

> KuppingerCole Leadership Compass Enterprise Endpoint Security: Anti-Malware Solutions, 2018



