



**SECURITY
DAYS**

CYBERSECURITY CHALLENGES, MARKET TRENDS AND ESET B2B OFFERING FROM ANTIVIRUS TO XDR PLATFORM

Michal Jankech



Digital Security
Progress. Protected.

&



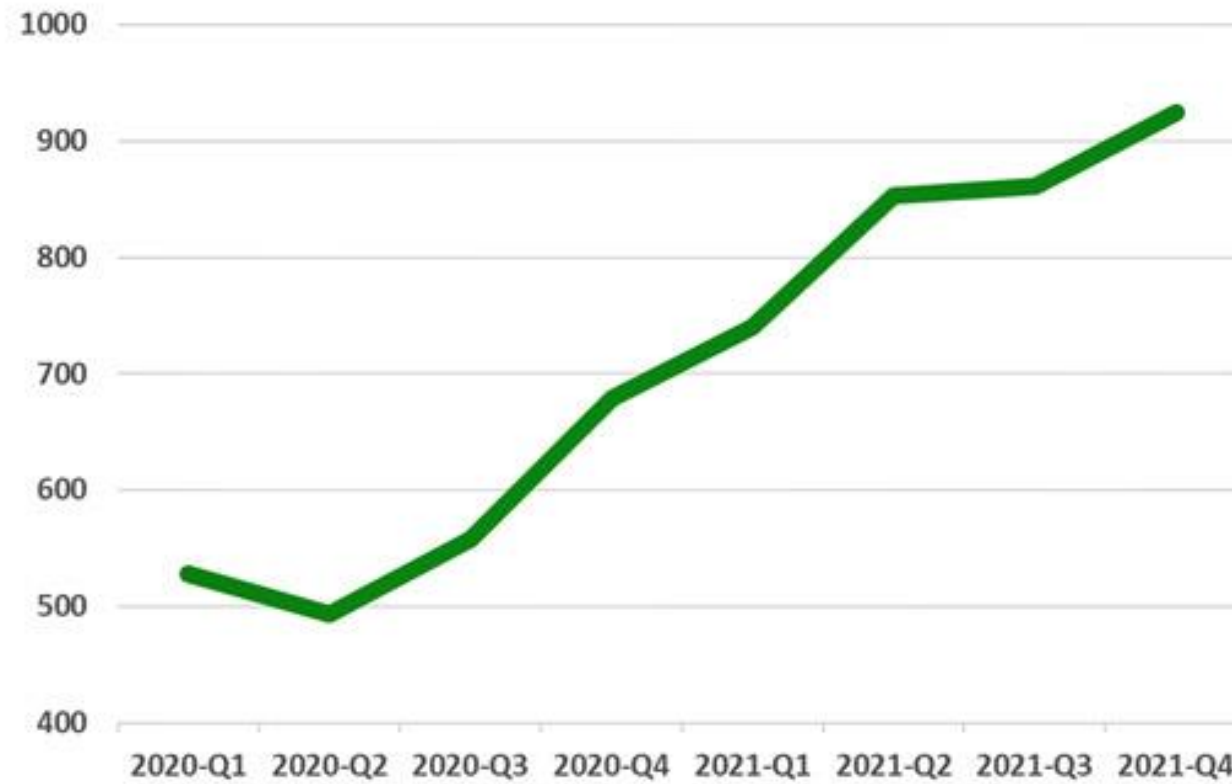
konferencie

Agenda

- Cybersecurity challenges
- Market Trends
- ESET Balanced Security Concept
- ESET B2B Offering Update
- ESET PROTECT Platform (XDR)
- Future of the offering

Cybersecurity challenges

Global Weekly Cyber Attacks per Organization(2020-2021)





+15% YoY
over the next 5 years

The most important **global** business risks for 2022



1

↑ 44%

2021: 3 (40%)

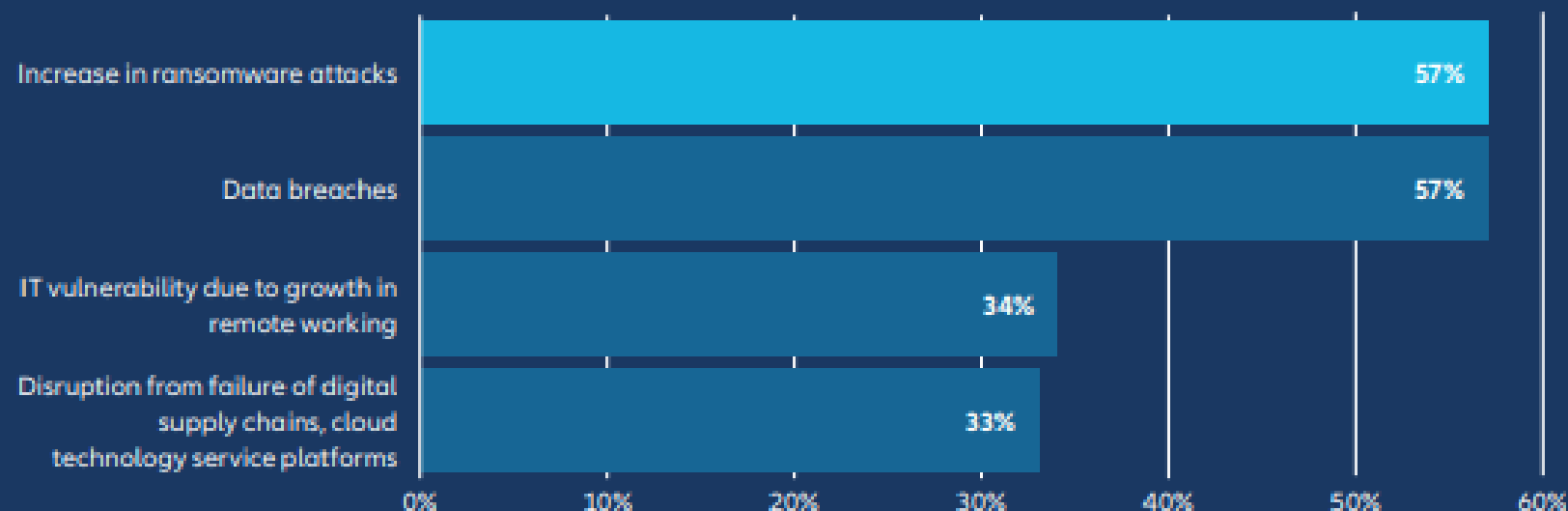
Cyber incidents

(e.g. cyber crime, IT failure/
outage, data breaches, fines
and penalties)



Which **cyber exposures** concern your company most over the next year?

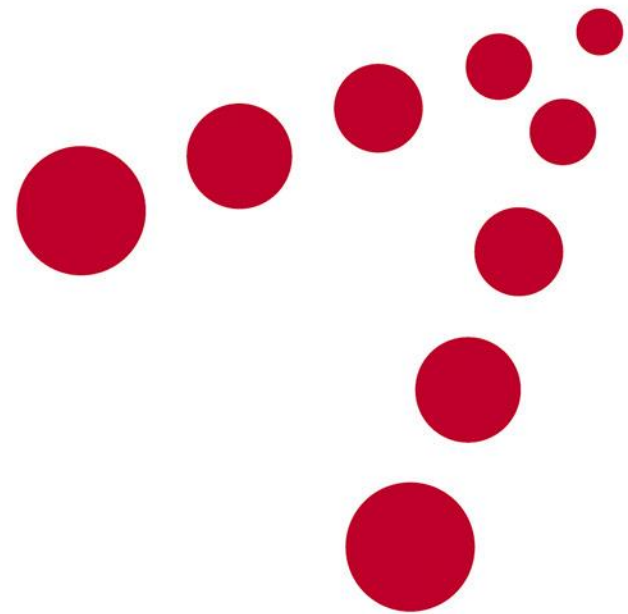
Top four answers



A ransomware attack is the most concerning cyber exposure for companies

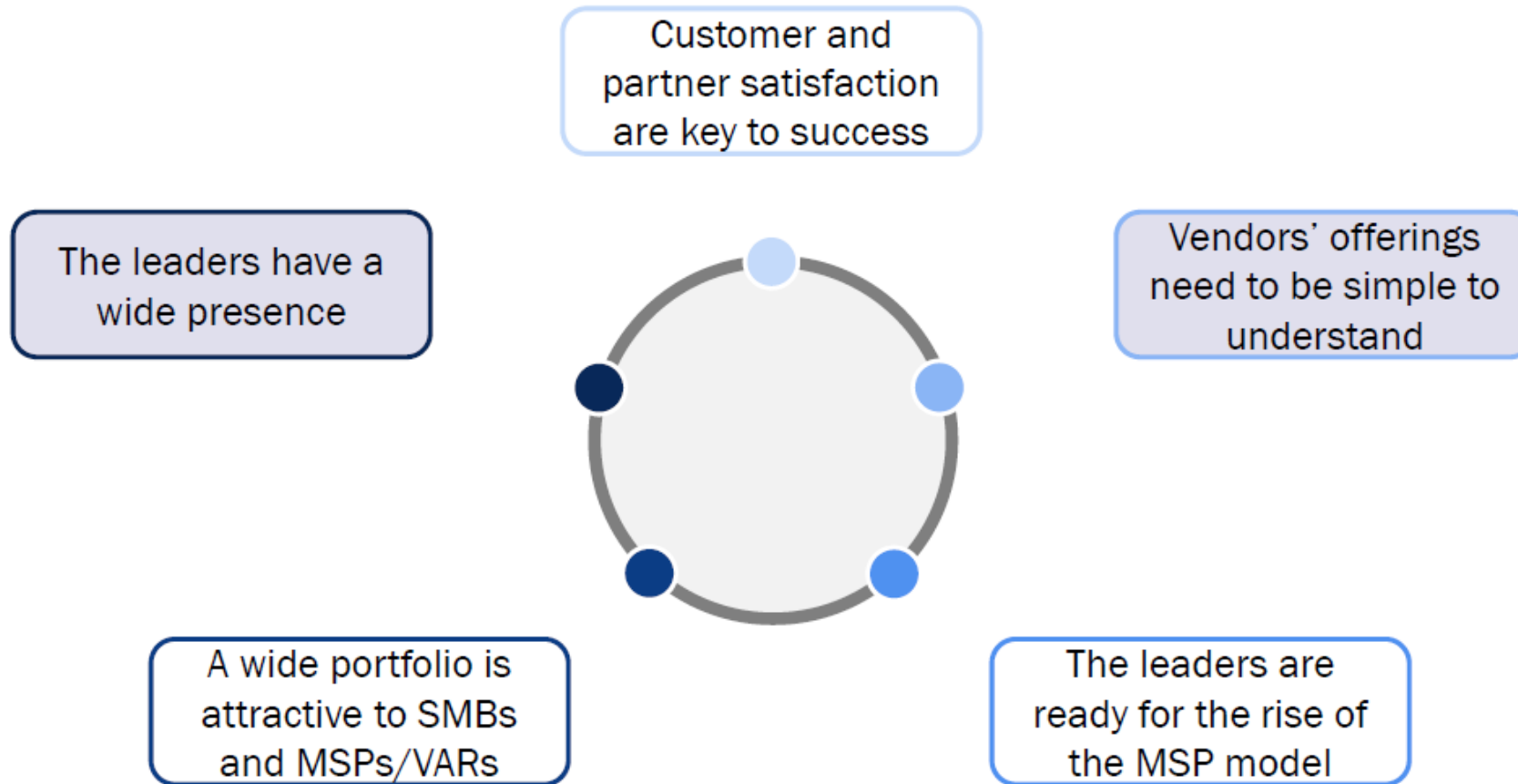
Category	T2-T3	2020-2021	Key points in T3 2021
Overall threat detections	+7.2% ↑	-16.0%	Top threat: HTML/Phishing.Agent trojan
Infostealers	-15.2% ↓	N/A	Rise in banking malware
Ransomware	+0.6% →	-44.6% ↓	Highest ransom ultimatum yet
Downloaders	+46.1% ↑	-39.2 % ↓	Emotet makes a comeback
Cryptocurrency threats	+7.7% ↑	N/A	Targeting of NFT platforms
Web threats	+2.6% ↑	-49.5% ↓	Rise in cryptocurrency-themed phishing
Email threats	+8.5% ↑	+145.4% ↑	Rise in phishing emails
Android threats	+2.8% ↑	N/A	Yearly increase in banking malware: 428%
macOS threats	-5.9% ↓	-36.6% ↓	Trojans one third of macOS detections
RDP attacks	+274% ↑	+897% ↑	Rise in attack attempts, fewer targets

Market trends

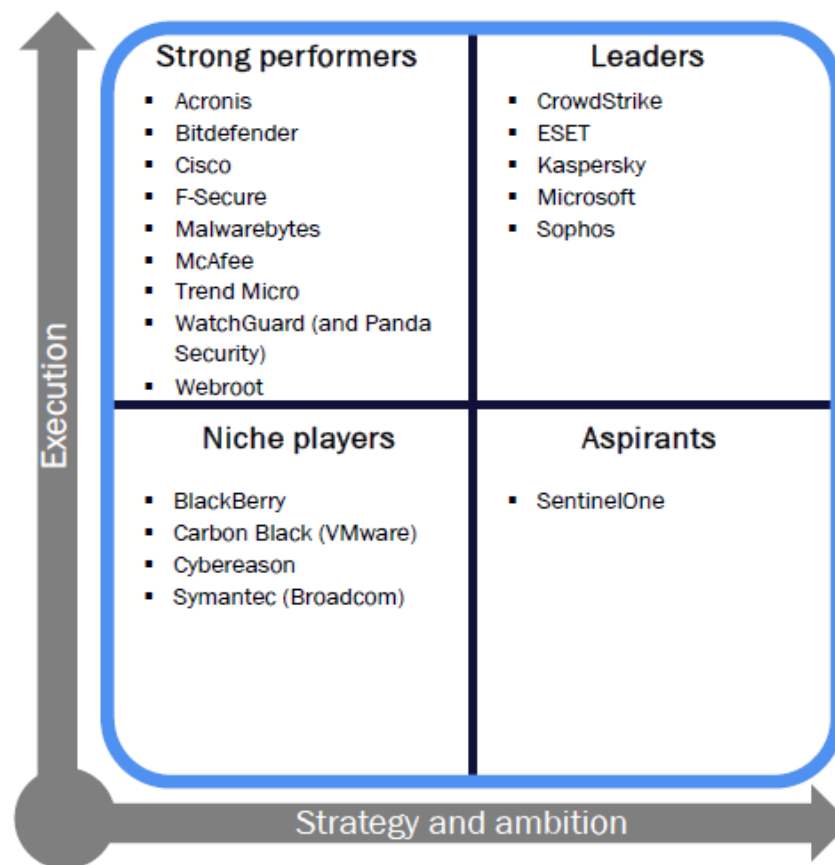


analysys
mason

Leaders: key learnings and considerations



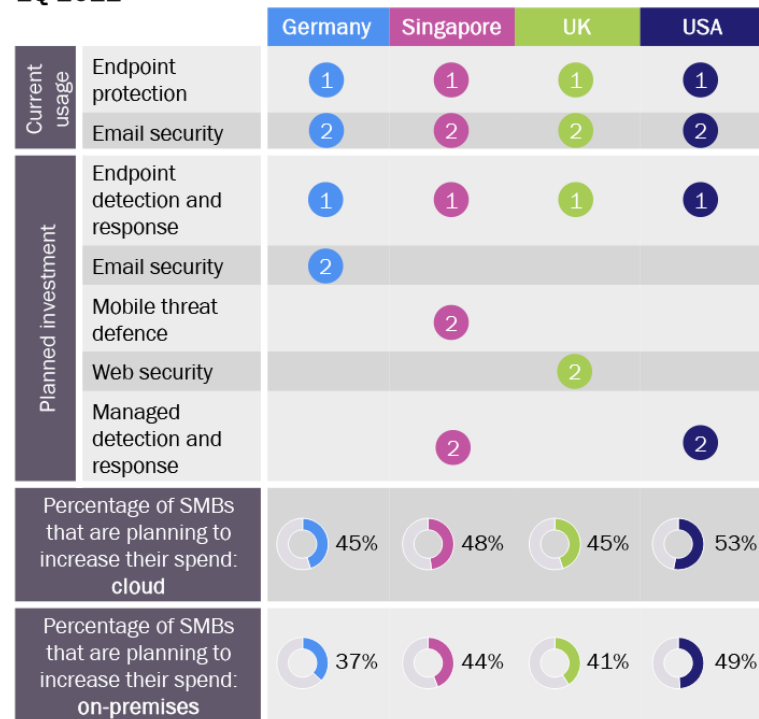
SMB Endpoint Security Vendor Scorecard 2021



Usage	Endpoint protection	
	Email security	
Investment	Endpoint detection and response	
	Email security	
	Mobile threat defence	
	Web security	
Investment	Managed detection and response	
percentage of SMBs that are planning to increase their spend: cloud		
percentage of SMBs that are planning to increase their spend: on-premises		

SMBs are most interested in solutions that protect their endpoints and email; many expect to increase their spending on security, but will need expert advice

Figure 23: Cyber-security solutions ranked by current usage and planned investments, Germany, Singapore, UK and USA, 1Q 2022¹



Source: Analysys Mason

Most SMBs reported using some form of cyber-security solution and have plans to increase their spending in this area. Securing data assets and protecting remote endpoints will remain key priorities.

The main security solutions used by businesses of all sizes in all four countries include endpoint protection, email security, firewalls and UTM solutions. Mobile threat defence (MTD) and web security are also common, especially among larger businesses.

The majority of the SMBs surveyed plan to add or upgrade at least one cyber-security solution. This will involve significant investments in both cloud-based and on-premises solutions. SMBs in the USA expect to increase their spending the most. They are likely to invest in endpoint detection and response (EDR), web and email security and MDM solutions. SMBs in Germany and Singapore are planning to deploy/upgrade data loss prevention solutions.

Implications for vendors. Two thirds of SMBs across all countries do not have dedicated in-house cyber-security specialists and are managing their security on an ad-hoc basis. Security vendors and service providers that can offer strategic cyber-security planning and easy-to-deploy, cost-effective solutions coupled with ongoing service plans will do well in the SMB space.

¹ Question: "Which of the following security solutions does your company currently use or plan to start using or upgrade in the next 12 months? n = 1149.

SMBs are most interested in solutions that protect their endpoints and email, many expect to increase their spending on security, but will need expert advice

Top 10 security solutions SMBs want to use

Top 10 security solutions SMBs want to use

Endpoint protection



Endpoint detection and response



Percentage of SMBs that are planning to increase their spend: cloud



45%



48%



45%



53%

IDC Survey Spotlight

What cyber technologies are Small and Medium Businesses Investing in?

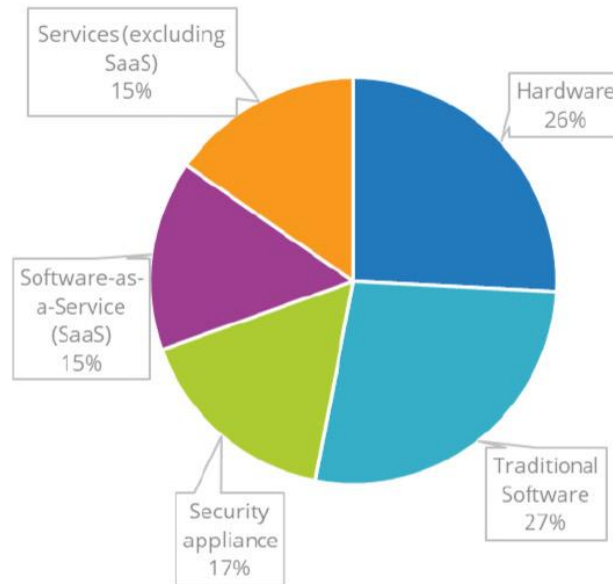


Shari Lava

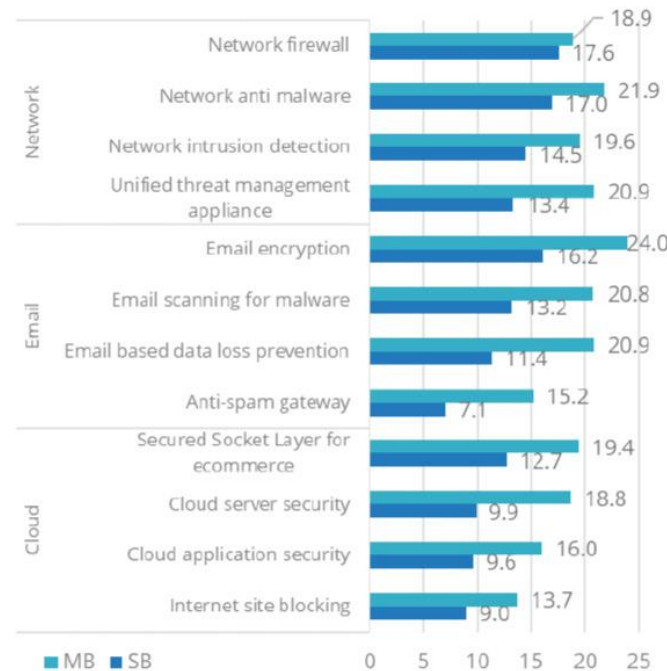
How is your total IT security spending allocated amongst security categories?

Which of the following network and end point security capabilities does your company plan to add in the next 12 months?

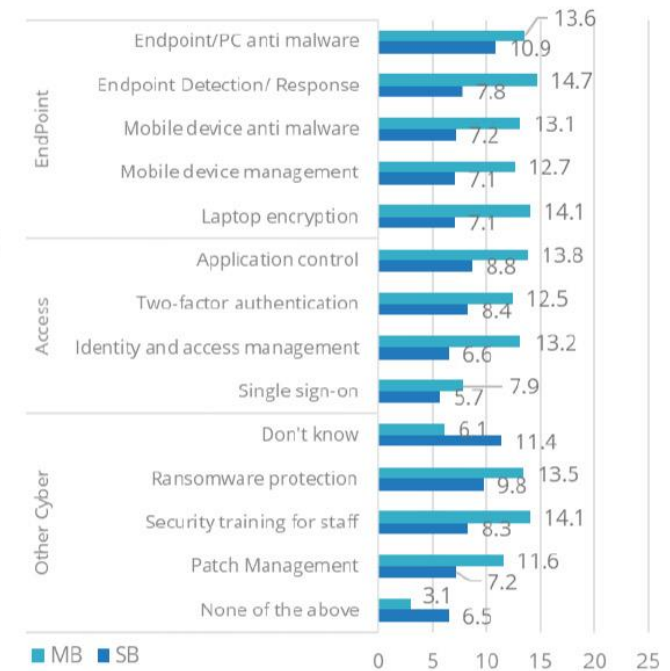
Current Security Budget Allocation



Planned Adoption of Cloud/ Network Security Technologies

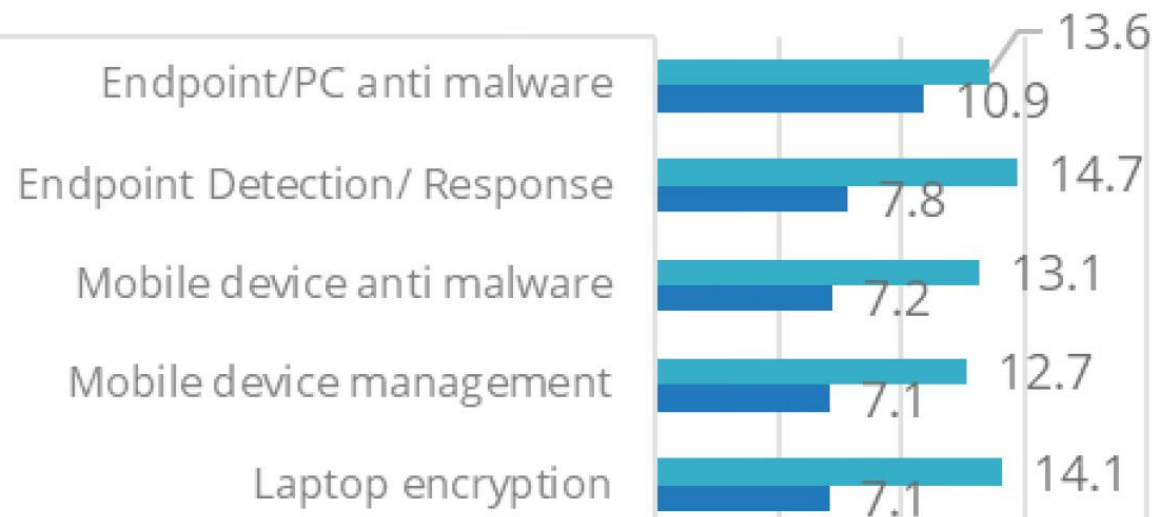


Planned Adoption of End-User /Other Security Technologies



IDC #US46380321 (August 2021)
Source: WW Small and Medium Business Survey, October 2020, n = 2463

EndPoint



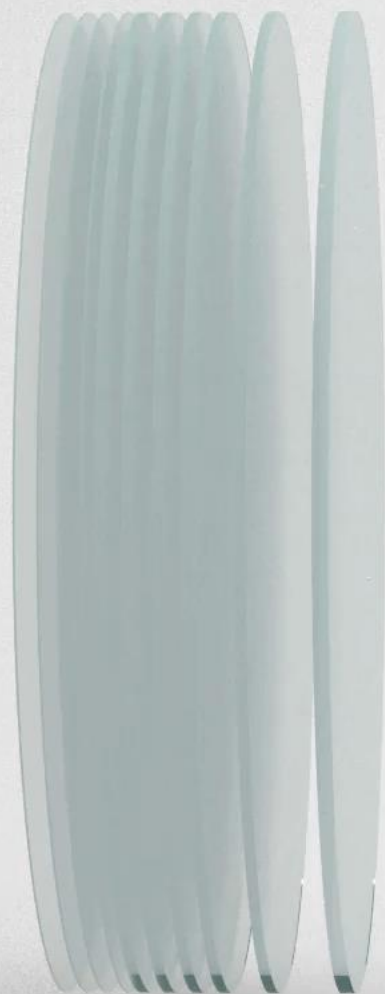
ESET Balanced Security



PROTECT

DETECT

RESPOND

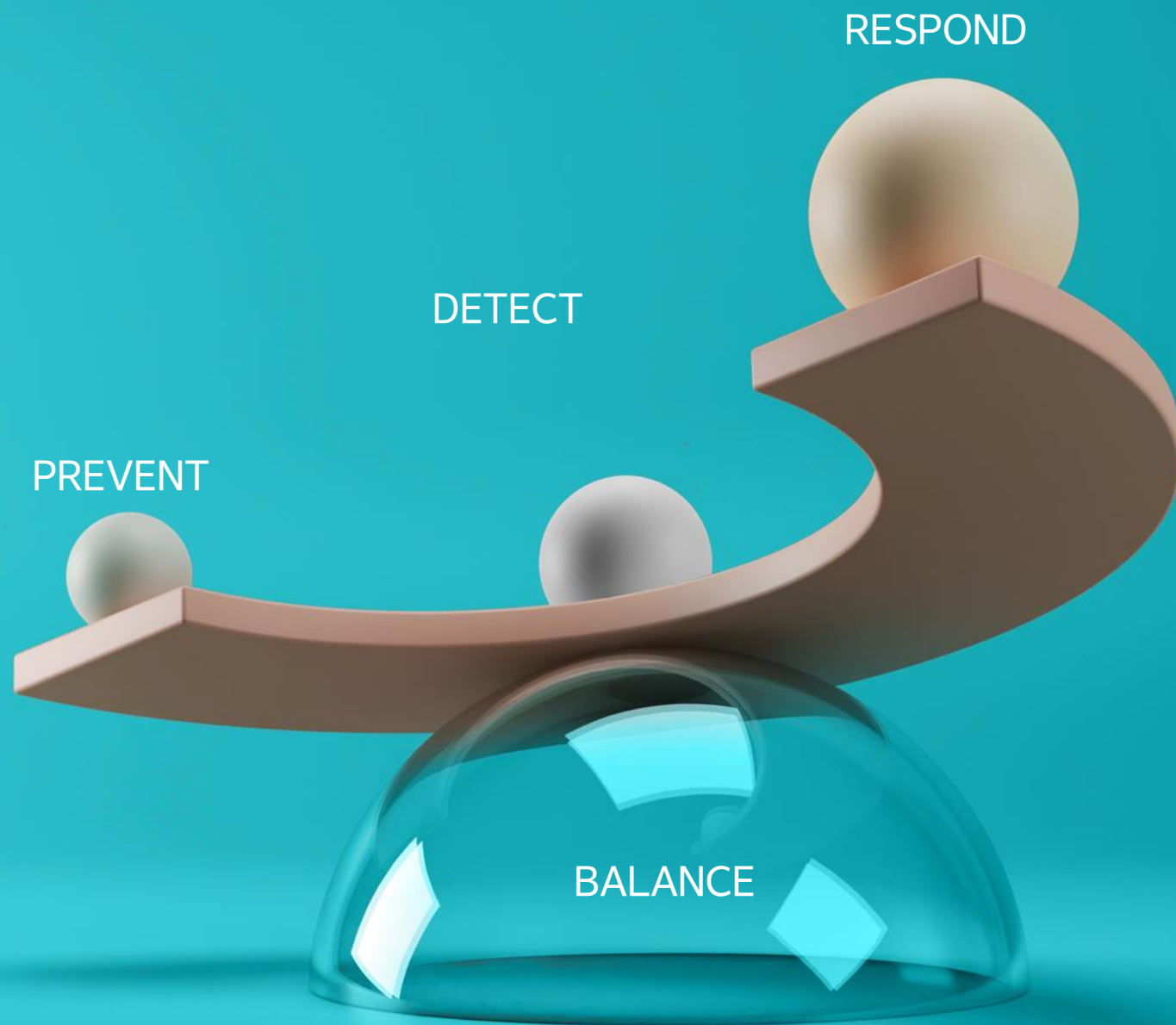


PREDICT

PREVENT / PROTECT

DETECT & RESPOND



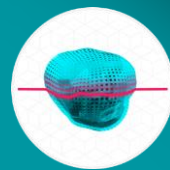




Reputation
and Cache



Ransomware
Shield



Advanced
Memory Scanner



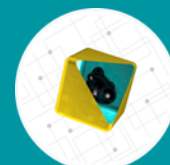
Brute-Force
Attack
Protection



Device
Control



DNA
Detections



In-Product
Sandbox



Deep Behavioral
Inspection



Exploit Blocker



Botnet
Protection



LiveGrid®
Protection



Secure
Browser



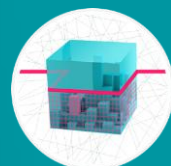
Script Scanner
& AMSI



Advanced
Machine Learning



Network Attack
Protection



UEFI
Scanner

POST EXECUTION

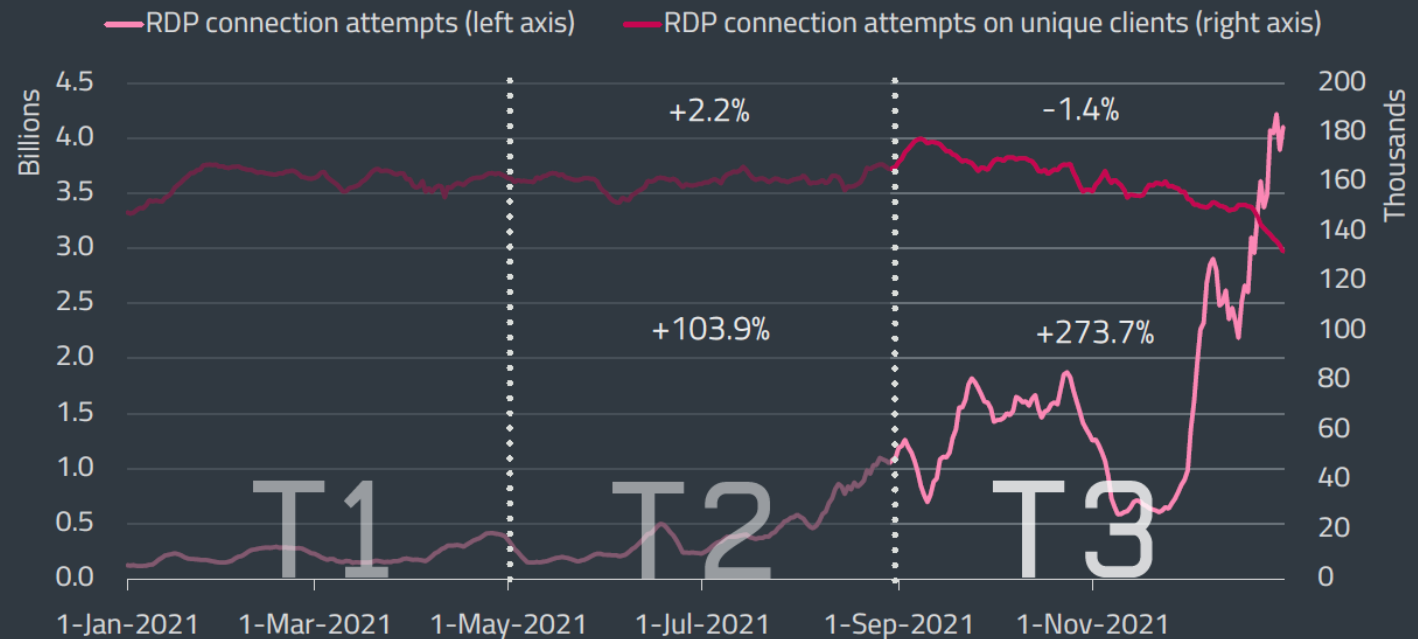
EXECUTION

PRE-EXECUTION



ESET Brute-Force Attack Protection

The last four months of 2021 brought a further acceleration of **brute-force attacks** against remote desktop protocol (RDP), with an **increase of 274%** between our T2 2021 and T3 2021 reports.



Trends of RDP connection attempts and unique clients in 2021, seven-day moving average

When “secure” isn’t secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer laptops

ESET researchers discover multiple vulnerabilities in various Lenovo laptop models that allow an attacker with admin privileges to expose the user to firmware-level malware



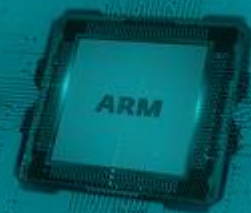
Martin Smolár

19 Apr 2022 - 11:30AM

Offering Update Q1/2022

NEW WINDOWS ON ARM64 DEVICE?

ESET protects both at work and at play



eset Digital Security
Progress. Protected.

ESET PARTNERS WITH INTEL

for software and
hardware-based detection

eset Digital Security
Progress. Protected.

intel.

UPDATED PRODUCT PORTFOLIO FOR YOUR BUSINESS DIGITAL SECURITY



Digital Security
Progress. Protected.



MULTI-LAYERED SECURITY

THREAT INTELLIGENCE

In-depth and actionable intelligence from ESET's world-renowned lab, provided by feeds and reports, that will notify you of organizations, cloud-based threats, IoT, APT, botnets and other types of attack that work together to protect your organization's endpoints, devices, file servers, mail servers and multi-factor authentication capabilities. ESET's unified security management platform delivers XDR and threat-hunting capabilities, and can be cloud-based or installed on-premises.

DETECTION AND RESPONSE

EXTENDED PROTECTION

Additional security layers comprising cloud-based threat defense against targeted attacks and new threat types, especially ransomware, plus dedicated protection for cloud office suites, and multi-factor authentication and encryption solutions to harden access protection.

ESSENTIAL PROTECTION

Multiple layers of prevention and detection, leveraging ESET's unique technologies, that work together to protect your organization's endpoints, devices, file servers, mail servers and SharePoint products.

PLATFORM AND SUPPORT

Access tailored support appropriate to your needs, plus deployment and configuration assistance. ESET's unified security management platform delivers XDR and threat-hunting capabilities, and can be cloud-based or installed on-premises.

		eset PROTECT ENTRY	eset PROTECT ADVANCED	eset PROTECT COMPLETE	eset PROTECT ENTERPRISE	eset PROTECT MDR
		Modern multilayered endpoint protection featuring strong machine learning and easy-to-use management	Best-in-class endpoint protection against ransomware and zero-day threats, backed by powerful data security	Complete, multilayered protection for endpoints, cloud applications and email, the #1 threat vector	Extended detection and response (XDR) that delivers enterprise-grade visibility, threat hunting and response options	Airtight protection of your IT environment, with cyber risk management and world-class ESET expertise on call
CORE COMPONENTS	ESET PROTECT PLATFORM CLOUD / ON-PREM	●	●	●	●	●
	MODERN ENDPOINT PROTECTION	●	●	●	●	●
	FILE SERVER SECURITY	●	●	●	●	●
	ADVANCED THREAT DEFENSE		●	●	●	●
	FULL DISK ENCRYPTION		●	●	●	●
	MAIL SECURITY			●	ⓘ	ⓘ
	CLOUD APP PROTECTION			●	ⓘ	ⓘ
	DETECTION & RESPONSE				●	●
OPTIONAL SOLUTIONS	SHAREPOINT SECURITY	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ
	ENDPOINT ENCRYPTION	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ
	AUTHENTICATION	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ
SERVICES	COMPLIMENTARY TECHNICAL SUPPORT	●	●	●	●	●
	PREMIUM SUPPORT ADVANCED	ⓘ	ⓘ	ⓘ	ⓘ	●
	DEPLOYMENT & UPGRADE	ⓘ	ⓘ	ⓘ	ⓘ	●
	SECURITY SERVICES	ⓘ	ⓘ	ⓘ	ⓘ	●
	MANAGED DETECTION & RESPONSE (MDR)				ⓘ	●

Additional solutions

ESET PROTECT Mail Plus: includes ESET PROTECT Platform, Advanced Threat Defense, Mail Security

ESET PROTECT Essential*: includes ESET PROTECT Platform, Endpoint Antivirus Protection

*Only available from your local partner or reseller

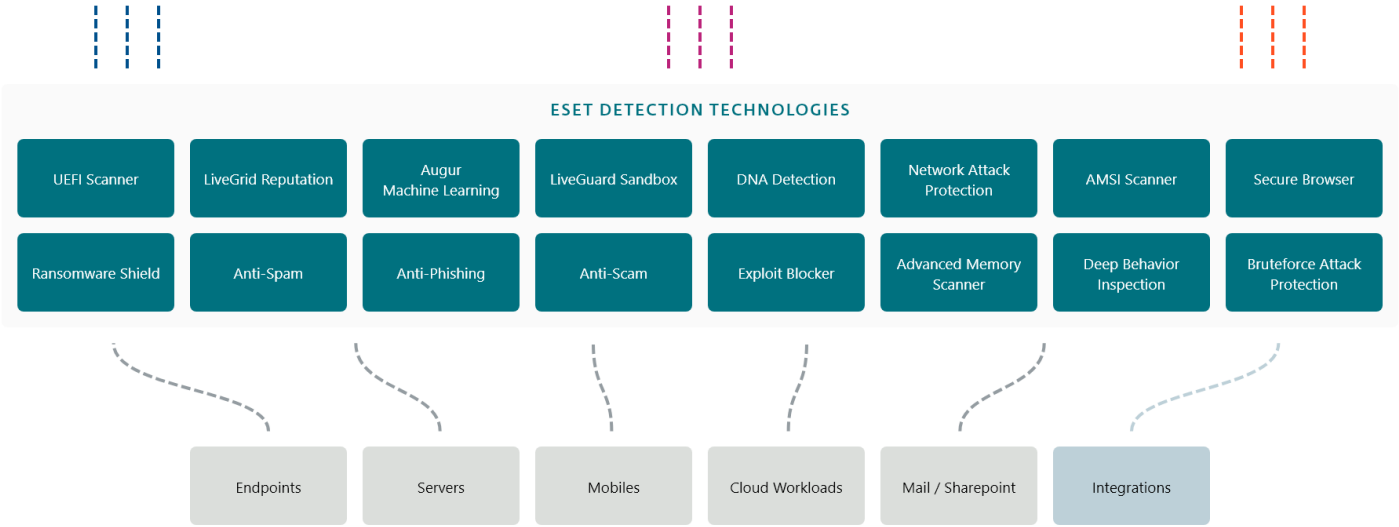
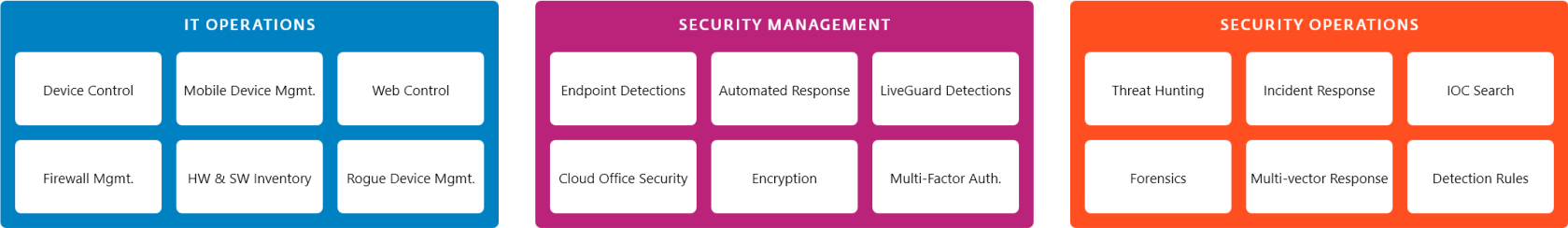
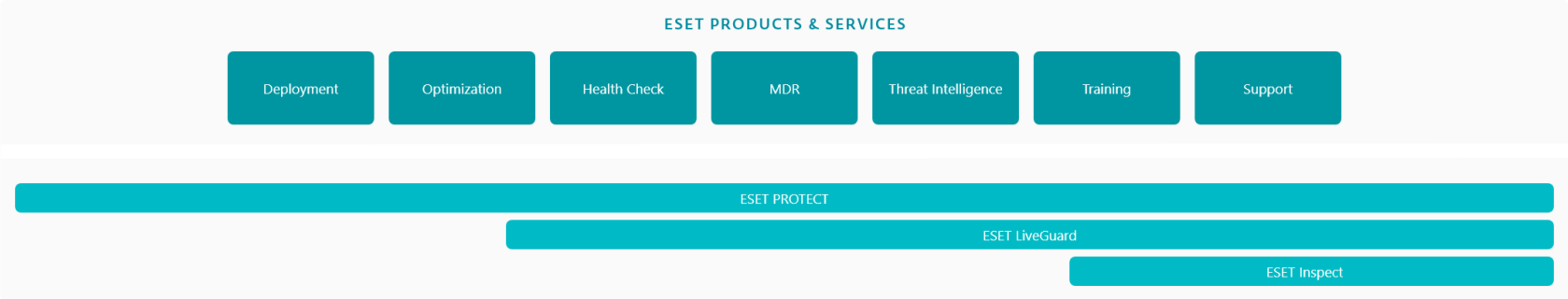
● Included

ⓘ Optional

ESET PROTECT Platform

(XDR)





Different P/D/R levels of our PROTECT Platform packages

	PREVENT	DETECT	RESPOND	MANAGE
PROTECT ENTRY	<ul style="list-style-type: none"> • Augur Machine Learning • Ransomware Shield • Exploit Blocker • DNA detections • Deep Behavioral Inspection • Real-Time Memory Scanning • Network Attack Protection • LiveGrid Detections • Bruteforce Attacks Protection • Script and AMSI scanning • Secure Browser • Webfiltering – Malware, Phishing, Scam, Spam • Built-in Threat Feeds • Device Control • Firewall • Botnet Protection • HIPS custom rules 	<ul style="list-style-type: none"> • Configurable detection thresholds for Malware, PUA, PUS, and Suspicious Apps. • UEFI firmware threats • SysInspector security snapshot 	<ul style="list-style-type: none"> • Automatic by Endpoint (block, quarantine, clean) • Automation in PROTECT (task, script, policy) • Manual (network isolation, reboot, shutdown, SysInspector scripts) 	<ul style="list-style-type: none"> • Software Inventory • Hardware Inventory • OS Patching • 3rd party software installation • Rogue device discovery • Mobile Devices (iOS / Android)
PROTECT ADVANCED	<ul style="list-style-type: none"> • ENTRY + • LiveGuard „multi vector“ cloud prevention sandbox with Cloud Machine Learning 	<ul style="list-style-type: none"> • ENTRY + • LiveGuard behavior report and sensitivity settings • Data at Rest via ESET Full Disk Encryption 	<ul style="list-style-type: none"> • ENTRY + • Automated network wide by LiveGuard (blocklist), based on detection thresholds 	<ul style="list-style-type: none"> • As in ENTRY
PROTECT ENTERPRISE	<ul style="list-style-type: none"> • ADVANCED + • Hash blacklisting 	<ul style="list-style-type: none"> • ADVANCED + • Inspect custom rules system • Inspect Executables / Script anomalous behavior reporting system • Inspect IOC search / hunting engine • Threat Intelligence Data 	<ul style="list-style-type: none"> • ADVANCED + • Automated actions within the Inspect rules system • Kill Process • Download executable • Add to blocklist • Remote Shell 	<ul style="list-style-type: none"> • As in ENTRY • Hash blocklist can be used for App control

From „Remote Administrator“ to „ESET PROTECT Platform“

Version	1.X – 5.X	6.X	7.X + ECA		8.X + PROTECT		9.X + PROTECT	
Year	<2014	2015-2018	2018-2020		2020-2021		2022	
Architecture	Native App	Web Based	Web Based		Web Based		Web Based	
Platform	On Prem, Win	On Prem, Win + Lin + Virtual Appliance + Azure Image	Cloud	On Prem, Win + Lin + Virtual Appliance + Azure Image	Cloud	On Prem, Win + Lin + Virtual Appliance + Azure Image	Cloud	On Prem, Win + Lin + Virtual Appliance
Name	Remote Administrator	Remote Administrator	Cloud Administrator	Security Management Center	PROTECT Cloud	PROTECT	PROTECT Cloud	PROTECT
Scalability	<10k	100k+	250	100k+	10k+	100k+	25k+ Inspect 5k	100k+ Inspect 15k
Integrates				EDTD Enterprise Inspector	EDTD	EDTD Enterprise Inspector	LiveGuard INSPECT Cloud MDM	LiveGuard INSPECT
Positioning	Remote Management Console	Remote Management Console	SMB focused Cloud based Remote Management Console	Security Management Console	Security Management Console	Security Management Console	Frontend to the ESET PROTECT XDR Platform	
Offering (primary)	Standalone licenses 5.X+ Bundles	Standalone licenses Bundles (EEPS, EEPA, ESB, ESE)	Bundles (EEPSC, EEPAC, ESBC)	Standalone licenses Bundles (EEPS, EEPA, ESB, ESE)	PROTECT solutions (ENTRY, ADVANCED, COMPLETE, ENTERPRISE*)	Standalone licenses PROTECT-OP solutions (ESSENTIAL, ESSENTIAL PLUS, ENTRY, ADVANCED, COMPLETE, ENTERPRISE)	PROTECT solutions (ENTRY, ADVANCED, COMPLETE, ENTERPRISE, MDR)	PROTECT-OP solutions (ENTRY, ADVANCED, COMPLETE, ENTERPRISE, MDR)

Future of our offering



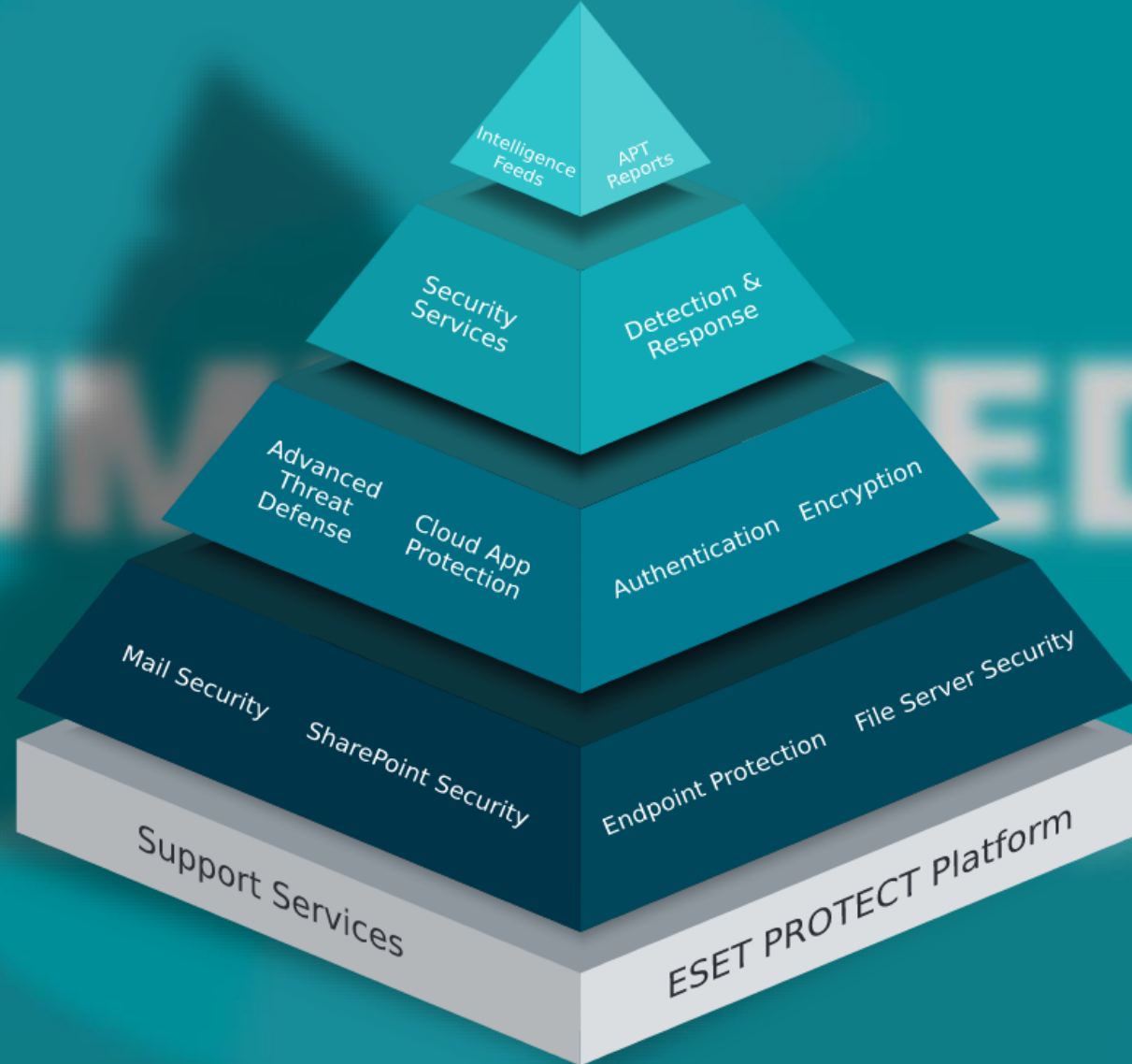
How the future
looks like?



How the future looks
like?

The background is a solid teal color with several overlapping circular and semi-circular shapes in varying shades of teal. These shapes create a layered, geometric effect. In the center, the word "SIMPLIFIED." is written in a white, bold, sans-serif font.

SIMPLIFIED.





UNIFIED.

eset HUB

DASHBOARD

CUSTOMERS

LICENSES & SUBS

DEVICES

SERVICES & SUP

REPORTS

Notifications

Users

Settings

Audit logs

ESET BUSINESS ECOSYSTEM

ESET HUB

SERVICE HUB

PARTNER PORTAL

EDUCATION PORTAL

TECHNICAL SUPPORT

KNOWLEDGEBASE & HELP

ESET PROTECT ECOSYSTEM

PROTECT

INSPECT

LIVEGUARD

MOBILE DEVICE MANAGEMENT

FULL DISK ENCRYPTION

CLOUD OFFICE SECURITY

THREAT INTELLIGENCE

SECURE AUTHENTICATION

QUICK LINKS

HELP

REECE ELLER

LOG OUT

ADD FILTER

SEARCH

PRESETS

TYPE	QUANTITY	STATUS	TRIAL	EXPIRATION
Fully-managed	300/300			Monthly subscription
Fully-managed	3867/4000			Monthly subscription
Co-managed	2568/2579		✓	7/3/2021
Unmanaged	2568/2579		✓	7/3/2021
Unmanaged	4/5			4/2/2024
Fully-managed	1000/1000			Monthly subscription
Co-managed	5500/6500			Monthly subscription
Unmanaged	5500/6500			Monthly subscription
Co-managed	600/680			Monthly subscription
Fully-managed	600/680			Monthly subscription
Unmanaged	5611/5613			Monthly subscription
Unmanaged	543/545			Monthly subscription
Unmanaged	8330/8330			Monthly subscription
Fully-managed	15/15		✓	7/2/2021
Fully-managed	1200/1205			22/2/2025
Co-managed	2458/2459			Monthly subscription

ADD LICENSE

EXPORT

Submit feedback

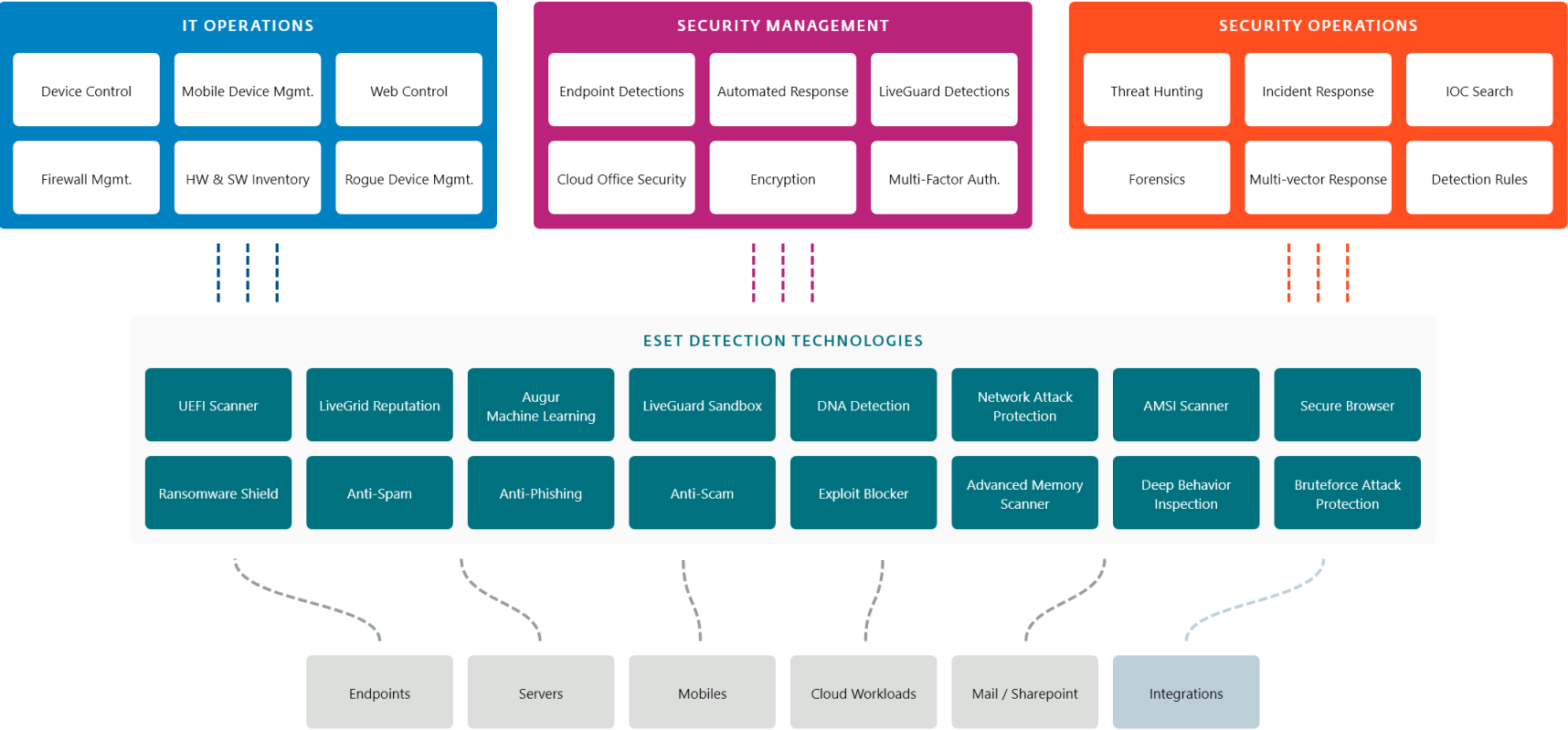
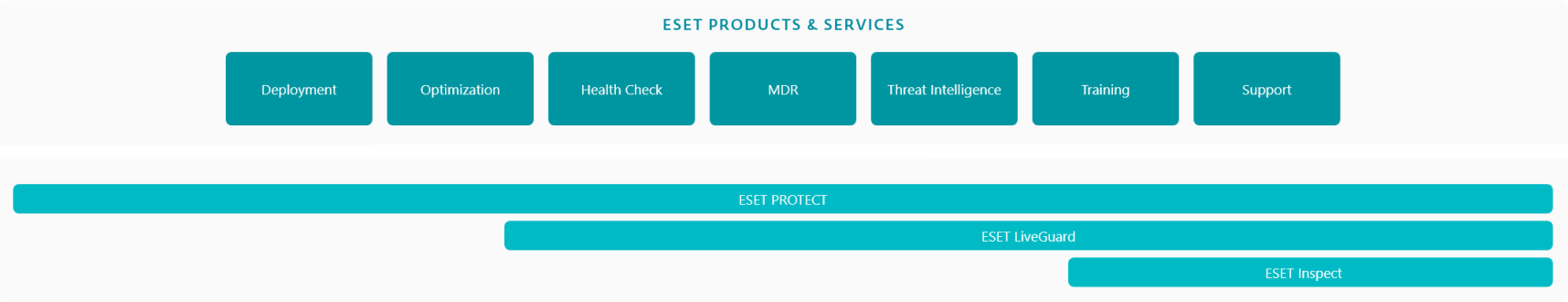
ch another,

The background is a solid teal color. Overlaid on this are several concentric circles and a large, stylized letter 'C' shape, all in varying shades of teal. The 'C' shape is formed by two concentric arcs, creating a thick, open letter. The word 'CONSISTENT.' is written in white, uppercase, sans-serif font across the center of the image, positioned within the 'C' shape.

CONSISTENT.



PLATFORM.



The background is a solid teal color with several overlapping circular and semi-circular shapes in varying shades of teal. These shapes create a layered, geometric effect. In the center, the text "CLOUD. FIRST." is written in a white, sans-serif font.

CLOUD. FIRST.



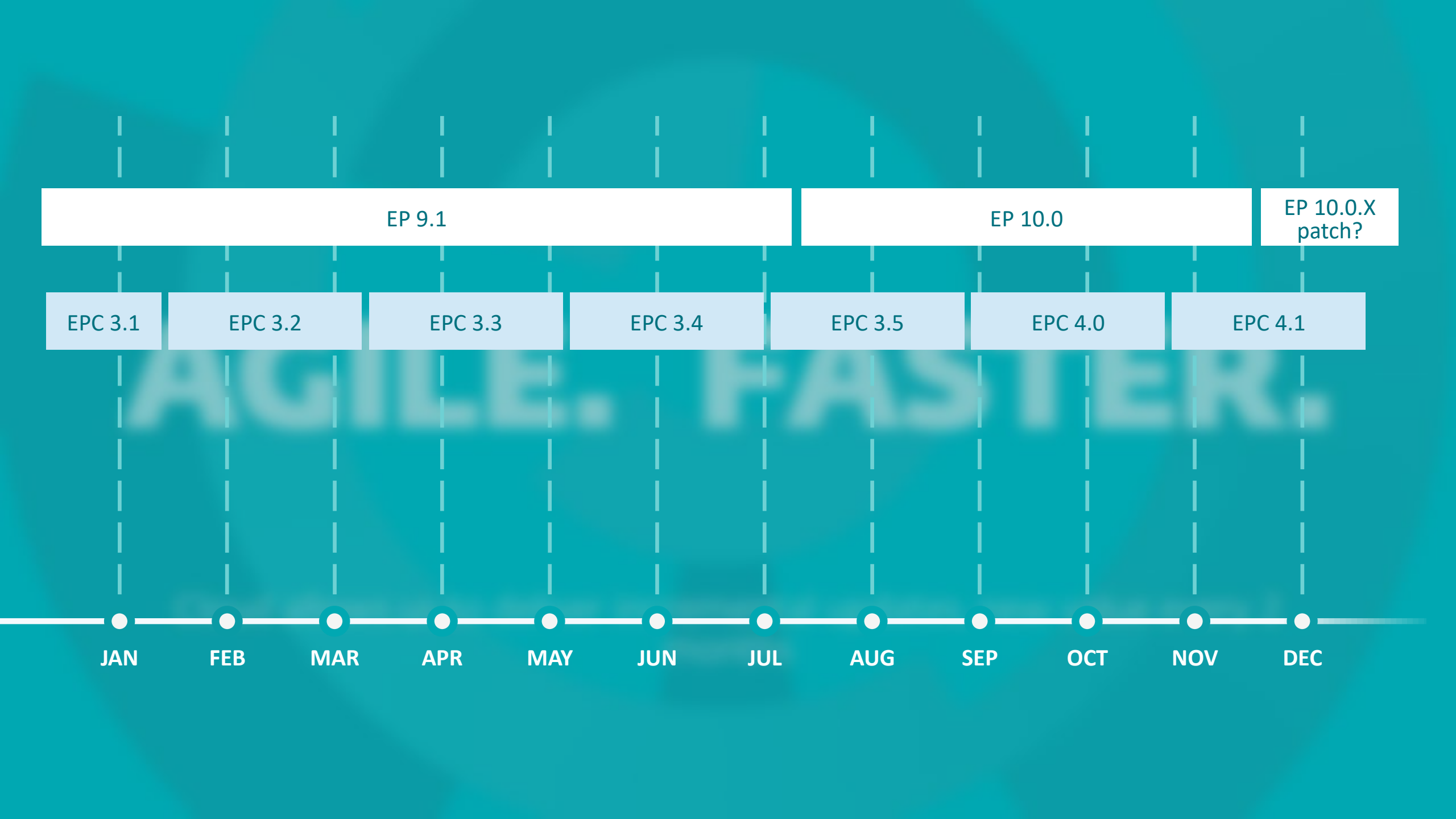


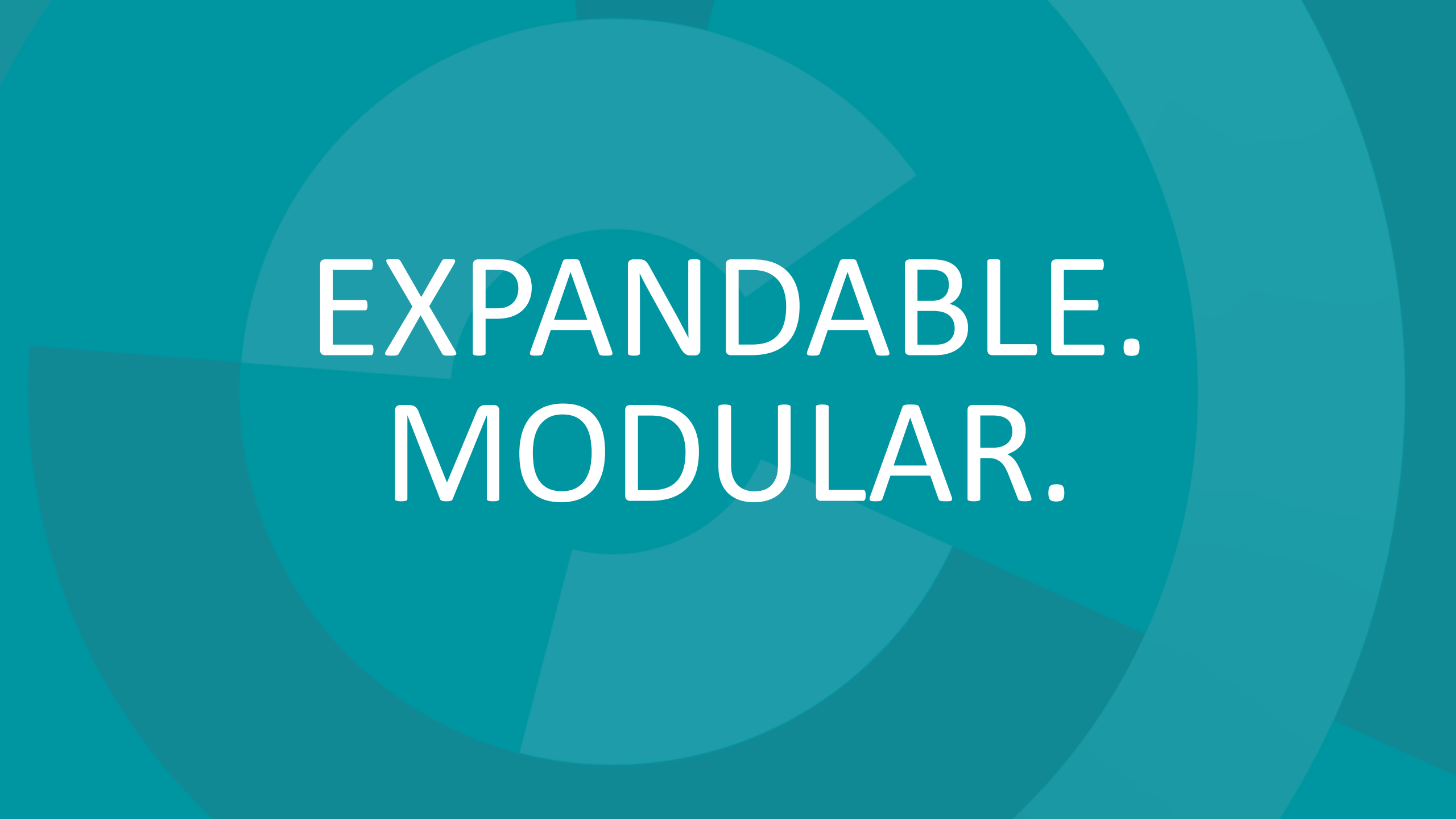
UP TO DATE.





AGILE. FASTER.





EXPANDABLE.
MODULAR.

	ENTRY	ADVANCED	COMPLETE	ENTERPRISE	FUTURE	MDR
EP						
EFDE						
LGA						
ECOS						
INSPECT						
CESA						
SERVICES						
VA PM	optional	optional	optional	optional	optional	optional
ECAT	optional	optional	optional	optional	optional	optional

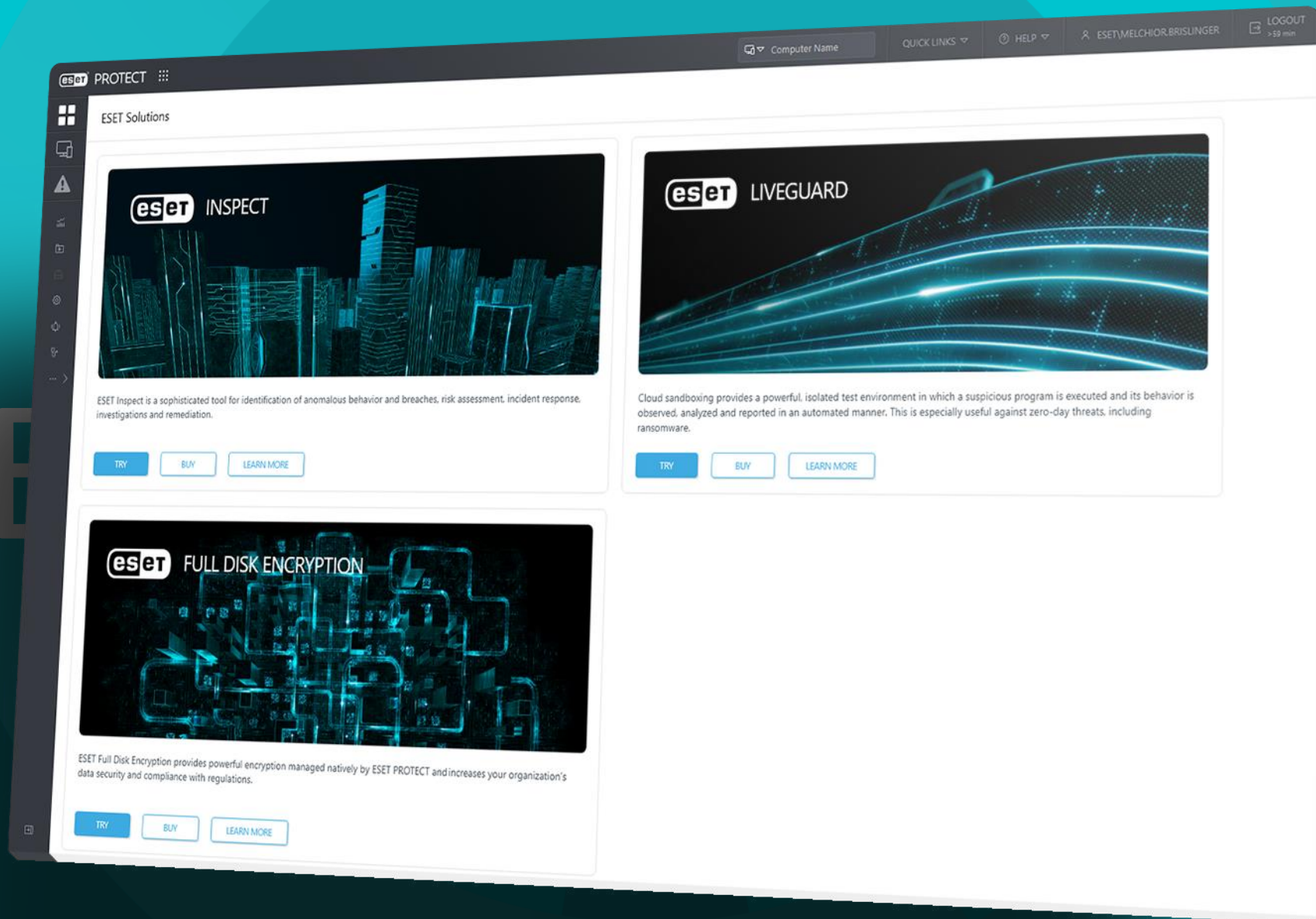


SUBSCRIPTION.

	1	1.3	1.6	2	2.3	4.6
MDR						
FUTURE						
ENTERPRISE						
COMPLETE						
ADVANCED						
ENTRY						



FEW CLICKS AWAY.



The background is a solid teal color with several overlapping circular and semi-circular shapes in varying shades of teal. These shapes create a layered, geometric effect. The word "PROTECT." is centered in the middle of the image in a white, sans-serif font.

PROTECT.

ESET PROTECT components

Includes ESET Endpoint Security
Endpoint Protection

Advanced **multilayered protection** for computers, smartphones and virtual machines. [Learn more](#)

Includes ESET Server Security
File Server Security

Real-time protection for your company's data passing through all general servers. [Learn more](#)

Includes ESET Full Disk Encryption
Full Disk Encryption

Robust encryption solution for system disks, partitions or entire devices to achieve legal compliance. [Learn more](#)

Management Console

Includes ESET PROTECT

Unified security management platform with XDR and threat hunting capabilities. Available as cloud or on-prem deployment. [Learn more](#)

Includes ESET LiveGuard Advanced
Advanced Threat Defense

Proactive cloud-based defense against zero-day and never-before-seen threat types. [Learn more](#)

Includes ESET Inspect
Extended Detection & Response

The XDR-enabling component of the ESET PROTECT platform, delivering breach prevention, enhanced visibility and remediation. [Learn more](#)

Includes ESET Detection & Response Ultimate
MDR Service

Investigate, identify and resolve threats. Full-fledged MDR with proactive threat hunting and monitoring. [Learn more](#)

Premium Support

Includes ESET Premium Support Advanced

Help from ESET experts, whenever you need it. [Get the maximum return on](#)



PROGRESS.

			ESET Protect ENTRY	ESET Protect ADVANCED	ESET Protect COMPLETE	ESET Protect ENTERPRISE	ESET Protect „FUTURE“	ESET Protect MDR
Standard offering	ESET PROTECT Platform		●	●	●	●	●	●
	Modern Endpoint Protection		●	●	●	●	●	●
	Server Security		●	●	●	●	●	●
	Advanced Threat Defense (LiveGuard)			●	●	●	●	●
	Full Disk Encryption			●	●	●	●	●
	Mail Security				●		●	
	Cloud App Protection				●		●	
	Cloud – Q1/2022 MSP – Q3/2022	Detection & Response				●	●	●
Optional offering	Sharepoint Security		◐	◐	◐	◐	◐	◐
	Endpoint Encryption		◐	◐	◐	◐	◐	◐
	Cloud H2/'22 – H1/'23	Authentication	◐	◐	◐	◐	◐	◐
	Future Additions H1/2023	Vulnerability and Patch Management	◐	◐	◐	◐	◐	◐
		Cybersecurity Awareness Training	◐	◐	◐	◐	◐	◐
Services	Standard Support		●	●	●	●	●	●
	Premium Support Essential		◐	◐	◐	◐	◐	
	Premium Support Advanced		◐	◐	◐	◐	◐	●
	Deployment and Upgrade		◐	◐	◐	◐	◐	●
	Detection and Response Essential		◐	◐	◐			
	Detection and Response Advanced					◐	◐	
	Detection and Response Ultimate							●



**SECURITY
DAYS**

Ďakujem za pozornosť!



Digital Security
Progress. Protected.

&



konferencie