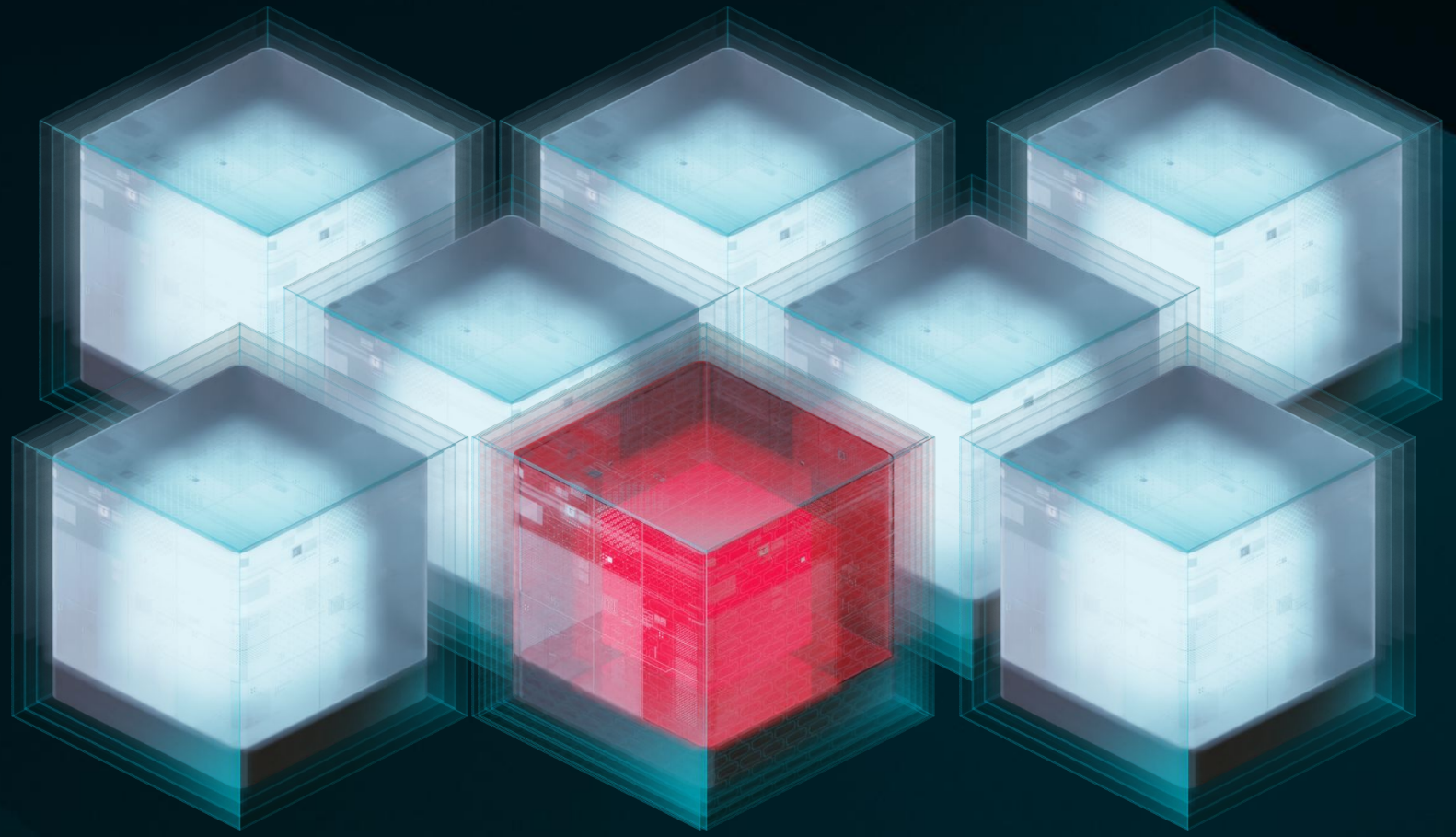
MODERNÉ SPÔSOBY OCHRANY INFRAŠTRUKTÚRY A AKO Z NICH VYŤAŽIŤ ČO NAJVIAC

Ondrej Krajč

Súčasnosť

Éra pokročilých kybernetických útokov



PREVENCIA

DETEKCIA

REAKCIA

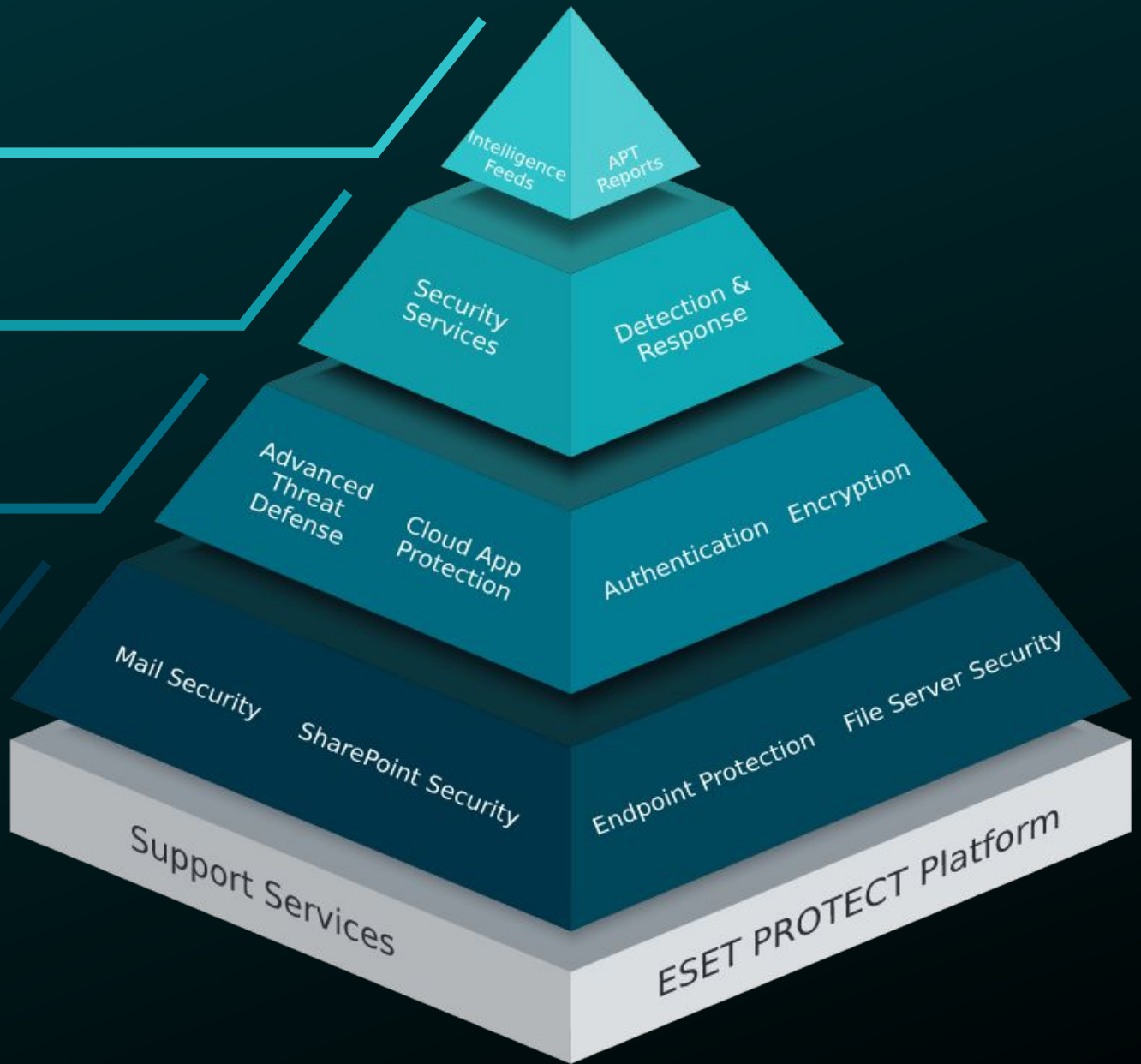
VIACÚROVŇOVÉ ZABEZPEČENIE

INFORMÁCIE O HROZBÁCH

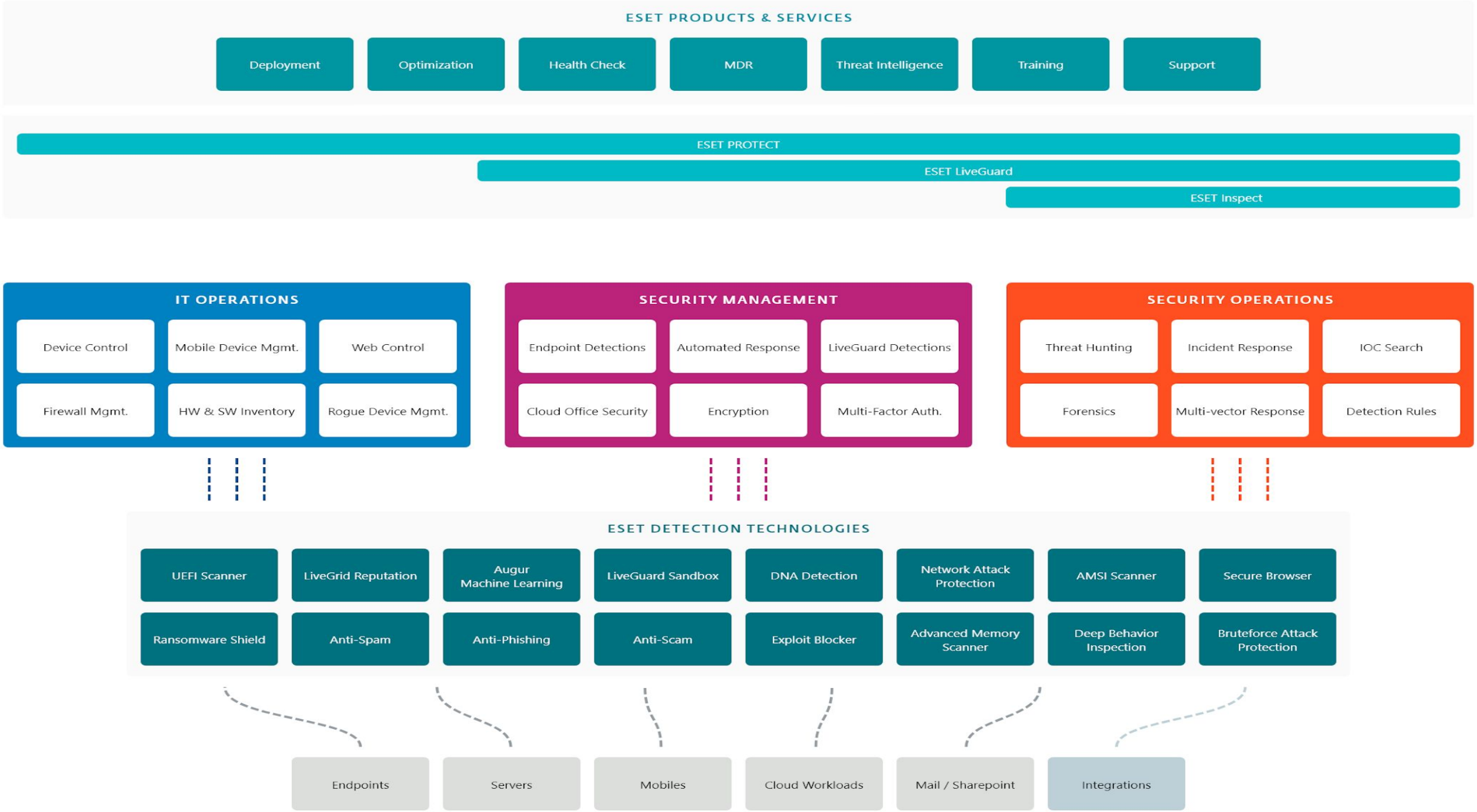
DETEKCIA A REAKCIA

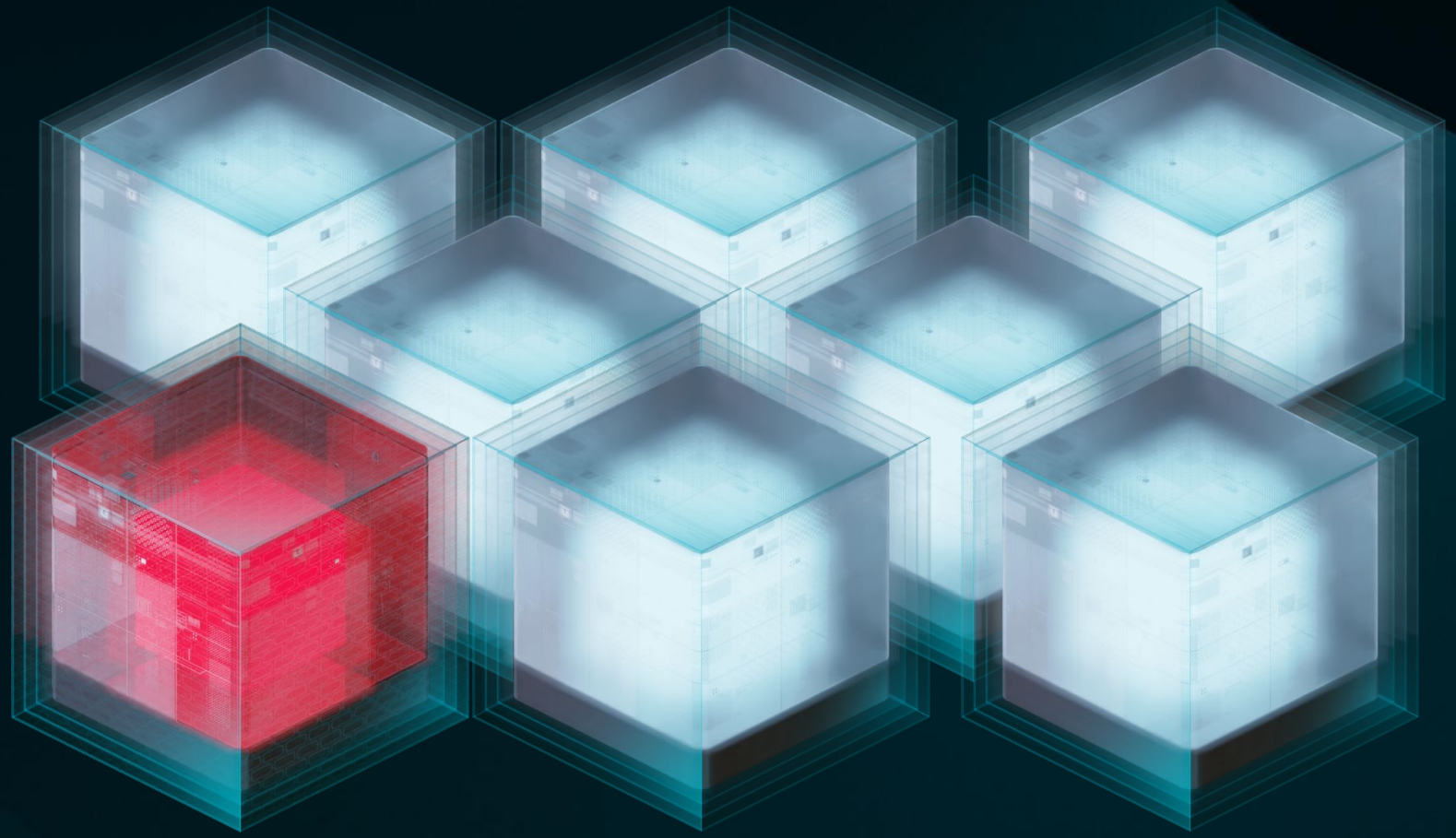
ROZŠÍRENÁ OCHRANA

ZÁKLADNÁ OCHRANA

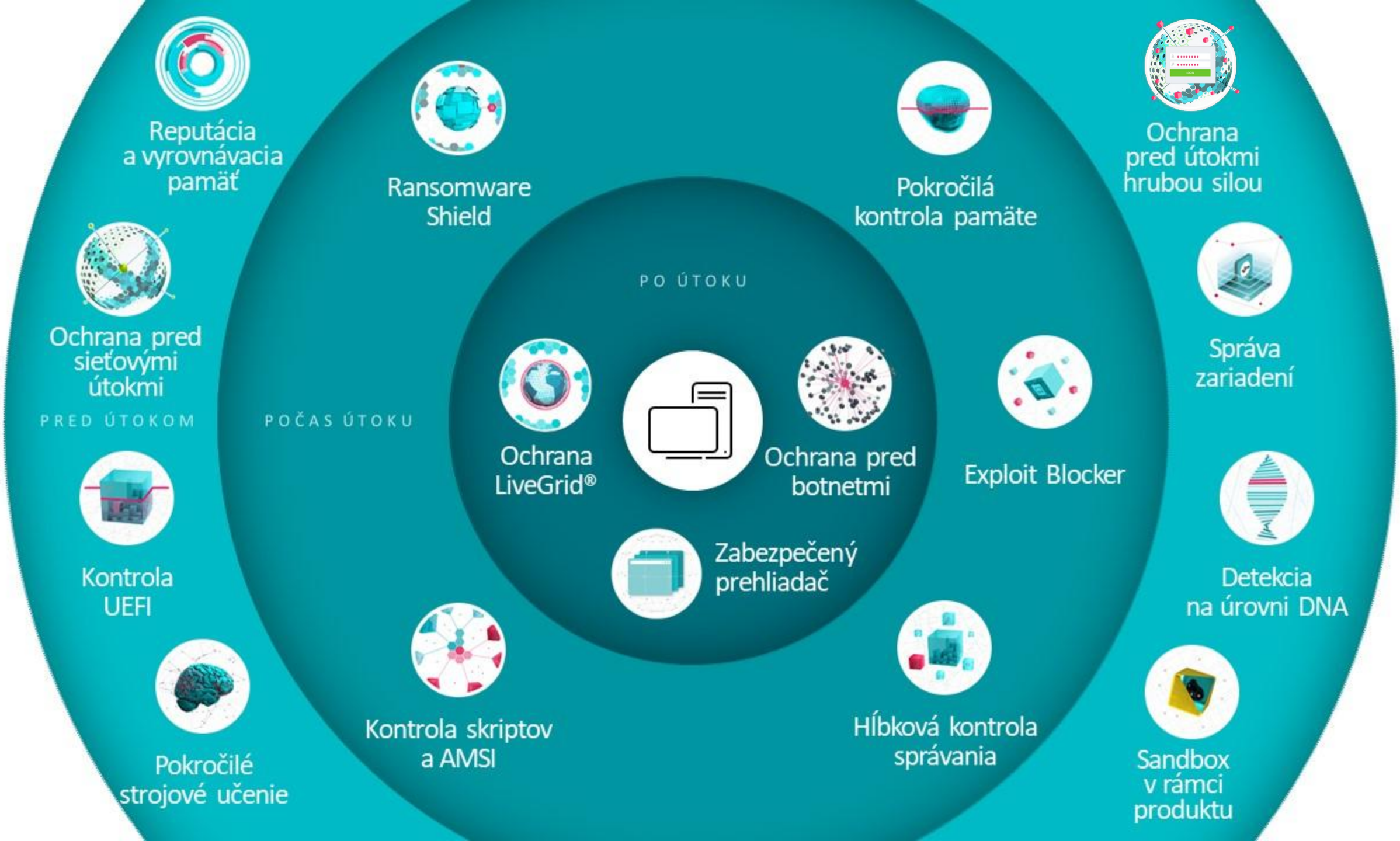


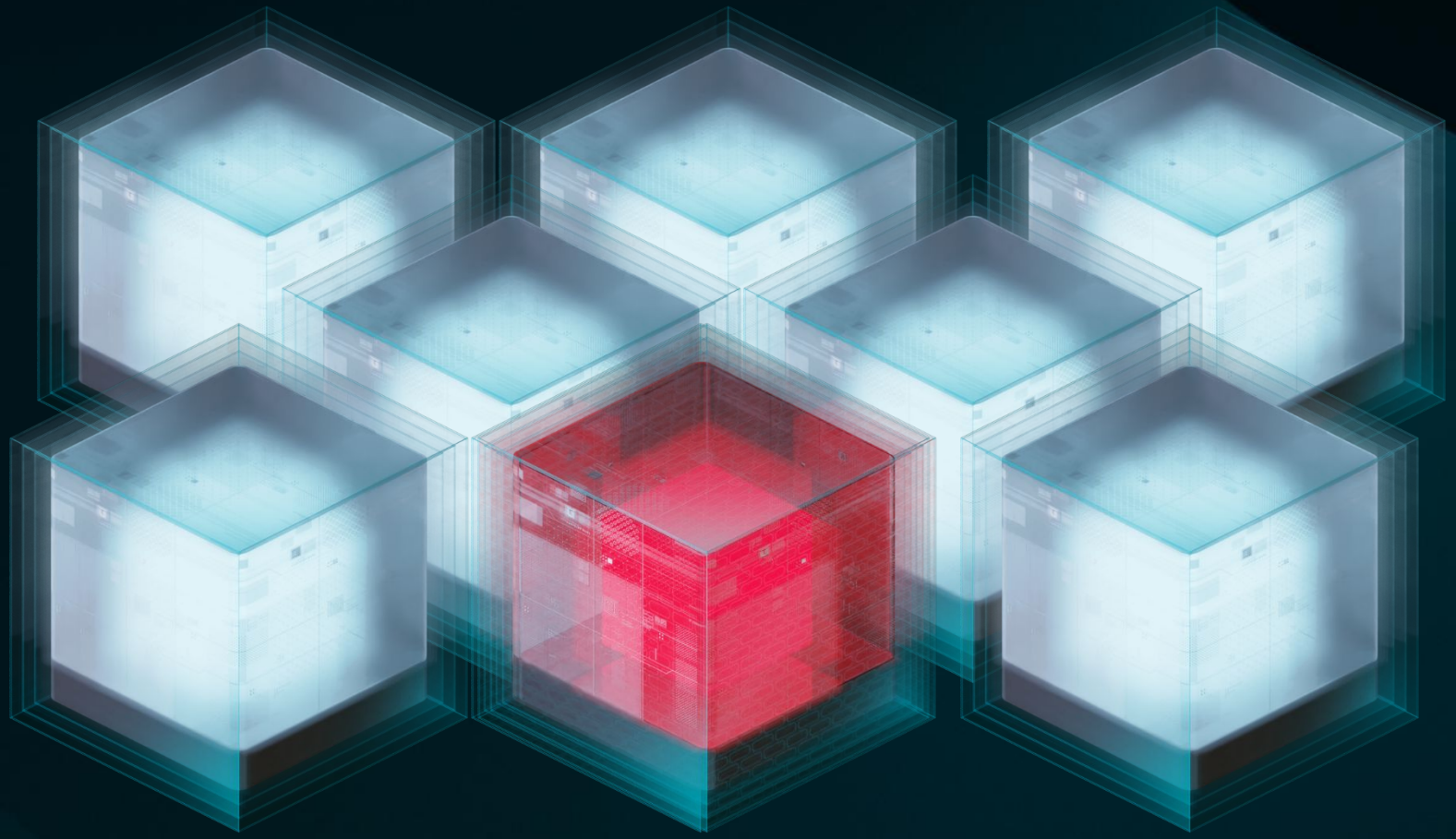
ESET PROTECT Ecosystem => XDR Platforma


ESET PRODUCTS & SERVICES
Deployment
Optimization
Health Check
MDR
Threat Intelligence
Training
Support
ESET PROTECT
ESET LiveGuard
ESET Inspect
IT OPERATIONS
Device Control
Mobile Device Mgmt.
Web Control
Firewall Mgmt.
HW & SW Inventory
Rogue Device Mgmt.
SECURITY MANAGEMENT
Endpoint Detections
Automated Response
LiveGuard Detections
Cloud Office Security
Encryption
Multi-Factor Auth.
SECURITY OPERATIONS
Threat Hunting
Incident Response
IOC Search
Forensics
Multi-vector Response
Detection Rules
ESET DETECTION TECHNOLOGIES
UEFI Scanner
LiveGrid Reputation
Augur Machine Learning
LiveGuard Sandbox
DNA Detection
Network Attack Protection
AMSI Scanner
Secure Browser
Ransomware Shield
Anti-Spam
Anti-Phishing
Anti-Scam
Exploit Blocker
Advanced Memory Scanner
Deep Behavior Inspection
Bruteforce Attack Protection
Endpoints
Servers
Mobiles
Cloud Workloads
Mail / Sharepoint
Integrations



PREVENCIA

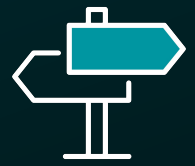

Reputácia a vyrovnávacia pamäť
Ransomware Shield
Pokročilá kontrola pamäte
Ochrana pred útokmi hrubou silou
Ochrana pred sieťovými útokmi
PRED ÚTOKOM
POČAS ÚTOKU
PO ÚTOKU
Správa zariadení
Ochrana LiveGrid®
Ochrana pred botnetmi
Exploit Blocker
Kontrola UEFI
Zabezpečený prehliadač
Detekcia na úrovni DNA
Kontrola skriptov a AMSI
Hĺbková kontrola správania
Pokročilé strojové učenie
Sandbox v rámci produktu



DETEKCIA

Detekcia bez podpory XDR a Inspect

Minimálny prehľad



Neistota

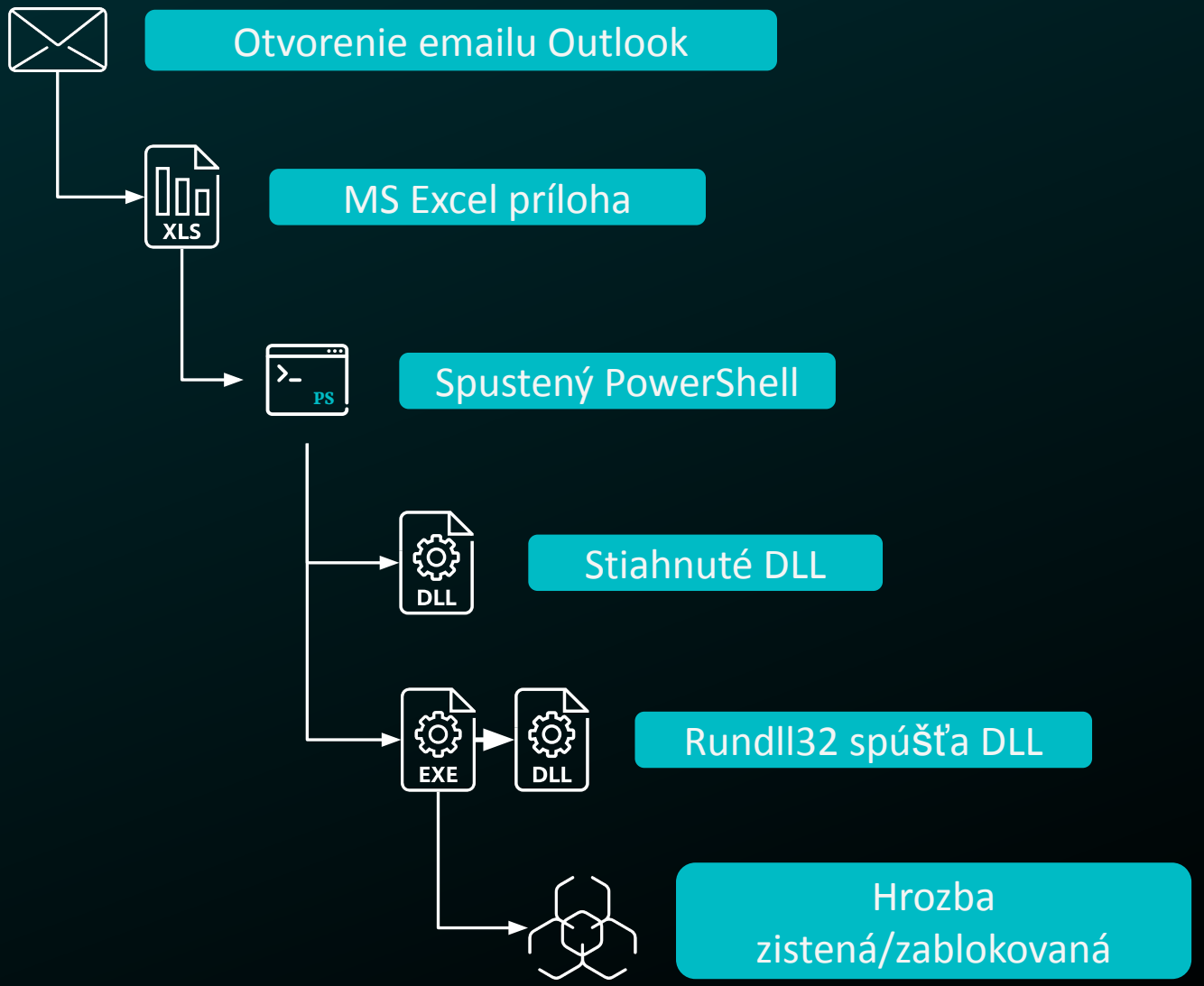
Rundll32 spúšťa DLL

Hrozba zistená/zablokovaná

Detekcia s podporou XDR a Inspect

Zvýšený prehľad

Pokoj v duši :)



ESET INSPECT CLOUD

DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE

BACK | All > ESETdemo > Desktops > cl1-it.esetdemo.local > rar.exe > rar.exe

Details | Aggregated Events | Detections | Raw Events | Loaded Modules (DLLs) | Scripts

rar.exe
PE: Command line RAR
Select Tags

SHA-1	3D42B2C0C6A7CBBADD299BD981B43FACE...
Signature type	Trusted
Signer Name	win.rar GmbH
Seen on	1 computer
First Seen	16 days ago - Mar 28, 2022, 1:29:04 PM
Last Executed	16 days ago - Mar 28, 2022, 1:56:41 PM

ESET LiveGrid®

Reputation	
Popularity	
First Seen	2 years ago

Events

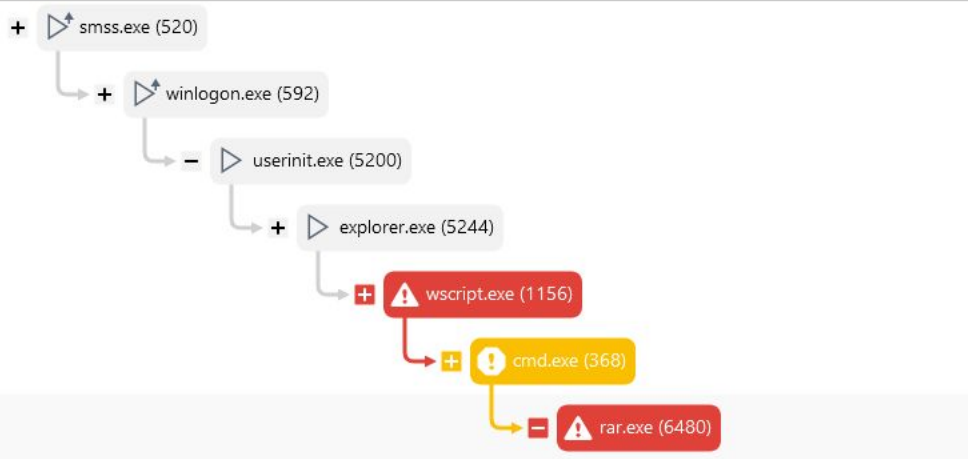
File	Registry	Network
4	0	0

cl1-it.esetdemo.local

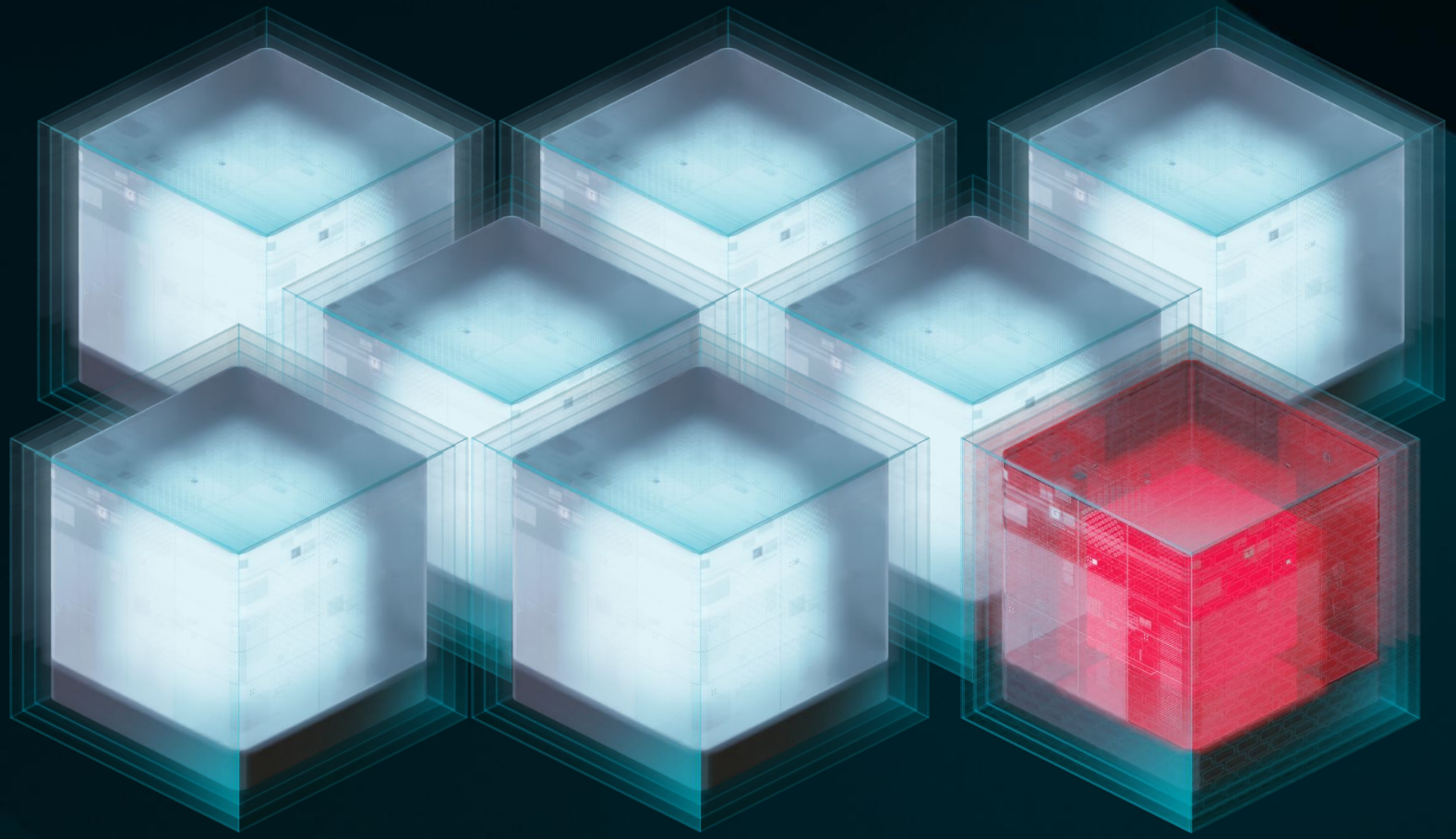
Parent Group	Desktops
Last Connected	11 hours ago - Apr 13, 2022, 1:37:01 AM
Last Event	11 hours ago - Apr 13, 2022, 1:36:26 AM
ESET Inspect Connector Version	1.7.1909
OS Name	Microsoft Windows 10 Enterprise
OS Version	10.0.19044.1645

Process	rar.exe (6480)
Command Line	a -dw -ep1 -inul -r -ai -y -ed -ibck -m0 -pflagC_psswrd "\Users\Administrator\Documents\trace_flagB_28-mar-22-13_56_41.rar" "\Users\Administrator\Documents\trace.log"
Path	%TMP%\winrar\
Started	16 days ago - Mar 28, 2022, 1:56:41 PM
Ended	16 days ago - Mar 28, 2022, 1:56:41 PM
Parent process	cmd.exe (368)
First dropper	7zg.exe (10992)

INCIDENT | DOWNLOAD FILE | KILL PROCESS



RAR encrypts and deletes files [B0601]



REAKCIA

ESET XDR a Inspect – “R” ako Reakcia

Blokovanie Hashu
Ukončenie procesu

Spustenie skenovania
Stiahnutie súboru

Reštartovanie
Vypnutie

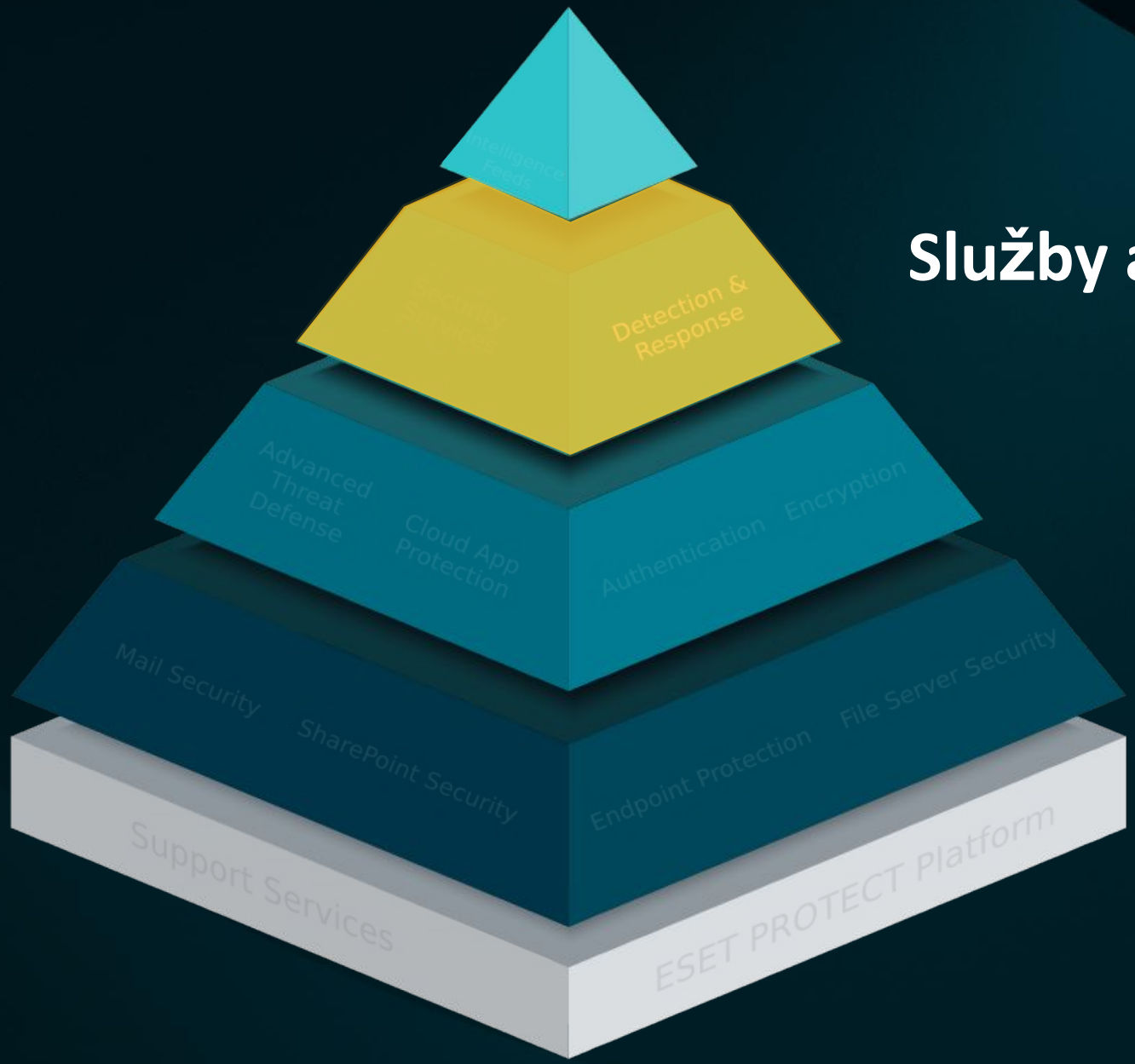
Sieťová izolácia

Vzdialený prístup
PowerShell

Hlavné výhody

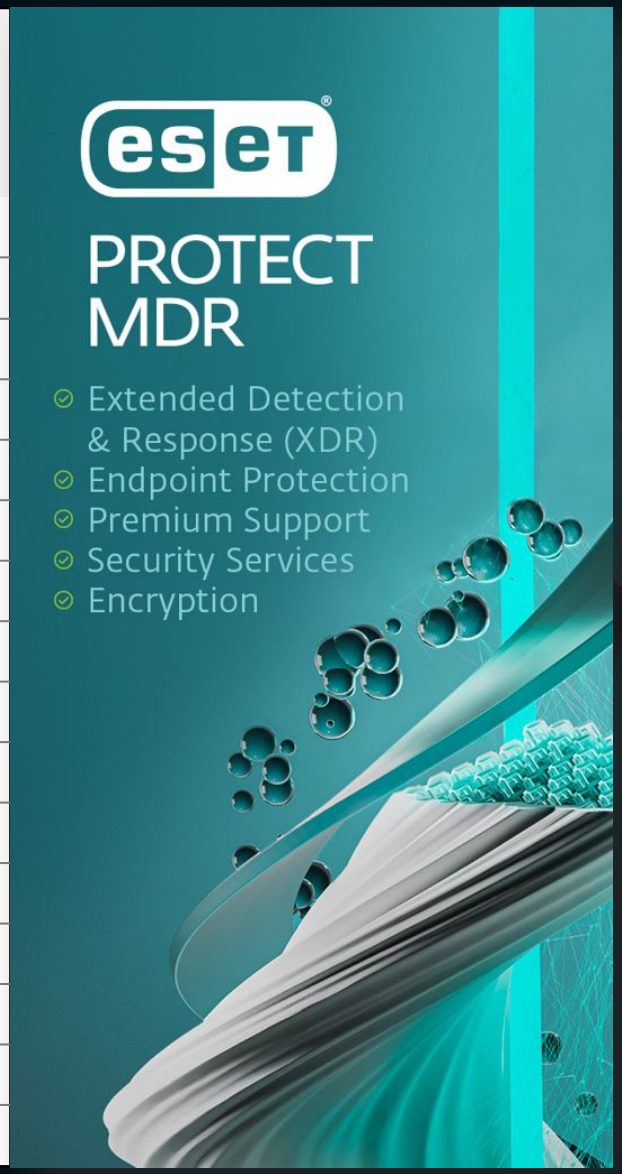
1. zrýchlenie odozvy na 0-day zraniteľnosti a APT’s
2. Odhaľovanie problematických užívateľov
3. izolovanie problematických staníc
4. kompletný prehľad
5. možnosť integrácie so SIEM

Služby a (MDR)


Intelligence Feeds
Security Services
Detection & Response
Advanced Threat Defense
Cloud App Protection
Authentication
Encryption
Mail Security
SharePoint Security
Endpoint Protection
File Server Security
Support Services
ESET PROTECT Platform

ESET PROTECT MDR

		ESET PROTECT MDR
Základné komponenty	Platforma ESET PROTECT	●
	Moderná ochrana koncových zariadení	●
	Zabezpečenie súborových serverov	●
	Pokročilá ochrana pred hrozbami	●
	Šifrovanie celého disku	●
	Ochrana e-mailovej komunikácie	◐
	Ochrana cloudových aplikácií	◐
	Detekcia a reakcia	●
Voliteľné riešenia	Zabezpečenie SharePointu	◐
	Šifrovanie koncových zariadení	◐
	Overovanie	◐
Služby	Doplnková technická podpora	●
	ESET Premium Support Advanced	●
	ESET Deployment & Upgrade	●
	ESET Security Services	●
	ESET Managed Detection & Response	●



ESET PREMIUM SUPPORT ADVANCED

	ŠTANDARDNÁ PODPORA	ESET PREMIUM SUPPORT ESSENTIAL	ESET PREMIUM SUPPORT ADVANCED
Časový limit odpovede na kritické incidenty (A)	podľa dostupnosti	2 hodiny	2 hodiny
Časový limit odpovede na závažné incidenty (B)	podľa dostupnosti	4 hodiny	4 hodiny
Časový limit odpovede na bežné požiadavky (C)	podľa dostupnosti	1 pracovný deň	1 pracovný deň
Dostupnosť technickej podpory	8:00 – 18:30 len v pracovných dňoch	nepretržite	nepretržite
Kontaktné osoby na strane zákazníka	obmedzené	neobmedzené	neobmedzené
Priorita v rámci telefonických požiadaviek	✘	áno	áno
Počet žiadostí oprávnených na spracovanie v rámci prémiovej podpory	✘	obmedzené	neobmedzené
Dedikovaný Technical Account Manager	✘	✘	áno
Prioritný prístup k podpore od ESET vývojárskych tímov	✘	✘	áno
Proaktívne informačné služby	✘	✘	áno
ESET Deployment & Upgrade	✘	✘	1
ESET Healthcheck	✘	✘	1

ESET DETECTION AND RESPONSE ULTIMATE

KATEGÓRIA AKTIVÍT	AKTIVITA	ŠTANDARDNÁ BEZPEČNOSTNÁ PODPORA	DETECTION AND RESPONSE ESSENTIAL	DETECTION AND RESPONSE ADVANCED	DETECTION AND RESPONSE ULTIMATE
Bezpečnostná podpora pre koncové zariadenia	Malvér: nezachytená detekcia	áno	áno	áno	áno
	Malvér: problém s liečením	áno	áno	áno	áno
	Malvér: infekcia ransomvérom	áno	áno	áno	áno
	Nesprávna detekcia	áno	áno	áno	áno
	Všeobecné: preskúmanie podozrivého správania	áno	áno	áno	áno
Vyšetrenie incidentov a reakcia na ne	Základná analýza súborov	✘	áno	áno	áno
	Podrobná analýza súborov	✘	áno	áno	áno
	Digitálna forenzná analýza	✘	áno	áno	áno
	Digitálna forenzná pomoc pri reakcii na incidenty	✘	áno	áno	áno
Bezpečnostná podpora pre EDR	Technická podpora – pravidlá	✘	✘	áno	áno
	Technická podpora – vylúčenia	✘	✘	áno	áno
	Všeobecné: otázky týkajúce sa bezpečnostného nástroja EDR	✘	✘	áno	áno
	EDR: počiatočná optimalizácia	✘	✘	áno	áno
	EDR: ESET Threat Hunting (vyhľadávanie hrozieb na vyžiadanie)	✘	✘	áno	áno
Bezpečnostné služby pre EDR	EDR: ESET Threat Monitoring (monitorovanie hrozieb)	✘	✘	✘	áno
	EDR: ESET Threat Hunting (proaktívne vyhľadávanie hrozieb)	✘	✘	✘	áno
Profesionálne Služby	ESET Deployment & Upgrade	✘	✘	✘	áno

Prečo MDR?

Komplexnosť nástroja

Viacero upozornení

Nedostatok kvalifikovaných IT Špecialistov

Obmedzený čas na monitorovanie hrozieb v XDR

ĎAKUJEM ZA POZORNOSŤ