SECURITY DAYS

AKO RIEŠENIA ESET POMÁHAJÚ ORGANIZÁCIÁM SPĹŇAŤ POŽIADAVKY LEGISLATÍVY

Július Selecký, Senior Technical Pre-Sales Representative, ESET

Digital Security
Progress. Protected.

&

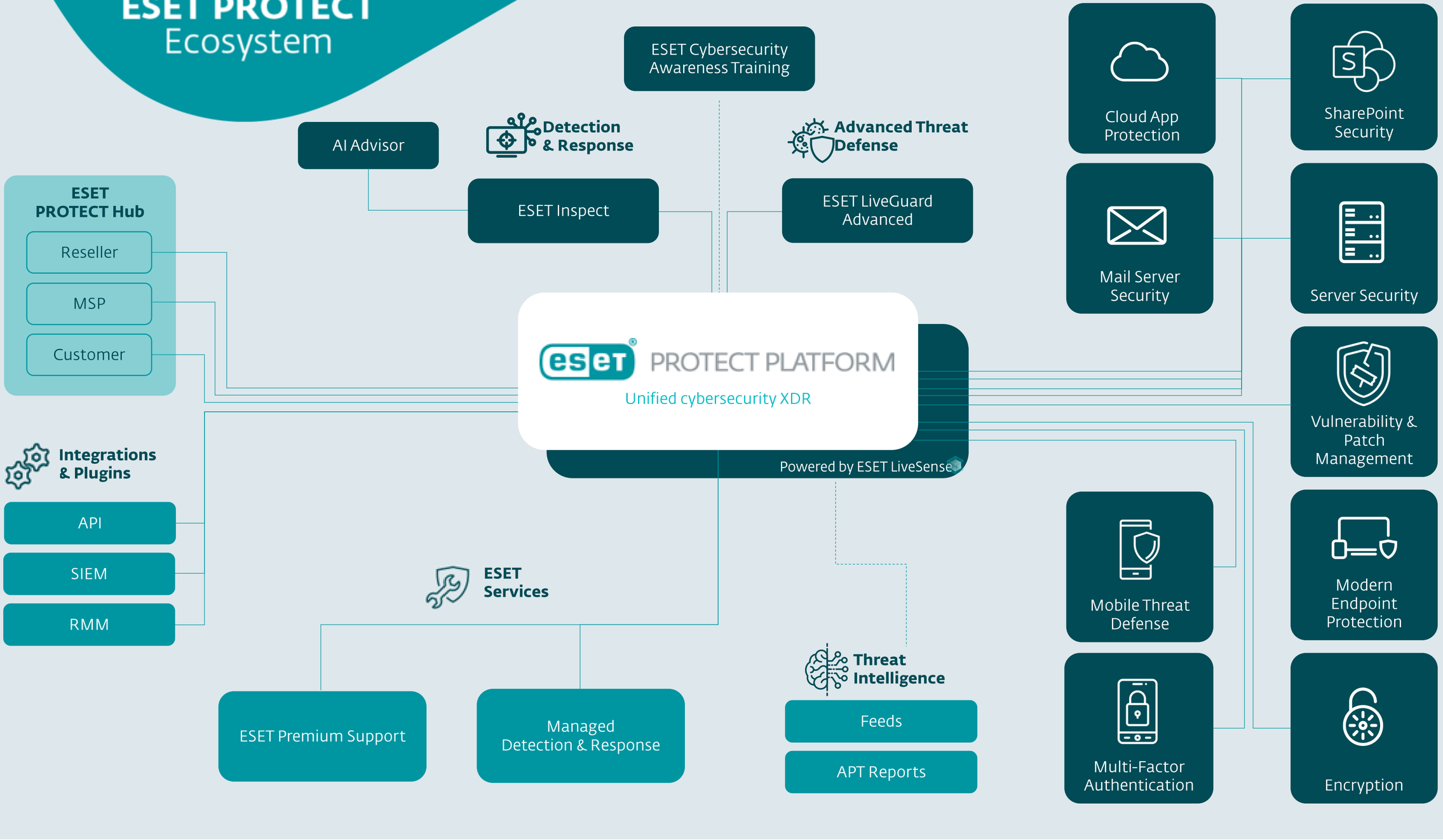
SME KONFERENCIE

Július Selecký

Senior Technical Pre-Sales Representative

julius.selecky@eset.com

ESET PROTECT Ecosystem



ESET LiveSense®

Na nasledujúcom obrázku sú zobrazené niektoré z kľúčových technológií spoločnosti ESET. Je uvedené, kedy a kde približne môžu detekovať a/alebo blokovať hrozbu počas jej životného cyklu v systéme.

PRE-EXECUTION LAYER

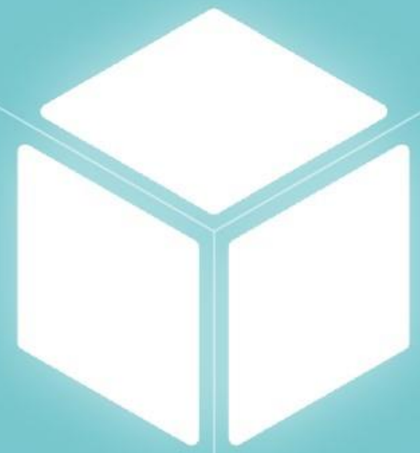
- Reputation and cache
- Network Attack Protection
- UEFI Scanner
- Advanced Machine Learning
- Brute-Force Attack Protection
- Device Control
- DNA Detections
- In-Product Sandbox

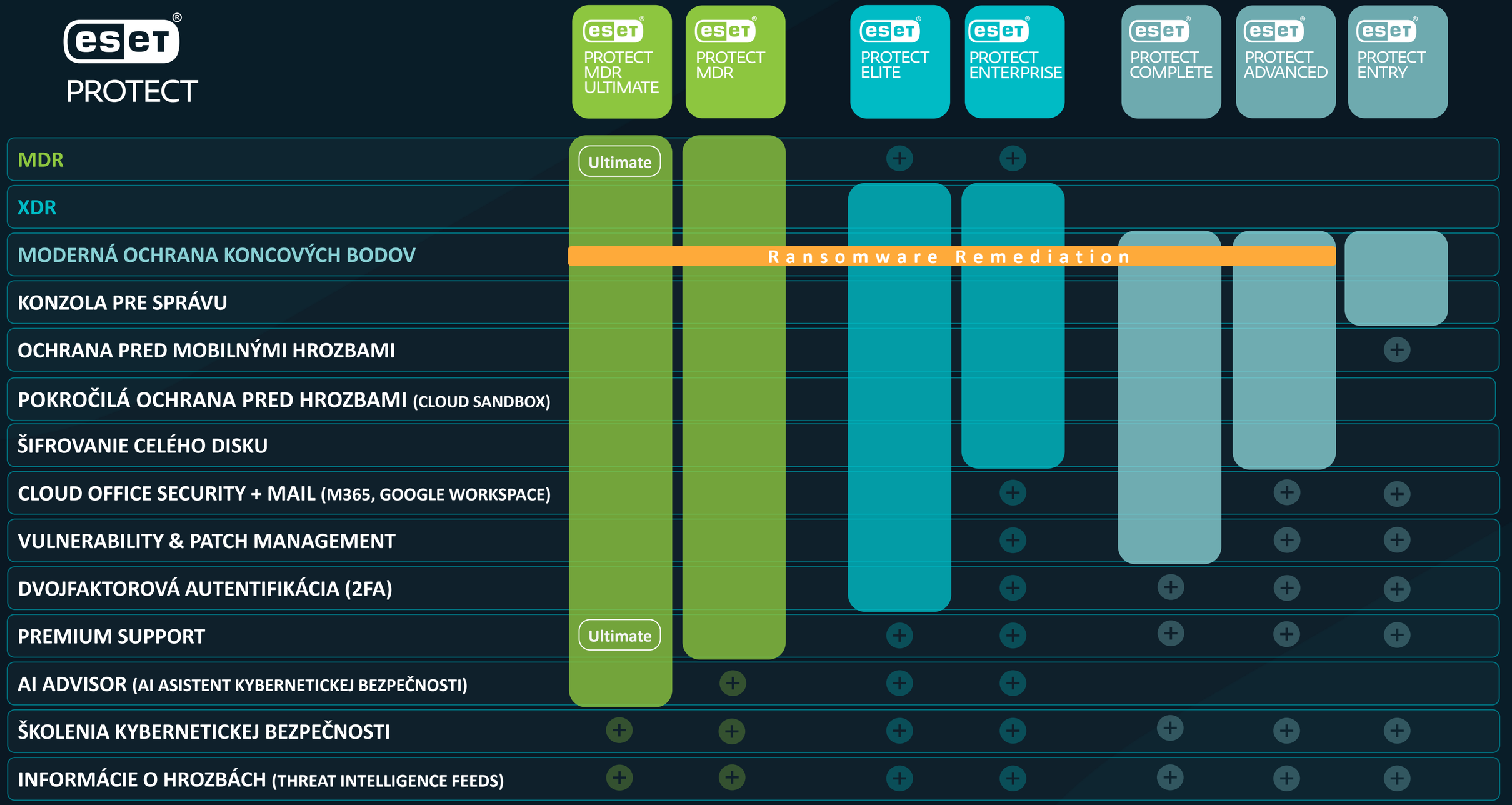
EXECUTION LAYER

- Ransomware Remediation
- Ransomware Shield
- Script Scanner & AMSI
- Advanced Memory Scanner
- Exploit Blocker
- Deep Behavioral Inspection

POST-EXECUTION LAYER

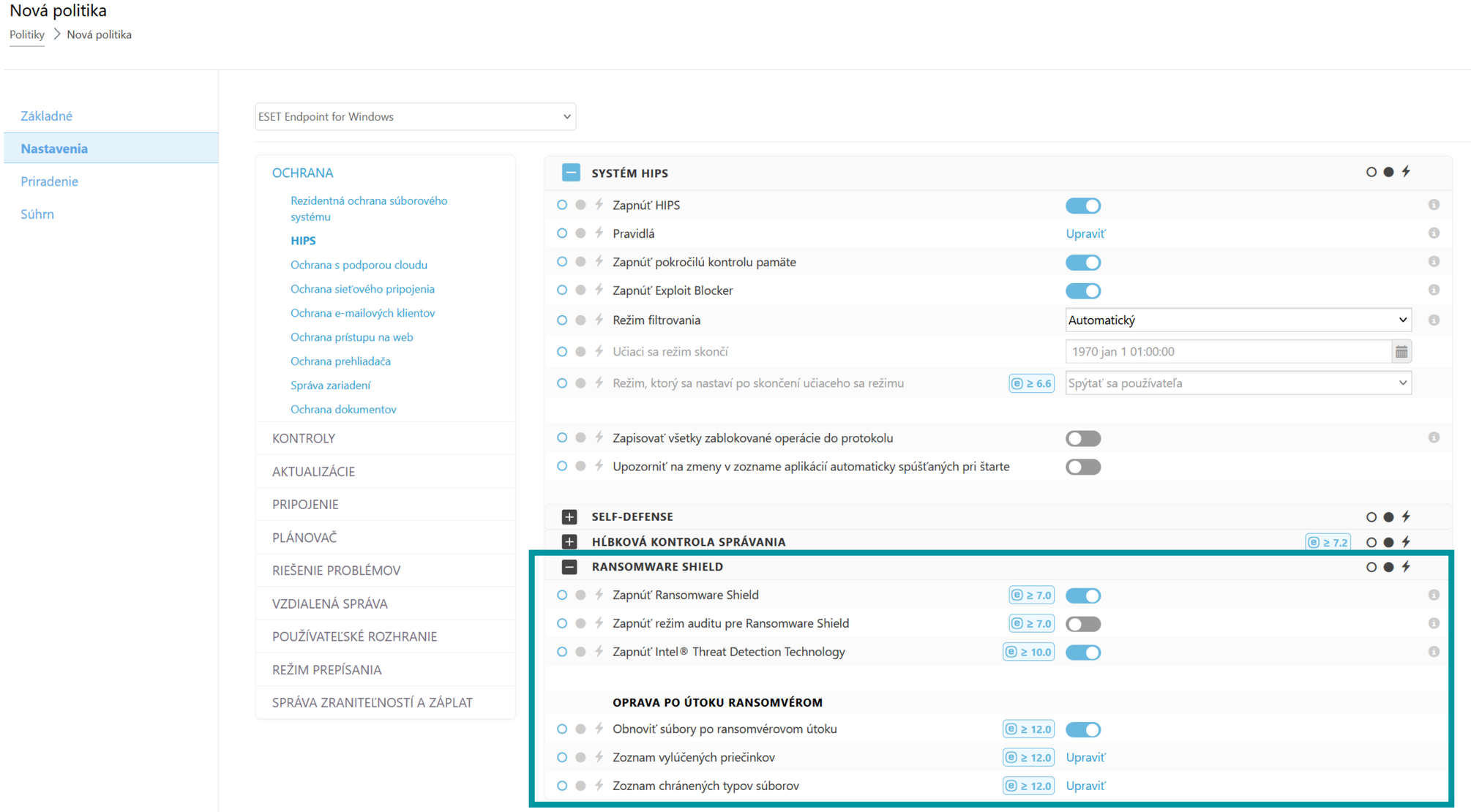
- LiveGrid® Protection
- Secure Browser
- Botnet Protection

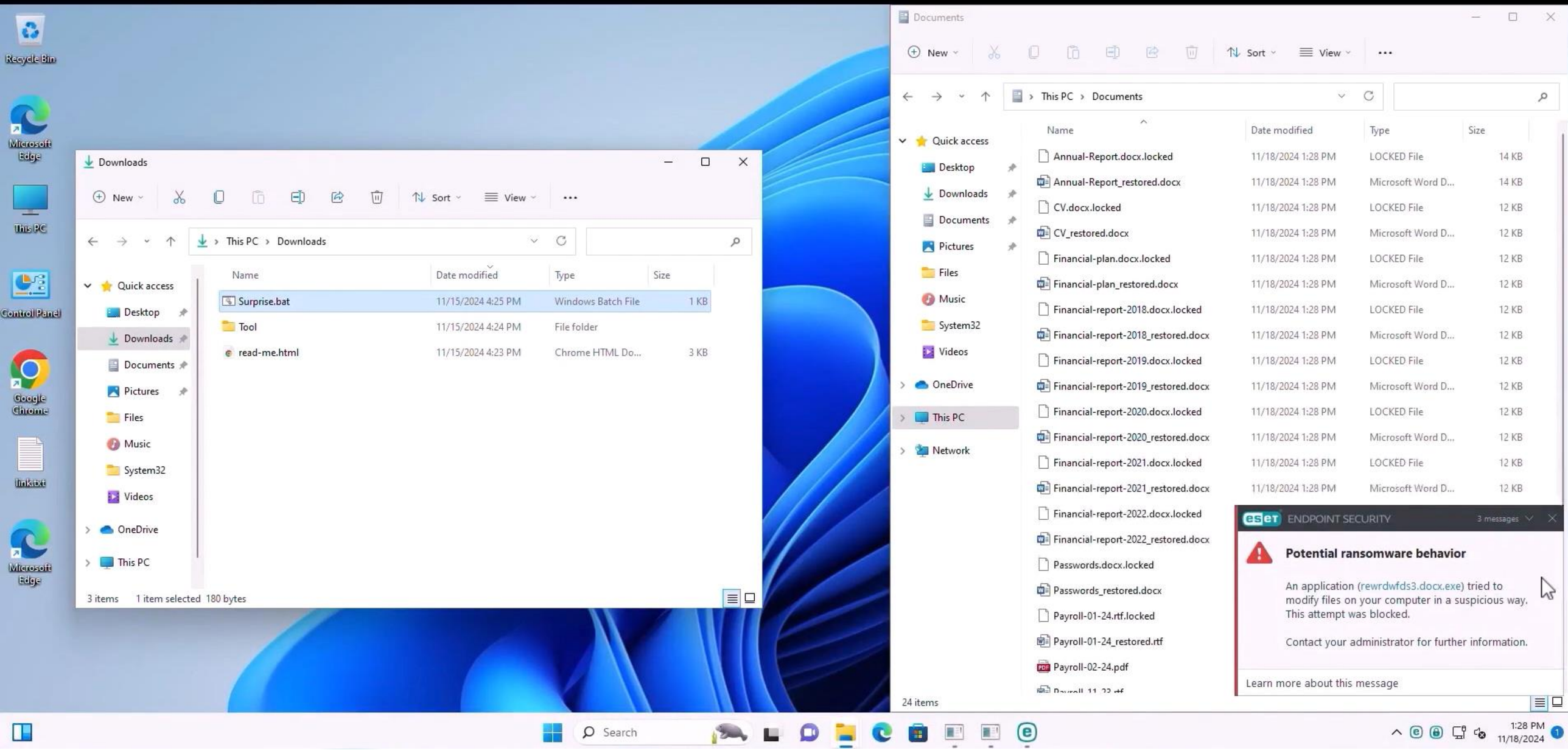


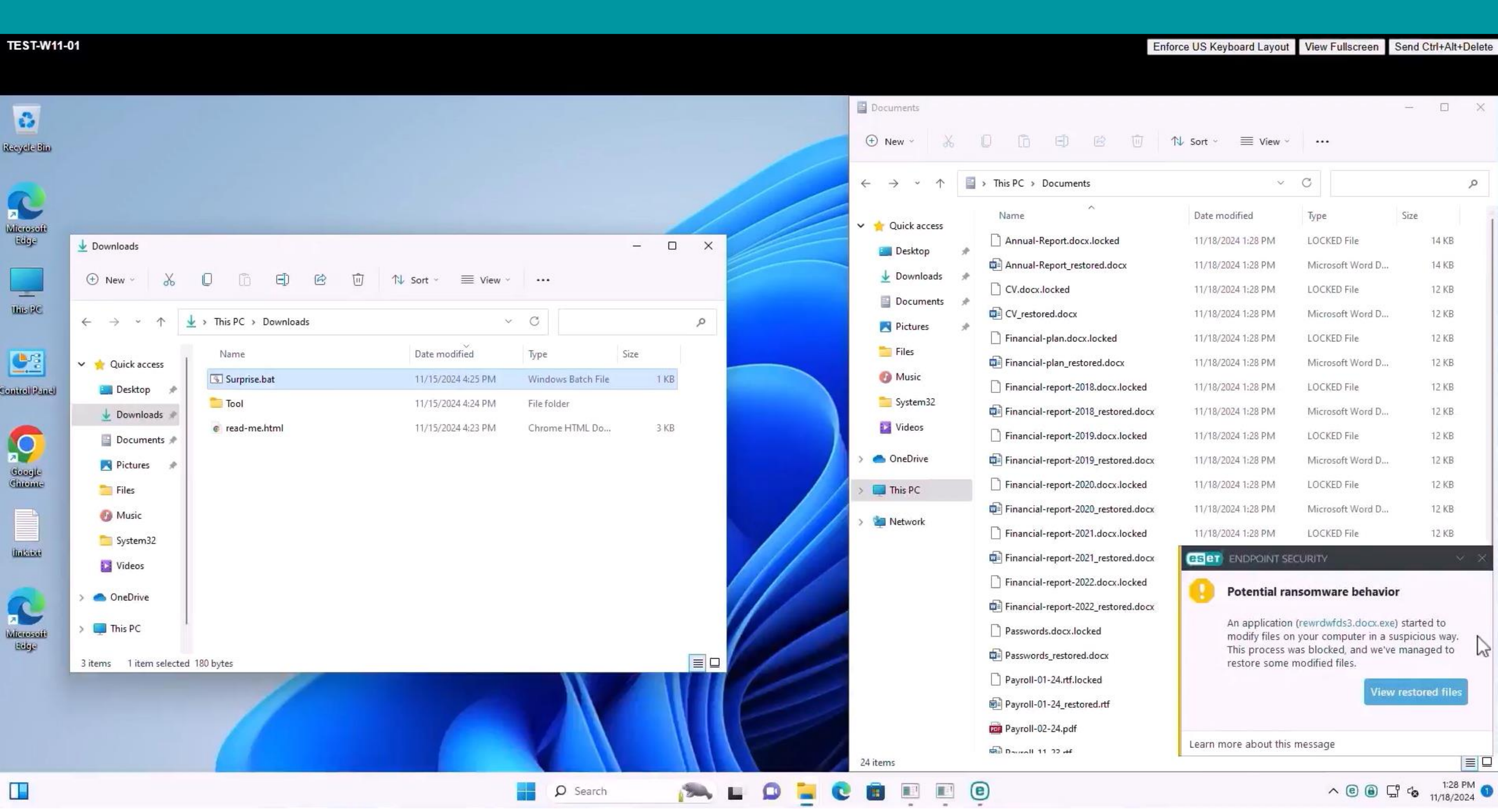

PROTECT
PROTECT MDR ULTIMATE
PROTECT MDR
PROTECT ELITE
PROTECT ENTERPRISE
PROTECT COMPLETE
PROTECT ADVANCED
PROTECT ENTRY
MDR
Ultimate
XDR
MODERNÁ OCHRANA KONCOVÝCH BODOV
Ransomware Remediation
KONZOLA PRE SPRÁVU
OCHRANA PRED MOBILNÝMI HROZBAMI
POKROČILÁ OCHRANA PRED HROZBAMI (CLOUD SANDBOX)
ŠIFROVANIE CELÉHO DISKU
CLOUD OFFICE SECURITY + MAIL (M365, GOOGLE WORKSPACE)
VULNERABILITY & PATCH MANAGEMENT
DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)
PREMIUM SUPPORT
Ultimate
AI ADVISOR (AI ASISTENT KYBERNETICKEJ BEZPEČNOSTI)
ŠKOLENIA KYBERNETICKEJ BEZPEČNOSTI
INFORMÁCIE O HROZBÁCH (THREAT INTELLIGENCE FEEDS)
doplnok

Proces viacvrstvovej ochrany

Ransomware Remediation




Recycle Bin
Microsoft Edge
This PC
Control Panel
Google Chrome
link.txt
Microsoft Edge
Downloads
New
Sort
View
This PC › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Files
Music
System32
Videos
OneDrive
This PC
Name
Date modified
Type
Size
Surprise.bat 11/15/2024 4:25 PM Windows Batch File 1 KB
Tool 11/15/2024 4:24 PM File folder
read-me.html 11/15/2024 4:23 PM Chrome HTML Do... 3 KB
3 items 1 item selected 180 bytes
Documents
New
Sort
View
This PC › Documents
Quick access
Desktop
Downloads
Documents
Pictures
Files
Music
System32
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Annual-Report.docx.locked 11/18/2024 1:28 PM LOCKED File 14 KB
Annual-Report_restored.docx 11/18/2024 1:28 PM Microsoft Word D... 14 KB
CV.docx.locked 11/18/2024 1:28 PM LOCKED File 12 KB
CV_restored.docx 11/18/2024 1:28 PM Microsoft Word D... 12 KB
Financial-plan.docx.locked 11/18/2024 1:28 PM LOCKED File 12 KB
Financial-plan_restored.docx 11/18/2024 1:28 PM Microsoft Word D... 12 KB
Financial-report-2018.docx.locked 11/18/2024 1:28 PM LOCKED File 12 KB
Financial-report-2018_restored.docx 11/18/2024 1:28 PM Microsoft Word D... 12 KB
Financial-report-2019.docx.locked 11/18/2024 1:28 PM LOCKED File 12 KB
Financial-report-2019_restored.docx 11/18/2024 1:28 PM Microsoft Word D... 12 KB
Financial-report-2020.docx.locked 11/18/2024 1:28 PM LOCKED File 12 KB
Financial-report-2020_restored.docx 11/18/2024 1:28 PM Microsoft Word D... 12 KB
Financial-report-2021.docx.locked 11/18/2024 1:28 PM LOCKED File 12 KB
Financial-report-2021_restored.docx 11/18/2024 1:28 PM Microsoft Word D... 12 KB
Financial-report-2022.docx.locked
Financial-report-2022_restored.docx
Passwords.docx.locked
Passwords_restored.docx
Payroll-01-24.rtf.locked
Payroll-01-24_restored.rtf
Payroll-02-24.pdf
24 items
ESET ENDPOINT SECURITY 3 messages
Potential ransomware behavior
An application (rewrdwfds3.docx.exe) tried to modify files on your computer in a suspicious way. This attempt was blocked.
Contact your administrator for further information.
Learn more about this message
Search
1:28 PM
11/18/2024

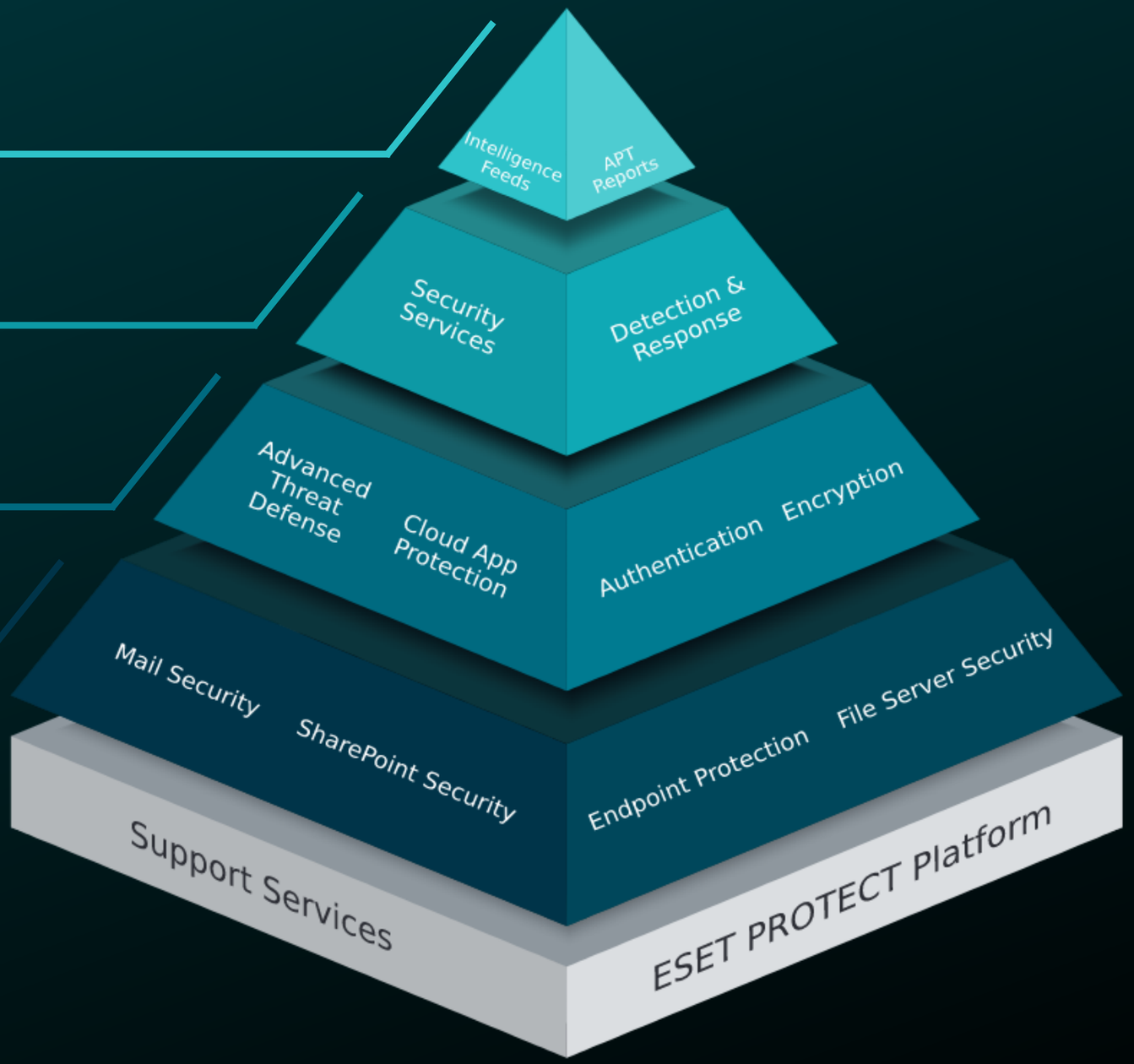

TEST-W11-01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Recycle Bin
Microsoft Edge
This PC
Control Panel
Google Chrome
Inkabxt
Microsoft Edge
Downloads
New
Sort
View
This PC › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Files
Music
System32
Videos
OneDrive
This PC
Name
Date modified
Type
Size
Surprise.bat
11/15/2024 4:25 PM
Windows Batch File
1 KB
Tool
11/15/2024 4:24 PM
File folder
read-me.html
11/15/2024 4:23 PM
Chrome HTML Do...
3 KB
3 items
1 item selected 180 bytes
Documents
New
Sort
View
This PC › Documents
Quick access
Desktop
Downloads
Documents
Pictures
Files
Music
System32
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Annual-Report.docx.locked
11/18/2024 1:28 PM
LOCKED File
14 KB
Annual-Report_restored.docx
11/18/2024 1:28 PM
Microsoft Word D...
14 KB
CV.docx.locked
11/18/2024 1:28 PM
LOCKED File
12 KB
CV_restored.docx
11/18/2024 1:28 PM
Microsoft Word D...
12 KB
Financial-plan.docx.locked
11/18/2024 1:28 PM
LOCKED File
12 KB
Financial-plan_restored.docx
11/18/2024 1:28 PM
Microsoft Word D...
12 KB
Financial-report-2018.docx.locked
11/18/2024 1:28 PM
LOCKED File
12 KB
Financial-report-2018_restored.docx
11/18/2024 1:28 PM
Microsoft Word D...
12 KB
Financial-report-2019.docx.locked
11/18/2024 1:28 PM
LOCKED File
12 KB
Financial-report-2019_restored.docx
11/18/2024 1:28 PM
Microsoft Word D...
12 KB
Financial-report-2020.docx.locked
11/18/2024 1:28 PM
LOCKED File
12 KB
Financial-report-2020_restored.docx
11/18/2024 1:28 PM
Microsoft Word D...
12 KB
Financial-report-2021.docx.locked
11/18/2024 1:28 PM
LOCKED File
12 KB
Financial-report-2021_restored.docx
Financial-report-2022.docx.locked
Financial-report-2022_restored.docx
Passwords.docx.locked
Passwords_restored.docx
Payroll-01-24.rtf.locked
Payroll-01-24_restored.rtf
Payroll-02-24.pdf
24 items
ESET ENDPOINT SECURITY
Potential ransomware behavior
An application (rewrdwfds3.docx.exe) started to modify files on your computer in a suspicious way. This process was blocked, and we've managed to restore some modified files.
View restored files
Learn more about this message
Search
1:28 PM
11/18/2024

THREAT INTELLIGENCE

DETEKCIA A REAKCIA

ROZŠÍRENÁ OCHRANA

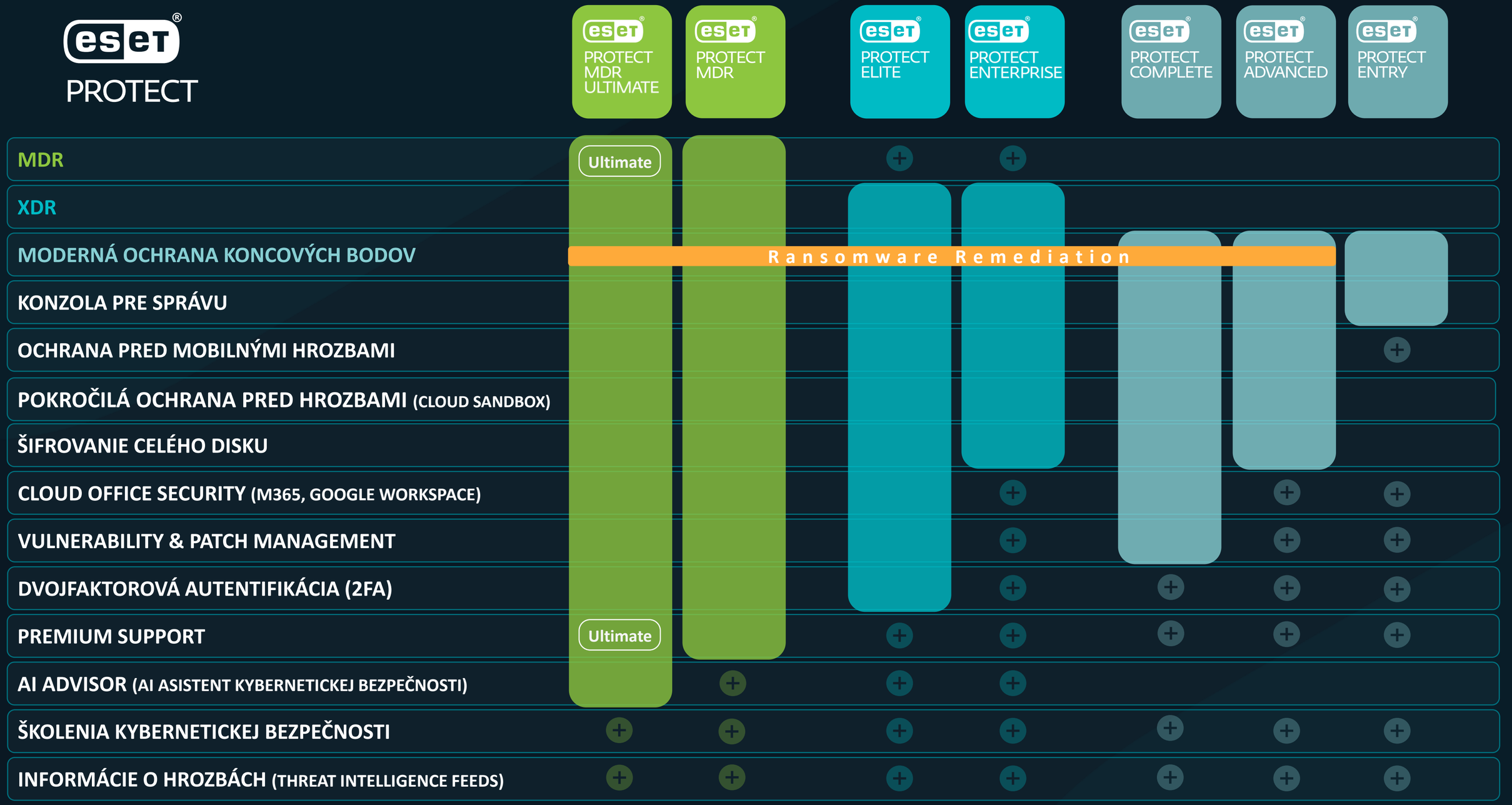
ZÁKLADNÁ OCHRANA



Bezpečnostné opatrenia § 20 ZoKB

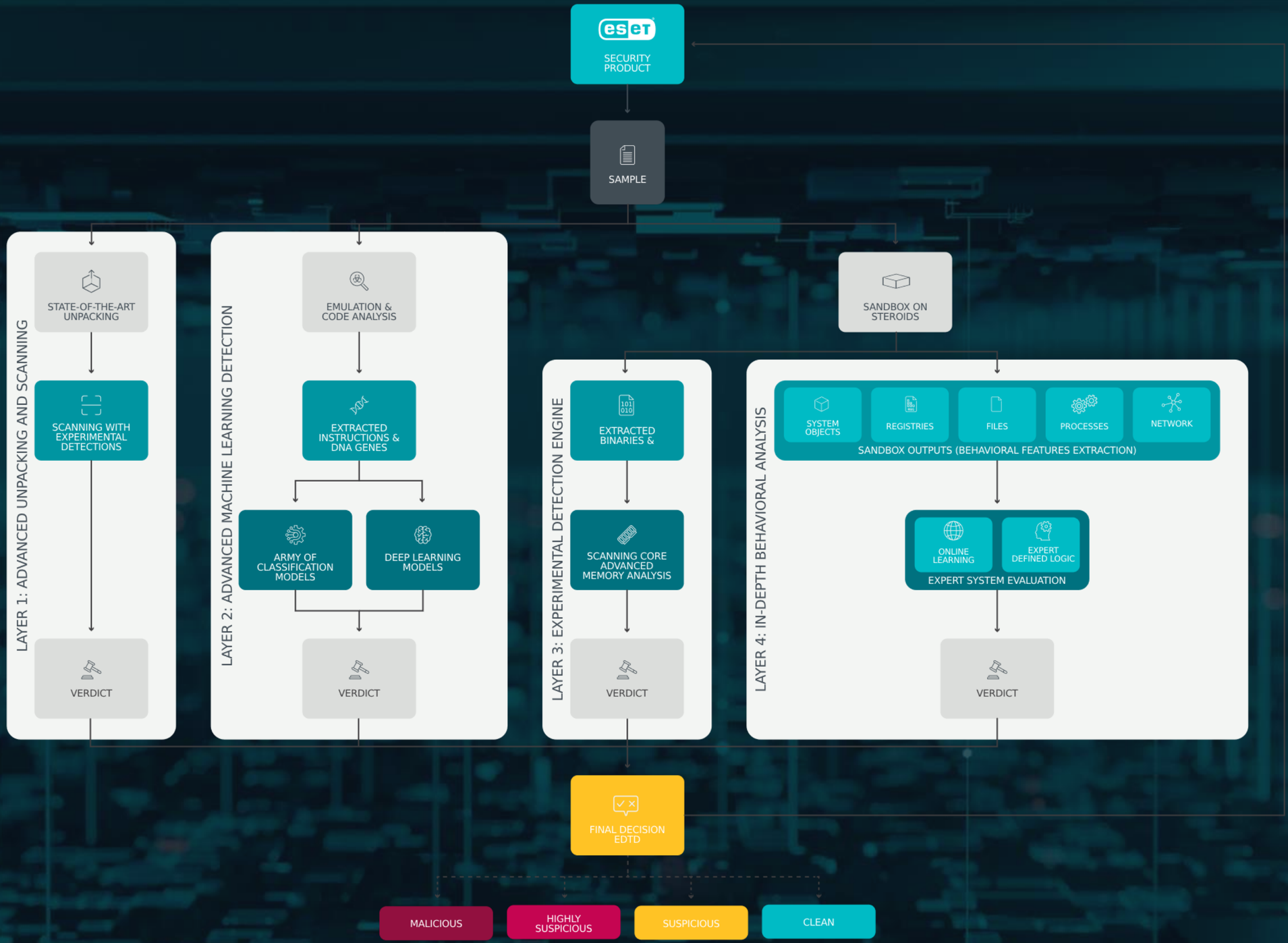
2) Bezpečnostné opatrenia zahŕňajú oblasti aspoň pre

b) správu zraniteľností,	ESET VULNERABILITY & PATCH MANAGEMENT
c) správu aktív a riadenie kybernetických hrozieb a rizík kybernetickej a informačnej bezpečnosti,	**ESET konzultačné služby**
d) riadenie udalostí a kybernetických bezpečnostných incidentov,	ESET INSPECT ESET MDR
h) kryptografické opatrenia a zásady používania kryptografie,	ESET FULL DISK ENCRYPTION
i) bezpečnosť a spôsobilosti ľudských zdrojov,	**Školenia kybernetickej bezpečnosti**
j) správa identít a prístupov,	ESET SECURE AUTHENTICATION
k) bezpečnosť pri prevádzke informačných systémov a sietí,	ESET INSPECT ESET MDR
l) ochranu proti škodlivému kódu a nežiaducemu obsahu,	ESET ENDPOINT SECURITY
m) systémovú, sieťovú a komunikačnú bezpečnosť,	ESET PROTECT ESET INSPECT
n) monitorovanie, zaznamenávanie a hlásenie udalostí,	ESET INSPECT ESET MDR


PROTECT
PROTECT MDR ULTIMATE
PROTECT MDR
PROTECT ELITE
PROTECT ENTERPRISE
PROTECT COMPLETE
PROTECT ADVANCED
PROTECT ENTRY
MDR
Ultimate
XDR
MODERNÁ OCHRANA KONCOVÝCH BODOV
Ransomware Remediation
KONZOLA PRE SPRÁVU
OCHRANA PRED MOBILNÝMI HROZBAMI
POKROČILÁ OCHRANA PRED HROZBAMI (CLOUD SANDBOX)
ŠIFROVANIE CELÉHO DISKU
CLOUD OFFICE SECURITY (M365, GOOGLE WORKSPACE)
VULNERABILITY & PATCH MANAGEMENT
DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)
PREMIUM SUPPORT
Ultimate
AI ADVISOR (AI ASISTENT KYBERNETICKEJ BEZPEČNOSTI)
ŠKOLENIA KYBERNETICKEJ BEZPEČNOSTI
INFORMÁCIE O HROZBÁCH (THREAT INTELLIGENCE FEEDS)
doplnok

LIVEGUARD ADVANCED

Proaktívna ochrana pred doposiaľ neznámymi
a zero-day hrozbami


SECURITY PRODUCT
SAMPLE
SANDBOX ON STEROIDS
LAYER 1: ADVANCED UNPACKING AND SCANNING
STATE-OF-THE-ART UNPACKING
SCANNING WITH EXPERIMENTAL DETECTIONS
VERDICT
LAYER 2: ADVANCED MACHINE LEARNING DETECTION
EMULATION & CODE ANALYSIS
EXTRACTED INSTRUCTIONS & DNA GENES
ARMY OF CLASSIFICATION MODELS
DEEP LEARNING MODELS
VERDICT
LAYER 3: EXPERIMENTAL DETECTION ENGINE
EXTRACTED BINARIES &
SCANNING CORE ADVANCED MEMORY ANALYSIS
VERDICT
LAYER 4: IN-DEPTH BEHAVIORAL ANALYSIS
SYSTEM OBJECTS
REGISTRIES
FILES
PROCESSES
NETWORK
SANDBOX OUTPUTS (BEHAVIORAL FEATURES EXTRACTION)
ONLINE LEARNING
EXPERT DEFINED LOGIC
EXPERT SYSTEM EVALUATION
VERDICT
FINAL DECISION EDTD
MALICIOUS
HIGHLY SUSPICIOUS
SUSPICIOUS
CLEAN

ESET LIVEGUARD

pondelok 25. novembra 2024 o 8:44

Neboli nájdené žiadne hrozby

SHA-1	FC3DF08EEE0FC6CA15AD421BC1681742FAA59273
SHA-256	0C5225252CA2246116DBEDF1B16E7DA0218BC202DCB871808C003B1335E3CBC4
Kategória	Spustiteľný súbor

Súbor
Podrobnosti

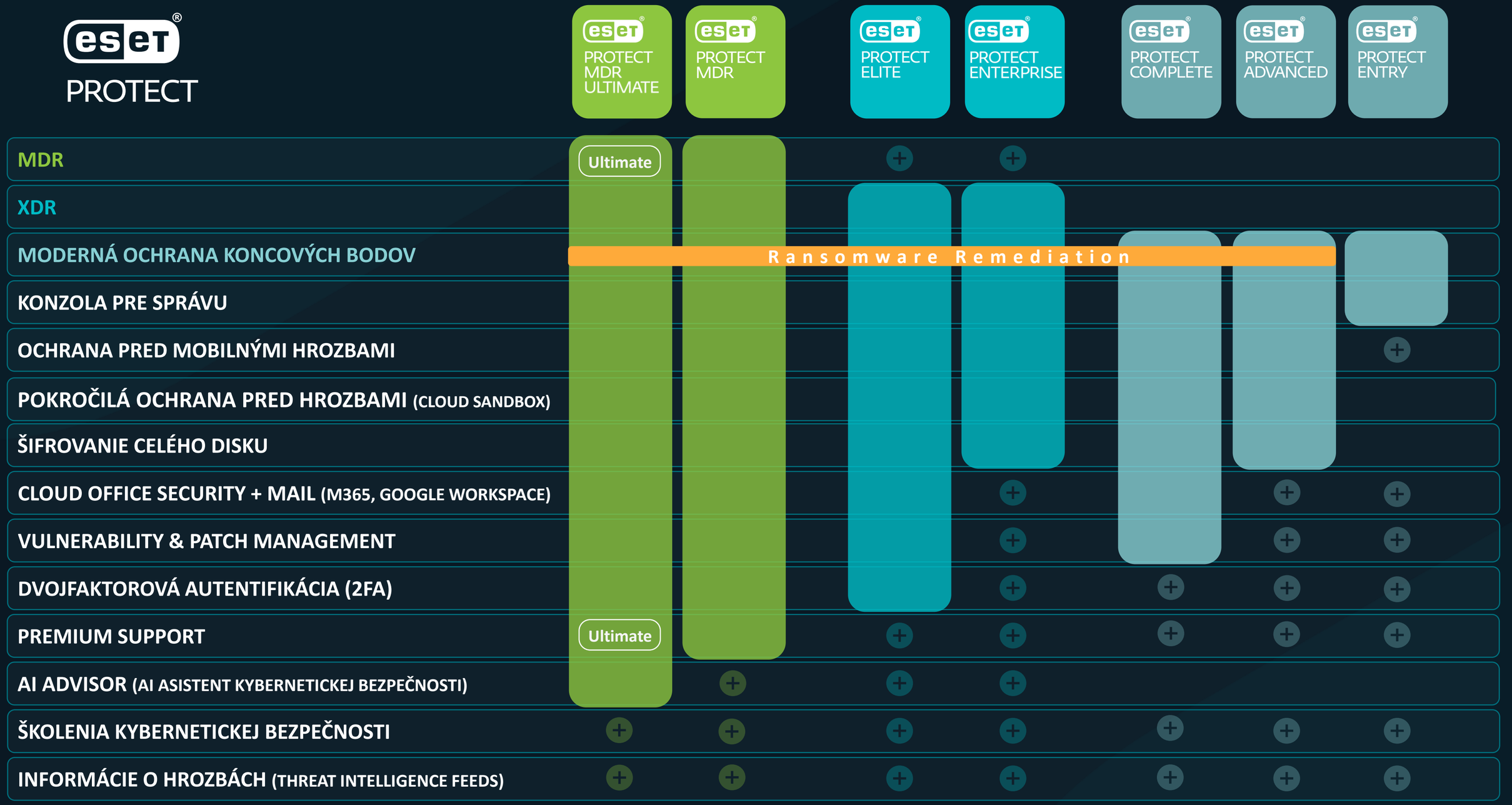
Názov súboru	d--H2WK9.exe.part
SHA-1	FC3DF08EEE0FC6CA15AD421BC1681742FAA59273
SHA-256	0C5225252CA2246116DBEDF1B16E7DA0218BC202DCB871808C003B1335E3CBC4
Kategória	Spustiteľný súbor
Veľkosť	1,23 MB

Sandbox
Podrobnosti

Nadradený príkazový riadok	"C:\Program Files\Mozilla Firefox\firefox.exe" -os-autostart
Cesta k nadradenému súboru	C:\Program Files\Mozilla Firefox\firefox.exe
Región	United States
Cesta k súboru	C:\Users\user\Downloads\d--H2WK9.exe.part

Analyzovaná aktivita

ESET LiveGuard nezachytil žiadne podozrivé správanie.


PROTECT
PROTECT MDR ULTIMATE
PROTECT MDR
PROTECT ELITE
PROTECT ENTERPRISE
PROTECT COMPLETE
PROTECT ADVANCED
PROTECT ENTRY
MDR
Ultimate
XDR
MODERNÁ OCHRANA KONCOVÝCH BODOV
Ransomware Remediation
KONZOLA PRE SPRÁVU
OCHRANA PRED MOBILNÝMI HROZBAMI
POKROČILÁ OCHRANA PRED HROZBAMI (CLOUD SANDBOX)
ŠIFROVANIE CELÉHO DISKU
CLOUD OFFICE SECURITY + MAIL (M365, GOOGLE WORKSPACE)
VULNERABILITY & PATCH MANAGEMENT
DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)
PREMIUM SUPPORT
Ultimate
AI ADVISOR (AI ASISTENT KYBERNETICKEJ BEZPEČNOSTI)
ŠKOLENIA KYBERNETICKEJ BEZPEČNOSTI
INFORMÁCIE O HROZBÁCH (THREAT INTELLIGENCE FEEDS)
doplnok

ESET FULL DISK ENCRYPTION

Ochrana údajov pre firmy všetkých veľkostí

FULL DISK ENCRYPTION

Hlavné funkcie

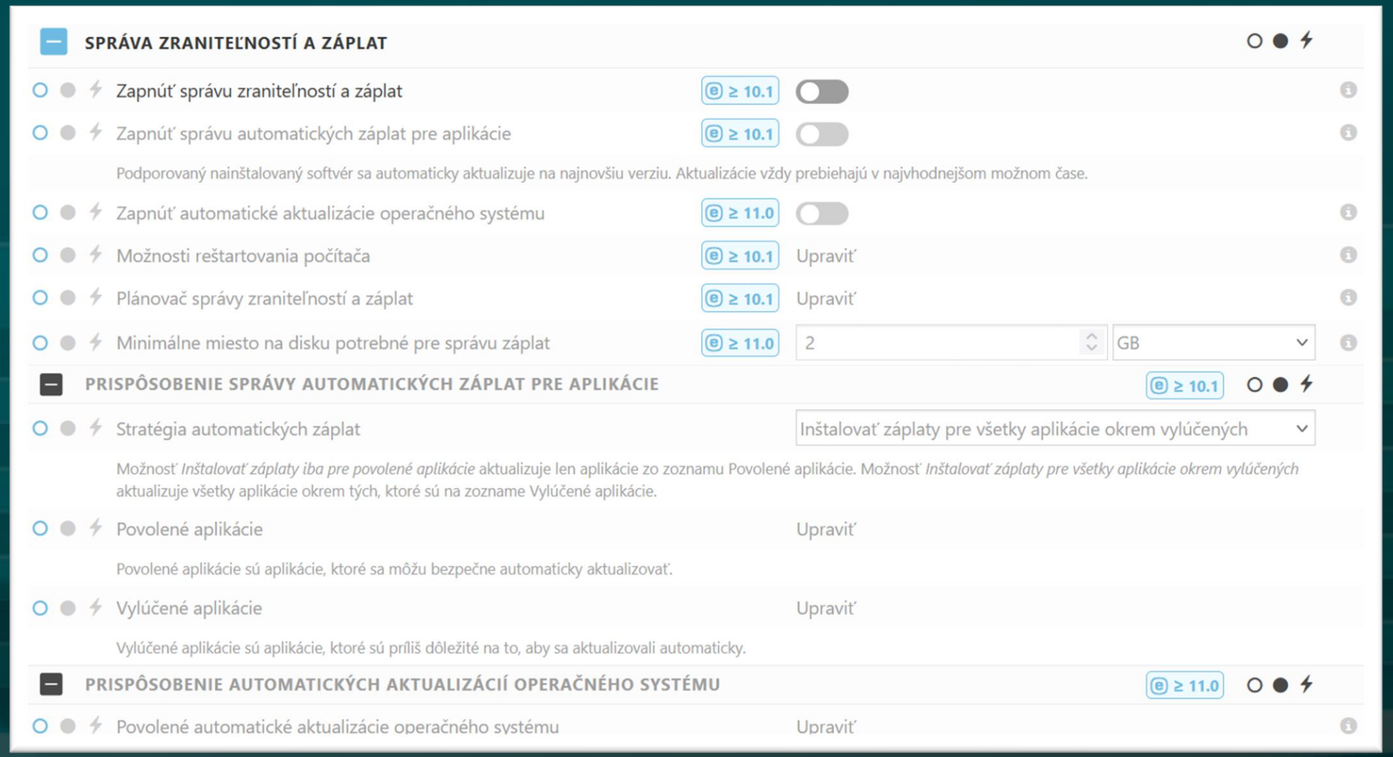
- Zabezpečenie na úrovni pred spustením systému
- Šifrovanie celého disku
- Možnosť správy cez ESET PROTECT
- Vzdialené nastavenie politiky hesiel
- Možnosť vzdialene blokovať a vymazávať heslá alebo rušiť ich platnosť v spravovaných koncových zariadeniach
- Správa všetkých produktov z jednej konzoly
- Ochrana identity a údajov
- Ochrana naprieč platformami
- Nasadenie jedným kliknutím
- Overené riešenie

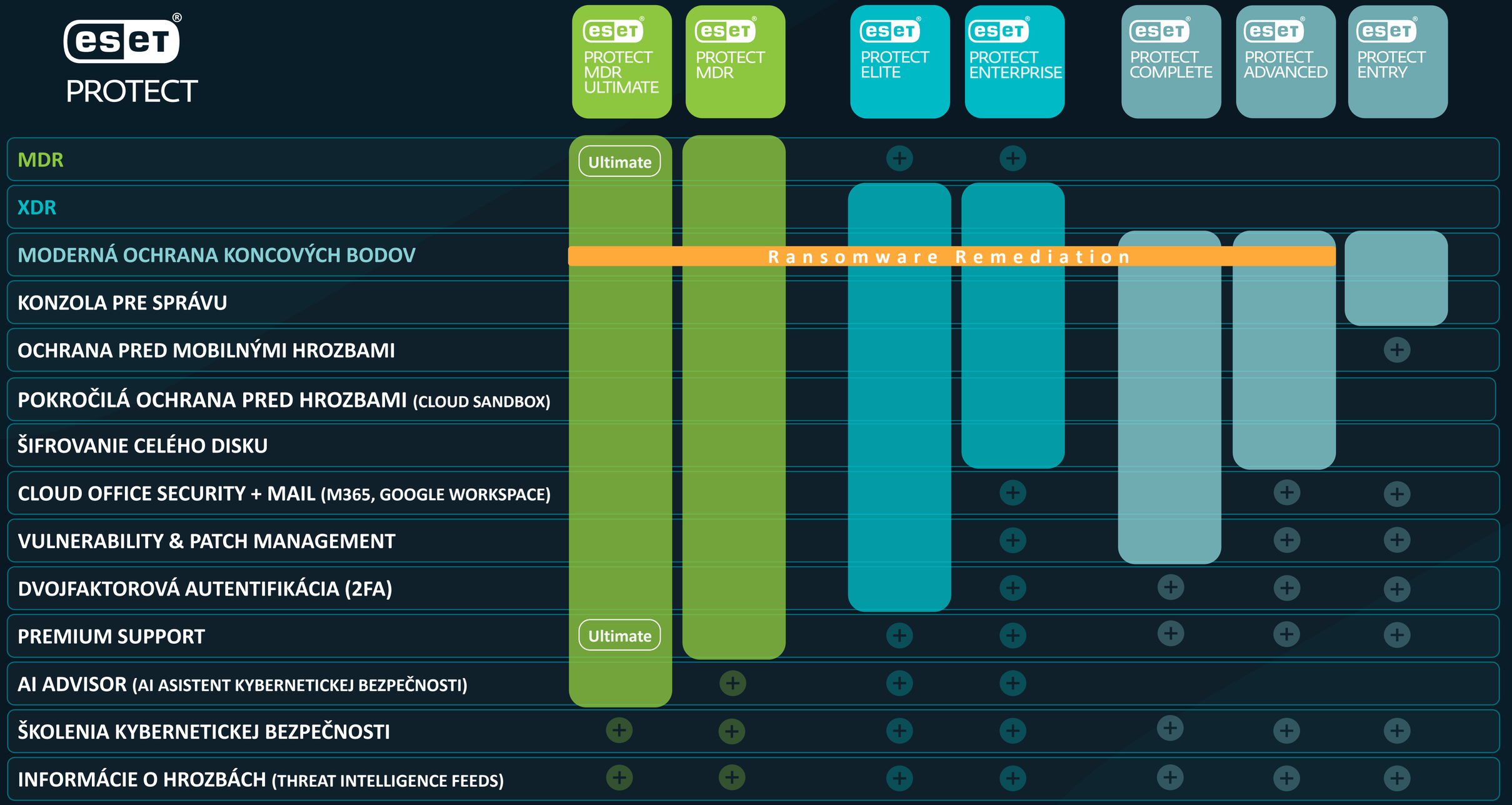
Správa zraniteľností

- **Čo je zranitelnosť?**

  (Slabé miesto informačného aktíva)

- **Opatrenia:**
  - aktívne sledovanie zraniteľností
  - cyklické vyhodnocovanie
  - automatické aktualizácie

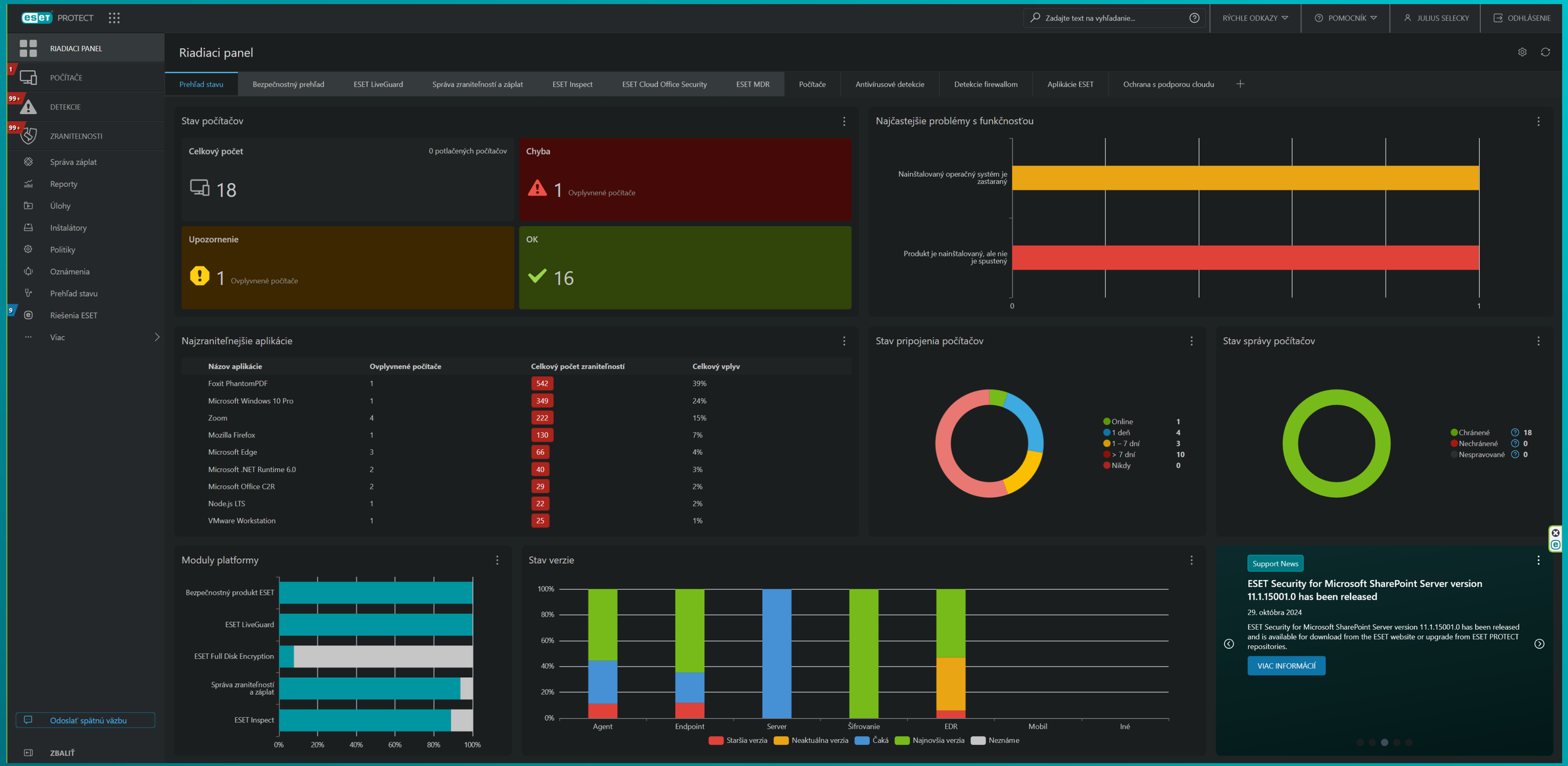



PROTECT
PROTECT MDR ULTIMATE
PROTECT MDR
PROTECT ELITE
PROTECT ENTERPRISE
PROTECT COMPLETE
PROTECT ADVANCED
PROTECT ENTRY
MDR
Ultimate
XDR
MODERNÁ OCHRANA KONCOVÝCH BODOV
Ransomware Remediation
KONZOLA PRE SPRÁVU
OCHRANA PRED MOBILNÝMI HROZBAMI
POKROČILÁ OCHRANA PRED HROZBAMI (CLOUD SANDBOX)
ŠIFROVANIE CELÉHO DISKU
CLOUD OFFICE SECURITY + MAIL (M365, GOOGLE WORKSPACE)
VULNERABILITY & PATCH MANAGEMENT
DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)
PREMIUM SUPPORT
Ultimate
AI ADVISOR (AI ASISTENT KYBERNETICKEJ BEZPEČNOSTI)
ŠKOLENIA KYBERNETICKEJ BEZPEČNOSTI
INFORMÁCIE O HROZBÁCH (THREAT INTELLIGENCE FEEDS)
doplnok

VULNERABILITY & PATCH MANAGEMENT

Aktívne vyhodnocovanie a oprava zraniteľností vo všetkých koncových zariadeniach

- centrálna správa nasadzovania záplat z konzoly ESET PROTECT Cloud
- automatizované kontroly na základe prispôsobiteľných pravidiel
- filtrovanie, zoskupovanie a triedenie zraniteľností podľa ich závažnosti
- možnosť automatických alebo manuálnych opráv
- prispôsobiteľné politiky záplat


PROTECT
Zadajte text na vyhľadanie...
RÝCHLE ODKAZY
POMOCNÍK
JULIUS SELECKÝ
ODHLÁSENIE
RIADIACI PANEL
POČÍTAČE
DETEKCIE
ZRANITEĽNOSTI
Správa záplat
Reporty
Úlohy
Inštalátory
Politiky
Oznámenia
Prehľad stavu
Riešenia ESET
Viac
Odoslať spätnú väzbu
ZBALIŤ
Riadiaci panel
Prehľad stavu
Bezpečnostný prehľad
ESET LiveGuard
Správa zraniteľností a záplat
ESET Inspect
ESET Cloud Office Security
ESET MDR
Počítače
Antivírusové detekcie
Detekcie firewallom
Aplikácie ESET
Ochrana s podporou cloudu
Stav počítačov
Celkový počet
0 potlačených počítačov
18
Chyba
1 Ovplyvnené počítače
Upozornenie
1 Ovplyvnené počítače
OK
16
Najčastejšie problémy s funkčnosťou
Nainštalovaný operačný systém je zastaraný
Produkt je nainštalovaný, ale nie je spustený
0
1
Najzraniteľnejšie aplikácie
Názov aplikácie
Ovplyvnené počítače
Celkový počet zraniteľností
Celkový vplyv
Foxit PhantomPDF 1 542 39%
Microsoft Windows 10 Pro 1 349 24%
Zoom 4 222 15%
Mozilla Firefox 1 130 7%
Microsoft Edge 3 66 4%
Microsoft .NET Runtime 6.0 2 40 3%
Microsoft Office C2R 2 29 2%
Node.js LTS 1 22 2%
VMware Workstation 1 25 1%
Stav pripojenia počítačov
Online 1
1 deň 4
1 – 7 dní 3
> 7 dní 10
Nikdy 0
Stav správy počítačov
Chránené 18
Nechránené 0
Nespravované 0
Moduly platformy
Bezpečnostný produkt ESET
ESET LiveGuard
ESET Full Disk Encryption
Správa zraniteľností a záplat
ESET Inspect
0%
20%
40%
60%
80%
100%
Stav verzie
100%
80%
60%
40%
20%
0%
Agent
Endpoint
Server
Šifrovanie
EDR
Mobil
Iné
Staršia verzia
Neaktuálna verzia
Čaká
Najnovšia verzia
Neznáme
Support News
ESET Security for Microsoft SharePoint Server version 11.1.15001.0 has been released
29. októbra 2024
ESET Security for Microsoft SharePoint Server version 11.1.15001.0 has been released and is available for download from the ESET website or upgrade from ESET PROTECT repositories.
VIAC INFORMÁCIÍ

RIADIACI PANEL
POČÍTAČE
INCIDENTY
ZRANITEĽNOSTI
Správa záplat
Detekcie
Reporty
Úlohy
Inštalátory
Politiky
Oznámenia
Prehľad stavu
Moduly platformy
Viac
Odoslať spätnú väzbu
ZBALIŤ

Riadiaci panel

Prehľad stavu | Incidenty | ESET LiveGuard | Správa zraniteľností a záplat | ESET Inspect | ESET Cloud Office Security | ESET MDR | Detekcie | Počítače | Antivírusové detekcie | Detekcie firewallom | Aplikácie ESET | Ochrana s podporou cloudu

Počet zraniteľností

S vysokým rizikom — vrátane 1 potlačených

965 zraniteľnosti/í

So stredným rizikom — vrátane 0 potlačených

216 zraniteľnosti/í

Počet zraniteľností v čase 30d

Počítače skontrolované na prítomnosť zraniteľností

Posledných 24 hodín	5
Posledné 1 – 3 dni	3
Viac ako 3 dni	3
Nie je k dispozícii	3

Najzraniteľnejšie počítače

Názov počítača	Typ počítača	Vysoko rizikové zraniteľnosti	Stredne rizikové zraniteľnosti	Celkový počet zraniteľností
Zdeno - Lenovo-t470p-i7	Počítač	131	104	235
Yoga13	Počítač	157	15	172
Dudo HP Virtual server	Server	131	31	162
Palo Radic - PC	Počítač	93	23	116
Lesny Palko	Počítač	106	9	115
Fildo-Majka Laptop	Počítač	92	10	102
Zuz_Vicanova_ntb	Počítač	70	4	74
Fildo - notebook	Počítač	52	8	60
Lesna Katka	Počítač	51	5	56

Najzraniteľnejšie počítače podľa zraniteľností OS

Názov počítača	Názov OS	Zraniteľnosti OS s vysokým rizikom	Zraniteľnosti OS so stredným rizikom	Celkový počet zraniteľností OS
Yoga13	Microsoft Windows 11 Pro	137	15	152
Zuz_Vicanova_ntb	Microsoft Windows 10 Home	69	4	73
Fildo-Majka Laptop	Microsoft Windows 11 Home	30	1	31

Najzraniteľnejšie aplikácie

Názov aplikácie	Ovplyvnené počítače	Celkový počet zraniteľností	Celkový vplyv
Zoom	4	240	21%
Microsoft Edge	2	218	18%
Microsoft Windows 11 Pro	1	152	13%
Mozilla Firefox	1	174	12%
Microsoft Office C2R	4	114	11%
Microsoft .NET Runtime 6.0	3	84	8%
Microsoft Windows 10 Home	1	73	7%
Microsoft Windows 11 Home	1	31	3%
VMware Workstation	1	27	2%

Najčastejšie zastarané aplikácie s dostupnými záplatami

Názov aplikácie	Ovplyvnené počítače
Microsoft Visual C++ Redistributable 2013	3
WinRAR	3
Microsoft .NET Desktop Runtime 8.0	2
LibreOffice	2
Microsoft Office MSI	2
Microsoft Visual C++ Redistributable 2010	2
Microsoft Visual C++ Redistributable	2
Microsoft Visual C++ 2015-2022 Redistributable	2
Mozilla Firefox	1

NÁZOV APLIKÁ...	DODÁVATEĽ AP...	VERZIA A...	SKÓRE...	CVE	MENO POČÍTAČA	KATEG...	PRVÝ VÝSKYT
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-5582	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-5584	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-5587	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-5588	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-6676	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-6677	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-6678	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-6682	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-7625	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-7626	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-7627	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	45	CVE-2015-7629	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-7630	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	45	CVE-2015-7631	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	45	CVE-2015-7632	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-7633	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-7634	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-7635	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-7636	pc-101	Zraniteľ...	17. septembra 2024 17:01:31
Adobe AIR	Adobe Systems Inc.	17.0.0.172	46	CVE-2015-7637	pc-101	Zraniteľ...	17. septembra 2024 17:01:31

Adobe AIR

Adobe AIR 17.0.0.172

Skóre rizika 46

Názov aplikácie	Adobe AIR
Dodávateľ aplikácie	Adobe Systems Inc.
Kategória	Zraniteľnosť aplikácie
CVE	CVE-2015-7625
Prvý výskyt	17. septembra 2024 17:01:31

Podrobnosti

Popis	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
Vydané	pred 9 rokmi – 15. októbra 2015 1:59:00
Posledná zmena	pred 8 rokmi – 1. júla 2017 3:29:00
CWE	CWE-119
Referencie	https://helpx.adobe.com/security/products/flash-player/apsb15-25.html http://www.securityfocus.com/bid/77065 http://rhn.redhat.com/errata/RHSA-2015-2024.html Zobraziť viac...

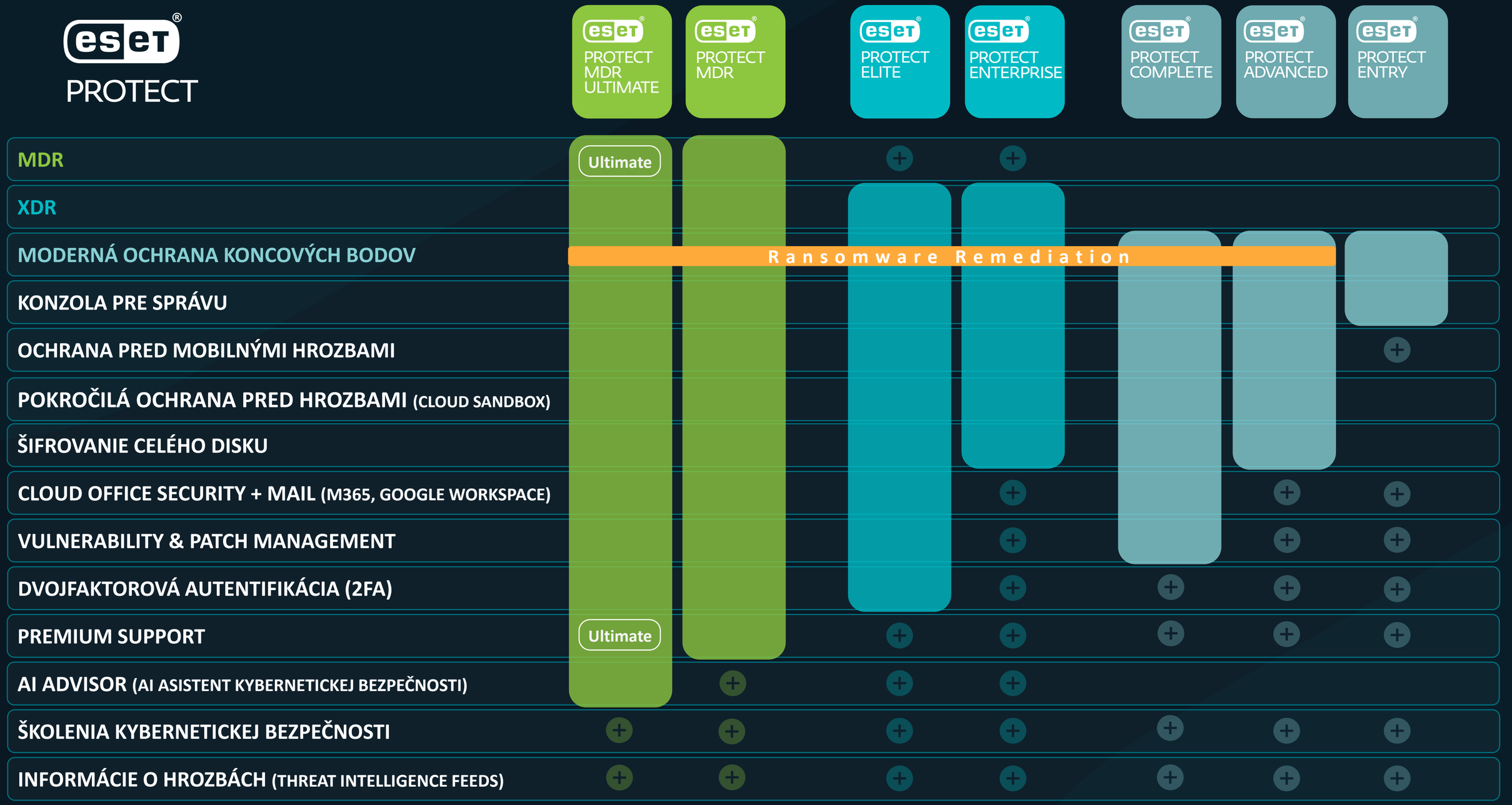
predpoklady

konzola

agent

endpoint

V&PM


PROTECT
PROTECT MDR ULTIMATE
PROTECT MDR
PROTECT ELITE
PROTECT ENTERPRISE
PROTECT COMPLETE
PROTECT ADVANCED
PROTECT ENTRY
MDR
Ultimate
XDR
MODERNÁ OCHRANA KONCOVÝCH BODOV
Ransomware Remediation
KONZOLA PRE SPRÁVU
OCHRANA PRED MOBILNÝMI HROZBAMI
POKROČILÁ OCHRANA PRED HROZBAMI (CLOUD SANDBOX)
ŠIFROVANIE CELÉHO DISKU
CLOUD OFFICE SECURITY + MAIL (M365, GOOGLE WORKSPACE)
VULNERABILITY & PATCH MANAGEMENT
DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)
PREMIUM SUPPORT
Ultimate
AI ADVISOR (AI ASISTENT KYBERNETICKEJ BEZPEČNOSTI)
ŠKOLENIA KYBERNETICKEJ BEZPEČNOSTI
INFORMÁCIE O HROZBÁCH (THREAT INTELLIGENCE FEEDS)
doplnok

ESET MAIL SECURITY

Kompletná ochrana poštových serverov

ESET CLOUD OFFICE SECURITY

Ochrana aplikácií Microsoft 365 a Google Workspace

CLOUD OFFICE SECURITY

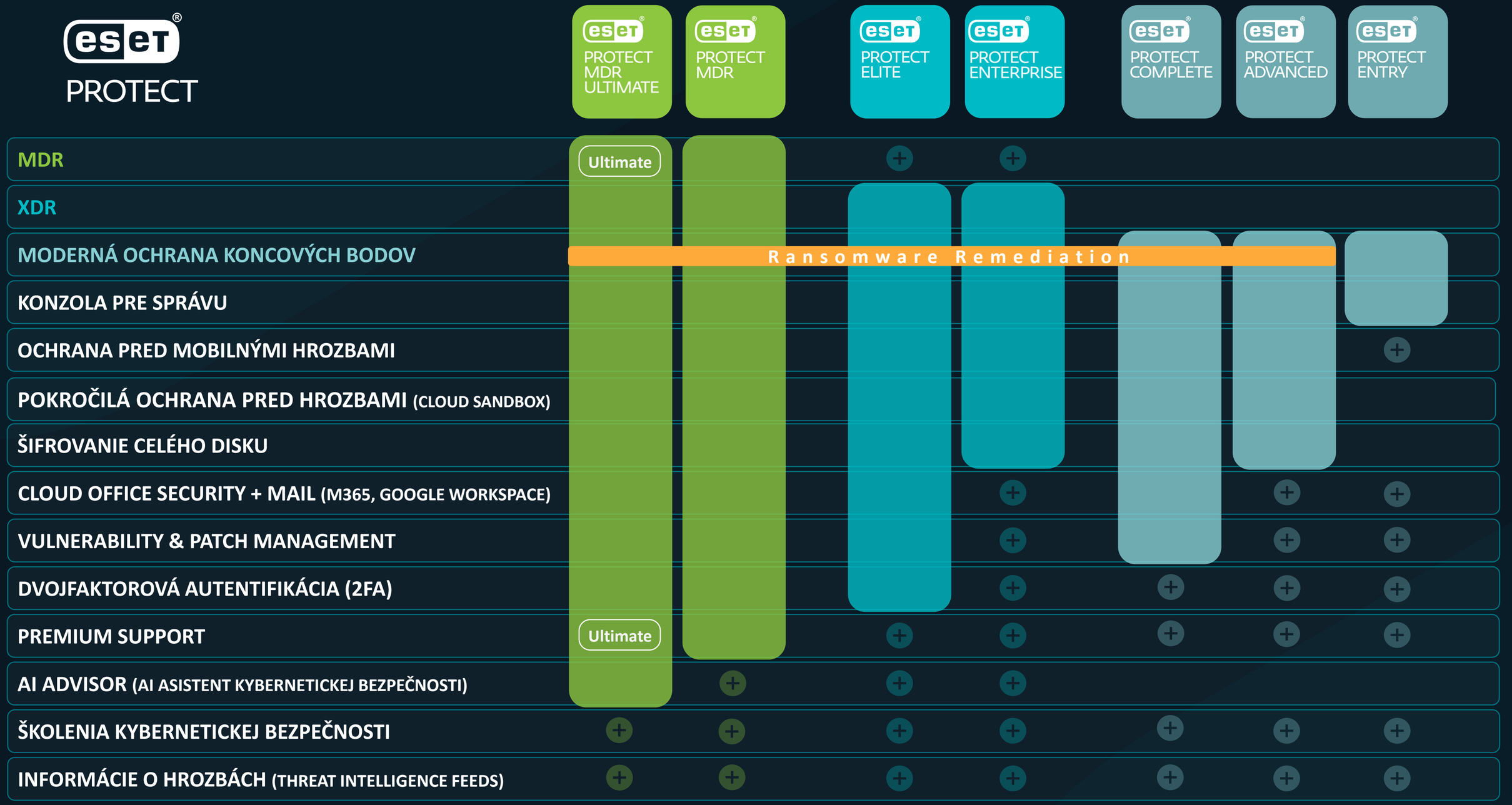
Key features

- Antispam
- Anti-malware
- Anti-phishing
- Anti-spoofing
- Homoglyph Detection
- Advanced Threat Defense
- Dashboard & Notifications
- Multitenancy with access management
- Quarantine manager & Email Clawback
- Policies and automation
- Deployment in just 5 minutes
- Protected applications

Exchange Online, SharePoint Online, Teams, OneDrive, Gmail, Google Drive

Riadenie prístupov

- **Čo je to prístup?**
- **Opatrenia:**
  - Jednoznačná identifikácia
  - Autorizácia len na nevyhnutné prostriedky IS
  - 2FA
  - .....


PROTECT
PROTECT MDR ULTIMATE
PROTECT MDR
PROTECT ELITE
PROTECT ENTERPRISE
PROTECT COMPLETE
PROTECT ADVANCED
PROTECT ENTRY
MDR
Ultimate
XDR
MODERNÁ OCHRANA KONCOVÝCH BODOV
Ransomware Remediation
KONZOLA PRE SPRÁVU
OCHRANA PRED MOBILNÝMI HROZBAMI
POKROČILÁ OCHRANA PRED HROZBAMI (CLOUD SANDBOX)
ŠIFROVANIE CELÉHO DISKU
CLOUD OFFICE SECURITY + MAIL (M365, GOOGLE WORKSPACE)
VULNERABILITY & PATCH MANAGEMENT
DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)
PREMIUM SUPPORT
Ultimate
AI ADVISOR (AI ASISTENT KYBERNETICKEJ BEZPEČNOSTI)
ŠKOLENIA KYBERNETICKEJ BEZPEČNOSTI
INFORMÁCIE O HROZBÁCH (THREAT INTELLIGENCE FEEDS)
doplnok

ESET SECURE AUTHENTICATION

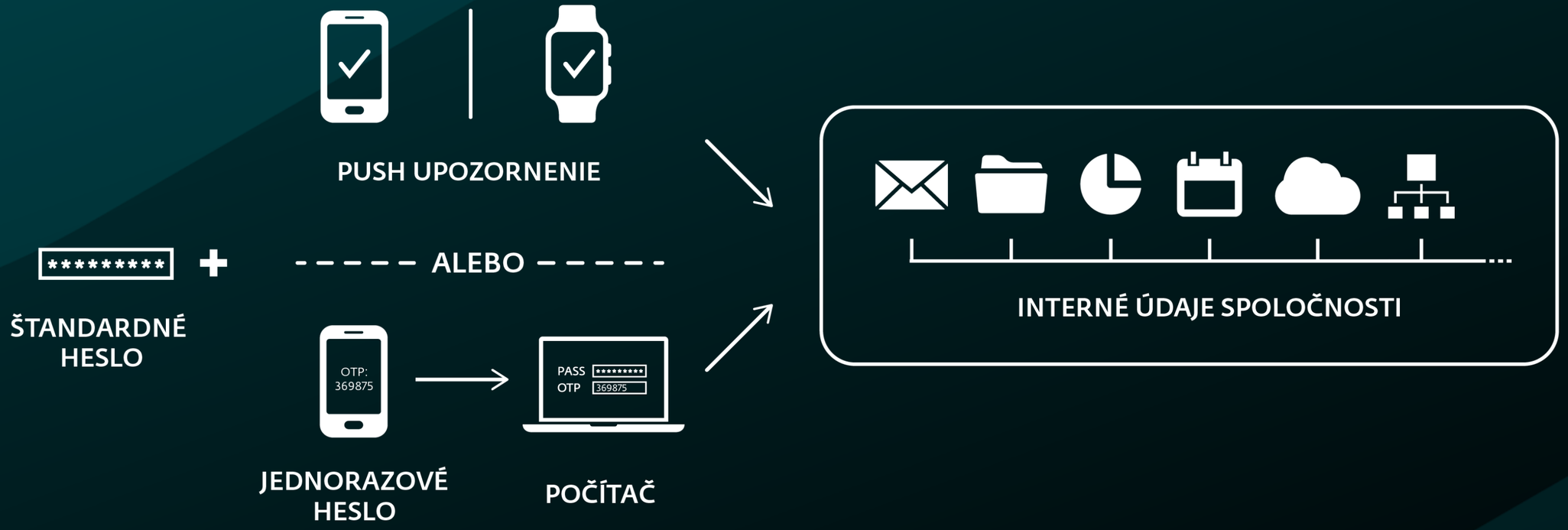
Dvojfaktorová autentifikácia, ktorá sa ľahko implementuje a používa

ESET SECURE AUTHENTICATION

61 % únikov údajov zahŕňalo prihlasovacie údaje

Pomáha riešiť riziká spojené s :

- externým prístupom k sieti zvonku
- zvyšujúcim sa počtom služieb
- zlým zaobchádzaním s heslami
- prácou na diaľku


PUSH UPOZORNENIE
****
ALEBO
ŠTANDARDNÉ HESLO
OTP: 369875
PASS *********
OTP 369875
JEDNORAZOVÉ HESLO
POČÍTAČ
INTERNÉ ÚDAJE SPOLOČNOSTI

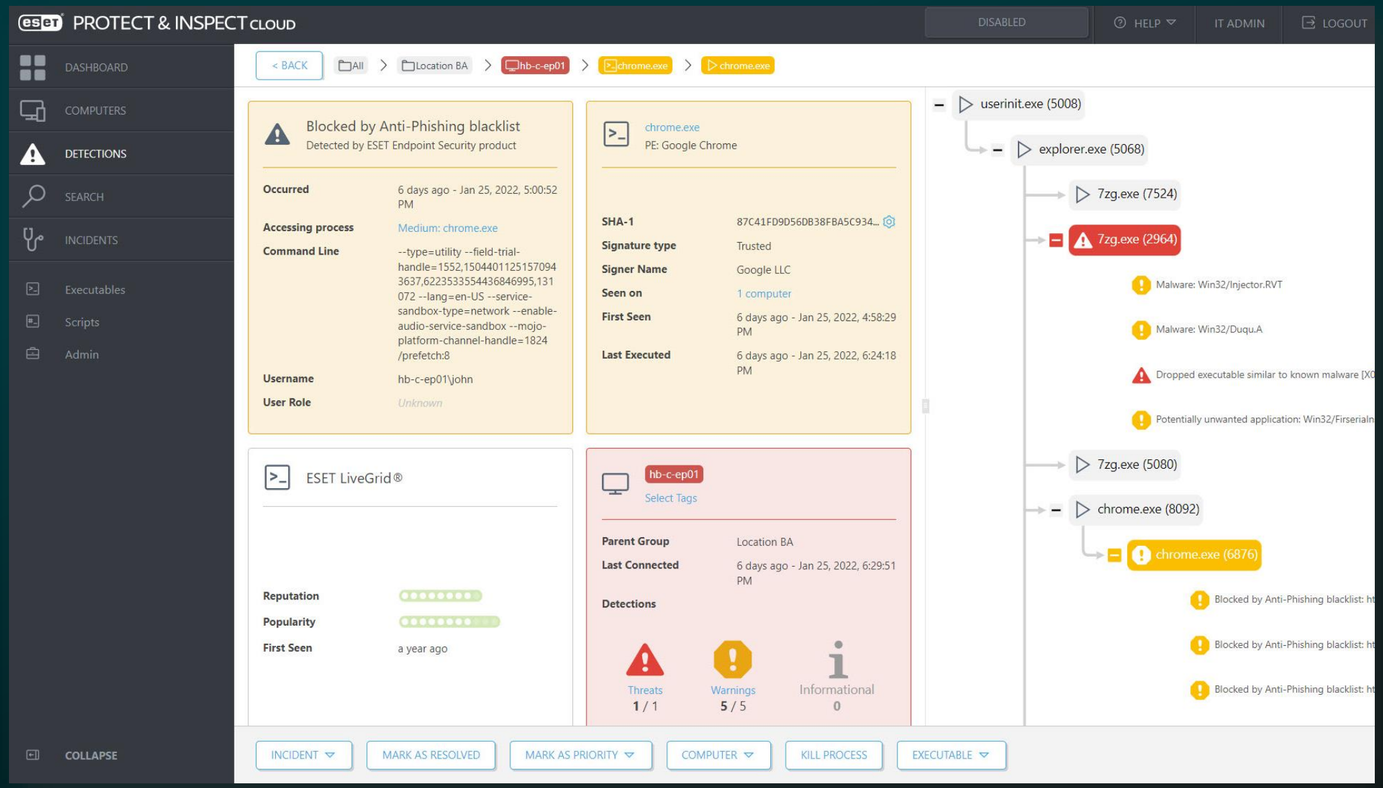
SECURE AUTHENTICATION

Príklady použitia

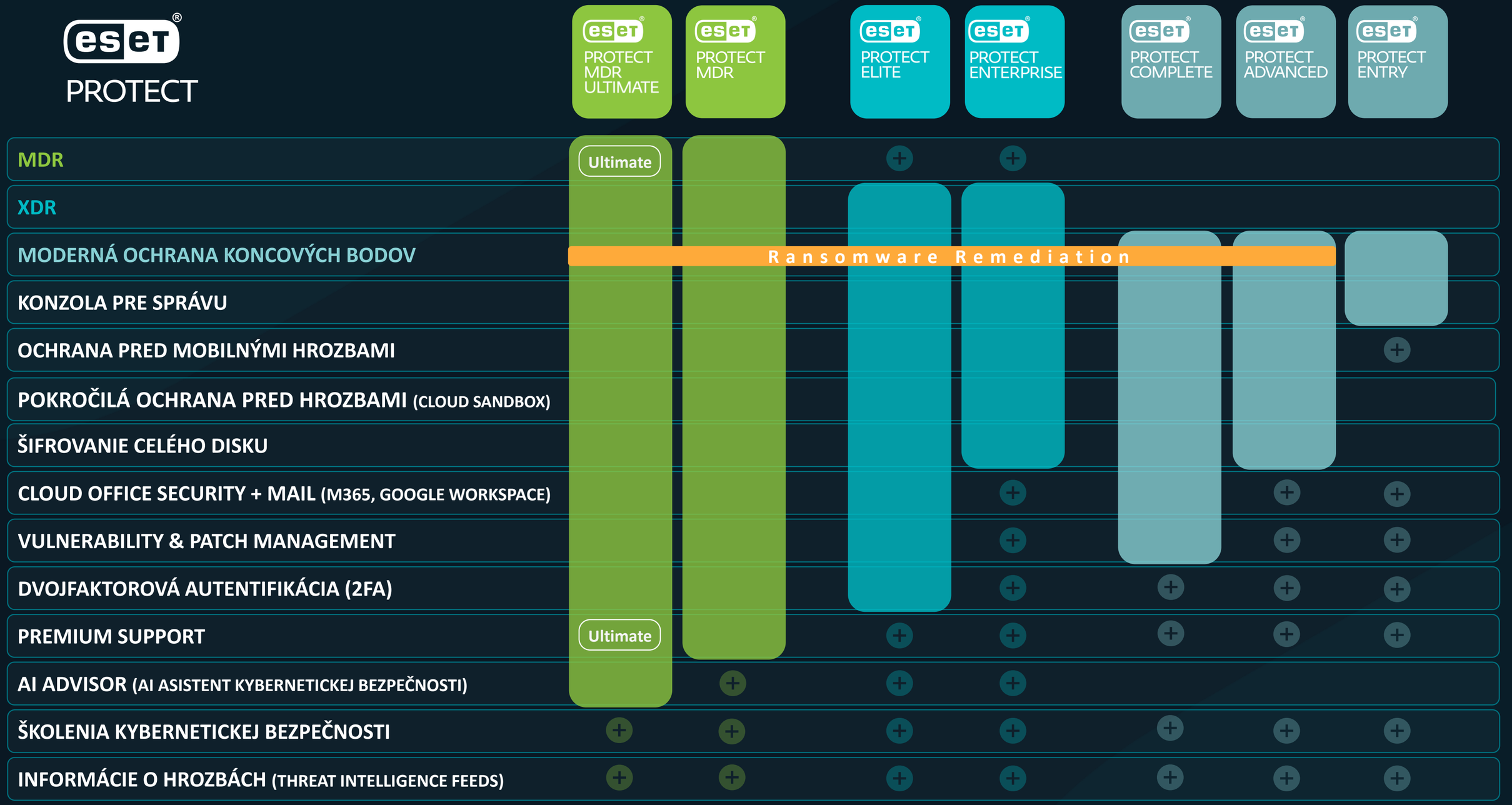
- Prihlásenie do fyzického lokálneho počítača/virtuálneho počítača/na vzdialenú plochu
- Prihlásenie do siete VPN
- Webmail, CRM a služby dostupné cez prehliadač
- Prihlásenie do úložiska tretej strany (Dropbox,…)
- SAML2 podpora
- SDK/API

Riadenie udalostí a kyber incidentov

- **Čo a ako riadiť?**
  - Incidenty
  - BCM
  - ……
- **Opatrenia:**
  - XDR platforma
  - zber a korelácia dát
  - multiplatformovosť
  - framework (MITRE ATT&CK ….)



ESET INSPECT


PROTECT
PROTECT MDR ULTIMATE
PROTECT MDR
PROTECT ELITE
PROTECT ENTERPRISE
PROTECT COMPLETE
PROTECT ADVANCED
PROTECT ENTRY
MDR
Ultimate
XDR
MODERNÁ OCHRANA KONCOVÝCH BODOV
Ransomware Remediation
KONZOLA PRE SPRÁVU
OCHRANA PRED MOBILNÝMI HROZBAMI
POKROČILÁ OCHRANA PRED HROZBAMI (CLOUD SANDBOX)
ŠIFROVANIE CELÉHO DISKU
CLOUD OFFICE SECURITY + MAIL (M365, GOOGLE WORKSPACE)
VULNERABILITY & PATCH MANAGEMENT
DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)
PREMIUM SUPPORT
Ultimate
AI ADVISOR (AI ASISTENT KYBERNETICKEJ BEZPEČNOSTI)
ŠKOLENIA KYBERNETICKEJ BEZPEČNOSTI
INFORMÁCIE O HROZBÁCH (THREAT INTELLIGENCE FEEDS)
doplnok

XDR?

Čo sa deje?

Ako sa to začalo?
Kde sa to začalo?
Kedy sa to začalo?
Čo to obsahuje?
Ako tomu vieme predísť?

Asi ide o kybernetický útok.

Nie sme si istí.
Nie sme si istí.
Nie sme si istí.
Nie sme si istí.
Nie sme si istí.

XDR Vám umožňuje odpovedať na tieto otázky

ESET INSPECT

Dobre prispôsobiteľné riešenie na detekciu
a následnú reakciu na útoky na koncové zariadenia

Poskytuje vynikajúci prehľad o hrozbách a systéme, umožňuje im vykonávať rýchlu a hĺbkovú analýzu príčin vzniku a okamžite reagovať na incidenty.

Toto riešenie zabezpečuje:

- ✓ Detekciu pokročilých pretrvávajúcich hrozieb
- ✓ Zastavenie bezsúborových útokov
- ✓ Blokovanie zero-day hrozieb
- ✓ Ochranu pred ransomvérom
- ✓ Zachytenie porušovania firemných pravidiel

Prehľad o stave koncových zariadení

Aktívne súčasti

Bezsúborové útoky

Hlavná príčina

Laterálny pohyb

Dotknuté dáta

Použité techniky

Pokročilá možnosť reakcie na vzniknuté hrozby

Blokovanie spustenia

Izolácia počítača

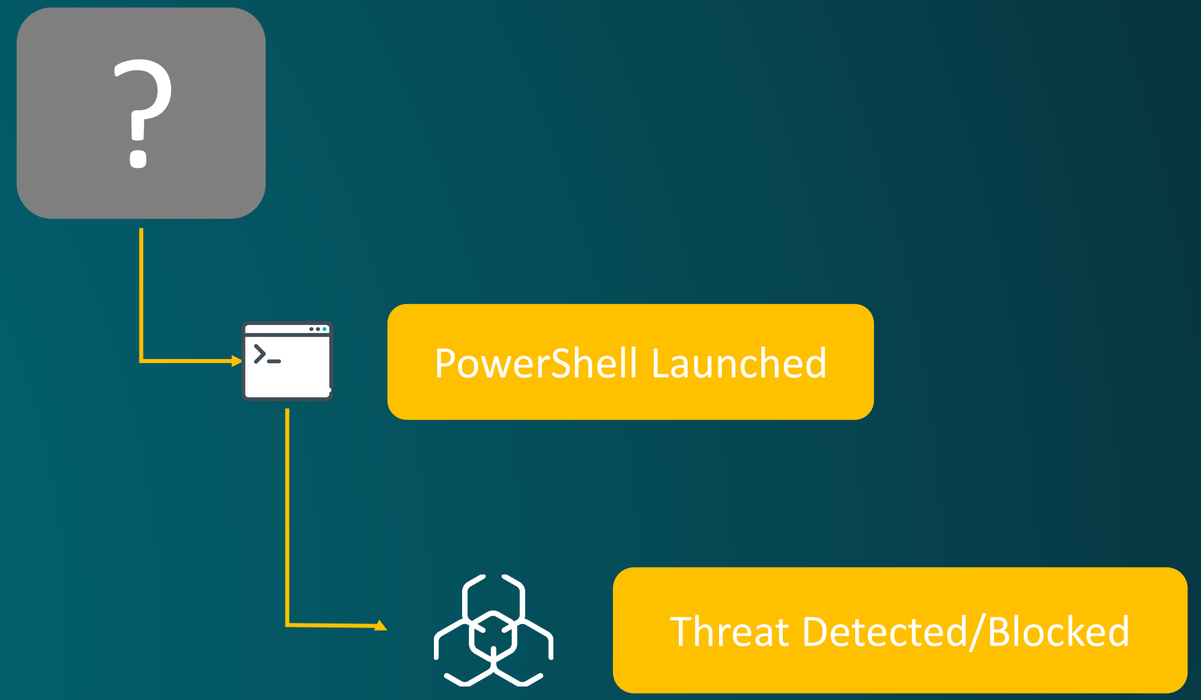
Ukončenie procesu

Vyliečenie súboru

Bežná viditeľnosť AV ochrany:

minimálna viditeľnosť

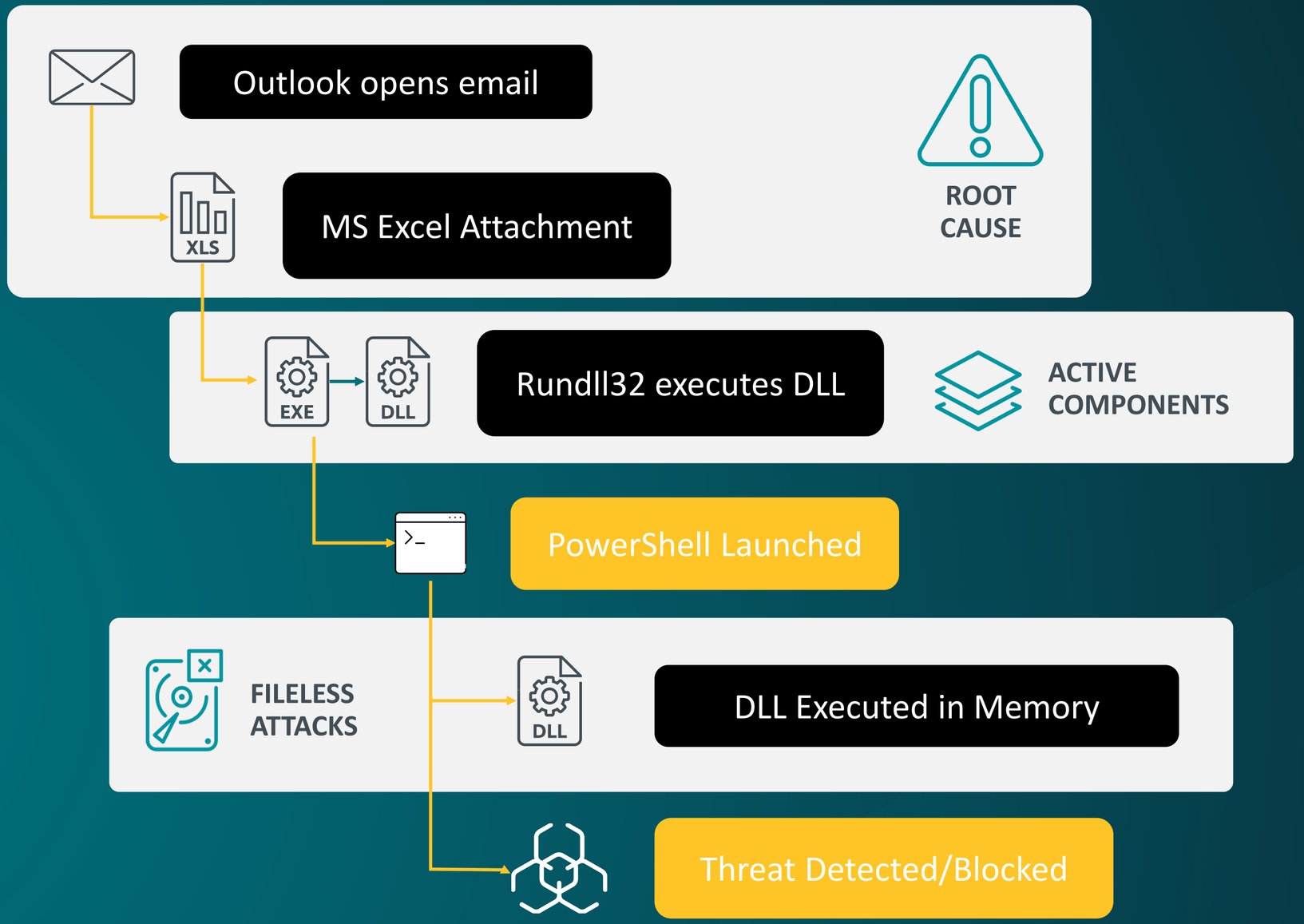
neistota



S ESET Inspect riešením:

zvýšená viditeľnosť

dodatočná kontrola

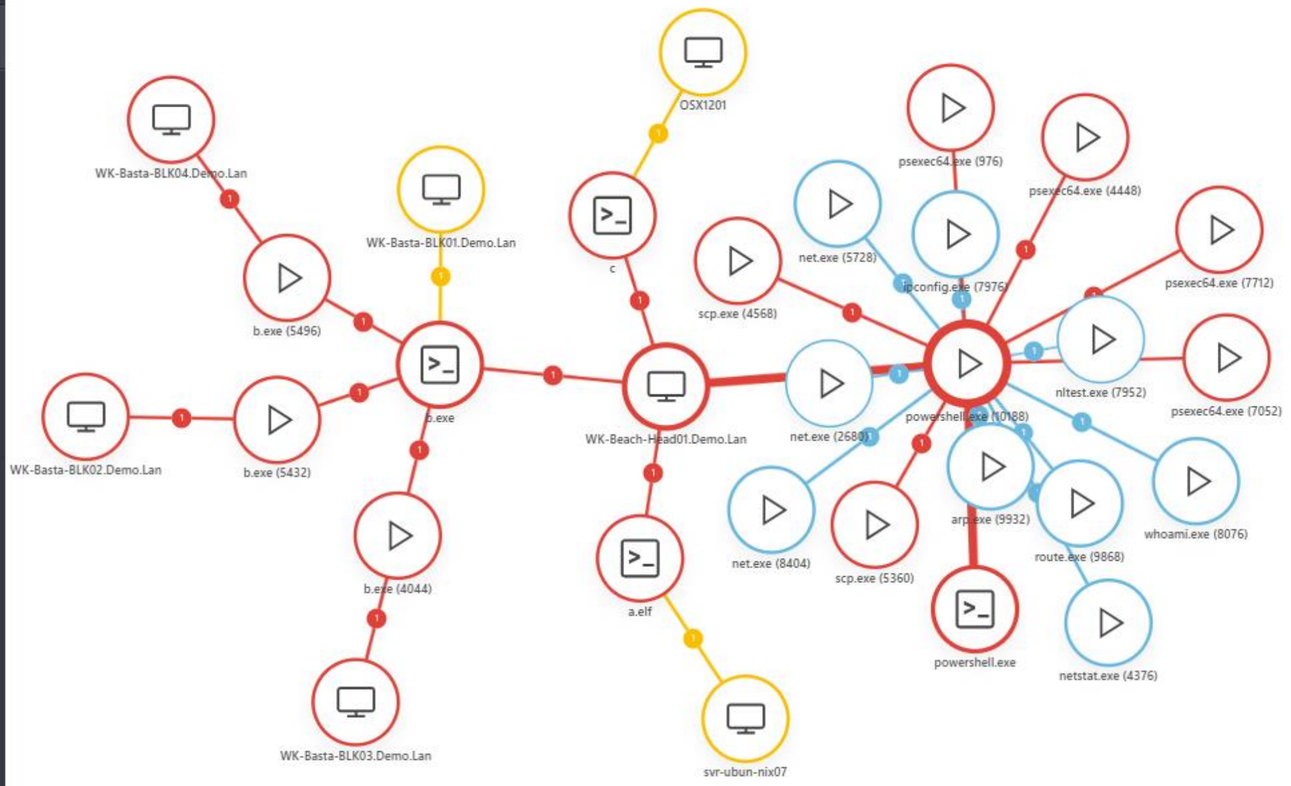


DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE

BACK

Filecoder activity across multiple endpoints

Timeline | Relation graph | Detections | Computers | Executables | Processes



INCIDENT | REMEDIATION | COMMENT | EDIT | ASSIGN | PROGRESS | GRAPH

Incident | Timeline

Filecoder activity across multiple endpoints

Status Open
Severity High
Assignee Michal Jankech
Tags Gartner Scenario 2 | Ransomware Atta... | Select tags
Description None

Threat indicators (28)

Rule Domain trust discovery [D1102]
Mitre att&ck™ techniques
T1482 - Domain Trust Discovery

Rule Domain trust enumeration via NLTest/ADFind [C1118]
Mitre att&ck™ techniques
T1482 - Domain Trust Discovery

View more

Computers (7)

wk-beach-head01.demo.lan
osx1201

View more

Executables (4)

c
powershell.exe

View more

Processes (19)

powershell.exe (10188)
nltest.exe (7952)

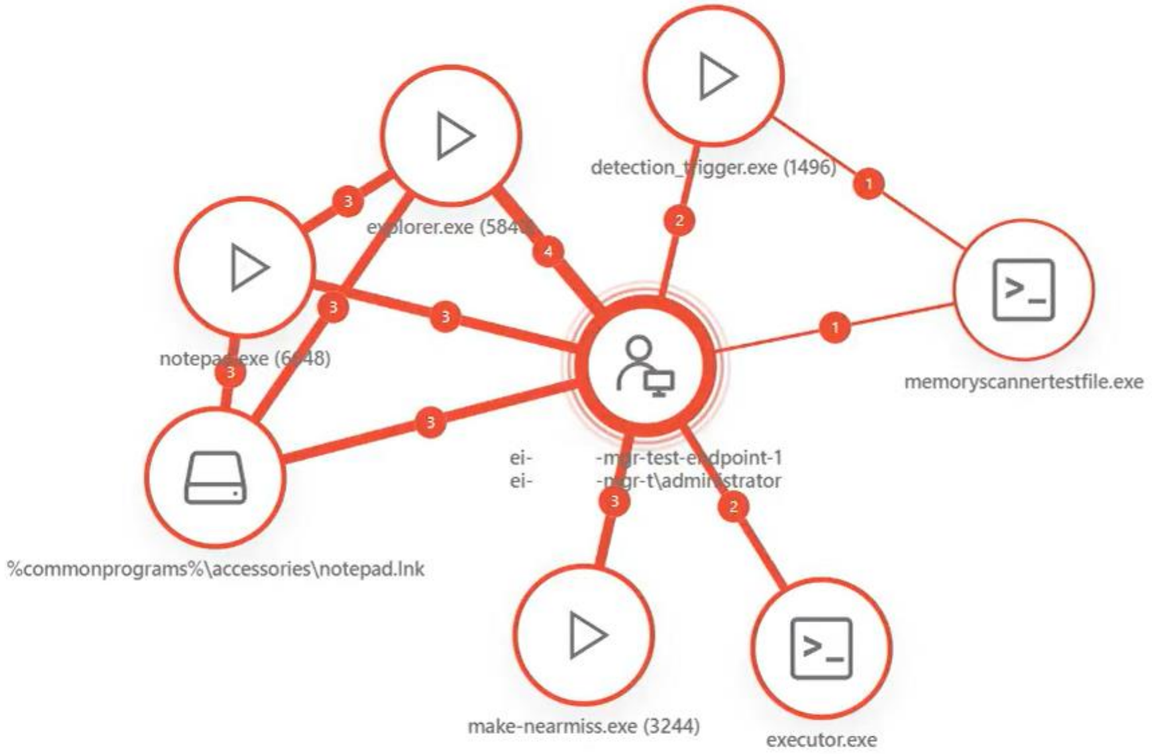
View more

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

BACK

Suspected Malware Execution and Botnet Activity on ei- -mgr-test-endpoint-1

Incident graph | Timeline | Detections | Computers | Executables | Processes



Incident | Timeline | Assistant

What data or information was accessed or exfiltrated?

The data accessed or exfiltrated includes a dropped executable named make-nearmiss.exe, which was flagged as similar to known malware but not confirmed as malware yet. Additionally, suspected botnet activity with the threat name Win32/BotnetProtectionTest was detected from source IP 127.0.0.1 to destination IP 127.0.0.1, initiated by the user ei- -mgr-t\administrator through httpclienttester.exe, which was blocked due to its unknown reputation and lack of signature.

IMPORTANT: Generated by AI. Verify information for accuracy.

What is the reputation of the dropped executable make-nearmiss.exe?

The dropped executable make-nearmiss.exe has a reputation of "trusted."

IMPORTANT: Generated by AI. Verify information for accuracy.

any more suggestions?

1. Can you provide more details about the source IP 127.0.0.1 and the destination IP 127.0.0.1 in the suspected botnet activity?
2. What action was taken in response to the suspected botnet activity with the threat name Win32/BotnetProtectionTest?
3. Can you provide information about the process httpclienttester.exe and its reputation?

IMPORTANT: Generated by AI. Verify information for accuracy.

Ask ESET AI Advisor anything...

Responses are generated by AI. Verify information for accuracy.

INCIDENT | REMEDIATION | COMMENT | EDIT | ASSIGN | PROGRESS | GRAPH

Monitorovanie, zaznamenávanie a hlásenie udalostí

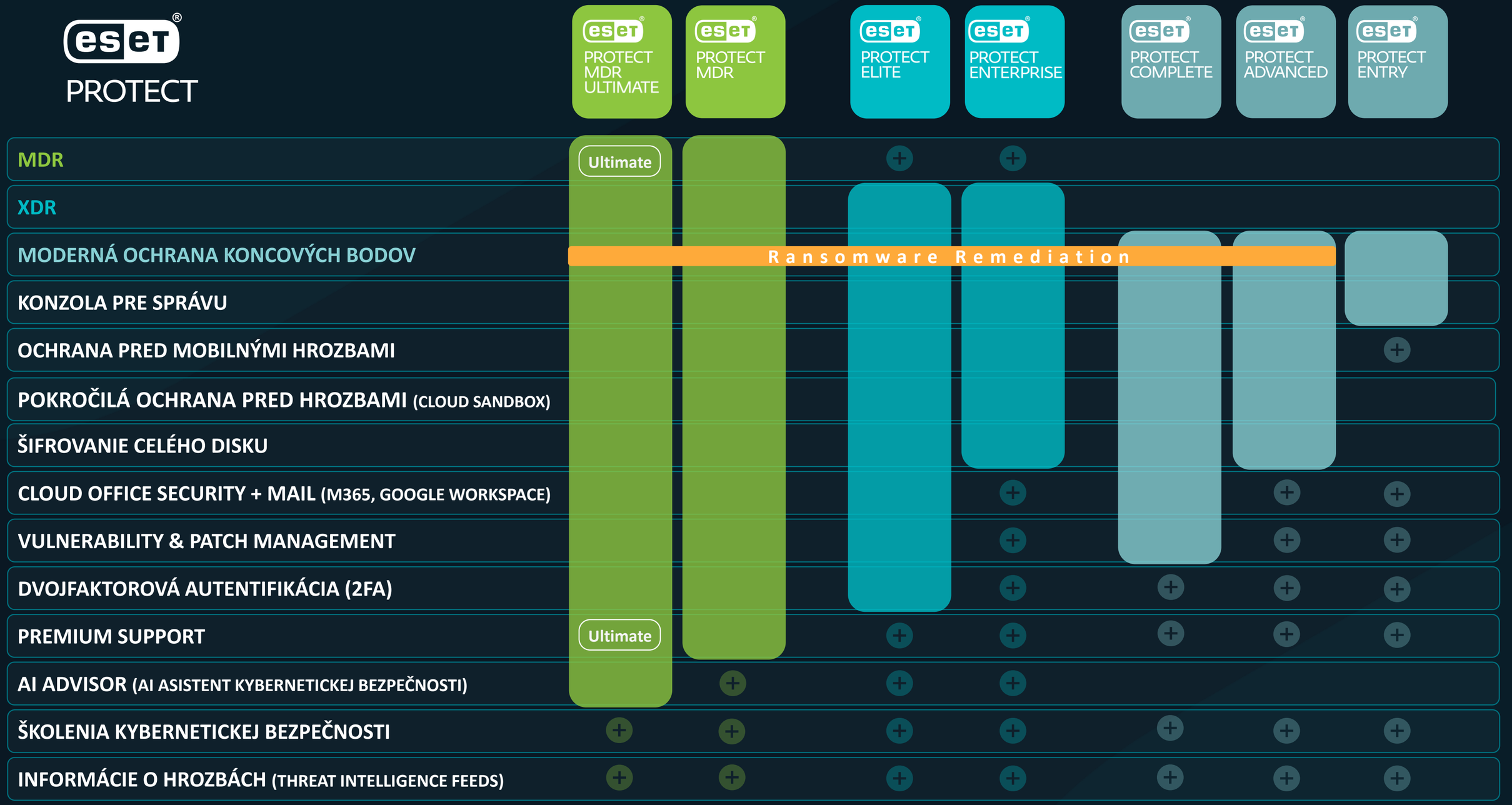
Kde vie ESET pomôcť?

- MDR (služby manažovanej bezpečnosti)

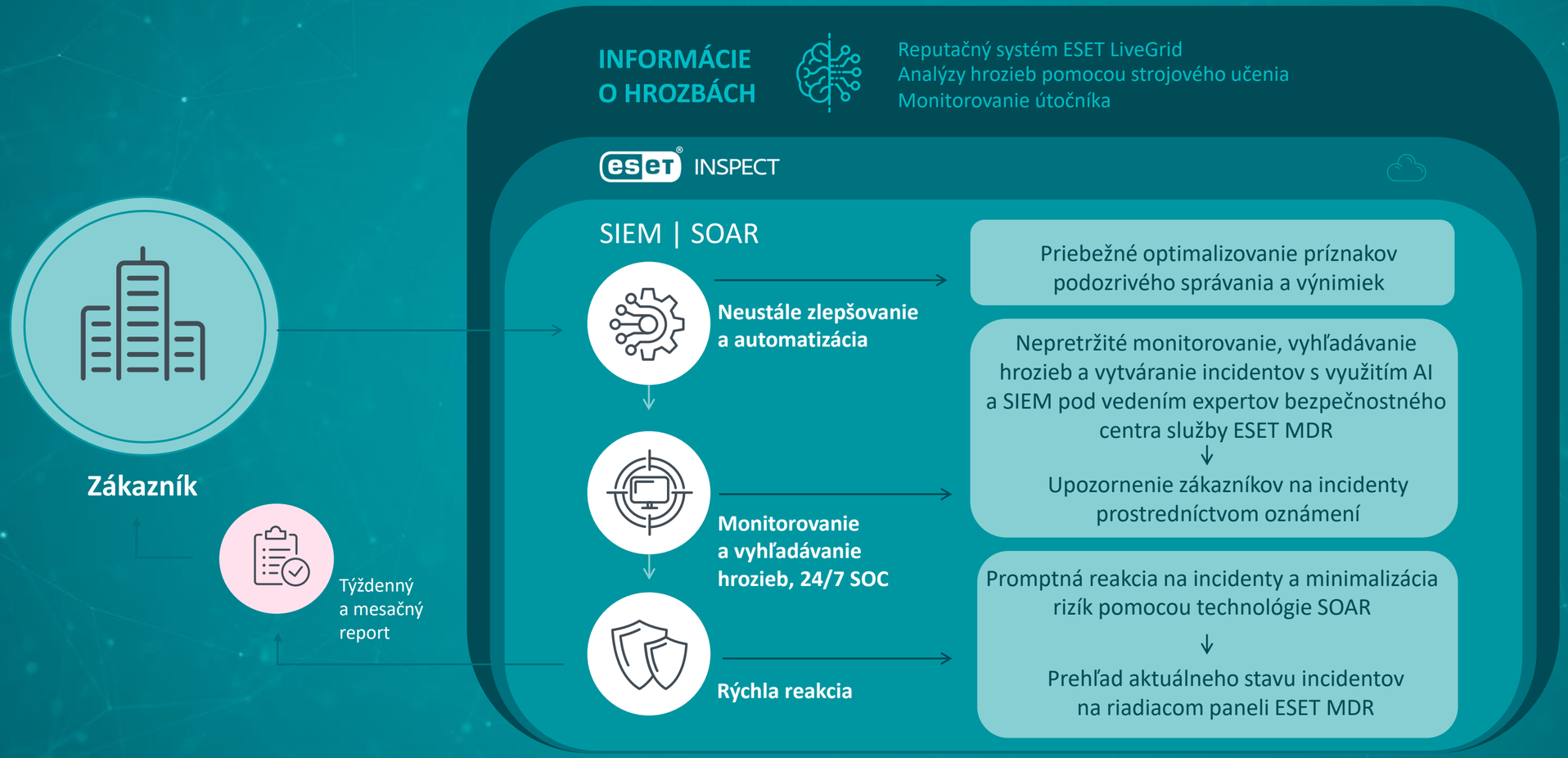
Čo obsahuje:

- nepretržité monitorovanie, triedenie a reakcie na hrozby
- reakcia na aktívne prebiehajúce kampane útočníkov
- knižnica príznakov podozrivého správania
- optimalizácia príznakov podozrivého správania a výnimiek
- expertíza dodávateľa
- ...

ESET PROTECT MDR ESET MDR


PROTECT
PROTECT MDR ULTIMATE
PROTECT MDR
PROTECT ELITE
PROTECT ENTERPRISE
PROTECT COMPLETE
PROTECT ADVANCED
PROTECT ENTRY
MDR
Ultimate
XDR
MODERNÁ OCHRANA KONCOVÝCH BODOV
Ransomware Remediation
KONZOLA PRE SPRÁVU
OCHRANA PRED MOBILNÝMI HROZBAMI
POKROČILÁ OCHRANA PRED HROZBAMI (CLOUD SANDBOX)
ŠIFROVANIE CELÉHO DISKU
CLOUD OFFICE SECURITY + MAIL (M365, GOOGLE WORKSPACE)
VULNERABILITY & PATCH MANAGEMENT
DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)
PREMIUM SUPPORT
Ultimate
AI ADVISOR (AI ASISTENT KYBERNETICKEJ BEZPEČNOSTI)
ŠKOLENIA KYBERNETICKEJ BEZPEČNOSTI
INFORMÁCIE O HROZBÁCH (THREAT INTELLIGENCE FEEDS)
doplnok

Ako funguje ESET MDR



DASHBOARD
COMPUTERS
INCIDENTS
VULNERABILITIES
Patch Management
Detections
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE

Dashboard

ESET MDR | Status Overview | ESET LiveGuard | ESET Vulnerability & Patch Management | ESET Inspect | ESET Cloud Office Security | Detections | Computers | Antivirus detections | Firewall detections | ESET applications | Cloud-bas

Incidents 30d

Total	High	Medium	Low
4	1	3	0

Top incidents awaiting user input 30d

Incident name	Author	Creation date	Impacted computers	Assigned to
Incident on computer...	Connect Apollo	09/04/2024, 12:31 PM	1	Connect Apollo

Incident pipeline 30d

Created incidents	4
Detections related to incidents	3
All detections	17,831

Incident status 30d

Open	2
Waiting for user input	1
Closed - Responded to	0
Closed - False positive	0
Closed - True positive	1
Closed - Canceled	0

Top impacted computers 30d

Computer name	Incidents	Group name	Last seen
c06-w10x64-rs5	1	/All/Companies/Apollo Connect Test	09/29/2024, 9:53 AM
1015	1	/All/Companies/Apollo Connect Test	09/27/2024, 9:53 AM
miso-windows11	1	/All/Companies/Apollo Connect Test	09/25/2024, 9:53 AM

Response actions 30d

Kill process	7
Clean and block	0
Block executable	3

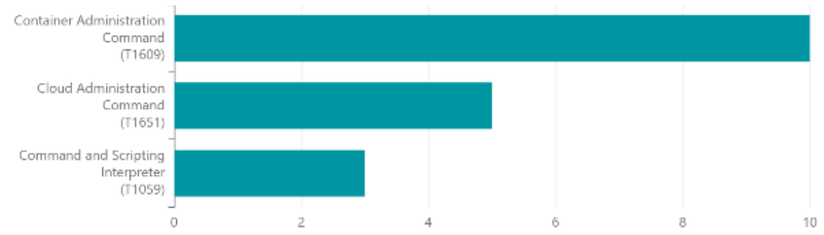
Incident response management

Protected	174
User-managed	3
Not monitored	40

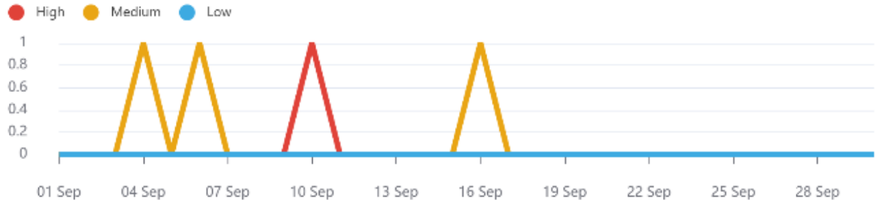
ESET MDR protection

Enabled	177
Enablement in progress	0
Removal in progress	0
Not yet enabled	40

Top MITRE ATT&CK™ techniques 30d



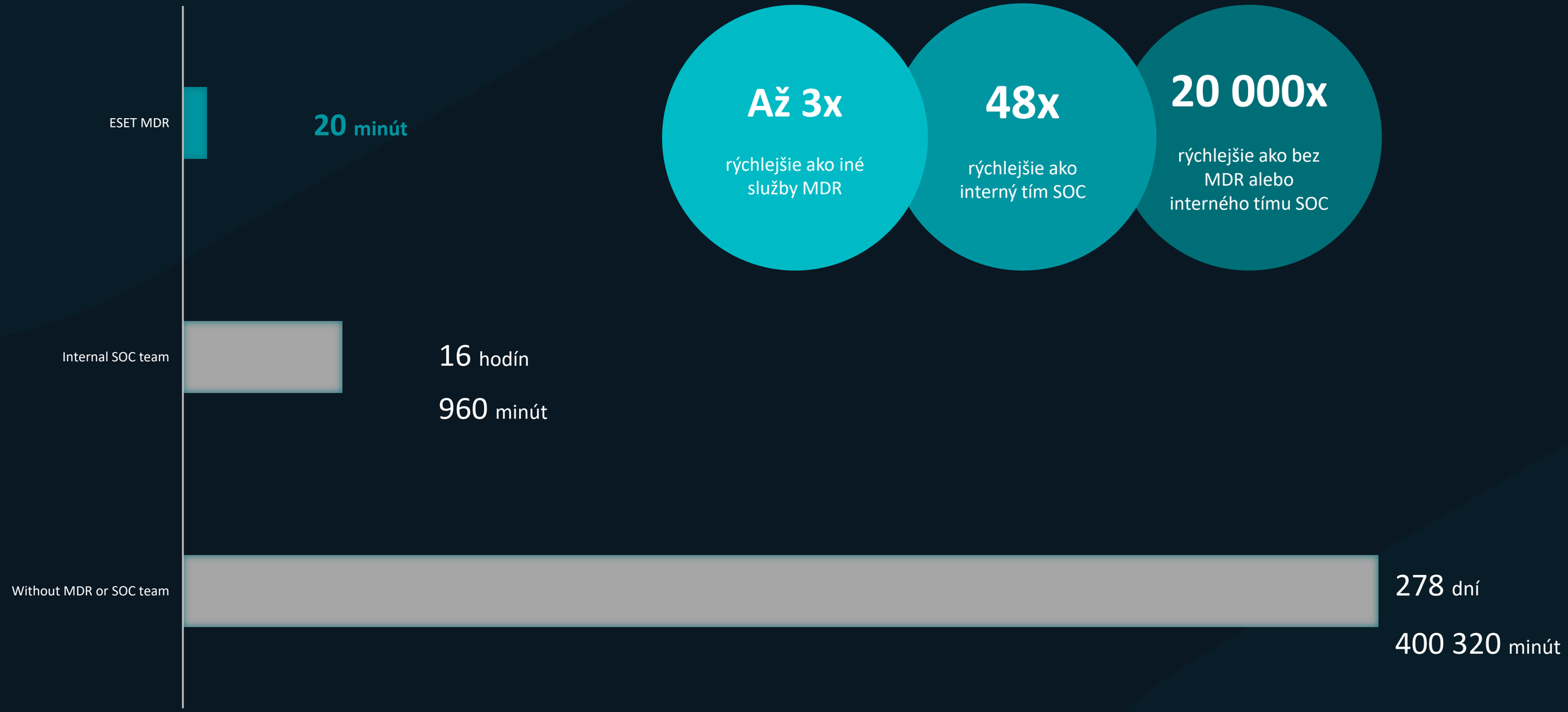
Incidents in time 30d



Špecifikácie ESET MDR služieb

	MDR	MDR Ultimate
24/7 monitorovanie, vyhľadávanie, triedenie a reakcia na hrozby pod vedením odborníkov	✓	✓
Tím Global Threat Intelligence	✓	✓
Optimalizácia vzorov správania a vylúčenia	✓	✓
Knižnica vzorcov správania	✓	✓
Prispôsobené reporty	✓ Štandard	✓ Pokročilé
Prispôsobené vyhľadávanie hrozieb		✓
Viditeľnosť vektorov útoku		✓
Pomoc pri riešení digitálnych forenzných incidentov (DFIR)		✓
Dedikovaný expert na incidenty		✓
Odborná pomoc pri upozorneniach MDR s väčším kontextom		✓

V čom je MDR výnimočné



Až 3x

rýchlejšie ako iné služby MDR

48x

rýchlejšie ako interný tím SOC

20 000x

rýchlejšie ako bez MDR alebo interného tímu SOC

ESET MDR v číslach

250+ zákazníkov

Monitorujeme viac ako 20 000+ staníc

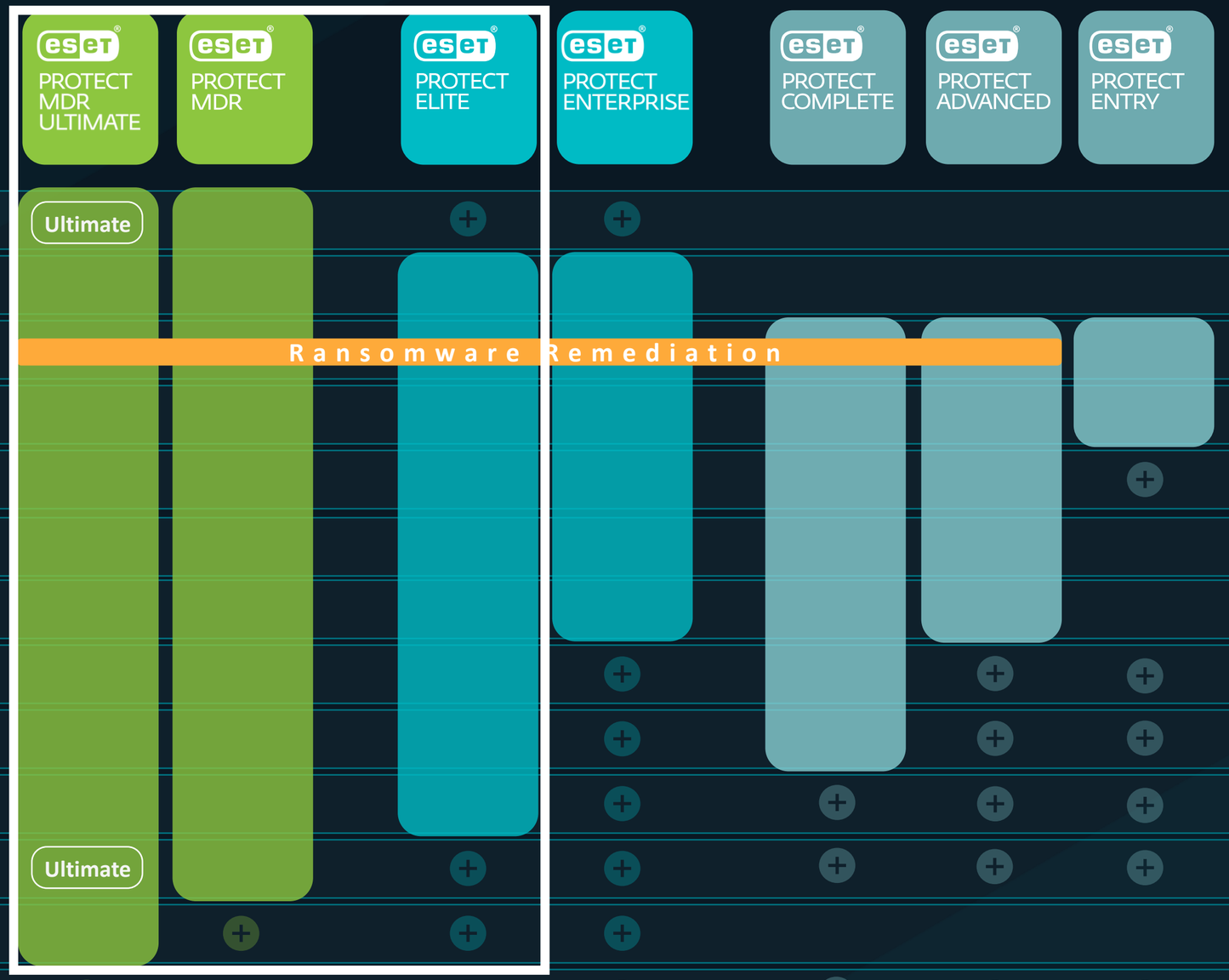
Počet riešených True Positive Incidentov: 200+

PROTECT ELITE

PROTECT MDR

PROTECT MDR ULTIMATE

ESET PROTECT



	PROTECT MDR ULTIMATE	PROTECT MDR	PROTECT ELITE	PROTECT ENTERPRISE	PROTECT COMPLETE	PROTECT ADVANCED	PROTECT ENTRY
MDR	Ultimate		+	+			
XDR							
MODERNÁ OCHRANA KONCOVÝCH BODOV							
KONZOLA PRE SPRÁVU							
OCHRANA PRED MOBILNÝMI HROZBAMI							+
POKROČILÁ OCHRANA PRED HROZBAMI (CLOUD SANDBOX)							
ŠIFROVANIE CELÉHO DISKU							
CLOUD OFFICE SECURITY (M365, GOOGLE WORKSPACE)				+		+	+
VULNERABILITY & PATCH MANAGEMENT				+		+	+
DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)				+	+	+	+
PREMIUM SUPPORT	Ultimate		+	+	+	+	+
AI ADVISOR (AI ASISTENT KYBERNETICKEJ BEZPEČNOSTI)		+	+	+			
ŠKOLENIA KYBERNETICKEJ BEZPEČNOSTI	+	+	+	+	+	+	+
INFORMÁCIE O HROZBÁCH (THREAT INTELLIGENCE FEEDS)	+	+	+	+	+	+	+

+ doplnok

SECURITY DAYS

Ďakujem za pozornosť

Digital Security
Progress. Protected. & SME KONFERENCIE