



# Ondrej Krajč

Technical Pre-Sales Representative

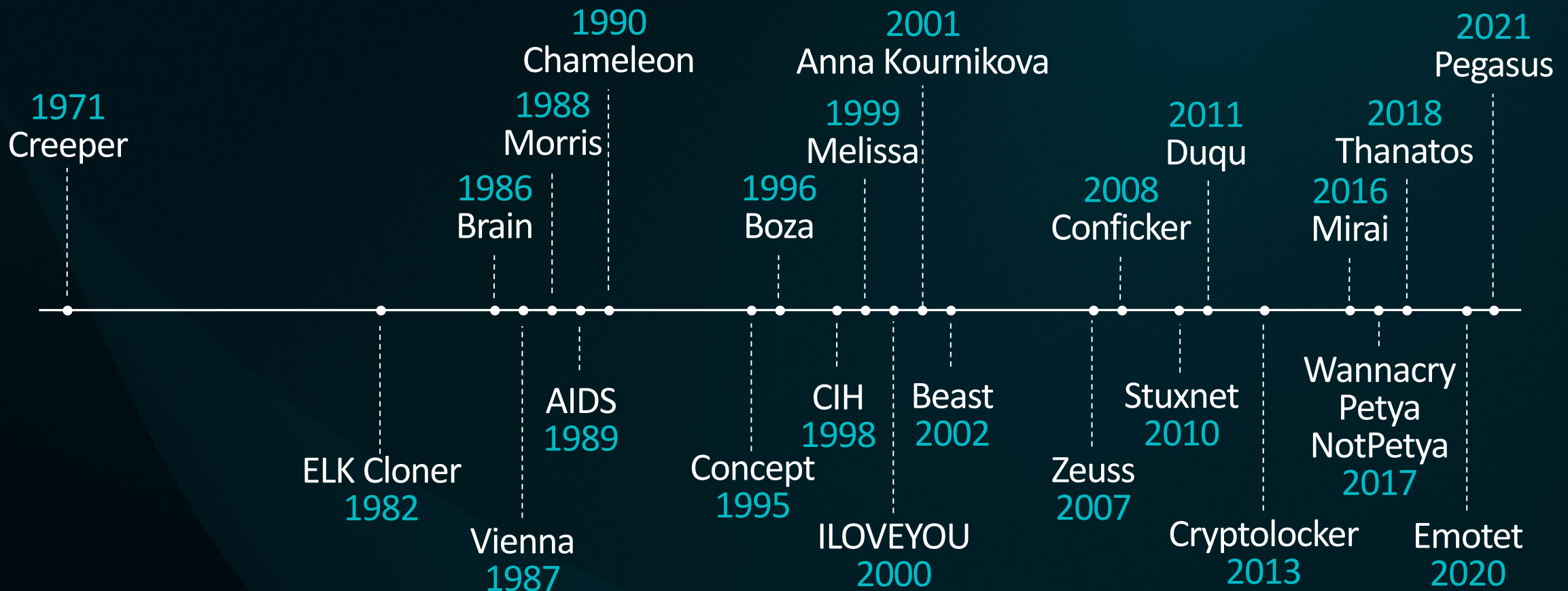
[ondrej.krajc@eset.sk](mailto:ondrej.krajc@eset.sk)



# Nové a vylepšené riešenia pre firemnú bezpečnosť

# Technológie urýchľujú ľudský pokrok

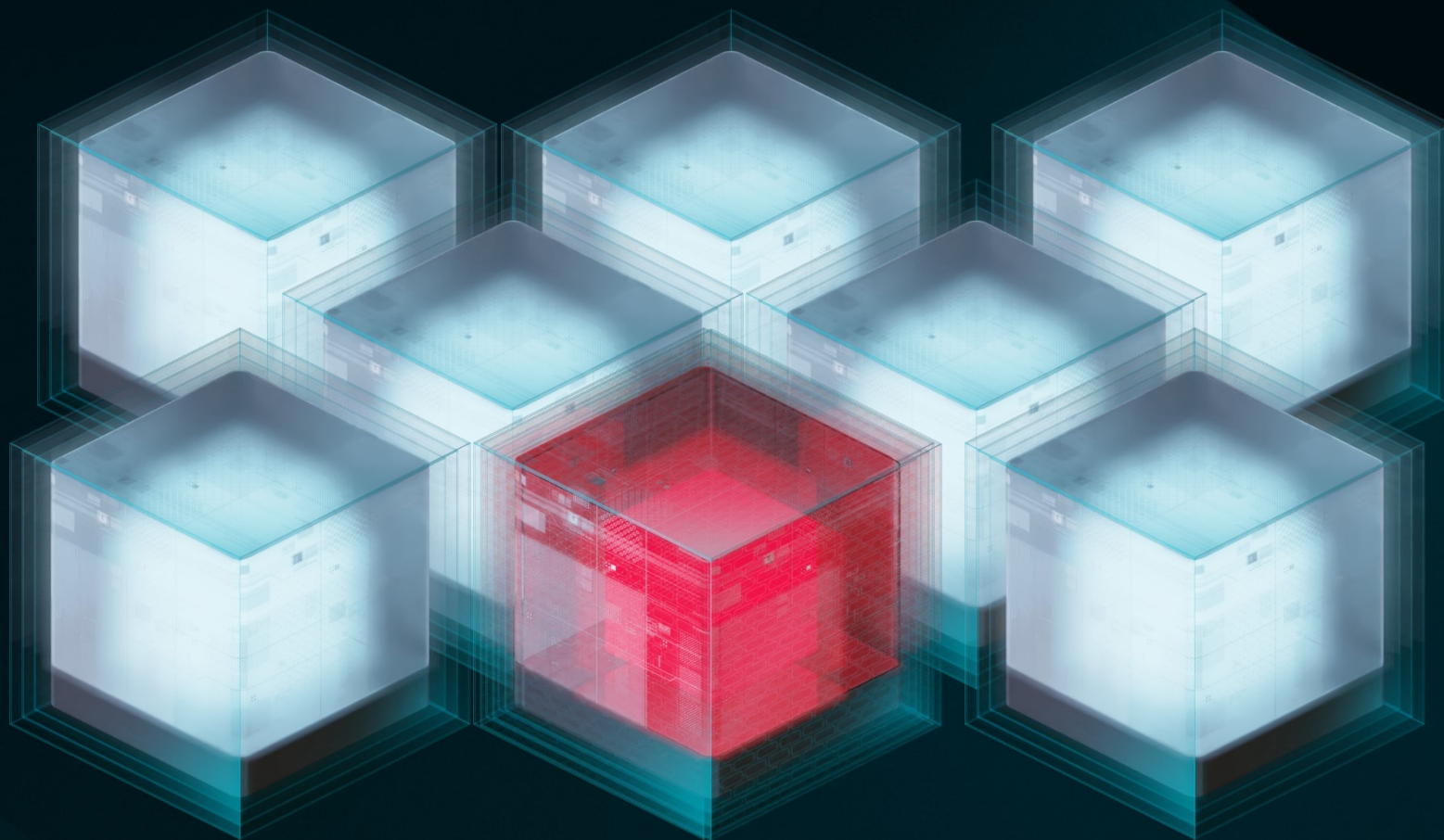
Vznik nových aspektov trestnej činnosti



# Súčasnosť

## Éra pokročilých kybernetických útokov





PREVENCIA

DETEKCIA

REAKCIA

# Produkty a úrovne zabezpečenia

## PROTECT Solution Levels

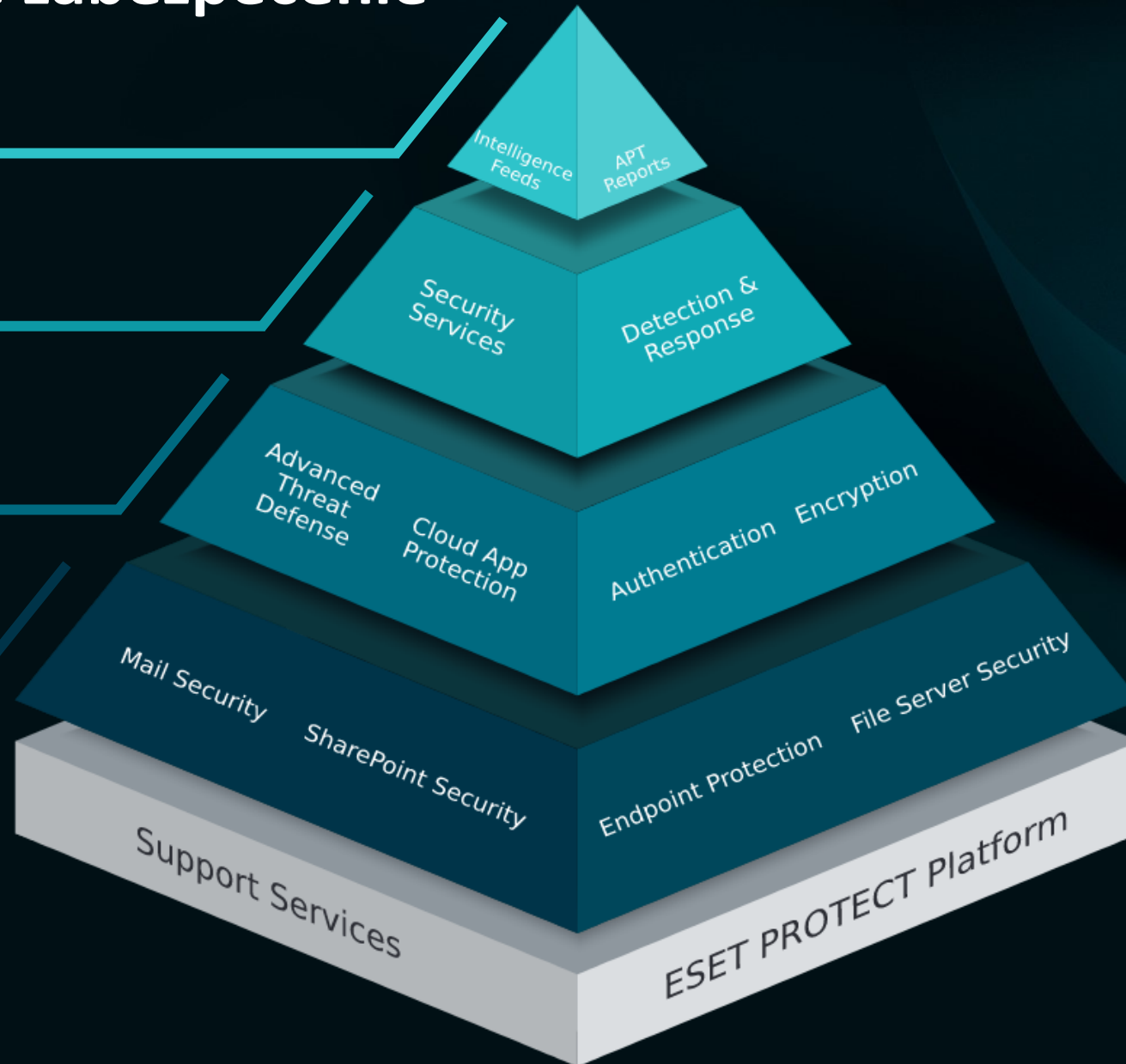
# Viacúrovňové zabezpečenie

INFORMÁCIE O HROZBÁCH

DETEKCIA A REAKCIA

ROZŠÍRENÁ  
OCHRANA

ZÁKLADNÁ  
OCHRANA



# ESET PROTECT Ecosystem => XDR Platforma



## ESET PRODUCTS & SERVICES



### IT OPERATIONS



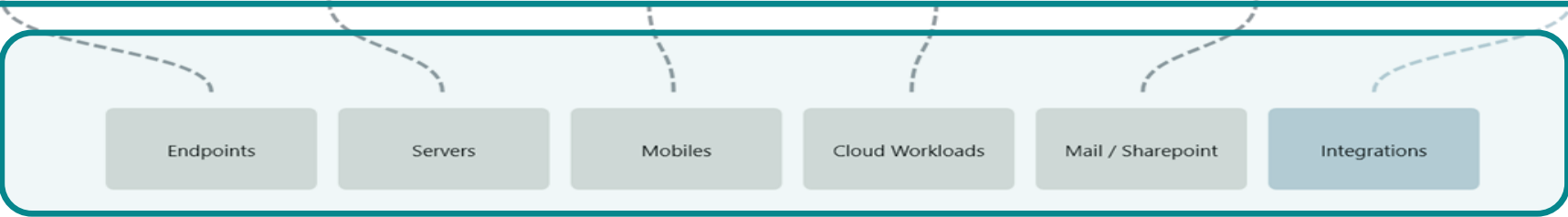
### SECURITY MANAGEMENT



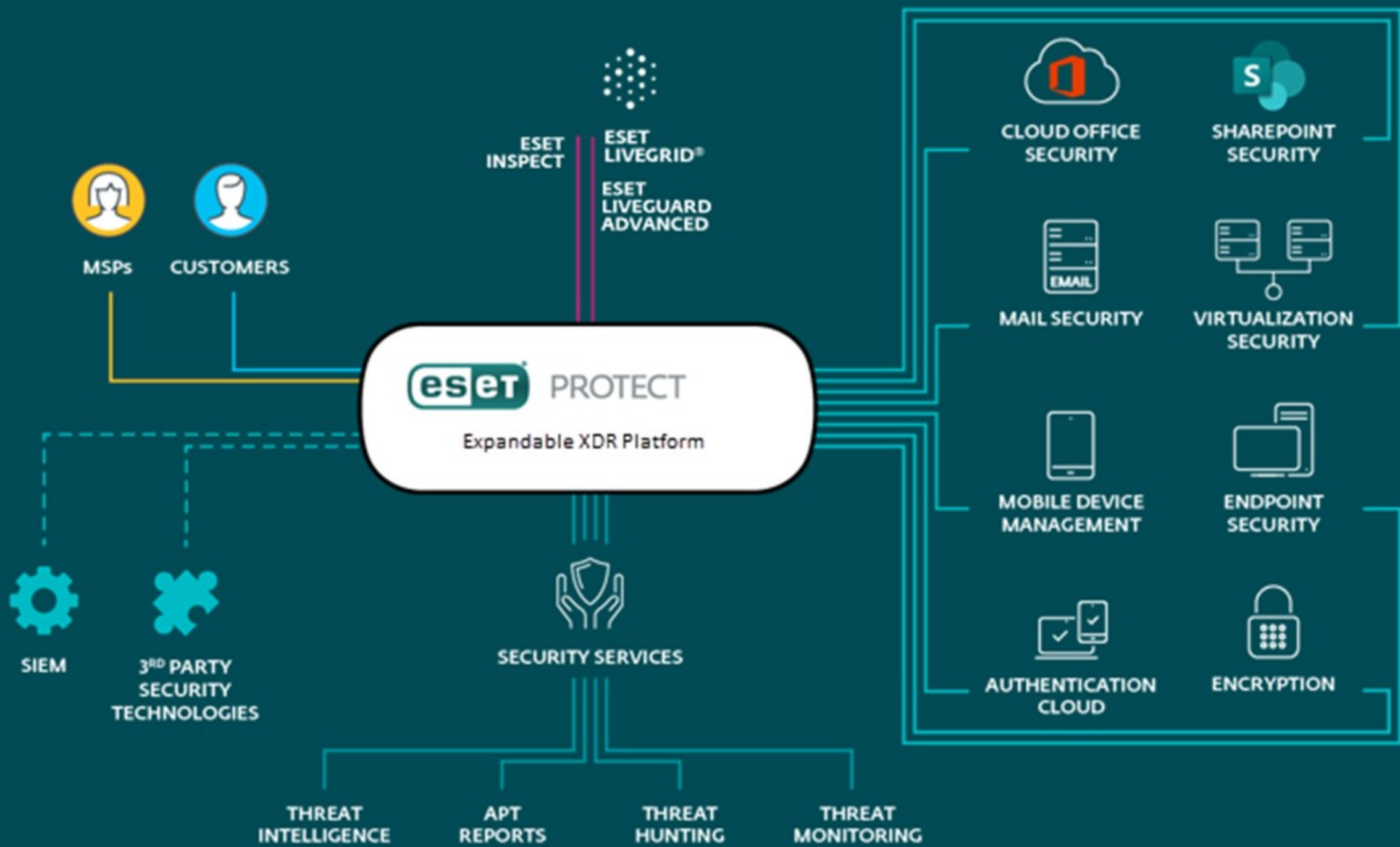
### SECURITY OPERATIONS



## ESET DETECTION TECHNOLOGIES



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



Spomenul niekto *novú generáciu*?



# Viacúrovňové zabezpečenie

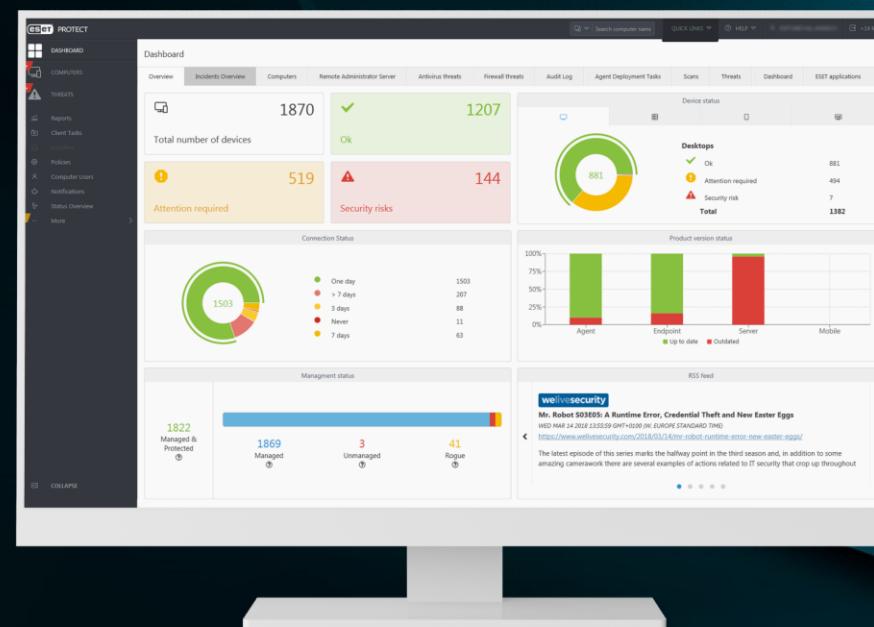




Jednotná platforma pre správu  
všetkých bezpečnostných riešení ESET

# Novinky v ESET Protect


- Automatické aktualizácie
- Brute-force attack protection management
- Live Guard dashboard
- Rýchly náhľad na PC a detekcie



**eset** PROTECT

# Automatické aktualizácie

## Automatic Product Updates ×



Automatic product updates will be enabled in your company network to ensure that you'll always have access to the latest features and achieve the highest possible security.

This change will be enabled for your network from .

To receive product updates automatically, install a product version that supports the auto-update feature.

[Which ESET products and versions support automatic updates?](#)  
[I want to install a product version that supports the auto-update feature](#)

[Configure product updates](#) [ENABLE NOW](#) [REMIND ME LATER](#)



# Bruteforce attack protection

The screenshot displays the ESET Protect management console. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Installers, Policies, Notifications, Status Overview, and More. The main area shows a 'New Policy' configuration screen with tabs for Basic, Settings, Assignments, and Summary. A 'Rules' dialog box is open, listing existing rules such as 'Block RDP brute force attack from a private network'. An 'Add rule' dialog box is also open, showing configuration options for a new rule.

**Add rule configuration:**

- Name: Untitled
- Enabled:
- Action: Allow
- Protocol: Remote Desktop Protocol (RDP)
- Profile: Any profile
- Max attempts: 10
- Blacklist retention period (min): 30
- Source IP: (empty field)
- Source zones: (empty list)

**Table of existing rules:**

	Max attempts	Blacklist retention period (min)
Block RDP brute force attack from a private network	12	10
Block RDP brute force attack from any network	10	10
Ignore SMB log attempt from a private network	0	0
Block SMB brute force attack from any network	40	10

# Live Guard dashboard

**eset** PROTECT cloud Computer Name QUICK LINKS HELP IGOR HULA LOGOUT

Dashboard

Status Overview **Security Overview** Dynamic Threat Defense Computers Antivirus detections Firewall detections ESET applications Cloud-based protection +

**9**

Unresolved Detections  
26 resolved in last 7 days

**5**

Warning  
17 resolved in last 7 days

**2**  
originally detected by  
Dynamic Threat Defense

**0**

Informational  
0 resolved in last 7 days

**4**

Critical  
9 resolved in last 7 days

**1**  
originally detected by  
Dynamic Threat Defense

Detections by severity in last 7 days

Unresolved detections

Method	Count
Antivirus	8
Web protection	1

Detections by detection method in last 7 days

Top 10 computers with detections in last 7 days

Computer name	Severity	Total
1. hb-c-e01	● 13 ● 10 ● 0	23
2. dark-nb	● 0 ● 4 ● 0	4
3. ASUS-MRC	● 0 ● 3 ● 0	3
4. hb-c-e03	● 0 ● 2 ● 0	2
5. DW-HPN-01	● 0 ● 1 ● 0	1
6. msi-JNK	● 0 ● 1 ● 0	1

Top 10 users with detections in last 7 days

User name	Severity	Total
1. HB-C-E01\adam	● 13 ● 8 ● 0	21
2. DARK-NB\admin	● 0 ● 3 ● 0	3
3. ASUS\Marcel	● 0 ● 3 ● 0	3
4. HB-C-E03\john	● 0 ● 2 ● 0	2
5. HB-C-E03\john	● 0 ● 2 ● 0	2
6. MSI\Filip	● 0 ● 1 ● 0	1

[Submit Feedback](#)

COLLAPSE

# Zvyšné vylepšenia

- indikátor posledného pripojenia
- prihlásený užívateľ na PC
- system updates management pre Android
- možnosť vytvoriť spúšťač priamo zo záložky client task details
- verzia Windows OS je reportovaná ako a samostatný symbol (napr. v Dynamických skupinách)
- zoznam analyzovaných súborov ESET LiveGuard Advanced je v záložkách detaily počítača, detekcie a karanténa
- nové produktové kategórie
- možnosť zrušiť upozornenia v rámci notifikácií pre „muted“ počítače
- podpora Java 17
- nové oprávnenie pre Inspect "Remote Shell Access"

# Viacúrovňové zabezpečenie



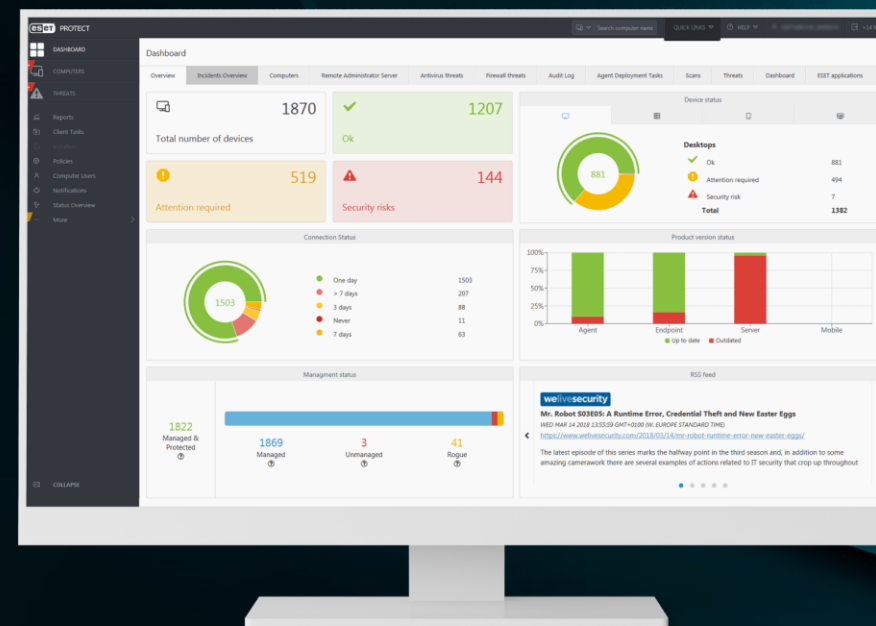


# ENDPOINT SECURITY

Viacvrstvová ochrana na všetkých platformách

# Vylepšenia v.9

- automatické aktualizácie
- notifikácie k EULA
- podpora Windows 11
- natívna podpora ARM64 architektúry



**eset** PROTECT



Reputácia  
a vyrovnávacia  
pamäť



Ransomware  
Shield



Pokročilá  
kontrola pamäte



Ochrana  
pred útokmi  
hrubou silou



Ochrana pred  
sieťovými  
útokmi

PRED ÚTOKOM



Správa  
zariadení

PO ÚTOKU



Ochrana  
LiveGrid®



Ochrana pred  
botnetmi



Exploit Blocker



Detekcia  
na úrovni DNA



Kontrola  
UEFI



Zabezpečený  
prehliadač



Híbková kontrola  
správania



Sandbox  
v rámci  
produktu

POČAS ÚTOKU



Kontrola skriptov  
a AMSI



Pokročilé  
strojové učenie

# Podporované operačné systémy

- Microsoft® Windows® 11
  - Microsoft® Windows® 10
  - Microsoft® Windows® 8.1
  - Microsoft® Windows® 8
  - Microsoft® Windows® 7 SP1 s najnovšími aktualizáciami \*
- 
- **Windows XP a Windows Vista už nie sú podporované**

# Viacúrovňové zabezpečenie







# LIVEGUARD ADVANCED

Proaktívna ochrana pred doposiaľ neznámymi  
a zero-day hrozbami



# ESET Dynamic Threat Defense LiveGuard Advanced

# Viacúrovňové zabezpečenie

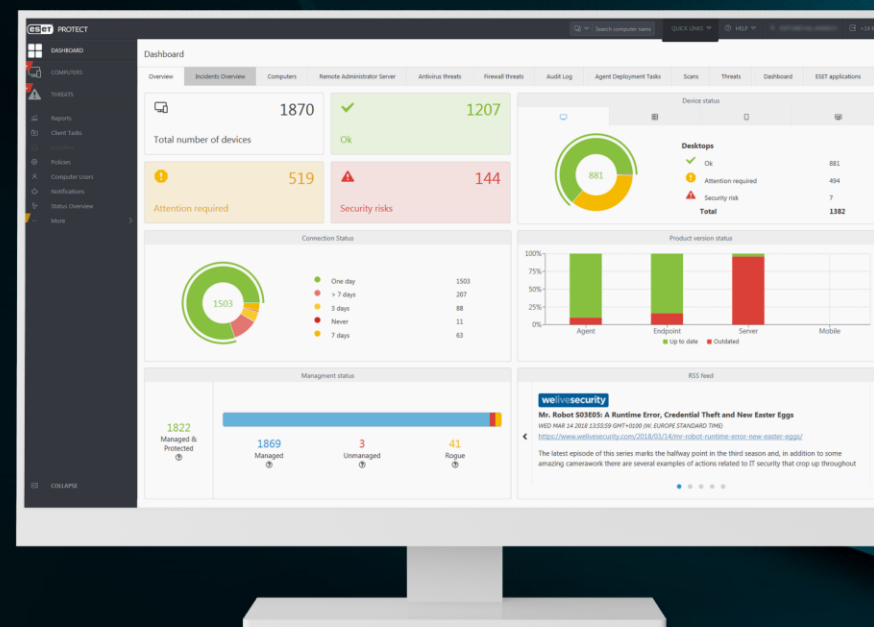


# **CLOUD OFFICE SECURITY**

Ochrana pre aplikácie služby Microsoft 365

# Novinky

- ESET Live Guard Advanced
- politiky Live Guard Advanced
- reporty o e-mailovej karanténe



# Viacúrovňové zabezpečenie



# ESET NISPEACE Enterprise Inspector

Prispôsobiteľné riešenie na detekciu  
a následnú reakciu na útoky na koncové zariadenia



# INSPECT CLOUD

# Vylepšenia ESET Inspect

- podpora Linux OS distribúcií
- intuitívnejšie možnosti reagovania na incident
- automatické výnimky (Questions view)
- ochrana prístupu na powershell terminál pomocou 2FA
- zjednotenie a konzistencia medzi konzolami ESET PROTECT and ESET Inspect
- MDR príznak incidentu
- popis Incidentu
- vyvolanie čistenia DB (on-prem)

# Viacúrovňové zabezpečenie



# ESET služby

## PROFESIONÁLNE SLUŽBY

---

- ✓ Riešenie problémov s ESET produktami
- ✓ Prioritná a garantovaná technická podpora (SLA)
- ✓ Inštalácia a konfigurácia ESET produktov
- ✓ Kontrola nastavení a odporúčania

## BEZPEČNOSTNÉ SLUŽBY

---

- ✓ Analýza podozrivých súborov
- ✓ Pomoc pri reakcii na malvérové incidenty
- ✓ Bezpečnostná podpora pre EDR
- ✓ Threat monitoring / Threat hunting

# ESET End of life / koniec životného cyklu

# End of Life cyklus





# EOL alebo Cut-off?

## EOL

- strata technickej podpory
- koniec vývoja
- nedostupnosť inštalátorov
- koniec aktualizácie modulov a DB

## Cut-off

- koniec aktualizácie modulov
- fázy cut-off procesu (Soft/Hard/Shut down)
- Paid Extended Support (PES) program
  - ESET Endpoint Security for Windows v.5
  - ESET Endpoint Antivirus for Windows v.5
  - ESET NOD32 Antivirus Business Edition v.4
  - ESET Smart Security Business Edition v.4
  - ESET Endpoint Security for Windows v.6.5 (on SHA-2)
  - ESET Endpoint Security for Windows v.6.5 (on SHA-1)
  - ESET Endpoint Security for Windows v.7.0-7.2



Shutting down

# EOL produkty pre rok 2022

- Endpoint Security + AV pre Windows v.8.0 → November 2022
- ESET Security Management Center v.7.1 → Jún 2022
- ESET Security Management Center v.7.2 → December 2022
- ESET Server security pre Windows v.6.5 → December 2022
- ESET Server security pre Windows v.7.0 / 7.2 → Jún 2022

# Verzia 6.5 a Windows XP

Verzia	Dátum vydania	Posledný build	Aktuálny stav	Plná podpora	Limitovaná podpora
6.5	May 14, 2017	6.5.2132.6	End of Life	Koniec	Koniec* (Február 28.2022)

• **SHA-1 systémy aktualizácie modulov 31. december 2022**

# Aktuálne informácie o EOL

The screenshot shows a Google search result for "Politika životného cyklu produktov určených pre firmy". The search bar contains "KB3" and "ESE". The search results include a link to "Riešenia ESET pre koncové zariadenia" and a dropdown menu showing "ESET Endpoint Antivirus". The main content is a table with columns: Version, Original Release Date, Latest build, Current Status, Full Support, and Limited Support. The table lists versions from 9.0 down to 6.6, with their respective release dates, latest builds, and support status (Full Support, Limited Support, or End of Life).

Politika životného cyklu produktov určených pre firmy

V nasledujúcom zozname kliknite na názov svojho produktu ESET a zobrazí sa úroveň podpory, ktorá je aktuálne pre produkt poskytovaná.

Riešenia ESET pre koncové zariadenia

▼ ESET Endpoint Antivirus

Version	Original Release Date	Latest build	Current Status	Full Support	Limited Support
9.0	November 30, 2021	9.0.2046.0	✓ Full Support	Until version 10 + 1 year	Until version 10 + 3 years
8.1	July 13, 2021	8.1.2037.9	✓ Full Support	Until November 30, 2022	Until November 30, 2024
8.0	December 9, 2020	8.0.2039.3	⚠ Limited Support	Ended (June 28, 2021)	Until November 30, 2022
7.3	June 30, 2020	7.3.2055.0	✓ Full Support	Until December 2022	Until December 2023
7.2	November 12, 2019	7.2.2072.0	⚠ End of Life	Ended	Ended (December 31, 2021)
7.1	April 11, 2019	7.1.2064.0	⚠ End of Life	Ended	Ended (December 31, 2021)
7.0	August 16, 2018	7.0.2120.0	⚠ End of Life	Ended	Ended (December 31, 2021)
6.6	August 24, 2017	6.6.2095.1	⚠ End of Life	Ended	Ended (March 31, 2021)

# Čo sa peče v najbližšom období

- ESA Cloud
- Vulnerability and Patch management
- Enterprise Integrations
- ESET Inspect integračný framework s API



30

rokov úplnej  
nezávislosti  
a inovácií

Jedna z mála súkromných celosvetových spoločností  
zameraných na IT bezpečnosť

Ďakujem za pozornosť!