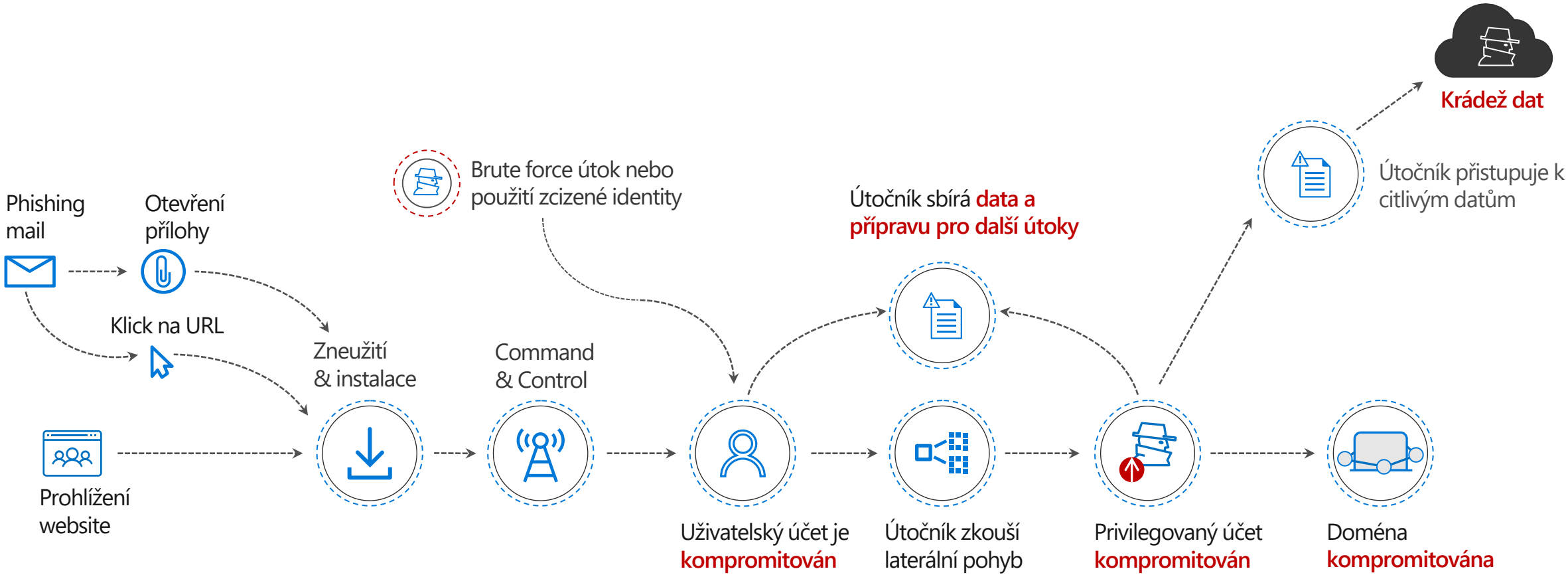
Moderní kybernetická bezpečnost potřebuje data a signály

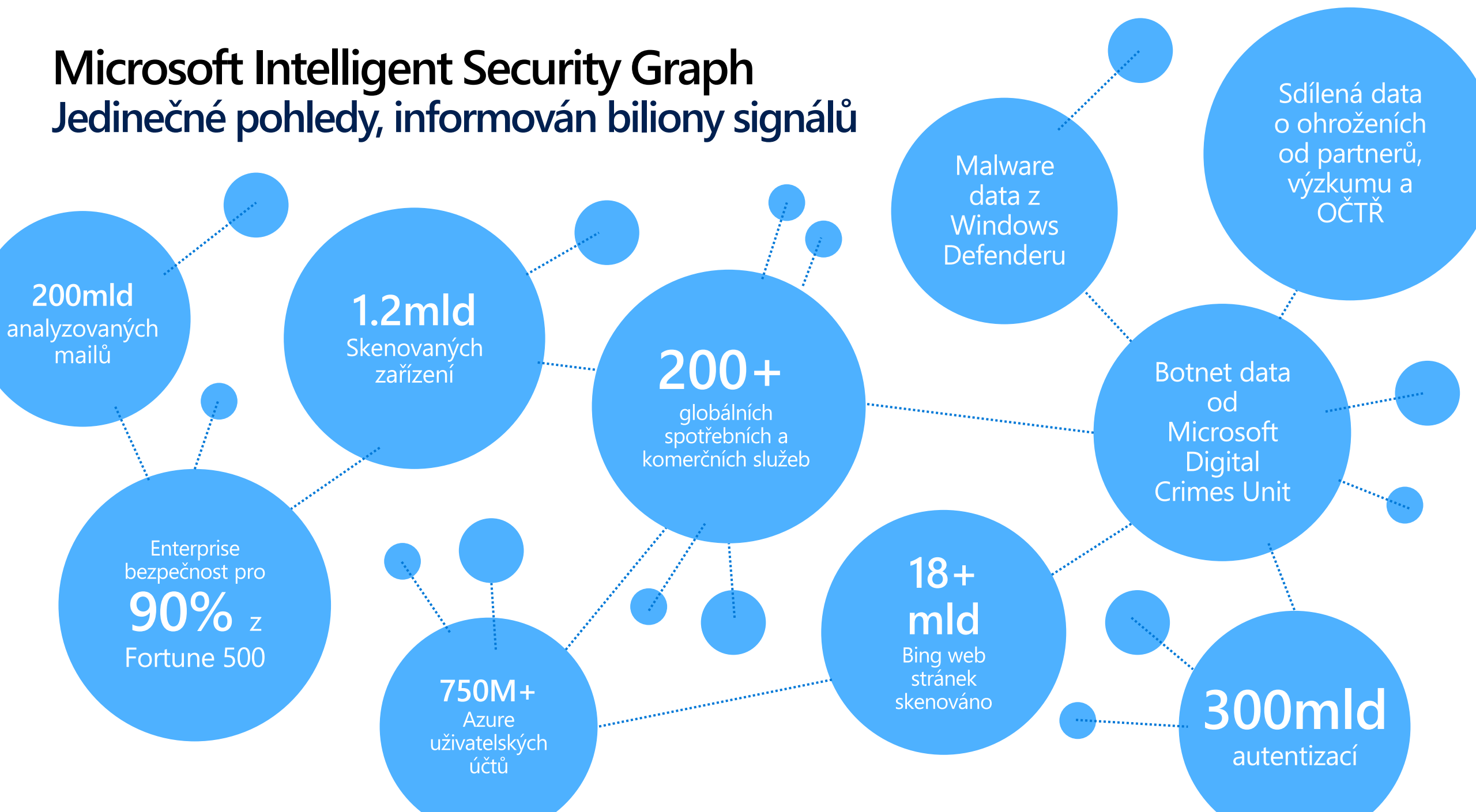
Dalibor Kačmář
dalibor.kacmar@microsoft.com
National Technology Officer
Microsoft

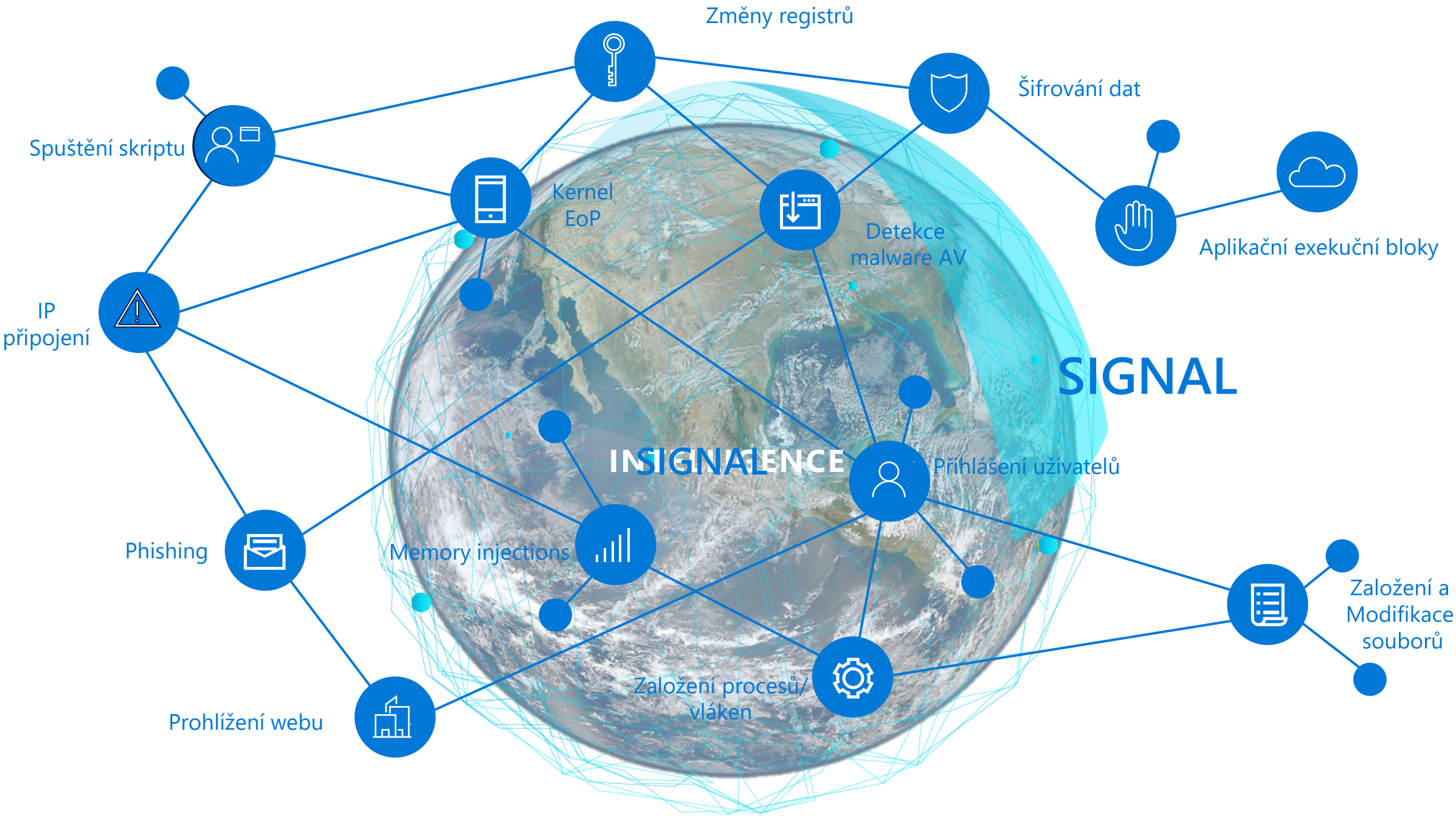
Maximální detekce během fází útoku



Microsoft Intelligent Security Graph

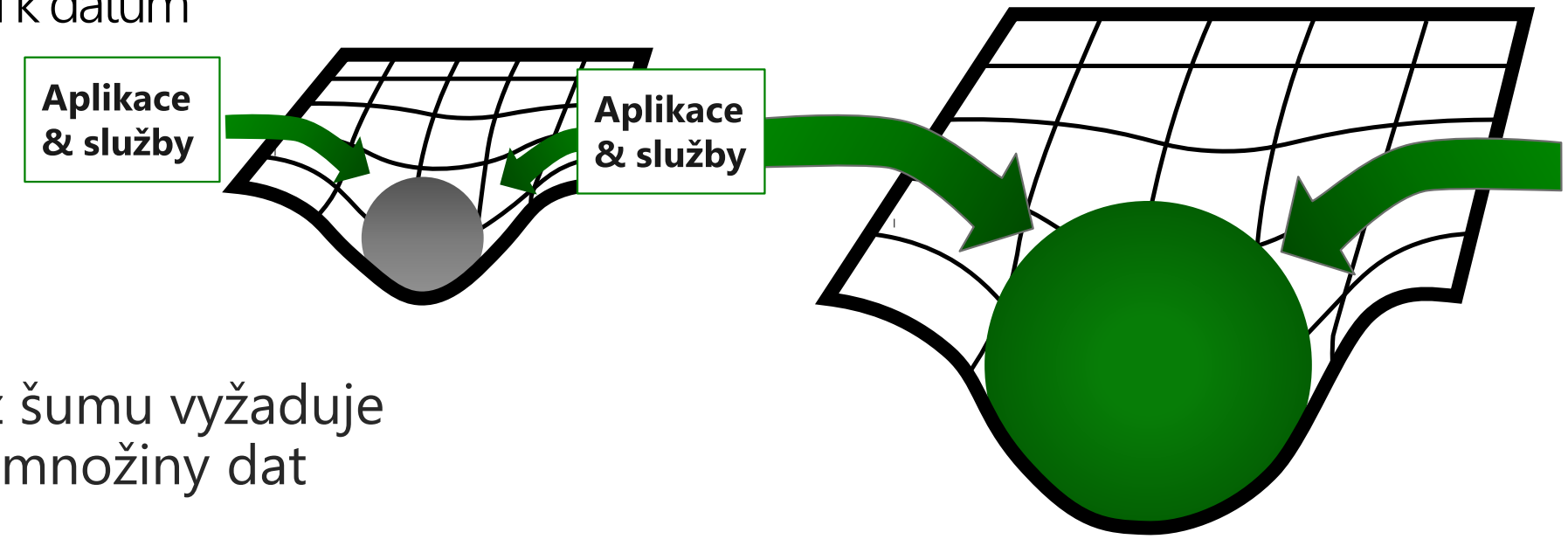
Jedinečné pohledy, informován biliony signálů




Změny registrů
Šifrování dat
Spuštění skriptu
Kernel
EoP
Detekce
malware AV
Aplikační exekuční bloky
IP
připojení
SIGNAL
INSIGNALENCE
Přihlášení uživatelů
Phishing
Memory injections
Založení a
Modifikace
souborů
Založení procesů/
vláken
Prohlížení webu

Přitažlivost dat

Přitahuje analytiku k datům



Získání signálu z šumu vyžaduje kontext z široké množiny dat

Nelze kopírovat všechna potřebná data z jedné lokace z důvodu šířky pásma

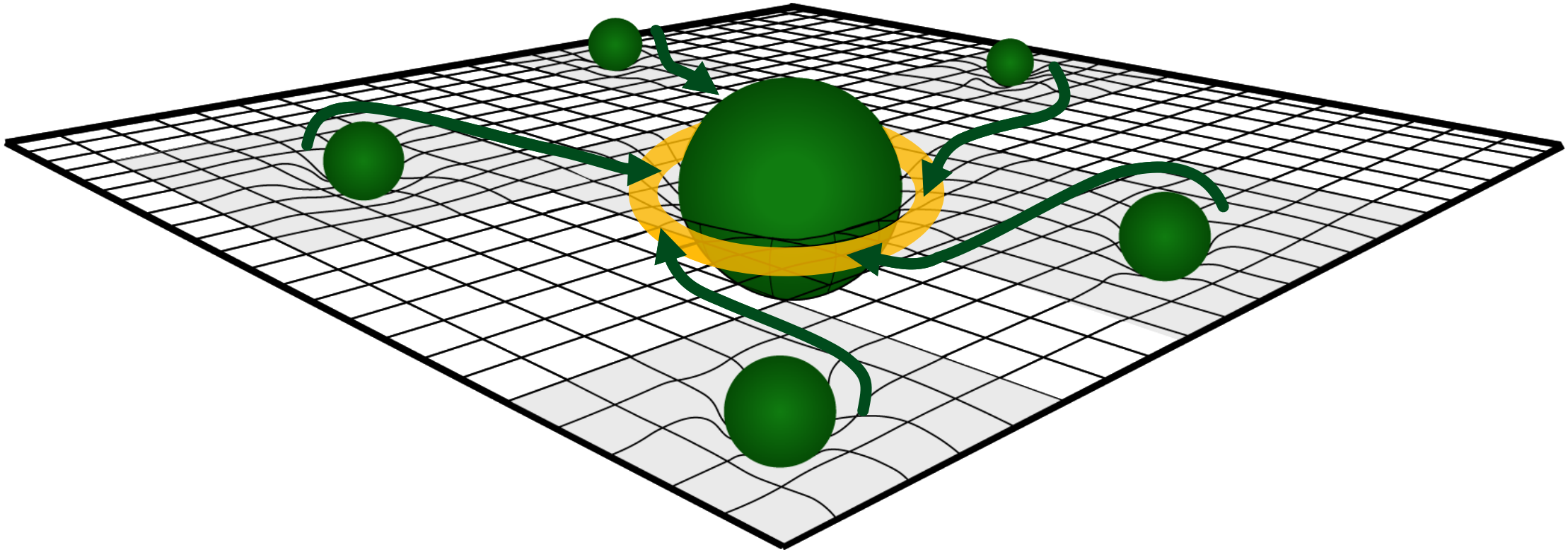
→ Musíme použít analytiku místně a centrálně integrovat

Data Gravity

$$\frac{\left(\text{Data Mass} \times \text{Application Mass}\right) \times \text{Number of Requests per second}}{\left(\text{Latency in seconds} + \left(\text{Average Request Size in MBs} \,/\, \text{Bandwidth in MBs per second}\right)\right)^2}$$

Racionalizace SOC signálů

SOCs pracují dnes s mnoha datovými zdroji

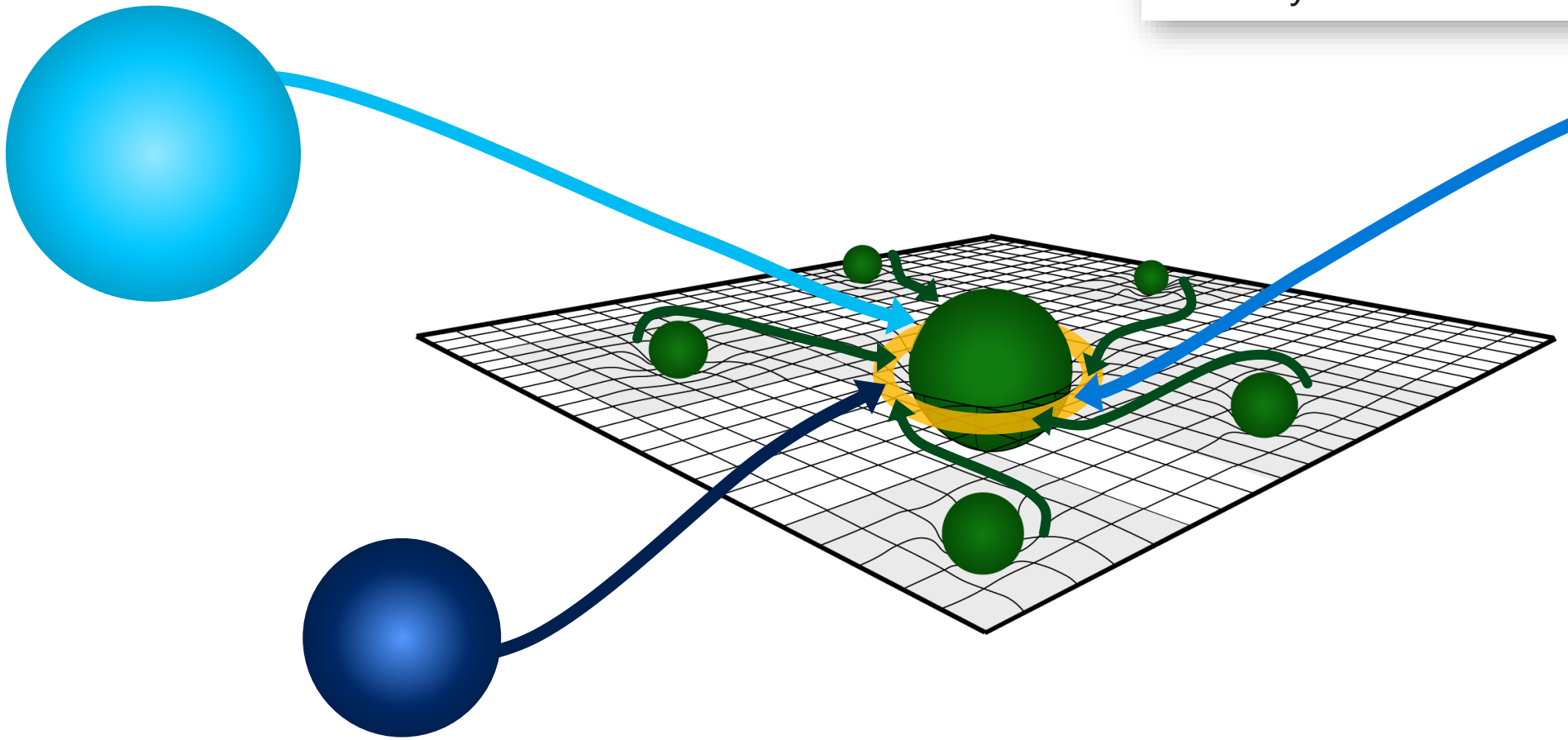


Microsoft Graph Security API umožňuje analytikům získat pohledy napříč lokálními bezpečnostními sadami dat

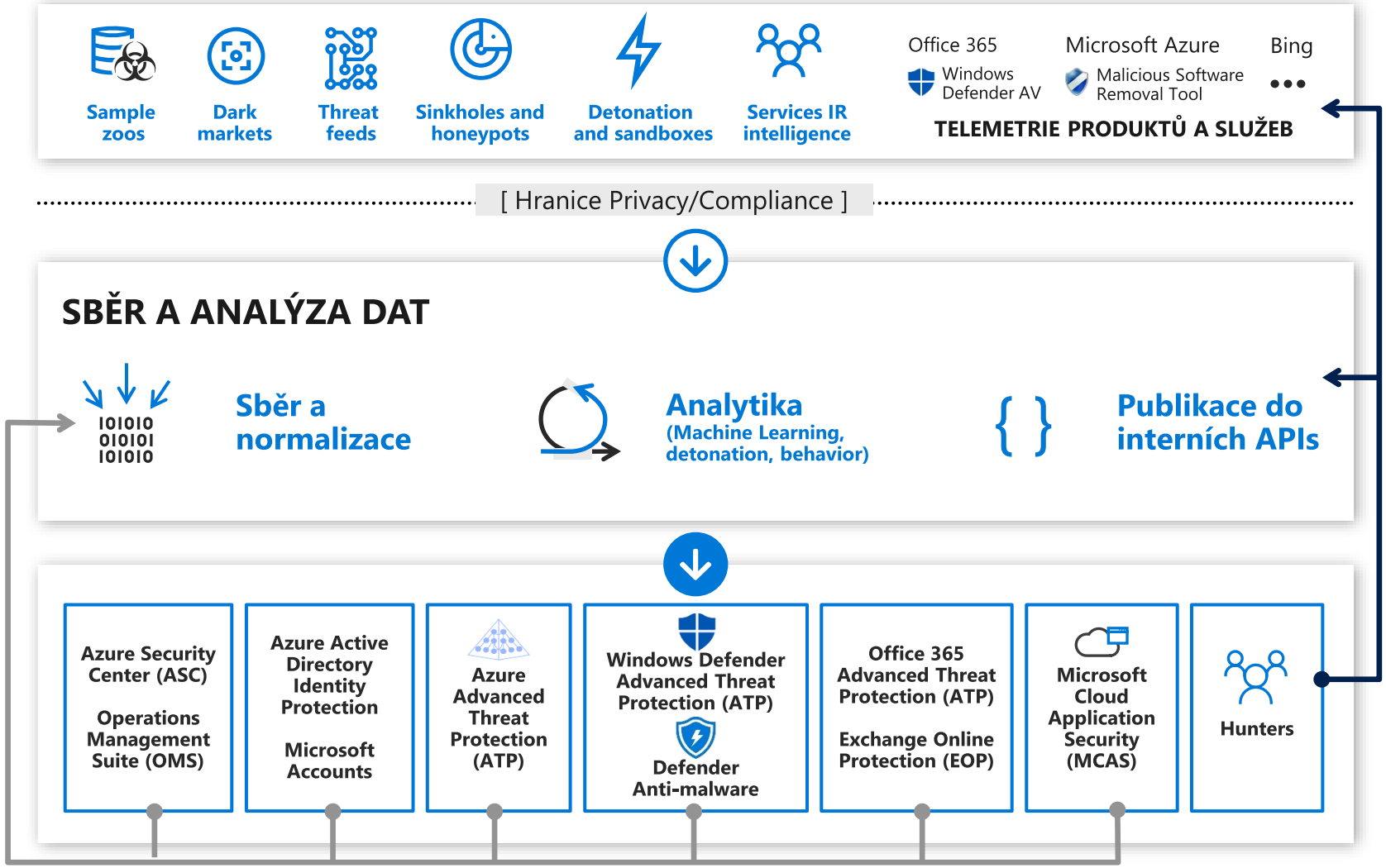
Graph Security API – unifikace signálů

Umožňuje analytikům získat pohledy a kontext napříč
- Lokálními daty a
- Bezpečnostními daty hostovanými v cloudu

Microsoft's Intelligent Security Graph
Masivní datová sada + analytika dávají možnosti Microsoftu dobře detekovat hrozby



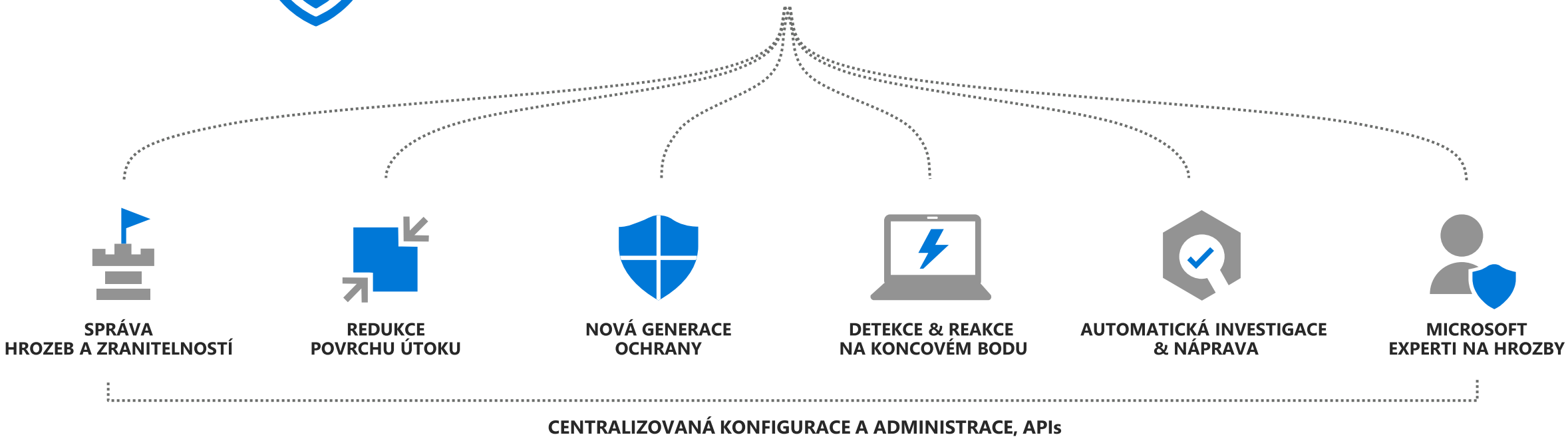
Od signálu k inteligenci:
Uvnitř *Microsoft Intelligent Security Graph*



- Produkty vytvořené se striktními privacy/compliance standardy
  Viz Microsoft Trust Center
- Analytika napomáhá k nových odhalením
- Produkty odesílají data do grafu
- Produkty používají Interflow APIs pro přístup k výsledkům
- Produkty generují data, zaváděná zpět do grafu
- Hunters identifikují útoky, vylepšují analytiku a poskytují zpětnou vazbu do návrhu produktu

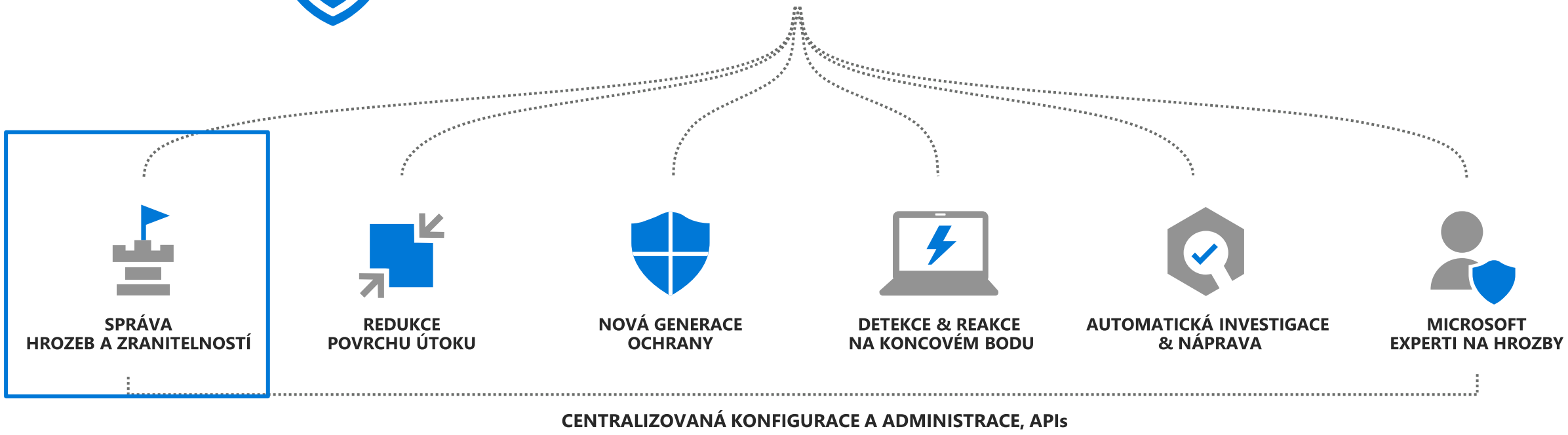
Microsoft Defender
Advanced Threat Protection

Integrovaný. Postaven s cloudem.



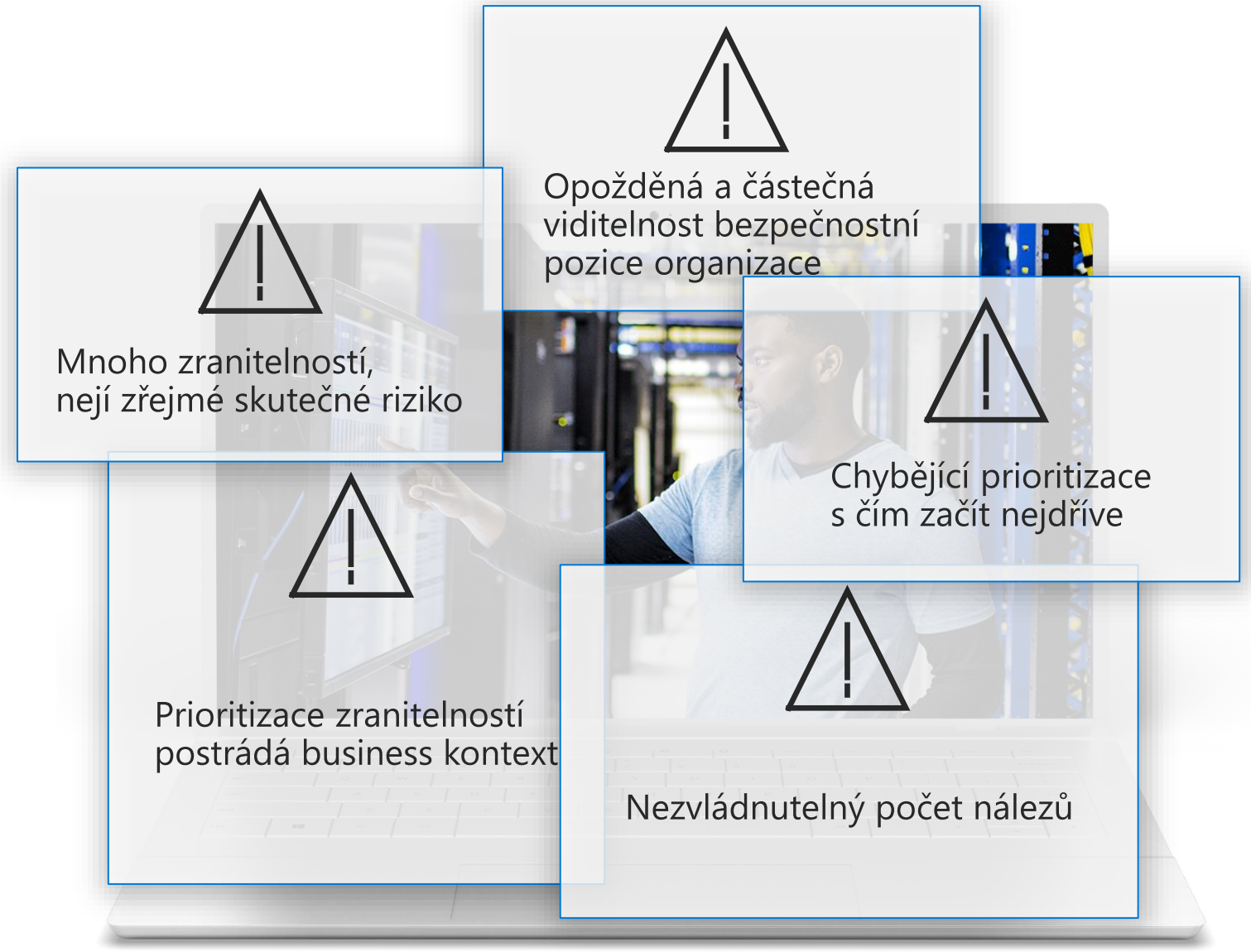
Microsoft Defender
Advanced Threat Protection

Integrovaný. Postaven s cloudem.



Potřeba správy hrozeb a zranitelností

OFF



Nová generace správy hrozeb & zranitelností

Správa zranitelností už není jen skenování

Detekce

Kontinuální detekce

zranitelných aplikací a konfigurací monitoringem koncových bodů pro okamžitou znalost situace

Prioritizace

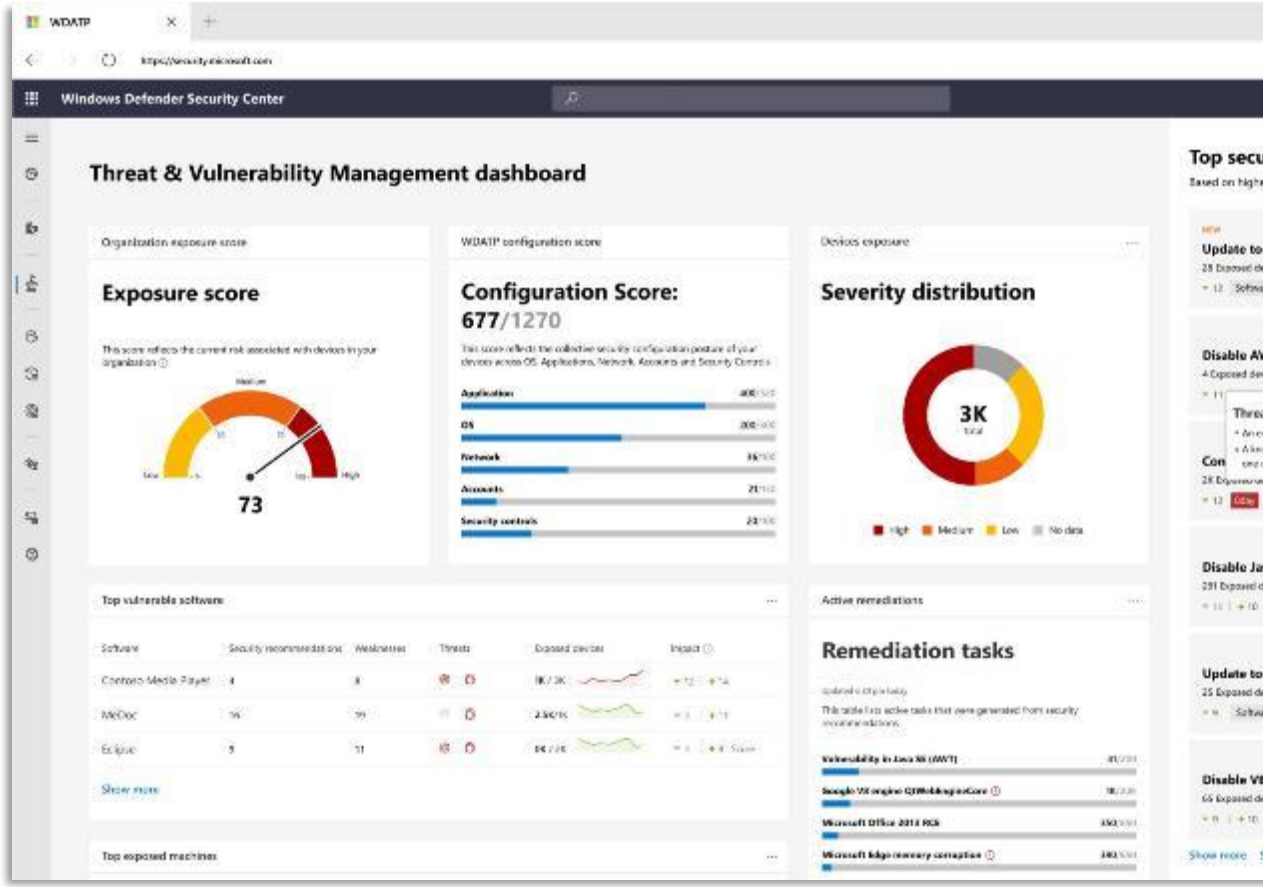
Kontextově řízená prioritizace

Nálezy obohacené o informace o hrozbách, business kontextu a skupinové znalosti pro vytvoření přesného reportu rizik

Mitigace

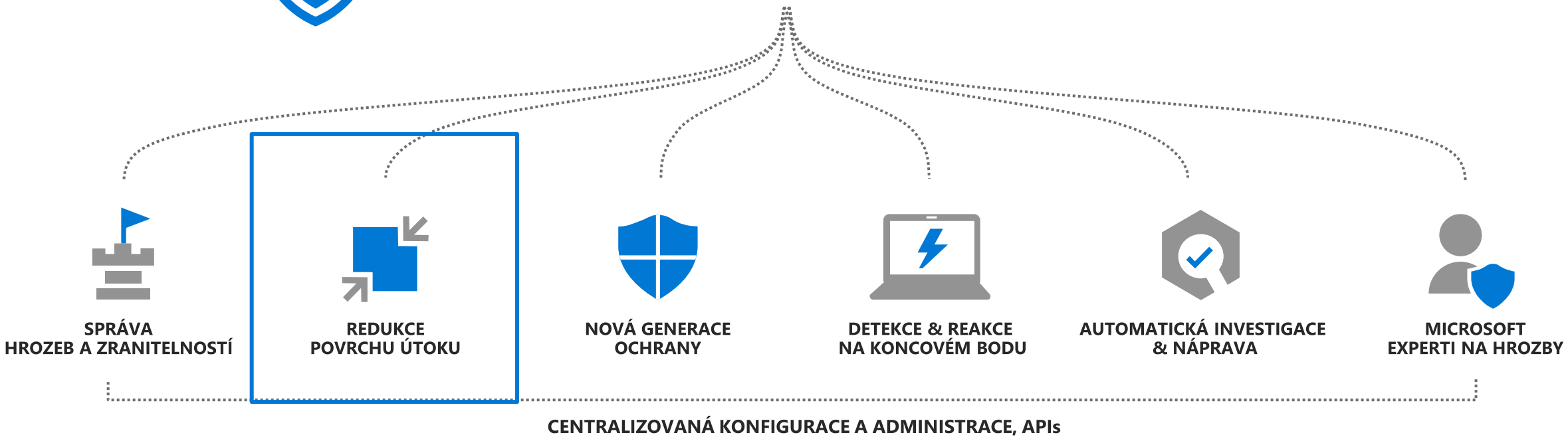
Přesná mitigace & automatické opravy

hrozeb pomocí přizpůsobeného plánu postaveném na organizačním riziku s využitím bezpečnostních řešení Microsoftu a partnerů



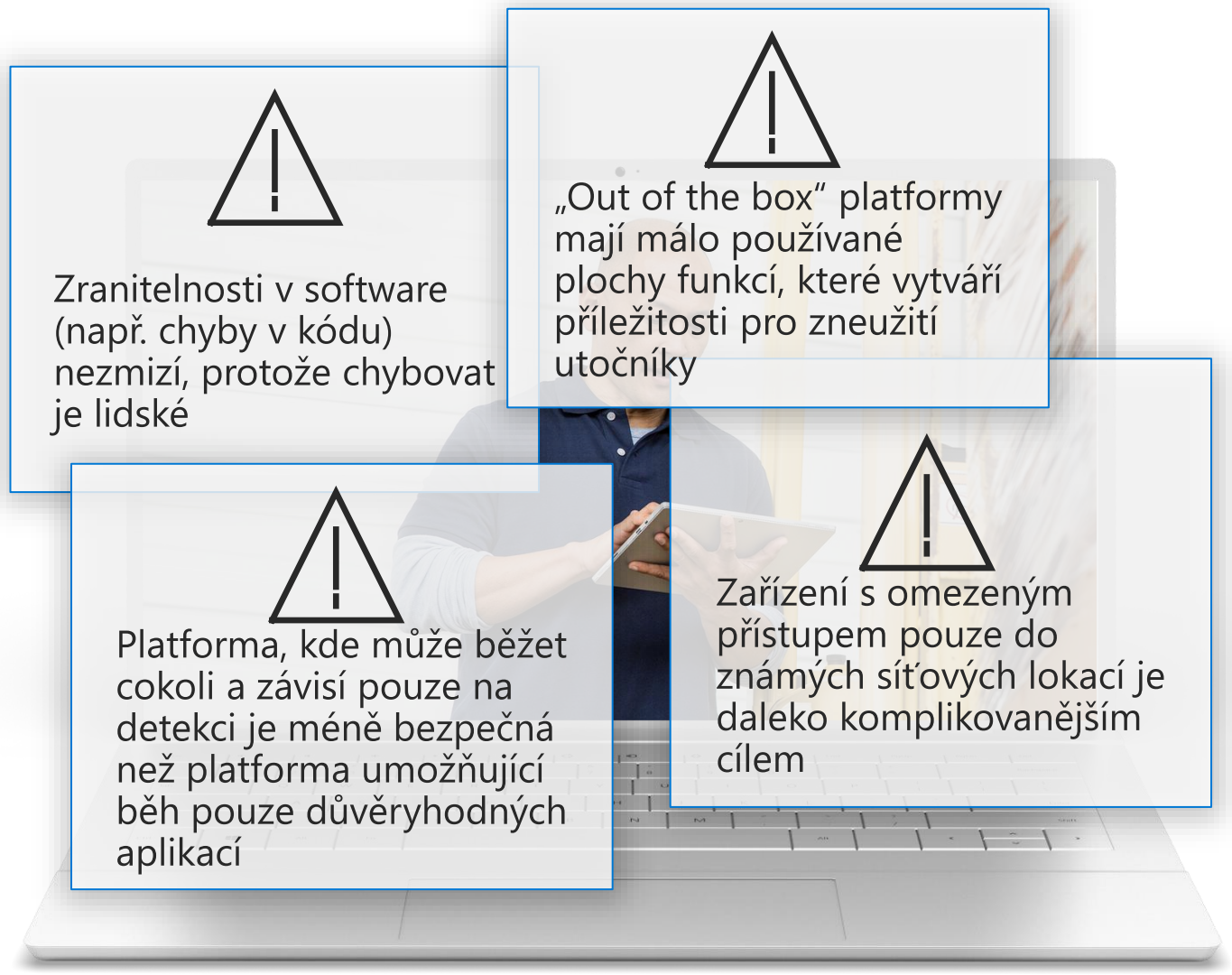
Microsoft Defender
Advanced Threat Protection

Integrovaný. Postaven s cloudem.



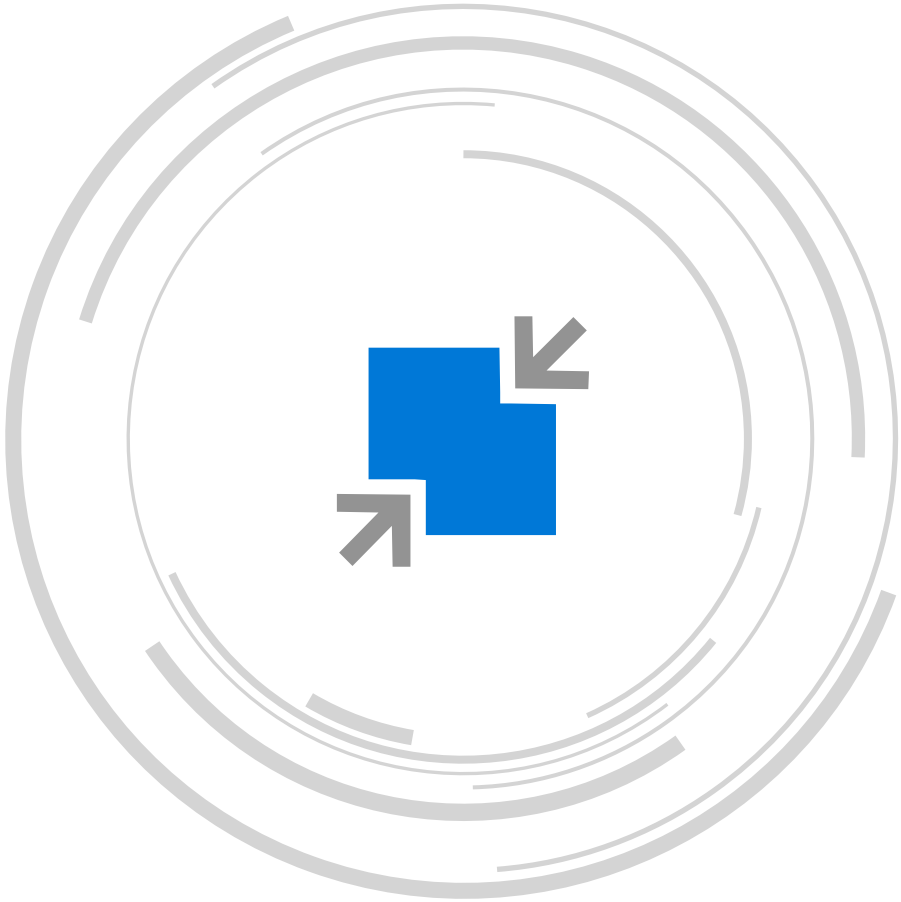
Potřeba pro redukci povrchu útoku

OFF



Redukce povrchu útoku

Odolání útokům a zneužití



HW ŘÍZENÁ IZOLACE

ŘÍZENÍ APLIKACÍ

OCHRANA PŘED ZNEUŽITÍM

OCHRANA SÍTÍ

ŘÍZENÝ PŘÍSTUP K ADRESÁŘŮM

Izolace přístupu k nedůvěryhodným webům

Izolace přístupu k nedůvěryhodným Office souborům

Prevence průniku do hostitele

Mitigace známých zneužití

Ochrana souborů před ransomware

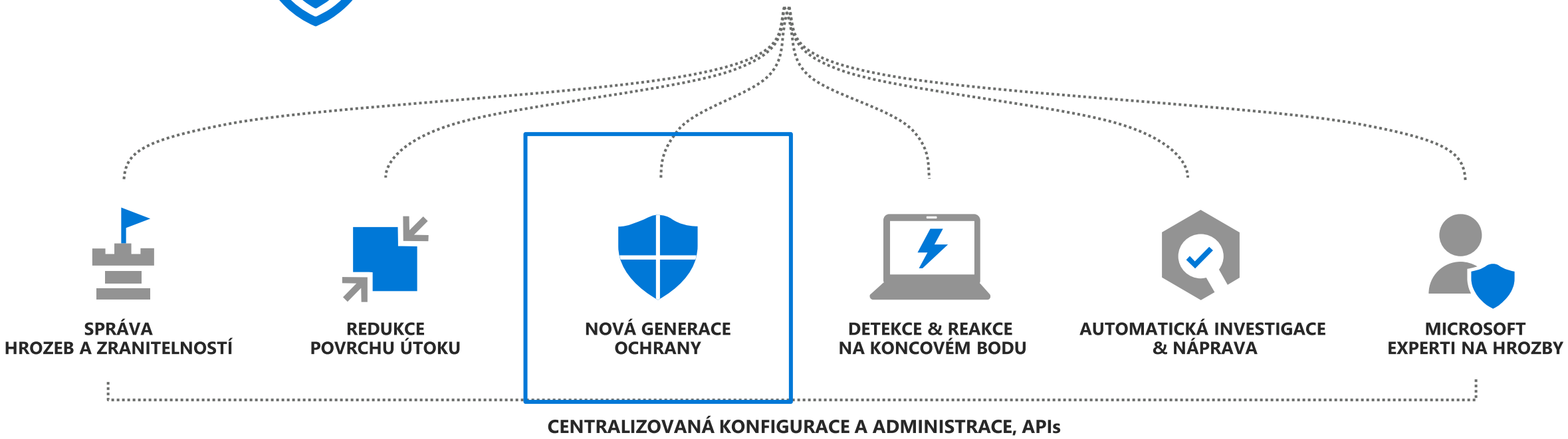
Blokování komunikace do destinací s nízkou reputací

Ochrana historických aplikací

Povolení běhu pouze důvěryhodných aplikací

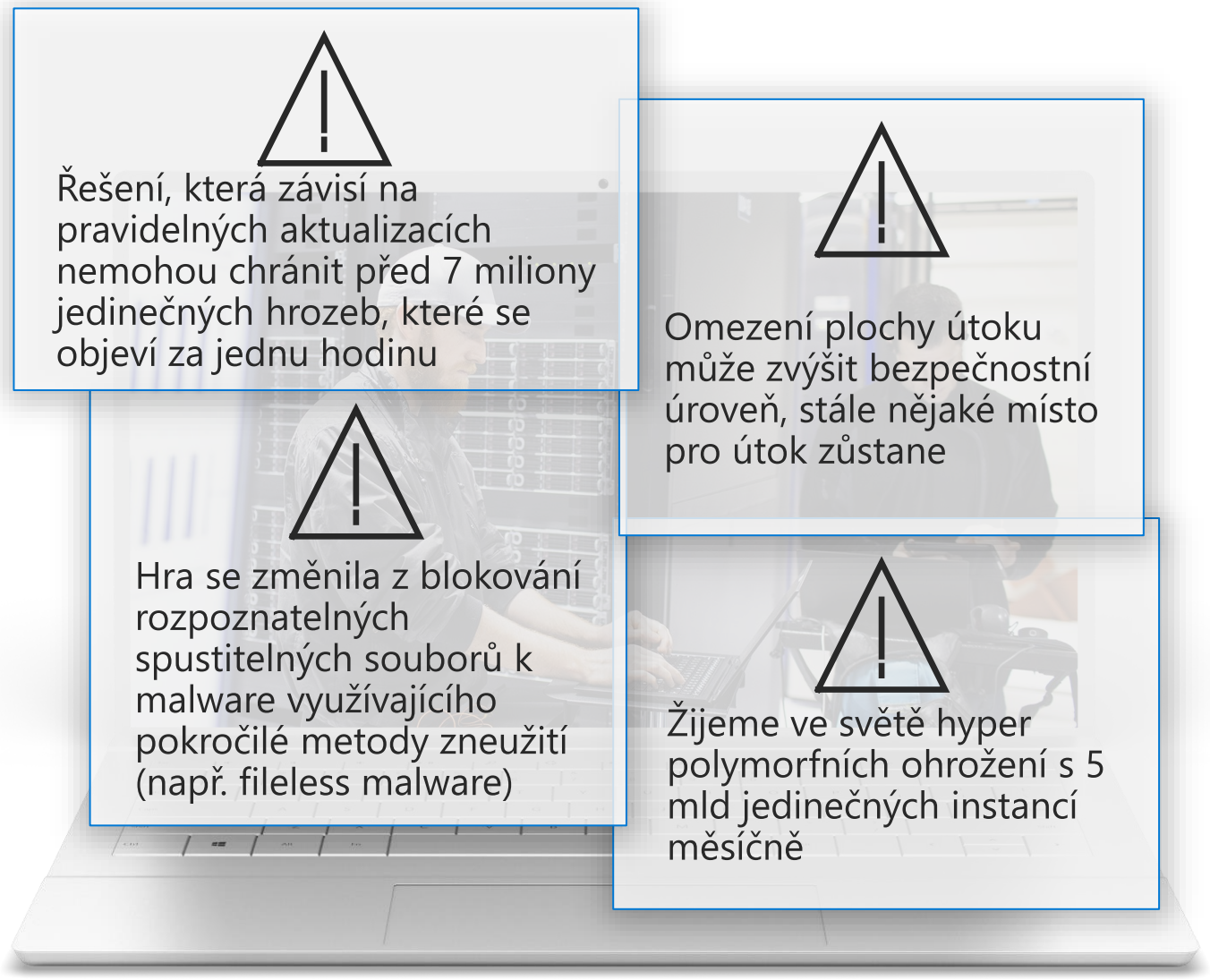
Microsoft Defender
Advanced Threat Protection

Integrovaný. Postaven s cloudem.

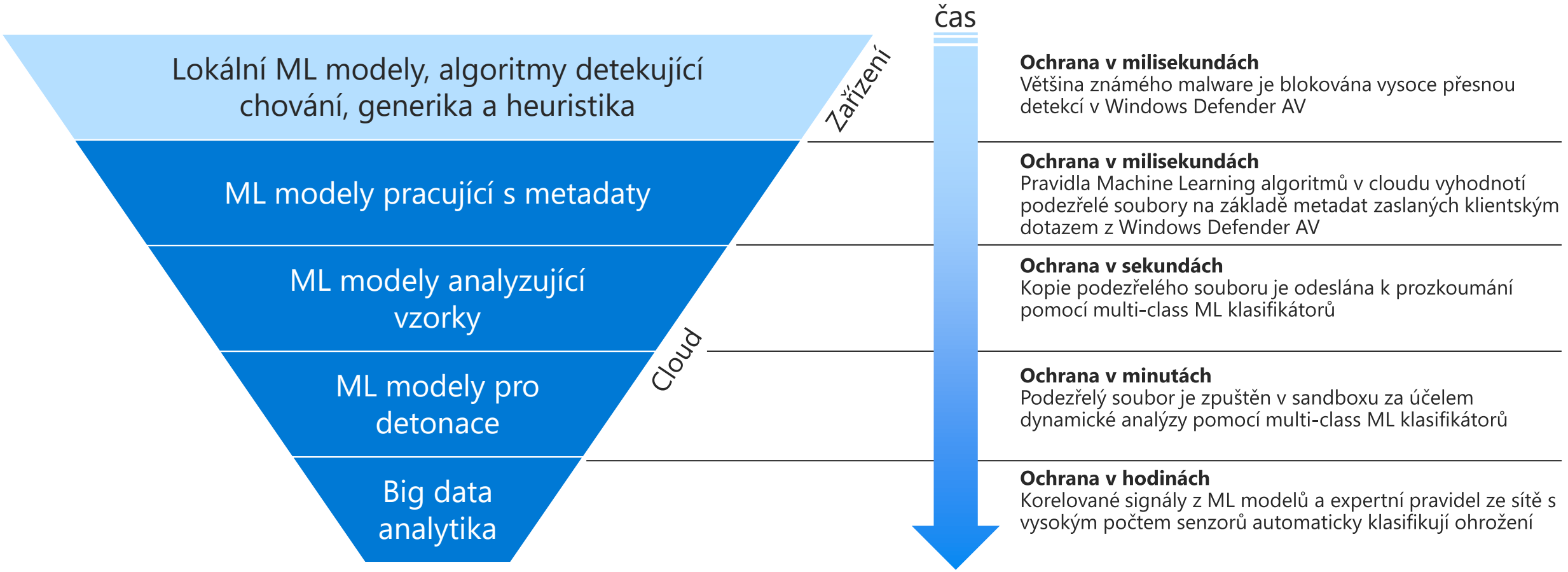


Potřeba nové generace ochrany

OFF

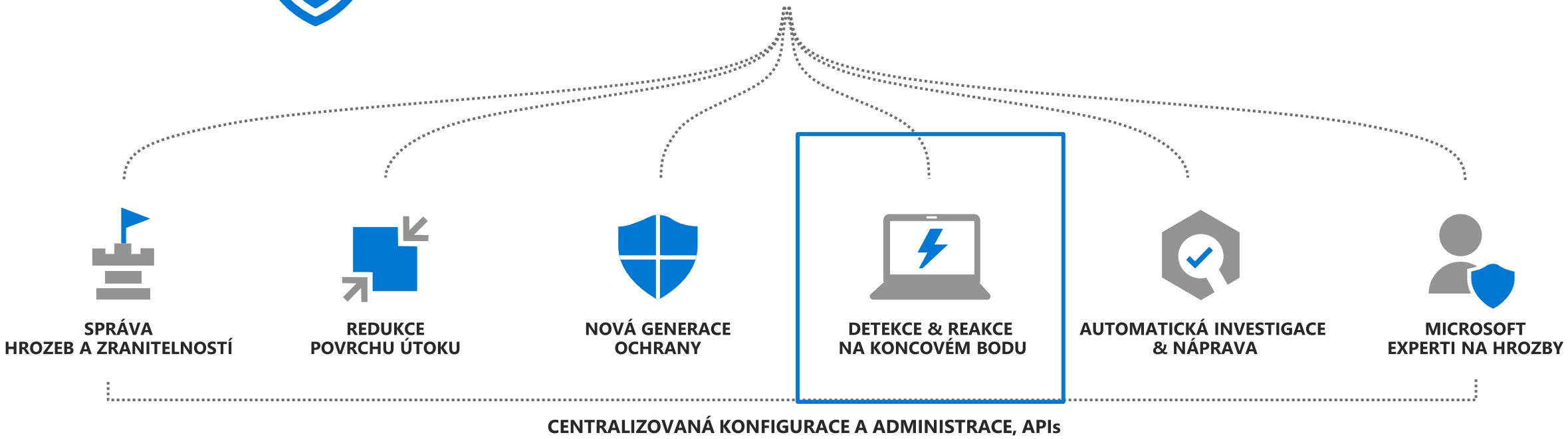


Nová generace ochrany: klientské zařízení + cloud



Microsoft Defender
Advanced Threat Protection

Integrovaný. Postaven s cloudem.



Potřeba pro detekci a reakci na koncovém bodu

OFF

CVE – Common Vulnerabilities and Exposures

AET – Advanced Evasion Technique

Detekce & reakce na koncovém bodu

Detekce. Vyšetření.
Odpověď na pokročilé útoky.

Klient

Záznamový senzor hluboce v OS

Cloud

Machine learning, detekce chování & anomálií

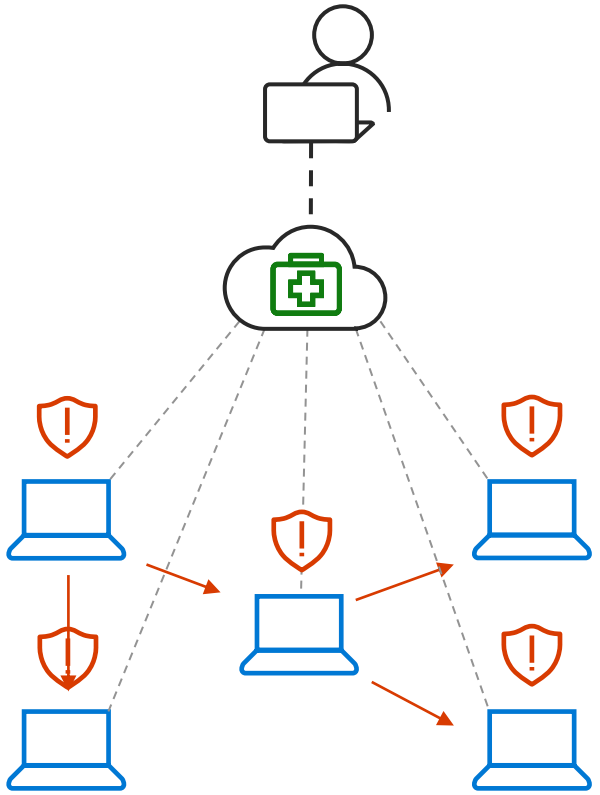
Reakce a omezení šíření

Sandbox analýza

Široké vyšetřování napříč stroji, soubory, uživateli, IPs, URLs

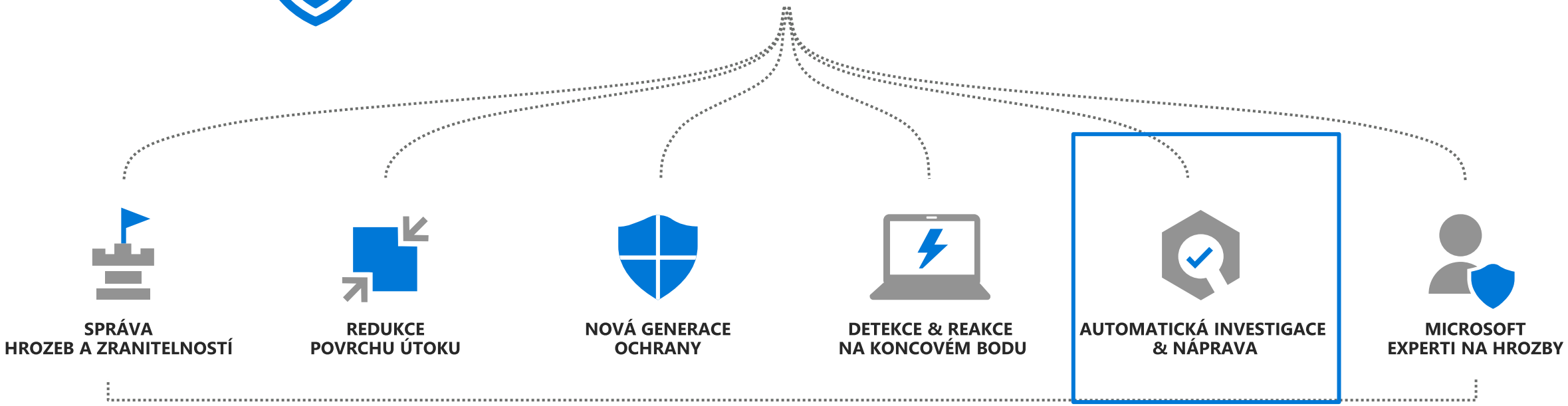
Historický a real-time threat hunting

Threat intelligence a přizpůsobitelné detekce



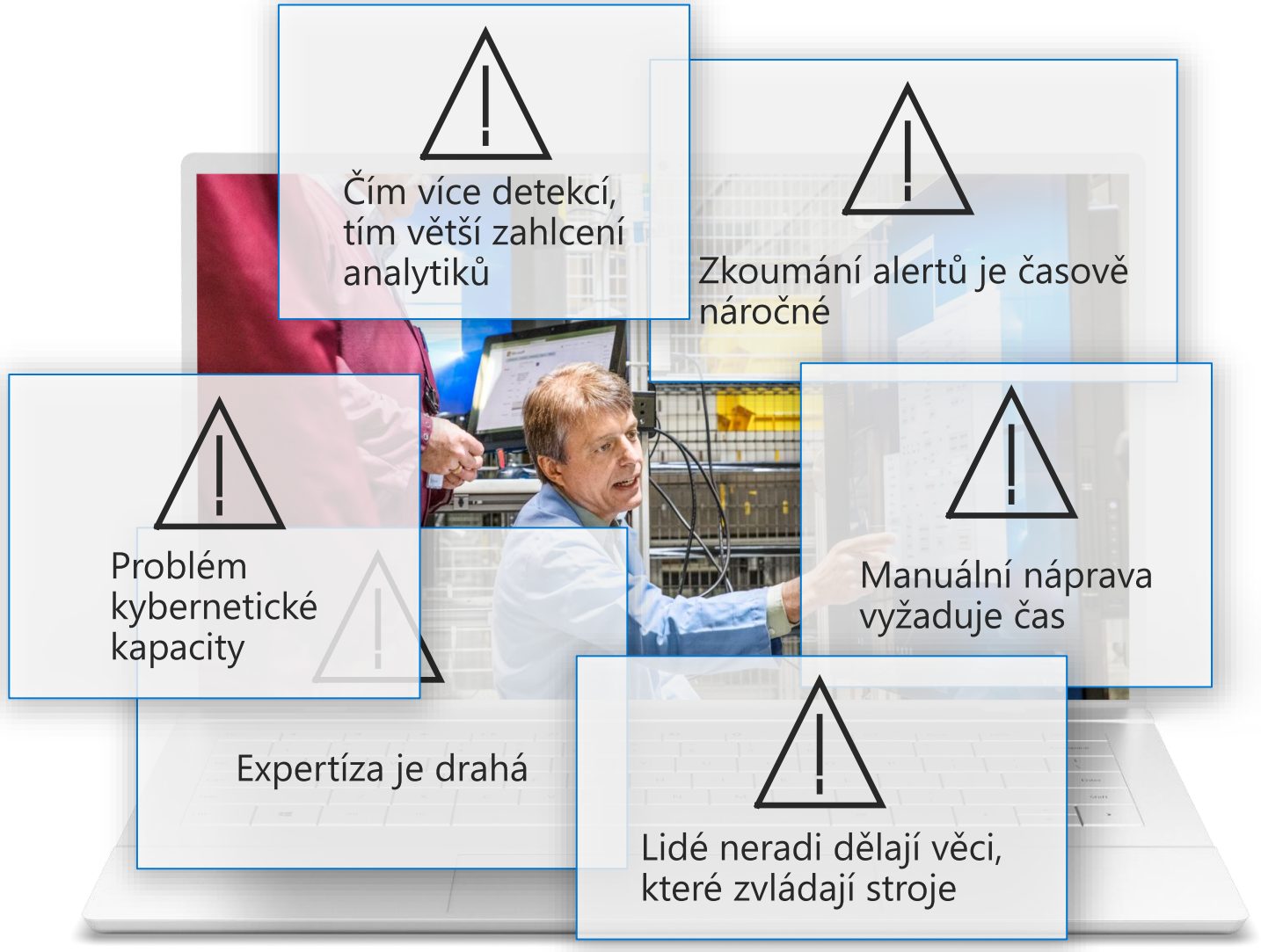
Microsoft Defender
Advanced Threat Protection

Integrovaný. Postaven s cloudem.



Potřeba automatizace

OFF



Automatické vyšetřování & náprava

Od alertu k nápravě v řádu minut

Klient

Forensic collector

Response orchestrator

Cloud

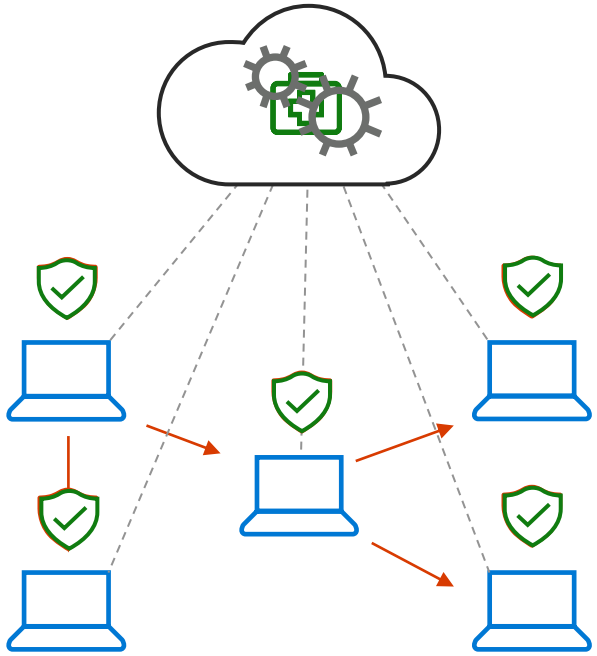
Historical endpoint data

Response orchestration

AI-based response playbooks

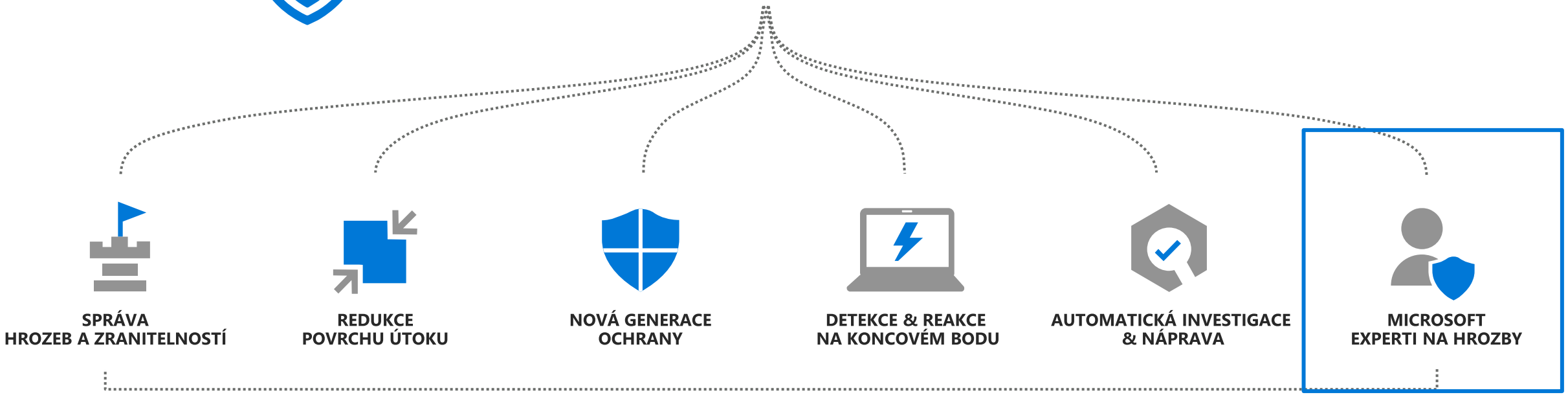
File/IP reputation

Sandbox



Microsoft Defender
Advanced Threat Protection

Integrovaný. Postaven s cloudem.



Potřeby pro řízený Hunting

OFF

Managed Threat Hunting Service

Další vrstva pohledu a analytiky pro zajištění, že hrozby nezůstanou nepovšimnuty

Nepřehlédněte prolomení

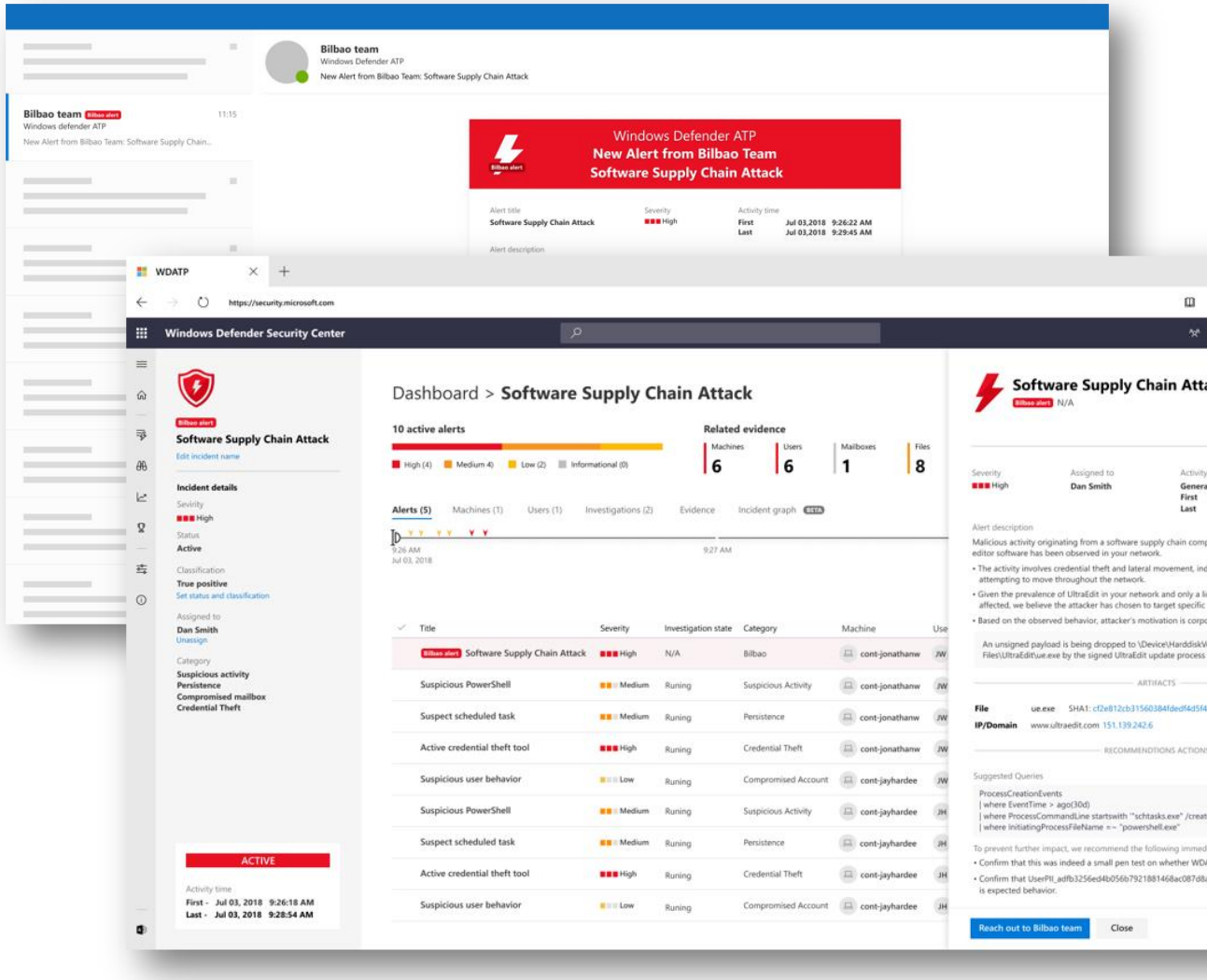
Jistěte si záda

Microsoft experti na hrozby proaktivně hledají anomálie nebi známá škodlivá chování ve vašem jedinečném prostředí.

Experti podle potřeby

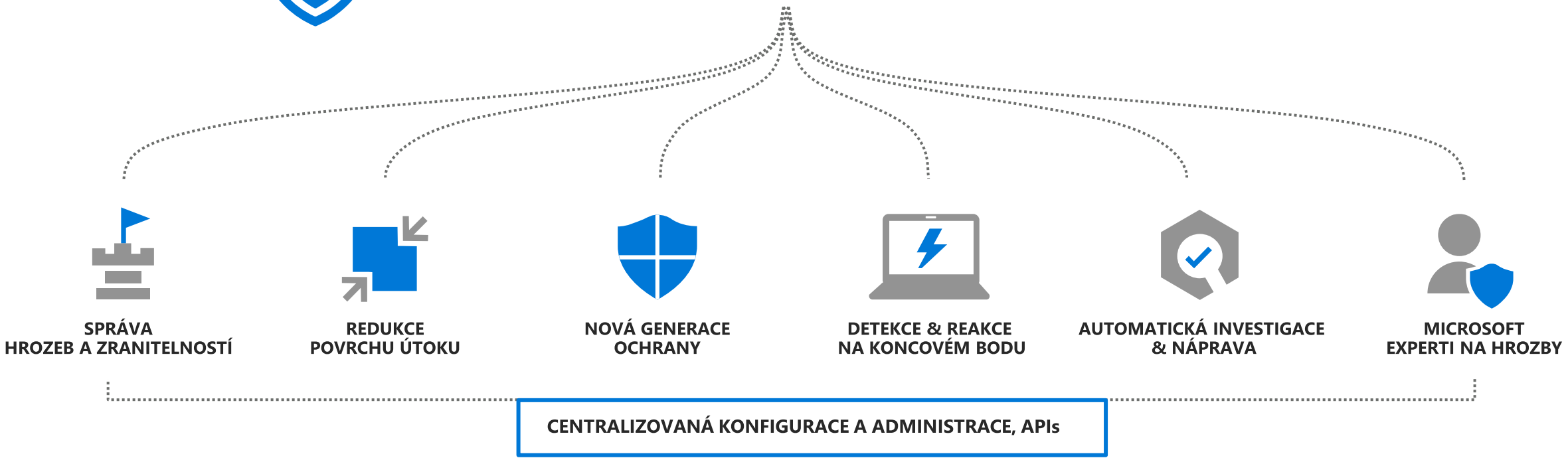
Světová třída expertů

Potřebujete poradit s alertem,malware nebo kontextem hrozby? Zeptejte se zkušených Microsoft expertů.



Microsoft Defender
Advanced Threat Protection

Integrovaný. Postaven s cloudem.



Potřeby pro správu bezpečnosti

OFF

Windows Defender ATP- Security management

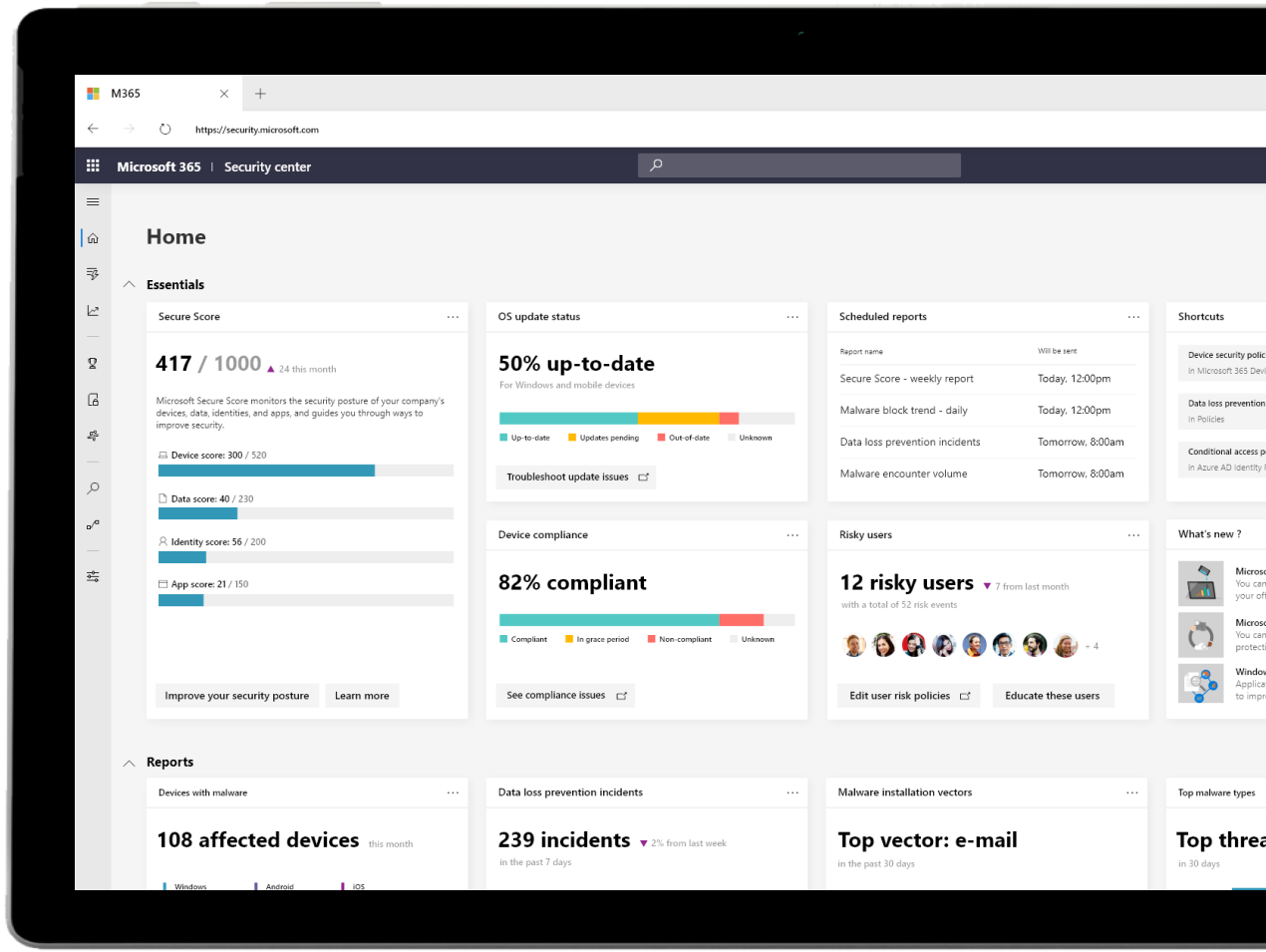
Rozumí tomu, co se děje, co se stalo a připraví vás pro budoucnost

Dashboardy a trendy

Monitorování hrozeb

Reporting hrozeb

Správa konfigurací



M365

https://security.microsoft.com

Microsoft 365 Security

Edit sections | Add cards

Detection

Active Incidents

27 active incidents Updated 6:20 pm today

High (4) | Medium (16) | Low (7)

Incident name	Severity	Last activity
Golden ticket compromise	High	June 18, 2018 11:12 AM
Phishing email campaign detected	High	June 18, 2018 11:10 AM
Suspicious PowerShell Activity	High	June 18, 2018 11:07 AM
Phishing email campaign detected	High	June 18, 2018 10:56 AM
Insider threat identified – sensitive data	Medium	June 18, 2018 10:52 AM
Potential Dofoil activity – malicious C2	Medium	June 18, 2018 10:50 AM
Windows Defender AV detected an active 'Azden' malware	Medium	June 18, 2018 11:12 AM
Windows Defender AV detected 'Reimage' unwanted software	Medium	June 18, 2018 11:11 AM

Show more

Identity protection

Users with threat detections

Updated 6:20 pm today

User	Alerts
Jesse Wallin	56
Robin Goolsby	45
Eva Macias	32
Jonathan Wolcott	27
Rex Fredrickson	16
Donovan Eagle	15
Jess Passmore	8
Antoine Hindman	4
Wayne Wallin	2

Show more

Device protection

34 devices at risk / 1,254

Updated 6:20 pm today

Device	Risk score
RDP_SRV_10	High
RDP_SRV_5	High
FIN_SRV_HQ	High
DC_SRV_US	High
cont-evamacias	High
cont-jonathanwolcott	High
cont-jesswallin	Medium
RDP_SRV_25	Medium
RDP_SRV_25	Medium

See more

Email protection

12 email accounts at risk /1,022

Updated 6:20 pm today

Email account	User

Device threat analytics

Assess your defenses against high-profile threats

Updated 6:20 pm today

Get interactive reports on Windows Defender ATP about emerging threats

Spectre and Meltdown	23 active/132
Advanced Trojan Outbreak	16 active/182
NotPetya	13 active/254

Threat News

"BadKitten" - New threat in town
Check organization vulnerability

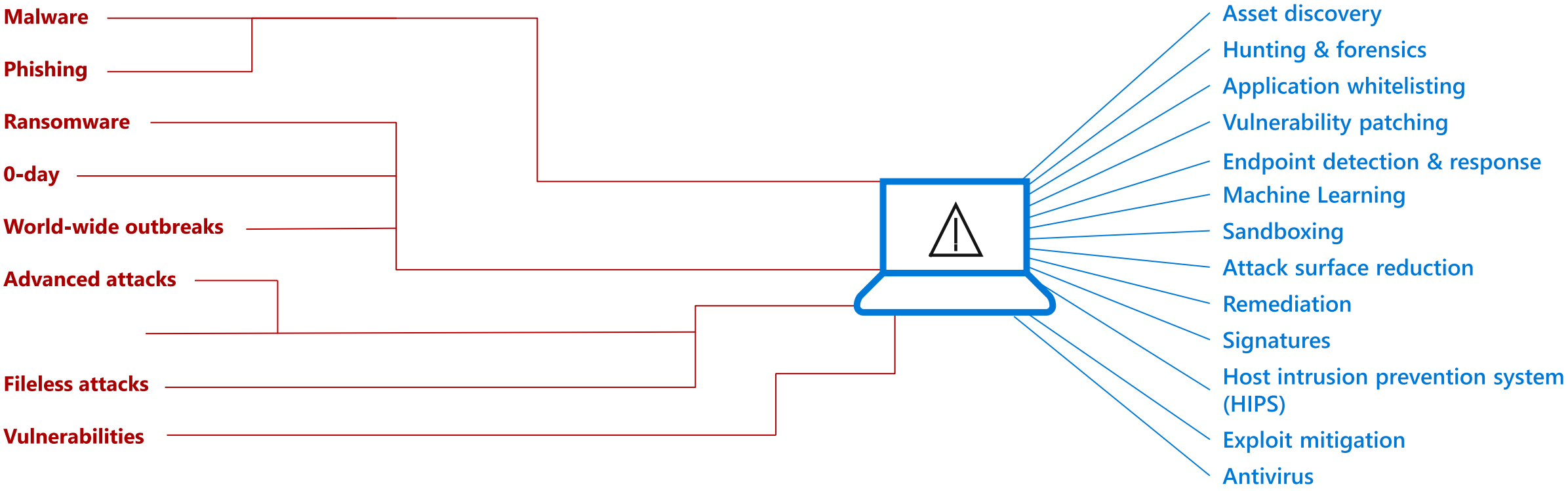
Start hunting!
GitHub shared new query

Ochrana koncového bodu je složitá

VÝKON
Dopad na koncové body

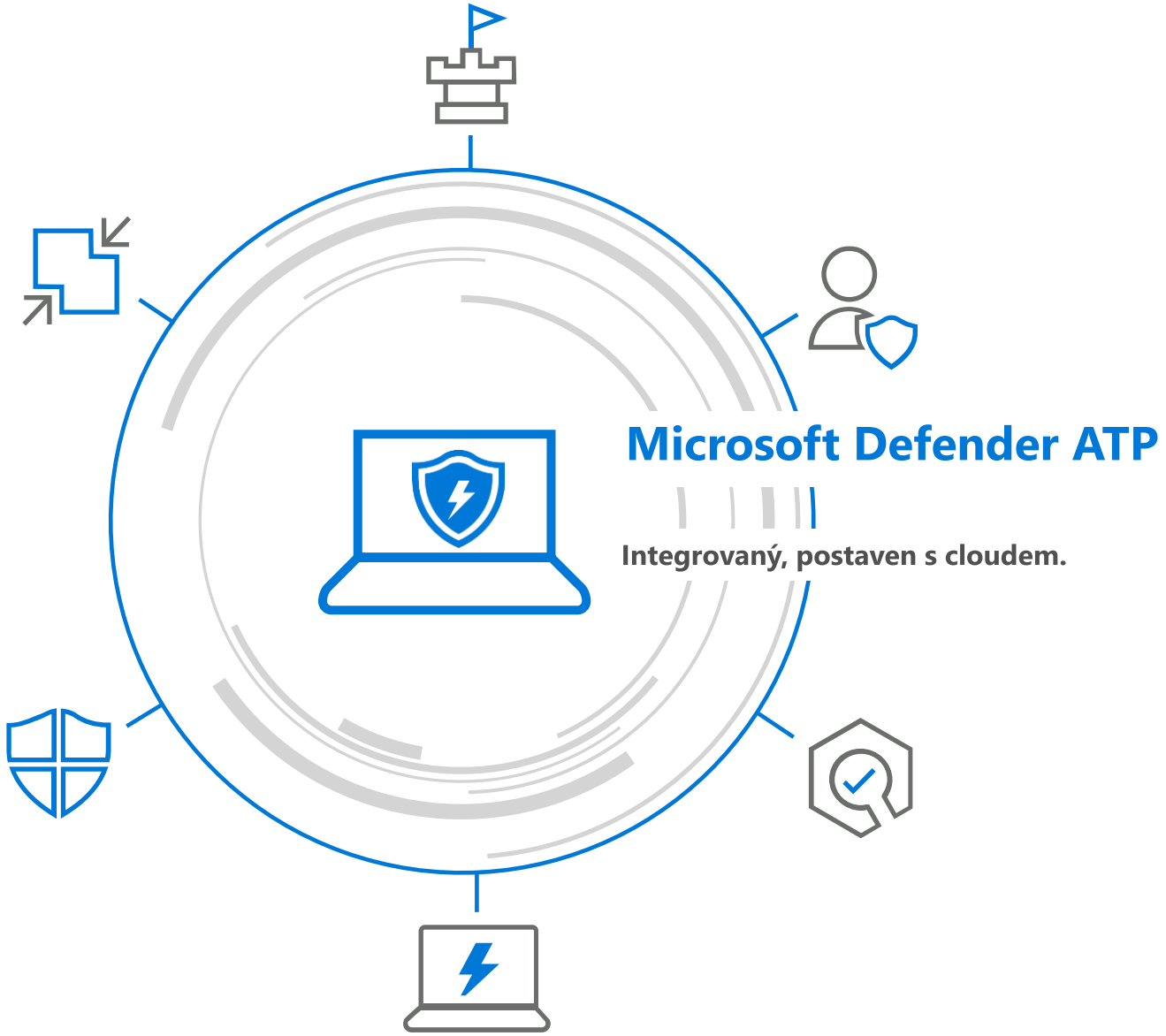
BEZPEČNOSTNÍ TÝM
Čas a znalosti

CENA
Více řešení a on-prem infrastruktura



Ochrana koncového bodu je byla složitá.

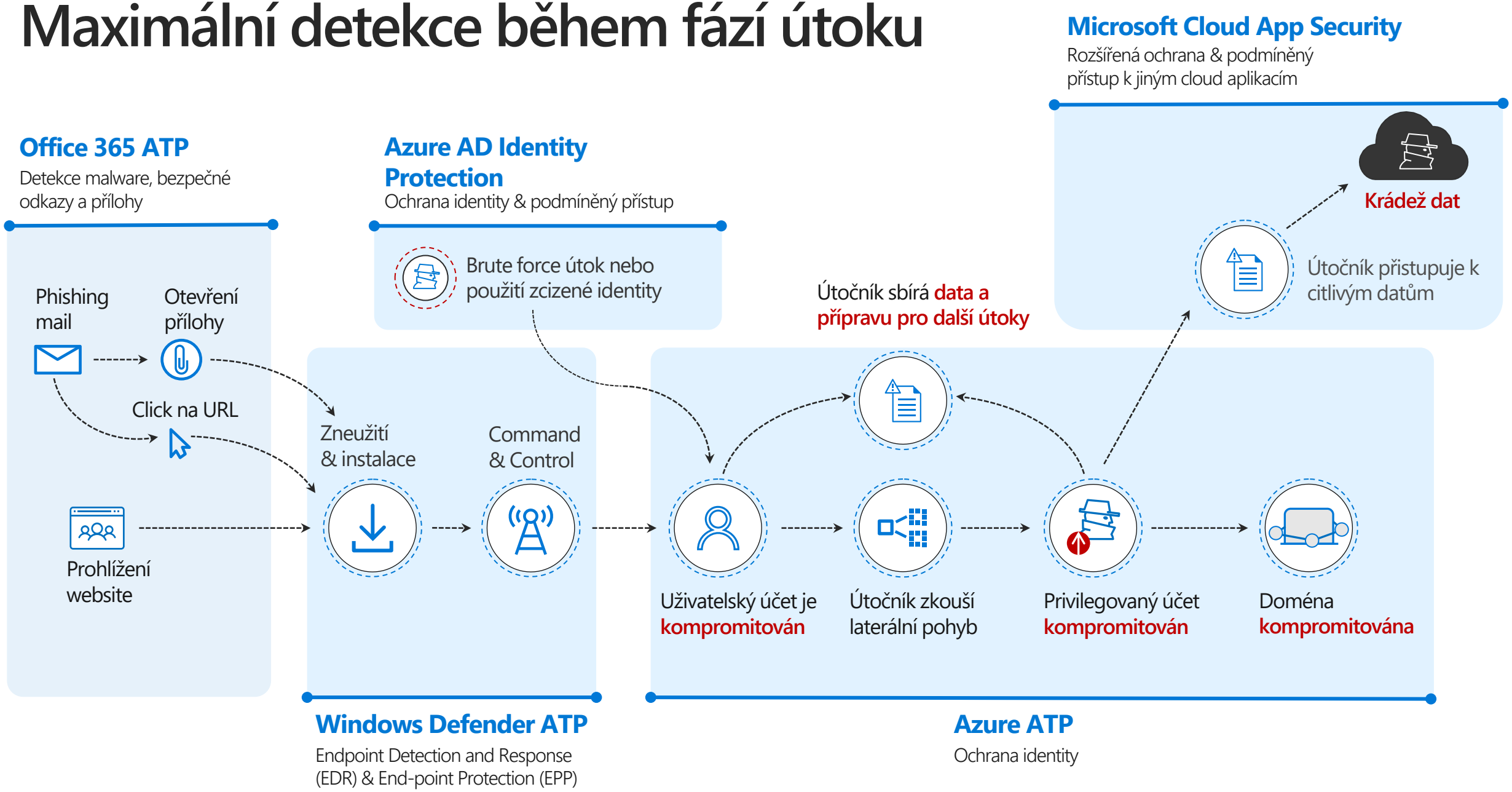
- Malware
- Phishing
- Ransomware
- 0-day
- World-wide outbreaks
- Advanced attacks
- Supply chain
- Fileless attacks
- Vulnerabilities



Microsoft Defender ATP

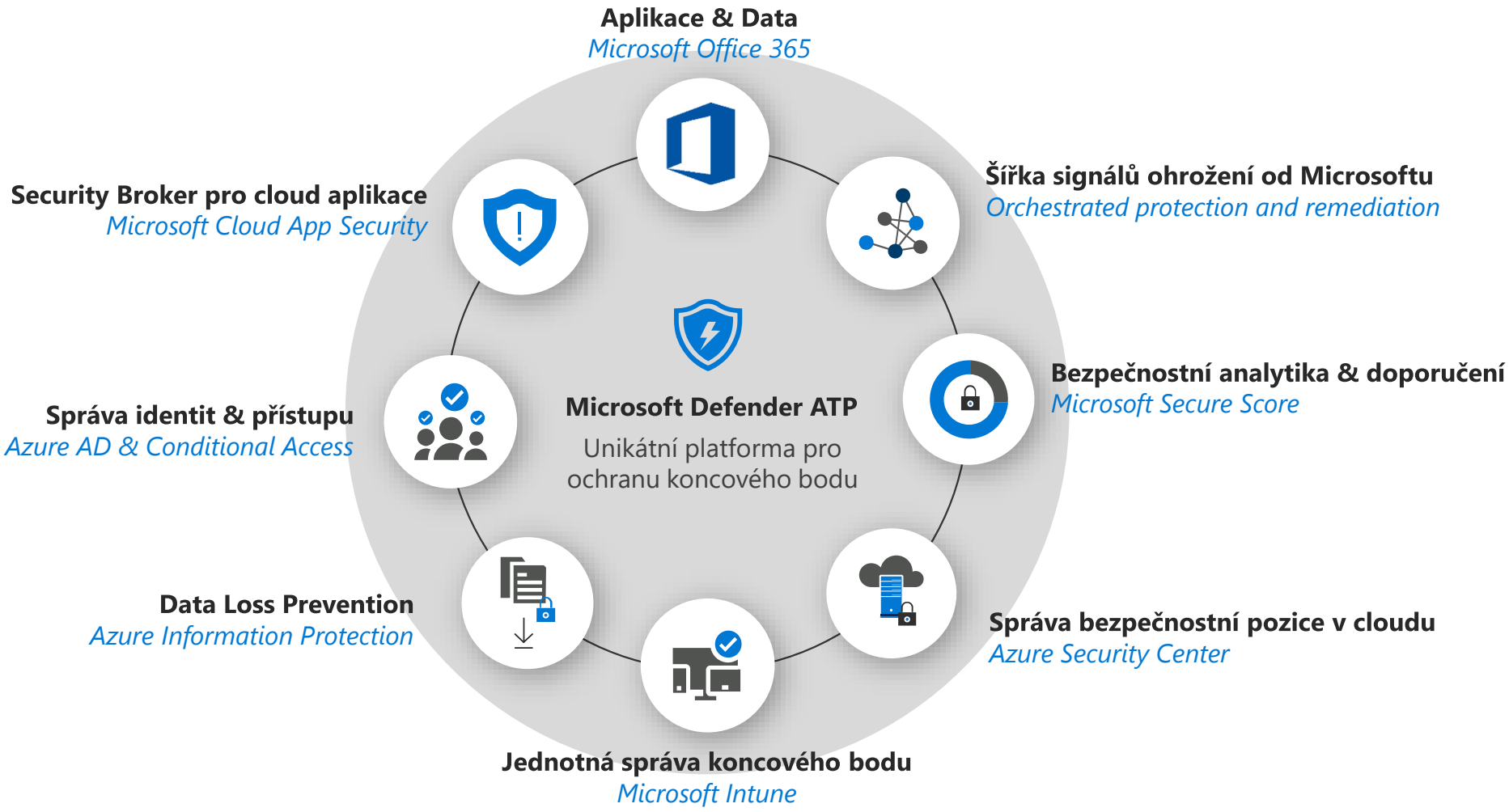
Integrovaný, postaven s cloudem.

Maximální detekce během fází útoku



Microsoft Defender ATP

Povýšení bezpečnosti ve všech scénářích



Microsoft Defender ATP

Integrovaný. Postaven s cloudem.

IT mu věří. Bezpečnostní týmy jej milují.