

OUR DEFENSE IN DEPTH APPROACH
INCLUDES EXTENSIVE MONITORING AND CONTROLS,
NETWORK PROTECTION,
DATA ENCRYPTION

OUR DEFENSE IN DEPTH APPROACH
INCLUDES EXTENSIVE MONITORING AND CONTROLS,
NETWORK PROTECTION,
DATA ENCRYPTION

OUR DEFENSE IN DEPTH APPROACH
INCLUDES EXTENSIVE MONITORING AND CONTROLS,
NETWORK PROTECTION,
DATA ENCRYPTION

OUR DEFENSE IN DEPTH APPROACH
INCLUDES EXTENSIVE MONITORING AND CONTROLS,
NETWORK PROTECTION,
DATA ENCRYPTION

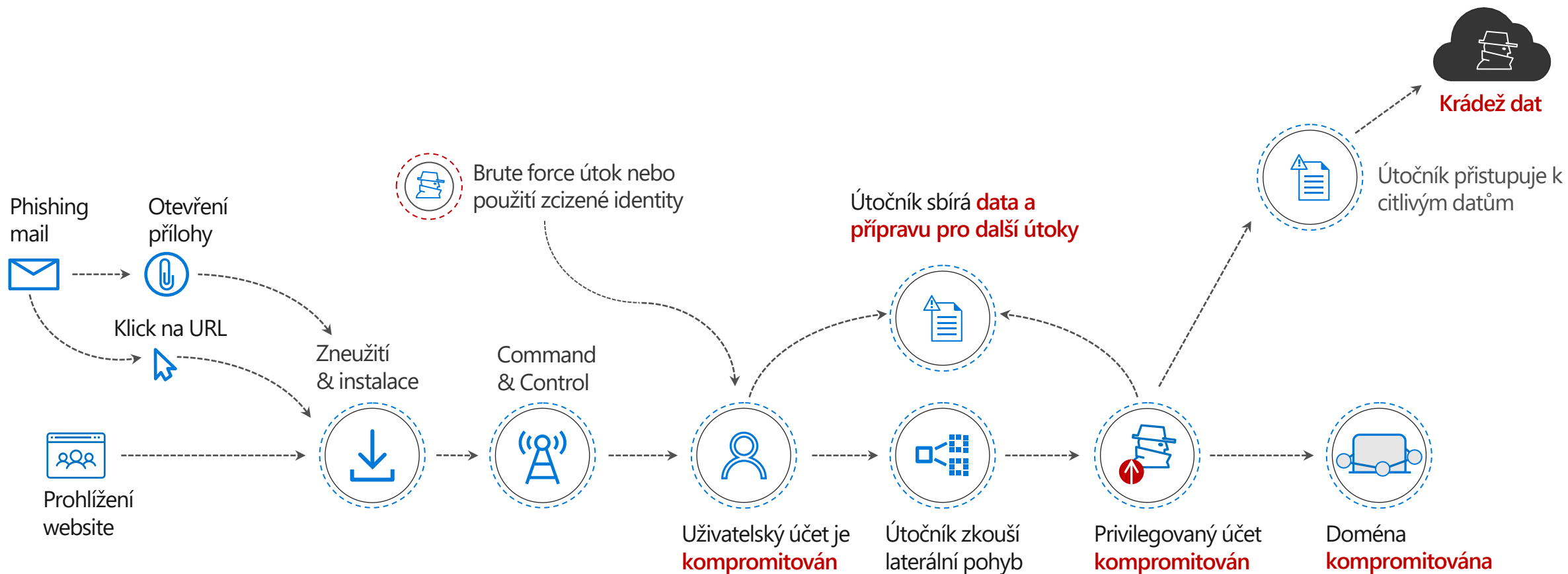
Moderní kybernetická bezpečnost potřebuje data a signály

Dalibor Kačmář

dalibor.kacmar@microsoft.com

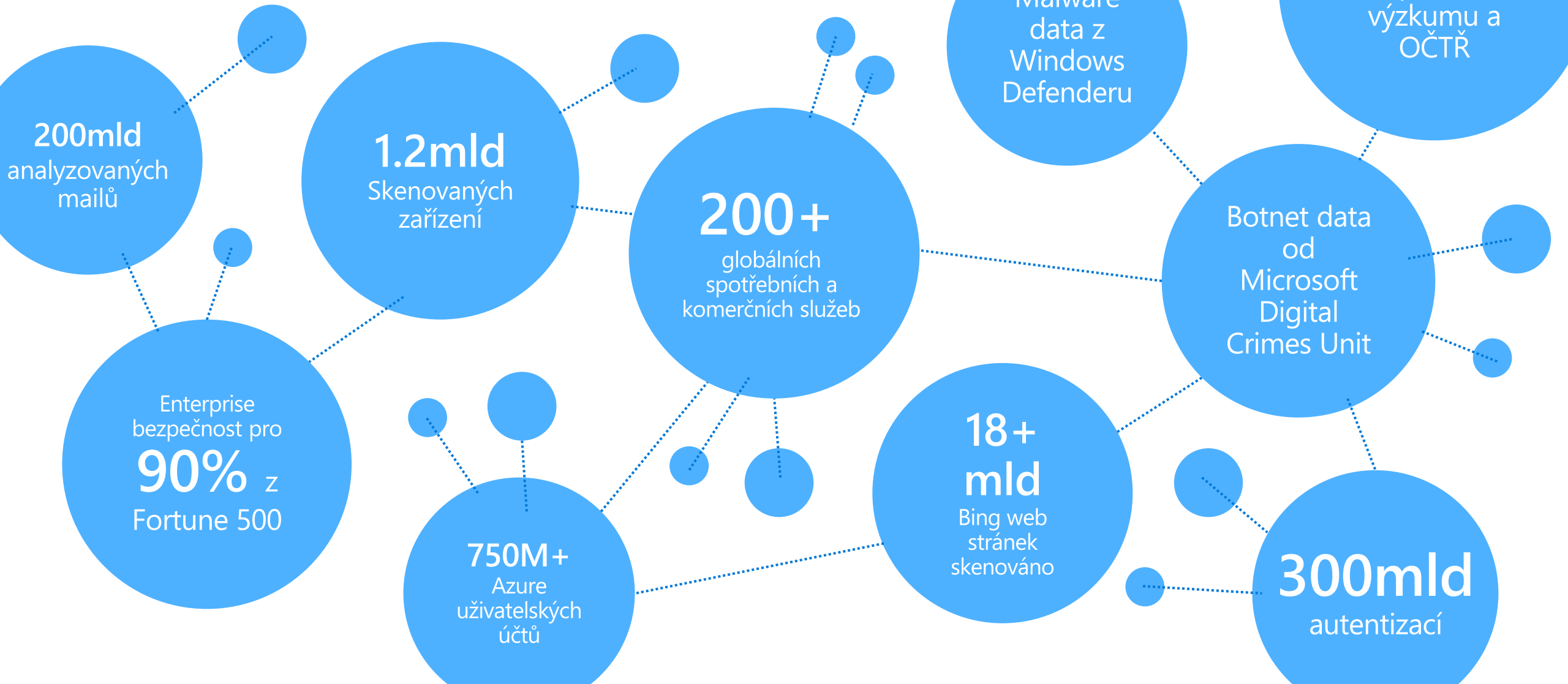
National Technology Officer
Microsoft

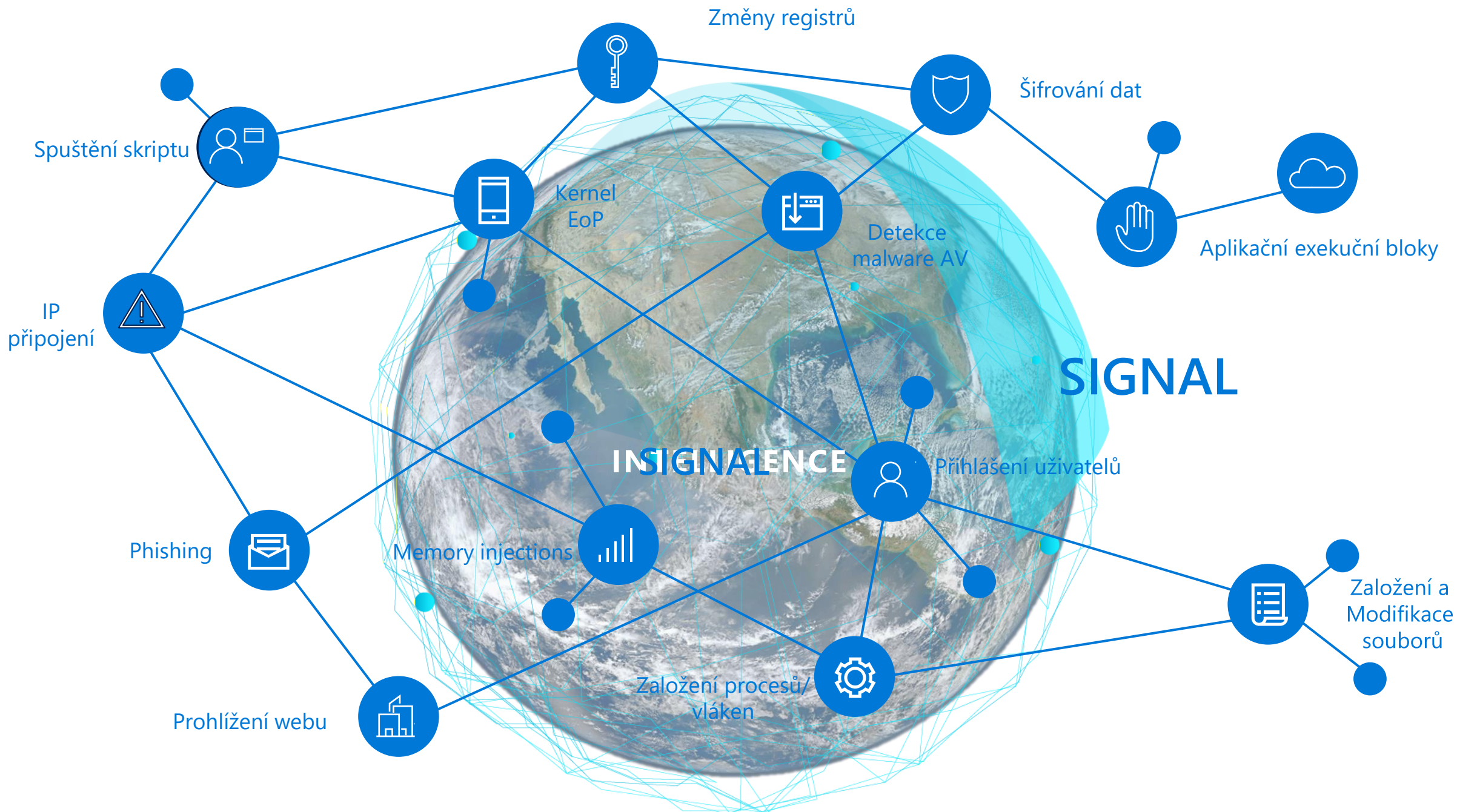
Maximální detekce během fází útoku



Microsoft Intelligent Security Graph

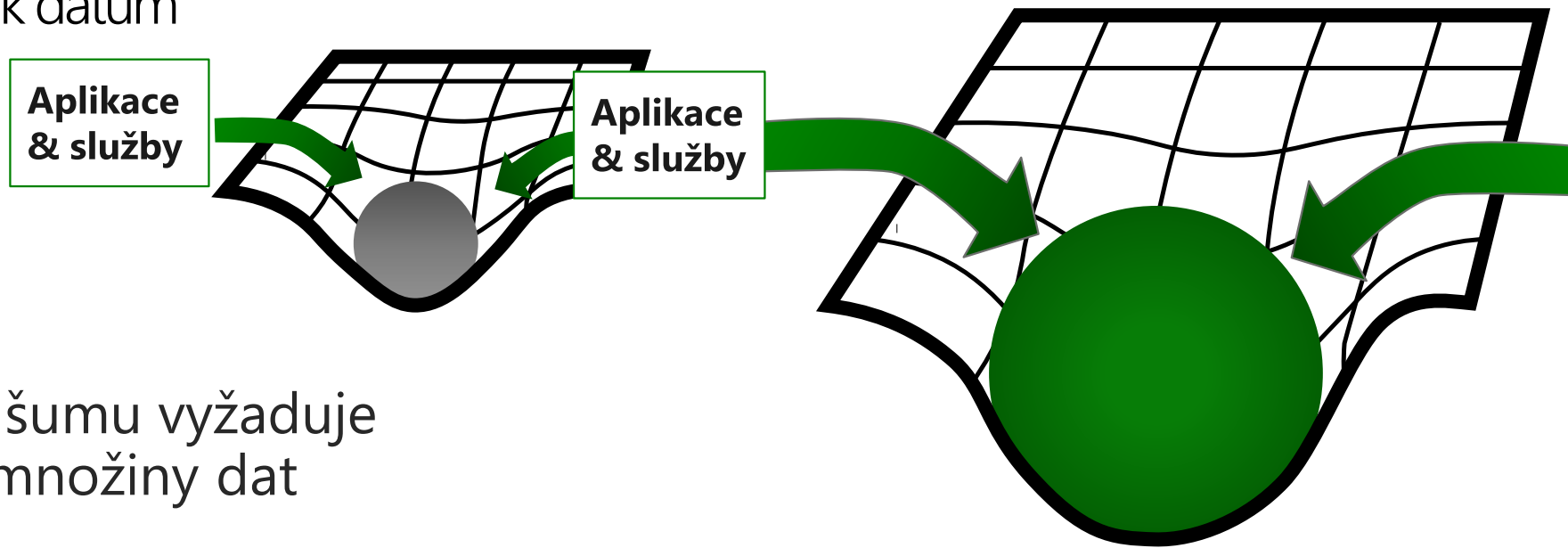
Jedinečné pohledy, informován biliony signálů





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

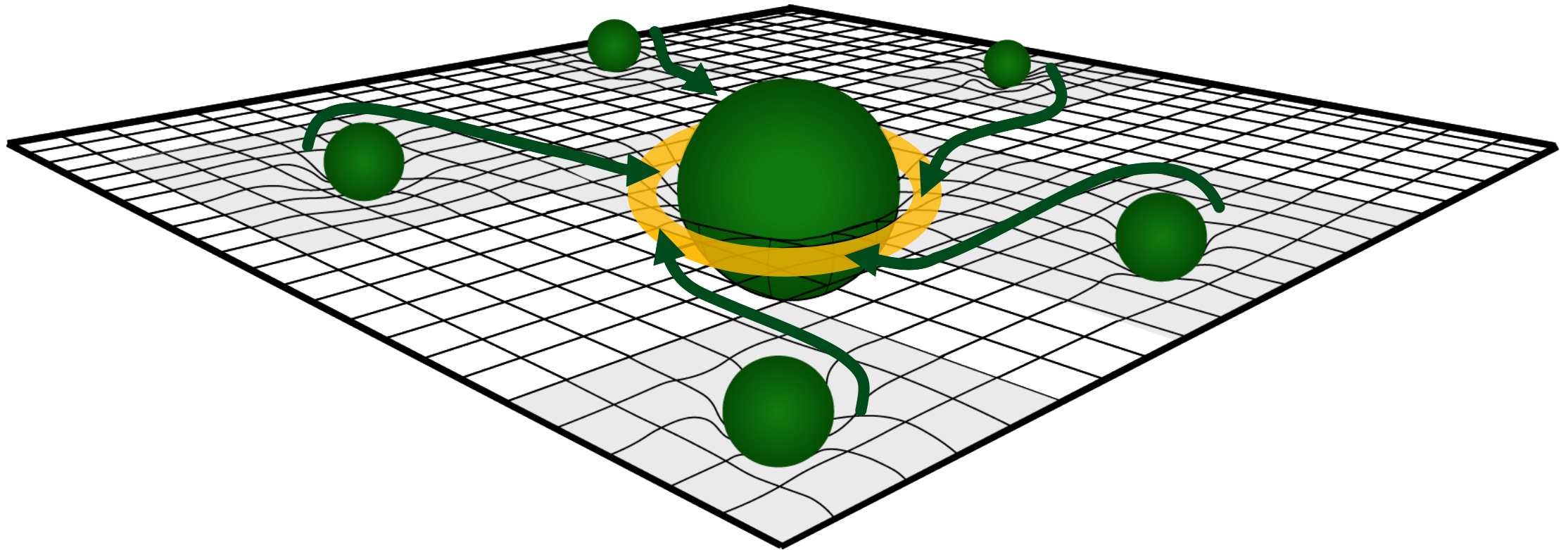
→ Musíme použít analytiku místně a centrálně integrovat

Data Gravity

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

Racionalizace SOC signálů

SOCs pracují dnes s mnoha datovými zdroji



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

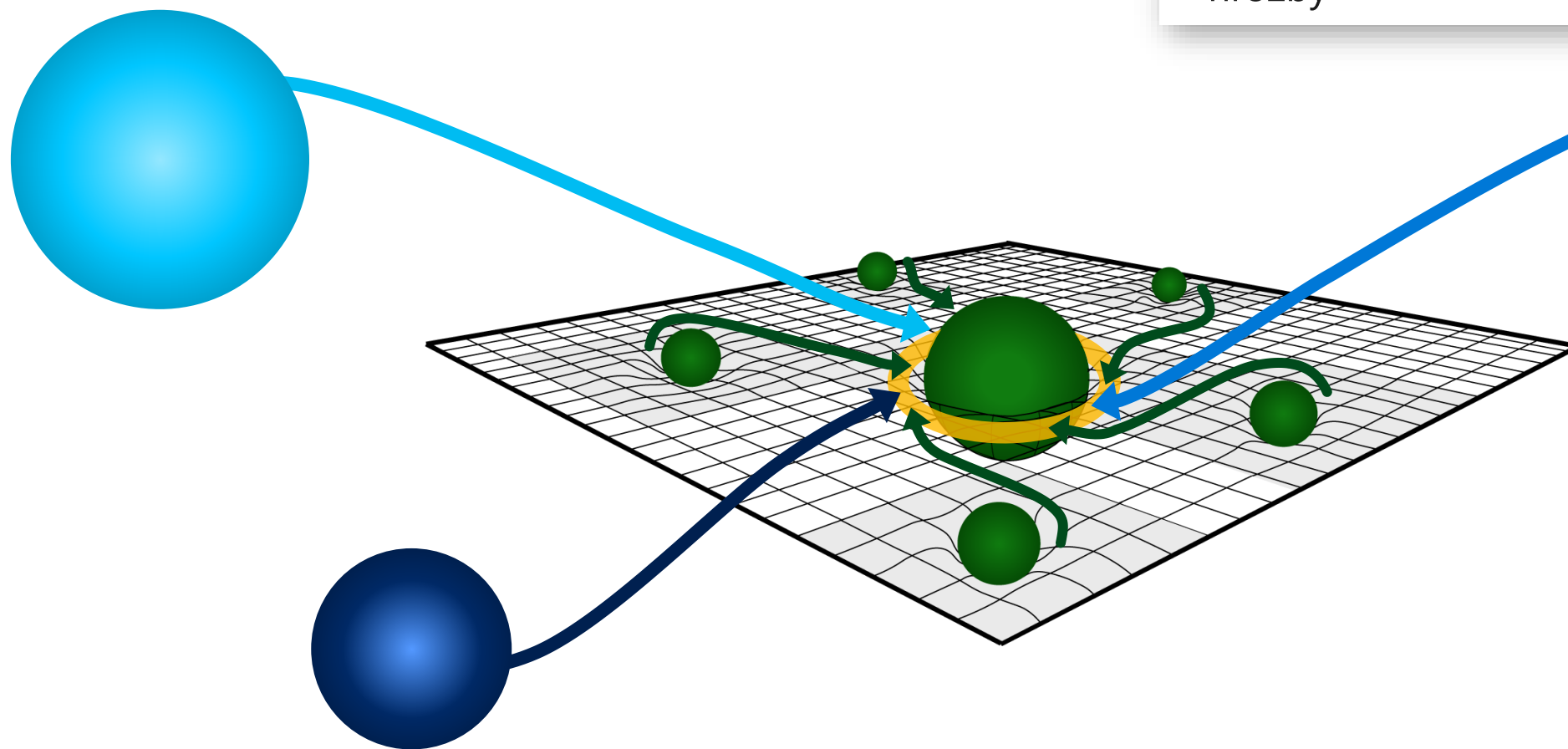
Graph Security API – unifikace signálů

Umožňuje analytikům získat pohledy a kontext napříč

- Lokálními daty a
- Bezpečnostními daty hostovanými v cloudu

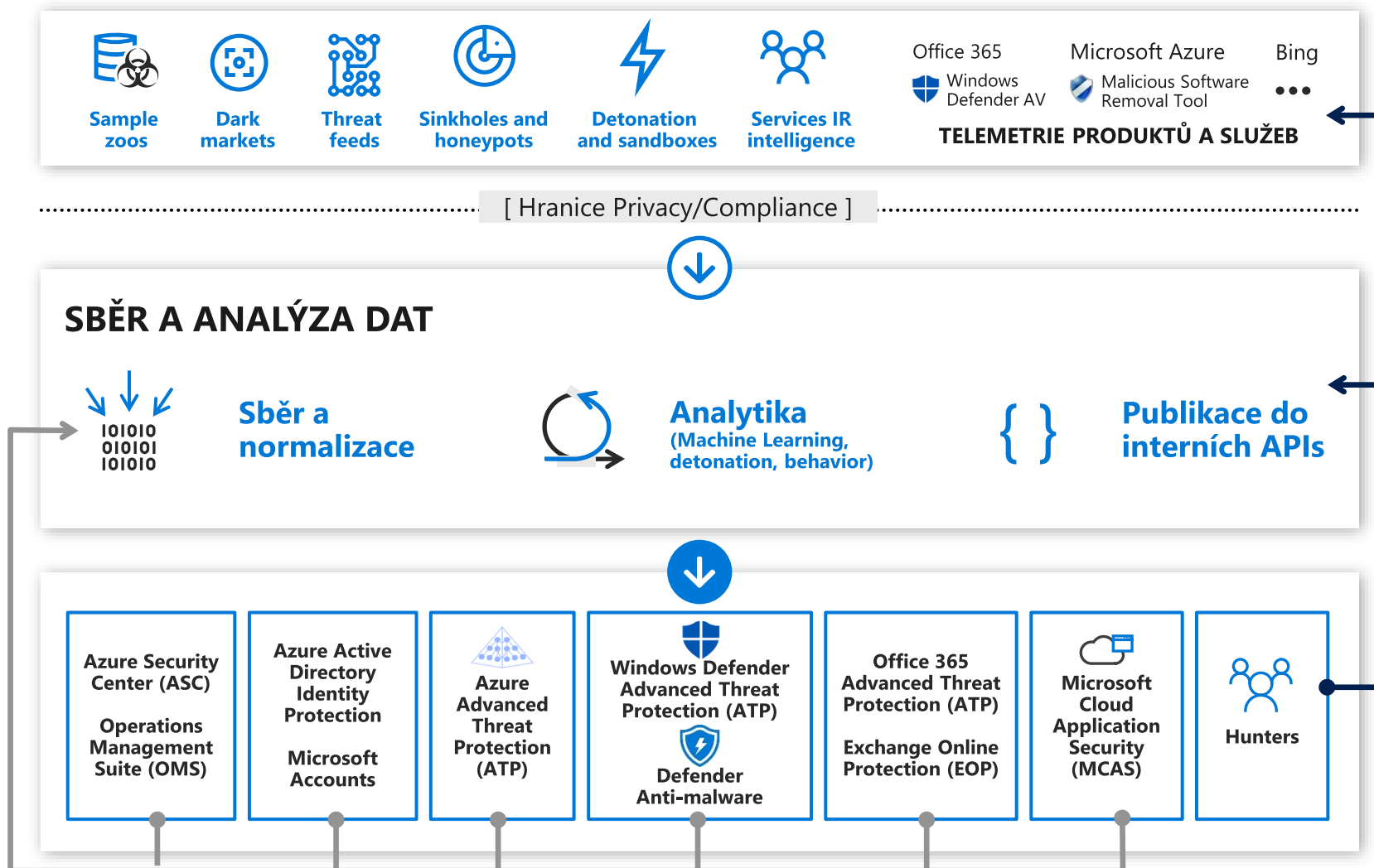
Microsoft's Intelligent Security Graph

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

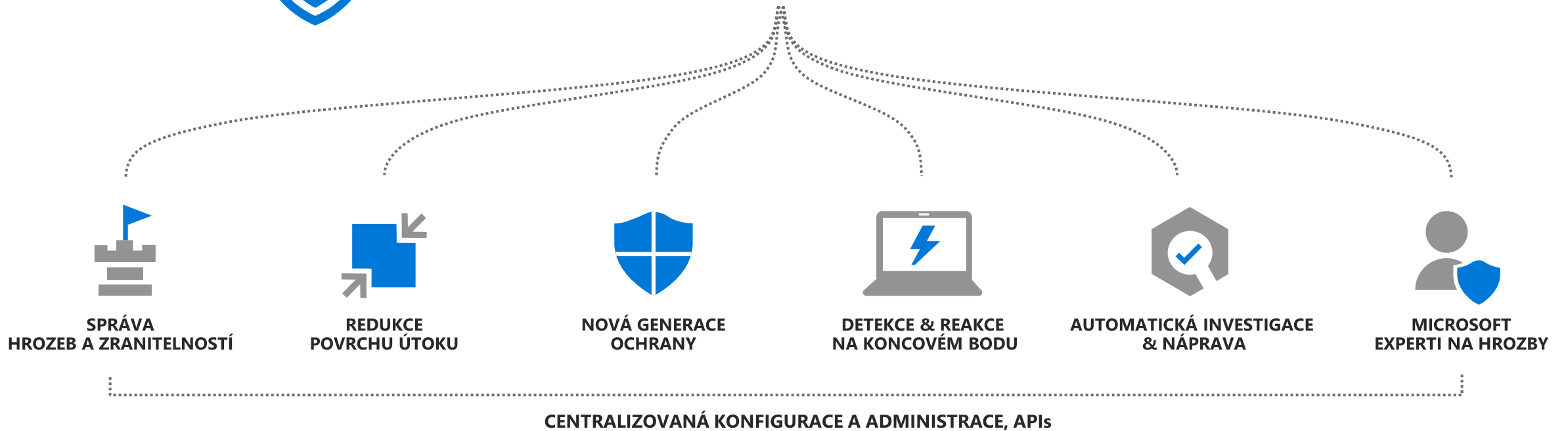
➔ Produkty generují data, zaváděná zpět do grafu

➔ 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.



CENTRALIZOVANÁ KONFIGURACE A ADMINISTRACE, APIs



Potřeba správy hrozeb a zranitelností

OFF



Mnoho zranitelností,
nejí zřejmé skutečné riziko



Opožděná a částečná
viditelnost bezpečnostní
pozice organizace



Chybějící prioritizace
s čím začít nejdříve



Prioritizace zranitelností
postrádá business kontext



Nezvládnutelný počet nálezů

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

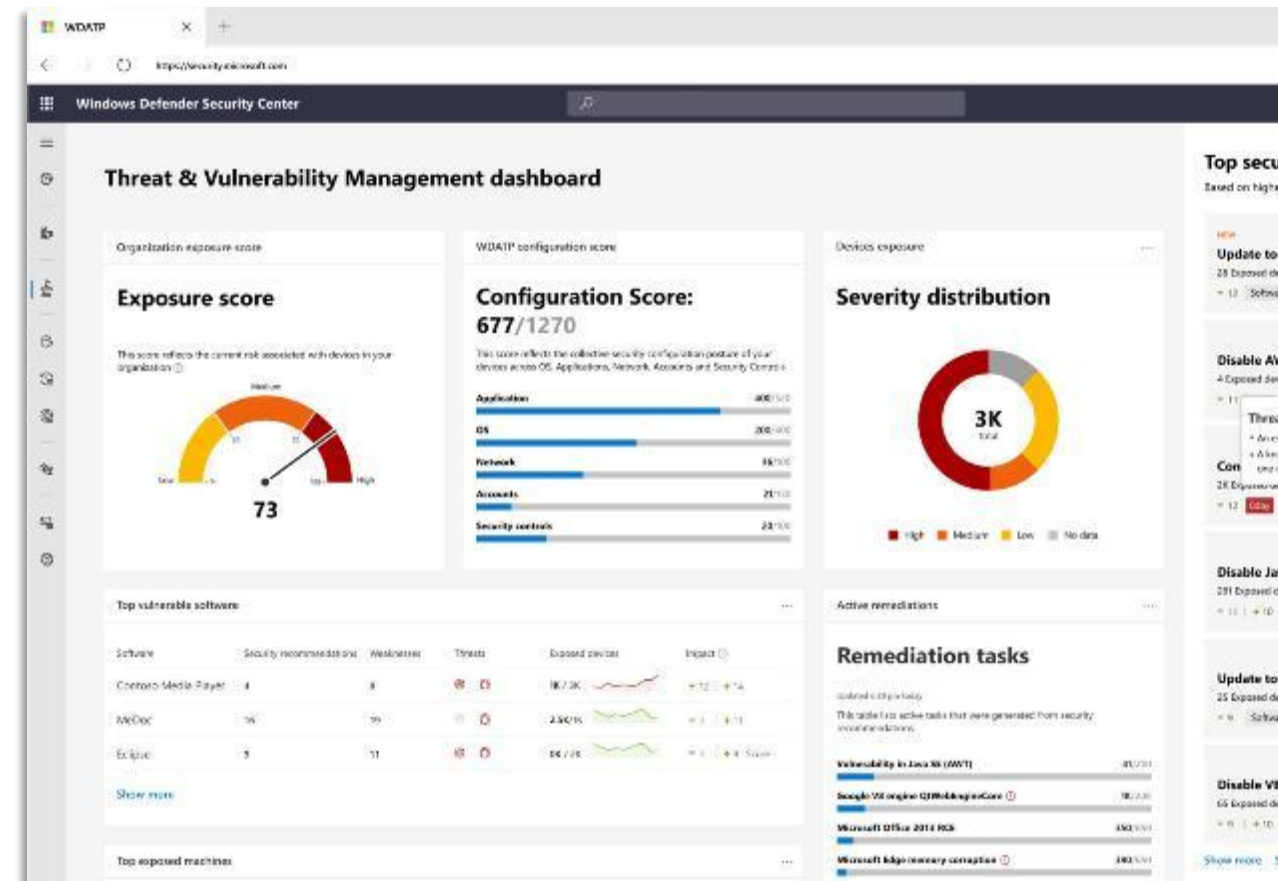
Kontextově řízená prioritizace

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

Mitigace

Přesná mitigace & automatické opravy

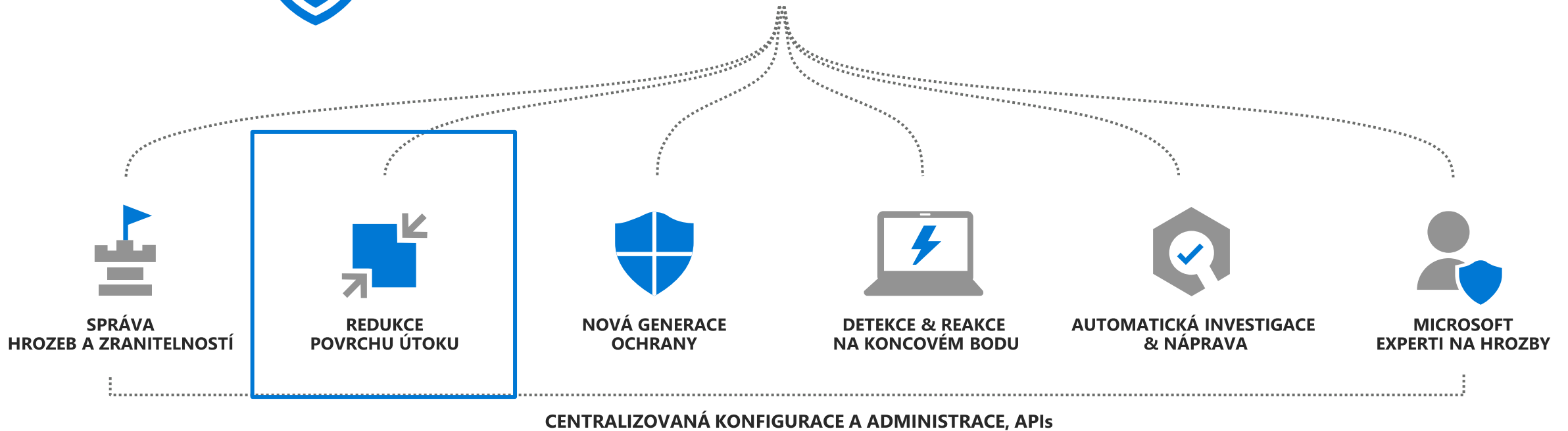
hrozeb pomocí přizpůsobeného plánu postaveném na organizačním riziku s využitím bezpečnostních řešení Microsoftu a partnerů



Microsoft Defender Advanced Threat Protection



Integrovaný. Postaven s cloudem.





Potřeba pro redukci povrchu útoku

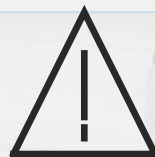
OFF



Zranitelnosti v software
(např. chyby v kódu)
nezmizí, protože chybovat
je lidské



„Out of the box“ platformy
mají málo používané
plochy funkcí, které vytváří
příležitosti pro zneužití
utočnicků



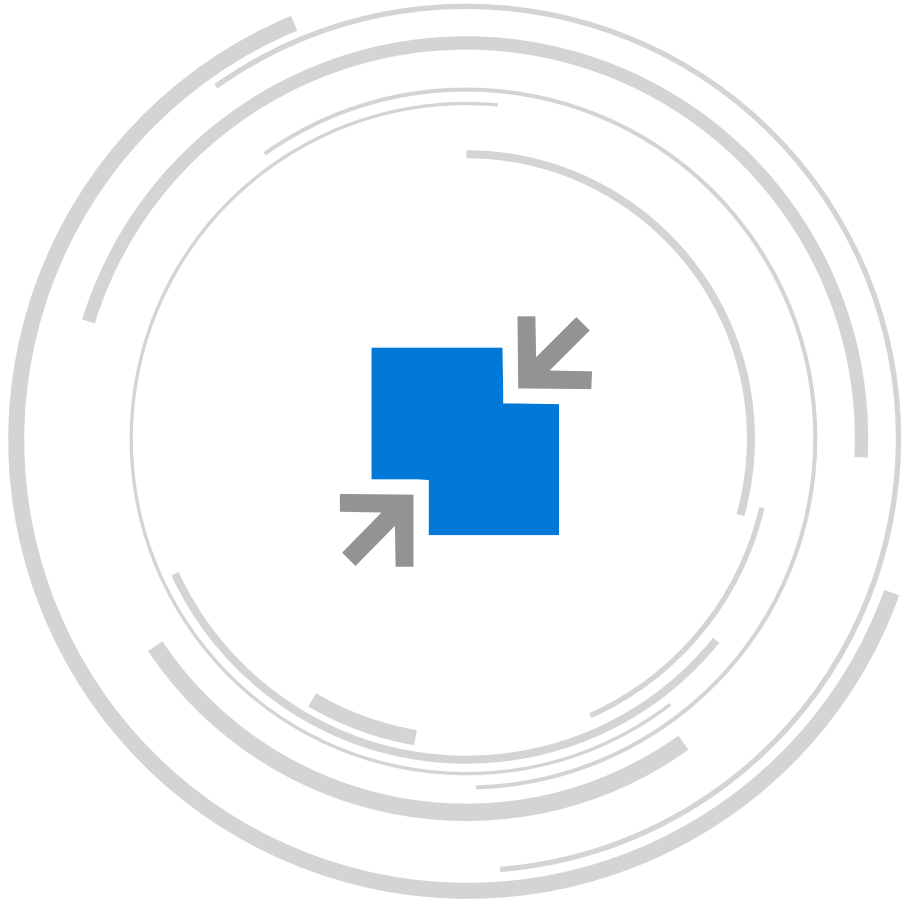
Platforma, kde může běžet
cokoli a závisí pouze na
detekci je méně bezpečná
než platforma umožňující
běh pouze důvěryhodných
aplikací



Zařízení s omezeným
přístupem pouze do
známých síťových lokací je
daleko komplikovanějším
cílem

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

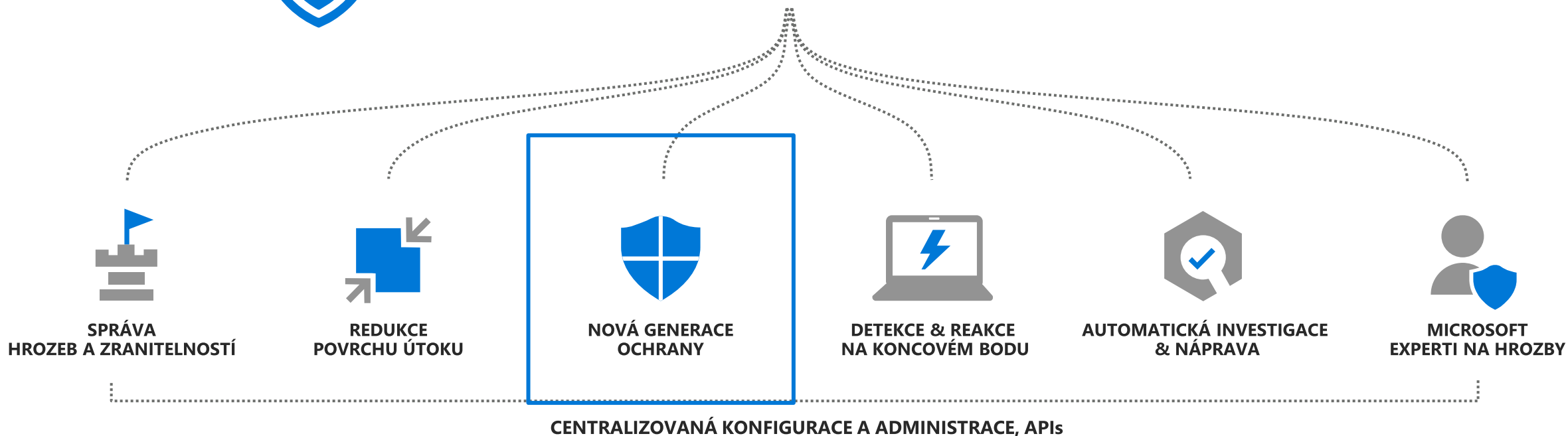
Ochrana historických aplikací

Povolení běhu pouze důvěryhodných aplikací

Microsoft Defender Advanced Threat Protection



Integrovaný. Postaven s cloudem.





Potřeba nové generace ochrany

OFF



Řešení, která závisí na pravidelných aktualizacích nemohou chránit před 7 miliony jedinečných hrozeb, které se objeví za jednu hodinu



Omezení plochy útoku může zvýšit bezpečnostní úroveň, stále nějaké místo pro útok zůstane

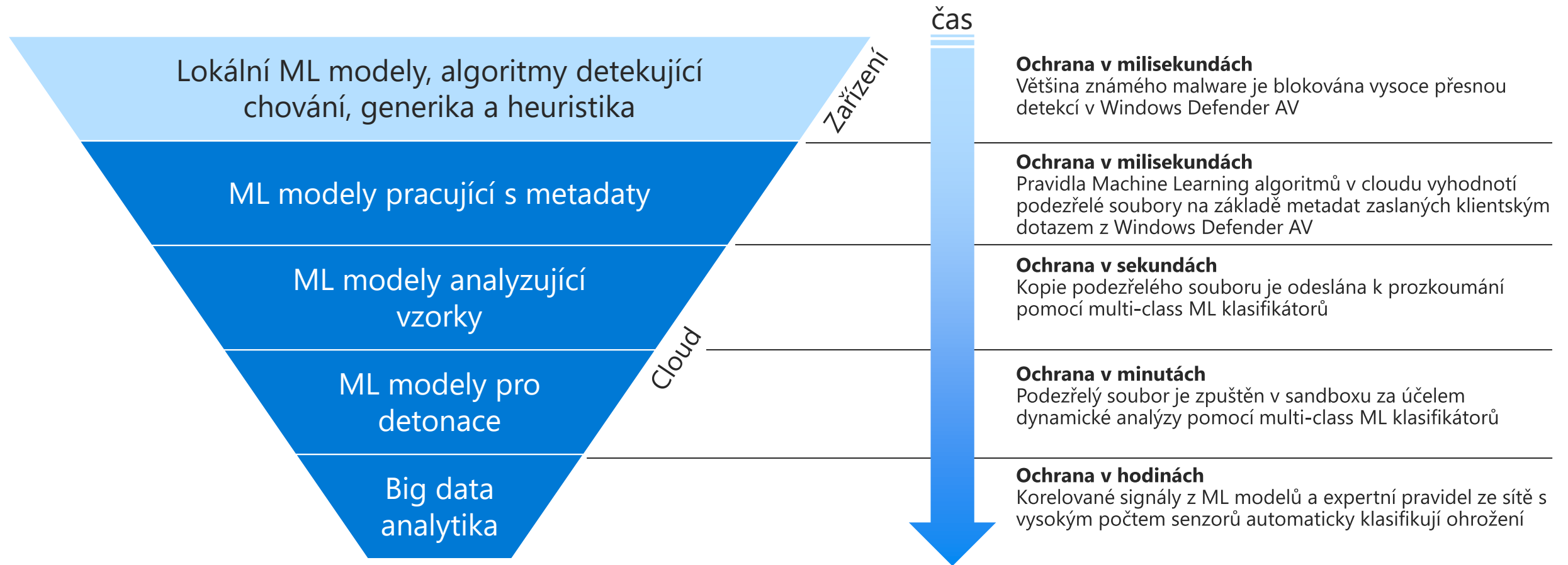


Hra se změnila z blokování rozpoznatelných spustitelných souborů k malware využívajícího pokročilé metody zneužití (např. fileless malware)



Žijeme ve světě hyper polymorfních ohrožení s 5 mld jedinečných instancí měsíčně

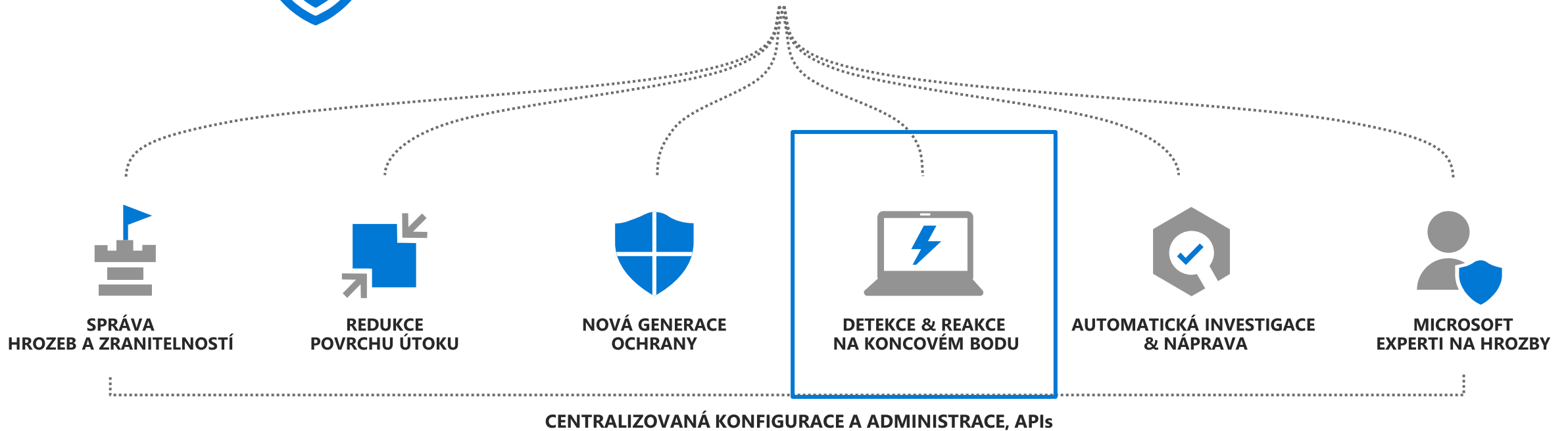
Nová generace ochrany: klientské zařízení + cloud



Microsoft Defender Advanced Threat Protection



Integrovaný. Postaven s cloudem.





Potřeba pro detekci a reakci na koncovém bodu

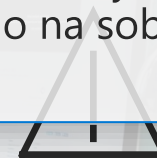
OFF



200+dní v průměru zůstává
útočník v cílové síti než je
detekován



46% kompromitovaných
systémů nemělo na sobě
malware



Složité se vyznat v
detekovaných hrozbách



99.9% zneužití zranitelností byly
použity rok po té, co byla
publikovány na CVE



Žijí mimo hranice. Útočníci
využívají vyhýbací techniky
(AET)

[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**

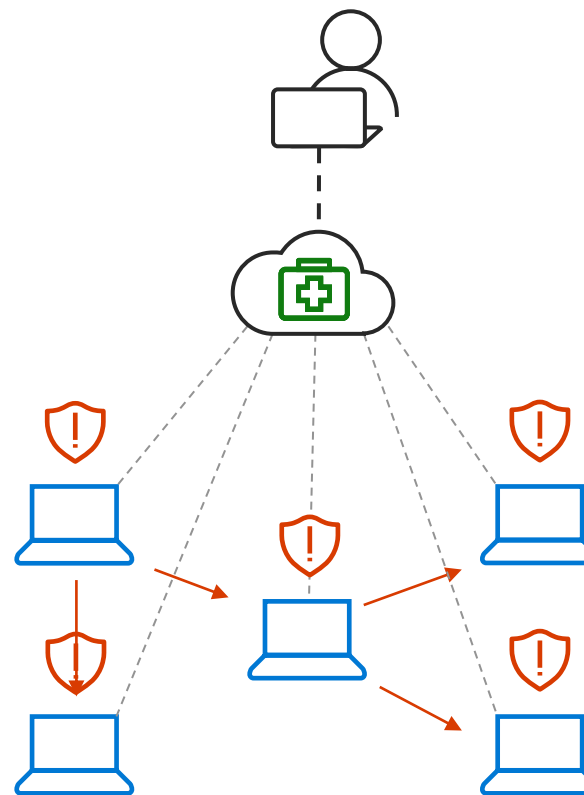
Reakce a omezení šíření

Sandbox analýza

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

**Historický a real-time
threat hunting**

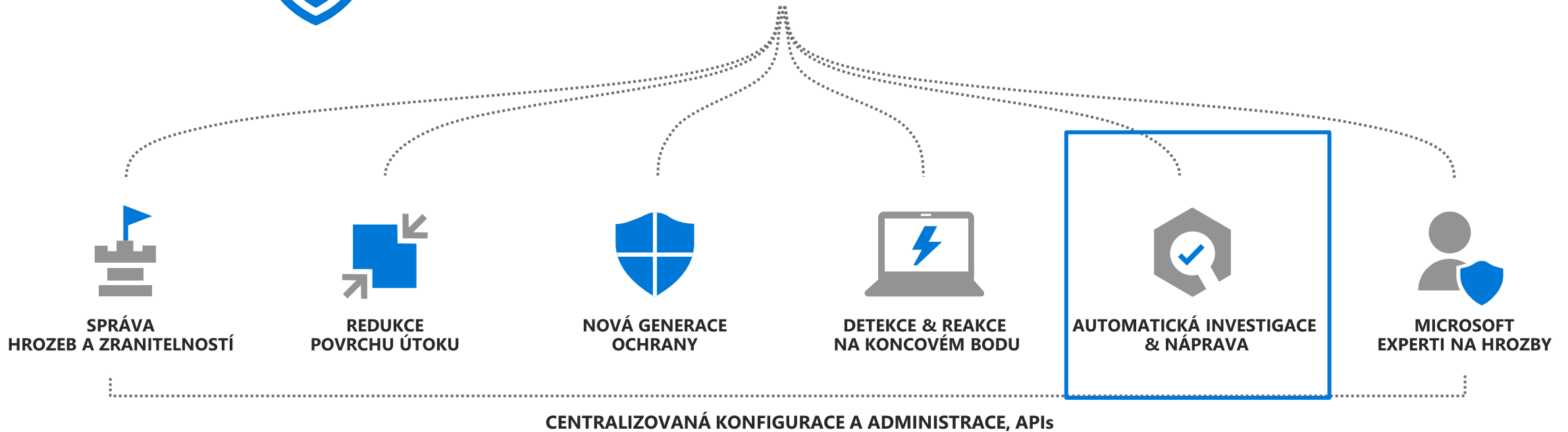
**Threat intelligence a
přizpůsobitelné detekce**



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 

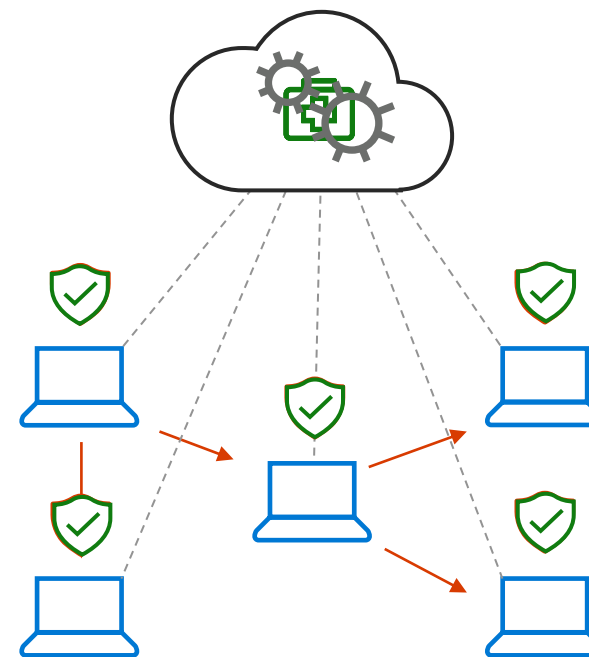
Historical endpoint data

Response orchestration

AI-based
response playbooks

File/IP reputation

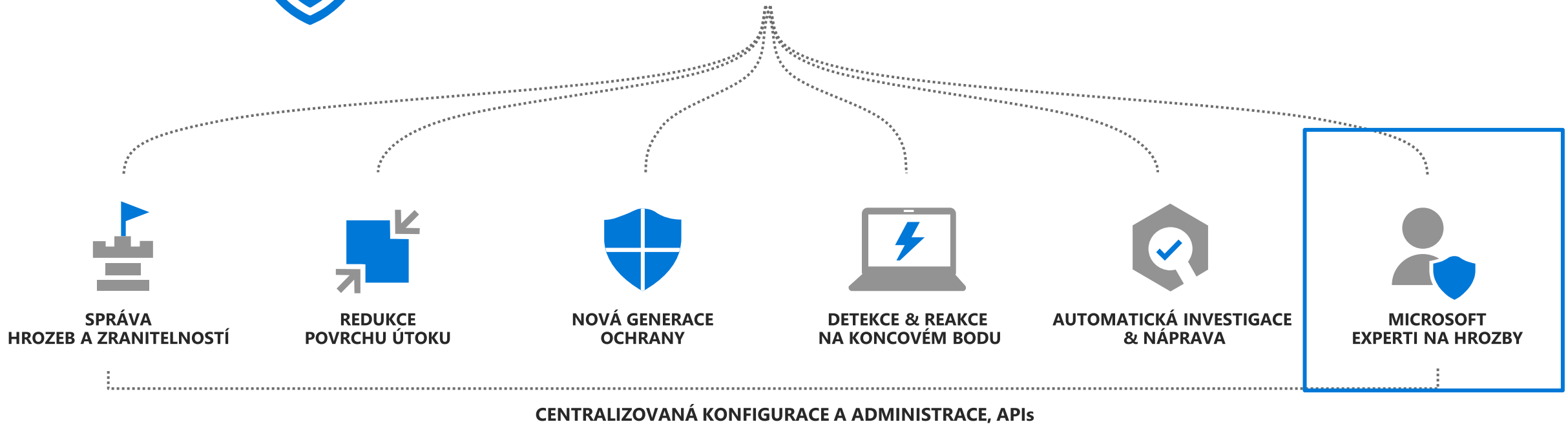
Sandbox



Microsoft Defender Advanced Threat Protection



Integrovaný. Postaven s cloudem.





Potřeby pro řízený Hunting

OFF



Potřeba
dodatečného
kontextu hrozby



Když je potřeba,
expert není k dispozici



Má tento alert nebo
událost význam pro mou
organizaci?



Chybějící doporučení
reakce pro zpracování
alertu



Důležité alerty mohou
zůstat nepovšimnuty

Managed Threat Hunting Service

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

Nepřehlédněte prolomení

Jistě si záda

Microsoft experti na hrozby proaktivně hledají anomálie nebo 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.

The screenshot displays the Windows Defender Security Center interface. At the top, a red banner indicates a 'New Alert from Bilbao Team: Software Supply Chain Attack'. Below this, the 'Dashboard > Software Supply Chain Attack' section shows 10 active alerts, categorized by severity (High, Medium, Low, Informational). A table lists specific alerts, including 'Software Supply Chain Attack', 'Suspicious PowerShell', 'Suspect scheduled task', 'Active credential theft tool', and 'Suspicious user behavior'. The interface also features a sidebar with incident details, including severity, status, classification, and assigned experts. A 'Reach out to Bilbao team' button is visible at the bottom right.

Title	Severity	Investigation state	Category	Machine	User
Software Supply Chain Attack	High	N/A	Bilbao	cont-jonathanw	JW
Suspicious PowerShell	Medium	Running	Suspicious Activity	cont-jonathanw	JW
Suspect scheduled task	Medium	Running	Persistence	cont-jonathanw	JW
Active credential theft tool	High	Running	Credential Theft	cont-jonathanw	JW
Suspicious user behavior	Low	Running	Compromised Account	cont-jayharder	JW
Suspicious PowerShell	Medium	Running	Suspicious Activity	cont-jayharder	JH
Suspect scheduled task	Medium	Running	Persistence	cont-jayharder	JH
Active credential theft tool	High	Running	Credential Theft	cont-jayharder	JH
Suspicious user behavior	Low	Running	Compromised Account	cont-jayharder	JH

Microsoft Defender Advanced Threat Protection

Integrovaný. Postaven s cloudem.



**SPRÁVA
HROZEB A ZRANITELNOSTÍ**



**REDUKCE
POVRCHU ÚTOKU**



**NOVÁ GENERACE
OCHRANY**



**DETEKCE & REAKCE
NA KONCOVÉM BODU**

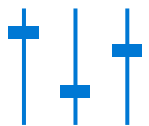


**AUTOMATICKÁ INVESTIGACE
& NÁPRAVA**



**MICROSOFT
EXPERTI NA HROZBY**

CENTRALIZOVANÁ KONFIGURACE A ADMINISTRACE, APIs



Potřeby pro správu bezpečnosti

OFF



Neexistuje jednotný
pohled



Více rozhraní pro správu
komponent bezpečnosti



Neexistující priority
s čím začít nejdříve



Konfigurace napříč
řešeními je složitá



Chybějící doporučení pro vaše
potřeby

Windows Defender ATP- Security management

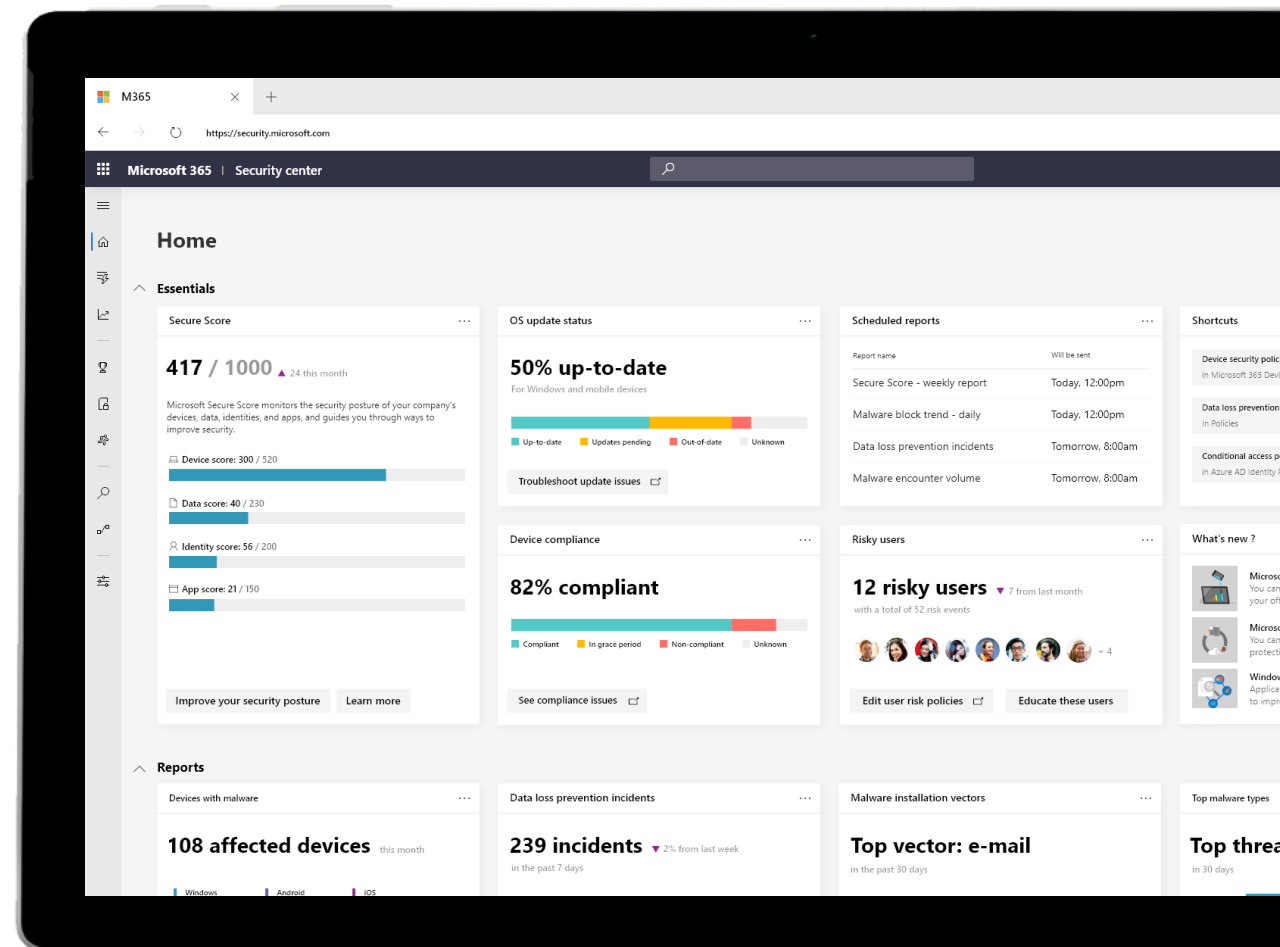
Rozumí tomu, co se děje, co se stalo a připraví vás pro budoucnost

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

Updated 6:20 pm today

/ 1,254

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

Show more

Email protection

12 email accounts at risk

Updated 6:20 pm today

/ 1,022

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



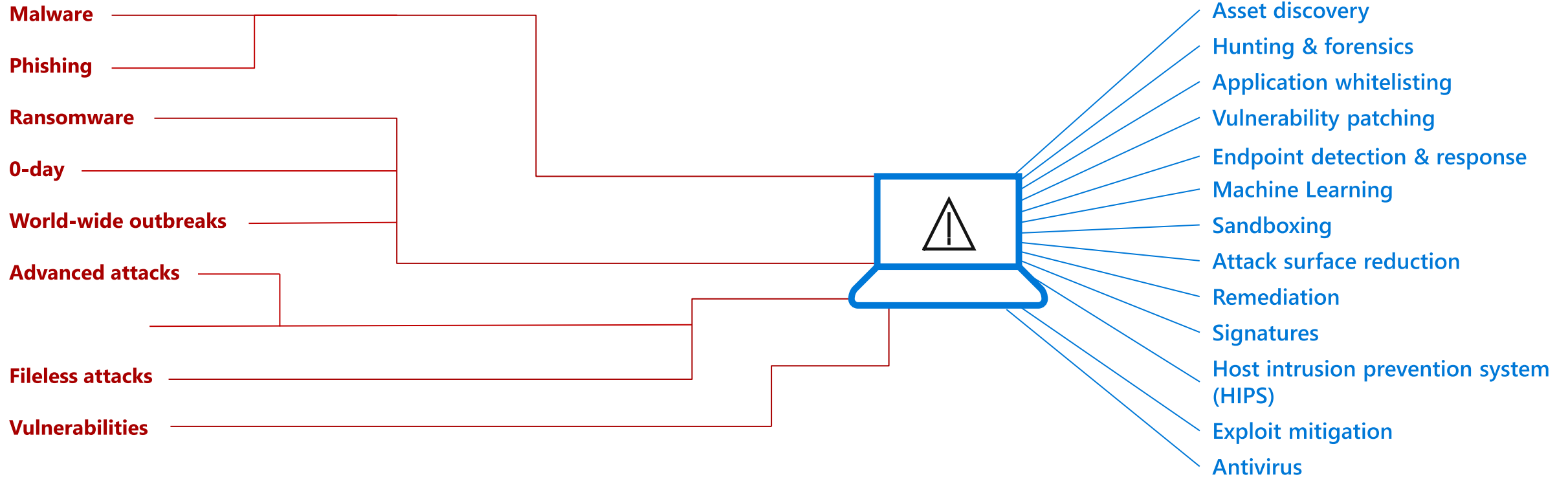
BEZPEČNOSTNÍ TÝM

Čas a znalosti

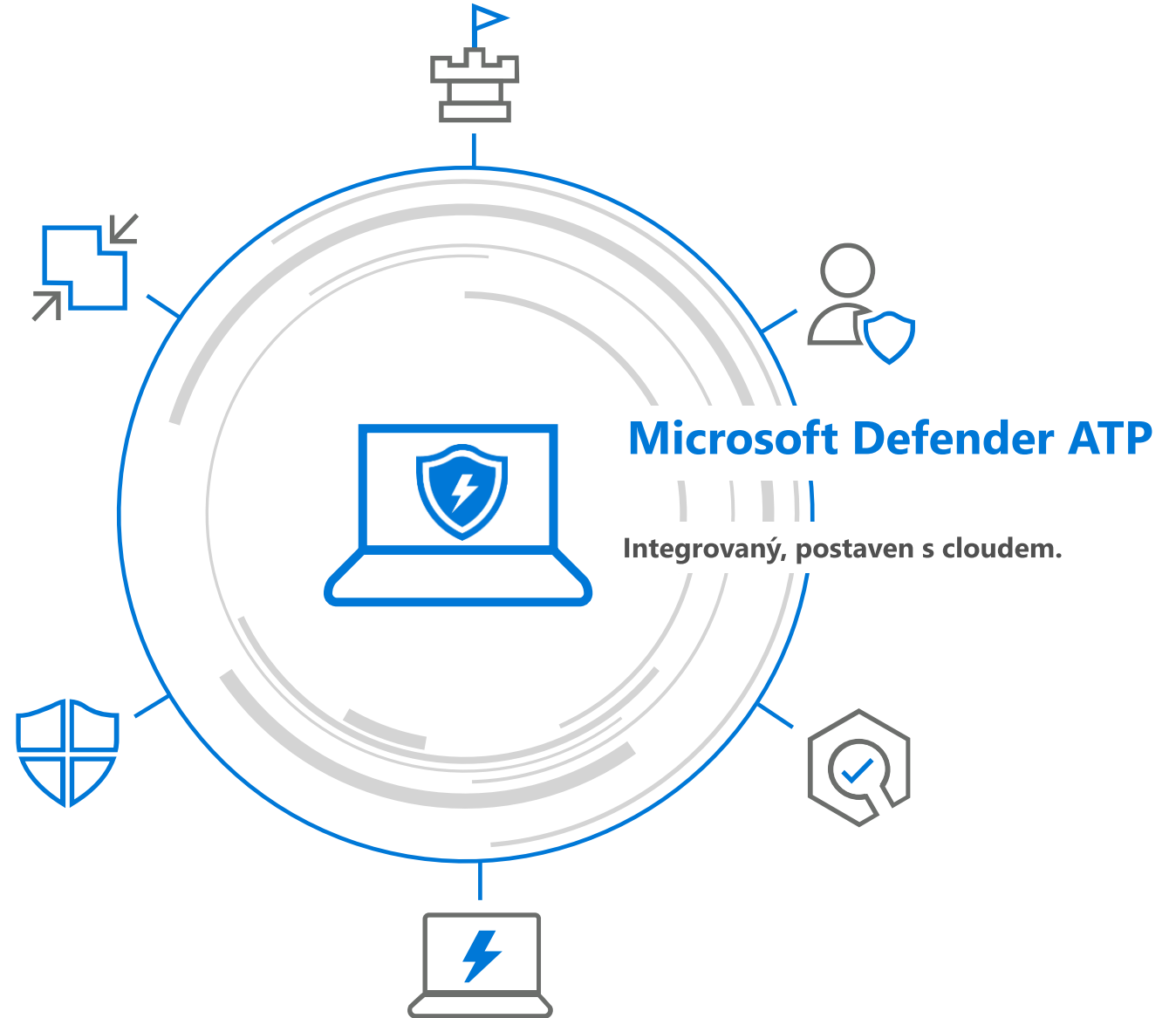
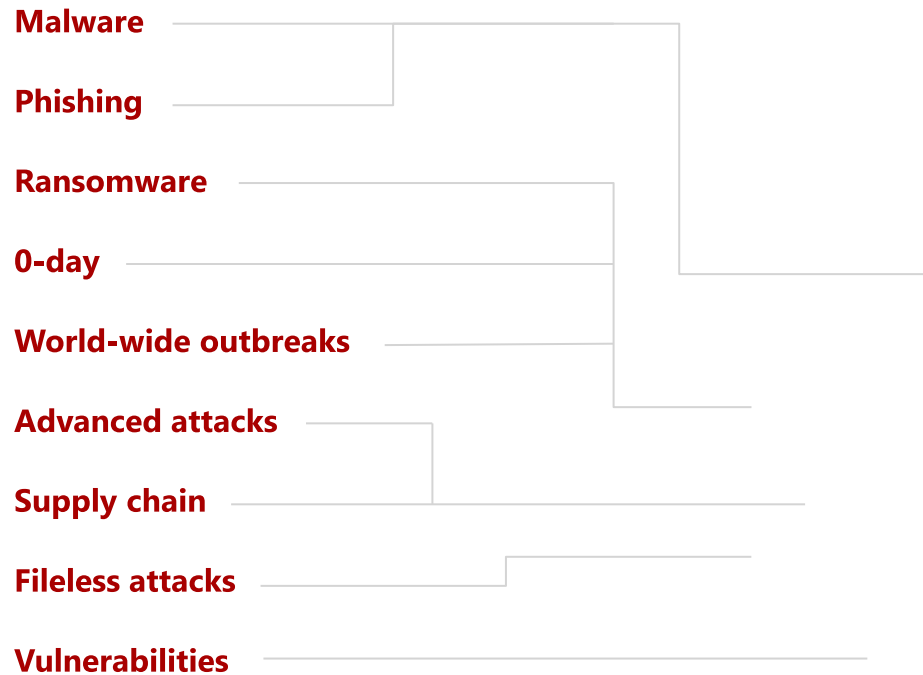


CENA

Více řešení a on-prem infrastruktura



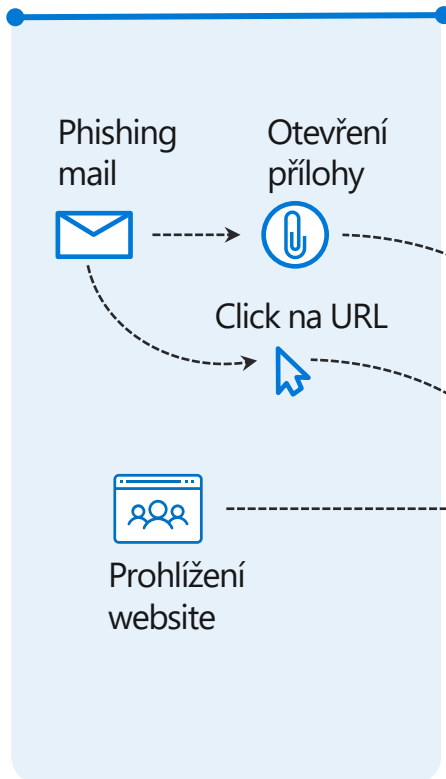
Ochrana koncového bodu je byla složitá.



Maximální detekce během fází útoku

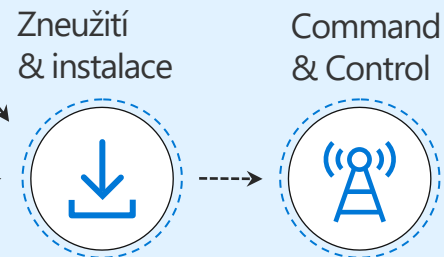
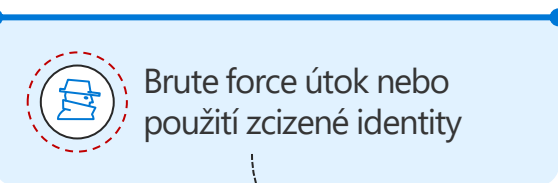
Office 365 ATP

Detekce malware, bezpečné odkazy a přílohy



Azure AD Identity Protection

Ochrana identity & podmíněný přístup

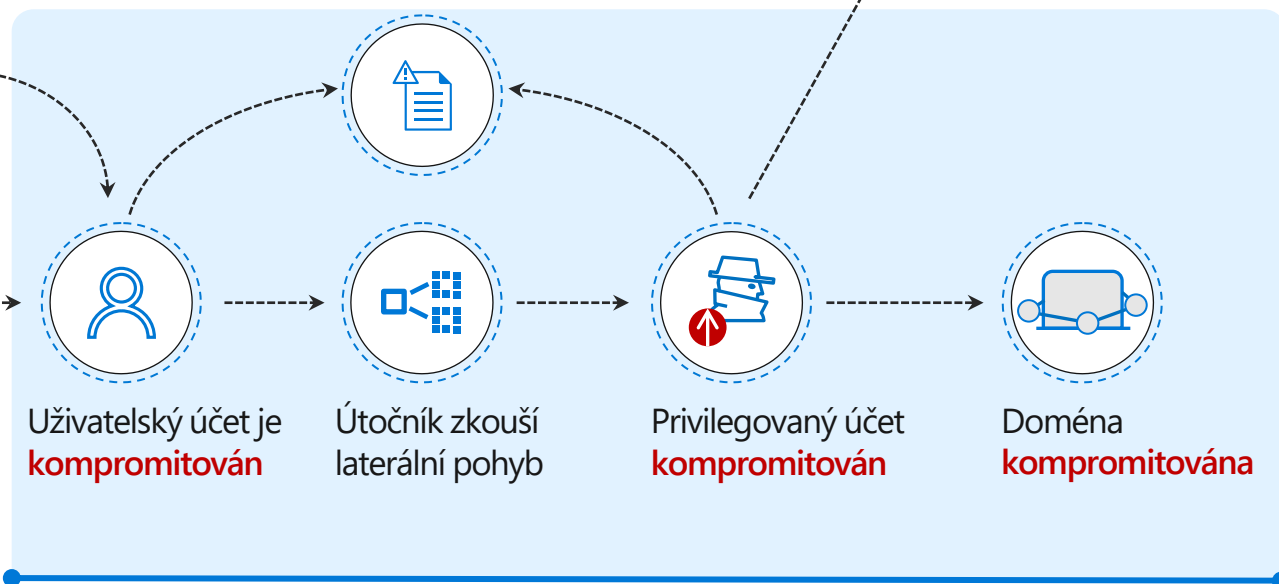


Command & Control

Windows Defender ATP

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

Útočník sbírá **data a** přípravu pro další útoky

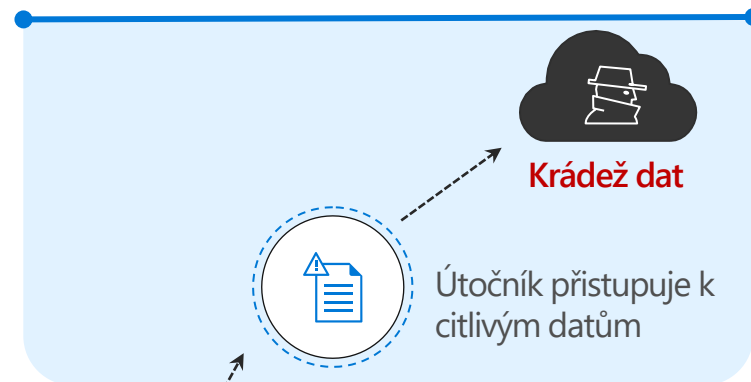


Azure ATP

Ochrana identity

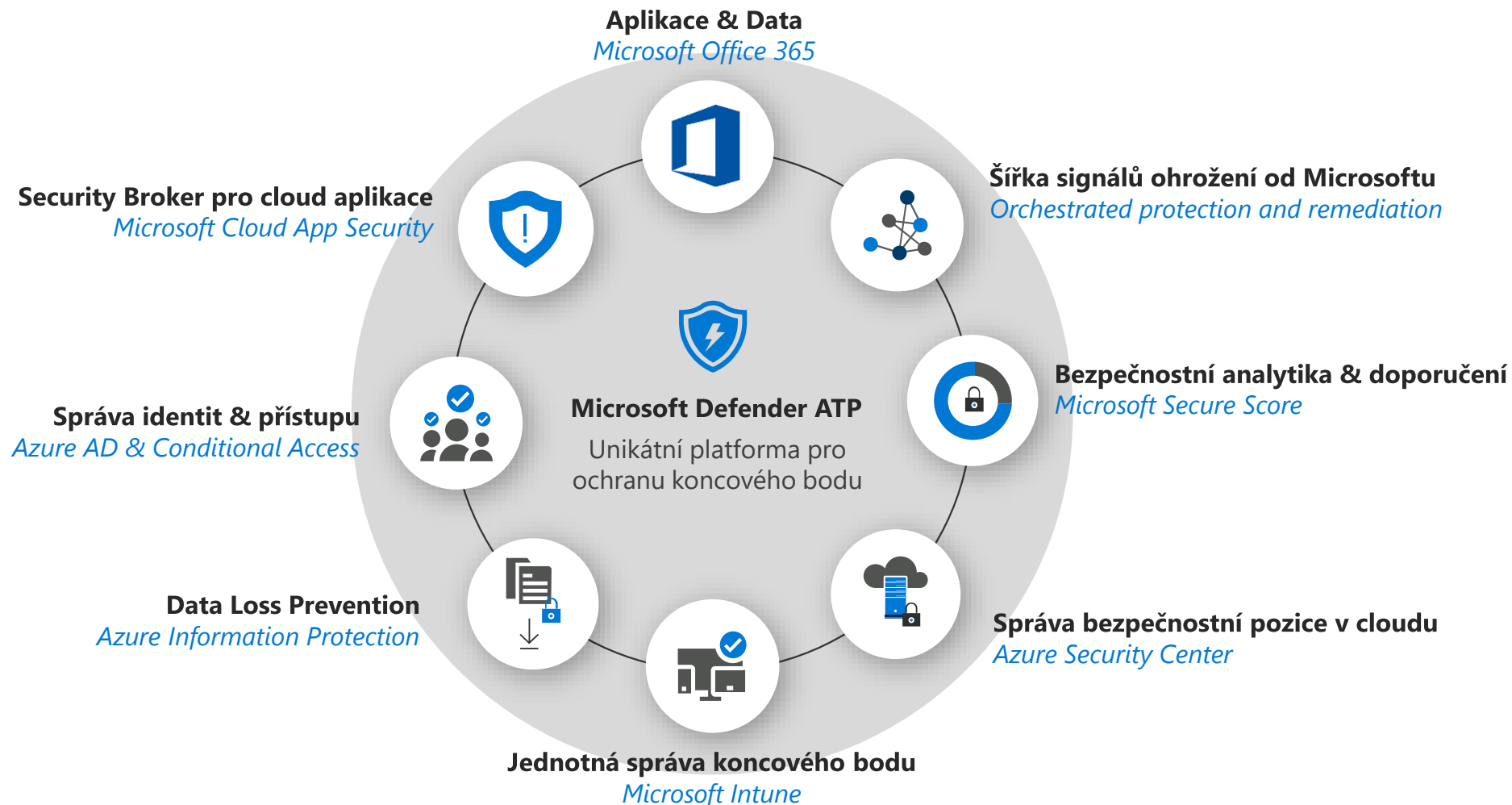
Microsoft Cloud App Security

Rozšířená ochrana & podmíněný přístup k jiným cloud aplikacím



Microsoft Defender ATP

Povýšení bezpečnosti ve všech scénářích





Microsoft Defender ATP

Integrovaný. Postaven s cloudem.

IT mu věří. Bezpečnostní týmy jej milují.