Microsoft

Praktický pohled na NIS2

V kontextu čísel z Microsoft Digital Defense Reportu

Tomáš Kantůrek, Microsoft
Michal Haas, Microsoft

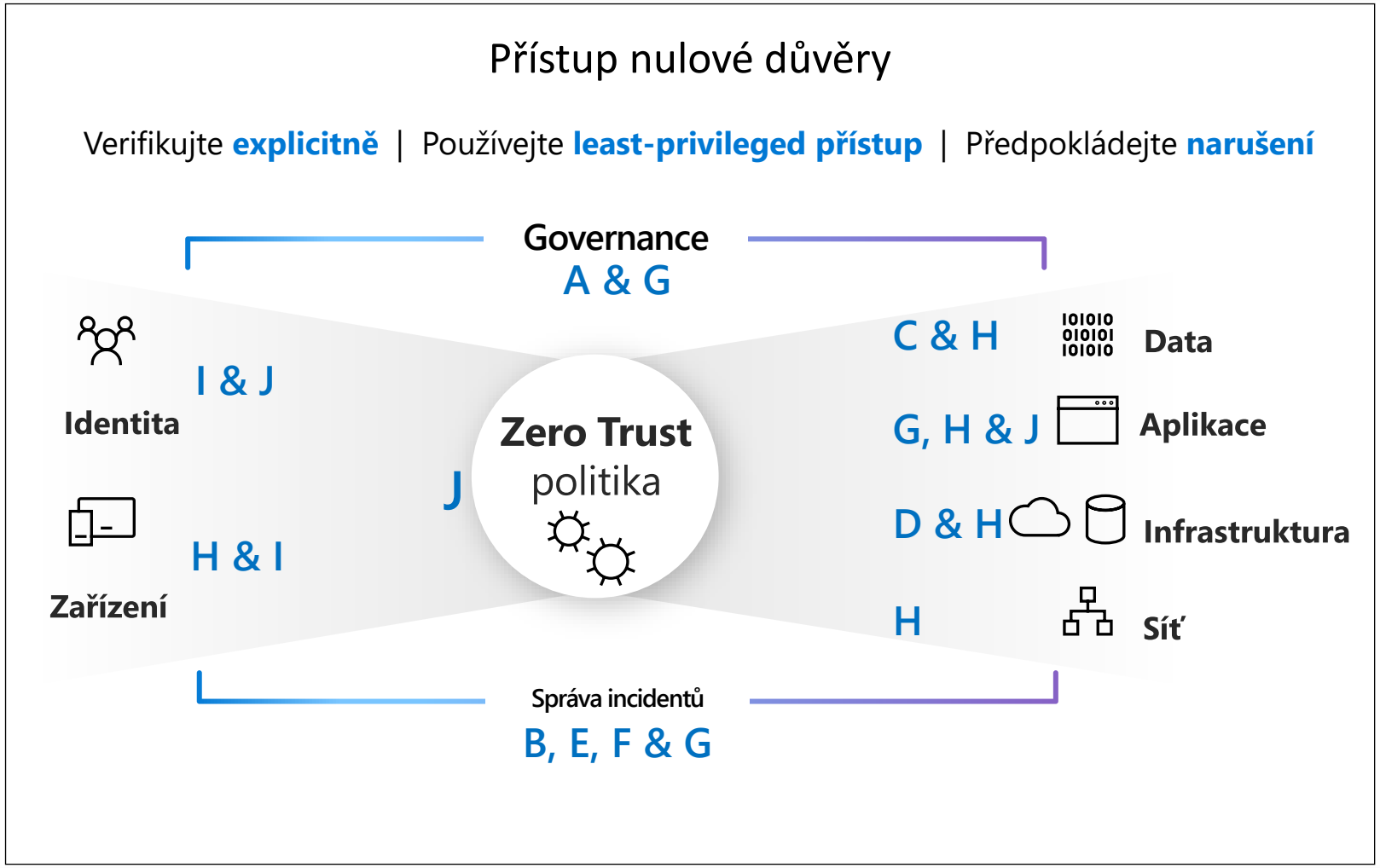
NIS 2 povinnosti

A. Politiky pro analýzy rizik a bezpečnosti informačních systémů;
B. Řešení incidentů;
C. Kontinuita provozu, jako je správa zálohování a zotavení po havárii a krizový management;
D. Bezpečnost dodavatelského řetězce, včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;
E. Bezpečnost při pořizování, vývoji a údržbě sítí a informačních systémů, včetně řešení a odhalování zranitelností;
F. Politiky a postupy pro posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik;
G. Základní postupy kybernetické hygieny a školení kybernetické bezpečnosti;
H. Zásady a postupy týkající se používání kryptografie a případně šifrování;
I. Bezpečnost lidských zdrojů, zásady řízení přístupu a správa aktiv;
J. Použití vícefaktorové autentizace nebo řešení průběžného ověřování, zabezpečené hlasové, obrazové a textové komunikace a zabezpečených systémů tísňové komunikace v rámci subjektu, je-li to vhodné.

NIS2 povinnosti mapují na koncept Zero Trust

NIS 2 povinnosti

A. Politiky pro analýzy rizik a bezpečnosti informačních systémů;
B. Řešení incidentů;
C. Kontinuita provozu, jako je správa zálohování a zotavení po havárii a krizový management;
D. Bezpečnost dodavatelského řetězce, včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;
E. Bezpečnost při pořizování, vývoji a údržbě sítí a informačních systémů, včetně řešení a odhalování zranitelností;
F. Politiky a postupy pro posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik;
G. Základní postupy kybernetické hygieny a školení kybernetické bezpečnosti;
H. Zásady a postupy týkající se používání kryptografie a případně šifrování;
I. Bezpečnost lidských zdrojů, zásady řízení přístupu a správa aktiv;
J. Použití vícefaktorové autentizace nebo řešení průběžného ověřování, zabezpečené hlasové, obrazové a textové komunikace a zabezpečených systémů tísňové komunikace v rámci subjektu, je-li to vhodné.



Zero Trust je cesta k souladu s NIS2

NIS2 transpozice do vyhlášek (draft)

Režim vyšších povinností

Organizační opatření

§4 Systém řízení bezp. informací
§5 Povinnosti vrcholného vedení
§6 Bezpečnostní role
§7 Řízení bezp. politiky a bezp. dokumentace
§8 Řízení aktiv
§9 Řízení rizik
§10 Řízení dodavatelů
§11 Bezpečnost lidských zdrojů
§12 Řízení změn
§13 Akvizice, vývoj a údržba
§14 Řízení přístupu
§15 Zvládání kybez událostí a incidentů
§16 Řízení kontinuity činností
§17 Audit kybernetické bezpečnosti

Technická opatření

§18 Fyzická bezpečnost
§19 Bezpečnost komunikačních sítí
§20 Správa a ověřování identit
§21 Řízení přístupových oprávnění
§22 Detekce kybernetických bezp. událostí
§23 Zaznamenávání událostí
§24 Vyhodnocování kybez událostí
§25 Aplikační bezpečnost
§26 Kryptografické algoritmy
§27 Zajišťování dostupnosti regulované služby
§28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Režim nižších povinností

Bezpečnostní opatření

§4 Zajišťování kybernetické bezpečnosti
§5 Povinnosti vrcholného vedení
§6 Bezpečnost lidských zdrojů
§7 Řízení kontinuity činností
§8 Řízení přístupu
§9 Řízení identit a jejich oprávnění
§10 Detekce a zaznamenávání kybez událostí
§11 Řešení kybernetických bezp. incidentů
§12 Bezpečnost komunikačních sítí
§13 Aplikační bezpečnost
§14 Kryptografické algoritmy

NIS2 transpozice do vyhlášek (draft)

Režim vyšších povinností

Organizační opatření

§4 Systém řízení bezp. informací
§5 Povinnosti vrcholného vedení
§6 Bezpečnostní role
§7 Řízení bezp. politiky a bezp. dokumentace
§8 Řízení aktiv
§9 Řízení rizik
§10 Řízení dodavatelů
§11 Bezpečnost lidských zdrojů
§12 Řízení změn
§13 Akvizice, vývoj a údržba
§14 Řízení přístupu
§15 Zvládání kybez událostí a incidentů
§16 Řízení kontinuity činností
§17 Audit kybernetické bezpečnosti

Technická opatření

§18 Fyzická bezpečnost
§19 Bezpečnost komunikačních sítí
§20 Správa a ověřování identit
§21 Řízení přístupových oprávnění
§22 Detekce kybernetických bezp. událostí
§23 Zaznamenávání událostí
§24 Vyhodnocování kybez událostí
§25 Aplikační bezpečnost
§26 Kryptografické algoritmy
§27 Zajišťování dostupnosti regulované služby
§28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Microsoft Security

NIS2 transpozice do vyhlášek (draft)

Režim vyšších povinností

Organizační opatření

§4 Systém řízení bezp. informací
§5 Povinnosti vrcholného vedení
§6 Bezpečnostní role
§7 Řízení bezp. politiky a bezp. dokumentace
§8 Řízení aktiv
§9 Řízení rizik
§10 Řízení dodavatelů
§11 Bezpečnost lidských zdrojů
§12 Řízení změn
§13 Akvizice, vývoj a údržba
§14 Řízení přístupu
§15 Zvládání kybez událostí a incidentů
§16 Řízení kontinuity činností
§17 Audit kybernetické bezpečnosti

Technická opatření

§18 Fyzická bezpečnost
§19 Bezpečnost komunikačních sítí
§20 Správa a ověřování identit
§21 Řízení přístupových oprávnění
§22 Detekce kybernetických bezp. událostí
§23 Zaznamenávání událostí
§24 Vyhodnocování kybez událostí
§25 Aplikační bezpečnost
§26 Kryptografické algoritmy
§27 Zajišťování dostupnosti regulované služby
§28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

IDENTITA

Microsoft Security

NIS2 transpozice do vyhlášek (draft)

Režim vyšších povinností

Organizační opatření

§4 Systém řízení bezp. informací
§5 Povinnosti vrcholného vedení
§6 Bezpečnostní role
§7 Řízení bezp. politiky a bezp. dokumentace
§8 Řízení aktiv
§9 Řízení rizik
§10 Řízení dodavatelů
§11 Bezpečnost lidských zdrojů
§12 Řízení změn
§13 Akvizice, vývoj a údržba
§14 Řízení přístupu
§15 Zvládání kybez událostí a incidentů
§16 Řízení kontinuity činností
§17 Audit kybernetické bezpečnosti

Technická opatření

§18 Fyzická bezpečnost
§19 Bezpečnost komunikačních sítí
§20 Správa a ověřování identit
§21 Řízení přístupových oprávnění
§22 Detekce kybernetických bezp. událostí
§23 Zaznamenávání událostí
§24 Vyhodnocování kybez událostí
§25 Aplikační bezpečnost
§26 Kryptografické algoritmy
§27 Zajišťování dostupnosti regulované služby
§28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

AKTIVA

Microsoft Security

NIS2 transpozice do vyhlášek (draft)

Režim vyšších povinností

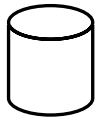
Organizační opatření

§4 Systém řízení bezp. informací
§5 Povinnosti vrcholného vedení
§6 Bezpečnostní role
§7 Řízení bezp. politiky a bezp. dokumentace
§8 Řízení aktiv
§9 Řízení rizik
§10 Řízení dodavatelů
§11 Bezpečnost lidských zdrojů
§12 Řízení změn
§13 Akvizice, vývoj a údržba
§14 Řízení přístupu
§15 Zvládání kybez událostí a incidentů
§16 Řízení kontinuity činností
§17 Audit kybernetické bezpečnosti

Technická opatření

§18 Fyzická bezpečnost
§19 Bezpečnost komunikačních sítí
§20 Správa a ověřování identit
§21 Řízení přístupových oprávnění
§22 Detekce kybernetických bezp. událostí
§23 Zaznamenávání událostí
§24 Vyhodnocování kybez událostí
§25 Aplikační bezpečnost
§26 Kryptografické algoritmy
§27 Zajišťování dostupnosti regulované služby
§28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

DATA



Microsoft Security

NIS2 transpozice do vyhlášek (draft)

Režim vyšších povinností

Organizační opatření

§4 Systém řízení bezp. informací
§5 Povinnosti vrcholného vedení
§6 Bezpečnostní role
§7 Řízení bezp. politiky a bezp. dokumentace
§8 Řízení aktiv
§9 Řízení rizik
§10 Řízení dodavatelů
§11 Bezpečnost lidských zdrojů
§12 Řízení změn
§13 Akvizice, vývoj a údržba
§14 Řízení přístupu
§15 Zvládání kybez událostí a incidentů
§16 Řízení kontinuity činností
§17 Audit kybernetické bezpečnosti

Technická opatření

§18 Fyzická bezpečnost
§19 Bezpečnost komunikačních sítí
§20 Správa a ověřování identit
§21 Řízení přístupových oprávnění
§22 Detekce kybernetických bezp. událostí
§23 Zaznamenávání událostí
§24 Vyhodnocování kybez událostí
§25 Aplikační bezpečnost
§26 Kryptografické algoritmy
§27 Zajišťování dostupnosti regulované služby
§28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

IDENTITA

Microsoft Defender

Microsoft Entra

AKTIVA

Microsoft Defender

Microsoft Intune

DATA

Microsoft Purview

INCIDENTY

Microsoft Defender

Microsoft Sentinel

Microsoft Security

NIS2 zásady mapované na Microsoft řešení

NIS2 zásada	Řešení společnosti Microsoft
Governance	Defender Cloud Security Posture Management (CSPM), Entra, Purview Compliance Manager s hodnotící šablonou NIS2 (hledat“ENISA”) + ISO šablony
Řízení rizika	Defender XDR a Purview Insider Risk Management
Správa aktiv	Defender CSPM, Defender for Endpoint
Dodavatelský řetězec	**Defender XDR**, **Entra** a DevOps, Dynamics Supply Chain Management
Ochrana služeb	Defender for API
Identita a přístup	Entra, Defender for Office 365
Zabezpečení dat	Purview (Information Protection, Data Loss Prevention, Insider Risk Management, Unified Data Governance, Data Lifecycle Management, Records Management), Microsoft 365 backup, Azure Backup, Defender for Office 365, Defender for Cloud Apps
Zabezpečení systému	Defender for Endpoint, Defender for IoT a Intune
Odolné sítě	Azure Network Security včetně integrace 3. strans s hlavními NDR vendory
Informovanost zaměstnanců	Purview Policy Tips, O365 Phishing Simulation a Learning Paths, Security Copilot
Monitorování bezpečnosti, správa incidentů	Microsoft Sentinel, **Security Copilot**
Proaktivní zabezpečení	Defender XDR
Reakce a obnovení	Defender XDR, Azure Backup and Recovery, Purview Data Lifecycle Management a Records Management
Poučení	N/A Open AI

https://www.itgovernance.co.uk/nis-regulations-cyber-assessment-framework

Microsoft Security

Microsoft Digital Defense Report

4 most prevalent attack notifications

Shared by Microsoft Defender Experts

Identity

Identity

Unmanaged Devices

80-90%

of all successful ransomware compromises originate through unmanaged devices.

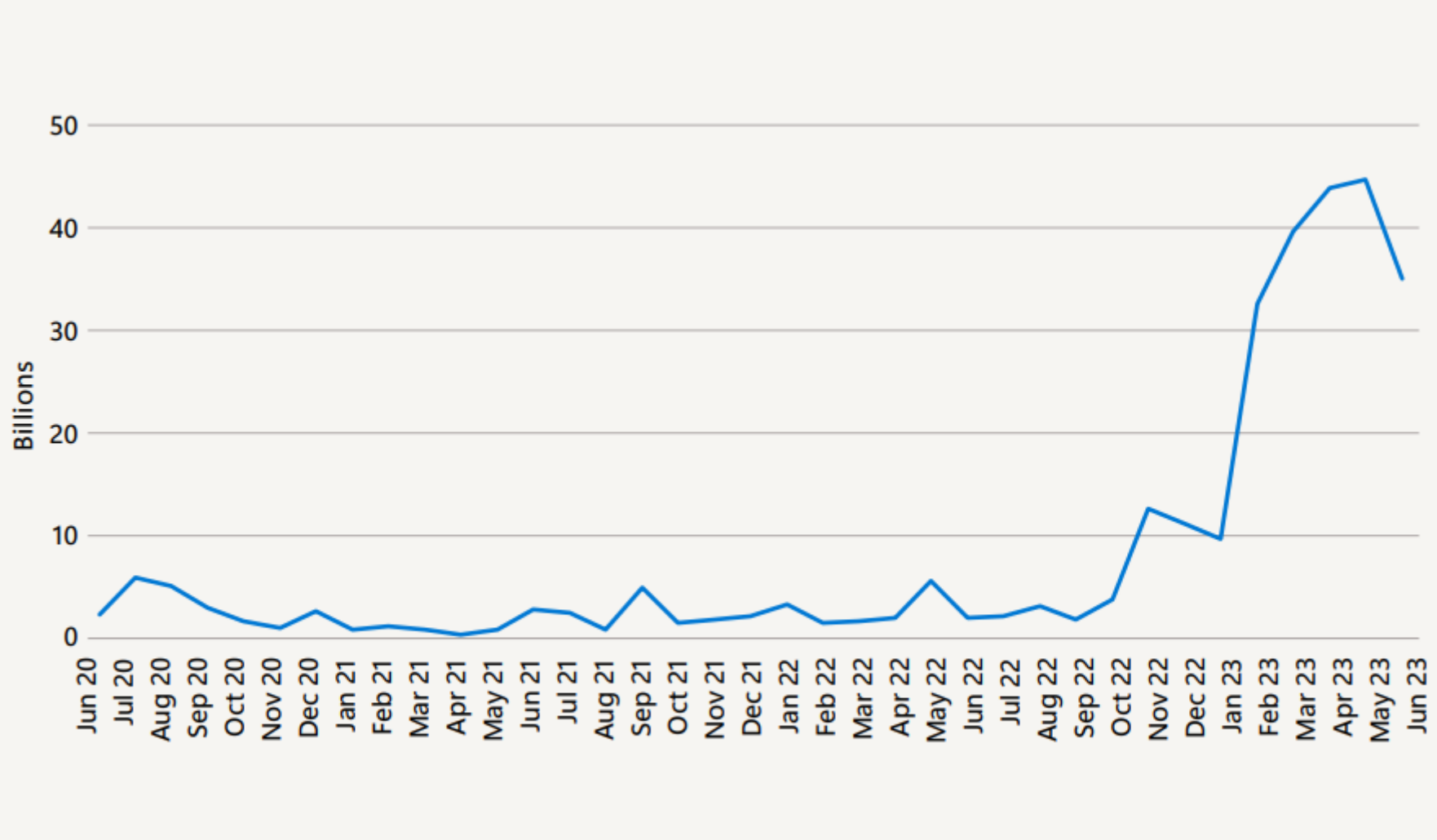
Find out more on page 18

Phishing - AiTM attacks

$200-$1000

Monthly licensing fees paid by cybercriminals to carry out daily phishing campaigns.

Identity Attack Vectors
Password based attacks



How can we protect?

MFA

is one of the (5) key measures directed to be implemented across the federal government.

up to **90%**

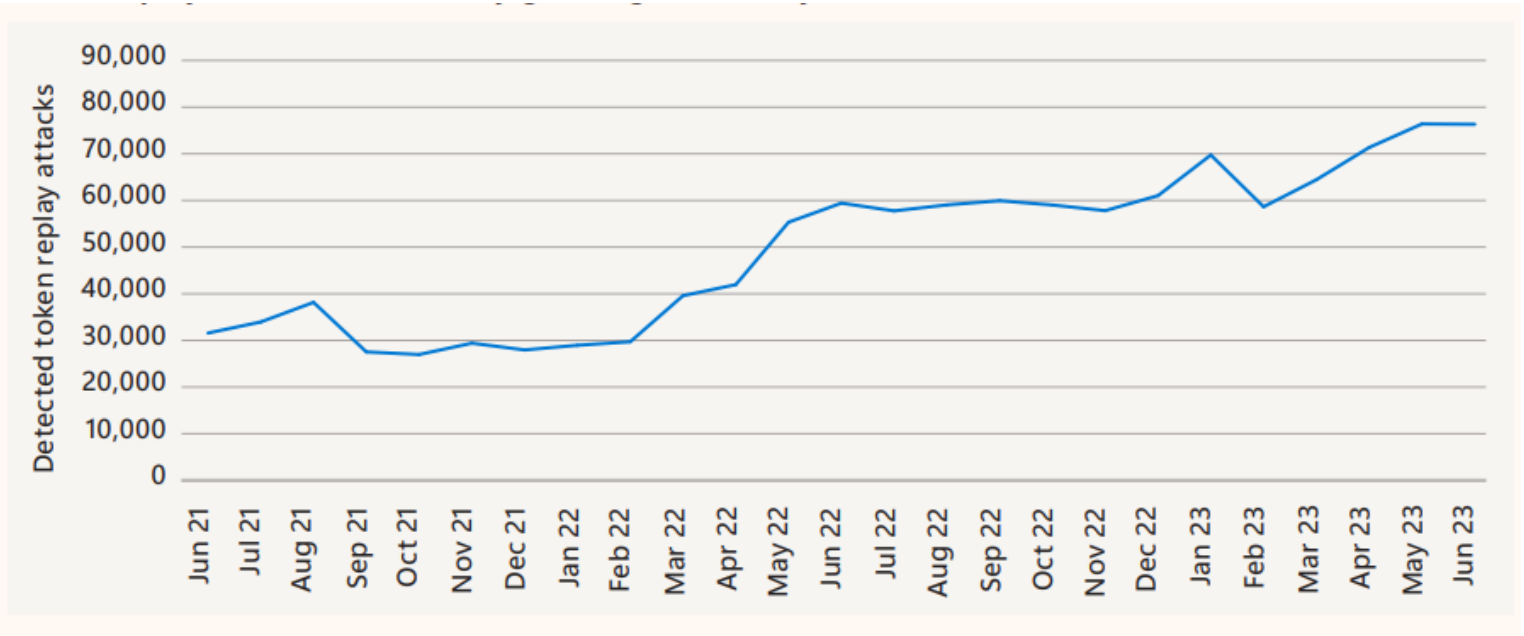
of cyber attacks can be prevented with MFA.

US National Security Cyber Chief, Chris Inglis

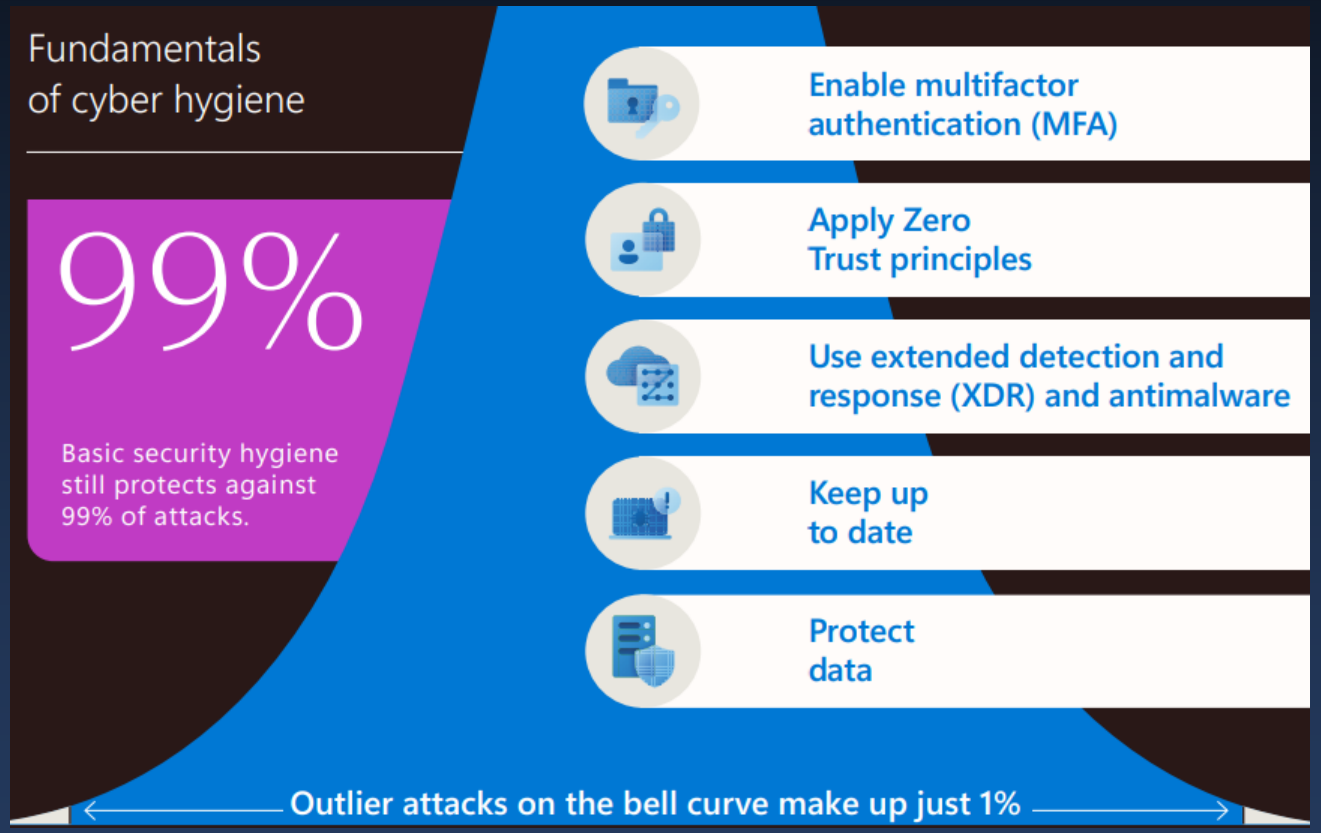
99.9%

of automated attacks on Microsoft platforms, websites and other online services can be blocked by MFA.

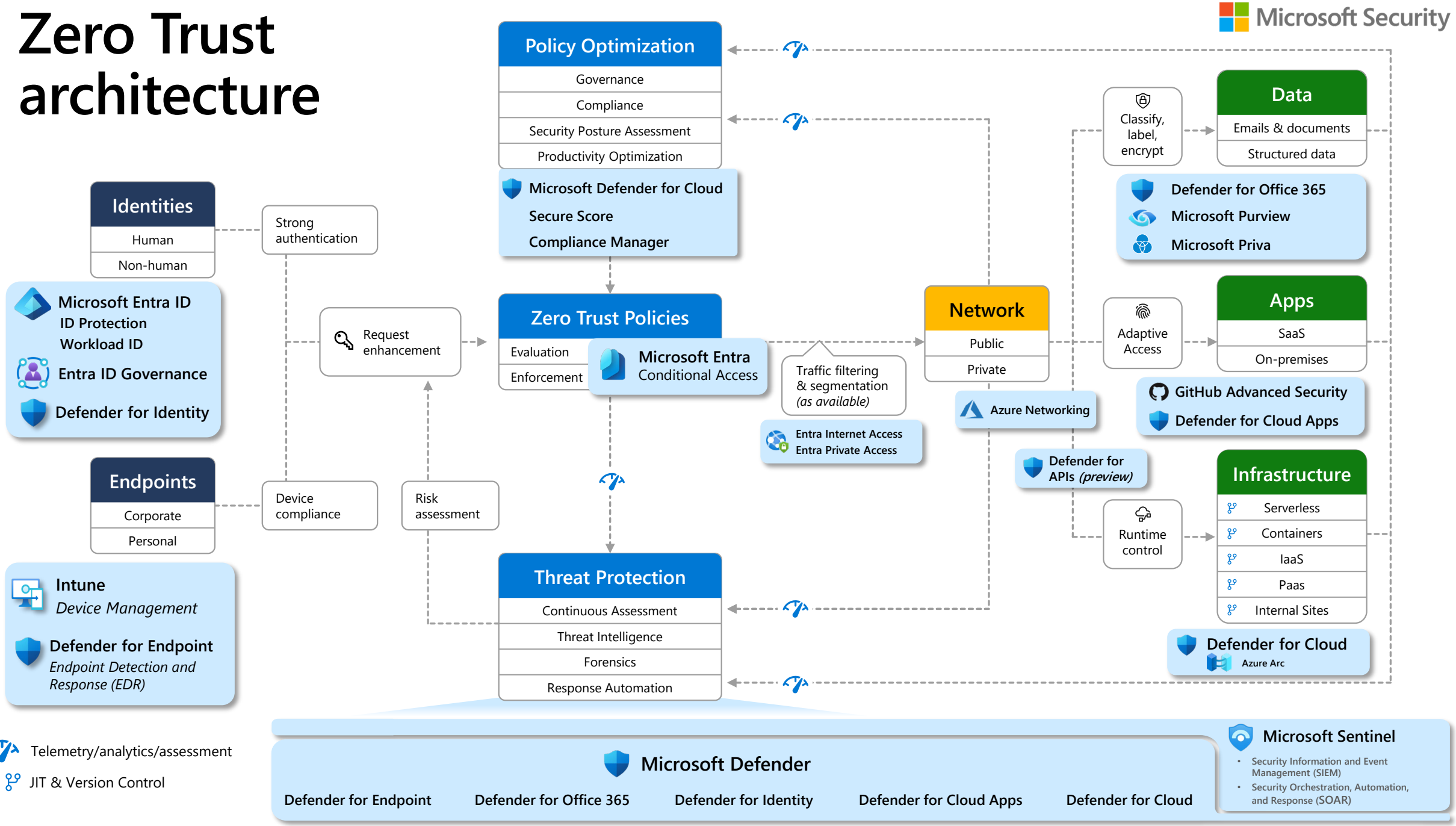
Identity Attack Vectors
Token Replay Attacks



How can we protect?



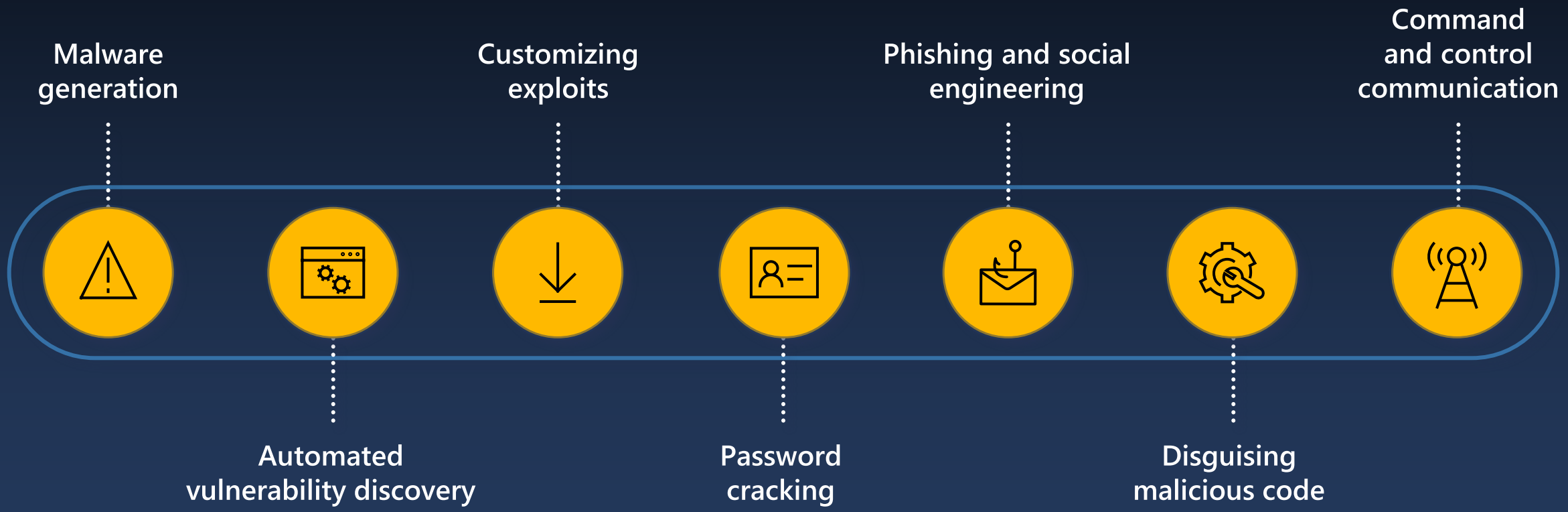
Zero Trust architecture



Can generative AI empower attackers?

What to expect from adversaries

AI-empowered attacks



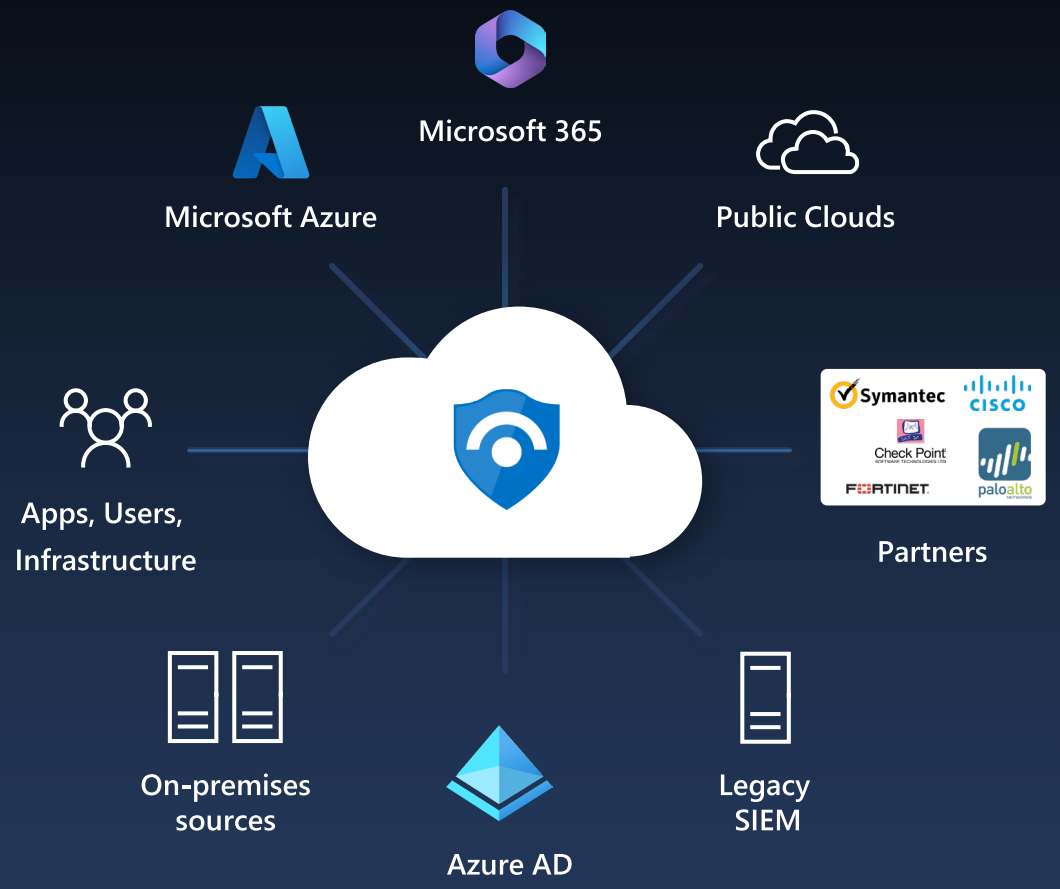

18:58
Umělá inteligence - AI, ChatGPT, OpenAI - sdílení zkušeností
Pepe Tarico · 6 h ·
KAŽDÝ OBYVATEL ČESKA KTERÝ KOUPÍ BALÍK AKCIÍ ČEZ ZA 6.000 KČ
DOSTANE 70.000 KČ MĚSÍČNĚ
6 h To se mi líbí Odpovědět 16
Václav Šik
No je to dost nebezpečný řekl bych.
4 h To se mi líbí Odpovědět 2
Robert Táborský
Je toho všude plno
2 h To se mi líbí Odpovědět 2
Skuna Gee
takhle dlouhou a uplne spisovnou vetu pan Babis nikdy nerekl 🙂 ...okamzite me to hrozne koplo do oka ...
4 h To se mi líbí Odpovědět 1
Ctirad Macháček
Moderátorka mi přišla uvěřitelná, ale v databázi AI chyběla Staroslověnština.
Pravidla
Napište veřejný komentář...
GIF


CNN Prima NEWS

How can AI help us?

Benefits of AI for security

- **Efficiency:** Prioritization and automation
- **Speed:** Ability to understand unique threats in real time
- **Scale:** Ability to process large volumes of data



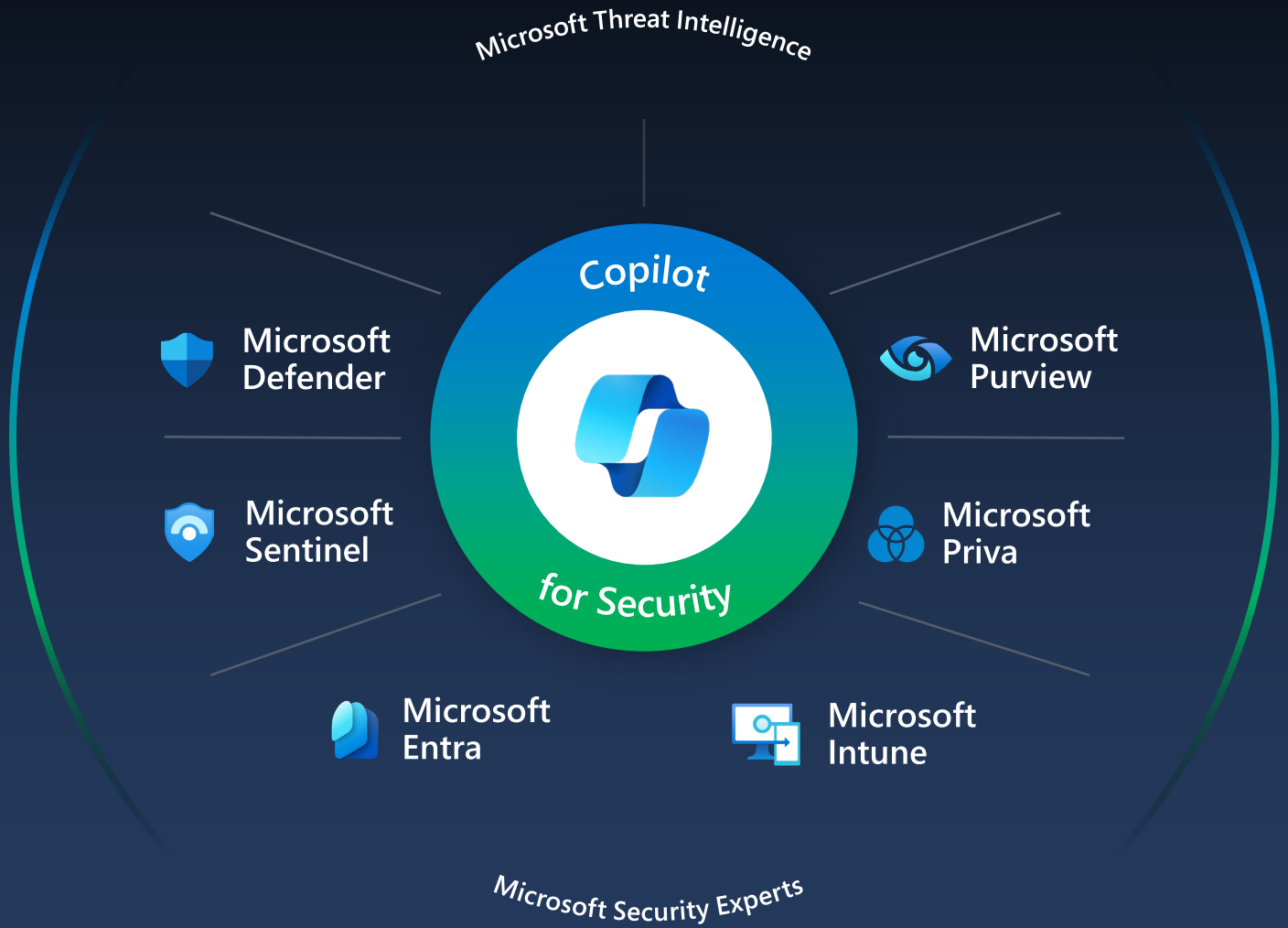
The Microsoft Sentinel platform has more than 10 petabytes of daily ingestion

Microsoft Security

Copilot for Security

Protect at the speed and scale of AI

Microsoft's End-to-End Security



Use cases

Primary use cases

Incident summarization

Impact analysis

Reverse engineering of scripts

Guided response

Additional use cases

Device management, identity management, data security and compliance, cloud security, threat hunting, security posture management, security reporting, and threat intelligence research

Microsoft Security

Děkujeme za pozornost