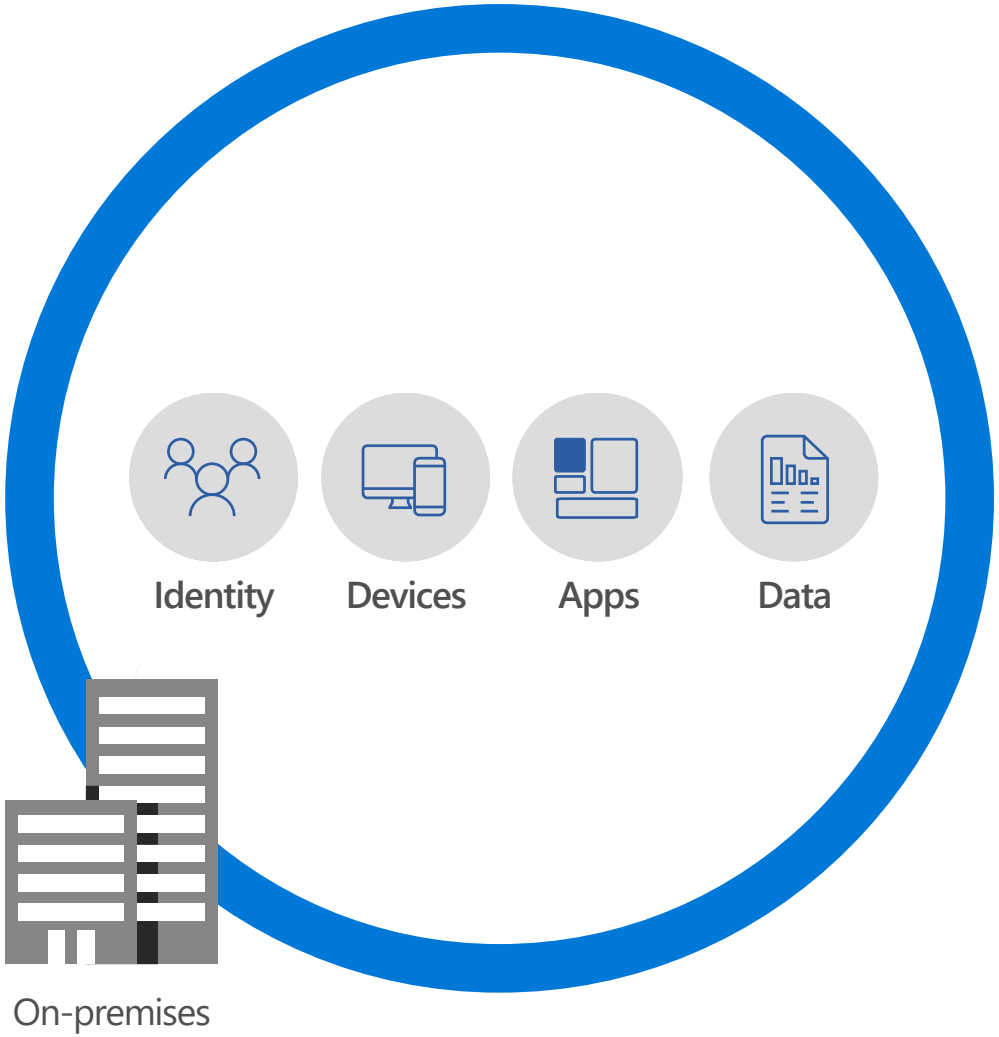
Microsoft

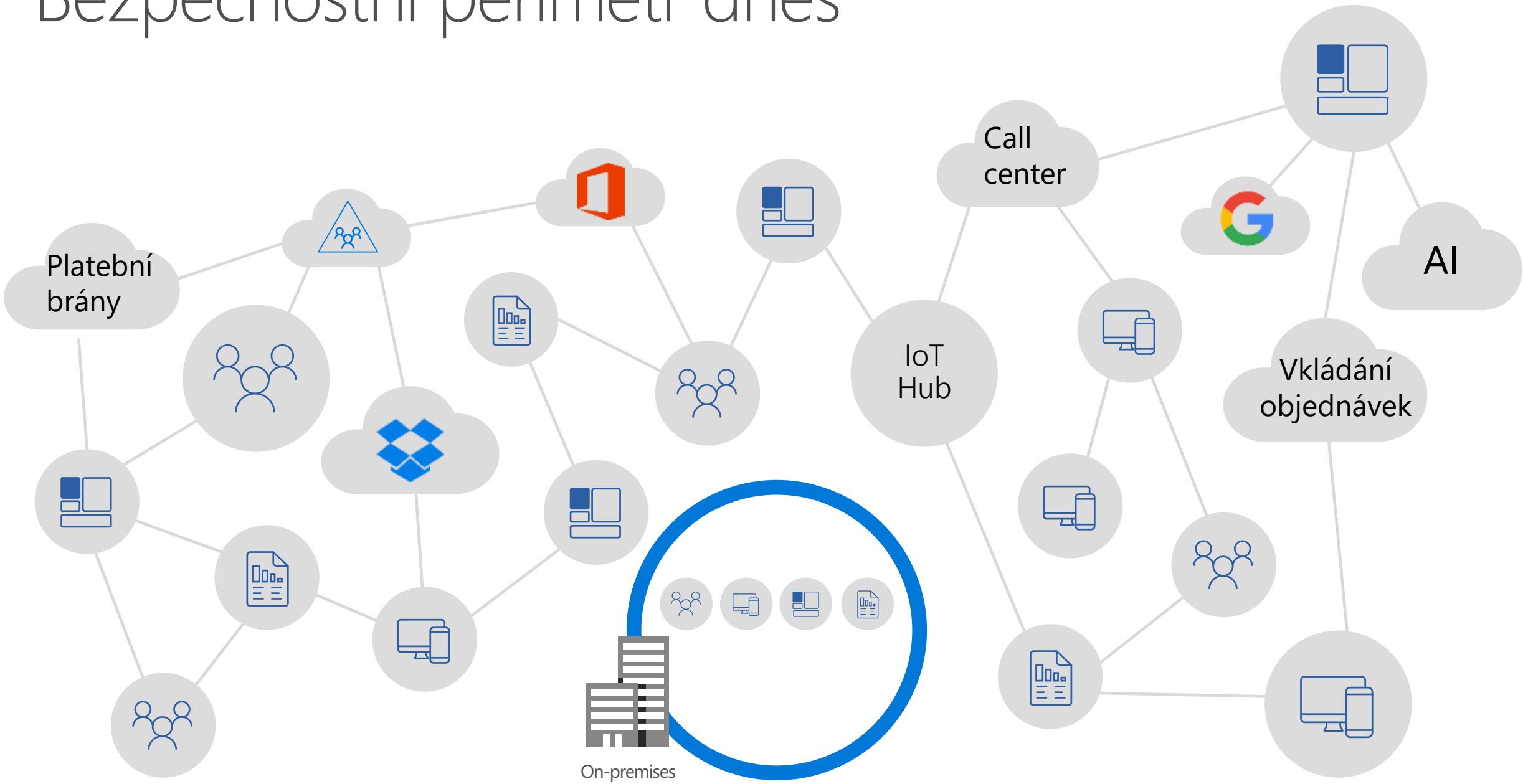
Využití cloud AI pro zmírnění pokročilých hrozeb v kritické informační infrastruktuře (KII)

Ing. Zdeněk Jiříček
National Technology Officer, Microsoft CZ/SK

Bezpečnostní perimetr se mění



Bezpečnostní perimetr dnes



CO MÁ ZAJISTIT IT PLATFORMA

Identity & Access Management
Řízení přístupu na základě rizika

Threat Protection
Ochrana před pokročilými hrozbami a automatizovaná detekce / zotavení

Information Protection
Řízení přístupu a ochrana aktiv

Security Management
Viditelnost a hodnocení hrozeb vs. zranitelností v reálném čase

Do jaké míry dokážeme řídit rizika přístupu k aktivům?

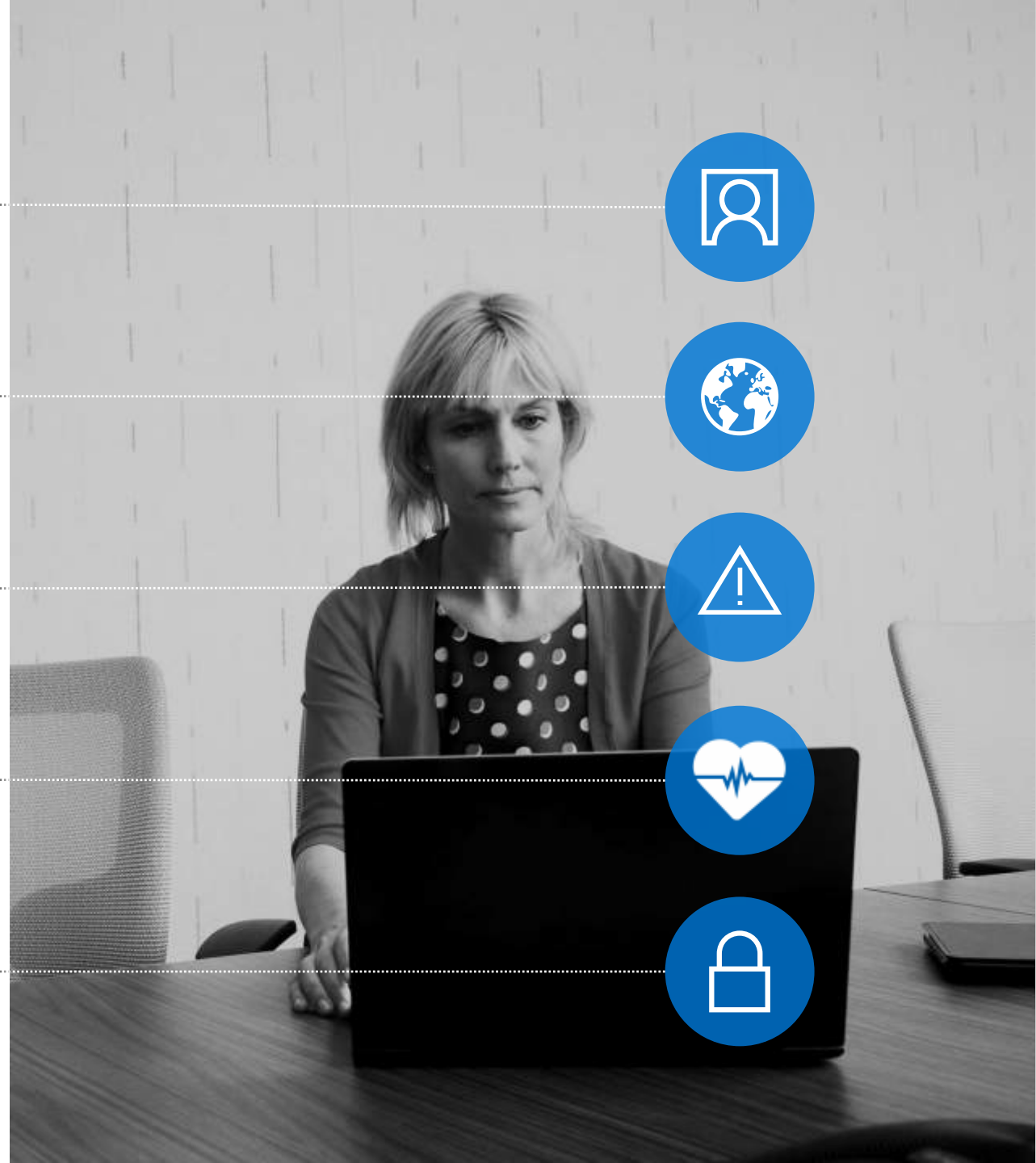
Víme, kdo skutečně žádá o přístup do systému?

Odkud se uživatel přihlašuje? Lokalita? Je to anonymní IP adresa?

K jakým aktivům má přistoupit? Jaké je jejich hodnocení dopadu?

Z jakého zařízení přistupuje? Je managed? Známe jeho „health status“?

Mají aktiva dodatečnou metodu autentizace a autorizace?



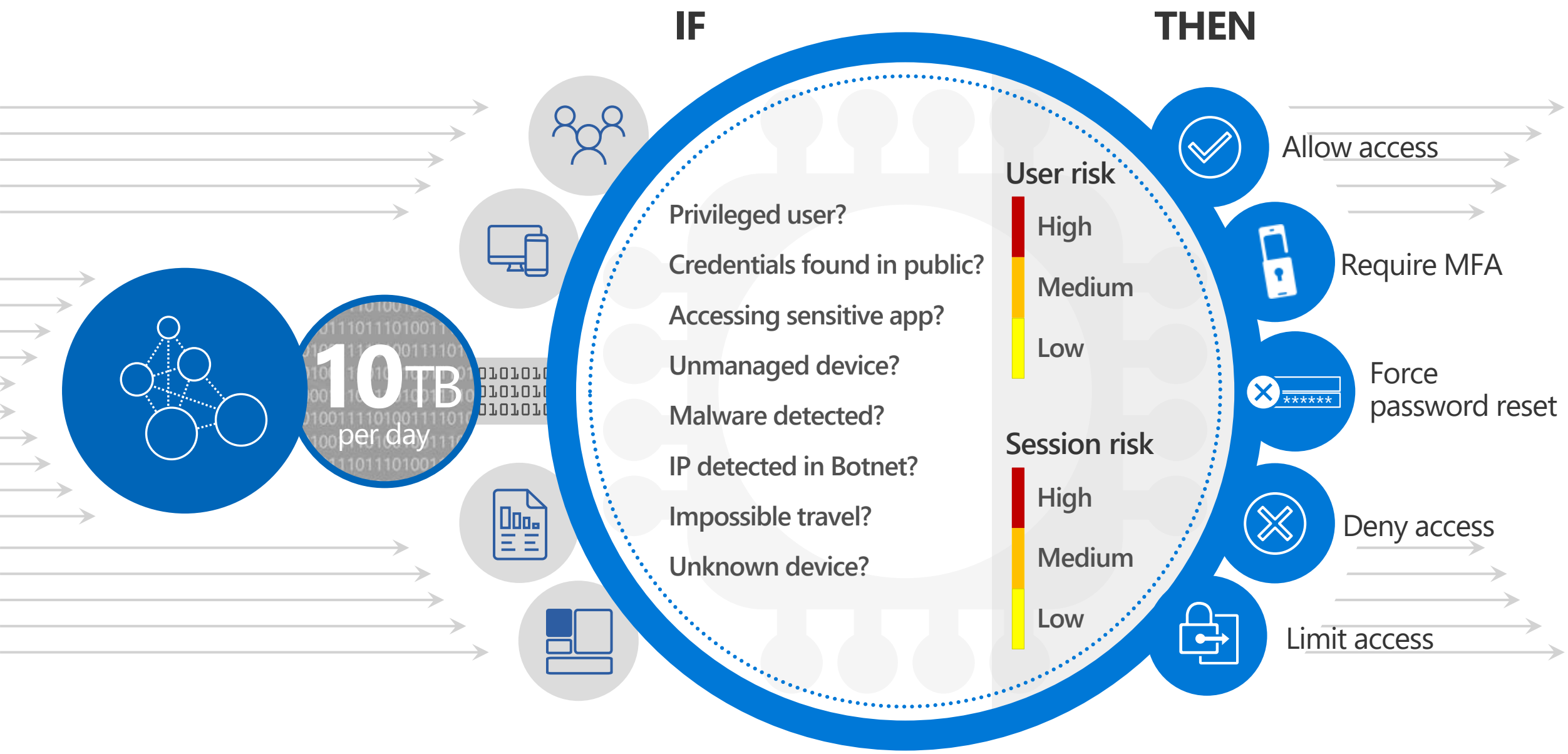
Dokážeme se obejít bez hesel?

Kombinace biometriky / PIN s TPM čipem konkrétního zařízení

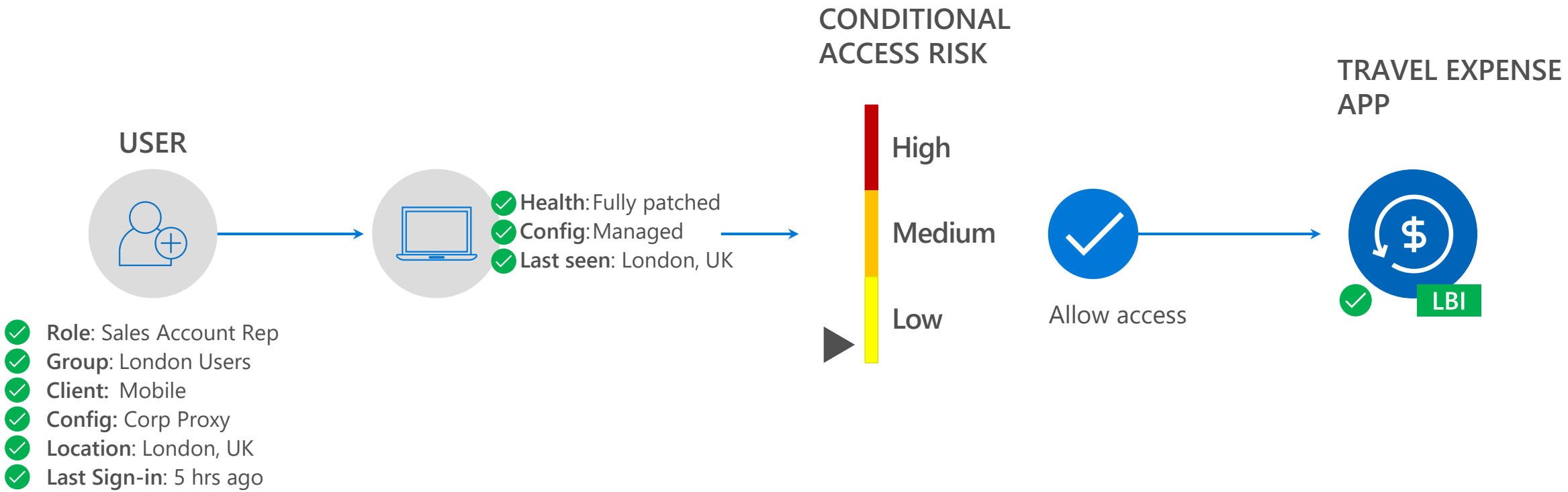
Windows Hello

Microsoft Authenticator

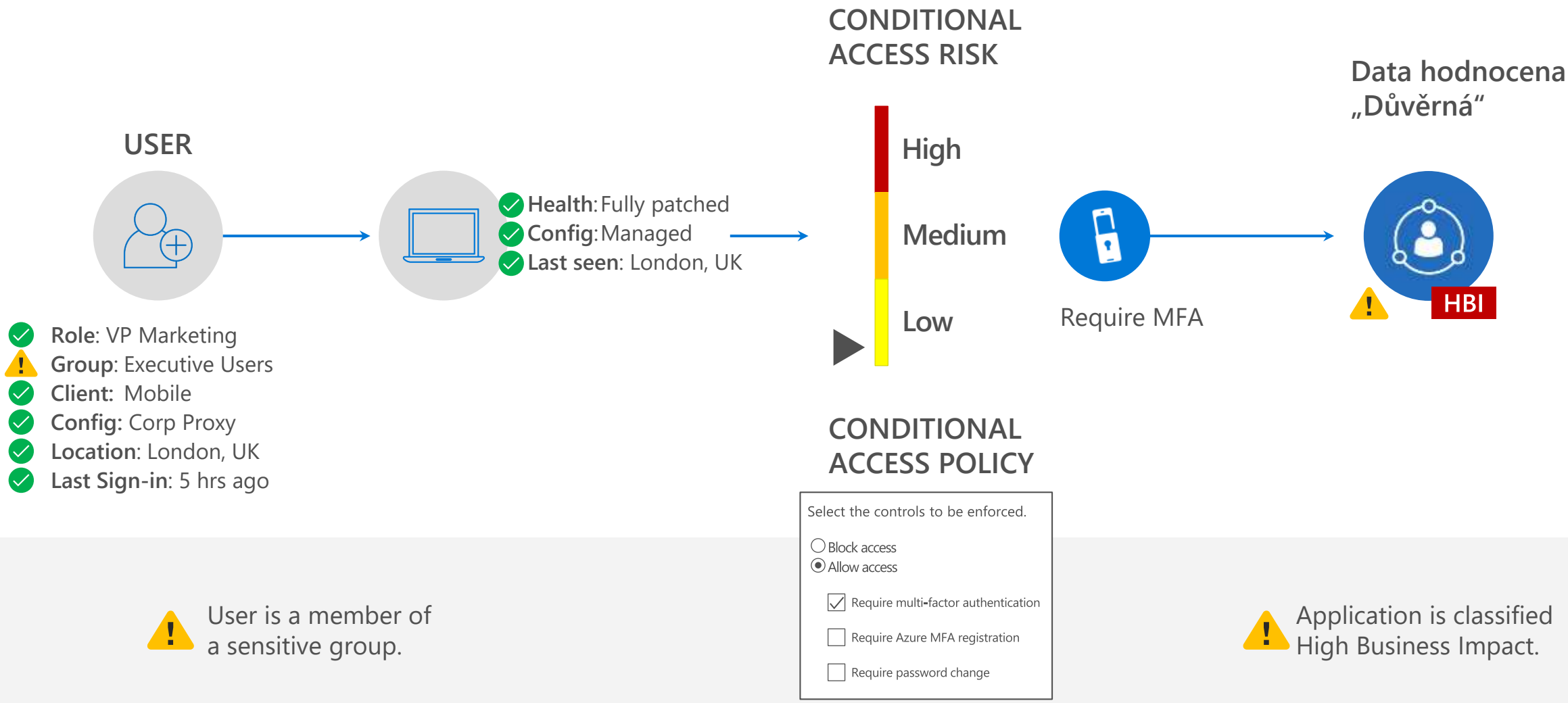
FIDO2 Security Keys


IF
THEN
10TB
per day
Privileged user?
Credentials found in public?
Accessing sensitive app?
Unmanaged device?
Malware detected?
IP detected in Botnet?
Impossible travel?
Unknown device?
User risk
High
Medium
Low
Session risk
High
Medium
Low
Allow access
Require MFA
Force password reset
Deny access
Limit access

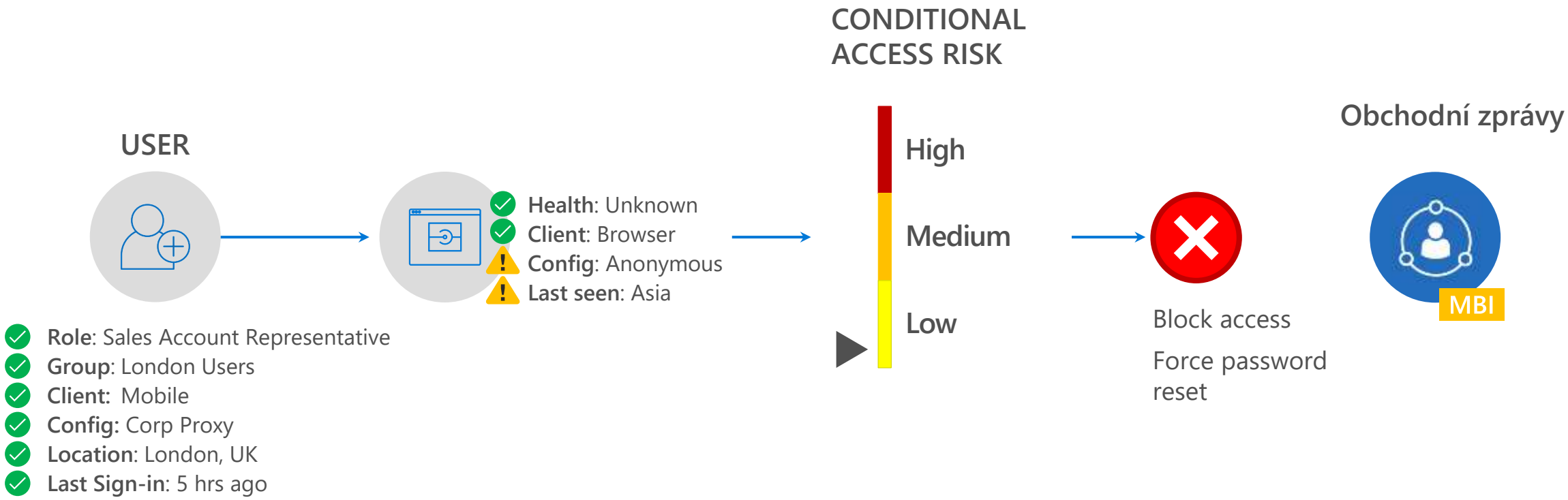
I want to control access based on conditions



I want to control access based on conditions



I want to control access based on conditions



Anonymous IP

Unfamiliar sign-in location for this user

Threat Protection

Ochrana proti moderním hrozbám, automatizovaná detekce, rychlé zotavení

Detekovat útoky kombinací signálů z on-premise i z cloudu

Endpoint monitoring: schopnost uvést do stavu karantény pro vyšetřování, případně dálkově smazat data

Advanced Threat Protection v emailu proti phishingovým útokům a zranitelnostem 0-Day

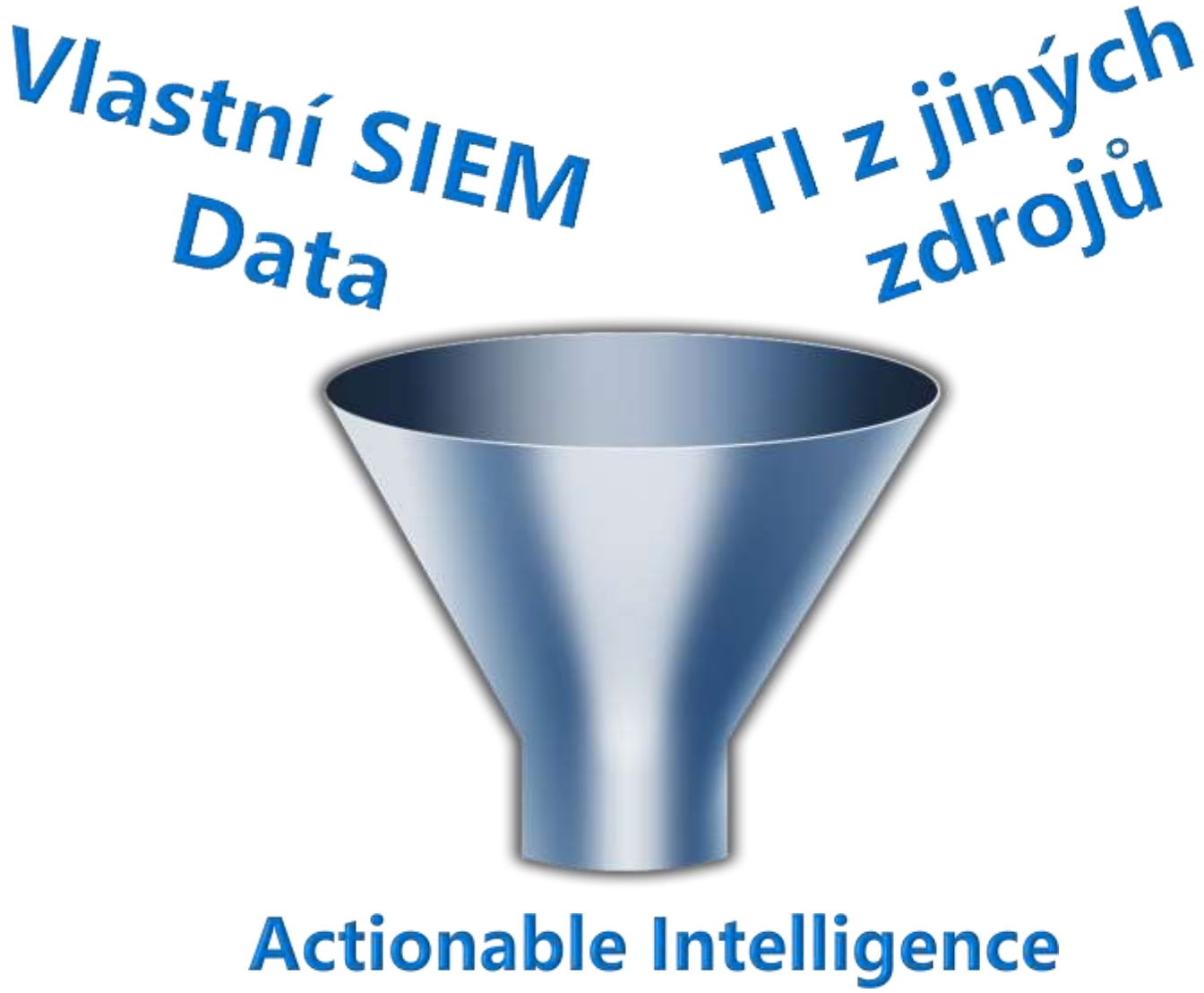
Automatické vyšetření alertů na zařízeních, dálková mitigace hrozby na napadených stanicích

Detekovat a odstranit ransomware, obnovit sooubory

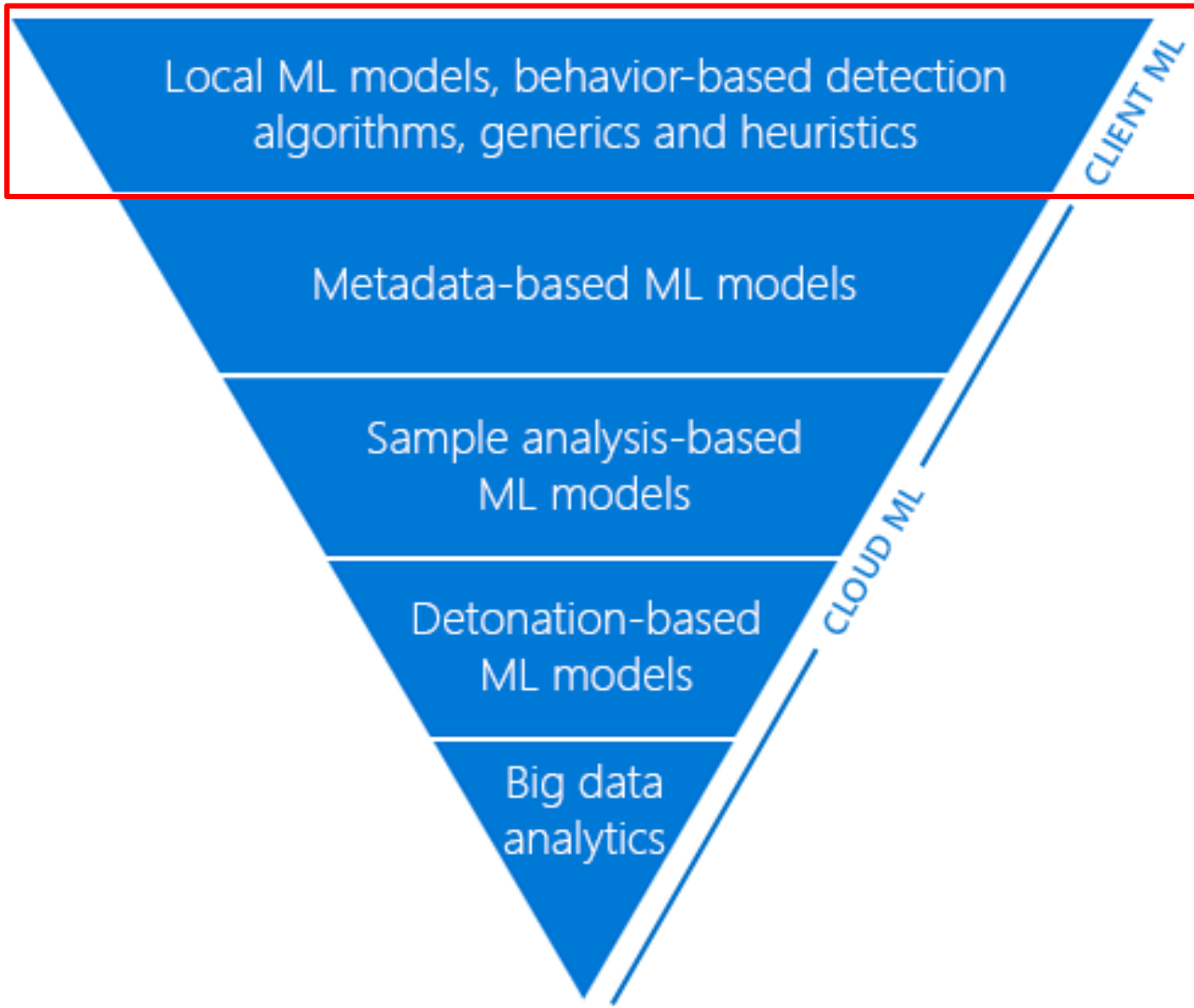
Automaticky detekovat anomálie a podezřelé chování s využitím **AI** – samoučících mechanismů

Snížit false positives agregováním signálů a nalezením konkrétního vektoru útoku

Účinnost využití Threat Intelligence ve firmě?



Vrstvená ochrana: klientské zařízení + cloud



Protection in milliseconds
Most common malware are blocked by high-precision detection in Windows Defender AV

Protection in milliseconds
ML-powered cloud rules evaluate suspicious files based on metadata sent by the Windows Defender AV client during query

Protection in seconds
A copy of the suspicious file is uploaded for inspection by multi-class ML classifiers

Protection in minutes
The suspicious file is executed in a sandbox for dynamic analysis by multi-class ML classifiers

Protection in hours
ML models and expert rules correlated signals from a vast network of sensors to automatically classify threats

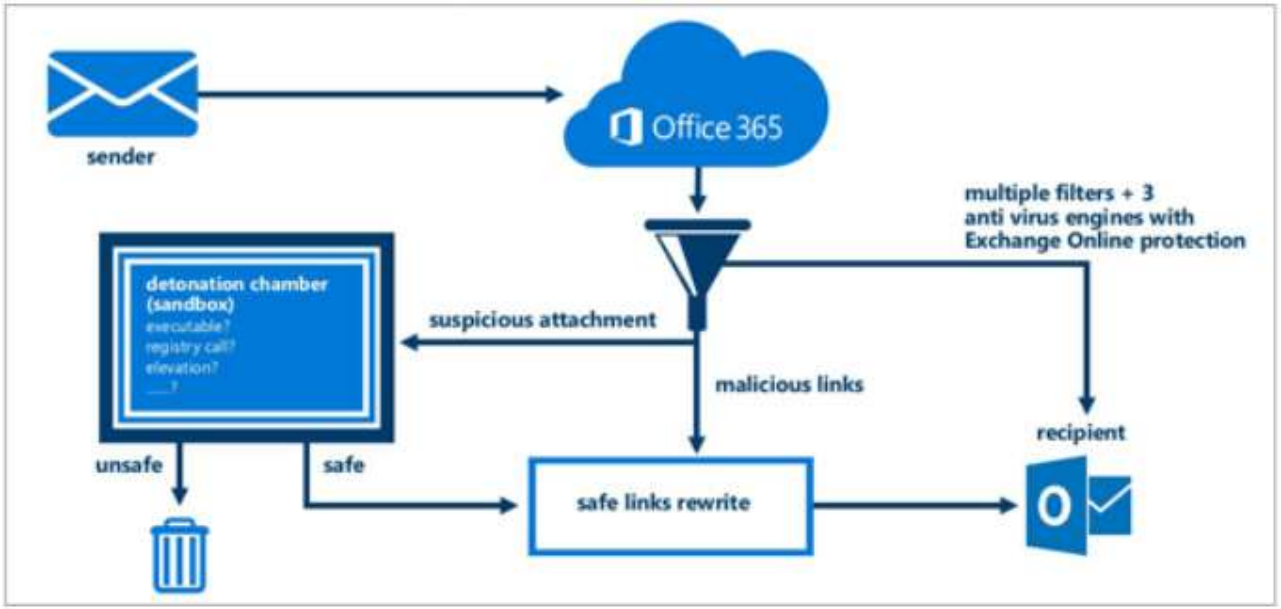
Exchange Online Advanced Threat Protection

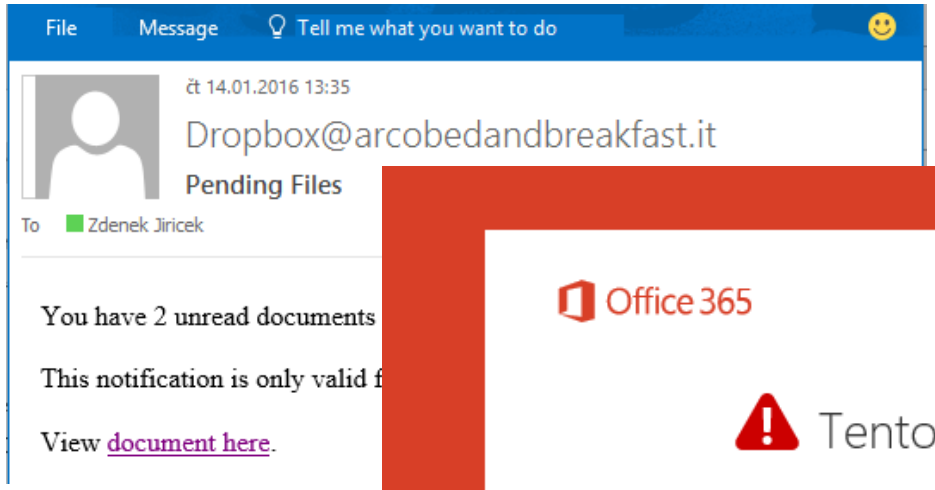
Safe Attachments

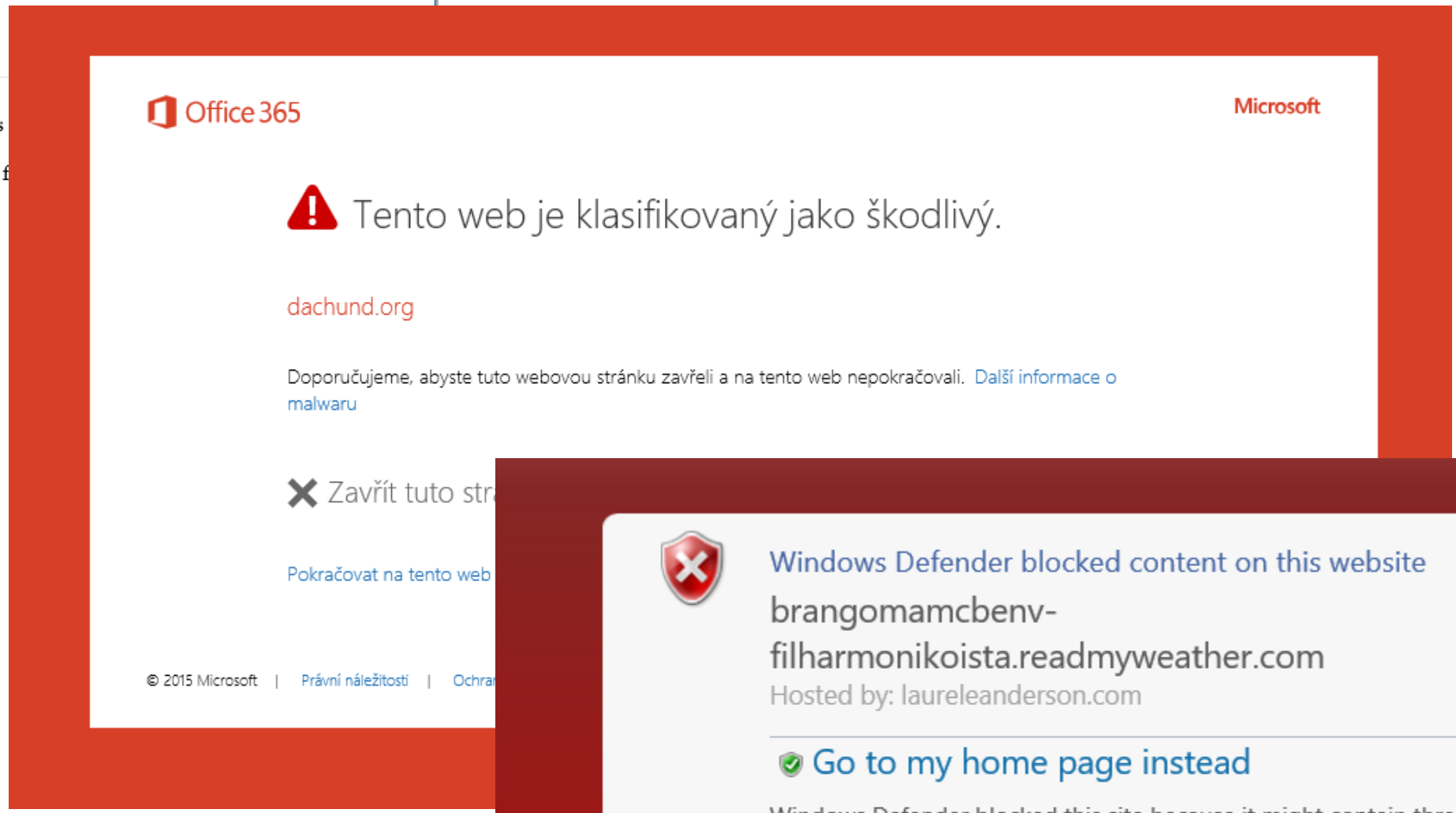
- Sandboxing příloh a test jejich chování
- Ochrana i před 0-day útoky

Safe Links

- Aktivuje URL přes dočasný proxy server
- Reputační databáze > 1 mil. URL linků




File
Message
Tell me what you want to do
čt 14.01.2016 13:35
Dropbox@arcobedandbreakfast.it
Pending Files
To
Zdenek Jiricek
You have 2 unread documents
This notification is only valid f
View document here.


Office 365
Microsoft
Tento web je klasifikovaný jako škodlivý.
dachund.org
Doporučujeme, abyste tuto webovou stránku zavřeli a na tento web nepokračovali. Další informace o malwaru
Zavřít tuto str
Pokračovat na tento web
© 2015 Microsoft | Právní náležitosti | Ochra

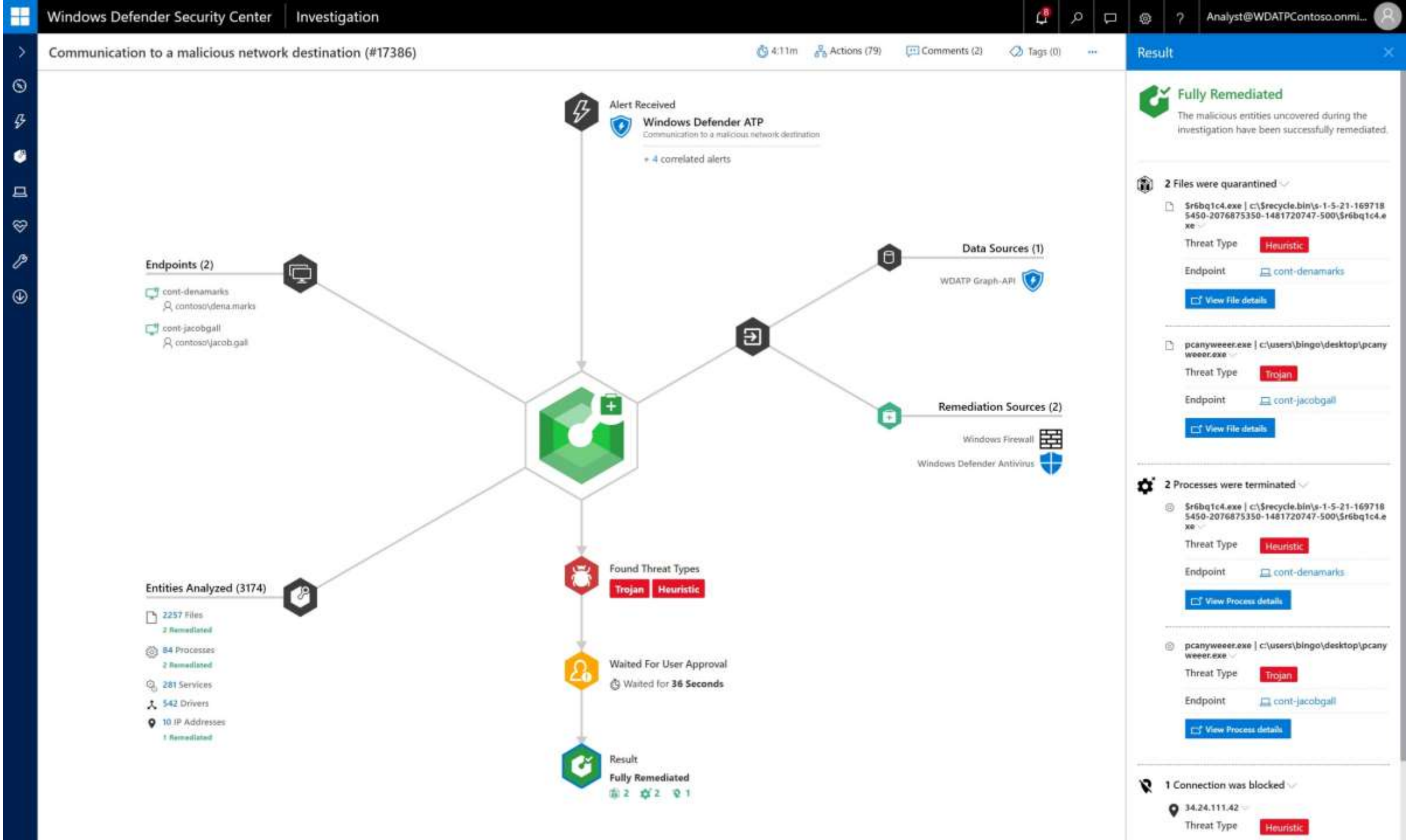
Windows Defender blocked content on this website
brangomamcbenv-filharmonikoista.readmyweather.com
Hosted by: laureleanderson.com
Go to my home page instead
Windows Defender blocked this site because it might contain threats to your PC or your privacy.

Co to je Win Defender ATP Auto-Incident Response?

- Auto-IR je:

  Napodobení ideálních kroků, které by člověk měl udělat **k vyšetření a zvládání** kyber hrozeb

- Co takové kroky jsou:
  - Analýza informací z alertu a korelace s jinými hlášeními
  - Mitigace hrozby / zranitelnosti
  - Určení rozsahu a analýza hrozby „lateral movement“
  - Opakování výše uvedeného pro každý další alert


Windows Defender Security Center
Investigation
Analyst@WDATPContoso.onmi...
Communication to a malicious network destination (#17386)
4:11m
Actions (79)
Comments (2)
Tags (0)
Alert Received
Windows Defender ATP
Communication to a malicious network destination
+ 4 correlated alerts
Endpoints (2)
cont-denamarks
contoso\dena.marks
cont-jacobgall
contoso\jacob.gall
Data Sources (1)
WDATP Graph-API
Remediation Sources (2)
Windows Firewall
Windows Defender Antivirus
Entities Analyzed (3174)
2257 Files
2 Remediated
84 Processes
2 Remediated
281 Services
542 Drivers
10 IP Addresses
1 Remediated
Found Threat Types
Trojan
Heuristic
Waited For User Approval
Waited for 36 Seconds
Result
Fully Remediated
2 2 1
Result
Fully Remediated
The malicious entities uncovered during the investigation have been successfully remediated.
2 Files were quarantined
$r6bq1c4.exe | c:\$recycle.bin\s-1-5-21-1697185450-2076875350-1481720747-500\$r6bq1c4.exe
Threat Type
Heuristic
Endpoint
cont-denamarks
View File details
pcanyweeer.exe | c:\users\bingo\desktop\pcanyweeer.exe
Threat Type
Trojan
Endpoint
cont-jacobgall
View File details
2 Processes were terminated
$r6bq1c4.exe | c:\$recycle.bin\s-1-5-21-1697185450-2076875350-1481720747-500\$r6bq1c4.exe
Threat Type
Heuristic
Endpoint
cont-denamarks
View Process details
pcanyweeer.exe | c:\users\bingo\desktop\pcanyweeer.exe
Threat Type
Trojan
Endpoint
cont-jacobgall
View Process details
1 Connection was blocked
34.24.111.42
Threat Type
Heuristic

Microsoft 365 Admin

https://protection.microsoft.com

Microsoft 365 Advanced Threat Protection

Dan Smith

Security dashboard

Attention required

10736 — In progress
Golden ticket compromise: user permissions mismatch
Windows Defender ATP
Azure ATP
12:05 PM

10654 — In progress
Compromised mailbox
Azure ATP
Office ATP
Windows Defender ATP
11:54 PM

10736 — Pending user action
Suspicious behavior by a scripting tool
Windows Defender ATP
01:35 PM

10564 — Pending user action
Attempt to tamper with the Windows Defender ATP sensor
Windows Defender ATP
01:15 PM

10652 — Pending user action
Trusted Installer hijack attempt
Windows Defender ATP
09:25 AM

10574 — Pending user action
Ransomware behavior in file system
Windows Defender ATP
10:35 AM

10483 — Pending user action
Suspicious root certificate installation
Windows Defender ATP
11:45 AM

10376 — Pending user action

Investigations

Investigations statistics

Alerts investigated	95%
Investigations completed	265
Successfully remediated	228
Average pending time	3 H
Average time to remediate	2.5 H
Hours automated	43 H

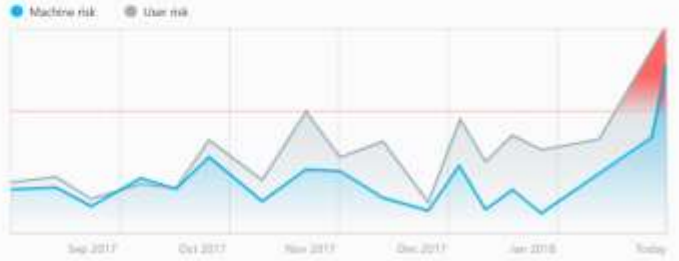
Machines at risk

Machine name	Risk Level	Alerts	User
FIN_SRV_HQ	High	1	Golden FinUser
RDP_SRV_10	Medium	2	Jonathan Wolcot
RDP_SRV_13	Medium	2	Jonathan Wolcot
RDP_SRV_14	Medium	2	Jonathan Wolcot
RDP_SRV_17	Medium	2	Jonathan Wolcot

Users at risk

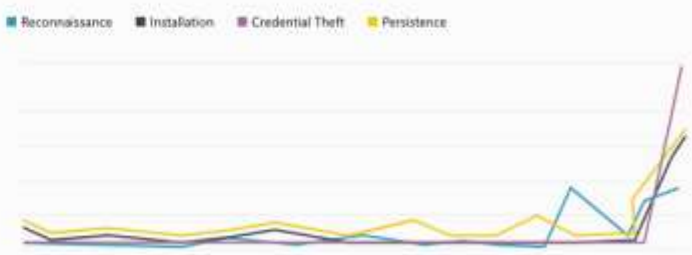
User name	Risk Level	Alerts	Machine
Jonathan Wolcot	High	56	28 machines
Golden FinUser	High	1	FIN_SRV_HQ
Lee Jones	Medium	1	cont-leejones
Michael Gray admin	Low	1	DC_SRV_US
Jon Snow	Low	3	cont-jonsnow

Organization Risk trends



Alerts categroy breakdown

Alerts categroy trends



Type here to search

4:56 PM
7/30/2018

Služba Microsoft Threat Experts (link)

- Je to zákaznický Threat Hunting Service, součást Microsoft Defender Advanced Threat Protection (ATP).
- Poskytuje **zákaznickým SOC** expertní podporu pro **identifikaci, šetření a zvládání** pokročilých hrozeb
- **Targeted attack notifications:** Custom alerty s rychlým vyhodnocením kritických hrozeb v cloudu - timeline, rozsah, způsoby průniku…
- **Experts On Demand:** Na vyžádání SOC zákazníka konzultace s forenzními experty Microsoftu: charakteristika útoku a útočníka, způsob detekce a zotavení.

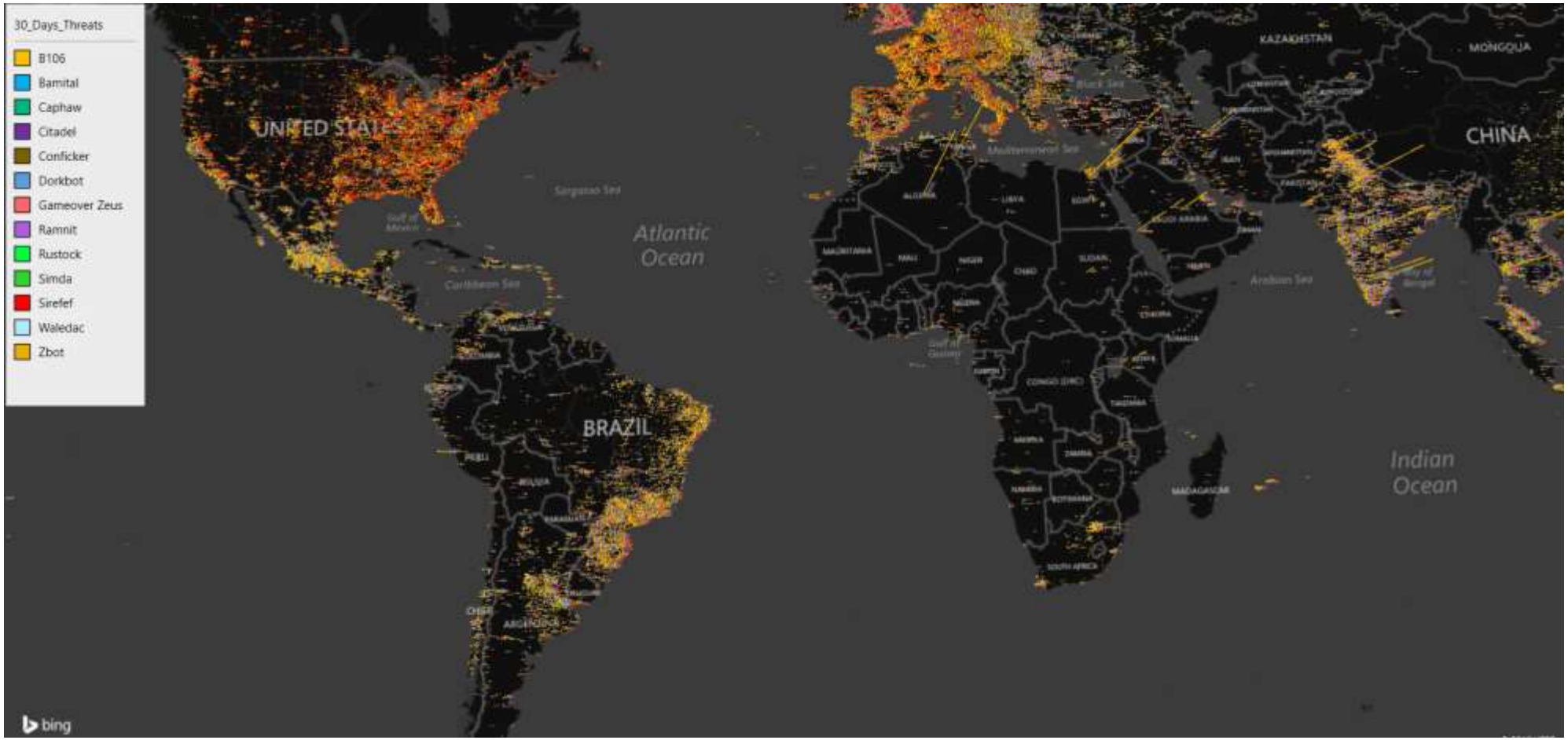
Cyber Threat Intelligence Program

Vyhodnotíme 50-100 milionů podezřelých IP adres denně

300 mil. - 1 mld. připojení denně

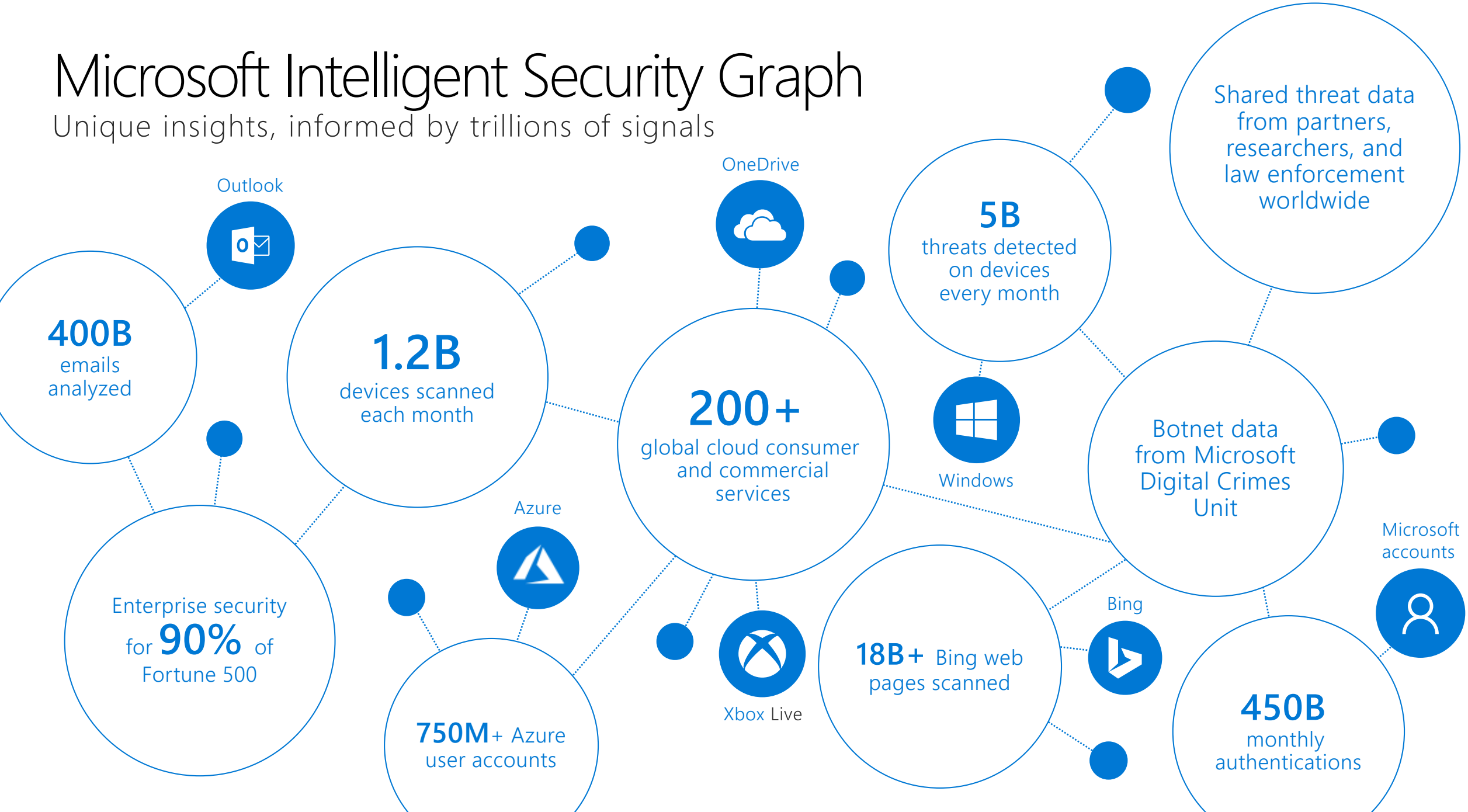
Objem se neustále mění

Actionable Threat Intelligence - data získaná z rozrušených botnetů

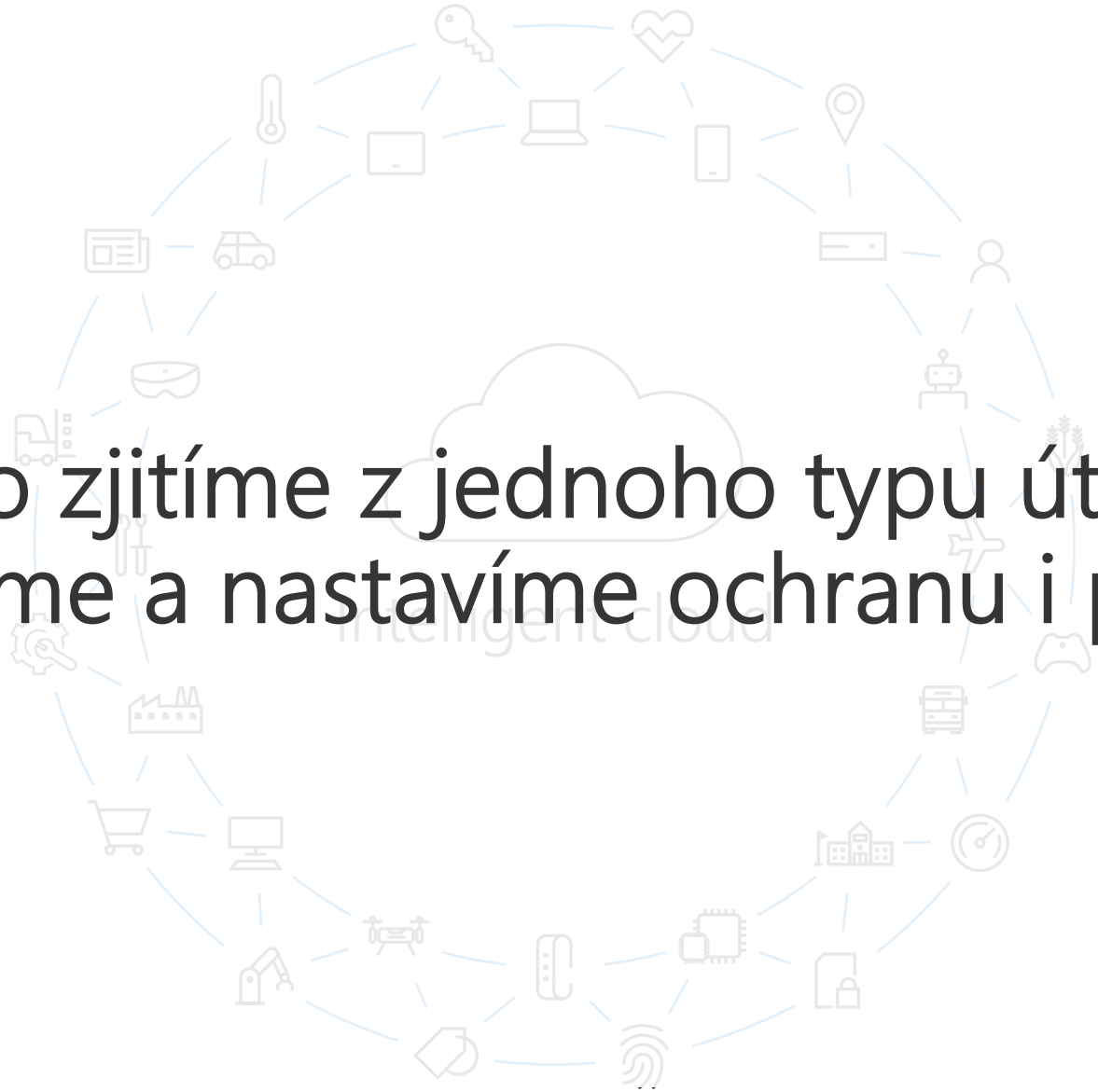


Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



The “Cloud Effect”



Co zjitíme z jednoho typu útoku,
zobecníme a nastavíme ochranu i pro ostatní

Shrnutí

Pokročilým hrozbám se nevyhneme jen prevencí

Kritická infrastruktura je zajímavá jako cíl
pro „state sponsored attacks“

Je to „my nebo oni“ –
AI je nástrojem efektivity útočníka nebo obránce

Automatizace zvládání incidentů a využití
cloud-based intelligence

Děkuji za pozornost!

Zdeněk Jiříček
National Technology Officer
zdenekj@microsoft.com