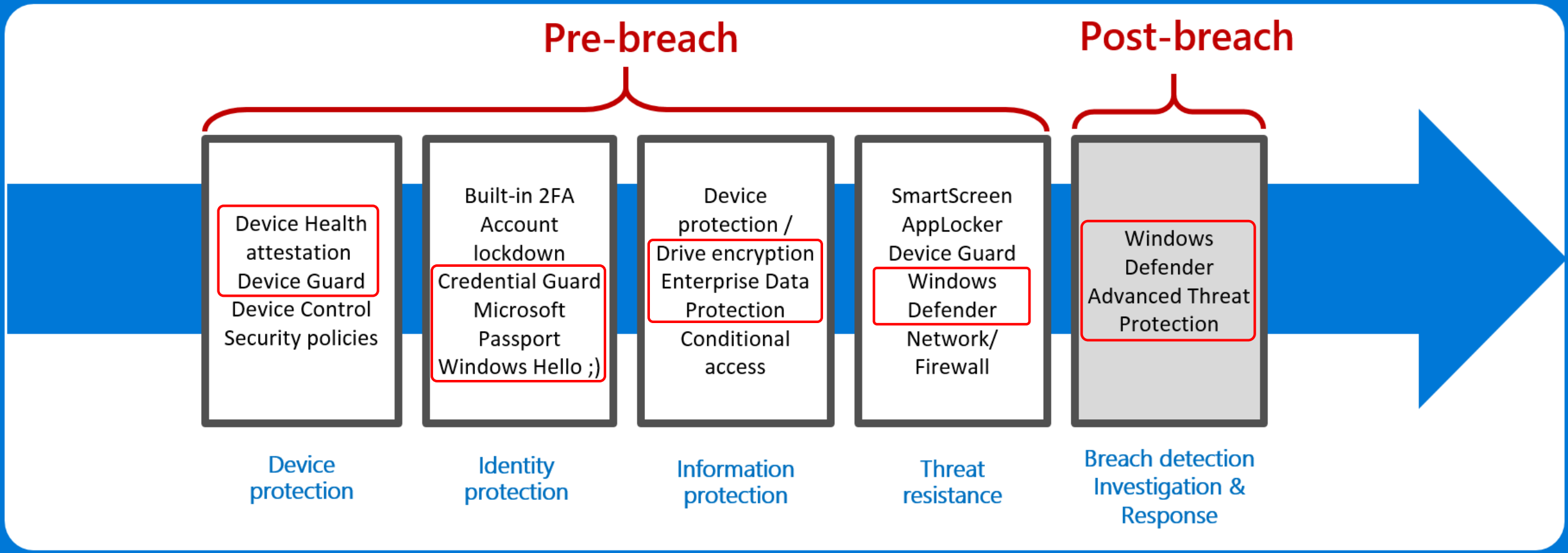
Microsoft

# Novinky v oblasti ochrany aktiv - 2016

Zdeněk Jiříček
National Technology Officer
Microsoft Česká republika

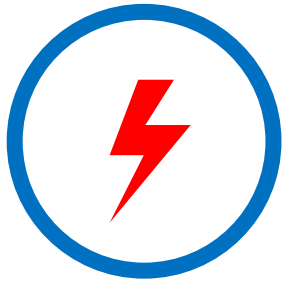
# Windows 10 a investice do zabezpečení




Windows 10

# Windows Defender Advanced Threat Protection

## Pomáhá firemním zákazníkům detekovat, prošetřit a zvládat pokročilé útoky



**Detekuje pokročilé útoky**
Korelace událostí na PC vůči informacím z cloudových senzorů a cloudové analytice hrozeb

**Reakce a prošetření**
Extrahuje signatury k prošetření a poskytne časovou linku bezpečnost. událostí 6 měsíců zpět

**Doporučí jak zvládat útoky**
Komplementární služba k Exchange Online ATP a k AD Advanced Threat Analytics

**V budoucnu:**
Microsoft Threat Intelligence Center – agregovaný výzkum skupin útočníků a způsobů vedení útoků

**Built into** Windows 10

InPrivate | Seville - Dashboard

seville.windows.com

# Windows Security Center | Dashboard

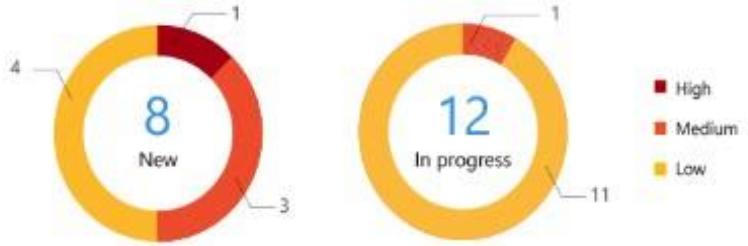
Timezone: UTC | Analyst@SevilleContoso.onmicrosoft.com

- Dashboard
- Alerts Queue
- Machines View

File | Search (File, IP, URL, Machine)

## ATP alerts

All time




### Latest ATP alerts

Go to all alerts

| | | |
|---|---|---|
| Feb 18 18:07:01 | NeroBlaze attack detected | High |
| Feb 18 11:54:02 | Outlook dropped and executed a PE file | Medium |
| Feb 18 14:34:00 | A suspicious Powershell commandline was executed | Medium |
| Feb 18 13:01:09 | A reverse shell was detected | Medium |

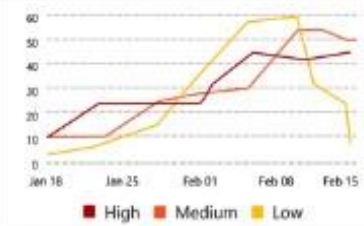
## Top machines with ATP alerts

Go to machine view

| | | | |
|---|---|---|---|
| CONT-LIZBEAN | 1 | 3 | 1 |
| CONT-LILYJARVIS | 0 | 0 | 1 |
| CONT-RODGERANDR | 0 | 0 | 1 |
| CONT-ERICGAYLOR | 0 | 0 | 1 |

## ATP alert trends

30 days




## ATP alerts mapping

30 days

## High severity malware

All time

| | | | |
|---|---|---|---|
| Ransomware | 5 | 1 | 12 |
| Backdoor | 7 | 0 | 16 |
| Exploit | 35 | 3 | 52 |
| Trojan | 17 | 0 | 25 |

## Machines reporting

30 days


## Status

| | |
|---|---|
| Service status | ✓ |
| Total machines reporting | 3,547 |
| Open message center | |

## Machine

Cont-LizBean-X1

Domain: Contoso.org
OS: windows10

## Machine IP Addresses

Last external IP: 40.122.164.91
Last internal IP: 10.0.0.13

## Machine Reporting

First seen: 6 days ago
Last seen: 6 minutes ago

## Alerts related to this machine

| | | | |
|---|---|---|---|
| 02.23.2016 | NeroBlaze attack detected | Command And Control | New |
| 02.23.2016 | A port scanning tool was detected | Suspicious Activity | New |
| 02.23.2016 | A potential reverse shell has been detected | Command And Control | New |
| 02.23.2016 | Anomaly detected in ASEP registry Software\Microsoft\Windows\CurrentVersion\Run | Persistence | New |
| 02.23.2016 | A suspicious Powershell commandline was executed on the machine | Lateral Movement | New |
| 02.23.2016 | Outlook dropped and executed a PE file. | Suspicious Activity | New |

## Machine in organization

Filter by: All Behaviors


| Description | Details |
|---|---|
| 02.21.2016 | |

# NeroBlaze attack detected

| NeroBlaze | NeroBlaze attack detected | 02.23.2016 16:39:42 | *Today* | Command And Control | cont-lizbean-x1 |
|---|---|---|---|---|---|

## NEROBLAZE

**Introduction**

Active since 2007, NeroBlaze is an activity group that has been used primarily to target government bodies, diplomatic institutions and political advisors. Frequent use of zero-day vulnerabilities, spear-phishing and a number of other distribution methods, makes NeroBlaze a highly resilient threat.

**Interests**

We have seen NeroBlaze target government agencies, diplomatic institutions, and military organizations/installations in NATO member states, and certain Eastern European countries. We have also observed it target organizations associated with political activism in central Asia.

**Tools, tactics, and processes**

NeroBlaze seeks out victim information through open-source intelligence and social media interaction. It uses simple spear phishing attacks to obtain victims' email account credentials, compiling information for further attacks. It uses email accounts from generic email providers in order to imitate the email provider to disguise the spear phishing emails as a notification from the generic email provider, such as 'a privacy alert.' NeroBlaze persistently sends spear phishing attacks over many months to the same victims.

NeroBlaze attacks higher-value targets with emails that contain lures designed to take control of the victims' machines. NeroBlaze uses a breadth of tactics using lure emails that include:

- URLs to websites containing zero-day exploits
- URLs to websites that use social engineering techniques that cause the victim to download malware
- Document attachments that contain zero-day exploits

NeroBlaze usually packages these emails into a lure that might be interesting to the victim. NeroBlaze tries to provide credibility to these emails by associating the sender with a real organization.

Note: NeroBlaze appears to have resources to acquire many zero-day exploits that cover a wide range of software products for these attacks.

After a successful attack, NeroBlaze proceeds to get a foothold onto the victim's network. This includes making use of malware backdoors and VPN clients to achieve persistent network access. NeroBlaze has also been observed using Kali Linux (a penetration testing Linux distribution) on the victim's network for further exploration of the victim's computer. Lateral movement is also commonly used through pass-the-hash and credential dumping using publicly available tools, such as Mimikatz.

Exfiltration of information from the victim's network can happen through dedicated command and control (C2) infrastructure. NeroBlaze attempts to disguise this traffic through domain names that are associated with common tasks on the network, such as updates and malware checks. On rare instances, we have observed that NeroBlaze uses legitimate servers, such as local SMTP mail servers, to extract information. Overall, NeroBlaze tries to blend into the network traffic to avoid suspicion.

**Areas affected**

**Recommended defenses**

- Use the latest, up-to-date operating system and software versions with latest security mitigations
- Conduct enterprise software security awareness training, and build awareness about malware infection prevention
- Institute second factor authentication
- Prepare your network to be forensically ready
- Keep personnel and personal data private
- Lock down privacy settings on social profiles
- Keep systems and software fully updated

Dismiss

### More info about this alert

A set of behaviors likely associated with the NeroBlaze adversary was detected on this machine.

### Recommended Actions

New

1. Contact your Incident Response team. NOTE: If you don't have an Incident Response team, contact the Microsoft Consulting Services (MCS)

# Trusted Cloud – naše principy

## Ke kterému cloudu má mít organizace či firma větší důvěru?

### Security

Implementujeme silná bezpečnostní opatření k zabezpečení Vašich dat.

### Privacy & Control

Umožníme Vám kontrolu nad Vašimi daty tak, aby byla zajištěna ochrana soukromí.

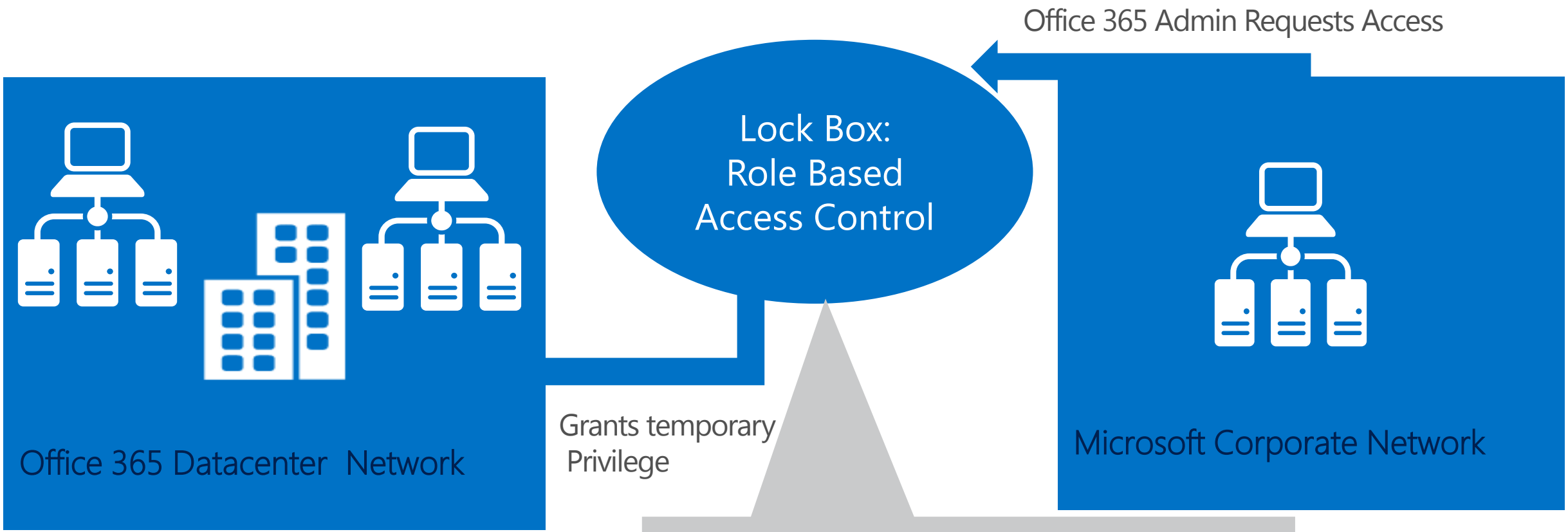
### Compliance

Pomůžeme Vám zajistit soulad s regulatorními požadavky.

### Transparency

Vysvětlíme srozumitelným jazykem, jak nakládáme s Vašimi daty.

# Restrikce přístupu na zákaznická data




Office 365 Plan **E5 „Customer Lock Box“** requires explicit customer approval to issue one-time credentials

**Grants least privilege required to complete task.**
**Verify eligibility by checking if**

1. Background Check Completed
2. Fingerprinting Completed
3. Security Training Completed

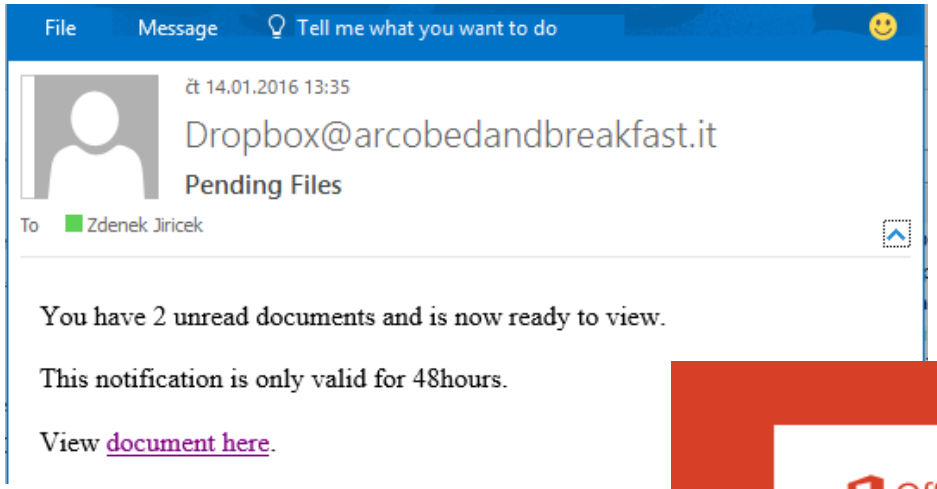
# Exchange Online Advanced Threat Protection

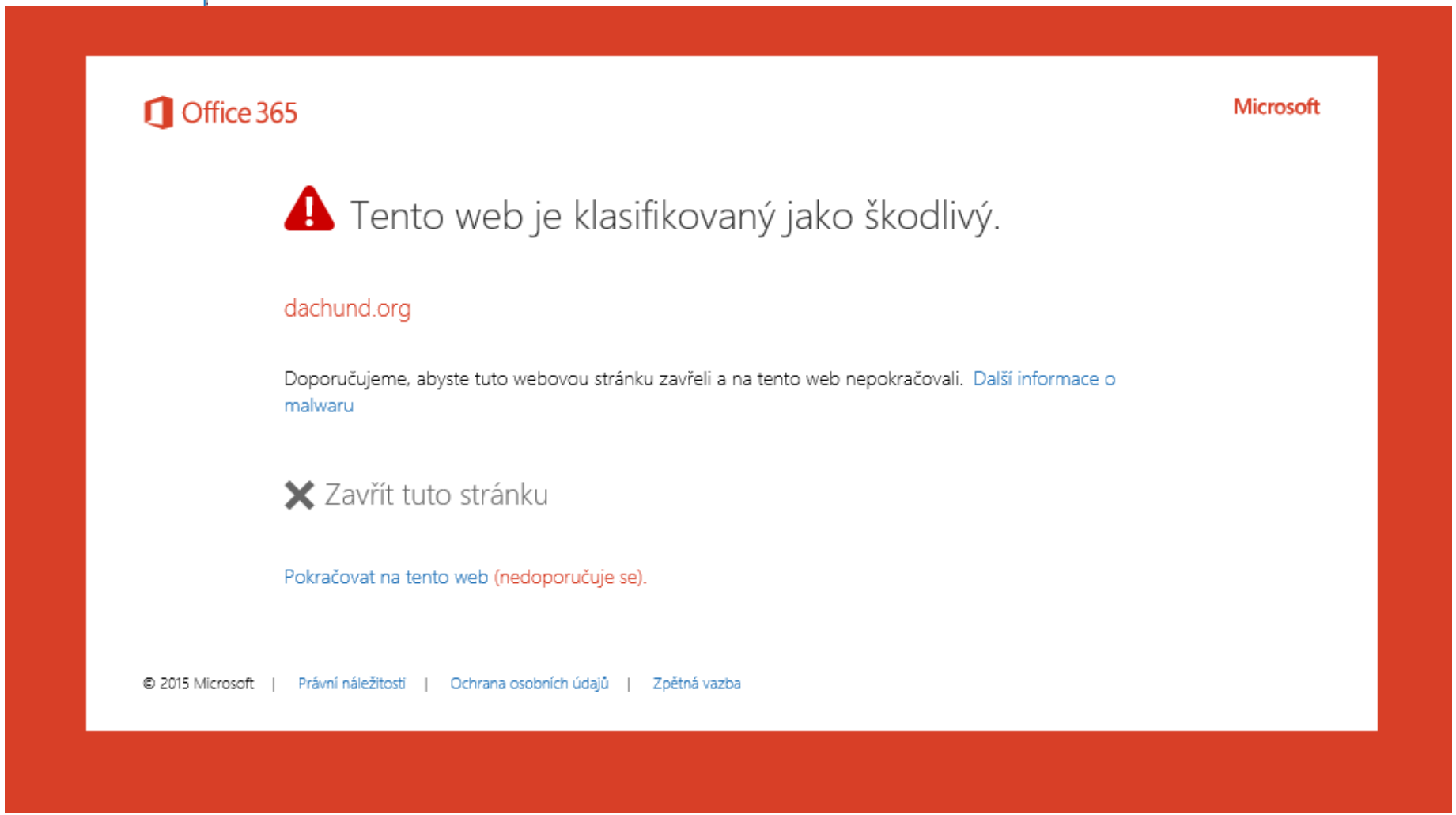
## Safe Attachments

- Sandboxing příloh a scan jejich chování
- Lepší ochrana před 0-day útoky
- Ochrana ještě než email skončí v Inboxu

## Safe Links

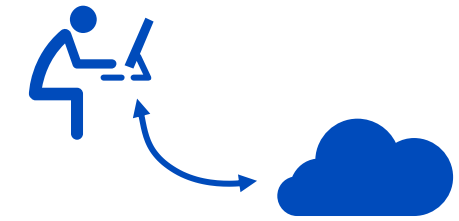
- „Time of user click“ URL protection
- Testuje náhrady URL přes objekty v emailu
- Aktivuje URL přes dočasný proxy server
- Reputační databáze > 1 mil. URL linků


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 and is now ready to view.
This notification is only valid for 48hours.
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 stránku
Pokračovat na tento web (nedoporučuje se).
© 2015 Microsoft | Právní náležitosti | Ochrana osobních údajů | Zpětná vazba

# Cloud - ochrana dat šifrováním

| | Office 365 OneDrive for Business | Microsoft Azure | Ochrana dat při přenosu |
|---|---|---|---|
| Nástroje zákazníka | RMS, S/MIME – nativně<br>PGP atd. – manuálně<br>3rd Party solutions<br>(př. Thales Cyris) | SQL Server TDE / CLE<br>SQL Always Encrypted<br>RMS SDK<br>3rd Party.. SafeNet, CloudLink | RMS, S/MIME<br>Na aplikační úrovni |
| Nástroje poskytované cloud. službou | Per-File Encryption<br>Advanced Encryption<br>Nativní služba | Azure Key Vault<br>Azure Disk Encryption (VHD)<br>StorSimple | Protokol SSL/TLS<br>Nově: Perfect Forward Secrecy (PFS) |
| Data v úložišti | Bitlocker<br>Šifrování AES-256<br>Destrukce NIST 800-88 | Bitlocker (volba zákazníka)<br>Šifrování AES-256<br>Destrukce NIST 800-88 | |



# Office 365 Advanced Encryption

## Co to je:

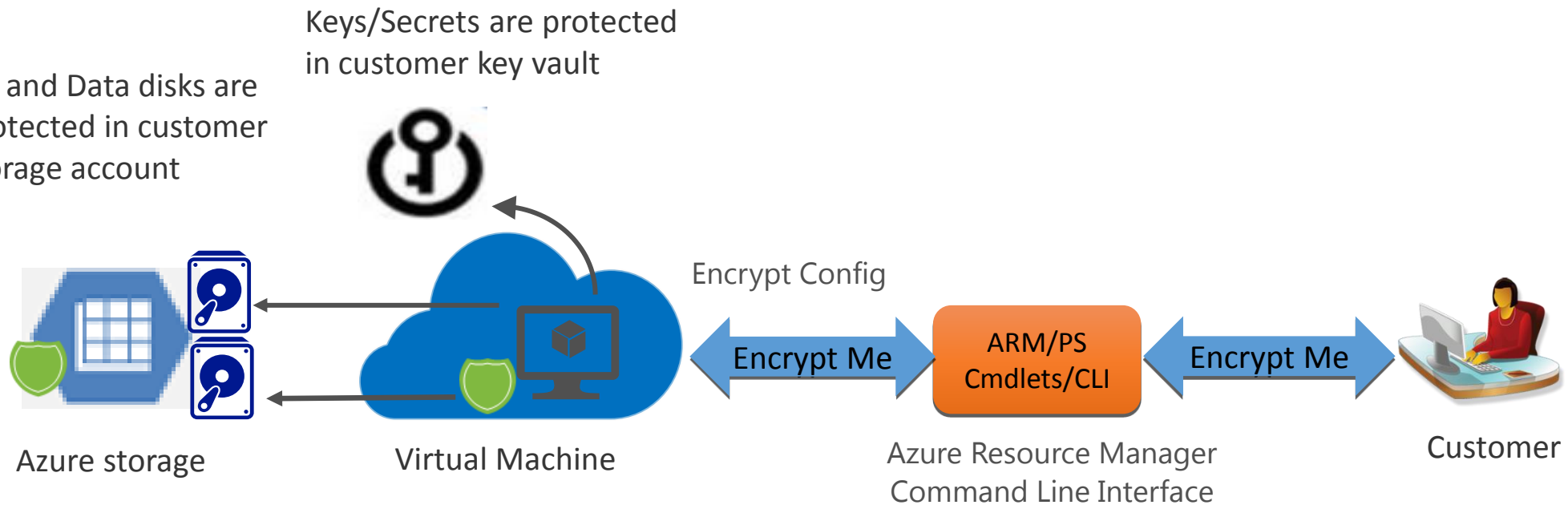
- Šifrování obsahu symetrickou šifrou
- Volba zákazníka mít pod kontrolou přístupový klíč (CYOK – Control Your Own Key), případně BYOK (Bring Your Own Key)
- Root key je uložen v Azure Key Vault
- Zákazník může pozastavit přístup k Root Key nebo jej úplně eliminovat
- Zákazník může mít rotaci Root Key (přešifrovat stávající symetrické klíče)

## Na co se vztahuje:

- Emaily + přílohy, složky
- Kalendáře, úkoly, poznámky
- Všechen obsah v SharePoint Online (Content Databases)
- Nezávislé na řízení přístupu „Customer Lockbox"

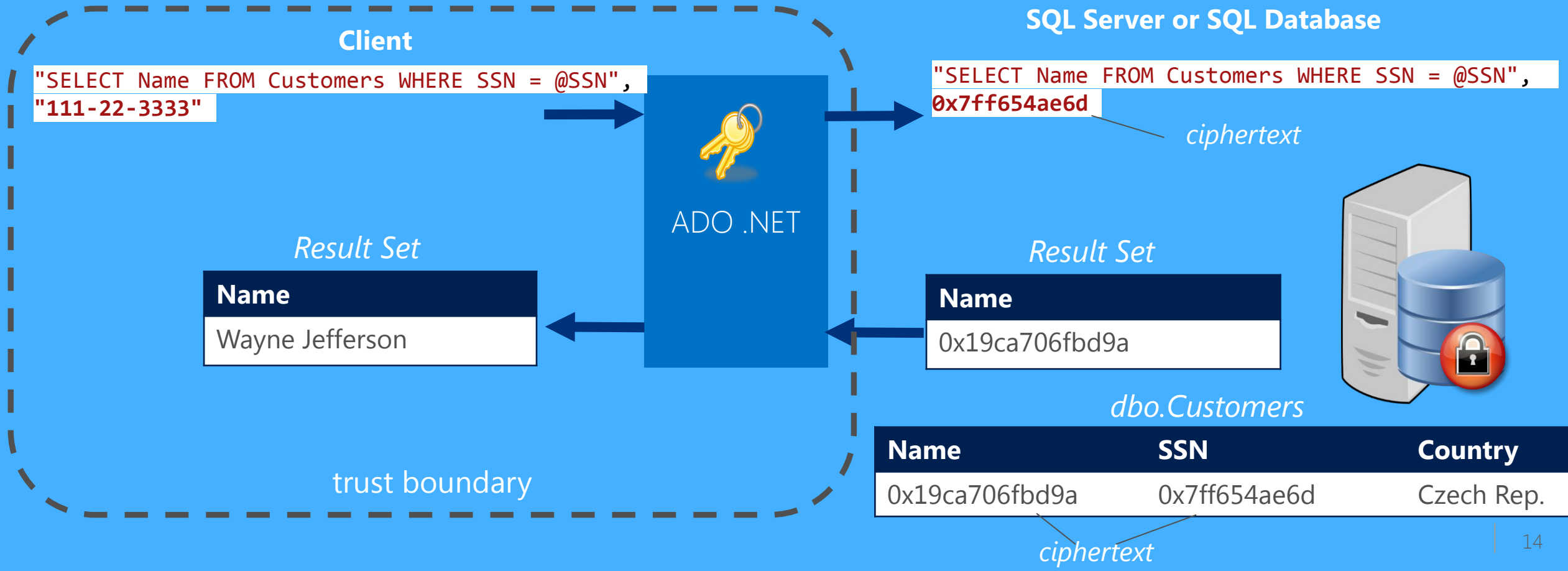
# Azure Disk Encryption – scénáře:

1. Šifrování celých **OS volumes** a kontrola autentizací při spuštění
2. Šifrování **Data volumes (VHD)** - data „at rest“
3. Ochrana klíčů a secrets v zákaznickém Azure Key Vault
4. Reporting stavu šifrování IaaS VM
5. Lze odstranit nastavení šifrování z IaaS VM



# SQL Database „Always Encrypted“

*Zašifrovaná citlivá data a jejich klíče nejsou nikdy v otevřeném textu v SQL Server VM*



# Soulad s regulatorními požadavky

## Horizontální:

Zákon o ochraně osobních údajů č. 101/2000 Sb.

Zákon o kybernetické bezpečnosti č. 181/2014 Sb.

## Vertikální:

Veřejná správa:
Zákon o ISVS č. 365/2000 Sb.

Vyhláška o výkonu činnosti bank atd. č. 163/2014 Sb.

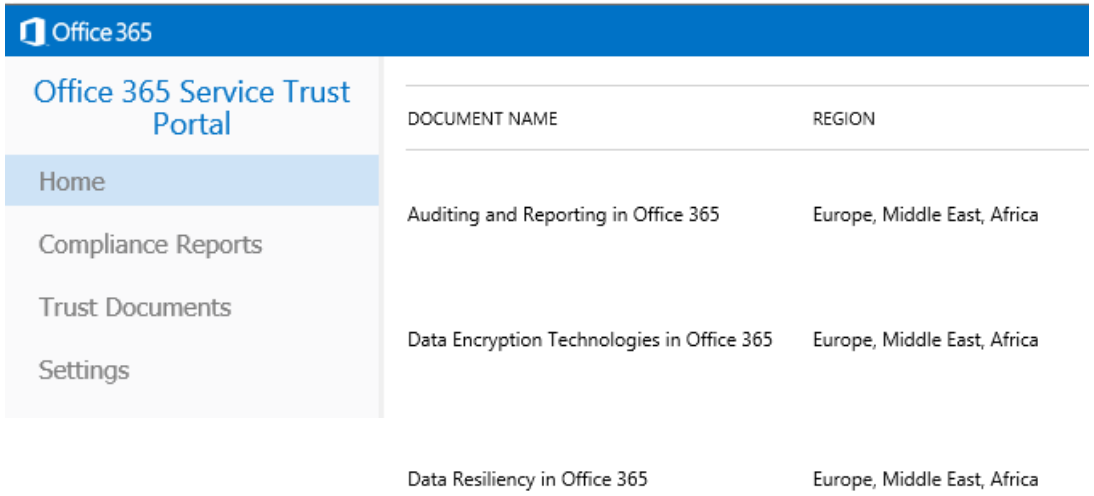
Viz nové Online Services Terms se Stand. smluv. doložkami EU

# Compliance resources

## Service Trust Portal

https://trustportal.office.com
folders:

- Compliance Reports (ISO 27k a SOC reports)
- Trust documents (security whitepapers)




## Document repository

- SOC 1 Type II audit report for Azure/O365/MCIO/CRM
- SOC 2 Type II audit report for Azure/O365/MCIO/CRM
- ISO 27001 / 27018 audit report for Azure/O365/MCIO/CRM
- Microsoft Security Policy
- Auditing and Reporting in Office 365
- Data Encryption Technologies in Office 365
- Data Resiliency in Office 365
- Azure Network Security Whitepaper
- Protecting Data in Azure Whitepaper
- Azure Security: Technical Insights Whitepaper
- Platform Penetration Tests for Azure
- Security Best Practices for Developing Azure Solutions
- **…. and many others**

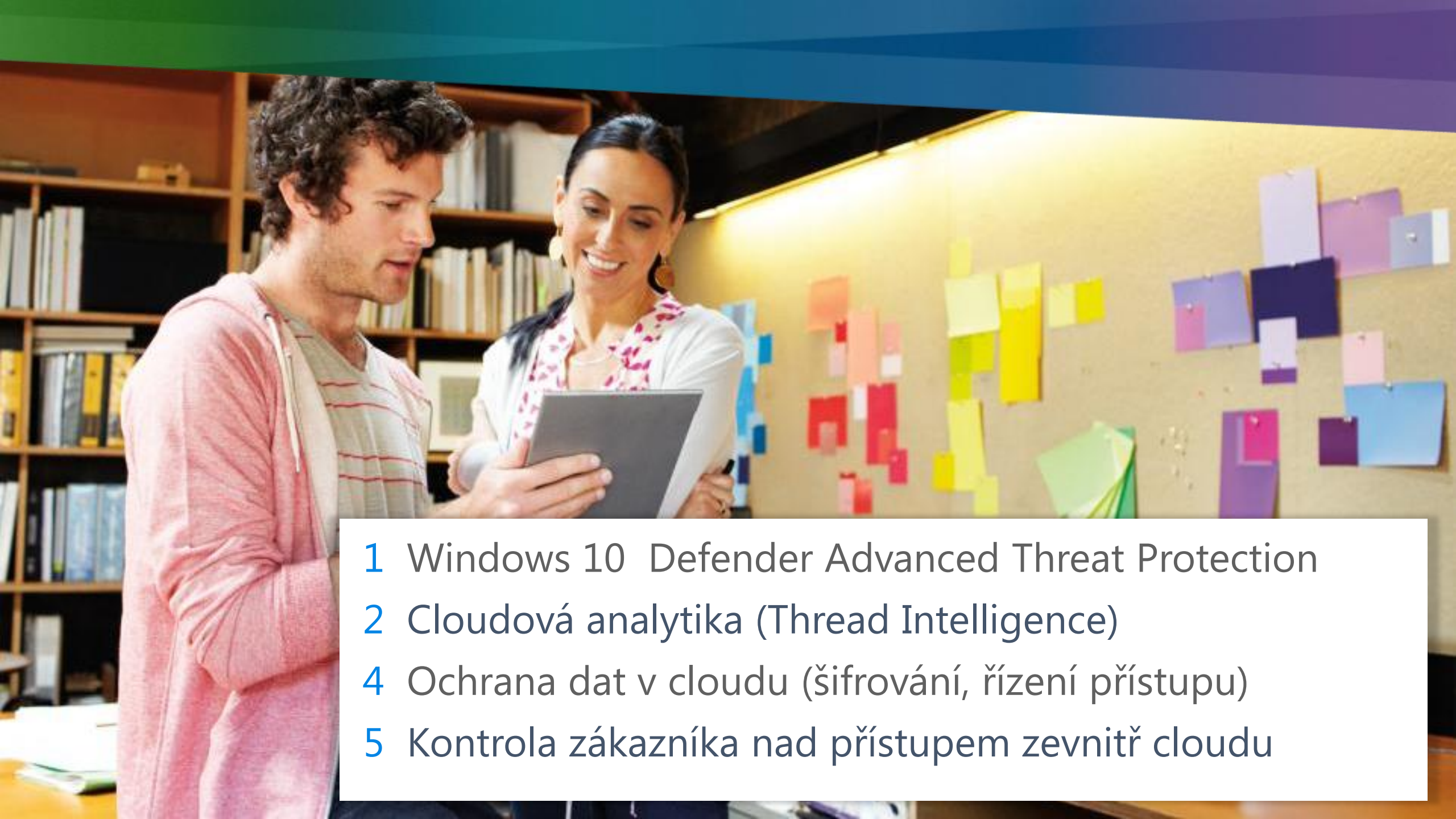
# Microsoft cloud resources

Microsoft Datacenters
microsoft.com/datacenters

Microsoft Transparency
microsoft.com/transparency

Microsoft Trust Center
microsoft.com/trust

Service Trust Portal
https://trustportal.office.com
(requires log-in)



1 Windows 10  Defender Advanced Threat Protection

2 Cloudová analytika (Thread Intelligence)

4 Ochrana dat v cloudu (šifrování, řízení přístupu)

5 Kontrola zákazníka nad přístupem zevnitř cloudu

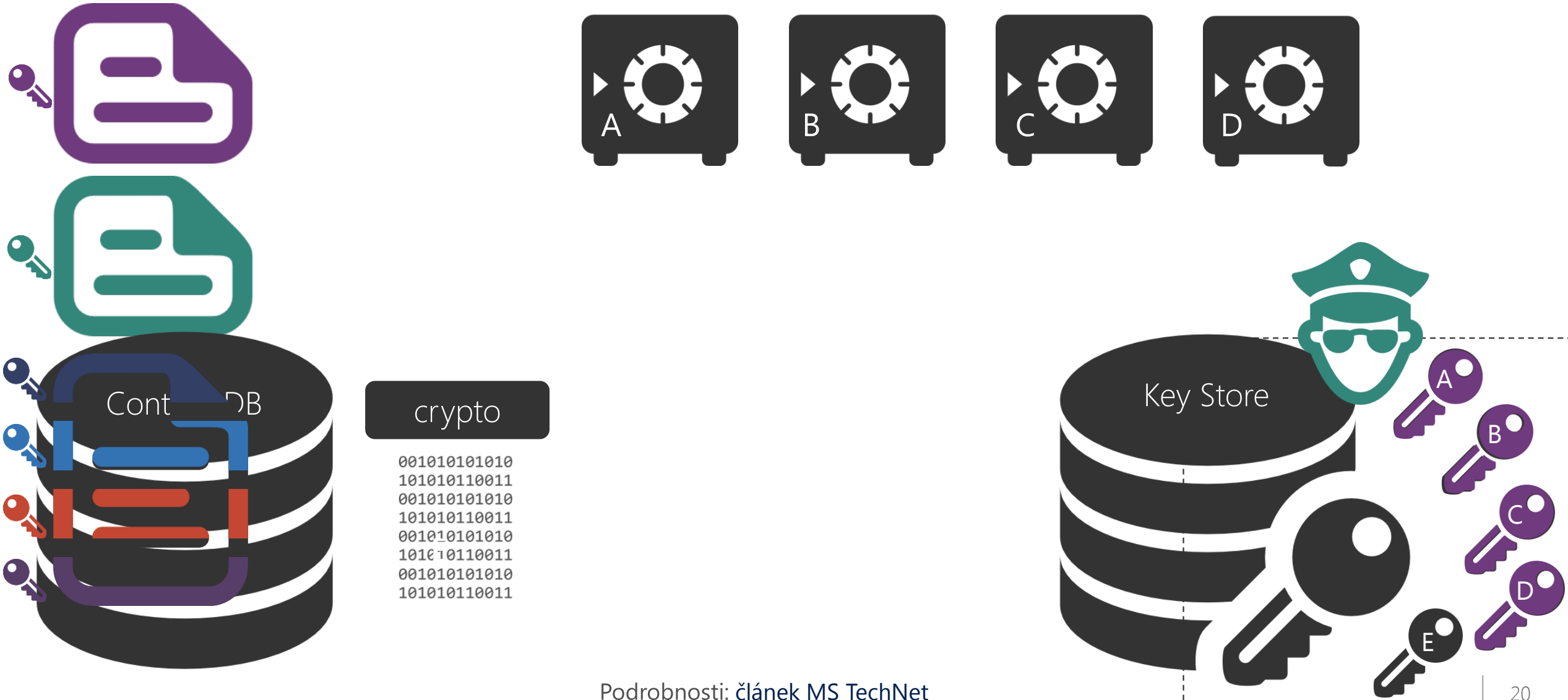
# Děkuji za pozornost!

Microsoft

Zdeněk Jiříček
National Technology Officer
zdenekj@microsoft.com

# Office 365 per-file encryption

SharePoint Online;
OneDrive for Biz
(folder level)




Podrobnosti: [článek MS TechNet]