

Zabezpečení koncových zařízení vašich uživatelů

Jan Pilař | VISION DAY 29. 11. 2017

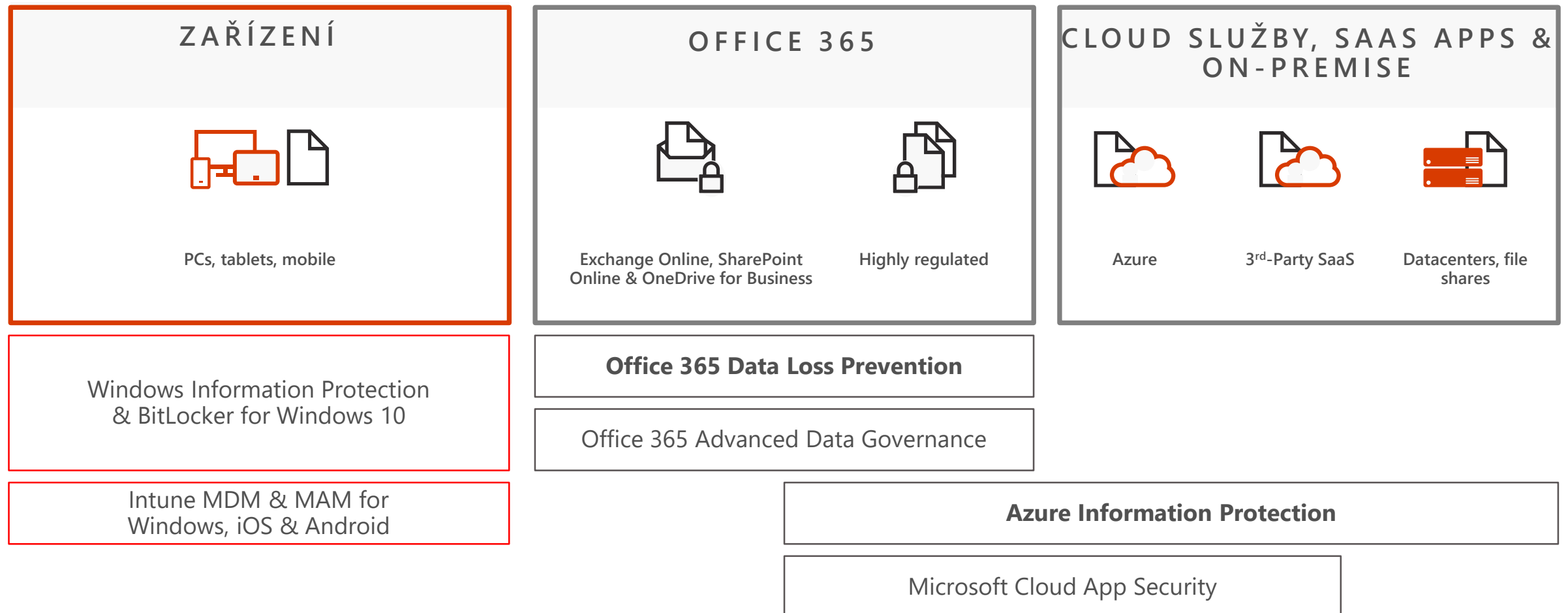
Technologický specialista - Modern Desktop

Jan.pilar@microsoft.com



Řešení ochrany informací Microsoft

Komplexní ochrana citlivých dat napříč zařízeními, cloud službami a on-premise prostředí



Proč je bezpečnost a detekce takové téma?

- Protože zabezpečení koncové stanice je často stále jen pomocí antiviru
- Protože útočníci používají moderní techniky a ne ty, proti který se často organizace brání
- Protože mnohem důležitější je detekce abnormálních aktivit a možnost rychlé reakce
- A k čemu je detekce bez reakce?
 - 93% napadení proběhne v řádech minut
 - 83% napadení trvá týdny než jsou detekovány a napraveny
 - Time, Intelligence, Detection & Response, automatization
- A to je ten rozdíl mezi EPP a EDR



CYBERCRIME PRICE LIST

ATTACK TOOLS



MALWARE	\$200	REMOTE ACCESS TROJAN
	\$50	PASSWORD STEALER
RANSOMWARE	200	SOPHISTICATED LICENSE FOR WIDESPREAD ATTACKS
	\$50	UNSOPHISTICATED LICENSE FOR TARGETED ATTACKS
	\$1	PC MALWARE INSTALLATION
SOFTWARE	\$400	1 MILLION MALICIOUS SPAM
	\$100	REMOTE DESKTOP CONTROL TOOL
PAYMENT & LOG-IN INFO	\$700	DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE
	\$5	CREDIT/DEBIT CARD FOR ONLINE USE
	\$10	CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC
	\$5	BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD)
	\$25	BANK ACCOUNT LOG-IN WITH ACCESS TO EMAIL, SECURITY ANSWERS, ETC.
	\$1	EXISTING PAYPAL ACCOUNT

DATA



PERSONAL INFORMATION	\$3	SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION
	\$150	CREDIT REPORT 750+ CREDIT SCORE
DATABASE RECORDS	\$25	1 MILLION COMPROMISED EMAIL/PASSWORDS

SERVICES



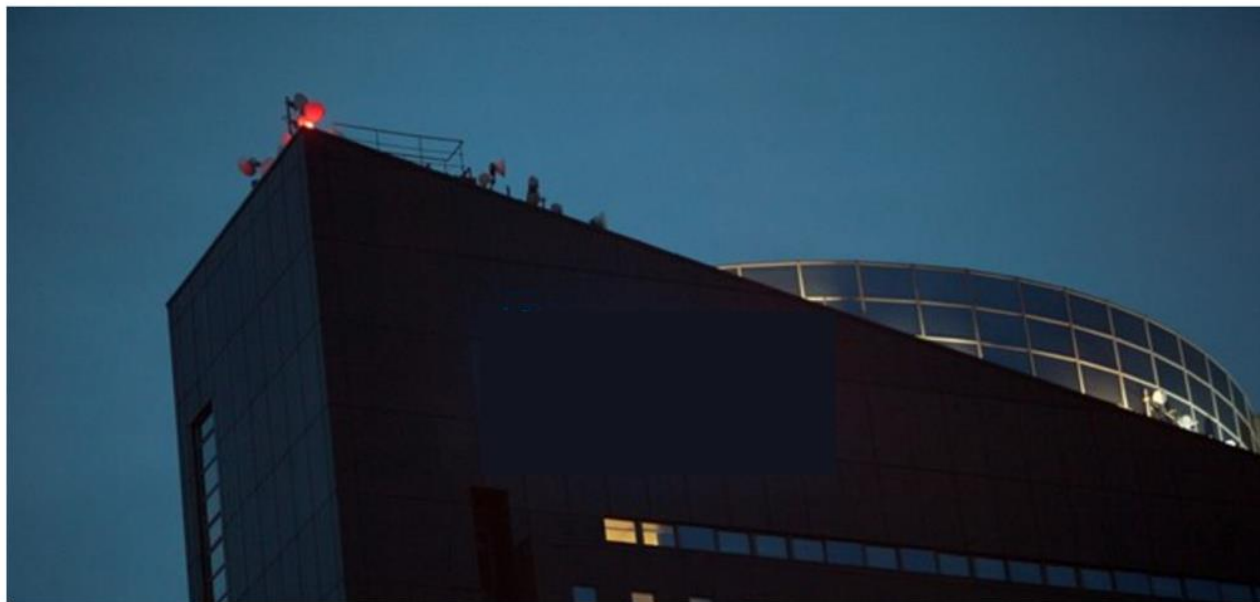
HACKING	\$100	EMAIL ACCOUNT
	\$100	SOCIAL MEDIA ACCOUNT
	\$300	CMS WEBSITE (WORDPRESS, ETC.)
USER OBFUSCATION	\$150	BULLETPROOF HOSTING IN A LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC.)
	\$20	VIRTUAL PRIVATE NETWORK (VPN)
MALWARE	\$1	PC MALWARE INSTALLATION
	\$25	MALICIOUS FILE ENCRYPTION
SPAM	\$20	500 SMS (FLOODING)
	\$400	500 MALICIOUS EMAIL SPAM
	\$20	500 PHONE CALLS (FLOODING)
	\$200	1 MILLION EMAIL SPAM (LEGAL)
FAKE DOCUMENTS	\$25	DIGITAL COPY OF FAKE CREDIT/DEBIT CARD
	\$25	DIGITAL COPY OF FAKE DRIVER'S LICENSE OR PASSPORT
	\$15	DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD



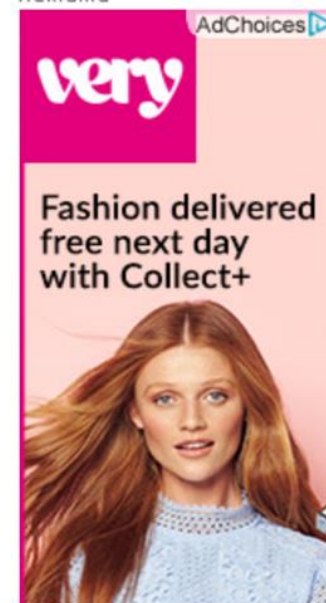
S ě unikla data o mzdách, zřejmě za tím je rozvod manažerky

3. ledna 2014 5:41

Z unikly citlivé údaje o obchodních plánech banky včetně příjmů nejvyššího managementu v dceřiných společnostech, jako je stavební spořitelna a penzijní společnost. Za únikem podle stojí rozvod jedné z manažerek banky.



Reklama



Hackeri měsíce stahovali data ze Zaorálkova e-mailu, útok mířil z ciziny

31. ledna 2017 12:01, aktualizováno 15:09    

E-mailové účty ministerstva zahraničí napadli neznámí hackeri. Útok trval několik měsíců, hackeri stahovali data také ze schránek ministra Lubomíra Zaorálka (ČSSD) i jeho náměstků. Podle šéfa diplomacie to připomínalo útok na americkou Demokratickou stranu před prezidentskými volbami.



Hackeri měsíce stahovali data ze Zaorálkova e-mailu | (2:40) | video: [ČTK](#)





T- e dostal pokutu za obří únik dat o klientech. Utekly adresy nebo výše plateb

AKTUALIZOVÁNO 16. 8. 2016



Ilustrační snímek. | Foto: ČTK

Operátor podle úřadu dostatečně nezabezpečil data svých klientů a má za to zaplatit pokutu ve výši 3,6 milionu korun. Bývalý zaměstnanec firmy nabízel na trhu data s údaji 1,2 milionu klientů



jobs.cz

Práce

- Front-end developer s váš
- Data Analyst & Miner – dle na 20 h týdně
- Country Manager Operati

People didn't invest
money in supporting kids.
So, he made the money
to help thousands.



I am an American
We are One Nation

[READ THEIR STORIES](#) **USA TODAY NETWORK**

TALKING TECH

[BUZZ](#)[VIDEO](#)[PODCASTS](#)[NEWSLETTER](#)

Hackers hid malware in CCleaner, a free app meant to clean out computers

[Elizabeth Weise](#), **USATODAY**

Published 10:24 a.m. ET Sept. 19, 2017

17k Shares

Windows 10 Enterprise – bezpečnost



Windows Bitlocker



Windows Information Protection



Proč vás to má zajímat

- Na mobilu používáme fotky a přistupujeme k emailu, že?
- A na počítači? Tam taky
- A kupříkladu ty fotky jsou **soukromé** a naopak email **pracovní**
- Uživatelé jsou již zvyklí **sdílet data**, mnohdy není připravená organizace a data končí na veřejných uložiscích
- 87% senior manažerů přiznává, že běžně nahrávají pracovní soubory do osobních emailových účtů nebo soukromých cloud účtů (Dropbox, uschovna.cz...)
- 58% omylem poslalo citlivé informace špatné osobě

Ochrana dat organizace

Přináší snadno použitelné oddělení firemních dat od soukromých

Ochrana dat bez ohledu na to, kde se nacházejí

Pouze důvěryhodné aplikace mohou přistupovat k datům

Ochrana pro telefony i počítače

Firemní aplikace a data
(spravované)

Soukromé aplikace a data
(nespravované)



Výměna dat je pod kontrolou



Office 365 Demos

Shared with external users

New Upload

All Documents

Documents

✓	Name	Modified	Modified By	Rating (0-5)	Checked Out To	+
	Contoso Electronics Sales Propos...	May 20	Demo User	★★★★★ 0		
	Fabrikam Invoice copy.docx	June 10	Garth Fort	★★★★★ 0		
	Product Sales.xlsx	May 20	Demo User	★★★★★ 0		

Drag files here to upload

File

Home

Insert

Draw

Layout

Review

View



Share

Calibri (Body)

11

B*I*U

Heading 1

Heading 2



changes comes great opportunity. Together, Litware and Contoso are ideally poised to take a market leadership position and deliver quality, consistency, and innovation to their customers.

Increasingly, people live life with their devices in hand. They are always on and always connected, so they require more from these devices—more power, more speed, more seamless integration. The industry challenge remains clear: Understand your customers, anticipate their future requirements, and deliver above their expectations.

That's why a Litware-Contoso partnership makes sense. No one in the consumer electronics market has a better understanding than Contoso of its long history of exciting innovation, turbulent disruption, and remarkable growth. And no one in the market consistently navigates through these changes and empowers its partners like Contoso.

Earning Summary

As you can see in figure 1 an unprecedented increase in TV sales in April has lead to a projected increase in 200% above initial estimates. This will have great impact on the market once this is shared to the analysts and is expected to increase Contoso share price considerably.





Twitter



Home



Moments



Notifications



Messages



Me



Search



New Tweet



Find People



Refresh

**Gartner** @Gartner_inc

2d

Gartner #Blog highlight by Avivah Litan, Insider threats escalate and thrive in the Dark Web. gtrn.it/28Sgl2e



U. of Washington retweeted

**Howard Behar** @howardbehar

2d

The world needs more women in STEM fields, that's why I'm sponsoring a 1wk Girls in STEM program at @UW this summer. ow.ly/CFlv301FAx0

**Bill Gates** @BillGates

Good to meet you
plans in the

Change this content to personal?

The ownership of this content will be changed from work to personal. Your organization may track this action.

Change to personal

Cancel

AFD_France @AFD_France

.@RiouxRemy meets @BillGates to develop the operational partnership between AFD and @gatesfoundation #health

**Microsoft Channel 9** @ch9

2d

Interview with Aaron Bjork dlvr.it/LgbCnL



140

Tweet

Windows Defender Advanced Threat Protection



Windows Defender Advanced Threat Protection

Detekce pokročilých útoků a speciálních průniků



Integrováno ve Windows 10 a podpora dalších OS

Žádný další deployment a infrastruktura.
Průběžné aktualizované, nižší náklady.



Zkoumá chování, detekce poháněná cloudem

Korelovaná upozornění na známé i neznámé soupeře
Real-time a historická data.



Bohatá časová osa pro zkoumání

Jednoduše pochopitelný rozsah průniku. Data napříč
koncovými zařízeními. Hluboká souborová a URL
analýza.



Unikátní threat intelligence znalostní báze

Optika na hrozby poskytovaná díky vlastním informacím i od třetích
stran



Odpověď přímo na Windows stacku

Bohatý SOC set nástrojů od zásahu proti konkrétní stanici tak
blacklisting napříč zařízeními i soubory



CO JE NOVÉHO, NYNÍ V FALL CREATORS UPDATE

- Reakce

- Izolování napadené stanice
- Sběr forensních dat
- Zastavení & vyčištění běžících procesů / souborů
- Blok souboru (vyžaduje WD-AV)
- Spuštění AV testu na dálku
- Zabránění spouštění aplikací mimo MS
- Automatické šetření a reakce! (v preview)

- Rozšířená detekce

- Vylepšení senzoru – útoky na paměť a kernel
- Vlastní TI “krmivo” – popis/anatomie útoku
- 3rd party TI “krmivo” – FireEye iSight Threat Intelligence

- Integrace napříč Microsoft security stackem

- Zobrazuje Windows Defender Antivirus a Device Guard události v Windows Security Center
- Office365 ATP integrace

- Vylepšení vyšetřování – změny dle ohlasu uživatelů

- Uživatelský pohled
- Výrazně lepší graf a strom popisující útok
- Virus-total integrace
- ...

Bohatá vizualizace

Windows Security Center

Alert

Analyst@WDATPContoso.onmicrosoft.com

>

ericlaptop > A suspicious Powershell commandline was found on the machine

A suspicious Powershell commandline was found on the machine

016 09:34:17

72d

Medium

Suspicious Activity

ericlaptop | northamerica/ersciple

Alert process tree

```
graph TD; wmiprvse.exe --> mshta.exe; mshta.exe --> powershell.exe; powershell.exe --> regsvr32.exe; regsvr32.exe --> abc.exe; regsvr32.exe --> 365010.lnk; regsvr32.exe --> 365011.lnk
```

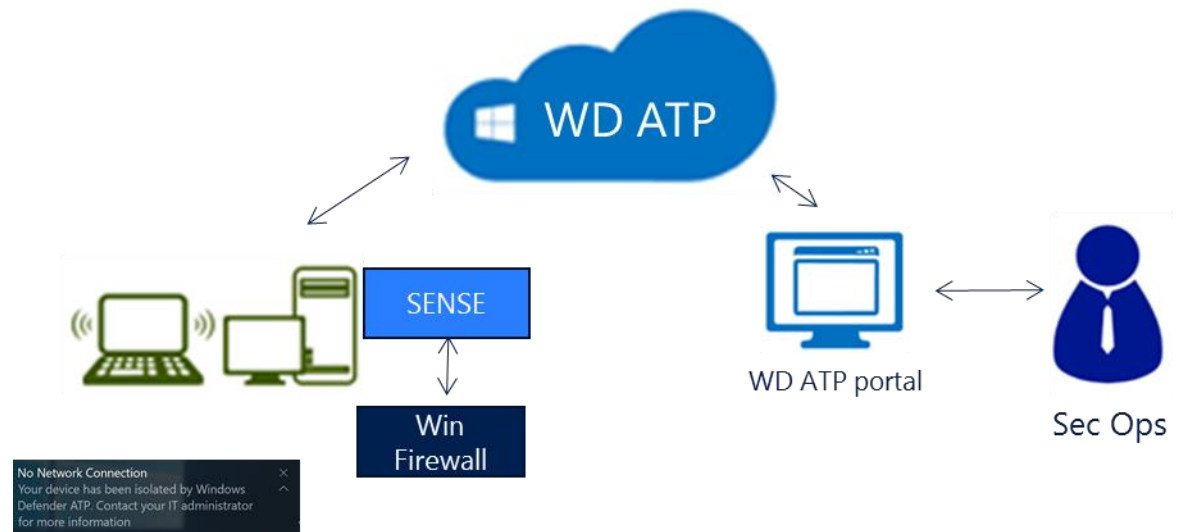
Incident Graph

```
graph LR; ericlaptop --> powershell_exe[powershell.exe ran command]; powershell_exe --> cont_lizbean[cont-lizbean]; powershell_exe --> salaries_docx[salaries.docx]; powershell_exe --> install_exe[install.exe]; powershell_exe --> powershell_command[Powershell command]; powershell_exe --> sl_exe[sl.exe]; powershell_exe --> 104209186[104.209.186]; cont_lizbean --> cont_allenmcgui[cont-allenmcgui]; cont_lizbean --> cont_yolandawil[cont-yolandawil]; cont_lizbean --> cont_summerfros[cont-summerfros]; cont_allenmcgui --> salaries_docx_2[salaries.docx]; cont_allenmcgui --> powershell_command_2[Powershell command]; cont_yolandawil --> salaries_docx_3[salaries.docx]; cont_yolandawil --> powershell_command_3[Powershell command]; cont_summerfros --> salaries_docx_4[salaries.docx]; cont_summerfros --> powershell_command_4[Powershell command];
```


IZOLOVÁNÍ CHRÁNĚNÉ STANICE

Izolování postiženého počítače a zastavení „krvácení“

- “Isolate machine” odpojí stanici od sítě
- Zachovává se komunikace do WD ATP služby
- Po odpojení je notifikace informující o přesném čase odpojení
- Akce izolace je zaznamenána v portálu (kdo izoloval, datum, důvod)
- Status izolace je k dispozici na při pohledu na detail stanice v WD ATP portálu

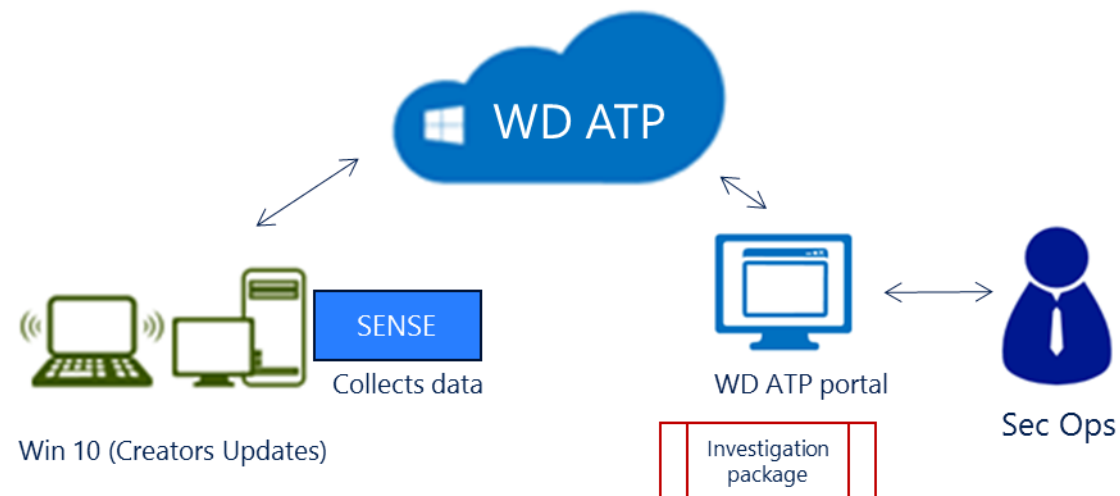


- SENSE klient využívá Windows Firewall Isolation API k odpojení stanice s Windows
- Bez problému pracuje s 3rd party instalovaným firewall

SBĚT FORENSNÍCH DAT

Sběr detailních dat k další analýze – otisk stanice

- “Collect investigation package” spustí proces sběru dat
- SENSE klient provede sběr dat a kompresi do balíčku
- Balíček je uložen v WD ATP službě s veškerým zachováním soukromí a bezpečnosti.
- Balík dat je ke stažení z portálu, velikost je ~5 MB - 50 MB
- Žádné UX na koncové stanici – transparentní pro uživatele



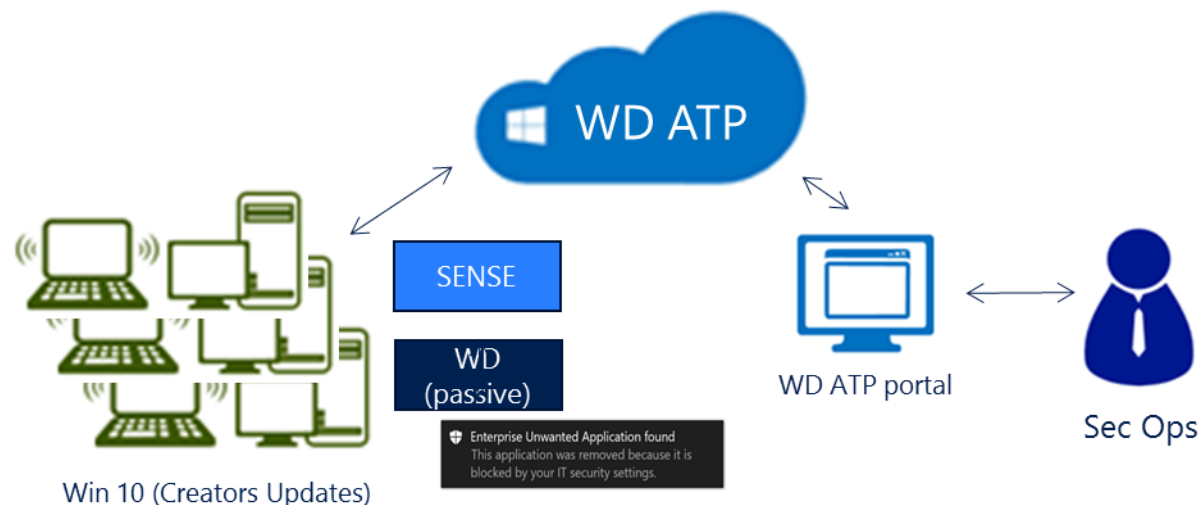
Collected data:

- Running processes
- Installed applications and services
- Persistency – ASEP Windows registry, Scheduled tasks
- Security Event logs
- Users and groups
- Previous processes running (prefetch files)
- Network connections (DNS cache, ARP cache, browser history)

ZASTAVENÍ & KARANTÉNA SOUBORU

Zamezení spouštění a karanténa škodlivých souborů, které obsahují incident

- “Stop and Quarantine file” zařídí:
 - Ukončení běžícího procesu
 - Karanténu souboru
 - Odebere závislosti (např. ASEP)
- Akce se uplatní na všech počítačích s Creators Update, kde by tento soubor v posledních 30 dnech vidět.
- Agregovaný přehled výsledků v portálu WD ATP
- Guardrails – není možnost smazat důvěryhodný soubor
- Upozornění na běžný soubor
- Možnost rollback a vyjmutí souboru z karantény lokálně na daném stroji.

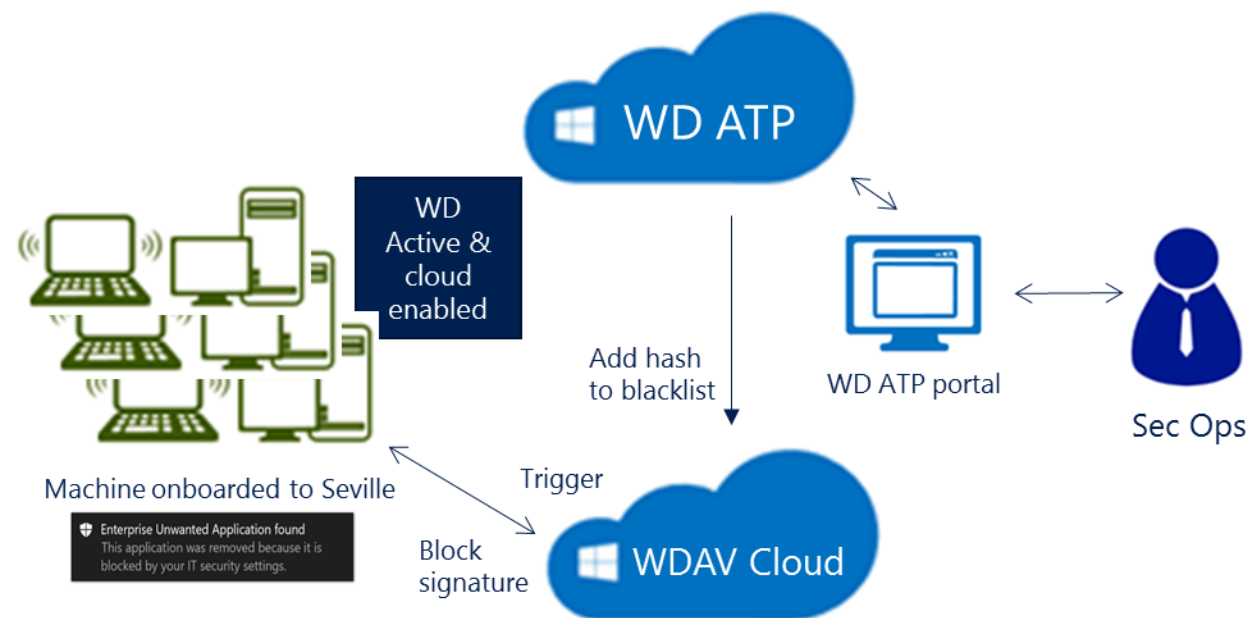


- Klient využívá WDAV k zastavení a karanténě souboru (WDAV není vyžadován jako primární a jediný antivirus na počítači)
- Notifikace o karanténě je na stanici vidět, včetně logu ve Windows

BLOKOVÁNÍ SOUBORU

Definice AV pro konkrétní organizaci, která blokuje hash souboru proti dalším akcím, jako je stažení a spouštění

- Funkce je k dispozici pouze pokud WDAV je aktivní a „Block at First Sight“ povolen
- “Block file” přidá hash souboru do blokových
- Jakékoliv budoucí spuštění souboru bude blokováno
- Při blokování souboru se uživateli zobrazí standardní notifikace od Windows Defender AV
- V časové ose stroje je vidět údaj o blokaci souboru
- Guardrails – není možné blokovat důvěryhodný soubor. Upozorňuje při pokusu blokovat zcela běžný soubor.
- Možnost odebrat soubor z blokových



- Blokování souboru vytvoří mikro-definici pro WDAV Block at First Sight službu
- Jakmile soubor se snaží spustit na stroji, je prověřován proti službě BaFS a získá příkaz k blokování.



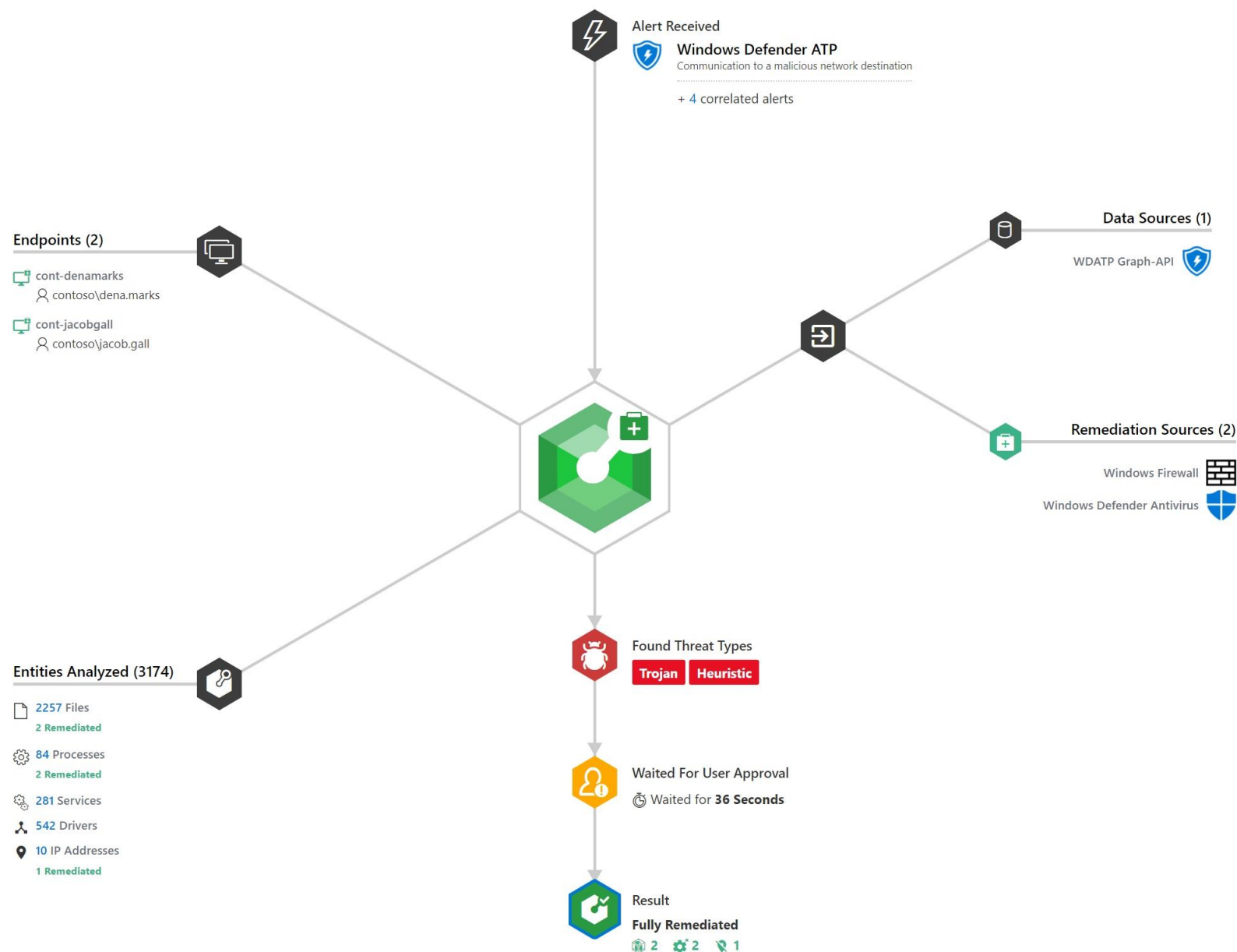
Communication to a malicious network destination (#17386)

4:11m

Actions (79)

Comments (2)

Tags (0)



Result



Fully Remediated

The malicious entities uncovered during the investigation have been successfully remediated.

2 Files were quarantined

\$r6bq1c4.exe | c:\\$recycle.bin\s-1-5-21-169718-5450-2076875350-1481720747-500\\$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-1-5-21-169718-5450-2076875350-1481720747-500\\$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**

Our security platform



Advanced Threat Analytics
Cloud App Security
Intune
Windows Server 2016
SQL Server 2016



Windows Trust Boot
Device Guard
Credential Guard
Windows Hello for Business
Windows Defender ATP
Windows Update for Business
Windows Information Protection



Azure Active Directory
Azure Security Center
Azure Rights Management System
Azure Storage Service Encryption
Azure Key Vault
Azure Information Protection



Advanced Threat Protection
Anti-Spam / Anti-Malware
Message Encryption
Data Loss Prevention
Threat Intelligence
Advanced Data Governance
Advanced eDiscovery
Secure Score
Customer Lockbox
Advanced Security Management



*THEY
DIDN'T
SEE IT
COMING.
BUT YOU CAN.*

Jan.pilar@microsoft.com