Microsoft 365

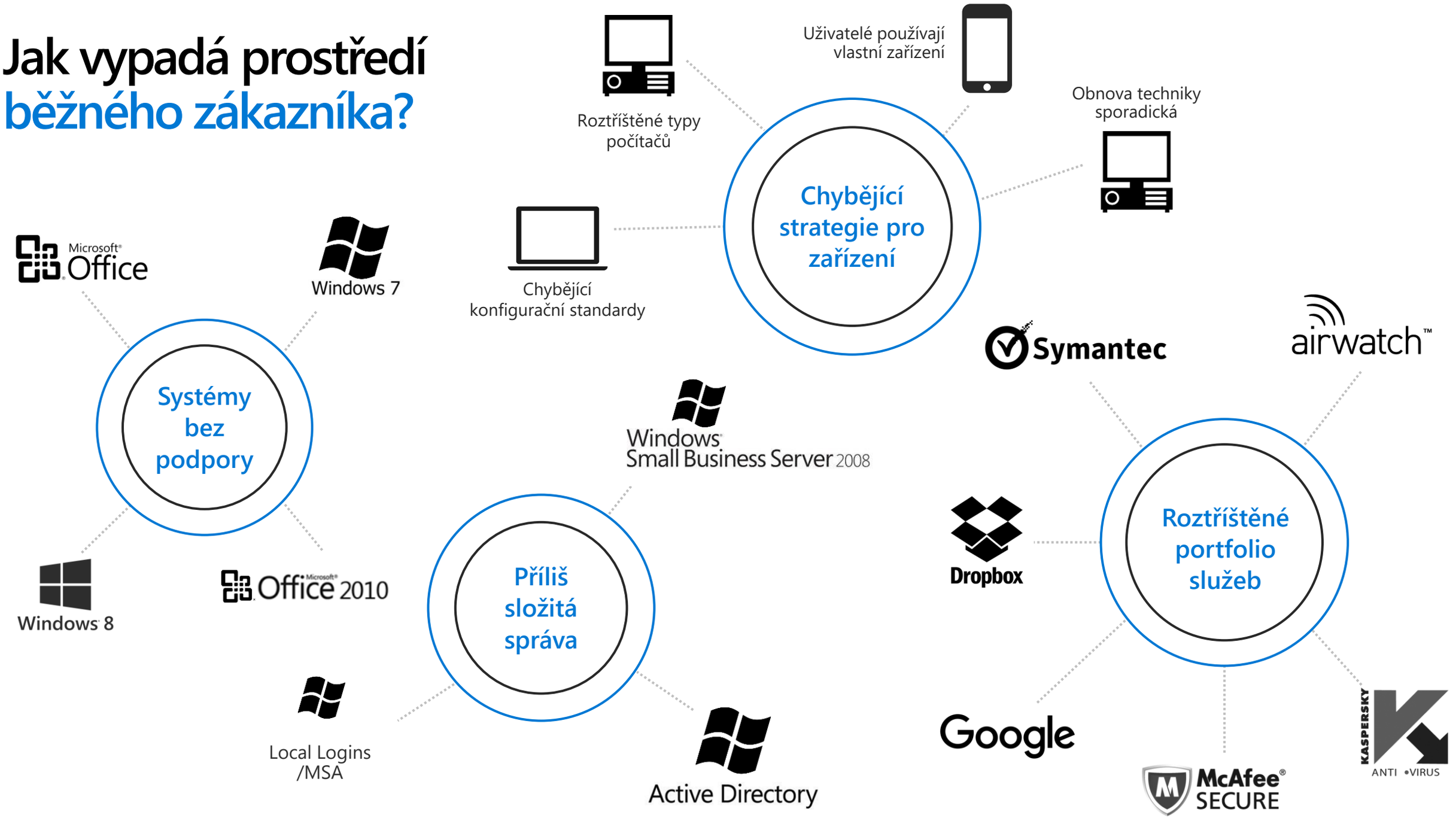
Bezpečně 365

Petr Vlk
KPCS CZ

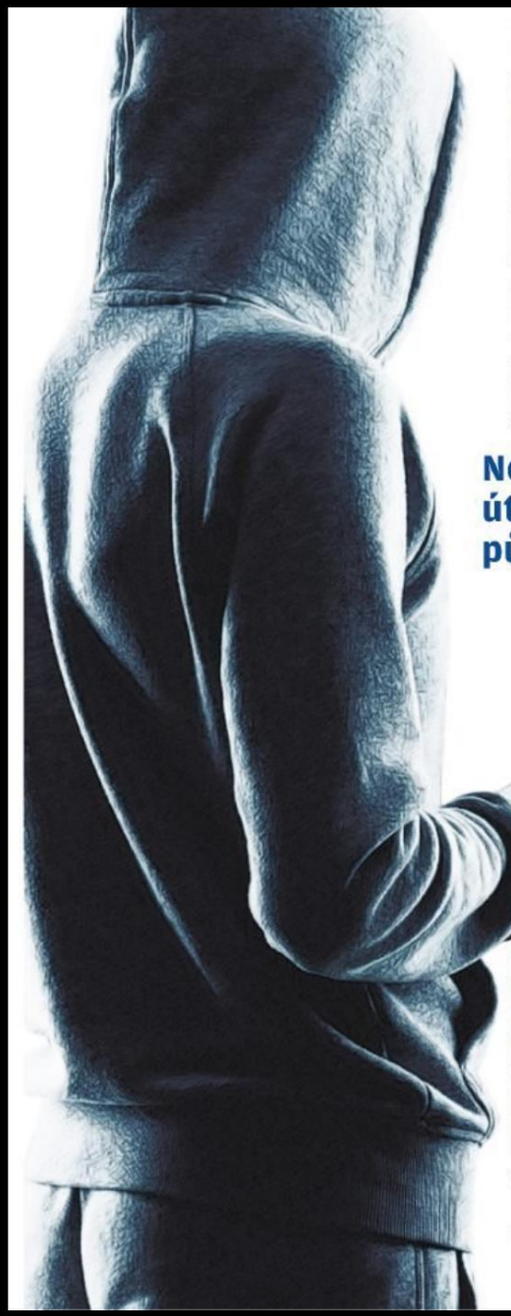

View all photos
Search the web and Windows


Microsoft
Microsoft
Windows 95

Jak vypadá prostředí běžného zákazníka?



Nebezpečné kybernetické útoky po síti za poslední půlrok



11. prosince 2019
Provoz benešovské nemocnice ochromil ruský vyděračský počítačový vir Ryuk, který napadl jejísystém, nešlo spustit přístroje ani síť. Operace byly zrušeny, provoz byl plně obnoven 30. prosince. Škody přesáhly 50 milionů.

23. prosince 2019
Společnost OKD z bezpečnostních důvodů přerušila těžbu ve všech svých dolech na Karvinsku. Důvodem byl hackerský útok, který ochromil její počítačovou síť. Těžba v dolech byla obnovena 27. prosince.

13. března 2020
Fakultní nemocnice Brno čelila kybernetickému útoku, postupně padaly počítačové systémy, a proto bylo potřeba vypnout všechny počítače. Základní provoz zůstal zachovaný. Vznikla škoda za desítky milionů korun.

30. března 2020
Počítačovou síť v Psychiatrické nemocnici Kosmonosy ochromil kyberútok. K 14. dubna bylo v provozu zhruba 70 % počítačů, zbytek by měl začít fungovat v příštích dnech.

7. dubna 2020
Terčem kybernetického útoku se stal městský úřad Prahy 3, jehož chod byl ochromen i po více než týdnu. Kromě webových stránek byly vypnuty všechny IT systémy radnice.

7. dubna 2020
Hackeři zaútočili na informační systém Povodí Vltavy, nefungovaly e-maily či spisová služba a další interní systémy. Přehrady nebo dodávky vody ohroženy nebyly.

3. a 8. dubna 2020
Napadeny byly informační systémy společnosti ČEZ Distribuce. Útok byl odvrácen.

17. dubna 2020
Fakultní nemocnice v Ostravě a Olomouci se staly terčem kybernetického útoku. Útok odrazily. Pokusy o vniknutí do sítí hlásily i nemocnice v pardubickém a karlovarském kraji. A útočníci měli spadeno i na ministerstvo zdravotnictví, potvrdil šéf resortu Adam Vojtěch (za ANO).

17. dubna 2020
Informační systémy pražského Letiště Václava Havla se pokusil napadnout neznámý útočník.

FOTO: MAFRA-ARCHIV // KOLÁŽ ŠIMON / LN

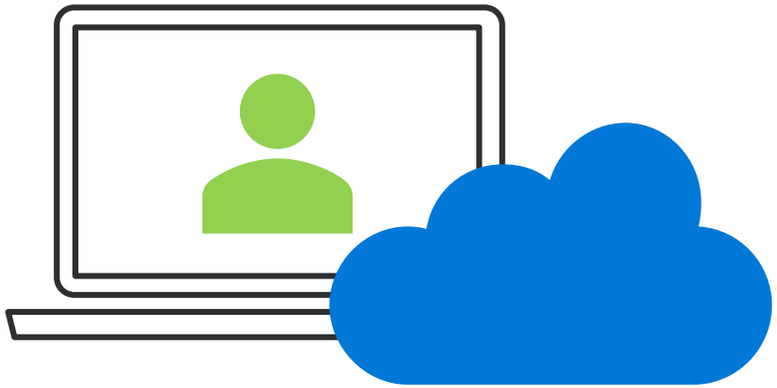
Moderní pracoviště

Čas

Bezpečnost

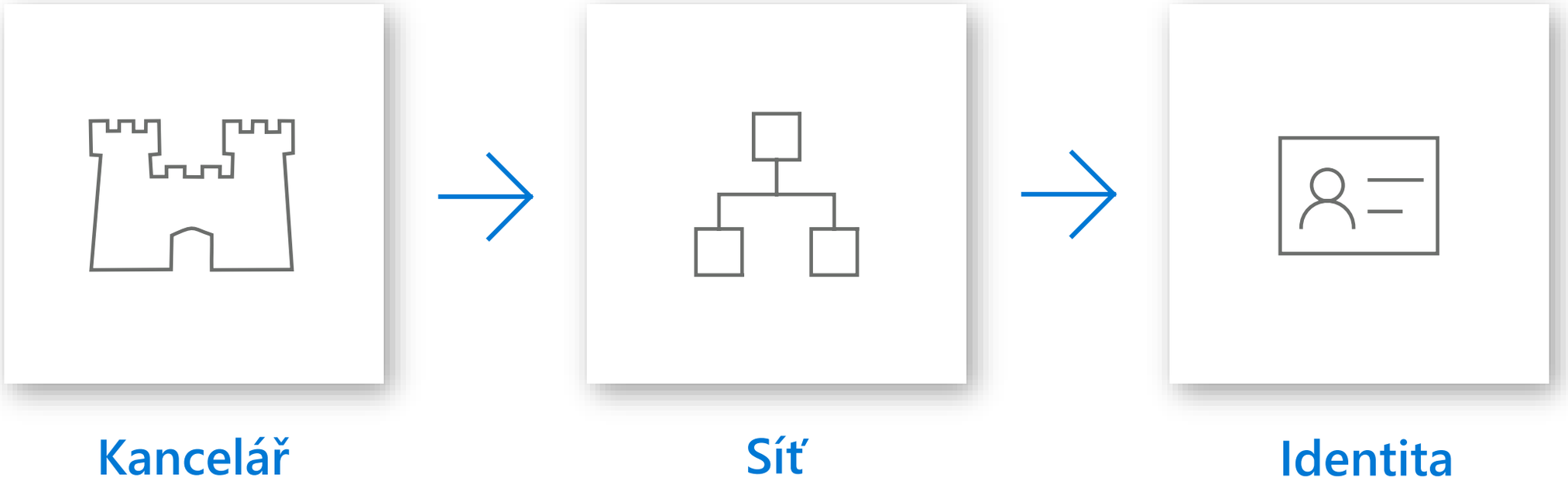
Služby

Poháněno Microsoft 365



Unikátní kombinace produktivity, zabezpečení a klientského přístupu

Evoluce bezpečnostního perimetru



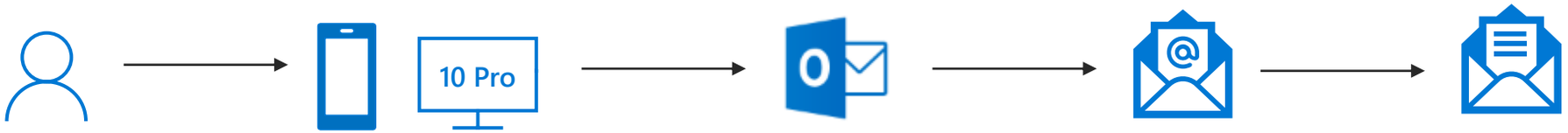
Kancelář

Síť

Identita

Různá rizika a vektory útoku vyžadují různé metody obrany a remediace

Otevřené cesty pro útočníka



Microsoft 365

Komplexní řešení pro malé i velké společnosti

Office 365

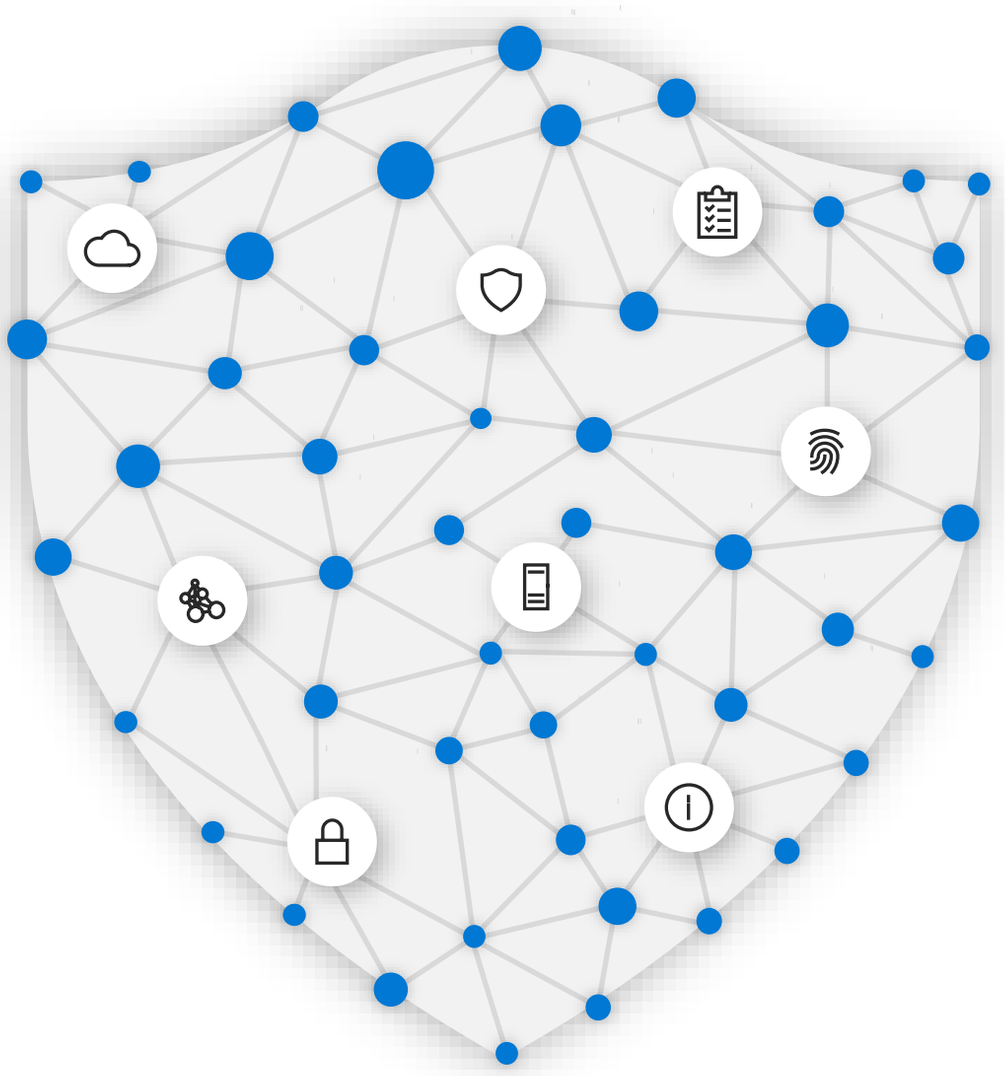
E-maily, dokumenty, spolupráce, komunikace, produktivita

Enterprise Mobility+Security

Identita, zařízení, data a jejich zabezpečení

Windows 10

Bezpečný přístup uživatele do cloudu



Uživatelé

Použitelnost

Flexibilita

Mobilita

IT

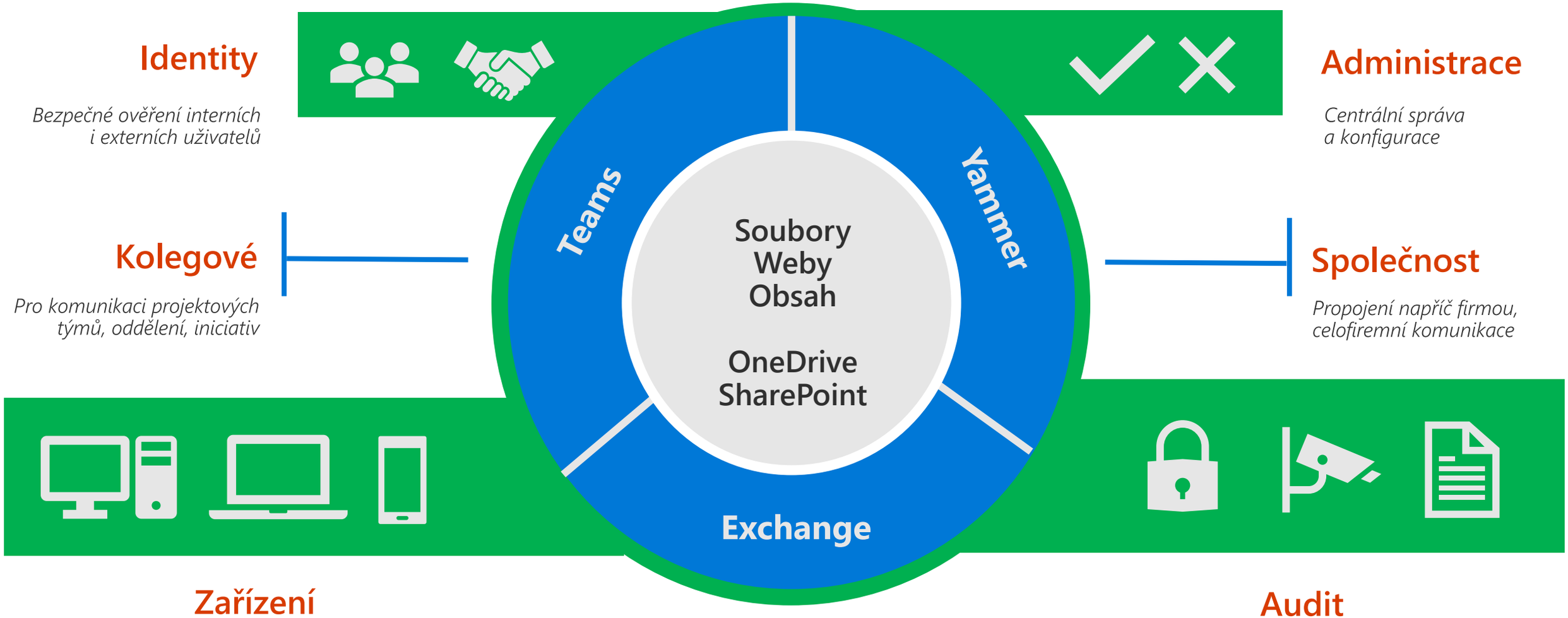
Správa

Zabezpečení

Předpisy

Moderní pracoviště

Microsoft 365: Moderní pracoviště



Identity

Bezpečné ověření interních i externích uživatelů

Administrace

Centrální správa a konfigurace

Kolegové

Pro komunikaci projektových týmů, oddělení, iniciativ

Společnost

Propojení napříč firmou, celofiremní komunikace

Zařízení

Konfigurace a správa koncových zařízení, mobilních telefonů a aplikací

E-mail

Pro cílenou a řízenou interní i externí komunikaci

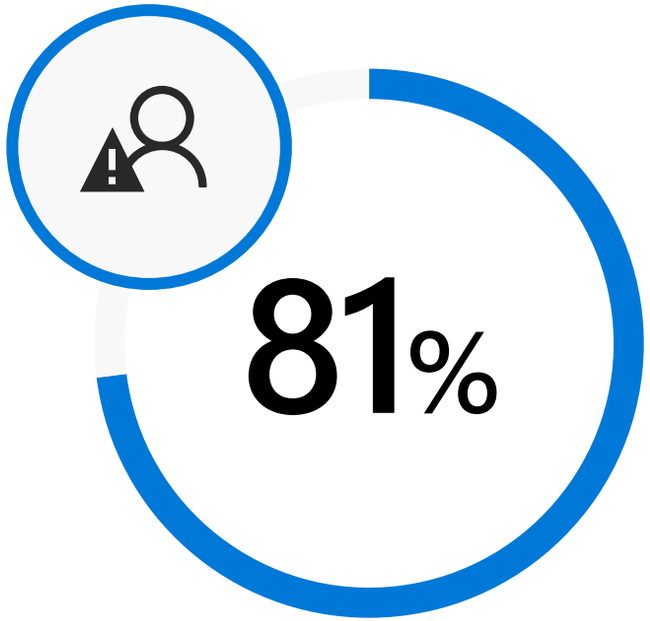
Audit

Ochrana dokumentů, dat, informací, audit aktivit, přehledné reporty, soulad s normami a certifikace

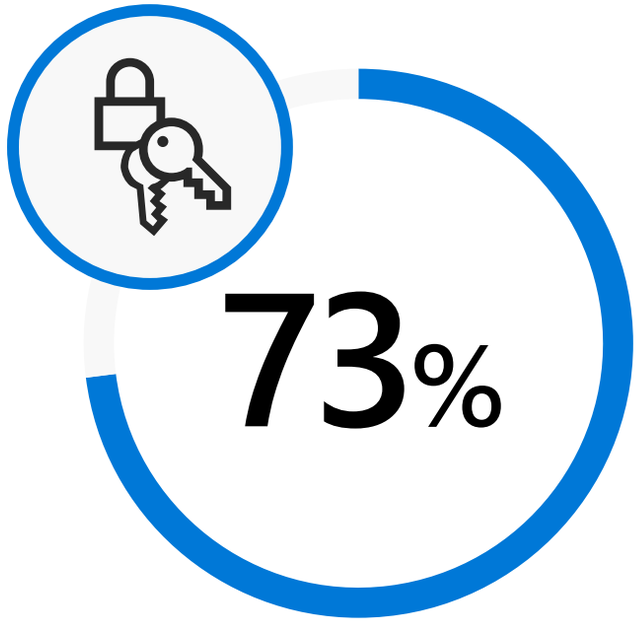
Microsoft 365 Groups

Členství napříč aplikacemi a službami

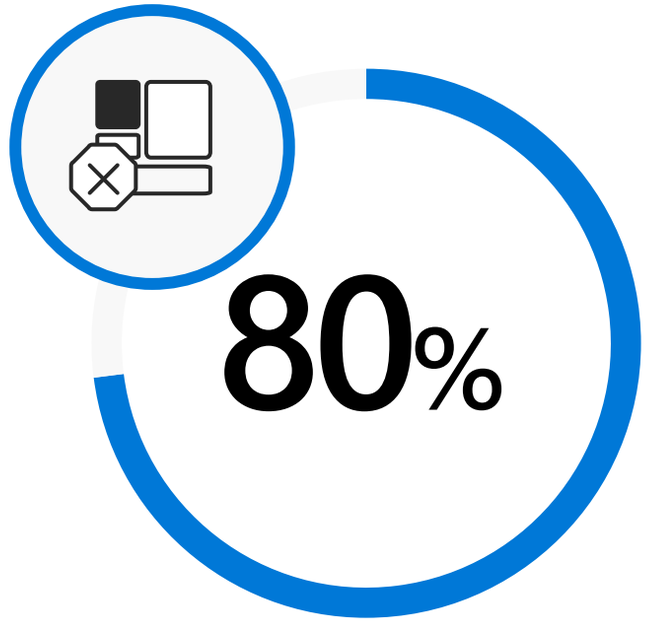
Hesla



úniků osobních dat způsobeno únikem hesla

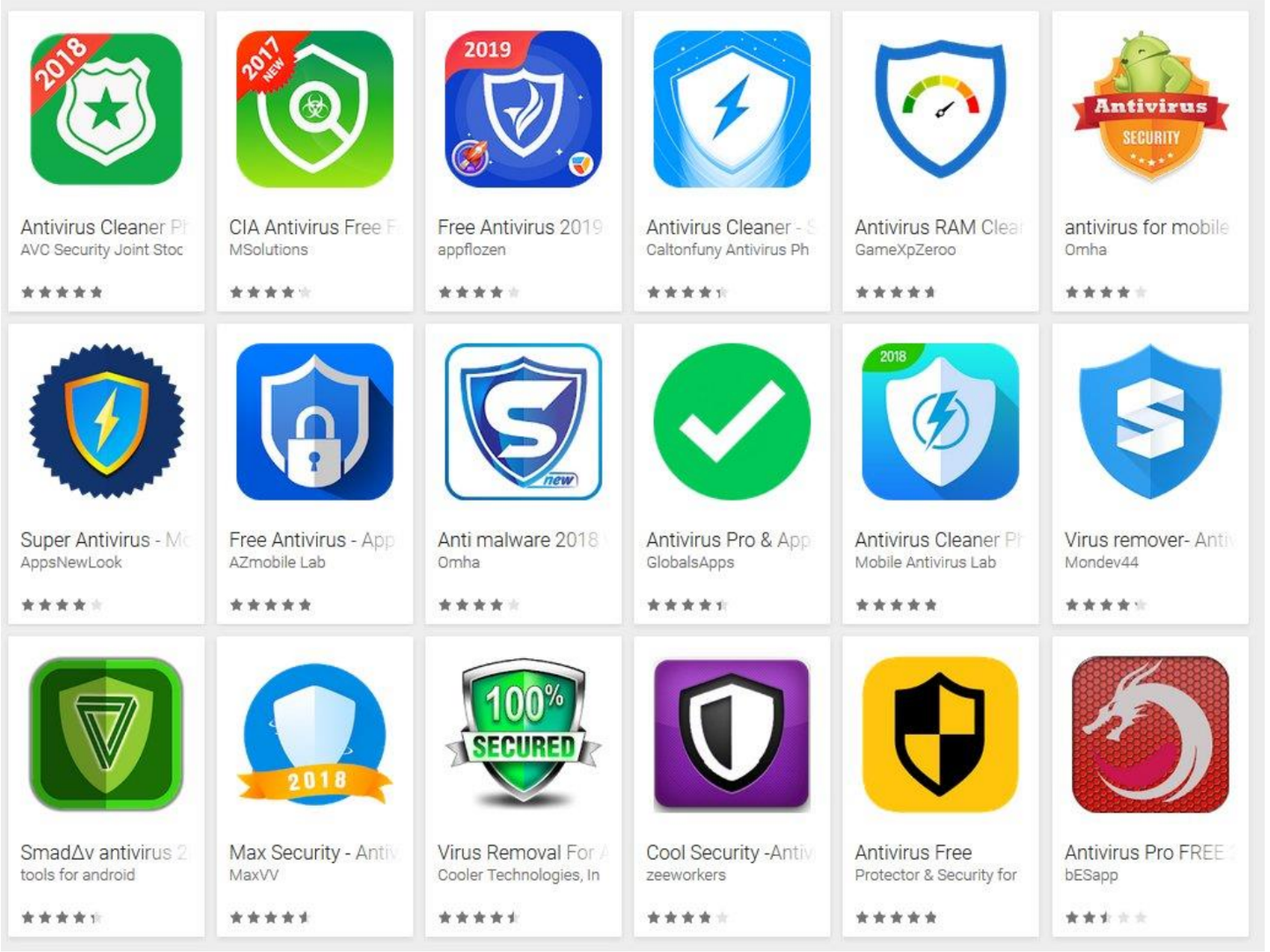


hesel jsou duplikáty nebo triviální kombinace

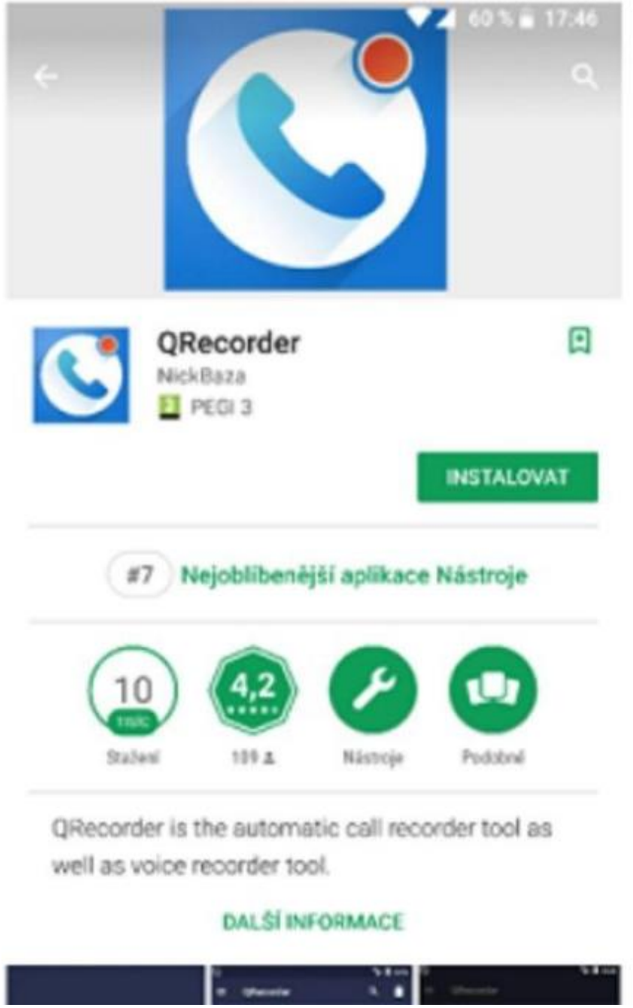


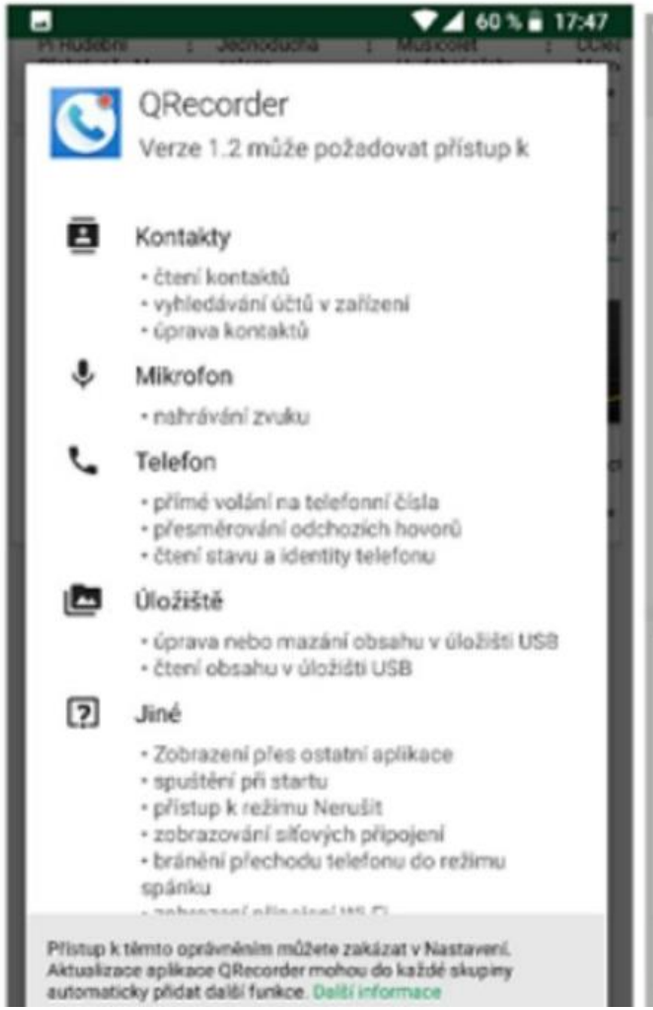
zaměstnanců používá stejná hesla pro práci i soukromí

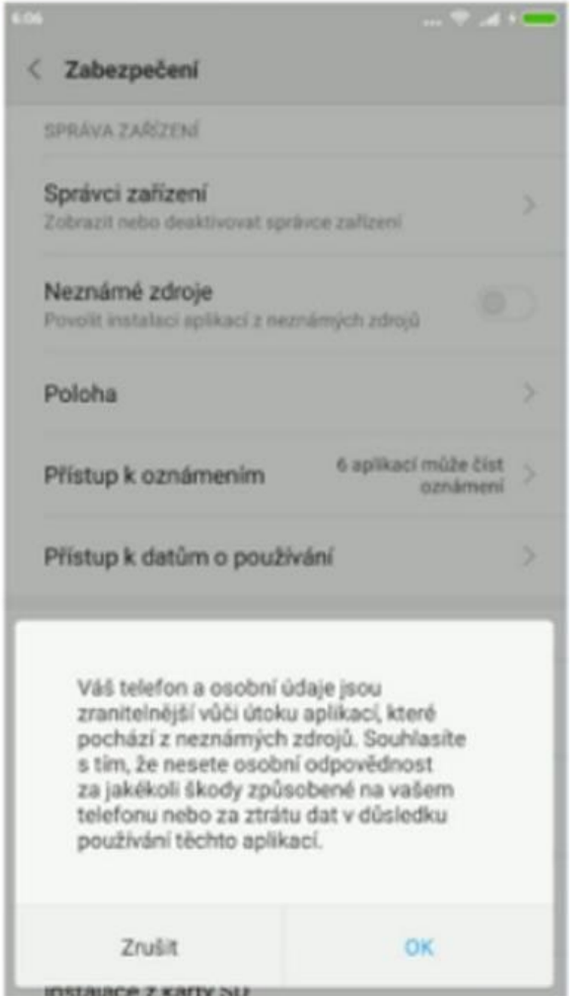
Mobilní zařízení



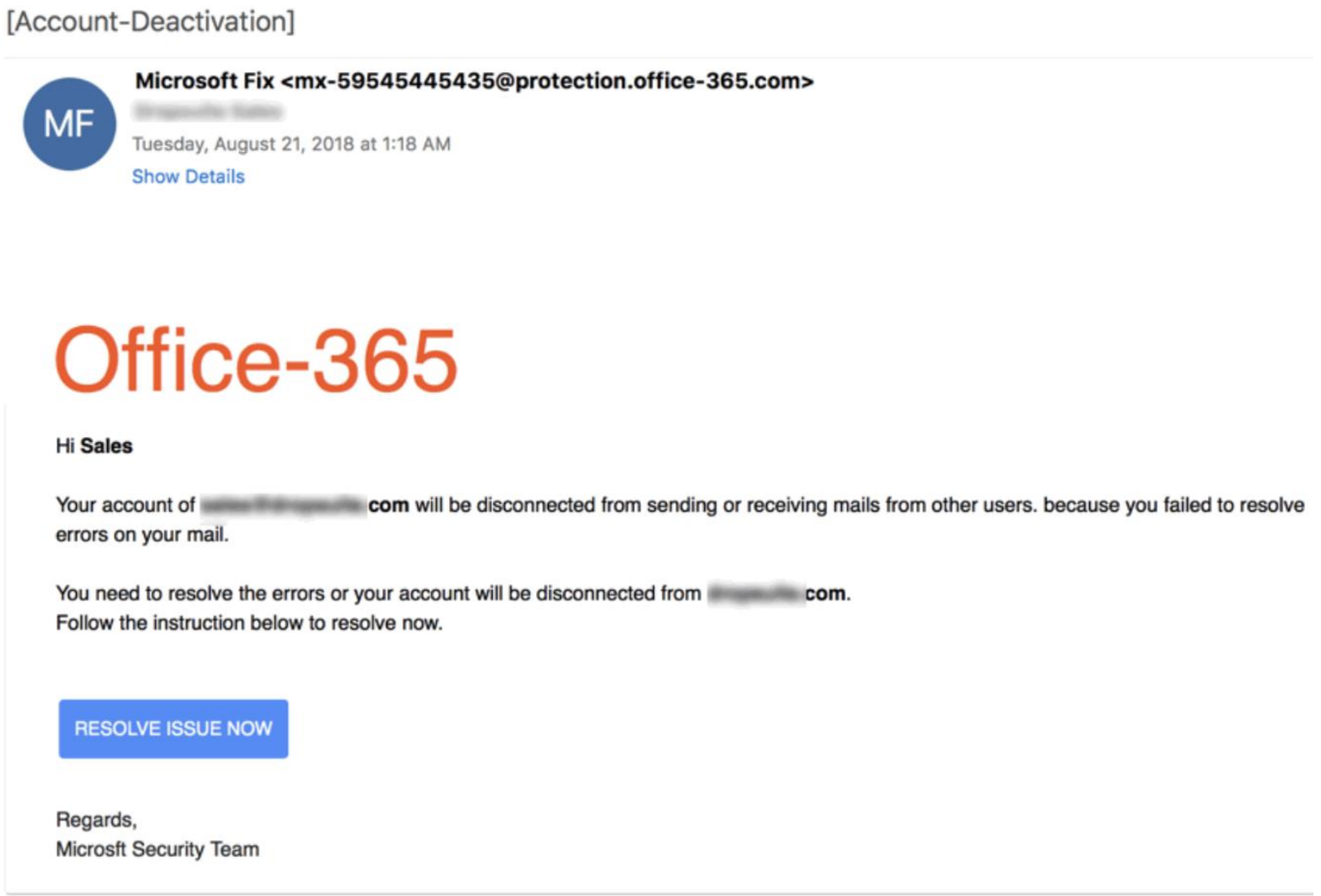
Mobilní zařízení







Phishing



[Account-Deactivation]

MF

Microsoft Fix <mx-59545445435@protection.office-365.com>

Tuesday, August 21, 2018 at 1:18 AM

Show Details

Office-365

Hi **Sales**

Your account of **com** will be disconnected from sending or receiving mails from other users. because you failed to resolve errors on your mail.

You need to resolve the errors or your account will be disconnected from **com**.
Follow the instruction below to resolve now.

RESOLVE ISSUE NOW

Regards,
Microsft Security Team

Phishing

Od: vse.cz - Email Support <sales7@agri-chemicals-ne.tk>
Odesláno: pondělí 27. ledna 2020 2:58
Komu: [redacted]
Předmět: info@vse.cz , Secured Email User Notification

Sent from a trusted sender.

MAIL SERVICE
Hello ***info***
We are closing all old versions and non-active users from 27/01/2020 07:01:18 AM (EDT).

Please confirm your email address info@vse.cz to keep your account from being deactivated.

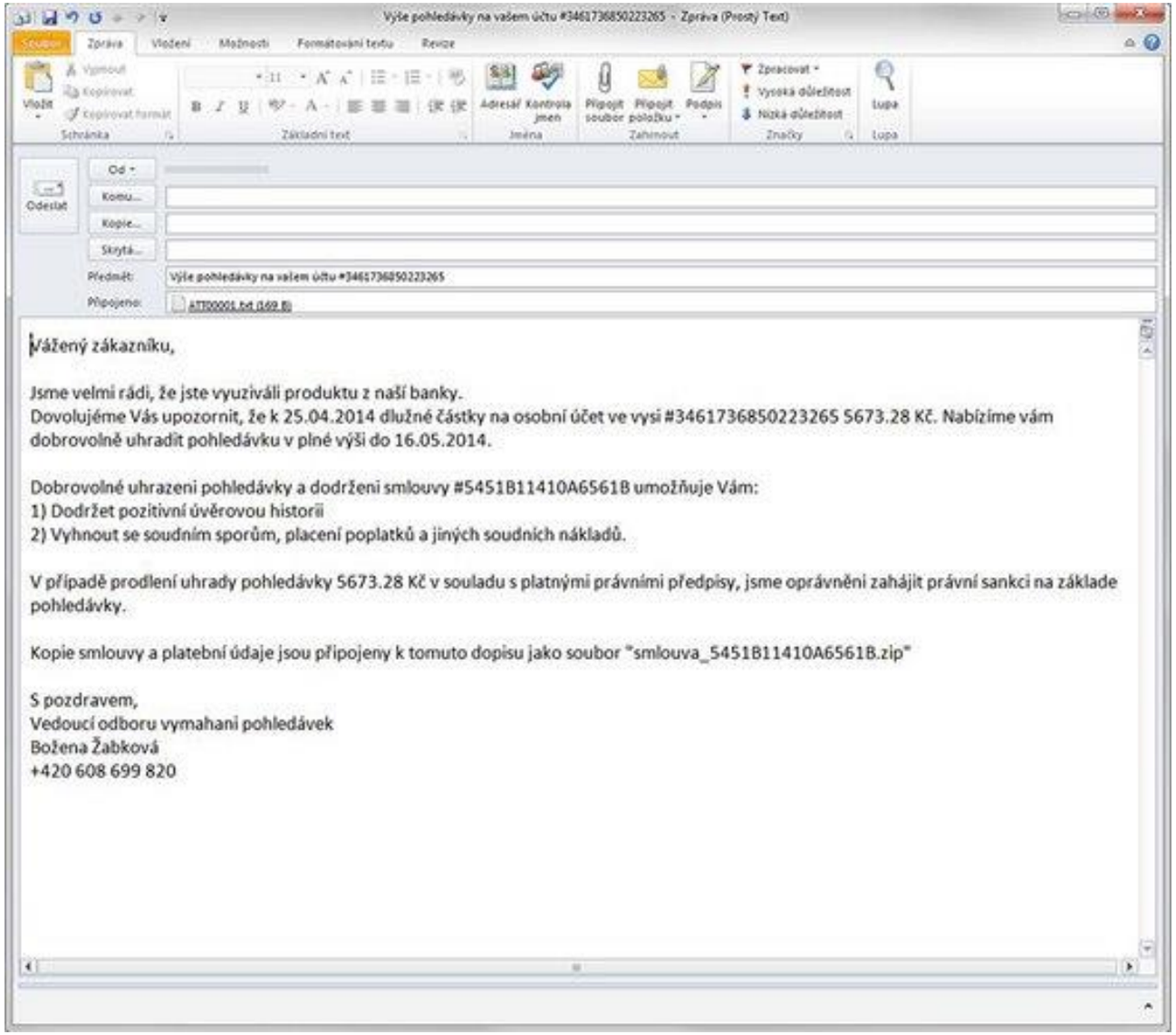
Confirm E-Mail

Account will be automatically deleted after (30/01/2020). You can change the frequency of these notifications within your mailbox portal.

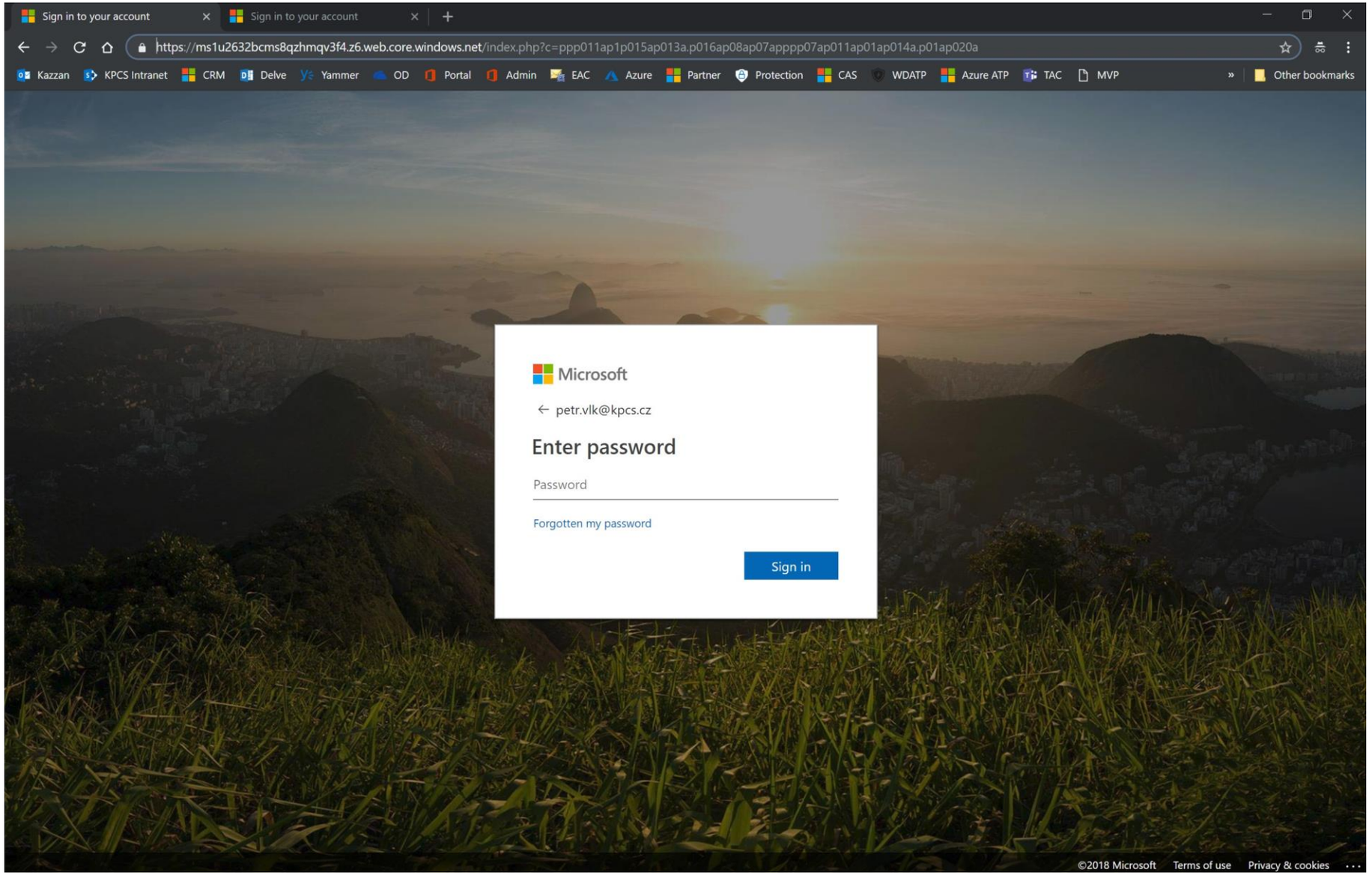
Best Regards

Administrator.

Phishing


Výše pohledávky na vašem účtu #3461736850223265 - Zpráva (Prostý Text)
Soubor
Zpráva
Vložení
Možnosti
Formátování textu
Revize
Vložit
Vyjmout
Kopírovat
Kopírovat formát
Schránka
Základní text
Adresář
Kontrola jmen
Jména
Připojit soubor
Připojit položku
Podpis
Zahrnout
Zpracovat
Vysoká důležitost
Nízká důležitost
Značky
Lupa
Odeslat
Od
Komu...
Kopie...
Skrytá...
Předmět:
Výše pohledávky na vašem účtu #3461736850223265
Připojeno:
ATT00001.txt (169 B)
Vážený zákazníku,
Jsme velmi rádi, že jste využiváli produktu z naší banky.
Dovolujéme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysi #3461736850223265 5673.28 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 16.05.2014.
Dobrovolné uhrazeni pohledávky a dodrženi smlouvy #5451B11410A6561B umožňuje Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.
V případě prodlení uhrady pohledávky 5673.28 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.
Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_5451B11410A6561B.zip"
S pozdravem,
Vedoucí odboru vymahani pohledávek
Božena Žabková
+420 608 699 820

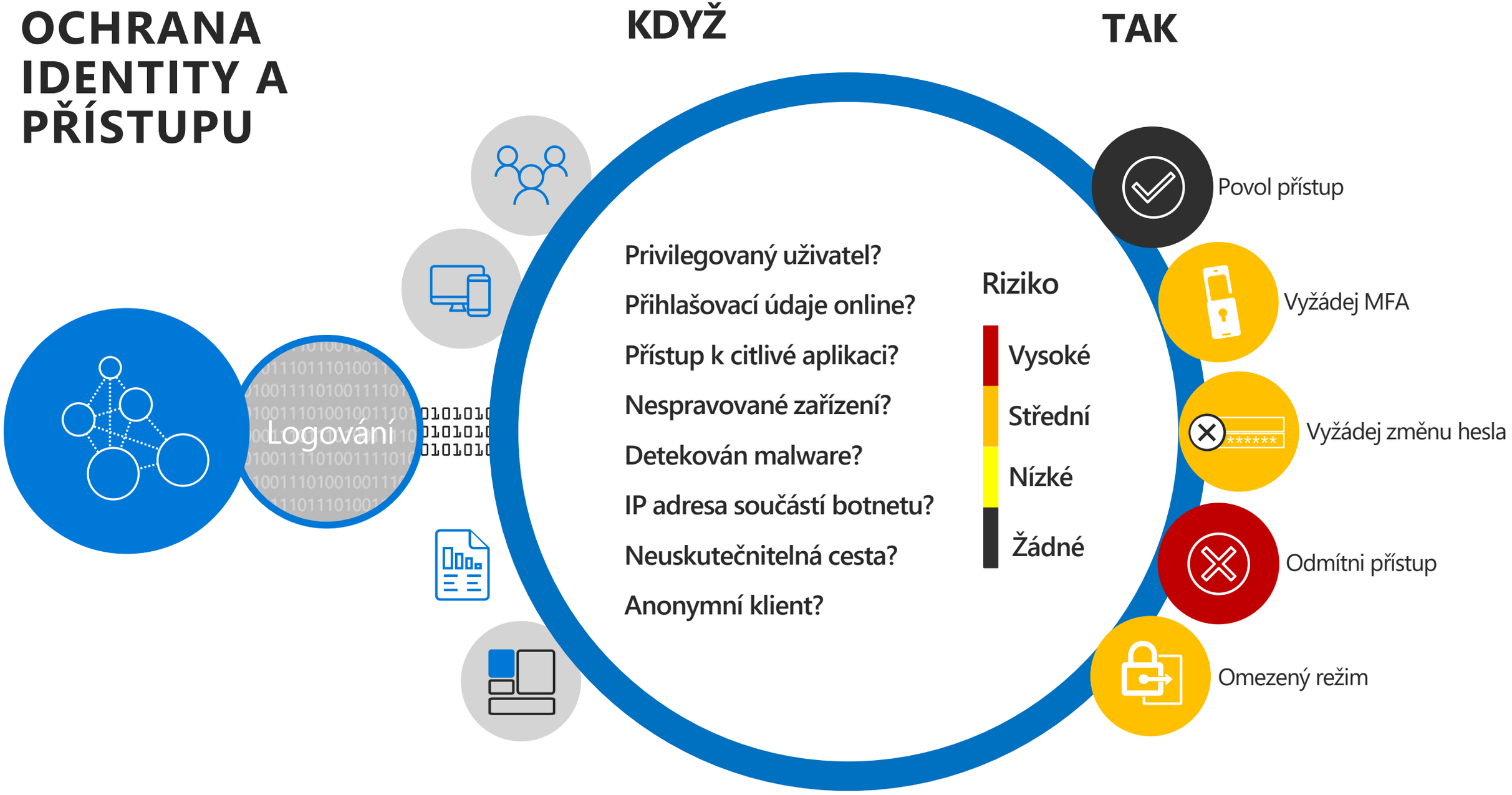
Phishing


Sign in to your account
Sign in to your account
https://ms1u2632bcms8qzhmqv3f4.z6.web.core.windows.net/index.php?c=ppp011ap1p015ap013a.p016ap08ap07apppp07ap011ap01ap014a.p01ap020a
Kazzan
KPCS Intranet
CRM
Delve
Yammer
OD
Portal
Admin
EAC
Azure
Partner
Protection
CAS
WDATP
Azure ATP
TAC
MVP
Other bookmarks
Microsoft
petr.vlk@kpcs.cz
Enter password
Password
Forgotten my password
Sign in
©2018 Microsoft
Terms of use
Privacy & cookies

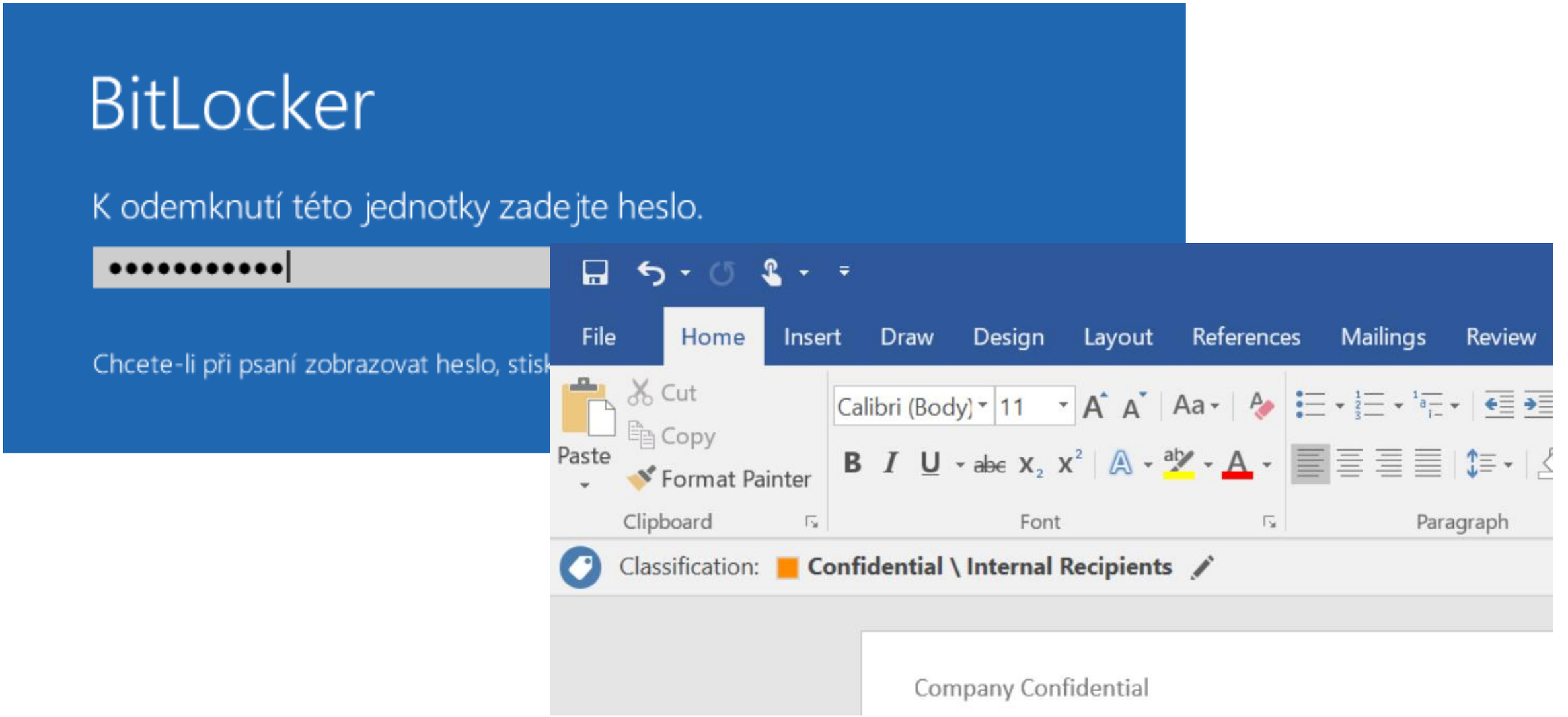
Phishing


http://www.jetdrop.co.uk/bin/themes/Sal
Přihlášení SERVIS 24 | Česká...
Soubor Úpravy Zobrazit Oblíbené položky Nástroje Nápověda
SERVIS 24
INTERNETBANKING
Hledat v Internetbankingu a na webu Fio
Nový produkt
Nastavení Odhlá
Nástěnka Poslat peníze Přehledy Platební karty Šablony Informace o účtu
Ověření vašich osobních údajů
Každoroční aktualizace vašich osobních údajů
Čas příjmu dočasného kódu pomocí SMS závisí na vaší síti. Za více než 3 minuty :
2:17
Chcete-li dokončit žádost o opětovné zapnutí, zadejte prosím váš referenční kód obdržený pomocí SMS :
Potvrdit
ČESKÁ spořitelna
Bezpečnost | Kontakty | O službě | Pro nevidomé | Demo | Více informací
2018 © Česká spořitelna, a. s. - všechna práva vyhrazena.

OCHRANA IDENTITY A PŘÍSTUPU



Uložení dat a šifrování

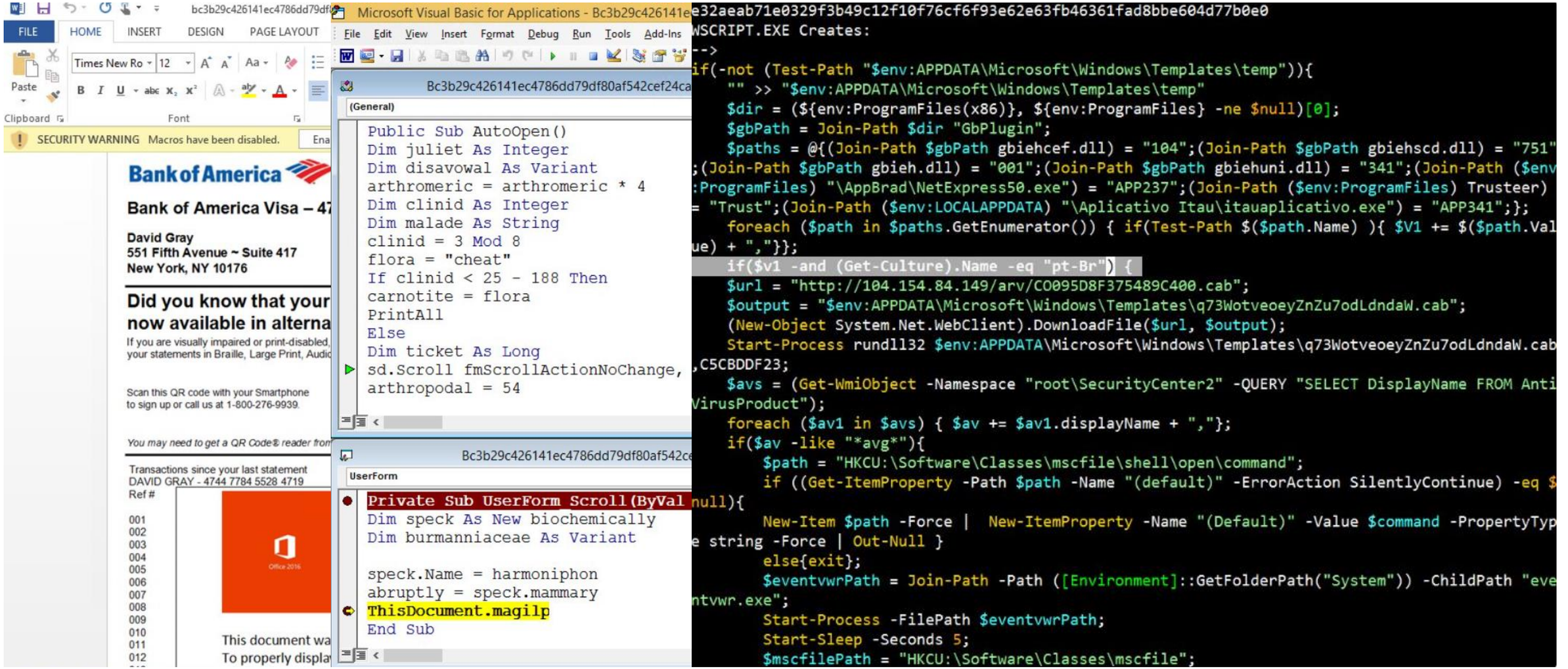


Aktualizace, konfigurace a evidence

16 řádků…

- Co ten skript asi dělá?
- A jak na to budete reagovat?

Nezáleží jen na jedné komponentě



Aktualizace, konfigurace a evidence

Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address:
Involved host name:
Source or intermediary sites:

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

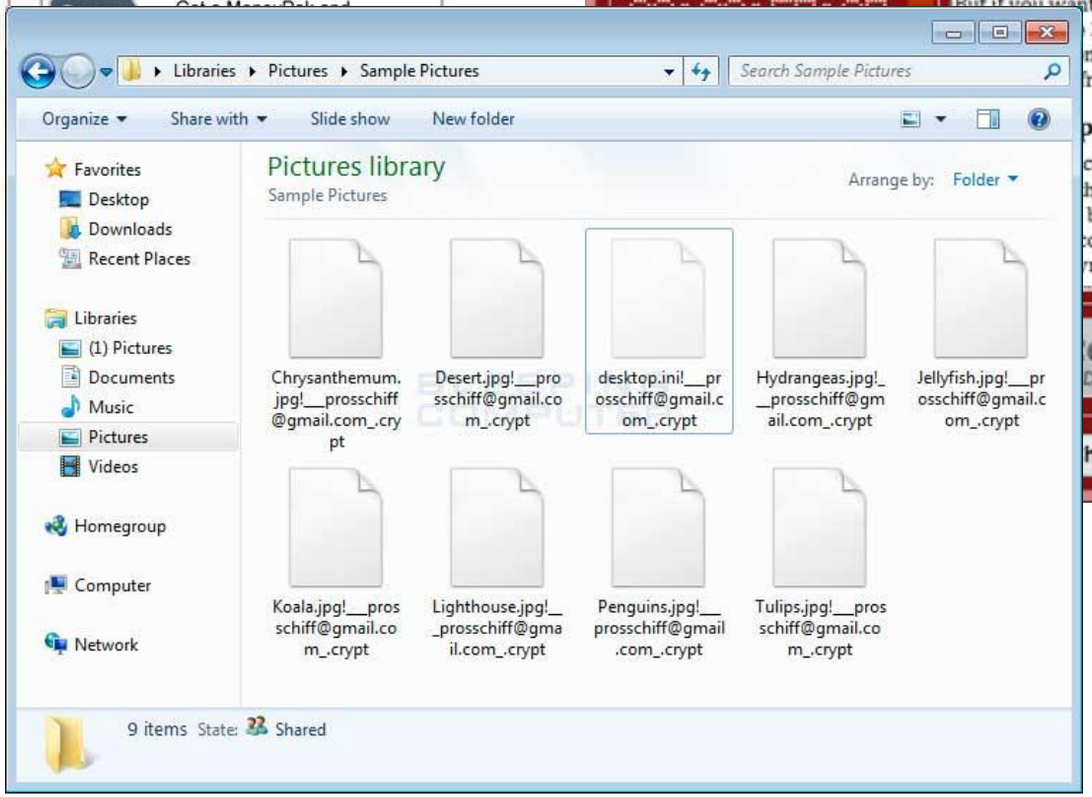
Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

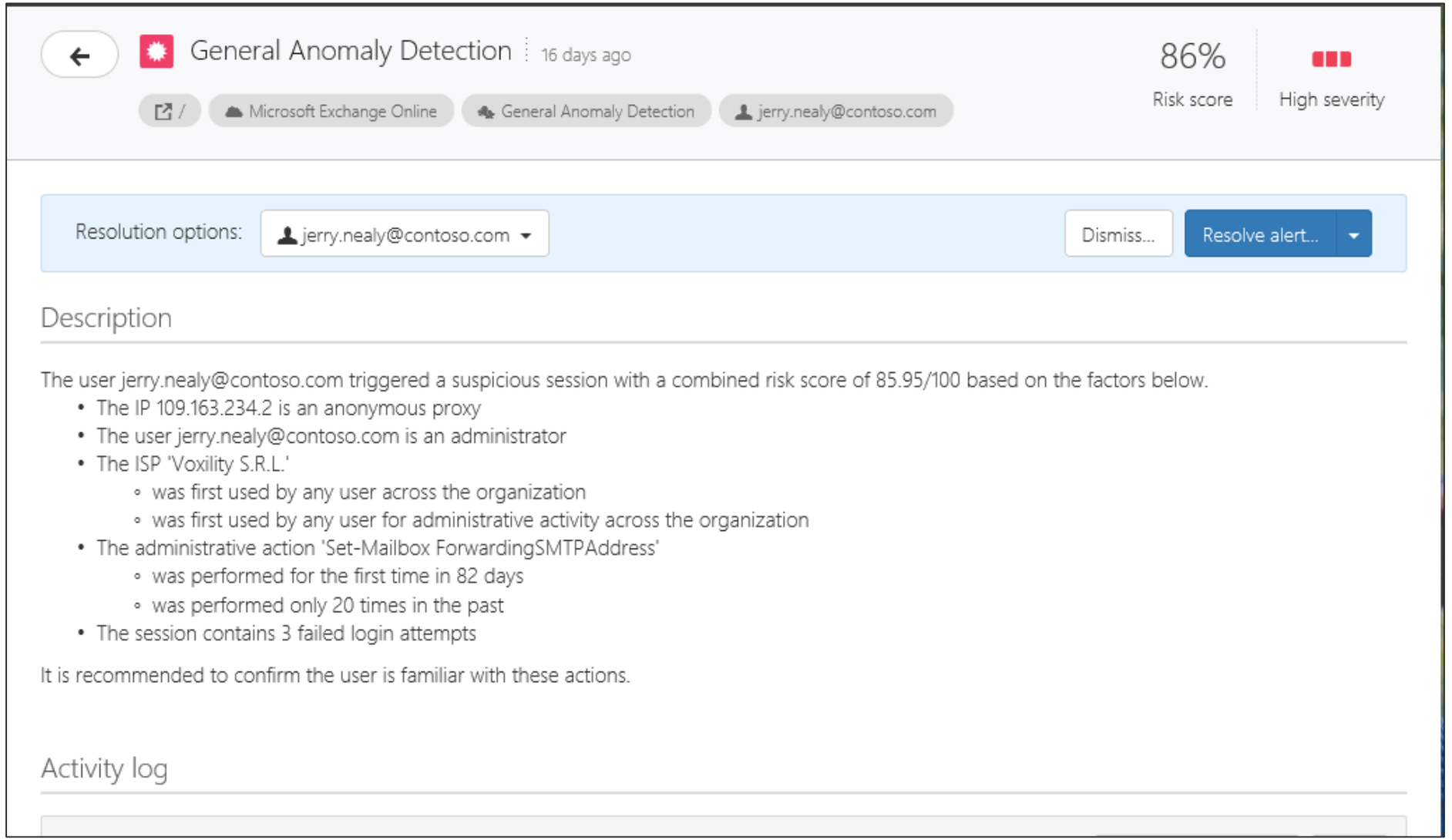
Permanent lock on

HOW TO UNLOCK YOUR COMPUTER:

1 $ Take your cash to one of this retail locations:
Walmart, CVS/pharmacy, Walgreens

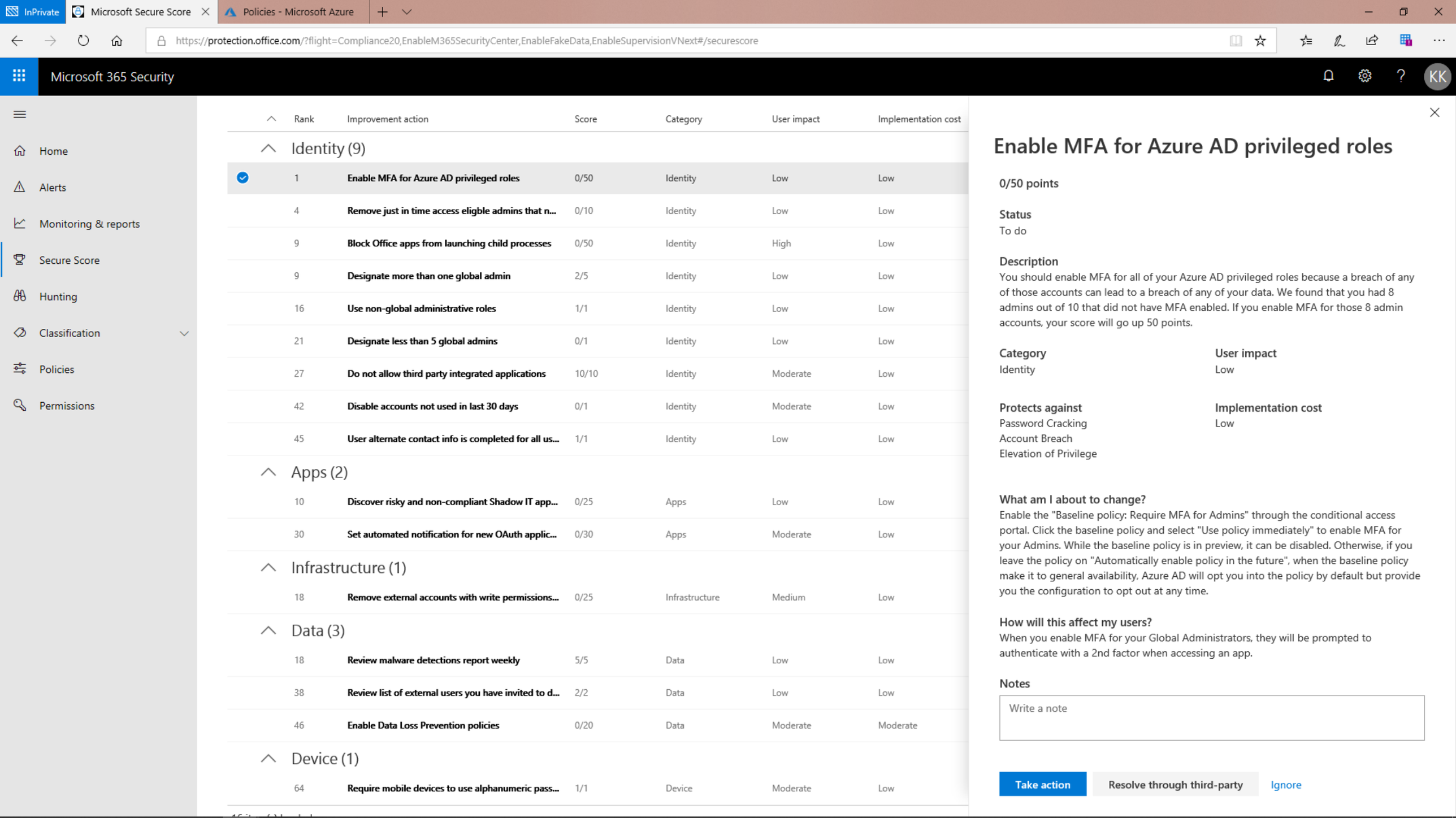


Anomálie


General Anomaly Detection
16 days ago
86%
Risk score
High severity
/
Microsoft Exchange Online
General Anomaly Detection
jerry.nealy@contoso.com
Resolution options:
jerry.nealy@contoso.com
Dismiss...
Resolve alert...
Description
The user jerry.nealy@contoso.com triggered a suspicious session with a combined risk score of 85.95/100 based on the factors below.
The IP 109.163.234.2 is an anonymous proxy
The user jerry.nealy@contoso.com is an administrator
The ISP 'Voxility S.R.L.'
was first used by any user across the organization
was first used by any user for administrative activity across the organization
The administrative action 'Set-Mailbox ForwardingSMTPAddress'
was performed for the first time in 82 days
was performed only 20 times in the past
The session contains 3 failed login attempts
It is recommended to confirm the user is familiar with these actions.
Activity log

Znáte kontext svého prostředí?

Demo?


InPrivate
Microsoft Secure Score
Policies - Microsoft Azure
https://protection.office.com/?flight=Compliance20,EnableM365SecurityCenter,EnableFakeData,EnableSupervisionVNext#/securescore
Microsoft 365 Security
KK
Home
Alerts
Monitoring & reports
Secure Score
Hunting
Classification
Policies
Permissions
Rank
Improvement action
Score
Category
User impact
Implementation cost
Identity (9)
1 Enable MFA for Azure AD privileged roles 0/50 Identity Low Low
4 Remove just in time access eligble admins that n... 0/10 Identity Low Low
9 Block Office apps from launching child processes 0/50 Identity High Low
9 Designate more than one global admin 2/5 Identity Low Low
16 Use non-global administrative roles 1/1 Identity Low Low
21 Designate less than 5 global admins 0/1 Identity Low Low
27 Do not allow third party integrated applications 10/10 Identity Moderate Low
42 Disable accounts not used in last 30 days 0/1 Identity Moderate Low
45 User alternate contact info is completed for all us... 1/1 Identity Low Low
Apps (2)
10 Discover risky and non-compliant Shadow IT app... 0/25 Apps Low Low
30 Set automated notification for new OAuth applic... 0/30 Apps Moderate Low
Infrastructure (1)
18 Remove external accounts with write permissions... 0/25 Infrastructure Medium Low
Data (3)
18 Review malware detections report weekly 5/5 Data Low Low
38 Review list of external users you have invited to d... 2/2 Data Low Low
46 Enable Data Loss Prevention policies 0/20 Data Moderate Moderate
Device (1)
64 Require mobile devices to use alphanumeric pass... 1/1 Device Moderate Low
Enable MFA for Azure AD privileged roles
0/50 points
Status
To do
Description
You should enable MFA for all of your Azure AD privileged roles because a breach of any of those accounts can lead to a breach of any of your data. We found that you had 8 admins out of 10 that did not have MFA enabled. If you enable MFA for those 8 admin accounts, your score will go up 50 points.
Category
Identity
User impact
Low
Protects against
Password Cracking
Account Breach
Elevation of Privilege
Implementation cost
Low
What am I about to change?
Enable the "Baseline policy: Require MFA for Admins" through the conditional access portal. Click the baseline policy and select "Use policy immediately" to enable MFA for your Admins. While the baseline policy is in preview, it can be disabled. Otherwise, if you leave the policy on "Automatically enable policy in the future", when the baseline policy make it to general availability, Azure AD will opt you into the policy by default but provide you the configuration to opt out at any time.
How will this affect my users?
When you enable MFA for your Global Administrators, they will be prompted to authenticate with a 2nd factor when accessing an app.
Notes
Write a note
Take action
Resolve through third-party
Ignore

Home
Alerts
Monitoring & reports
Secure Score
Hunting
Classification
Policies
Permissions

Monitoring & reports

View status and trends for the security of your Microsoft 365 devices, data, identities, apps, and infrastructure. Learn more

Group by category

Identities (3)

Identity protection

55 users at risk

High risk Medium risk No risk

View all users

Cloud App Security - Anomaly detection

Users with detections

User	Alerts
Armin Hoffman	56
Emil Ruder	45
Josef Muller Brockmann	32
Adrian Frutiger	27
Max Miedinger	16
Max Bill	15
Le Corbusier	8
Ralph Schraivogel	4
Niklaus Troxler	2

See more

Global admins

Reduce global admins

8 global admins

Global admins have access to all your data and tools. Limiting the number of users with this role lowers the risk to your organization.

Manage roles

Data (7)

Feedback

InPrivate | Monitoring & reports - | Policies - Microsoft Azure

https://protection.office.com/?flight=Compliance20,EnableM365SecurityCenter,EnableFakeData,EnableSupervisionVNext#/reports

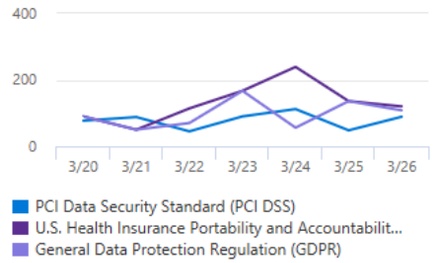
Microsoft 365 Security

KK

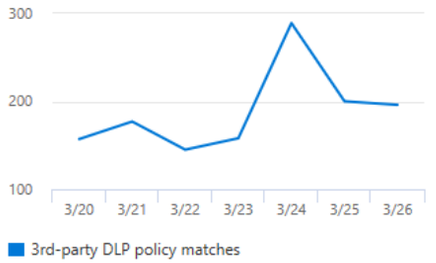
- Home
- Alerts
- Monitoring & reports
- Secure Score
- Hunting
- Classification
- Policies
- Permissions

Data (7)

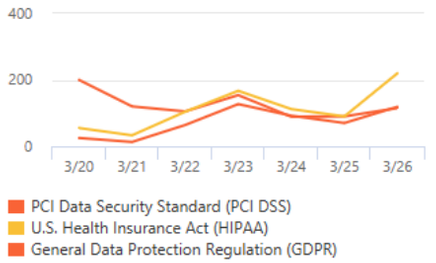
DLP policy matches



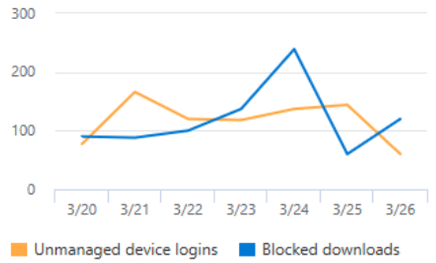
3rd-party DLP policy matches



DLP false positive and override



Conditional access app control



Users sharing files

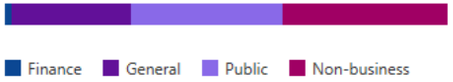
Users who shared the most files in cloud apps

User	Files shared
Kelly Wilson	140
Marco Dinkins	132
Roseann Albert	112
Lisa Sherman	88
Damian Mattos	72
Russell Lynch	55
Niklas Bosley	32
Le Corbusier	23
Ralph Schraivogel	16

Show more

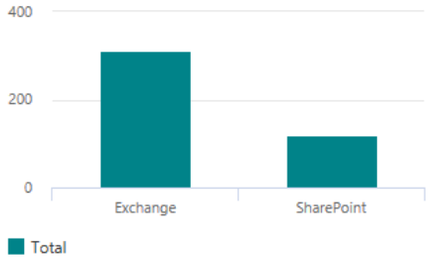
Top Labels

123 Non-business



Manage labels

Top Labels by location



Feedback

InPrivate | Monitoring & reports - | Policies - Microsoft Azure

https://protection.office.com/?flight=Compliance20,EnableM365SecurityCenter,EnableFakeData,EnableSupervisionVNext#/reports

Microsoft 365 Security

KK

- Home
- Alerts
- Monitoring & reports
- Secure Score
- Hunting
- Classification
- Policies
- Permissions

Devices (11)

Device protection

34 devices at risk

Device	Risk level
tocohen1	High
tocohen2	Moderate
tocohen3	Low
tocohen4	High
tocohen5	High
tocohen6	High
tocohen7	High
tocohen8	High
tocohen9	High

View details

Attack surface reduction rules

90% of devices use attack surface reduction rules

Updated 7:50 PM today

Block mode | Audit mode | Mixed mode | Off

Device settings by rule

Execution of executable content (exe, dll, ps, j...	112.6k/112.6k	Office apps launching child processes	112.6k/112.6k
Office apps/macros creating executable content	89.8k/112.6k	Office apps injecting into other processes (no...	84.4k/112.6k
js/vbs executing payload downloaded from In...	86.3k/112.6k	Obfuscated js/vbs/ps/macro code	73.5k/112.6k
Win32 imports from Office macro code	89.9k/112.6k	Executables that don't meet a prevalence, age...	101.3k/112.6k
Advanced ransomware protection	84.5k/112.6k	Flag credential stealing from the Windows loc...	74.7k/112.6k
Process creation from PSExec and WMI comm...	76.7k/112.6k	Untrusted and unsigned processes that run fro...	78k/112.6k

Block mode | Audit mode | Off

View all devices | View devices in audit mode | View devices with ASR off

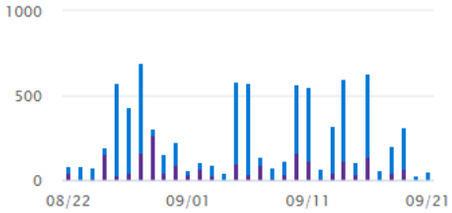
Attack surface reduction rule detections

Possible malware or breach activity on your devices

updated 7:50 PM today

8.3k detections
145 unique files
6k affected devices

Detections over time



Blocked | Audited

View detected files | Simulate exclusions

Device compliance

35% noncompliant

Noncompliant | In grace period
Compliant | Not evaluated

See compliance issues

Device malware detections

15 unresolved malware

Active | Action failed | Allowed
Not executed

View details

Device threat analytics

Assess your defenses against high-profile threats

Read about the latest attack campaigns, malware outbreaks, and other notable threats. Review devices with related alerts and devices that don't have the recommended mitigations.

View all threats

GADOLINIUM / FoggyBrass	12 / 16
Dofoil / CoinMiner	10 / 13
Zacinlo(Detrahere)	1 / 7
EternalBlue endures	2 / 4
Emotet distributes Trickbot	3 / 3

Feedback

InPrivate | Monitoring & reports - | Policies - Microsoft Azure

https://protection.office.com/?flight=Compliance20,EnableM365SecurityCenter,EnableFakeData,EnableSupervisionVNext#/reports

Microsoft 365 Security

KK

- Home
- Alerts
- Monitoring & reports
- Secure Score
- Hunting
- Classification
- Policies
- Permissions

Apps (8)

Cloud App Security - OAuth apps

248 privileged apps

High Medium Low

App	Permission level
Boomerang	High
Yesware email tracking	High
Jira for Outlook	High
Pickit Free Images	Medium
officeatwork Template Chooser	Medium
MyScript Math Sample	Medium

Show more

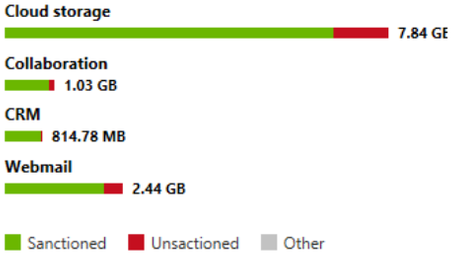
Cloud app accounts for review

User accounts that require attention based on Cloud App Security alerts

Last 30 days, updated 6:20 pm today

3 suspicious admin activity
46 possible impersonations
136 inactive accounts

Discovered cloud apps (categories)



Cloud app activity locations

Common countries where your users are accessing cloud apps

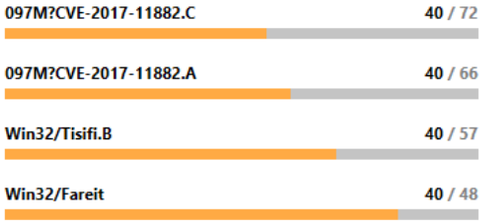
Last 30 days, updated 6:20 pm today

101.4k from the United States
9k from France
18.5k from China

Email threat analytics

Investigate high-profile threats that arrive on email

View data on trending and widespread mailware campaigns and assess their impacts to your data and email accounts.



Email protection

12 email accounts at risk

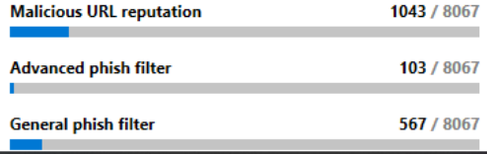
Email account	User
armin.hoffman@contoso.com	Armin Hoffman
mike.dearson@contoso.com	Mike Dearson
eva.macias@contoso.com	Eva Macias

Malicious content blocked

Updated 6:20 pm today

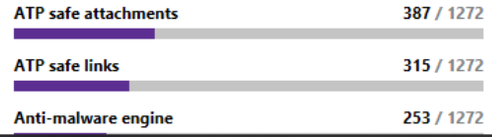
8067 phishing blocks

Total phishing attempts blocked by Office365 ATP features



1272 malware blocks

Total malware in email or content blocked by Office365 ATP features



Malware in email

Last 30 days, updated 6:20 pm today

610 Win32/Tisifi.B
382 Win32/Fareit
143 Win32/Dridex

Feedback

Home
Alerts
Monitoring & reports
Secure Score
Hunting
Classification
Policies
Permissions

lee.rob@contoso.com	Lee Rob
michael.lee@contoso.com	Michael Lee

See more

User impersonation	98 / 8067
Domain impersonation	112 / 8067
Phish zap	55 / 8067

Infrastructure (3)

Infrastructure health

Some resources need attention

Health status of your resources protected by Azure Security Center

Updated 6:20 pm today

- 28 compute resources
- 14 networking resources
- 19 storage and data resources
- 12 application resources
- 2 IOT resources
- 4 miscellaneous resources

Critical Warning Healthy

View details

Azure security subscription coverage

80% covered

Covered (standard) Covered (free) Not covered

Improve coverage

Azure policy compliance

91% compliant

Compliant Not compliant

View details

Feedback

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 / 1,254

Updated 6:20 pm today

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

See more

Email protection

12 email accounts at risk /1,022

Updated 6:20 pm today

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

Black Energy 13 active/142

Threat News

"BadKitten" - New threat in town
Check organization vulnerability

Start hunting!
GitHub shared new query

M365

https://security.microsoft.com

Microsoft 365 Security

Incidents

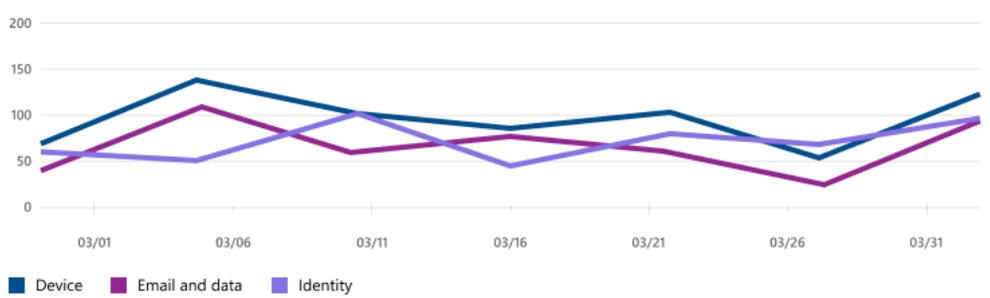
Active incidents

27 active incidents

Updated 6:20 pm today

High (4) Medium (16) Low (7)

Incident scope



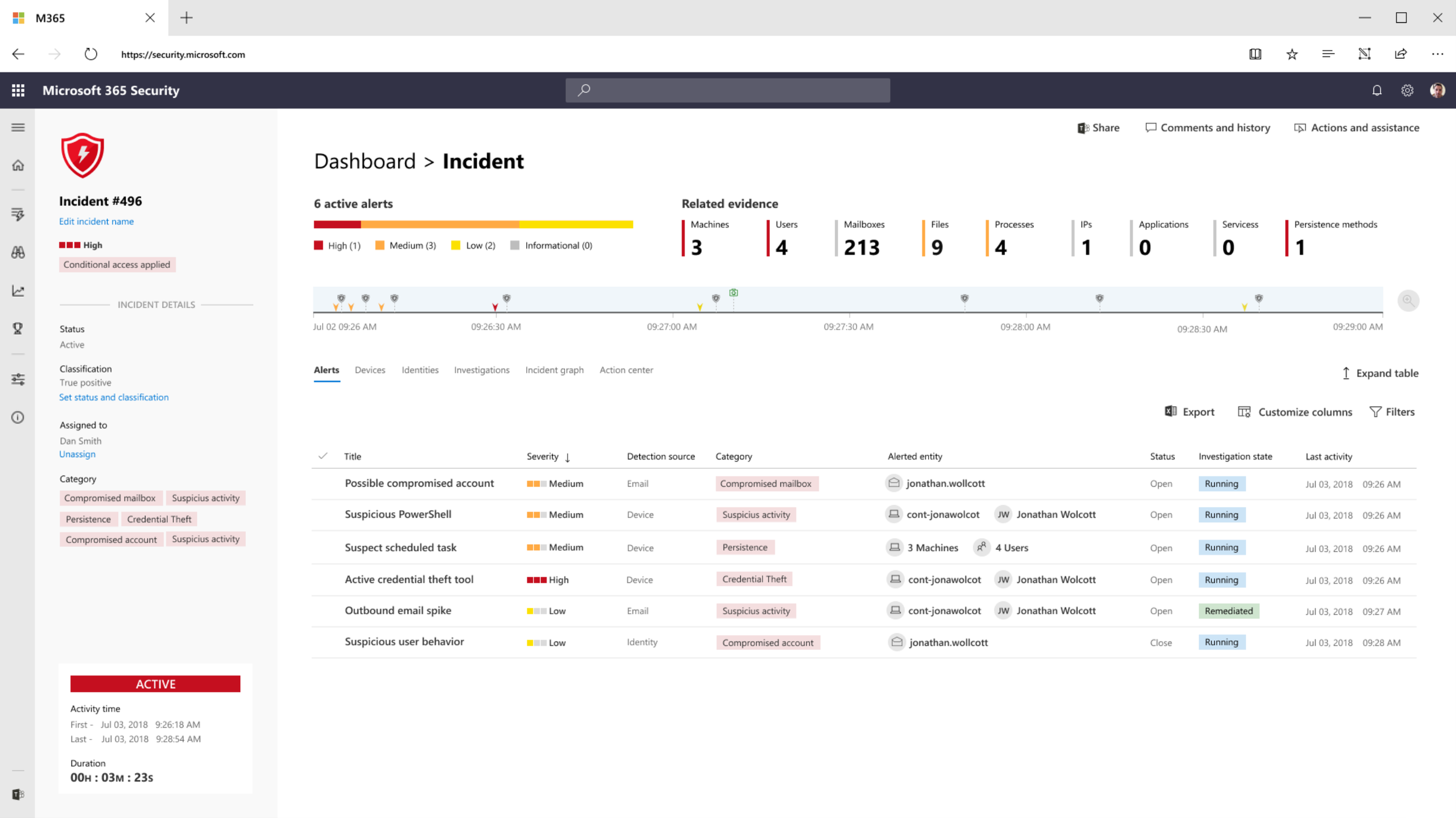
Incident by status

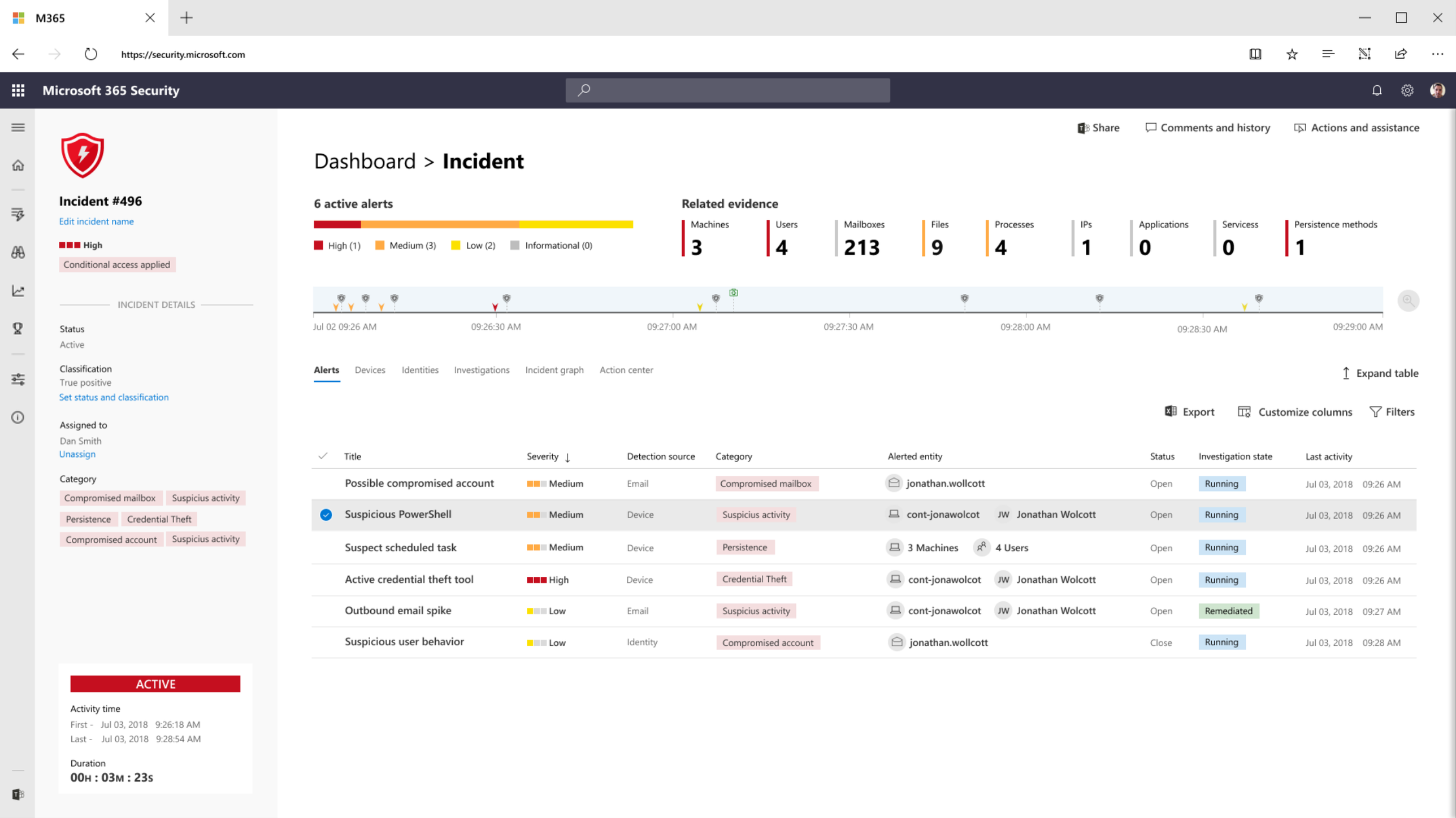
New	Investigating	Resolved
12	15	40+

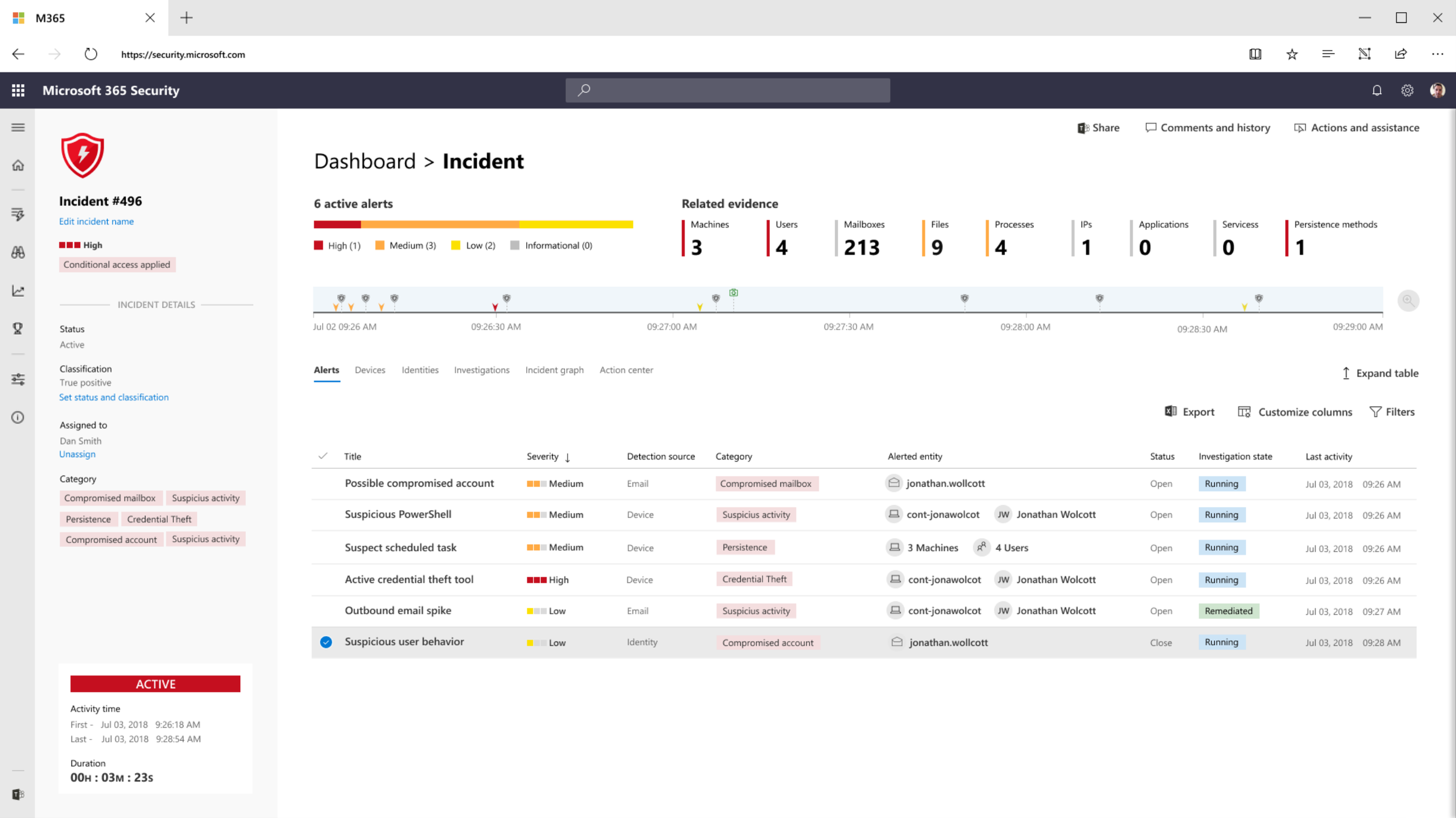
Updated 6:20 pm today

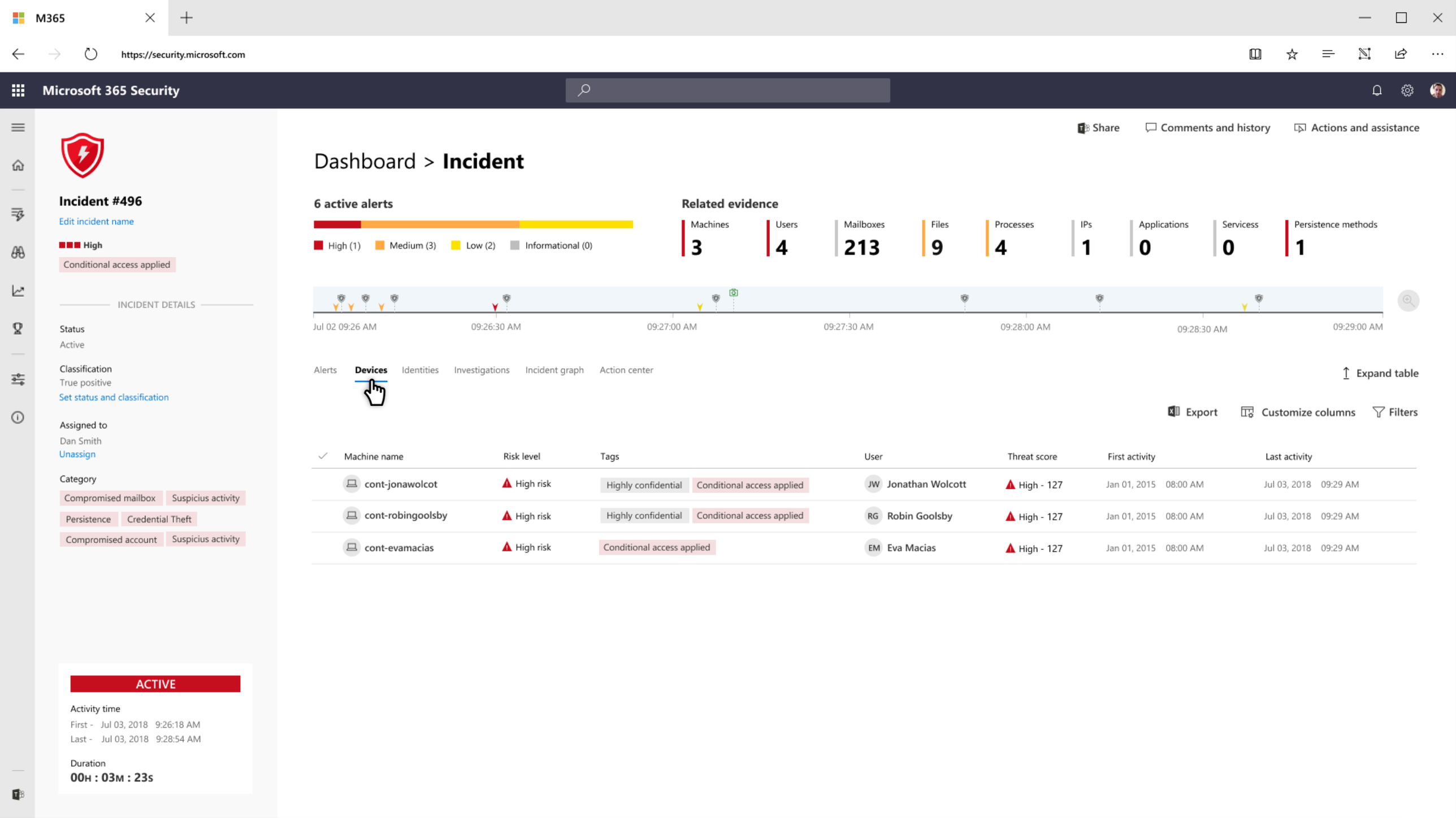
Export Customize columns Filter

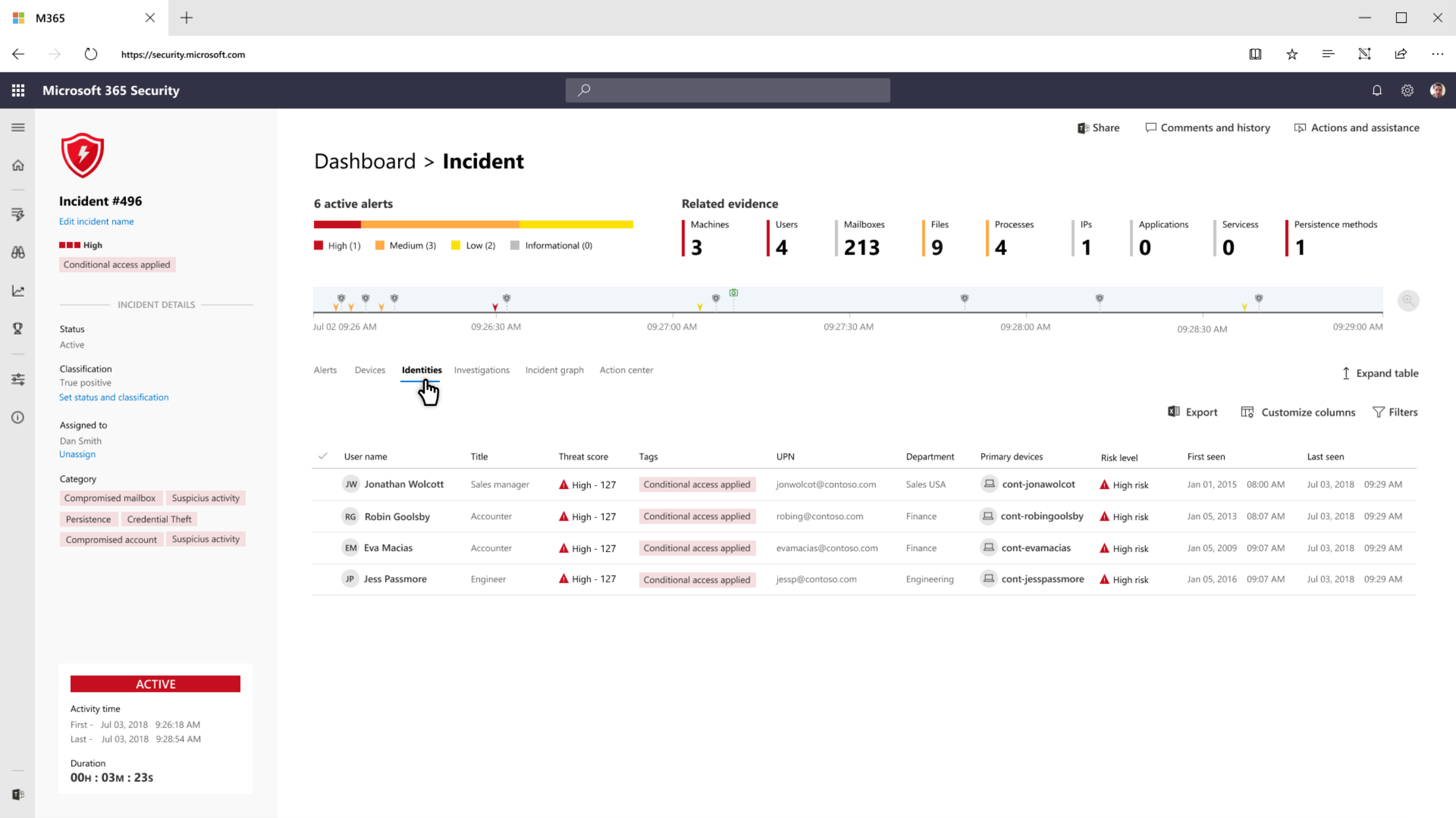
Incident name	Severity	Category	Detection source	Alerted entity	Last activity	Classification	Status
Incident #496	High	Credential Theft, Compromised Account	Email, Device, User	204 email accounts, cont-jonawolcot, JW Jonathan Wolcott	April 10, 2018 10:26:22	True	Acrtive
Comm cation from remote process, Remote shell, Kernel...	High	Privilege Escalation	Device, User	4 machines, 8 users	April 10, 2018 10:26:00	Not set	Active
InstallCore unwanted software	High	Persistence	Device, User	3 machines, 3 users	April 10, 2018 10:23:29	True	Acrtive
Malicious URL, Active Speesipro malware	High	Suspicious Activity	Email, Device, User	12 email accounts, 2 machines, 2 users	April 10, 2018 09:25:24	True	Active
Ransomware attack	High	Suspicious Activity, Persistence	Email	213 email accounts, 4 users	April 10, 2018 10:25:23	True	Acrtive
Suspicious file, Suspicious script	Medium	Suspicious Activity	Device, User	3 machines, 4 users	April 10, 2018 09:24:23	True	Active
Malicious URL, Active Speesipro malware	Medium	Reconnaissance	Device, User	2 machines, 5 users	April 10, 2018 08:15:24	True	Acrtive
Suspicious script	Medium	Reconnaissance	Device, User	2 machines, 3 users	April 10, 2018 10:25:26	True	Active
Incident #436	Medium	Reconnaissance	Device, User	cont-evamacias, EM Eva Macias	April 10, 2018 09:24:23	True	Acrtive
Incident #415	Medium	Suspicious Activity	Device, User	4 machines, 4 users	April 10, 2018 10:25:22	True	Active


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Machine name
Risk level
Tags
User
Threat score
First activity
Last activity
cont-jonawolcot
High risk
Highly confidential
Conditional access applied
JW Jonathan Wolcott
High - 127
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM
cont-robingoolsby
High risk
Highly confidential
Conditional access applied
RG Robin Goolsby
High - 127
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM
cont-evamacias
High risk
Conditional access applied
EM Eva Macias
High - 127
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
User name
Title
Threat score
Tags
UPN
Department
Primary devices
Risk level
First seen
Last seen
Jonathan Wolcott
Sales manager
High - 127
Conditional access applied
jonwolcot@contoso.com
Sales USA
cont-jonawolcot
High risk
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM
Robin Goolsby
Accounter
High - 127
Conditional access applied
robing@contoso.com
Finance
cont-robingoolsby
High risk
Jan 05, 2013 08:07 AM
Jul 03, 2018 09:29 AM
Eva Macias
Accounter
High - 127
Conditional access applied
evamacias@contoso.com
Finance
cont-evamacias
High risk
Jan 05, 2009 09:07 AM
Jul 03, 2018 09:29 AM
Jess Passmore
Engineer
High - 127
Conditional access applied
jessp@contoso.com
Engineering
cont-jesspassmore
High risk
Jan 05, 2016 09:07 AM
Jul 03, 2018 09:29 AM

M365

https://security.microsoft.com

Microsoft 365 Security

Share | Comments and history | Actions and assistance

Dashboard > **Incident**

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

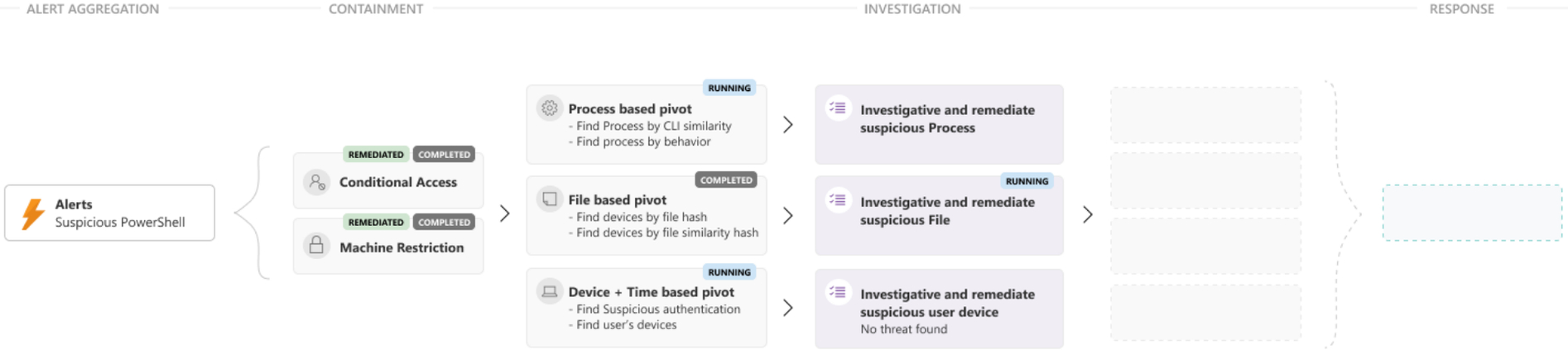
Duration
00H : 03M : 23S

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

Triggering alert	Investigation state	Investigated entities	Start date	Duration
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
Suspicious PowerShell	Running	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20



Share | Comments and history | Actions and assistance

Dashboard > **Incident**

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

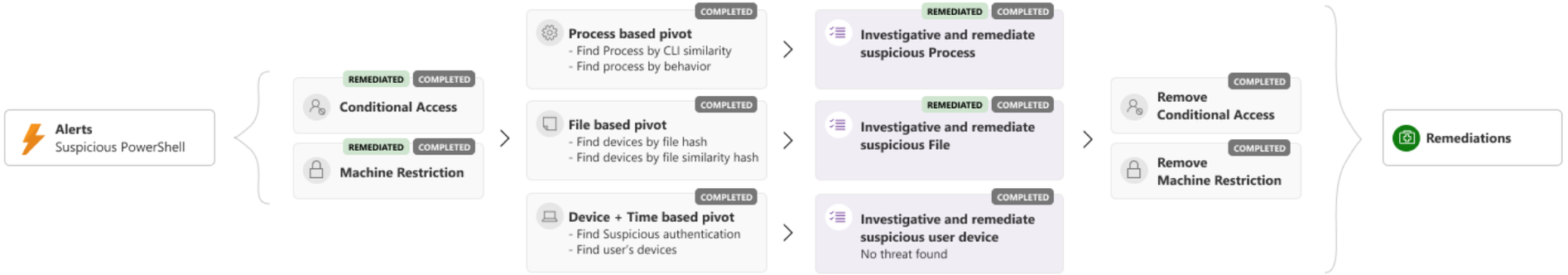
Duration
00H : 03M : 23S

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

Triggering alert	Investigation state	Investigated entities	Start date	Duration
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20



M365

https://security.microsoft.com

Microsoft 365 Security

Share | Comments and history | Actions and assistance

Dashboard > **Incident**

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

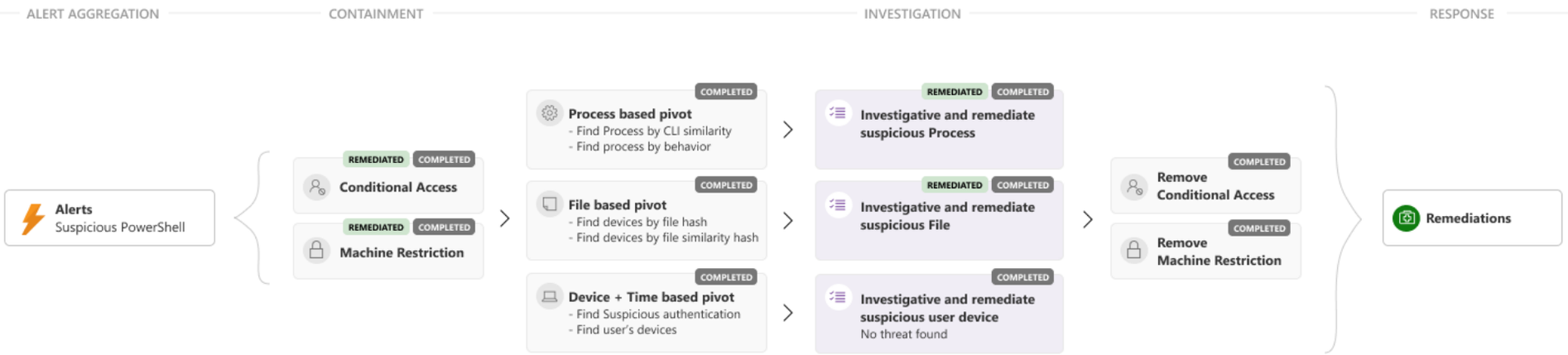
Duration
00H : 03M : 23S

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

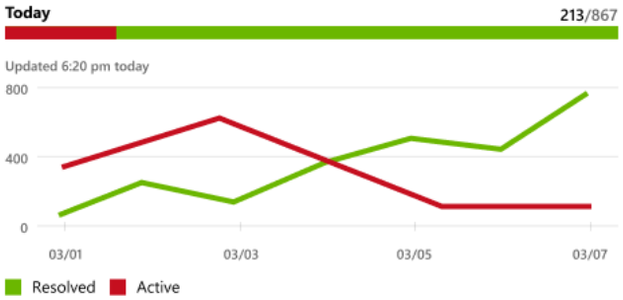
Triggering alert	Investigation state	Investigated entities	Start date	Duration
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20



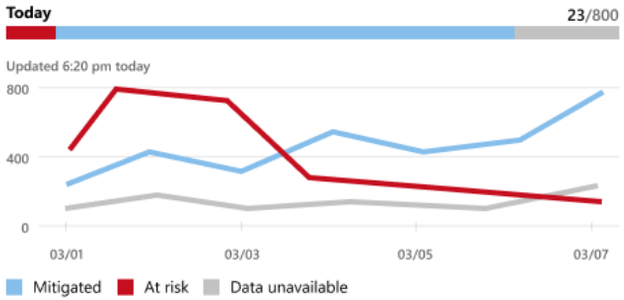
Start investigation | Share

RSS feeds > Threat analytics > **BadKitten**

213 active alerts in 20 machines



Machines mitigation status



Top impacted users

Updated 6:20 pm today

User	Risk	Alerts
JW Jonathan Wolcott	High	56
EM Eva Macias	High	45
RG Robin Goolsby	High	32

Show more

BadKitten

Published: 2018-03-06 11:00 (-7) | 2018-03-06 11:00 (-7)

Executive Summary
Beginning approximately 9:00 PST on March 6th, 2018, Next-gen protection reported blocking more than 80,000 instances of an unidentified, sophisticated trojan.

Analysis
Based on preliminary analysis, this malware exhibits cross-process injection techniques, persistence mechanisms, and evasion methods. The delivery vector(s), associated threats, and impact of the outbreak are as yet unknown.

Detection Details
Next-gen protection Protections Samples of the as-yet unidentified malware may trigger the following cloud detections:

Fuery (for example, Trojan:Win32/Fuery.A!cl)
Fuerboos (for example, Trojan:Win32/Fuerboos.A!cl)
Cloxer (for example, Trojan:Script/Cloxer or Trojan:Win32/Cloxer)
Azden (for example, Trojan:Win32/Azden.A!cl)
Next-gen protection , client-side antivirus definitions are not available.

Windows Defender Advanced Threat Protection Alerts with the following titles may appear in the Security Center console:
Known Malware Samples: Unidentified outbreak malware detected
Change log 2018-03-06 11:00 – First published

Remediation tasks

Task	Category	Unmitigated machine	Unavailable machine status
OS security updates	Malware	0	4,647
Disable VBA	Office	0	8
Address these vulnerabilities	OS updates	0	8

EMAIL AND DATA

Investigate activities that put your users and data at risk, and take action to protect your organization.
Get started by investigating suspicious emails that reached your users at Threat explorer

DEVICE AND IDENTITY

Proactively hunt for threat activity across your devices and identities using powerful, customizable queries.

- Database schema
- Community
  - GitHub shared queries
    - Find email links that resulted in ...
      - BadKitten
      - Uncommon access to LSASS
      - Downloaded documents
      - Browser query
      - Uncommon access to LSASS
      - Downloaded documents
      - File downloads from
      - Uncommon access to LSASS
  - Recommended queries
- Shared queries
- My queries
- Schedule queries

Help | Expand view

Advanced hunting > Find email links that resulted in BadKitten downloads on endpoints

Get started | Find email links that resulted in BadKitten... | Create new

Run query | Save | Schedule query | Last 30 days

```
// Check for browser sessions initiated from links opened by Outlook to specific known BadKitten infrastructure IP addresses
let infraIP =
NetworkCommunicationEvents
| where RemoteIP in
("139.59.208.246","130.255.73.90","31.3.135.232","52.174.55.168","185.121.177.177","185.121.177.53");
let emailLinks =
    MiscEvents
    // Filter on link clicks from Outlook (do case insensitive match using =~)
    | where ActionType == "BrowserLaunchedToOpenUrl" and isnotempty(RemoteUrl) and InitiatingProcessFileName =~ "outlook.exe"
    | project ComputerName, MailLink=RemoteUrl;
FileCreationEvents
| where isnotempty(FileOriginUrl) and InitiatingProcessFileName in~ ("chrome.exe", "browser_broker.exe")
| project FileName, FileOriginUrl, FileOriginReferrerUrl, ComputerName, EventTime, SHA1
| join kind=inner (emailLinks) on ComputerName, $left.FileOriginUrl == $right.MailLink
```

Export | Customize columns | Filters

Event time	UserID	User name	Email address	Sources email address	Mail subject	Mail count
Jul 23, 2018 06:54:34 AM	031f21af47b08f3f88ff20	RG Robin Goolsby	robing@contoso.com	Invoce_2232@gmail.com	Please review this invoice	1
Jul 03, 2018 08:43:31 AM	031f21af47b74v3f88ff2t	RF Rex Fredrickson	rexf@contoso.com	Invoce_2232@gmail.com	Your amazon order is now available	1
Jul 07, 2018 06:43:31 AM	e1ff19c8brg653073aff38	JP Jess Passmore	jessp@contoso.com	Invoce_2232@gmail.com	Please review ASAP	1

EMAIL AND DATA

Investigate activities that put your users and data at risk, and take action to protect your organization.
Get started by investigating suspicious emails that reached your users at Threat explorer

DEVICE AND IDENTITY

Proactively hunt for threat activity across your devices and identities using powerful, customizable queries.

- Database schema
- Community
  - GitHub shared queries
    - Find email links that resulted in ...
      - BadKitten
      - Uncommon access to LSASS
      - Downloaded documents
      - Browser query
      - Uncommon access to LSASS
      - Downloaded documents
      - File downloads from
      - Uncommon access to LSASS
  - Recommended queries
- Shared queries
- My queries
- Schedule queries

Help | Expand view

Advanced hunting > Find email links that resulted in BadKitten downloads on endpoints

Get started | Find email links that resulted in BadKitten... | Create new

Run query | Save | Schedule query | Last 30 days

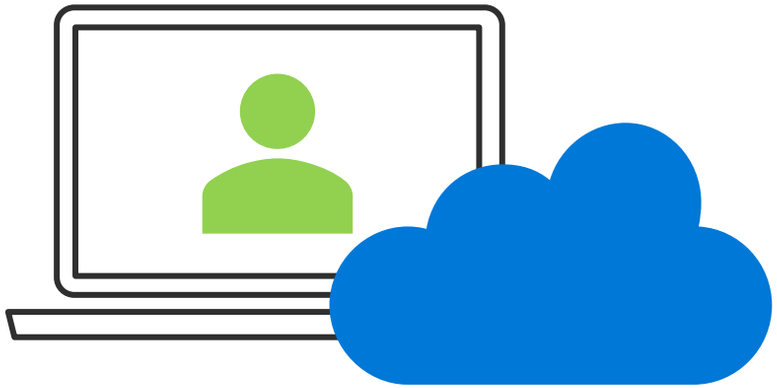
```
// Check for browser sessions initiated from links opened by Outlook to specific known BadKitten infrastructure IP addresses
let infraIP =
NetworkCommunicationEvents
| where RemoteIP in
("139.59.208.246","130.255.73.90","31.3.135.232","52.174.55.168","185.121.177.177","185.121.177.53");
let emailLinks =
    MiscEvents
    // Filter on link clicks from Outlook (do case insensitive match using =~)
    | where ActionType == "BrowserLaunchedToOpenUrl" and isnotempty(RemoteUrl) and InitiatingProcessFileName =~ "outlook.exe"
    | project ComputerName, MailLink=RemoteUrl;
FileCreationEvents
| where isnotempty(FileOriginUrl) and InitiatingProcessFileName in~ ("chrome.exe", "browser_broker.exe")
| project FileName, FileOriginUrl, FileOriginReferrerUrl, ComputerName, EventTime, SHA1
| join kind=inner (emailLinks) on ComputerName, $left.FileOriginUrl == $right.MailLink
```

Export | Customize columns | Filters

Event time	UserID	User name	Email address	Sources email address	Mail subject	Mail count
Jul 23, 2018 06:54:34 AM	031f21af47b08f3f88ff20	RG Robin Goolsby	robing@contoso.com	Invoce_2232@gmail.com	Please review this invoice	1
Jul 03, 2018 08:43:31 AM	031f21af47b74v3f88ff2t	RF Rex Fredrickson	rexf@contoso.com	Invoce_2232@gmail.com	Your amazon order is now available	1
Jul 07, 2018 06:43:31 AM	e1ff19c8brg653073aff38	JP Jess Passmore	jessp@contoso.com	Invoce_2232@gmail.com	Please review ASAP	1

Demo?!

Poháněno Microsoft 365

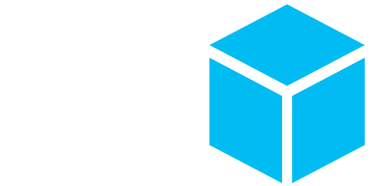


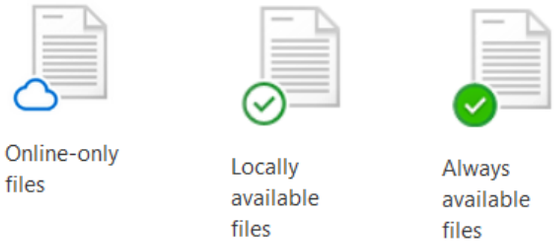
Unikátní kombinace produktivity, zabezpečení a klientského přístupu

Windows AutoPilot

Exchange Online

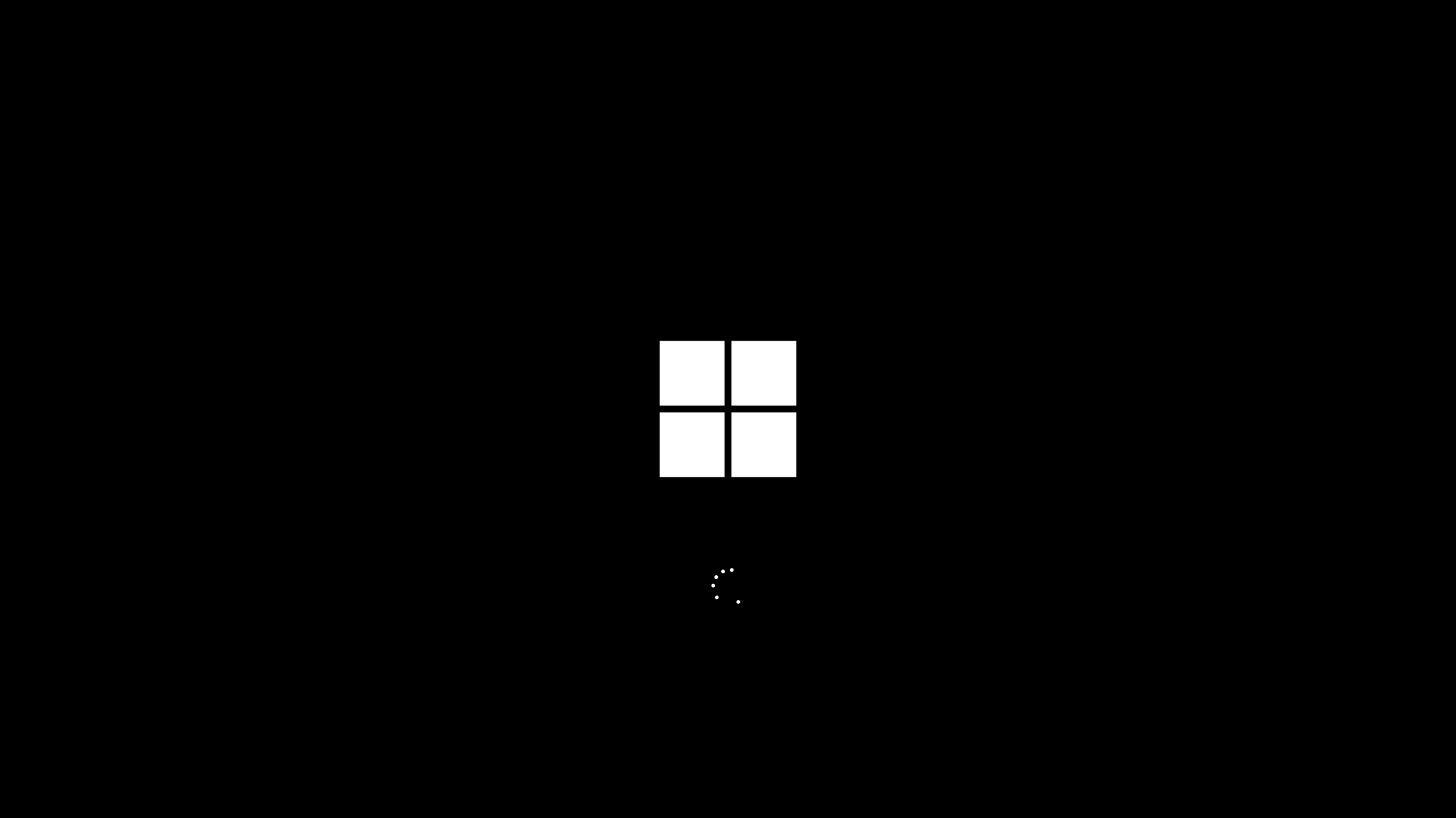
Office





Microsoft 365 powered device

Surface



Continue in English?

English

Français

Español

中文繁体

中文简体

Next

Let's start with region. Is this right?

United Arab Emirates

United Kingdom

United States

Uruguay

Uzbekistan

Vanuatu

Vatican City

Venezuela

Yes

Is this the right keyboard layout?

US

United States-Dvorak for left hand DVORAK L

United States-Dvorak for right hand DVORAK R

United States-International QWERTY

Albanian QWERTZ

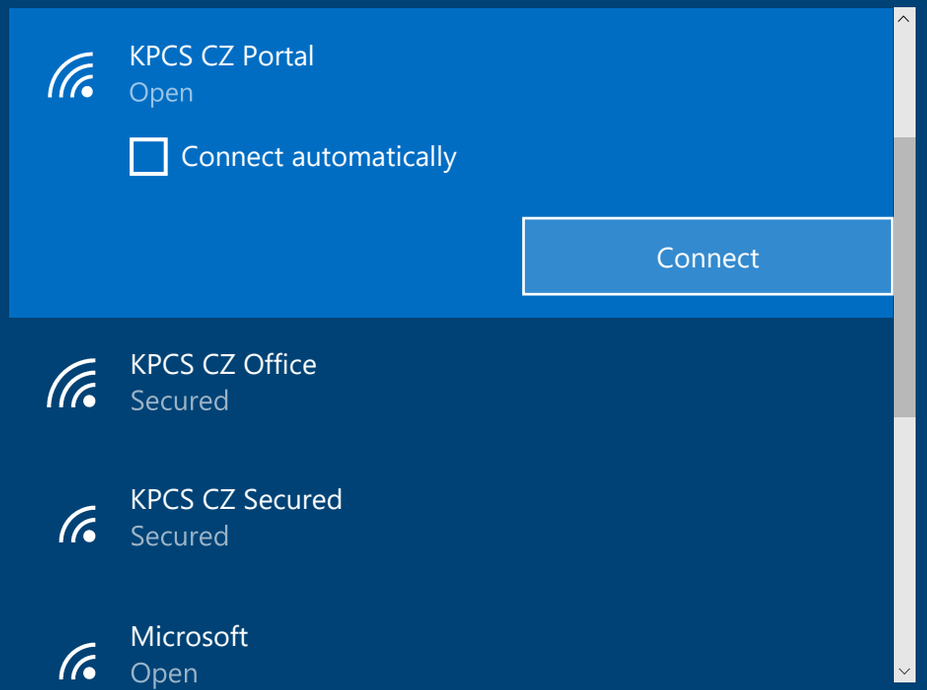
Azerbaijani PUSUDB

Azeri Latin QUERTY

Belgian (comma) AZERTY

Yes

Let’s connect you to a network



Skip for now

Now let's get you connected to a network. That way you get updates, apps and cat videos as soon as possible. How about the first one on the list? Want to use that one?

Network

Alright, you're connected. Just a moment...

Network

Now we'll check for any updates...

Account

Welcome, Petr!

Enter password for your KPCS CZ email account

vlk@kpcs.cz

Password

Start over with a different account

Forgot password?

Next

Listening...

Network

Please wait while we setup your device...

Network

Just a moment...

We’re getting everything ready for you.

Don’t turn off your PC

We’re getting everything ready for you.

Don’t turn off your PC

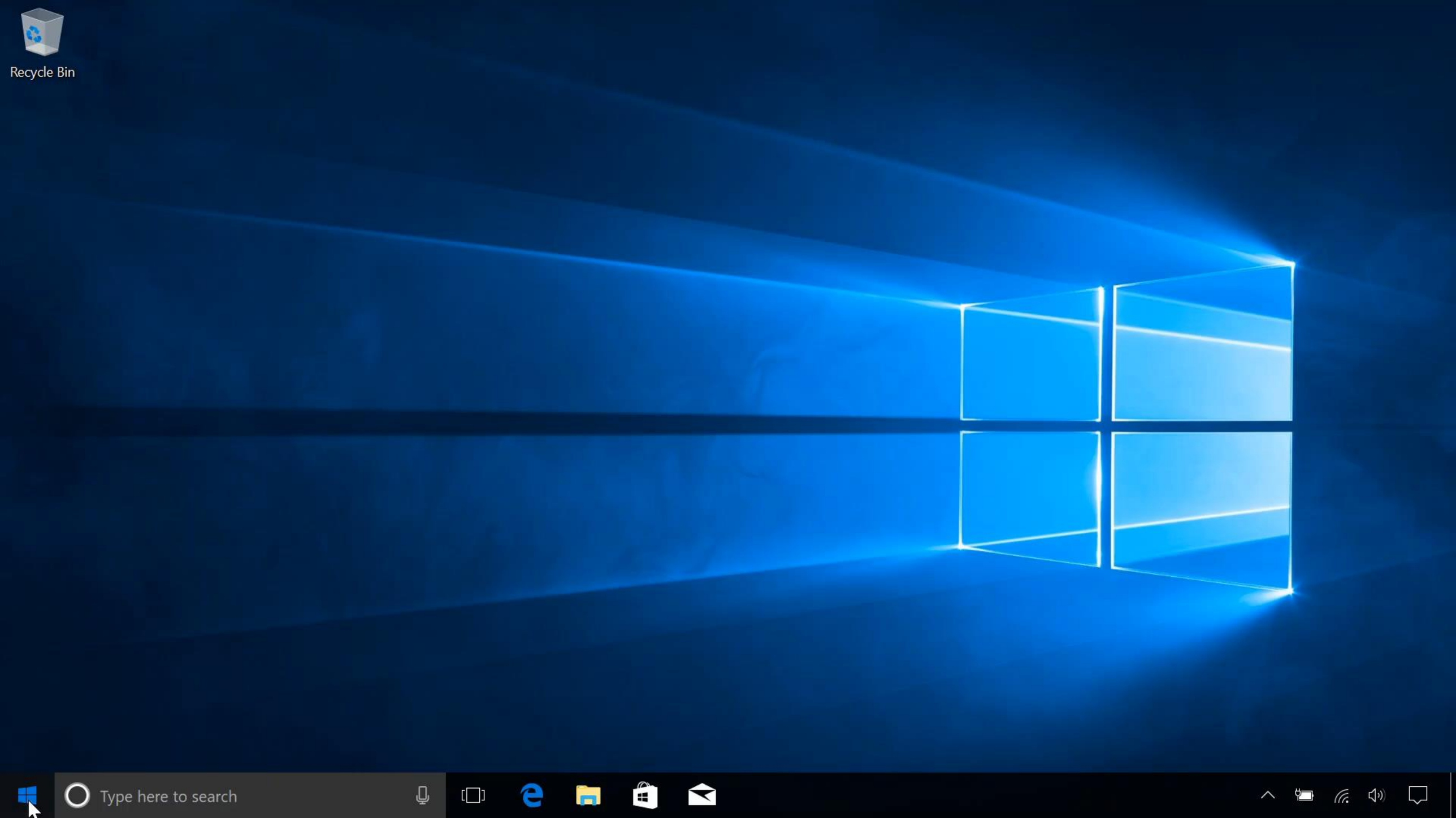
Setting up your device for work

Security setup complete

Network setup complete

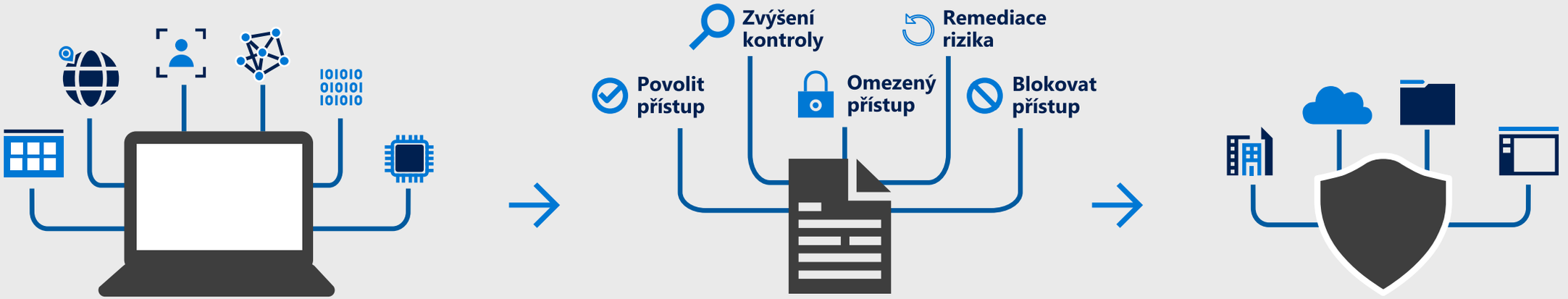
Application installation complete

Leave everything to us. (Don’t turn off this device.)


Recycle Bin
Type here to search

Zero Trust

Nikdy nevěřte. Vždy ověřte.



Signál

pro informované rozhodnutí

Rozhodnutí

na základě politiky

Vynucení

politik napříč systémy

Demo!

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies

Security Operations Center (SOC)

Microsoft Threat Experts | Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt | MSSP | Cloud App Security | Azure Security Center | Microsoft Defender | Office 365 | Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Information Protection

Cloud App Security

Azure Information Protection (AIP)

- Discover
- Classify
- Protect
- Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Classification Labels

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score | Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | **3rd party IaaS** | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

NGFW | Edge DLP | SSL Proxy | IPS/IDS

Azure Firewall | Security Appliances

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...

Shielded VMs | Azure Stack | VMs

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Windows 10 Enterprise Security

Network protection | Credential protection | Exploit protection | Reputation analysis | Full Disk Encryption | Attack surface reduction | App control | Isolation | Antivirus | Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT | Azure IoT Security | Azure Sphere | IoT Security Maturity Model | IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center | **Intelligent Security Graph**

Microsoft

Bezpečně 365

Petr Vlk
Enterprise Architect
KPCS CZ
vlk@kpcs.cz
www.kpcs.cz


KPCS