



Weekly Technical Office Hours for Partners

Remote Work in challenging times

Friday, April 24, 2020

The meeting will start at
WEST 12:00 - CET 13:00 – EEST 14:00

Technical Office Hours for WE Microsoft Partners: Remote Work in challenging times



Agenda

- 1. Introduction**
- 2. Secure Remote Work: threats, scenarios and best practices**
- 3. Q & A**
- 4. Poll – Proposed topics for next session**
- 5. How to get further help**
 - Support channels and options

Our Virtual Team



Toni Willberg
Cloud Solution Architect (Azure)



Matteo Malagnino
Cloud Solution Architect (Security)



Nuria Baeza Garcia
Partner Tech. Architect (Security)



Stefano Ceruti
Partner Tech. Architect (Teams)



Olivier van der Kruijf
Cloud Solution Architect (Azure)



Sara Canteiro
Partner Tech. Architect (Teams)



Aline Harmand
Partner Tech. Strategist



Juha Saarinen
Partner Tech. Architect (Teams)

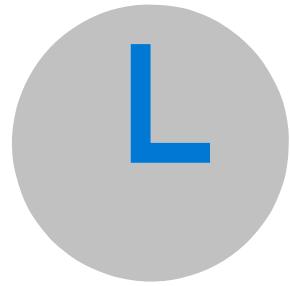


Jos Verlinde
Partner Tech. Architect (Teams)

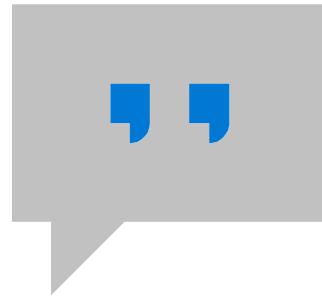


Philippe Goldstein
Partner Tech. Manager

WE Weekly Technical Office Hours – How it works



60 minutes
40 min, presentation
20 min, Q&A



Questions via
chat through

Q&A

The screenshot shows a 'Live event Q&A' window. At the top, there are three icons: a person, a gear, and an information sign. Below that is a header bar with 'Live event Q&A' and a help icon. The main area has tabs for 'Featured' and 'My questions', with 'My questions' currently selected and highlighted in blue. Below the tabs, there are three user profiles with their names and a 'Reply' button next to each. At the bottom right of the main area, there are two emoji buttons: one with sunglasses and another with a smiley face. Below the main area, there's a section titled 'Ask a moderator' with the sub-instruction: 'Questions won't be visible to everyone until a moderator approves them'. There are input fields for 'Your name (optional)' and 'Ask a question', and a checkbox for 'Post as anonymous'.

(WEEKLY) Technical Office Hours for WE Microsoft Partners:

Remote Work in challenging times

JOIN
UPCOMING
SESSION



Currently we are receiving a lot of questions from our partners and customers with regards to recommendations and help on working remotely.

To address the main technical topics around **working remotely**, Microsoft's Western Europe OCP Technical Team is setting up a series of Weekly Office Hours for Partners,

- every Wednesday at 12:00 – 13:00 CET (11:00 – 12:00 WEST)
- every Friday at 13:00 – 14:00 CET (12:00 – 13:00 WEST)

Wednesdays



Fridays



All sessions will be held in English.

<https://aka.ms/WE-TechOfficeHours>

Next
Session
Details

Upcoming
Sessions

Materials &
Recordings

Other
Resources

Feedback
Form

Don't miss a session;

Update your calendar by
using the invites above.

Influence the Agenda

Please fill the following survey to influence the agenda and help us delivering session relevant for you.



or <http://aka.ms/WE-TechOfficeHoursAgenda>

Secure Remote Work: threats, scenarios and best practices



Matteo Malagnino
Cloud Solution Architect (Security)

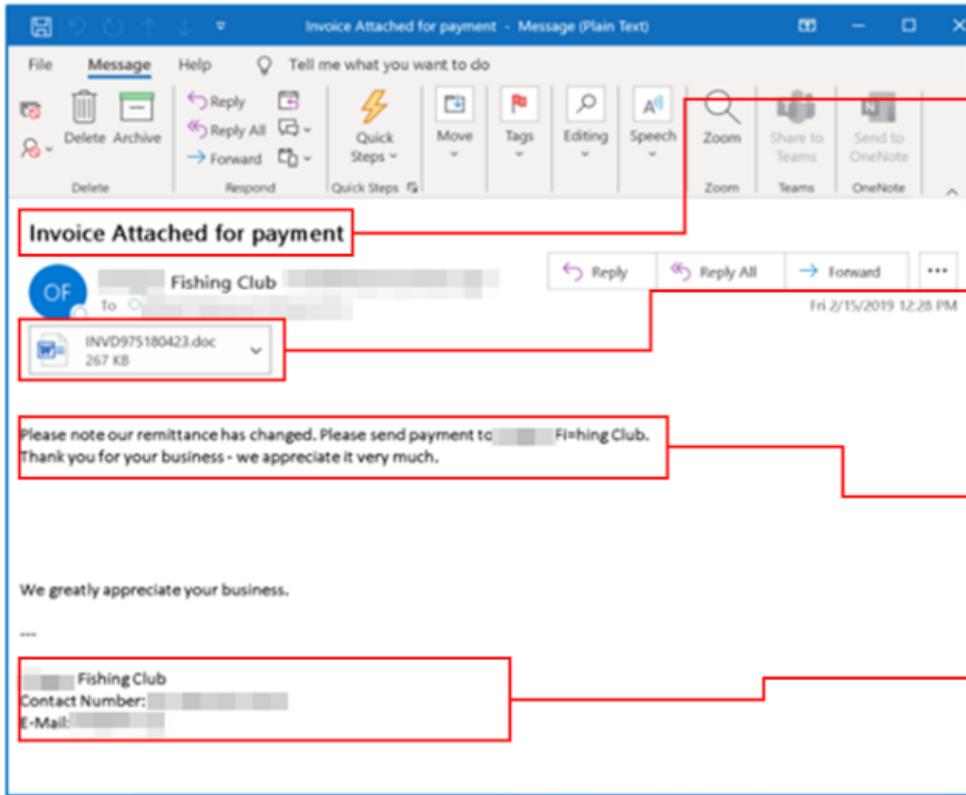
The COVID-19 threat landscape

Attackers are capitalizing on fear. We're watching them. We're pushing back.



The phishing campaign

Typical malware campaigns before crisis



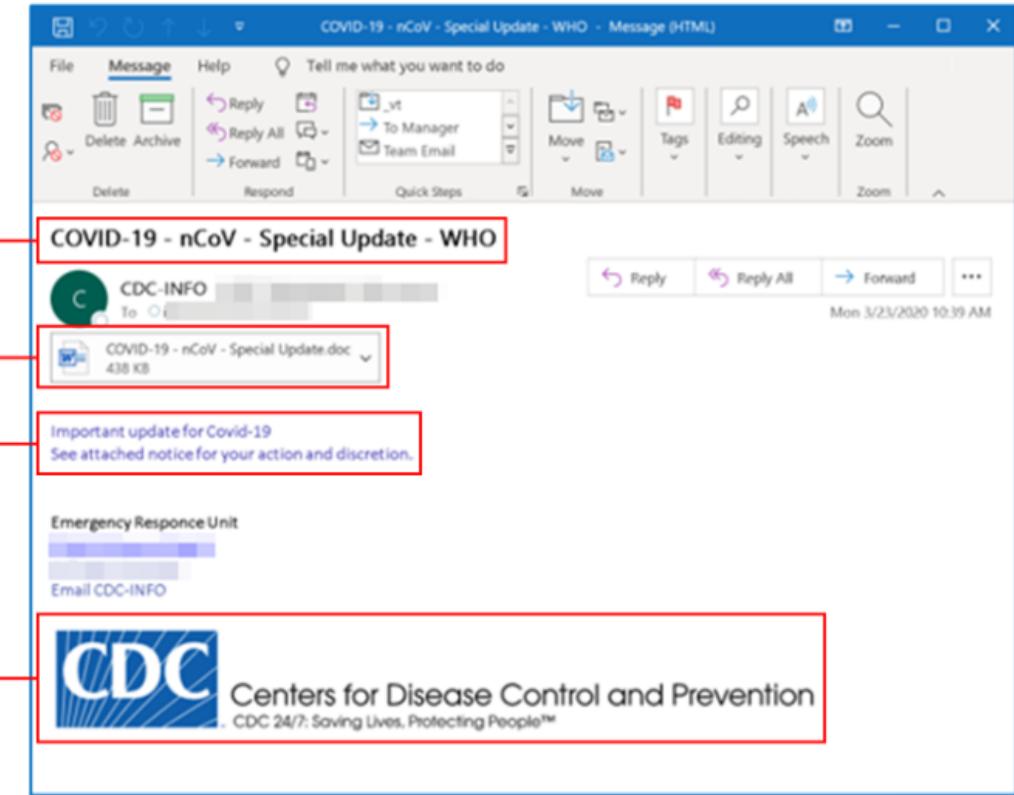
Subject lines updated with COVID-19 lure

Attached document has malicious macro that downloads Emotet or Trickbot

Messages take advantage of fear and need for info

Campaigns spoof orgs and agencies to fake legitimacy

COVID-19 themed campaigns



The trendy and pervasive Trickbot and Emotet malware families are very active and rebranding their lures to take advantage of the outbreak. We have observed 76 threat variants to date globally using COVID-19 themed lures (map below).

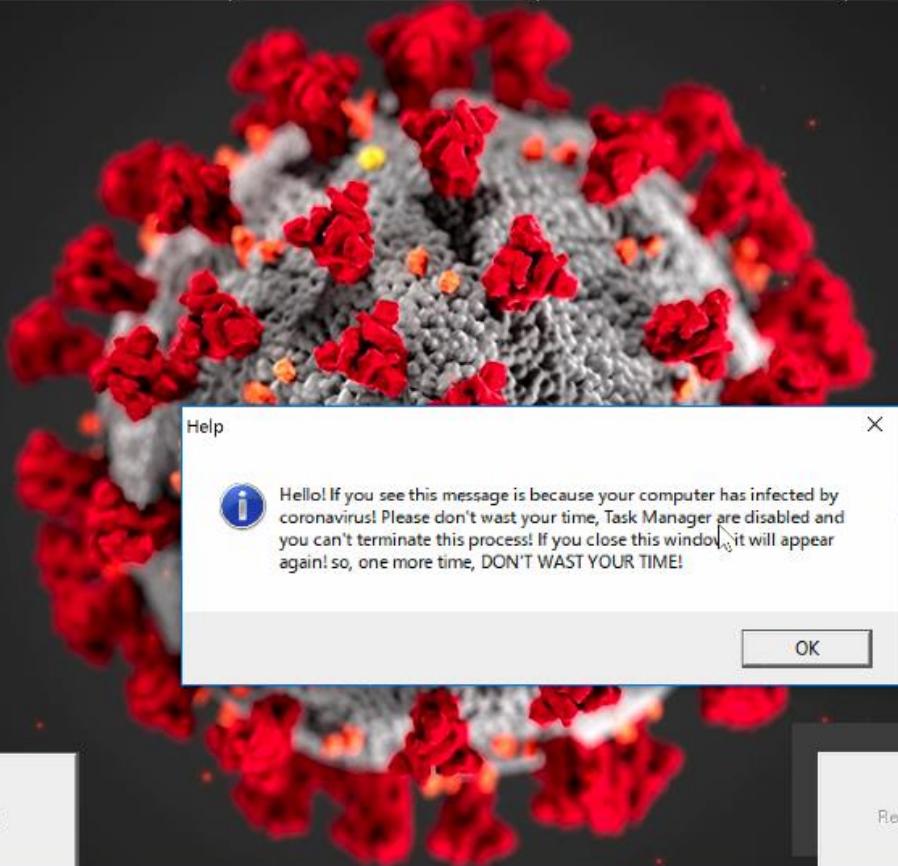
The phishing campaign



The trendy and pervasive Trickbot and Emotet malware families are very active and rebranding their lures to take advantage of the outbreak. We have observed 76 threat variants to date globally using COVID-19 themed lures.

The infection

coronavirus has infected your PC!



cursor.cur	2020/04/23 9:29
end.exe	2020/04/23 9:29
mainWindow.exe	2020/04/23 9:29
run.exe	2020/04/23 9:29
Update.vbs	2020/04/23 9:29
wallpaper.jpg	2020/04/23 9:29

Created By Angel Castillo. Your Computer Has Been Trashed.
Discord: Windows Vista#3294

The infection

coronavirus has infected your PC!

```
wscript.sleep 120000
```

```
x=msgbox ("The update server could not be resolved. Check your Internet settings or contact your system administrator.",16,"COVID-19")
```

cursor.cur
end.exe

2020/04/23 9:29
2020/04/23 9:29

Help
 Hello! If you can again! si

COVID 19

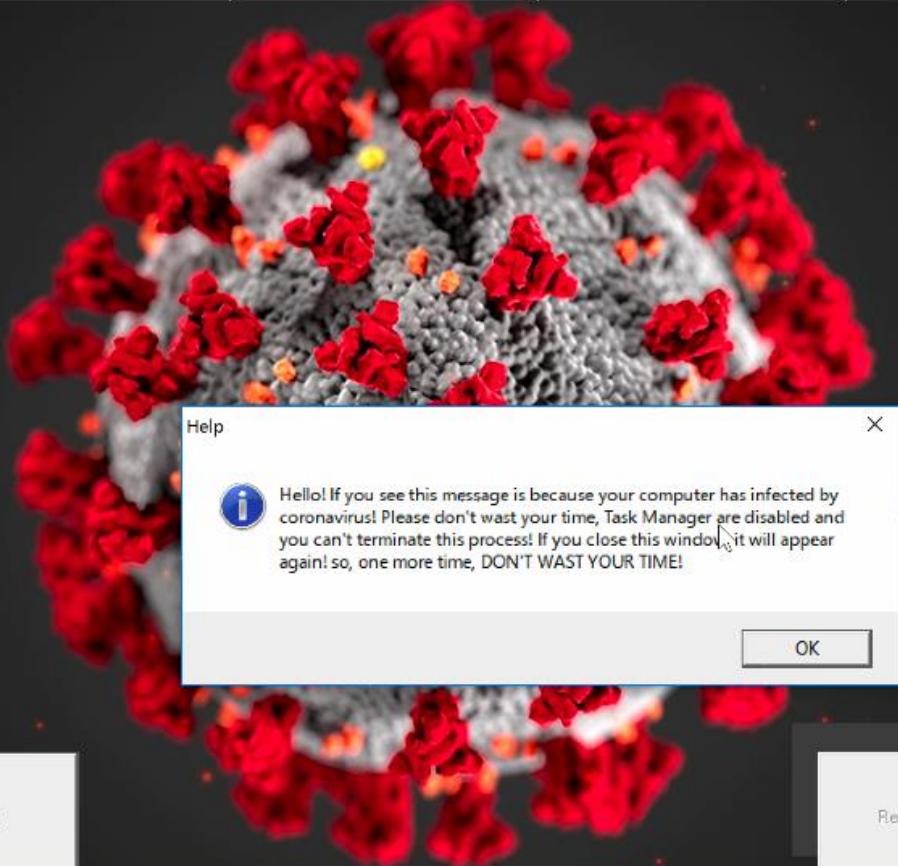
 The update server could not be resolved. Check your Internet settings or contact your system administrator.

OK

Help

The infection

coronavirus has infected your PC!



cursor.cur	2020/04/23 9:29
end.exe	2020/04/23 9:29
mainWindow.exe	2020/04/23 9:29
run.exe	2020/04/23 9:29
Update.vbs	2020/04/23 9:29
wallpaper.jpg	2020/04/23 9:29

Created By Angel Castillo. Your Computer Has Been Trashed.
Discord: Windows Vista#3294

The campaign

While phishing email is a common attack vector, it's only one of the many points of entry for attackers. Defenders need a much broader view and solutions for remediation than visibility into just one entry method. An attacker's primary goal is to gain entry and expand across domains so they can persist in an organization and lie in wait to steal or encrypt as much sensitive information as they can to reap the biggest payout. Defenders require visibility across each of these domains and automated correlation across emails, identities, endpoints, and cloud applications to see the full scope of compromise. Only with this view can defenders adequately remediate affected assets, apply Conditional Access, and prevent the same or similar attacks from being successful again.

<https://www.microsoft.com/security/blog/2020/04/08/microsoft-shares-new-threat-intelligence-security-guidance-during-global-crisis/>

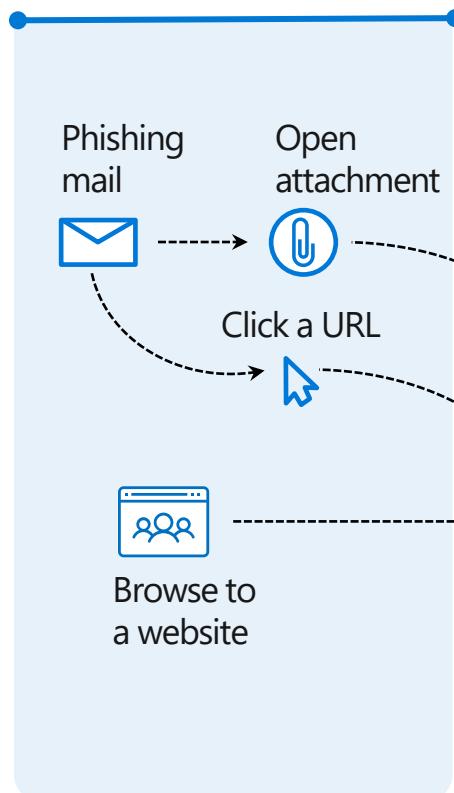
Tips & Trick, best practices on how to protect



Protection across the attack kill chain

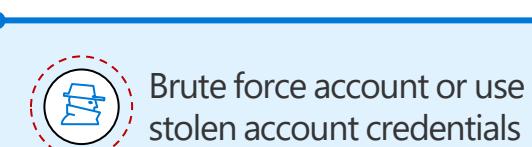
Office 365 ATP

Malware detection, safe links, and safe attachments



Azure AD Identity Protection

Identity protection & conditional access

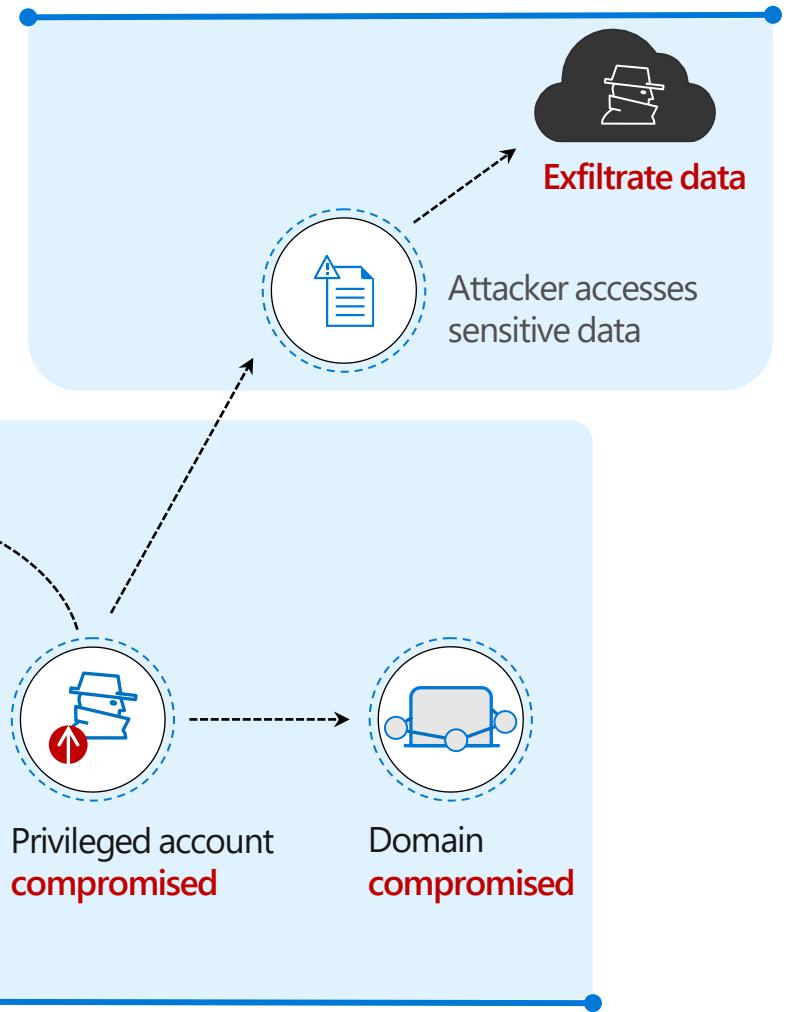


Windows Defender ATP

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

Microsoft Cloud App Security

Extends protection & conditional access to other cloud apps



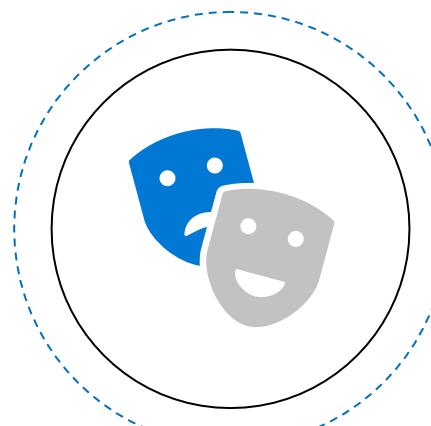
Azure ATP

Identity protection

O365 ATP

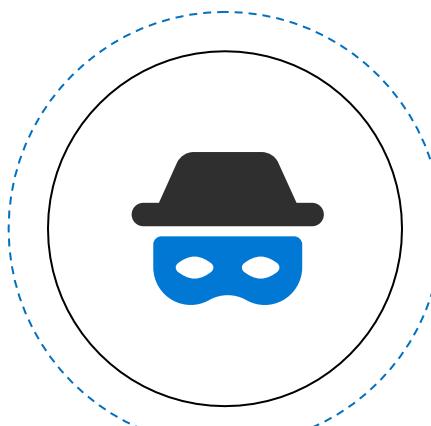
[**Office 365 ATP**](#), Microsoft's cloud-based email filtering service, which shields against phishing and malware, including features to safeguard your organization from messaging-policy violations, targeted attacks, zero-days, and [malicious URLs](#). Intelligent recommendations from [Security Policy Advisor](#) can help reduce macro attack surface, and the [Office Cloud Policy Service](#) can help you implement security baselines.

O365 ATP



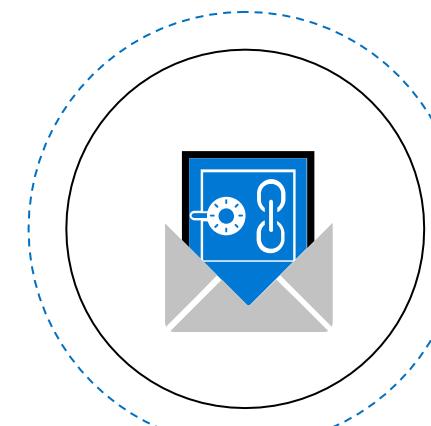
Spoofing

DMARC, DKIM, and SPF
Intra-org spoof detection
Cross-domain detection



Impersonation

User impersonation
Domain impersonation
Brand impersonation
Mailbox Intelligence



Content analysis & detonation

Malicious attachments
Malicious URLs
Detect text lures
Internal Safe Links

Malicious URLs detection

- We check every URL against reputation data built from numerous 3rd party feeds as well as other internal Microsoft sources, in addition to every previous detonation in O365
- We use Advanced Machine learning during mail flow to identify messages with suspicious or malicious links
- Links that require deeper inspection are proactively sent to the sandbox for detonation
- In addition links are detonated per recipient safe-links policy
- We also detonate URLs at Time of Click to catch URL weaponization after delivery
- We also support Safe-Links within Office clients
- We remove messages with newly discovered malicious URLs using ZAP (Zero-hour Auto Purge)



URL
Reputation
Blocking



ML
Models



URL Detonation



Linked Content
Detonation



Safe Links



Safe Links for
Office Clients



Zero-hour
Auto-Purge

ATP Safe Links – Capabilities shown within policies

Safe links policy for your organization

Settings that apply to content across Office 365
When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.

Block the following URLs:

- Enter a valid URL
- http://www.quicksticks.org*
- messaging.sharepointapcprd662.prdexchangepenz.net*
- https://alislarnifoods.com*
- *cxn1.com
- cxn1.com*
- https://xeroaccountingaustralia.com*

Settings that apply to content except email
These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

- Office 365 ProPlus, Office for iOS and Android

For the locations selected above:

- Do not track when users click safe links
- Do not let users click through safe links to original URL

Safe Links will be used in:
Office 365 ProPlus (Word, Excel, PowerPoint, and Visio on Windows; and Word, Excel, and PowerPoint on Mac)
Office Online (Word Online, Excel Online, PowerPoint Online, and OneNote Online)
Word, Excel, and PowerPoint for iOS and Android

Apps not currently supported: OneNote (desktop version)
Non Office 365 ProPlus products (such as Office 2016, Office 365 Home, Office 365 Personal, and the consumer version of Office Online)
Office apps for iOS and Android not listed above

When a user clicks a URL in one of the supported apps, Office 365 will first check to see if it's malicious. If it is, the user is directed to a warning page for further action.

Save Cancel

ATP Safe Links – Organizational policy

Safe links policy - [InPrivate] - Microsoft Edge

https://protection.office.com/ecp/SafeLinks/EditSafeLinksPolicy.aspx?ActivityCorrelationID=de5086c9-eefc-43d0-8f3e-0a2a2a2a2a2a

Safe Links Policy - All Employees

general
▶ **settings**
applied to

Select the action for unknown potentially malicious URLs in messages.

Off

On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.

Apply real-time URL scanning for suspicious links and links that point to files.
 Wait for URL scanning to complete before delivering the message.

Apply safe links to messages sent within the organization.

Do not track when users click safe links.

Do not let users click through safe links to original URL.

Do not rewrite the following URLs:

- Enter a valid URL
- http://*.sharepoint.com
- *microsoft.com*

Save Cancel

ATP Safe Links – Recipient-based policy

Safe Links can apply **URL detonation for all URLs** within emails. In addition, by using machine learning models to determine suspicious messages, it is **also capable of identifying suspicious URLs and detonate them preemptively**.

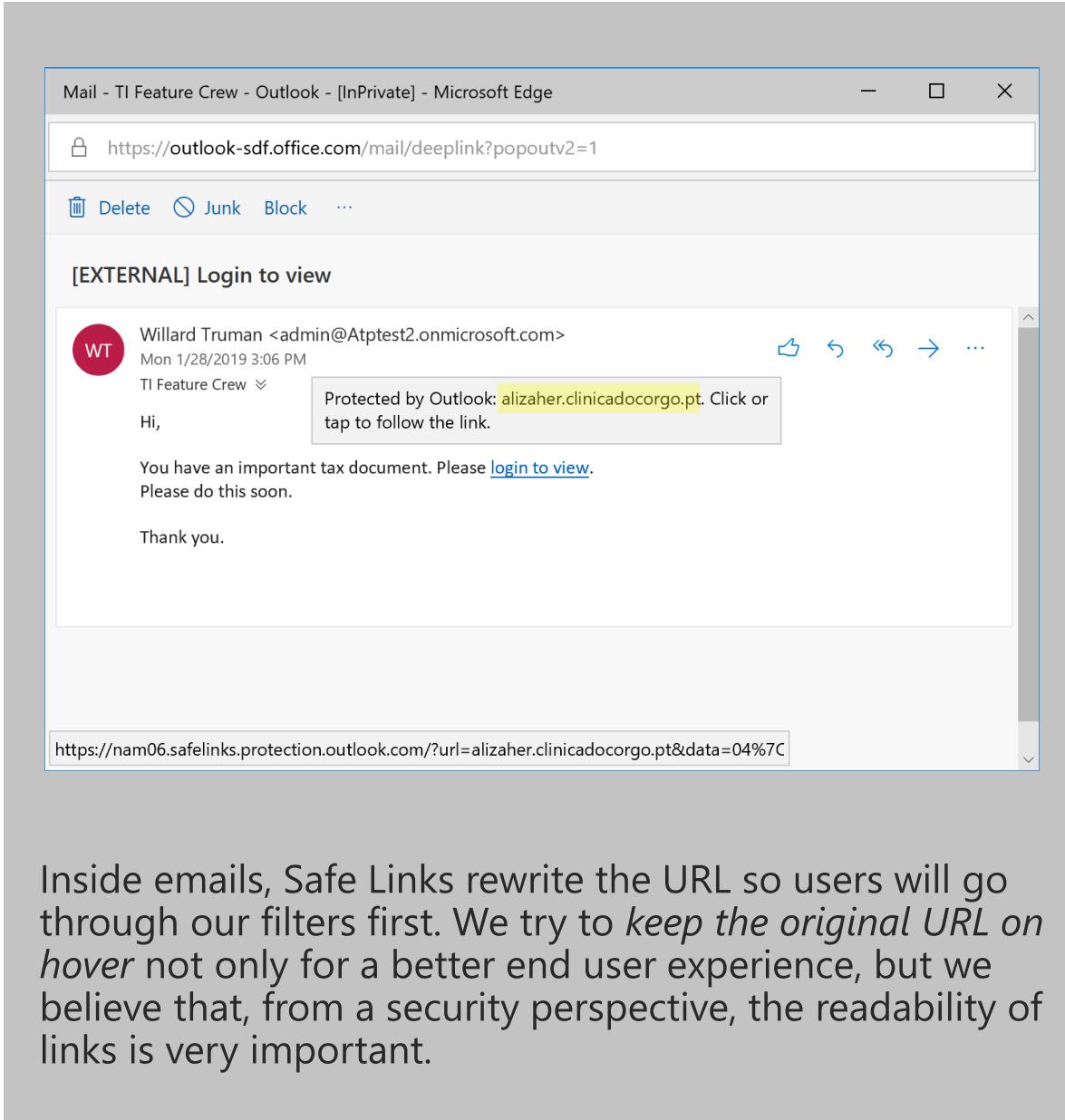
Also, there's the capability of holding off mail delivery until all links have been scanned and found to be safe. *(Coming soon!)*

Admins have the option to enable Safe Links to protect URLs from intra-org emails.

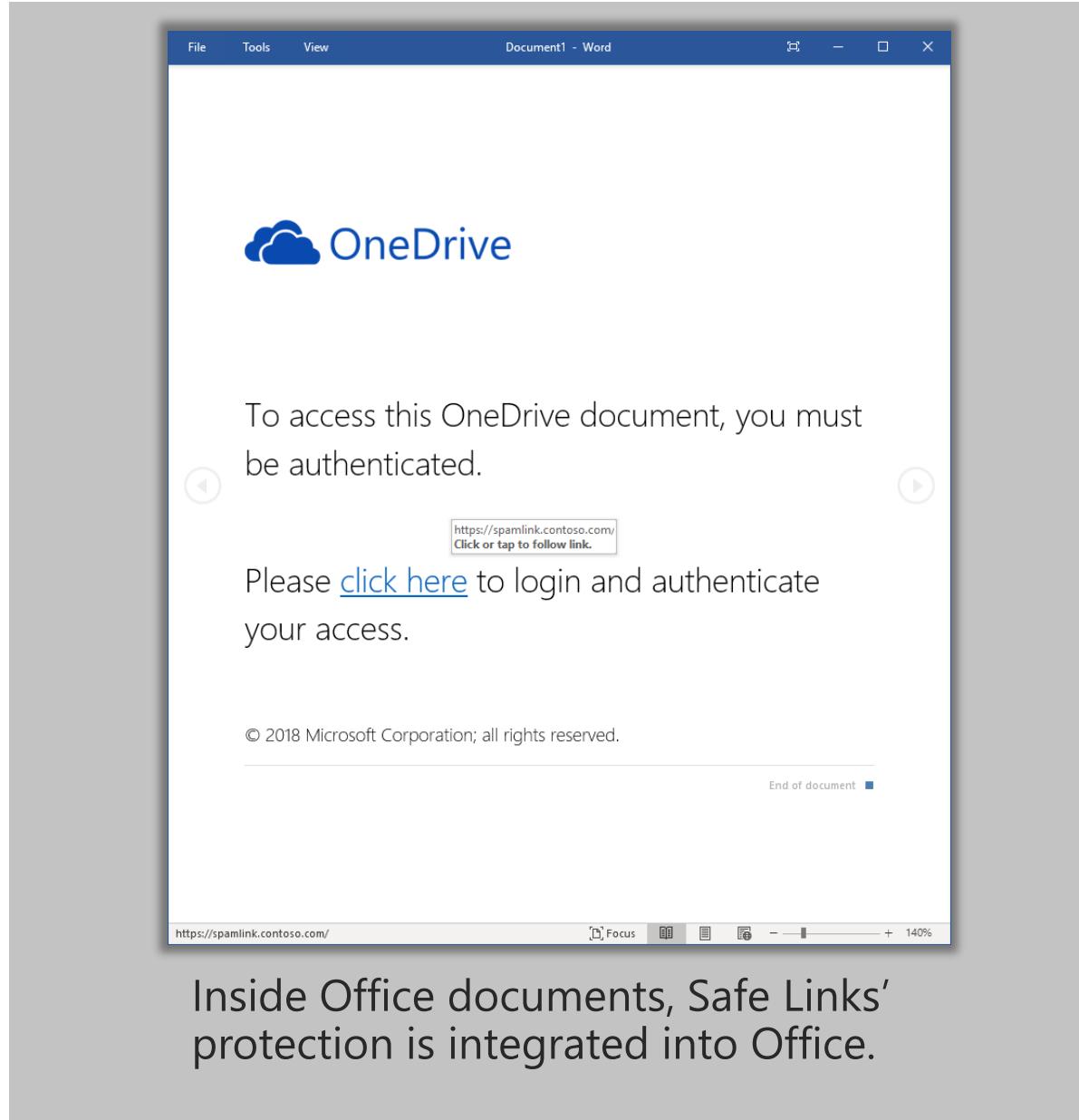
Admins have the ability to **block malicious URLs in real time**.

Safe Links can protect users from linked threats within Office.

ATP Safe Links Protection in Emails & Office, with Native Link Rendering



Inside emails, Safe Links rewrite the URL so users will go through our filters first. We try to *keep the original URL on hover* not only for a better end user experience, but we believe that, from a security perspective, the readability of links is very important.



A malicious threat is blocked

The screenshot shows a Microsoft ATP Safe Links warning dialog box. At the top, there's a Microsoft logo with a purple oval around it. Below the logo, a red shield icon with a white 'X' is displayed next to the text "This website has been classified as malicious." A purple arrow points from this text to the label "Customized branding" on the right. The main body of the dialog is red and contains the message "Opening this website might not be safe." followed by the URL "http://alizaher.clinicadocorgo.pt". Below this, a message reads: "We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data." At the bottom left is a blue button labeled "X Close this page". To its right is a link "Continue anyway (not recommended)". At the very bottom, it says "Powered by Office 365 Advanced Threat Protection".

Customized
branding

Malicious URL is
blocked by ATP
Safe Links, with
custom
organizational
branding at the top.

URL

High-severity alert: A potentially unsafe URL click was detected.

Office365Alerts@microsoft.com
Mon 1/28/2019 3:11 PM
anach@o365TISDFV2.onmicrosoft.com; Mimi Fang; John E; Ross Admin; Brad Chen +12 others

 Office 365

A high-severity alert has been triggered

⚠ A potentially unsafe URL click was detected.

Severity: ● High
Time: 1/28/2019 11:07:50 PM (UTC)
Activity: Unsafe URL click
Details: We have detected that tifc@o365tisdfv2.onmicrosoft.com has recently clicked on a link that was found to be unsafe.

[View alert details](#)

Thank you,
The Office 365 Team

 Microsoft
One Microsoft Way
Redmond, WA
98052-6399 USA
[Privacy](#) | [Legal](#)

A potentially unsafe URL click was detected

[Resolve](#) [Suppress](#) [Notify users](#)

Severity	● High
Time	Jan 28, 2019 3:11:36 PM
Threat type	Potentially unsafe URL click was detected
Hit count	1 View message list
Details	We have detected that one of your users has recently clicked on a link that was found to be unsafe -V1.0.0.1 By the time this alert was triggered, tifc@o365tisdfv2.onmicrosoft.com was allowed to access http://alizaher.clinicadocorgo.pt/
Status	Active
Comments	New alert Edit
Alert policy	A potentially unsafe URL click was detected
Notification sent to	TenantAdmins View policy

[View messages in Explorer](#) [Close](#)

Alert email

Alert details

Defender ATP

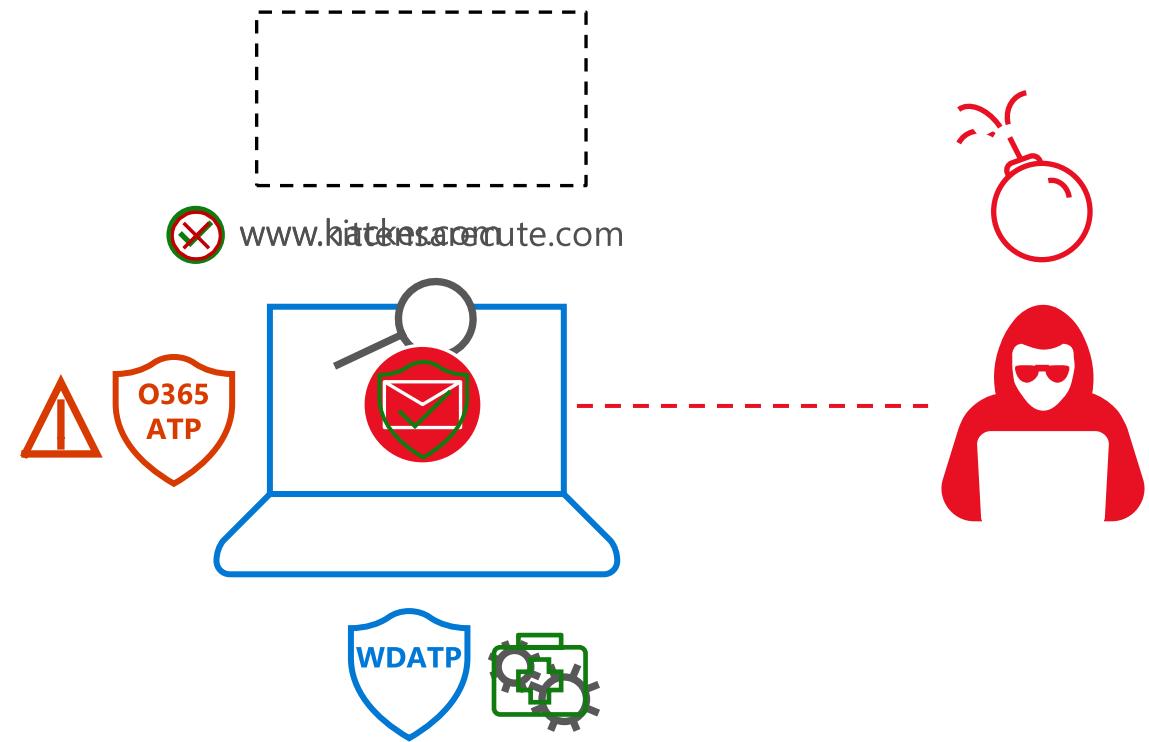
Protect endpoints with Microsoft Defender ATP, which covers licensed users for up to five concurrent devices that can be easily onboarded at any time. Microsoft Defender ATP monitors threats from across platforms, including macOS. Our [tech community post](#) includes additional guidance, best practices, onboarding, and licensing information

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





Microsoft Defender Advanced Threat Protection

Built-in. Cloud-powered.



THREAT & VULNERABILITY
MANAGEMENT



ATTACK SURFACE
REDUCTION



NEXT GENERATION
PROTECTION



ENDPOINT DETECTION
& RESPONSE



AUTO INVESTIGATION
& REMEDIATION



MICROSOFT
THREAT EXPERTS

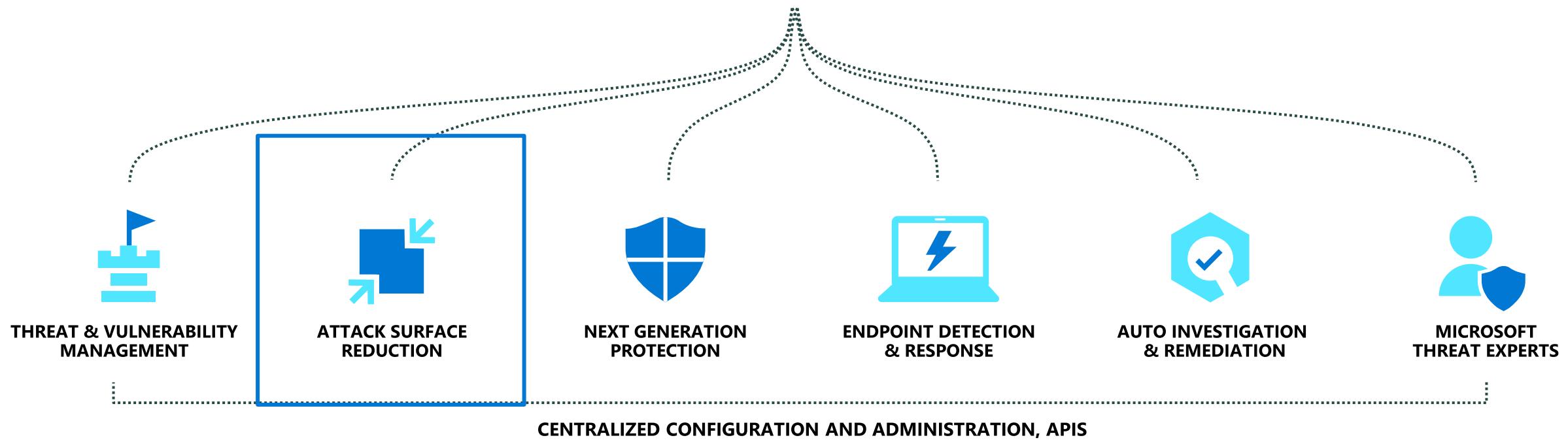


CENTRALIZED CONFIGURATION AND ADMINISTRATION, APIs



Microsoft Defender Advanced Threat Protection

Built-in. Cloud-powered.





The need for Attack Surface Reduction



⚠️ Vulnerabilities in software (i.e.: code defects) aren't going to stop shipping as to error is human

⚠️ Out of the box platforms include rarely used surface areas of functionality that represents exploitable opportunities to attackers

⚠️ A platform configured to trust any application and depends on detection for security is dramatically less secure than one configured to run only trusted apps

⚠️ A device constrained to accessing only reputable network locations is an increasingly hard target

Attack Surface Reduction

Resist attacks and exploitations



HW BASED ISOLATION

Isolate access to untrusted sites

APPLICATION CONTROL

Isolate access to untrusted Office files

EXPLOIT PROTECTION

Host intrusion prevention

NETWORK PROTECTION

Exploit mitigation

CONTROLLED FOLDER ACCESS

Ransomware protection for your files

Block traffic to low reputation destinations

Protect your legacy applications

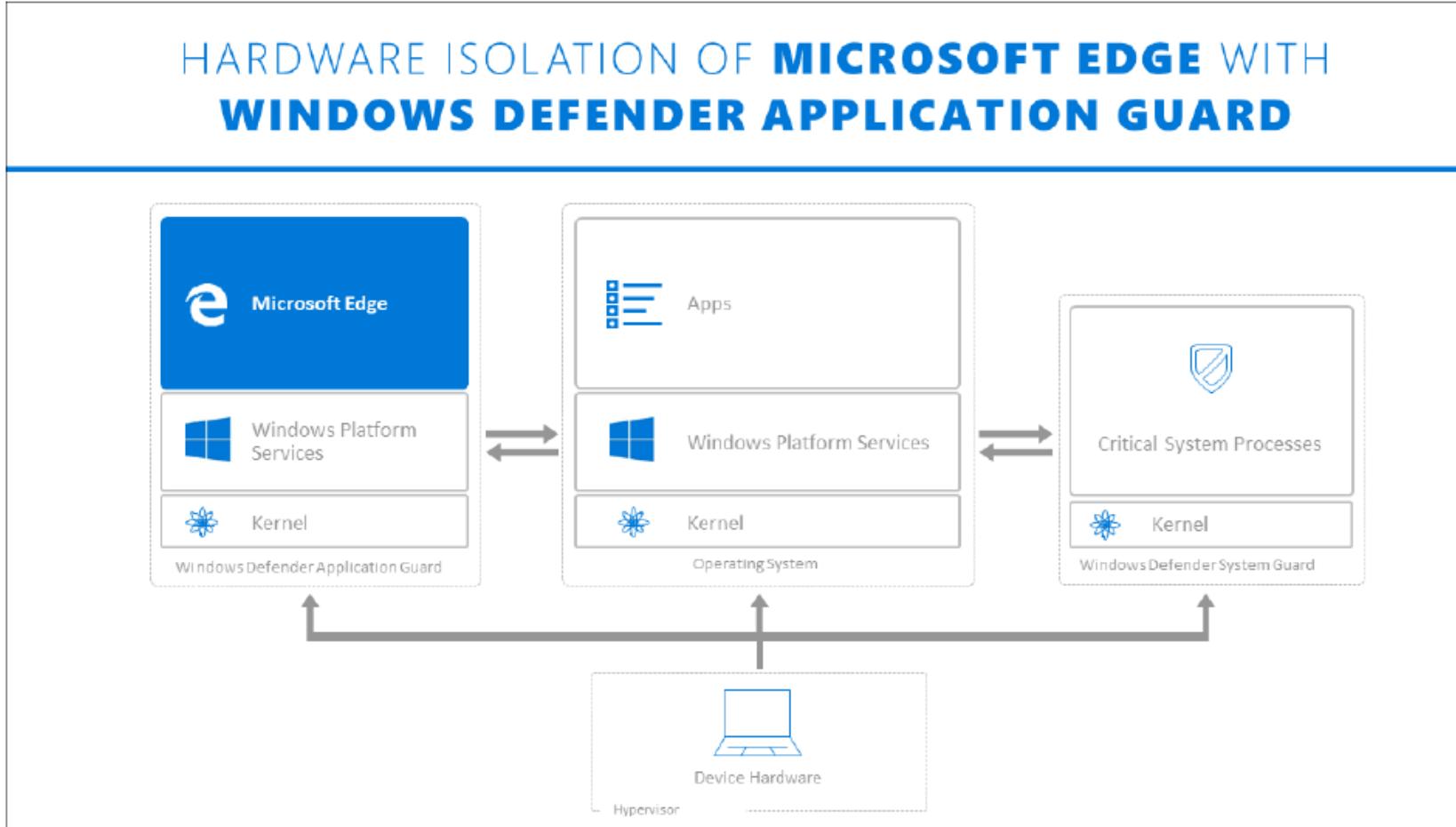
Only allow trusted applications to run

Attack Surface Reduction

ARTICLE	DESCRIPTION
Hardware-based isolation	Protect and maintain the integrity of a system as it starts and while it's running. Validate system integrity through local and remote attestation. And, use container isolation for Microsoft Edge to help guard against malicious websites.
Application control	Use application control so that your applications must earn trust in order to run.
Exploit protection	Help protect operating systems and apps your organization uses from being exploited. Exploit protection also works with third-party antivirus solutions.
Network protection	Extend protection to your network traffic and connectivity on your organization's devices. (Requires Windows Defender Antivirus)
Controlled folder access	Help prevent malicious or suspicious apps (including file-encrypting ransomware malware) from making changes to files in your key system folders (Requires Windows Defender Antivirus)
Attack surface reduction	Reduce vulnerabilities (attack surfaces) in your applications with intelligent rules that help stop malware. (Requires Windows Defender Antivirus)
Network firewall	Prevent unauthorized traffic from flowing to or from your organization's devices with two-way network traffic filtering.

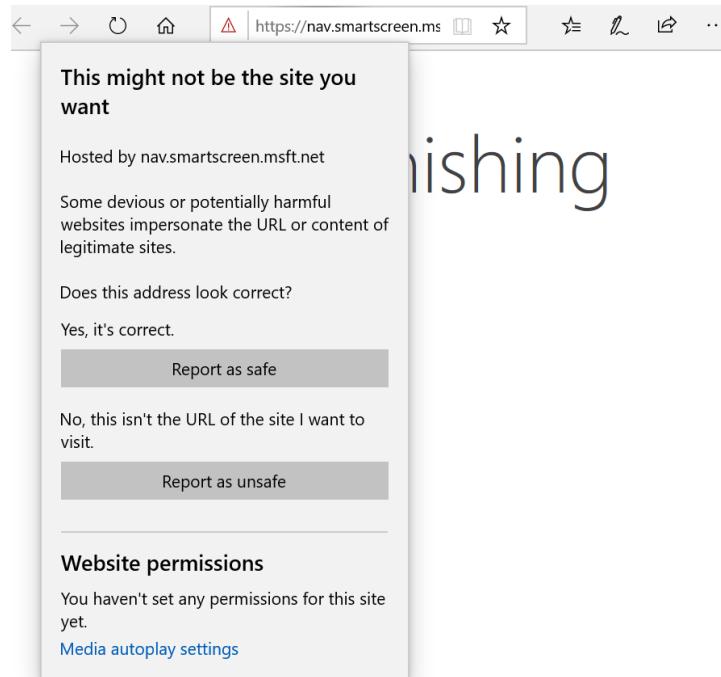
Attack Surface Reduction – Hardware based isolation

Windows Defender Application Guard



Web Threat Protection

- Phishing
- URL Threats & Exploits
- PUA
- Tech Scams



This screenshot shows a browser window with a red SmartScreen warning overlay. The address bar shows https://nav.smartscreen.ms. The warning message reads: "This website has been reported as unsafe. Hosted by nav.smartscreen.msft.net. We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information." A red button labeled "Back to safety" is visible. Below the warning, there is a section titled "More information" with the message "This website has been reported to contain the following threats:" followed by a list of threats and two links: "Report that this site does not contain threats" and "Disregard and continue (not recommended)". The footer of the page says "Windows Defender SmartScreen".



Can't connect securely to this page

This might be because the site uses outdated or unsafe TLS security settings. If this keeps happening, try contacting the website's owner.

Try this

- Go back to the last page



Virus & threat protection

Connection blocked

Your IT administrator caused Windows Security to block this network connection. Contact your IT help desk.

Can't connect securely to this page

This might be because the site uses outdated or unsafe TLS security settings. If this keeps happening, try contacting the website's owner.

Try this:

- Go back to the last page

Windows Security

This content is blocked

For your protection, your administrator is not allowing you to access content from Gmail.

OK Unblock

Identity protection

Enable multi-factor authentication (MFA) and Conditional Access through Azure Active Directory to protect identities. This is more important than ever to mitigate credential compromise as users work from home. We recommend connecting all apps to Azure AD for single sign-on – from SaaS to on-premises apps; enabling MFA and applying Conditional Access policies; and extending secure access to contractors and partners. Microsoft also offers a [free Azure AD service](#) for single sign-on, including MFA using the Microsoft Authenticator app

MCAS

Microsoft Cloud App Security can [help protect against](#) shadow IT and unsanctioned app usage, identify and remediate cloud-native attacks, and control how data travels across cloud apps from Microsoft or third-party applications.

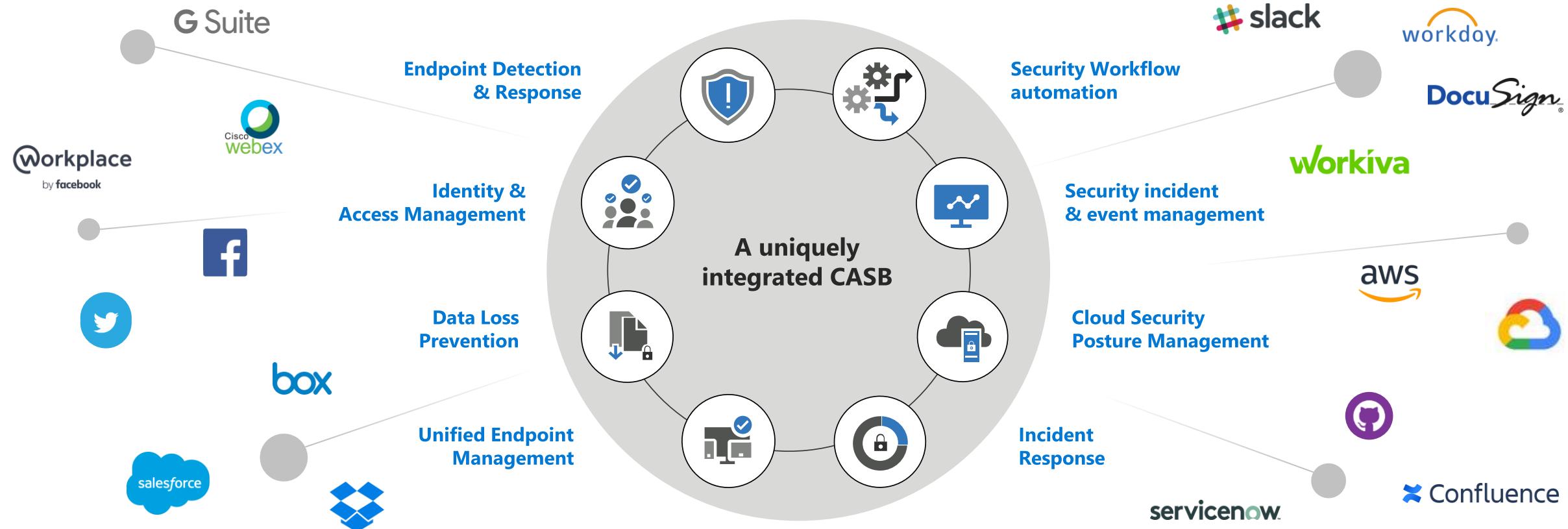
Microsoft Cloud App Security

The go-to CASB for Office 365 and Azure that loves 3rd party

Simple deployment

Natively integrated across the broader Microsoft product stack to deliver unique capabilities

Rooted in supporting any app



Microsoft Cloud App Security architecture

Discovery

Use traffic log data to discover the cloud apps in your organization and get detailed insights about traffic- and user data

Managing discovered cloud apps

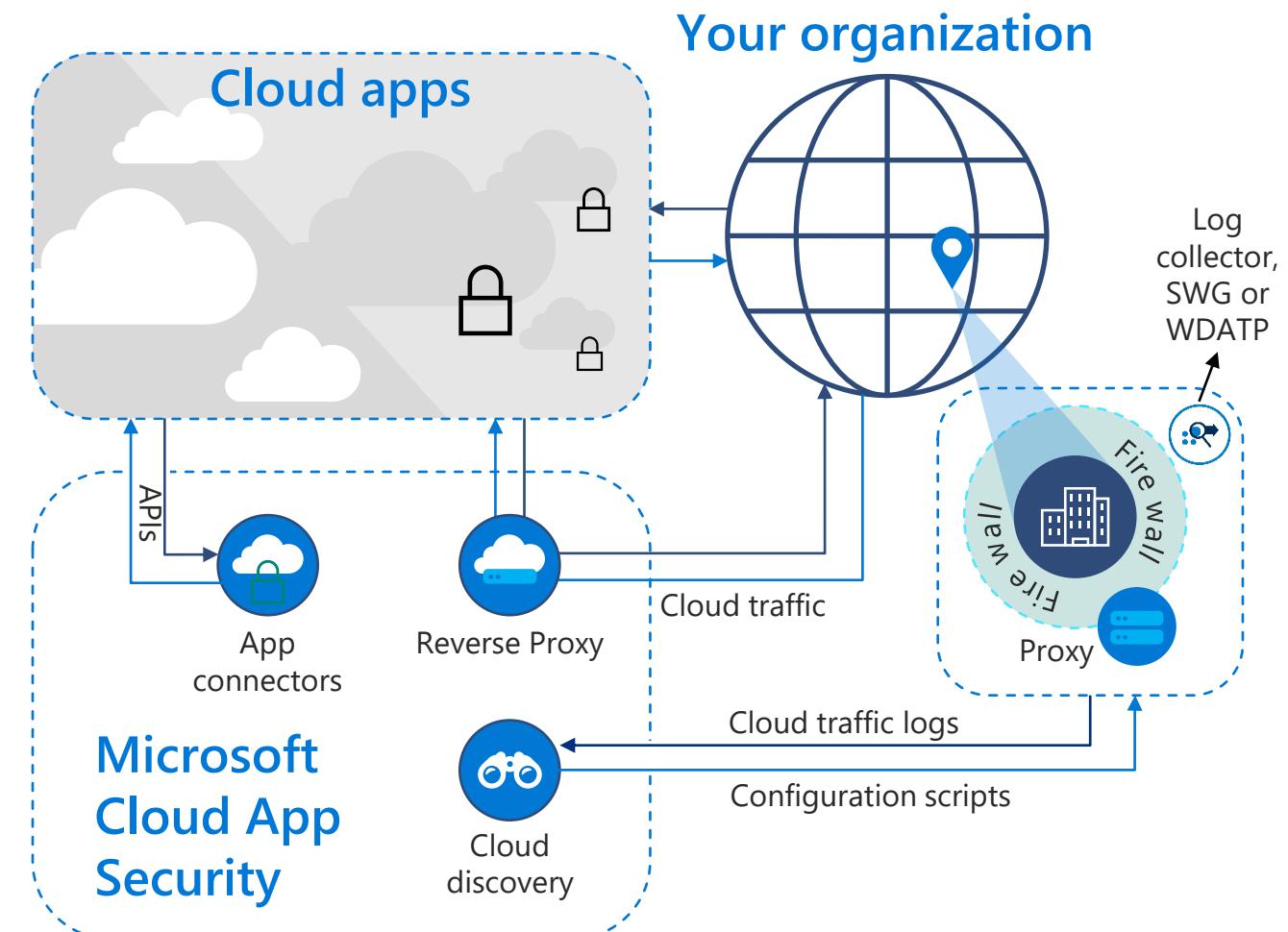
Evaluate the risk of discovered cloud apps and take action by sanctioning, tagging or blocking them

App connectors

Be alerted on user or file behavior anomalies and control the data stored in your cloud apps leveraging our API connectors

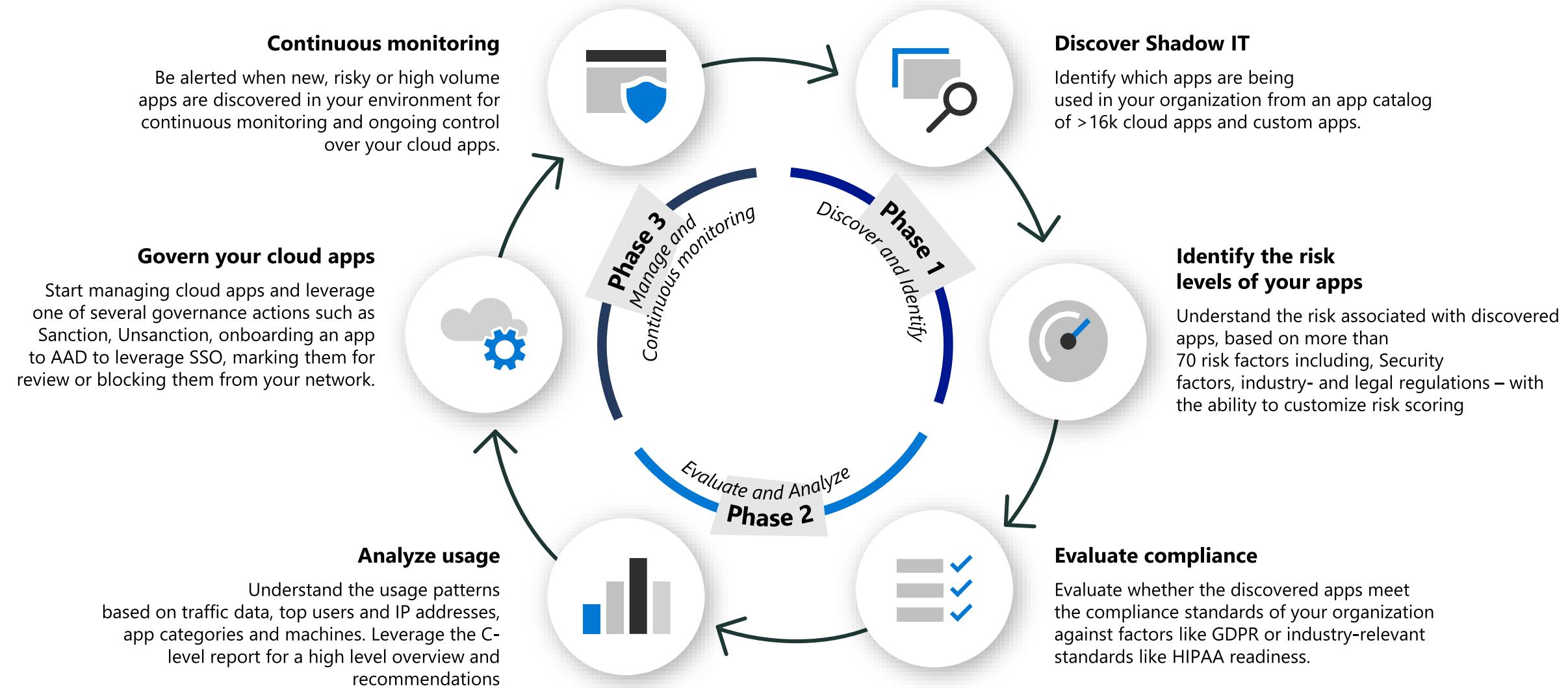
Conditional Access App Control

Leverage our reverse proxy infrastructure and integration with Azure AD Conditional Access to configure real-time monitoring and control



Shadow IT management lifecycle

Safely adopting cloud apps



Cloud Discovery

Continuous report
GlobalTimeframe
Last 30 days[Dashboard](#) [Discovered apps](#) [IP addresses](#) [Users](#)

Updated on Mar 26, 2019

QUERIES	APPS	APP TAG	RISK SCORE	COMPLIANCE RISK FACTOR	SECURITY RISK FACTOR	Save as	Advanced
Select a query...	Apps...	<input checked="" type="checkbox"/> <input type="checkbox"/> None	<input type="radio"/> 0 <input type="radio"/> 3 <input type="radio"/> 10	Select factors...	Select factors...		

Browse by category:

1K+ Search for category...

1 - 5 of 5 discovered apps

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Last seen (...)	Actions
MEGA Cloud storage	3	90 MB	46 MB	86	62	56	Mar 25, 2019	
SendMyWay Cloud storage	3	90 MB	47 MB	83	70	45	Mar 25, 2019	
PowerFolder Cloud storage	3	94 MB	49 MB	88	73	52	Mar 25, 2019	
NetFortris Cloud storage	3	83 MB	42 MB	80	65	42	Mar 25, 2019	
OwnCube Cloud storage	3	93 MB	48 MB	85	72	45	Mar 25, 2019	

- [TAG APP](#)
- [Sanctioned](#)
- [Unsanctioned](#)
- [Custom app](#)
- [Accounting Dept](#)
- [Deprecated](#)
- [In legal review](#)
- [In review](#)
- [In technical POC](#)
- [Managed](#)

Tag an app as unsanctioned to block it from being accessed by users in the future

This website is blocked by your organization. Contact your administrator for more information.
mega.nz

[Back to safety](#)

Windows Defender SmartScreen

Protect your files and data in the cloud

Data is ubiquitous and you need to make it accessible and collaborative, while safeguarding it



Understand your data and exposure in the cloud



- Connect your apps via our API-based App Connectors
- Visibility into sharing level, collaborators and classification labels
- Quantify over-sharing exposure, external- and compliance risks



Classify and protect your data no matter where it's stored



- Govern data in the cloud with granular DLP policies
- Leverage Microsoft's IP capabilities for classification
- Extend on-prem DLP solutions
- Automatically protect and encrypt your data using Azure Information Protection



Monitor, investigate and remediate violations



- Create policies to generate alerts and trigger automatic governance actions
- Identify policy violations
- Investigate incidents and related activities
- Quarantine files, remove permissions and notify users

Key threat alerts and mitigation actions

- Identify high-risk and anomalous usage
- Exfiltration of data to unsanctioned apps
- Rogue 3rd party applications
- Ransomware attacks
- Mitigate ransomware attacks
- Suspend user sessions
- Revoke OAuth app access

Cloud App Security

Alerts > Ransomware activity 3 MONTHS AGO

Ransomware activity 16.220.196.35 billd@mcas-test9.com Microsoft OneDrive for Business

Resolution options: Bill Dortch

Description

The user billd@mcas-test... Additional risks in this user's account

- This user uploaded files to Microsoft OneDrive for Business

View related activity
View related governance
View related alerts
View owned files
View files shared with this user

Activity log

OFFICE 365

Require user to sign in again
Suspend user
Account settings in app

MICROSOFT ONEDRIVE FOR BUSINESS

Suspend user
Require user to sign in again
Suspend user

1 - 10 of 1,240 activities

User	App	IP address	Location	Device
billd@mcas-test9.com	Microsoft On...	16.220.196.35	United Kin...	💻 Windows 📱
billd@mcas-test9.com	Microsoft On...	16.220.196.35	United Kin...	💻 Windows 📱
billd@mcas-test9.com	Microsoft On...	16.220.196.35	United Kin...	💻 Windows 📱

SHOW SIMILAR

General User IP address

16.220.196.35 OPEN ALERTS ACTIVITIES ADMIN ACTIVITIES IP ACTIVITIES (30 DAYS) See all

United Kingdom, England, London
ISP: Microsoft Corporation

131 13 0

Filter by this IP address

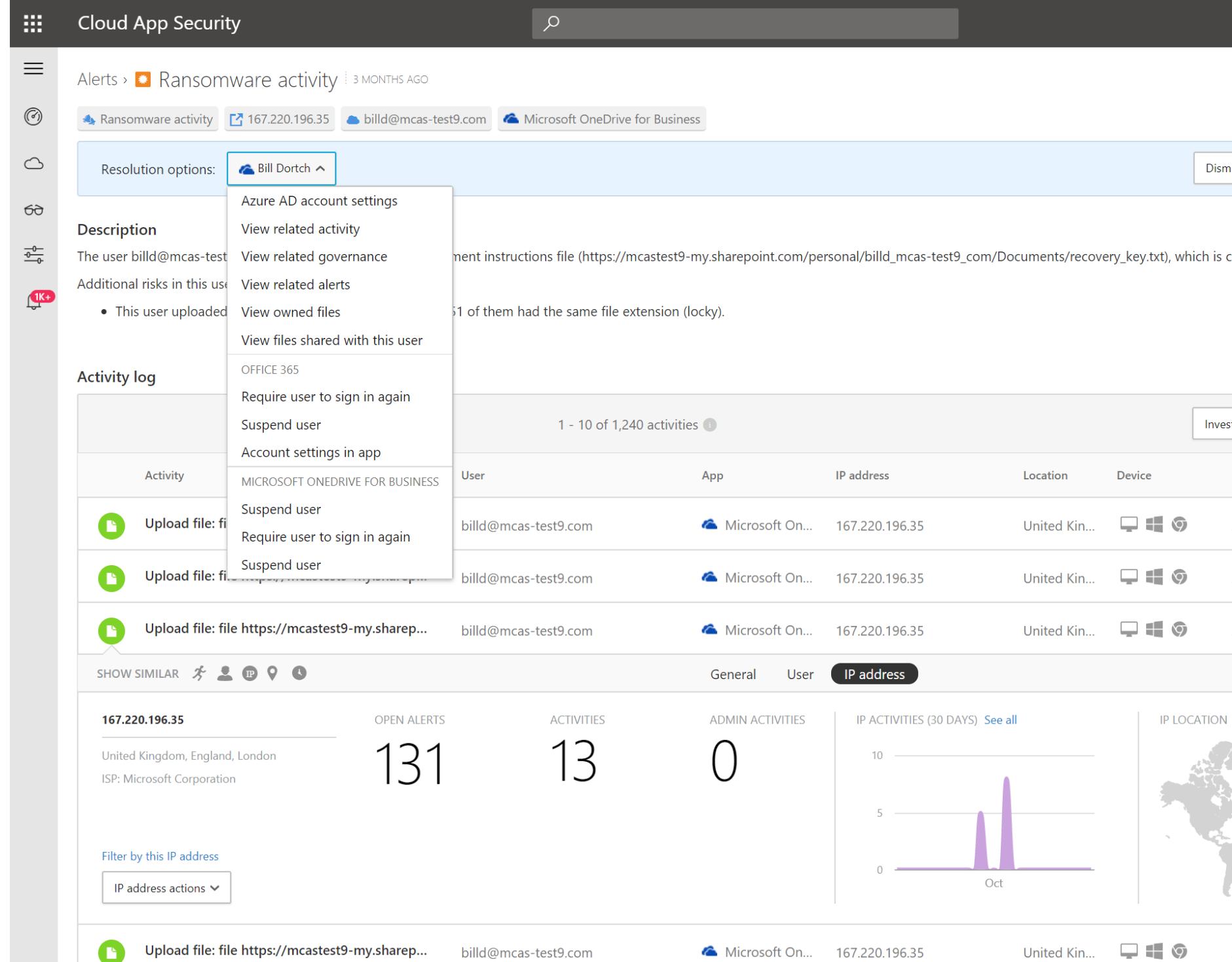
IP address actions

Upload file: file https://mcastest9-my.share...

billd@mcas-test9.com Microsoft On... 16.220.196.35 United Kin... 💻 Windows 📱

Oct

IP LOCATION



Comprehensive Threat Protection for your cloud apps

- Built-in Threat Protection policies**
- More than 15 out-of-the-box policies that alert you on some of the most common cloud threats such as impossible travel, impersonation activities or ransomware detection
- Malware Detonation**
- Intelligent heuristics identify potentially malicious files and detonate them in a sandbox environment - for existing and newly uploaded files
- Customize policies to alert and remediate**
- Customize what you want to be alerted on to minimize noise and configure automatic remediation

Cloud App Security

Alerts

RESOLUTION STATUS: OPEN, DISMISSED, RESOLVED

CATEGORY: Select risk category...

SEVERITY: Low (Yellow), Medium (Orange), High (Red)

APP: Select apps...

USER NAME: Select users...

1 - 12 of 12 alerts

Alert	App	Resolution	Severity	Date
Risky OAuth apps 178.17.166.149 Bill Dorch	Salesforce - General	RESOLVED	Low	2 d
Ransomware activity 178.17.166.149 Bill Dorch	Amazon Web Service	RESOLVED	High	2 d
Malware campaign caught in delivery 178.17.166.149 Bill Dorch	Slack - General - General	RESOLVED	Low	2 d
Activity from a Tor IP address 79.137.68.85 Bill Dorch	Box - General - General	RESOLVED	Medium	2 d
Alert on any session coming from a Risky IP address 79.137.68.85 Bill Dorch	Office 365	DISMISSED	Low	2 d
Logon from a risky IP address 79.137.68.85 Bill Dorch	Workplace by Facebook...	DISMISSED	High	2 d
Logon from a risky IP address 79.137.68.85 Bill Dorch	Microsoft SharePoint O...	DISMISSED	High	2 d

Policies

NAME	TYPE	STATUS	SEVERITY	CATEGORY
<input type="text" value="Policy name..."/>	<input type="button" value="Select type..."/>	<input type="button" value="ACTIVE"/> <input type="button" value="DISABLED"/>		Threat detection
<p>1 - 20 of 32 Policies</p>				
Policy	Count	Severity	Category	
Potential ransomware activity Alert when a user uploads files to the cloud that might be infected with ransomware.	6 open alerts		Threat detection	
Logon from a risky IP address Alert when a user logs on to your sanctioned apps from a risky IP address. By default...	48 open alerts		Threat detection	
Malware campaign caught in delivery Several emails containing malware were detected within one session, indicating a pos...	0 open alerts		Threat detection	
Multiple failed user log on attempts to an app Alert when a single user attempts to log on to a single app, and fails more than 10 ti...	11 open alerts		Threat detection	Jun 3, 2018
Mass download by a single user Alert when a single user performs more than 30 downloads within 5 minutes.	18 open alerts		Threat detection	Aug 12, 2018

Out of the box Threat Protection policies



- ✓ Microsoft Flow
- ! Microsoft OneDrive for Business - General
- ! Microsoft Power BI
- ! Microsoft SharePoint Online - General
- ! Microsoft Teams - General
- ✓ Microsoft Office Online
- ✓ Microsoft Office Online
- ! Active Directory
- ✓ Microsoft Secure Score
- ✓ MyCustomApp
- ✓ Salesforce - EU
- ✓ Salesforce - General
- ✓ Atlassian - General
- ✓ Dropbox - General
- ✓ Dropbox - US
- ✓ DropBox [Deprecated]
- ✓ G Suite - General
- ✓ Microsoft AppSource
- ✓ Microsoft 365

Top users By investigation priority

over the last week

127	Stella Middleton
65	Lazelle Fuller (Admin)
34	Asbury Freeman
33	Valjean Stanley
32	Willman Dorsey

Activity map

over the last month ▾



Trends

Activities

Active users

over the last month ▾



G Suite - General

Microsoft SharePoint Online - General

Box - General

Office 365 - General

10,000



Microsoft Exchange Online - General

Microsoft Power BI

Microsoft Teams - General

Microsoft OneDrive for Business



ServiceNow

Yammer

Microsoft Office Online

Google Docs

Top users by investigation priority on the Cloud App Security Dashboard

User actions ▾

Stella Middleton
Marketing manager
Sensitive Admin

124

USER THREAT

Investigation priority 127 Alerts 12

Identity risk score High MFA Not enabled

Last seen 9 days ago

USER EXPOSURE

Devices 6 (owns 3) Accounts 4 •

Resources 2 Locations 3

Discovered apps 250 • Matched files 3

CONTACT INFORMATION [View more](#)

Email evam@contoso.com

Phone +972 (74) 7569213

Manager Felicia Florick

User risk Additional data Discovered apps Matched files

Investigation priority score

127

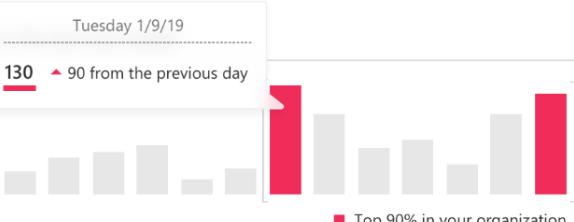


- 8 alerts Score: 70
- 7 risky activities Score: 12
- 6 ASI alerts Score: 45

Score is based on the last 7 days [How do we score?](#)

- User's score compared to the organization 91%
User's score compared to user's peers 56%

User risk



Alerts and risky activities that contributed to the score (last 7 days) [View all user alerts \(12\)](#)

Time	Score Change	Action	Date	Device	Killchain phase
Today	+20	Mass download alert	1/9/19, 12:46 PM	WK-Win10-PC	Target
	+8	Log on	1/9/19, 11:02 PM		
	+12	Resource access - Device: WK-Win10-PC	1/9/19, 11:02 PM	Device: WK-Win10-PC	
Yesterday	+18	Risky sign-in	1/8/19, 11:02 PM		Track
	+10	Can compromise a sensitive user using lateral movement path	1/8/19, 10:54 AM		
	+12	Suspicious VPN connection	1/8/19, 9:45 AM		Track
1/4/19	+8	Log on	1/9/19, 11:02 PM	Device: WK-Win10-PC	



Scott Smith - Risky sign-ins (Preview)

[Learn more](#) [Columns](#) [Refresh](#) [Download](#) [Script](#) [Select all](#) [Confirm compromised](#) [Confirm safe](#)

Welcome to the new 'Risky sign-ins' report of the refreshed Azure AD Identity Protection. Please share your feedback when prompted.

Search is case sensitive and supports 'starts with' operator

User	Application	Status	Risk State	Risk Level (Aggregate)	Risk Level (Real-time)
Scott Smith	Filter by app name or application...	All	2 selected	0 selected	0 selected

Request Id	Conditional Access
Filter by Request Id	All

Date	Show dates as:	Risk event type(s)
Last 1 month	Local <input checked="" type="button"/> UTC	0 selected

[Apply](#) [Reset](#)

DATE	USER	APPLICATION	STATUS	RISK STATE	RISK LEVEL (AGGREGATE)	RISK LEVEL (REAL-TIME)	REQUEST ID	CONDITIONAL ACCESS
3/2/2019, 7:54:54 PM	Scott Smith	Azure Portal	Success	At risk	Medium	-	9801eb73-9acc-4072-8...	Not Applied

Details

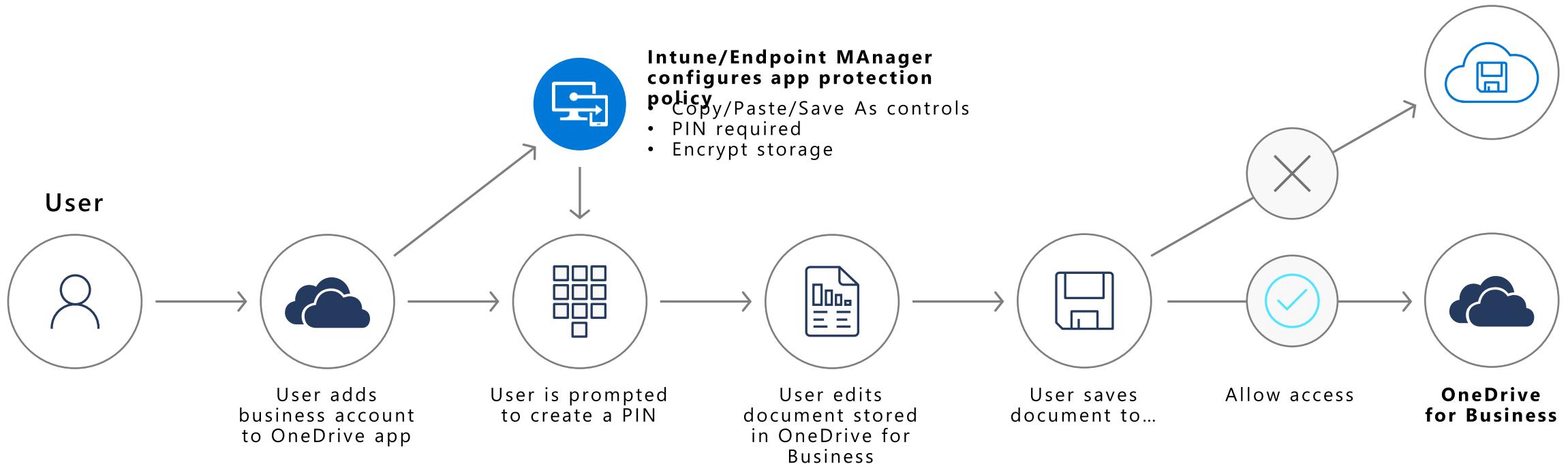
[Confirm compromised](#) [Confirm safe](#) [Risky users report](#)

[Basic info](#) [Device info](#) [Risk info](#) [MFA info](#) [Conditional Access](#)

SIGN-IN RISK STATE: At risk	SIGN-IN RISK LEVEL (AGGREGATE): Medium	SIGN-IN RISK LEVEL (REAL-TIME): Medium	SIGN-IN RISK DETAIL: -
--------------------------------	---	---	---------------------------

RISK EVENT	RISK EVENT STATE	TIME DETECTED	TYPE
(MCAS) Suspicious inbox manipulation rules	At risk	3/2/2019, 7:51 PM	Offline

Protect sensitive data on unmanaged devices



Unboxing the Secure Remote Work workshop



<https://www.microsoft.com/microsoft-365/partners/microsoft-365-accelerators#microsoft-365-partner-accelerators-secure-remote-work>

Secure Remote Work in a Day

Help customers RAPIDLY deploy Remote Work scenarios to empower employees to stay connected, while maintaining security & control.

Quick steps of Remote Work enablement

1

Enable Cloud or Hybrid Identity

Single Sign on & Self- Service
Password Reset

2

Rapid Deployment of Teams

Guided Checklists, activation, installation &
configuration

3

Providing Adoption Kit

End user training, workload introductions & support
resources

4

Secure access to Teams

Conditional Access & Multi-Factor Authentication

Follow-up M365 Partner Workshops



Teamwork
Workshops

Teams Adoption,
Meetings, Calling,
Solutions



Security
Workshops

Advanced Security,
Azure Sentinel,
Compliance



Management
Workshops

Windows Virtual
Desktop (Q1)

Secure Remote Work Workshop funding

Partner funding is available for eligible partners and customers. Funding is designed to enable partners to deliver rapid deployment & adoption engagements to assist customers with business continuity.



\$2500
per engagement

Customer Requirements

- **Existing Office/M365 customers:**
> 1000 Exchange Online qualified entitlements
- **Non-Office 365 customers:**
> 1000 PC Install Base

Program Dates

- **First day to nominate customers:**
April 16, 2020

Partner Requirements

- Co-sell Ready or Fast Track Ready
- SSPA Compliant

Proof of Execution

- Customer Satisfaction Survey
- Partner Findings Survey
- Deployment Plan

Funding Available

- \$2,500 for completion of the workshop

Partners can nominate customers here: aka.ms/SecureRemoteWorkWorkshop

Scope of the Secure Remote Work Workshop

Goal:

Help customers rapidly deploy remote Work scenarios to empower employees to stay connected, while maintaining security & control.

Scope:

Enable Identity - Single Sign on & Self- Service Password Reset

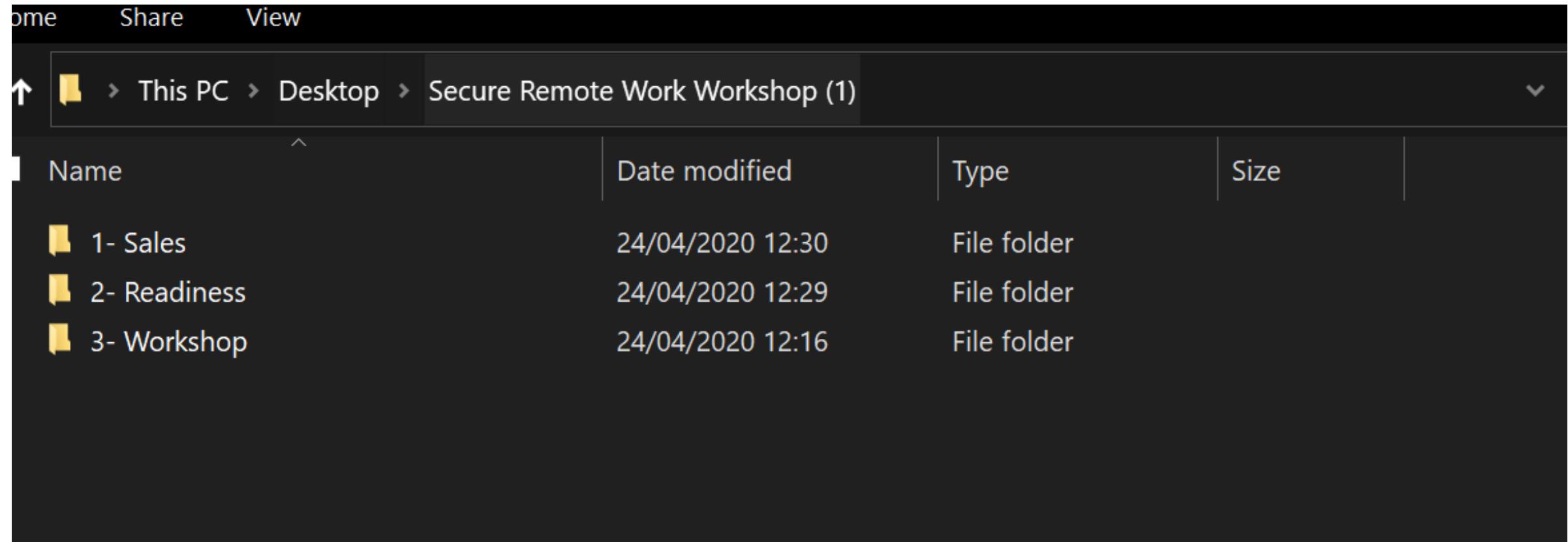
Rapid Deployment of Teams - Guided Checklists, activation, installation & configuration

Providing Teams Adoption Kit -End user Training, workload introductions & support resources

Secure access to Teams - Applying baseline security like Conditional Access & MFA



Unboxing the Secure Remote Work workshop



A screenshot of a Windows File Explorer window. The title bar shows 'Home Share View'. The address bar shows the path: 'This PC > Desktop > Secure Remote Work Workshop (1)'. The main area is a table listing three sub-folders:

Name	Date modified	Type	Size
1- Sales	24/04/2020 12:30	File folder	
2- Readiness	24/04/2020 12:29	File folder	
3- Workshop	24/04/2020 12:16	File folder	

Security



Design

During this session we will:

- Review and decide on Azure AD Self-Service Password Reset (SSPR)
- Review and decide on Azure AD Multi-factor Authentication (MFA)
- Review and decide on Azure AD Conditional Access (CA)

TIP: Even if we want to go fast to start remote working with Teams, we need the bare minimum security coverage with MFA and CA to help address this.



Open Q & A

Please ask any question in the Q&A

We will read your questions and answer them in this meeting , or a next meeting.



Poll



Which Topics should we cover next?

Planned Sessions	Main Topics
Friday, April 24, 2020	Secure Remote Work: threats, scenarios and best practices
Wednesday, April 29, 2020	Teams for Education
Friday, May 01, 2020	Bank holiday
Wednesday, May 06, 2020	Teams for Healthcare

- 1) Power Platform (how to leverage, deep dive on Crisis Communication App,...)
- 2) Information Protection
- 3) Any Other Suggestions?

Partner Support Resources

WE Weekly Technical Office Hours

- **Goal:** address the main technical topics around working remotely and leveraging Microsoft technology (incl. Teams, Security, Power Platform, Windows Virtual Desktop...)
- Weekly Sessions – aka.ms/WE-TechOfficeHours
 - **Wednesdays at 12:00 – 13:00 CET** (11:00 – 12:00 WEST, 13:00 – 14:00 EEST)
 - **Fridays at 13:00 – 14:00 CET** (12:00 – 13:00 WEST, 14:00 – 15:00 EEST)
- Hosted and moderated by **experts** on these topics, from **WE OCP Technical Team, EMEA Partner Tech Services and Corp Engineering Team**

Get help now

- Check out the [Technical Support Options](#) for Microsoft Partners
<https://support.microsoft.com/en-us/help/4020188/technical-support-for-microsoft-partners>
- If you have a **dedicated Partner Development Manager / Partner Technology Strategist** – reach out to them [directly](#) with your query
- If you do not have a dedicated Partner Development Manager / Partner Technology Strategist, and you need **guidance on a specific customer scenario** (pre-sales technical or deployment assistance) – make use of your [advisory hours](#) and reach out to [Partner Technical Services](#)

Secure Remote Work Workshop

aka.ms/RemoteWorkWorkshop

Partner-led ONE day engagement to help customers **RAPIDLY deploy Remote Work scenarios** to empower employees to stay connected, while **maintaining security & control**.



Preparation

Define scope, identify stakeholders, and gather information on current environment and workloads to be enabled or optimized for Remote Work.



Design

Determine the Identity, Teams, Office 365 and Security requirements to deploy Remote Work scenarios securely.



Deployment Plan

Develop joint deployment plan, including timelines and next actions.

Secure Remote Work Workshop - for Business

The Secure Remote Work Workshop for business - a free online tool that available within the [Commercial Consulting Tool \(CCT\)](#) - available in late April.

This assessment is optimized for customers [under 1000](#) seats and includes 3 tailored deliverables:

- subscription recommendation
- basic deployment pre-flight check
- detailed deployment checklist for partners

The screenshot shows the Microsoft Commercial Consulting Tool (CCT) interface. At the top, there's a banner with a photo of people working at a desk. Below it, the title "Commercial Consulting Tool" is displayed, followed by a brief description: "This tool empowers sellers to comprehensively assess complex customer scenarios, help customers discover the benefits of the Microsoft modern workplace solutions, and provide customer-friendly recommendations that increase sales and customer success." On the left, there's a "Solution Areas" section with icons and descriptions for Productivity, Security, Collaboration, Communication, Surface, and Deployment. On the right, there's a "What's new" section with a card for "Learn about Microsoft 365 Business with help from an 'expert'" and another for "Microsoft Azure within reach: Winning the SMB customer". A "View All" button is at the bottom right of the news section.

Virtual End-to-End Microsoft Security Bootcamp



We're excited to invite you to our three half days security bootcamp with our Engineering experts to learn more about **Microsoft Security solutions**. This training focuses on providing practice leads, security architects, and consultants **a deeper understanding of the capabilities within the Microsoft Security stack**.

- **Targeted audience:** individuals who have fundamental technical skills in security and want to expand their security practices and increase their expertise in Microsoft Security solutions,
- **When:** April 28-30, 2020
- **Registration and agenda:** [Link](https://learning.eventbuilder.com/SecurityBootcamp) <https://learning.eventbuilder.com/SecurityBootcamp>

Microsoft Teams Virtual Calling and Meetings Bootcamp



We are excited to invite you to a five half-days virtual technical bootcamp with subject matter experts from Microsoft where you'll learn the landscape of **Teams architecture, governance, and manageability** with special tech focus on Meetings and Teems Room.

- **Targeted audience:** Individuals responsible for Teams practice development and those willing to sharpen their tech expertise with Microsoft Teams Calling
- **When:** May 4-6, 11&13, 2020
- **Registration and agenda:** [Link](https://learning.eventbuilder.com/CallingAndMeetingsBootcamp) <https://learning.eventbuilder.com/CallingAndMeetingsBootcamp>

Other Partner Resources

- **Best practices and discussion for remote work**
 - [Best practices](#), based on Microsoft internal learnings
 - (new) [Microsoft Tech Community](#) forum for discussing / sharing best practices
- **Enabling Microsoft Teams**
 - We recommend that partners lead with the [CSP Trial](#). See details in our [news article](#).
 - For customers who **don't align to the CSP Trial**, partners can get access to the **Office 365 E1 Trial** for them. Go to [Partner Center Support](#) and click on *CSP > Cannot find an offer in the catalog*.
- **Resources for Education Partners**
 - Check out the [EDU Partner Flash on Yammer](#)
 - **[Office 365 A1 – Free](#)** versions to **all educational institutions**: unlimited chat, built-in group and one-on-one audio or video calling, 10 GB of team file storage, and 2 GB of personal file storage per user. You also get real-time collaboration with the Office apps for web, including Word, Excel, PowerPoint, and OneNote. No restrictions for # of users.
 - **[Microsoft Teams for Free](#)** (**Individuals** and **IT roll-out** – in Office 365 A1 above): unlimited chat, built-in group and one-on-one audio or video calling, 10 GB of team file storage, and 2 GB of personal file storage per user.
 - **[Minecraft: Education Edition](#)**: We've extended access to Minecraft: Education Edition to all free and paid O365 Education accounts through the end of June 2020 and published a [M:EE remote learning toolkit](#) with links to >100 Minecraft lessons and STEM curriculum.

Feedback Form

- Feedback on sessions
- Topic suggestions

Please take 1 minute to fill the survey and help us improve!



or <https://aka.ms/WE-TechOfficeHoursSurvey>

Thank You!

