Microsoft

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)

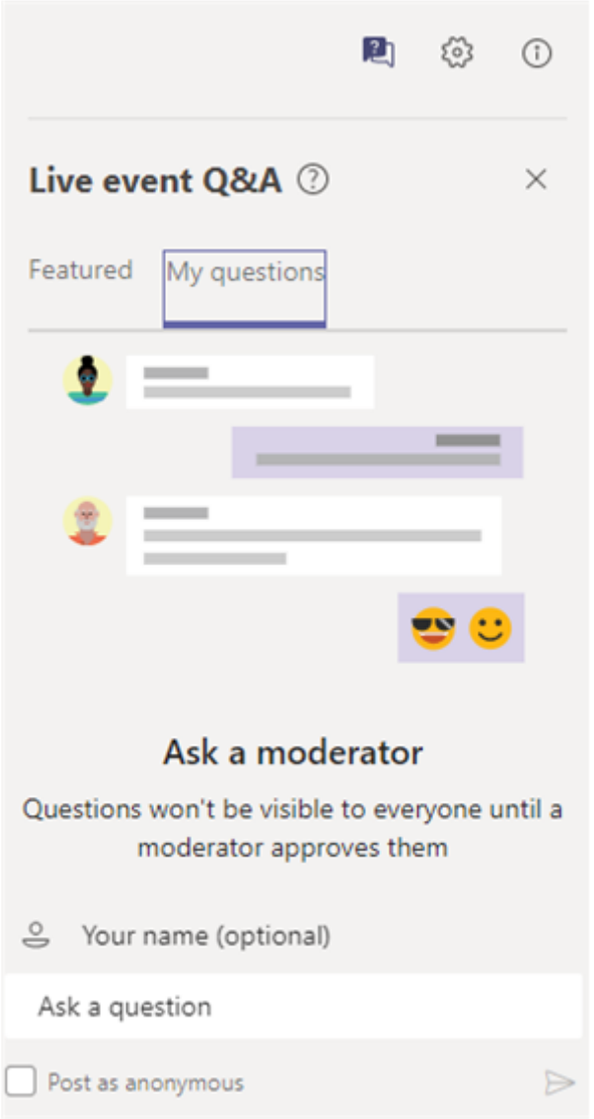
Philippe Goldstein
Partner Tech. Manager

WE Weekly Technical Office Hours – How it works

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

Questions via chat through

Q&A



(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)

All sessions will be held in **English**.

https://aka.ms/WE-TechOfficeHours

Wednesdays

Fridays

Don't miss a session;

Update your calendar by using the invites above.

Next Session Details

Upcoming Sessions

Materials & Recordings

Other Resources

Feedback Form

Hey, This landing page is actually a PowerPoint. Click through to see the next slides.

Microsoft

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

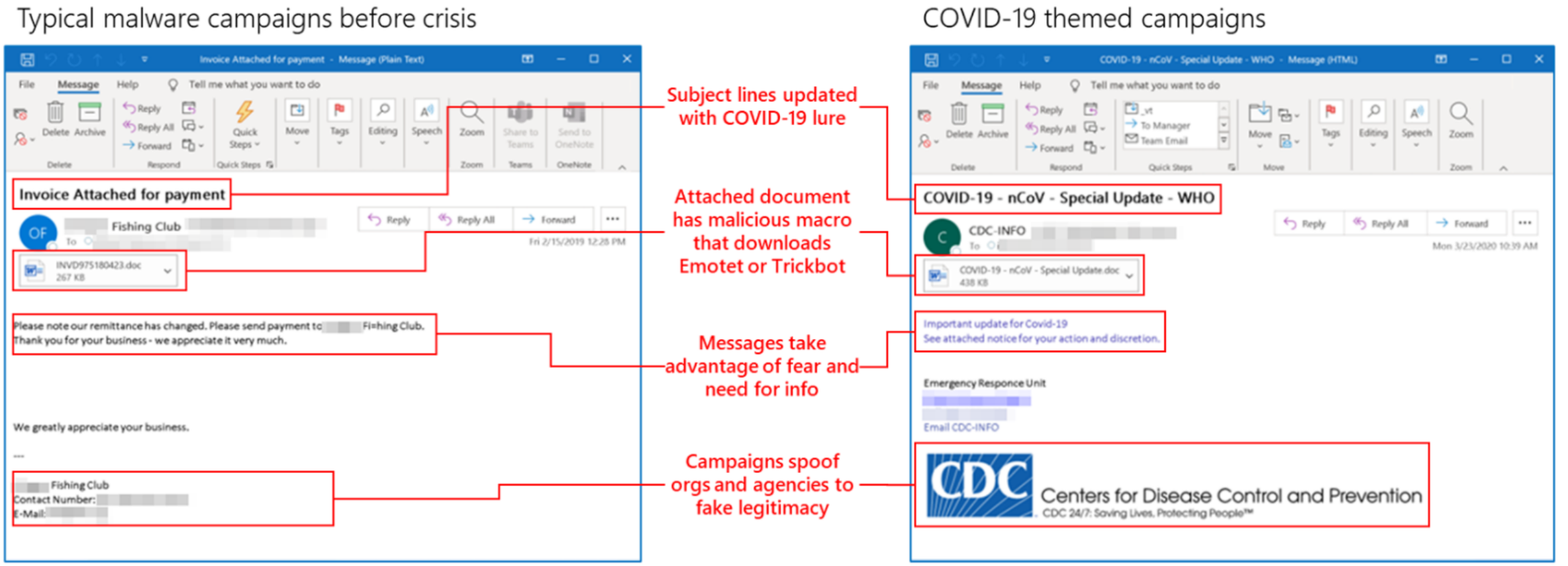
Secure Remote Work:
threats, scenarios and best practices

Matteo Malagnino
Cloud Solution Architect (Security)

The COVID-19 threat landscape

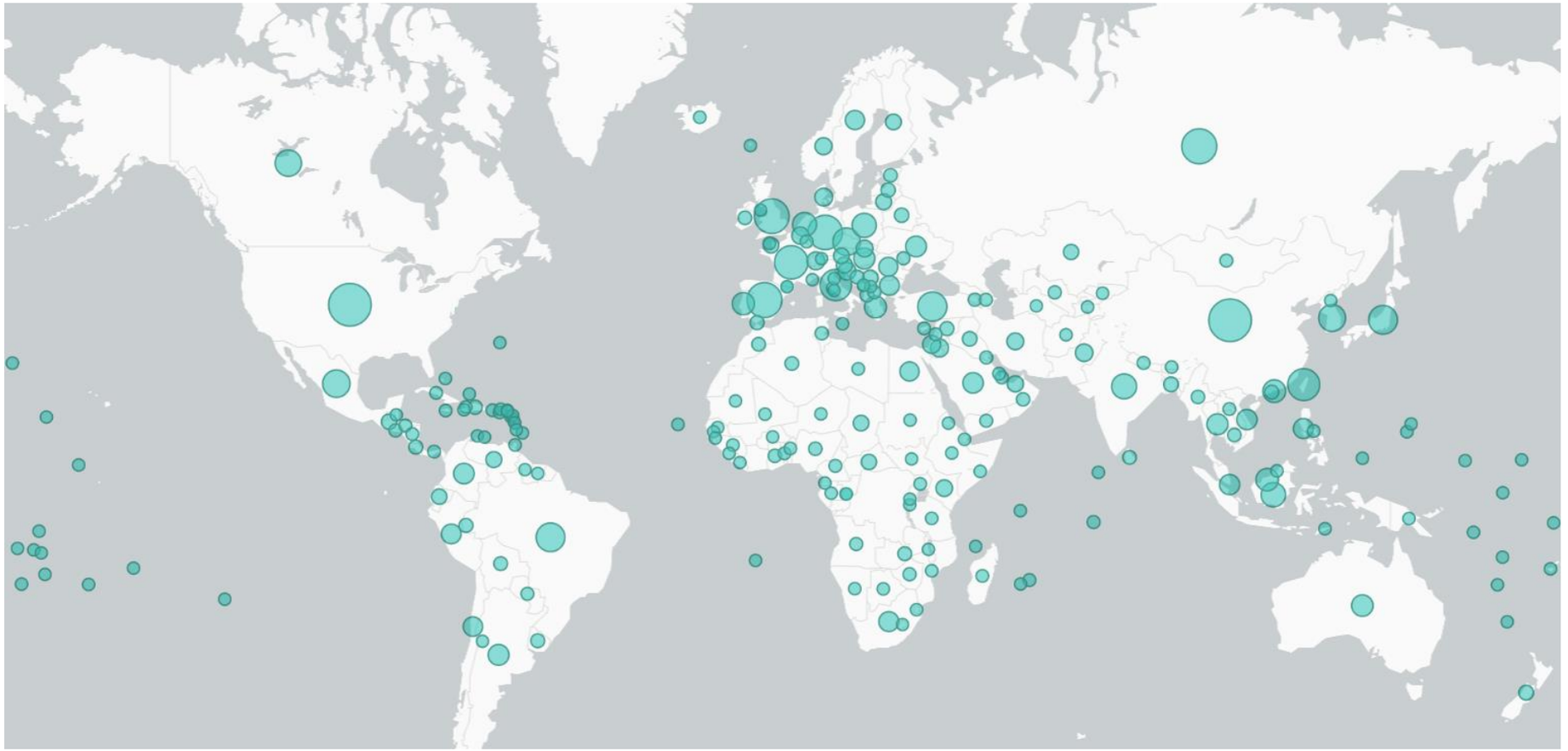
Attackers are capitalizing on fear. We're watching them. We're pushing back.

The phishing campaign



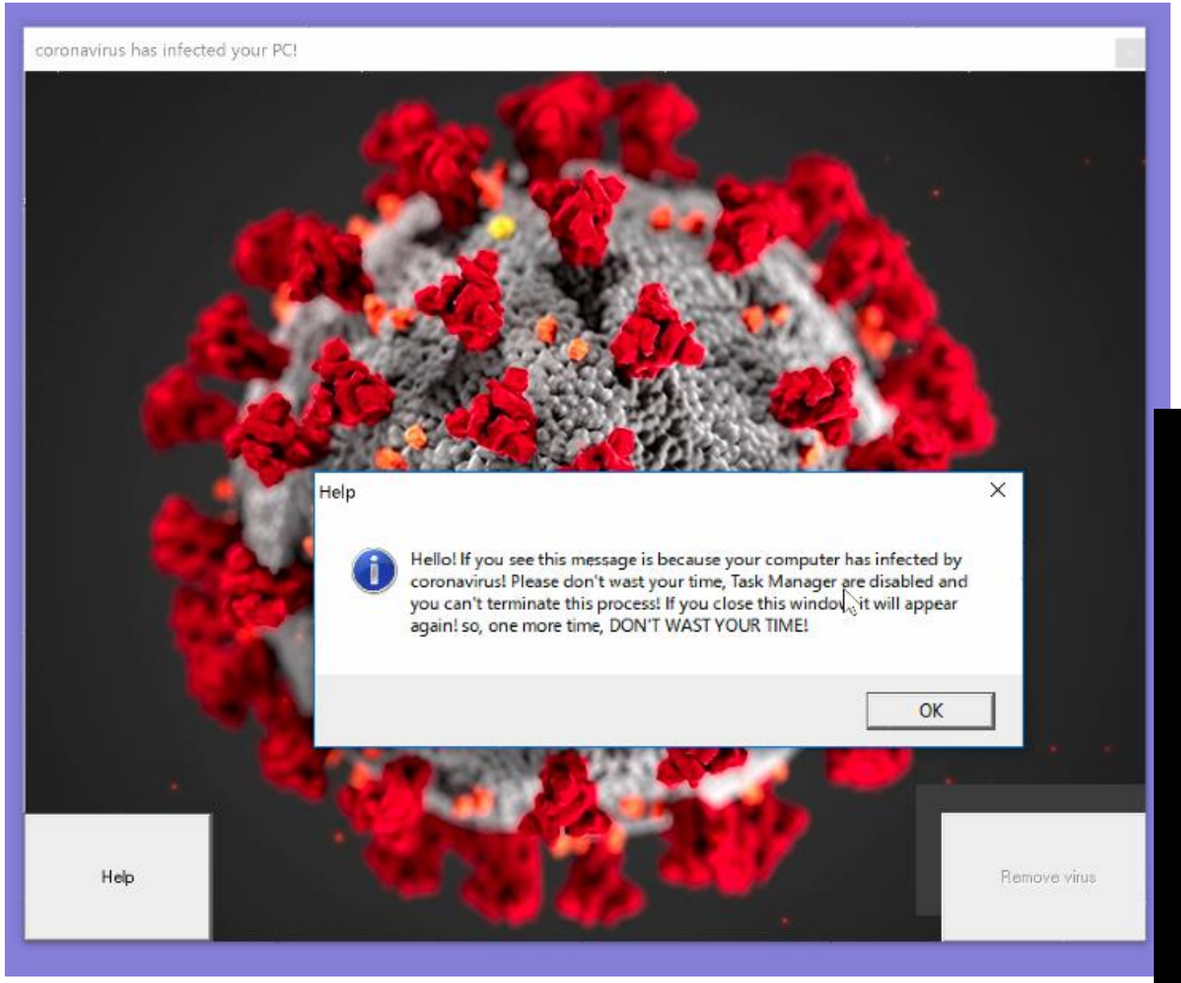
The trendy and pervasive Trickbot and Emotet malware families are very active and rebranding their lures to take advantage of the outbreak. We have observed 76 threat variants to date globally using COVID-19 themed lures (map below).

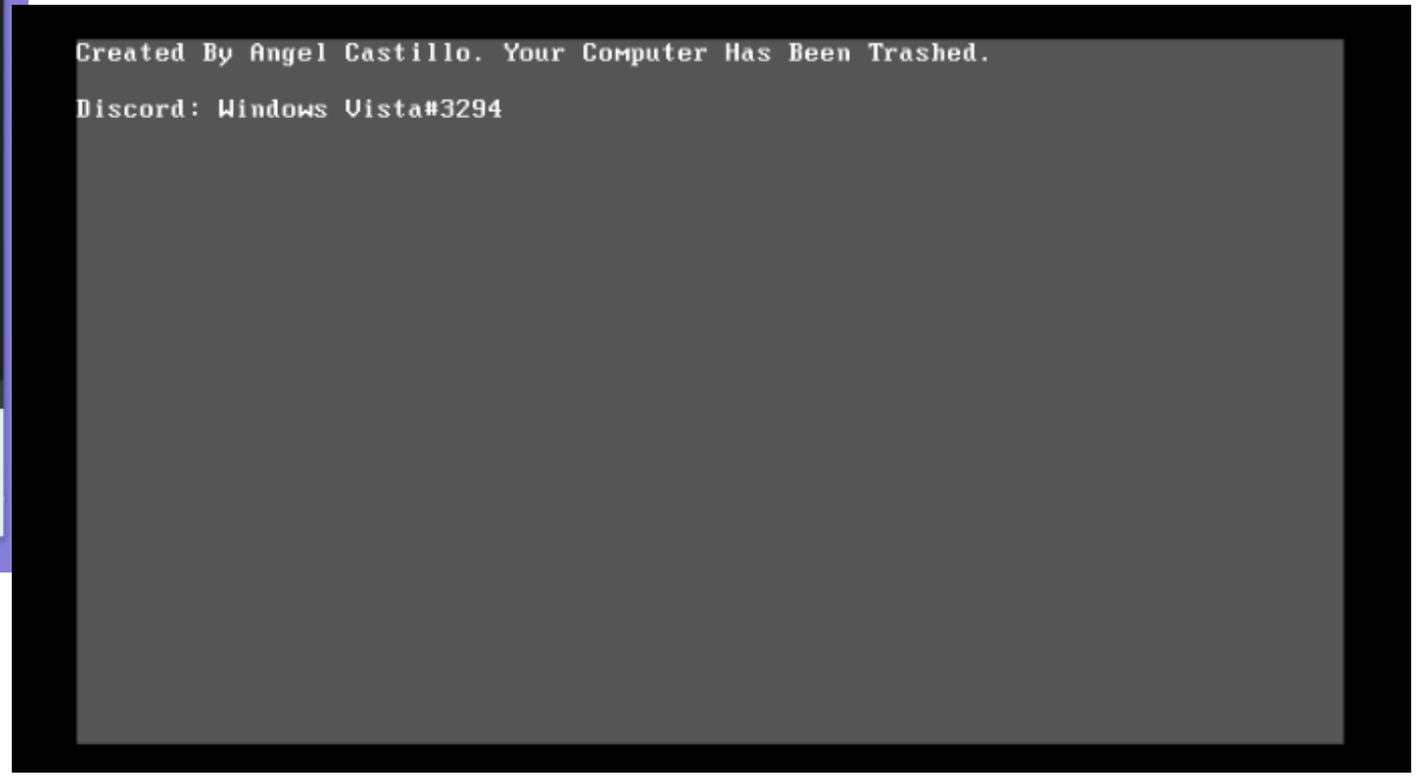
The phishing campaign



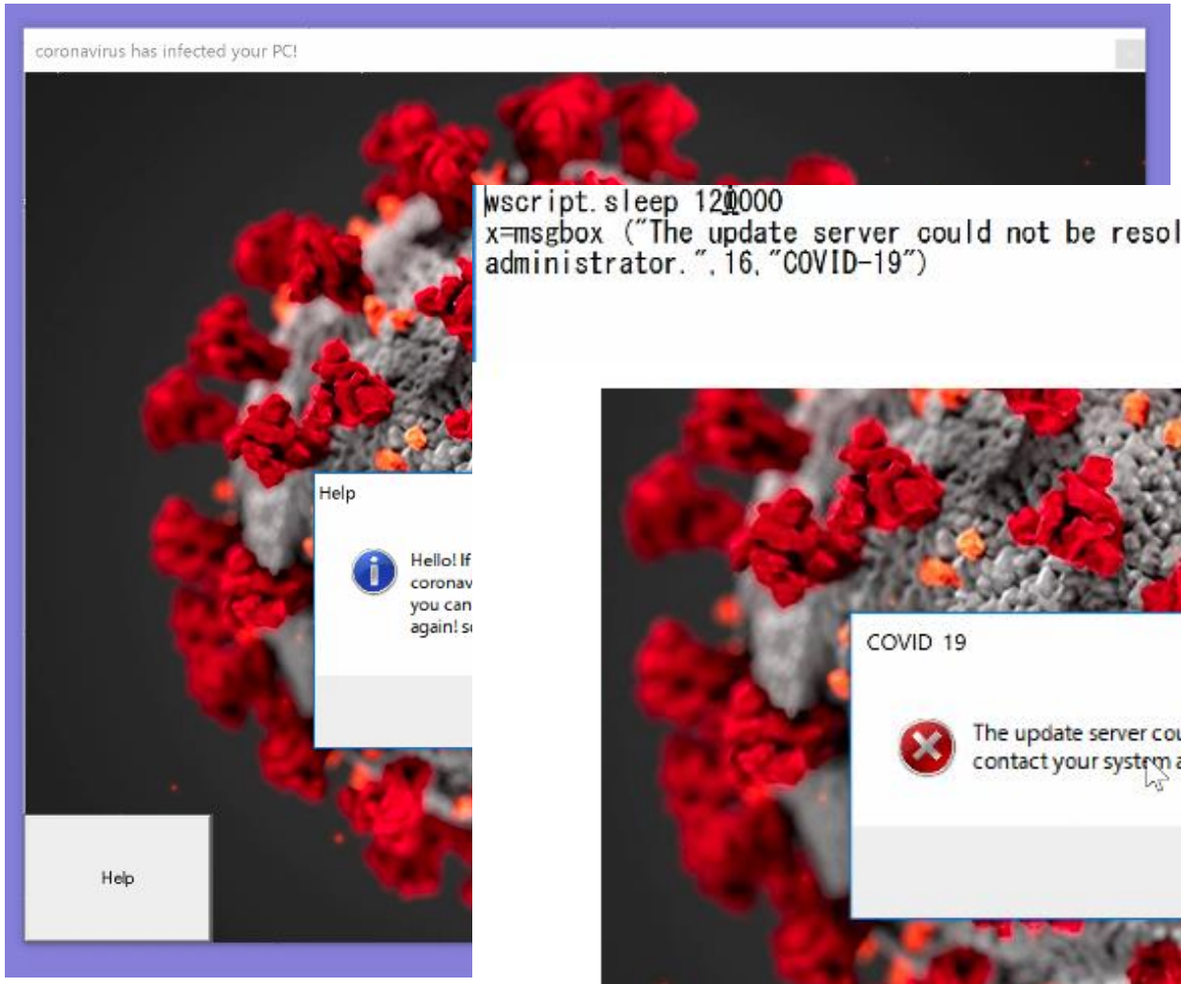
The trendy and pervasive Trickbot and Emotet malware families are very active and rebranding their lures to take advantage of the outbreak. We have observed 76 threat variants to date globally using COVID-19 themed lures.

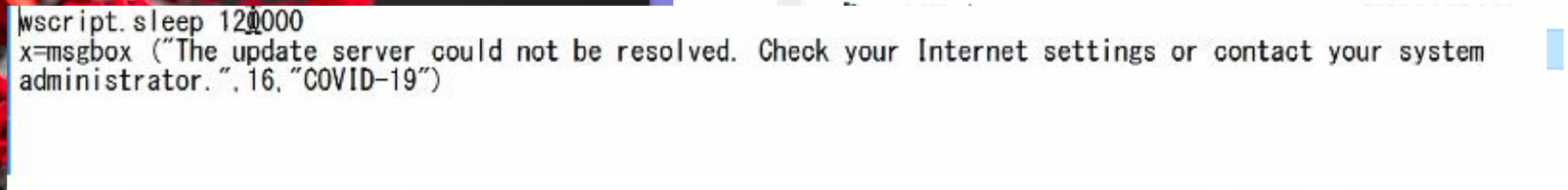
The infection

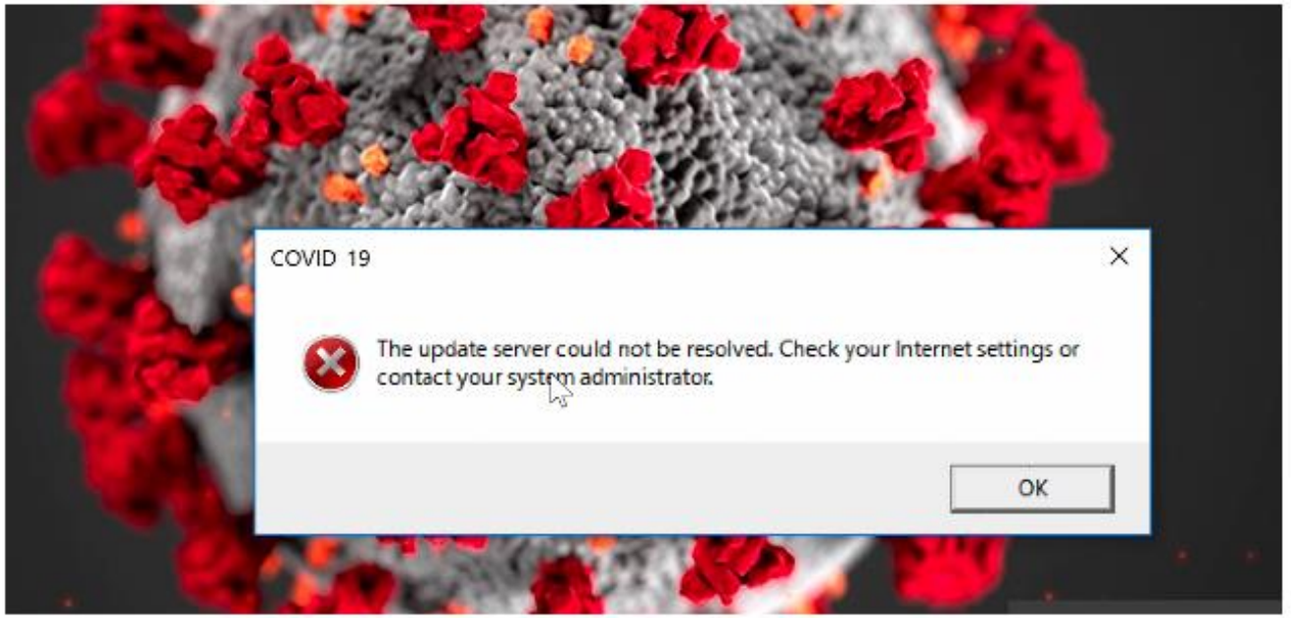




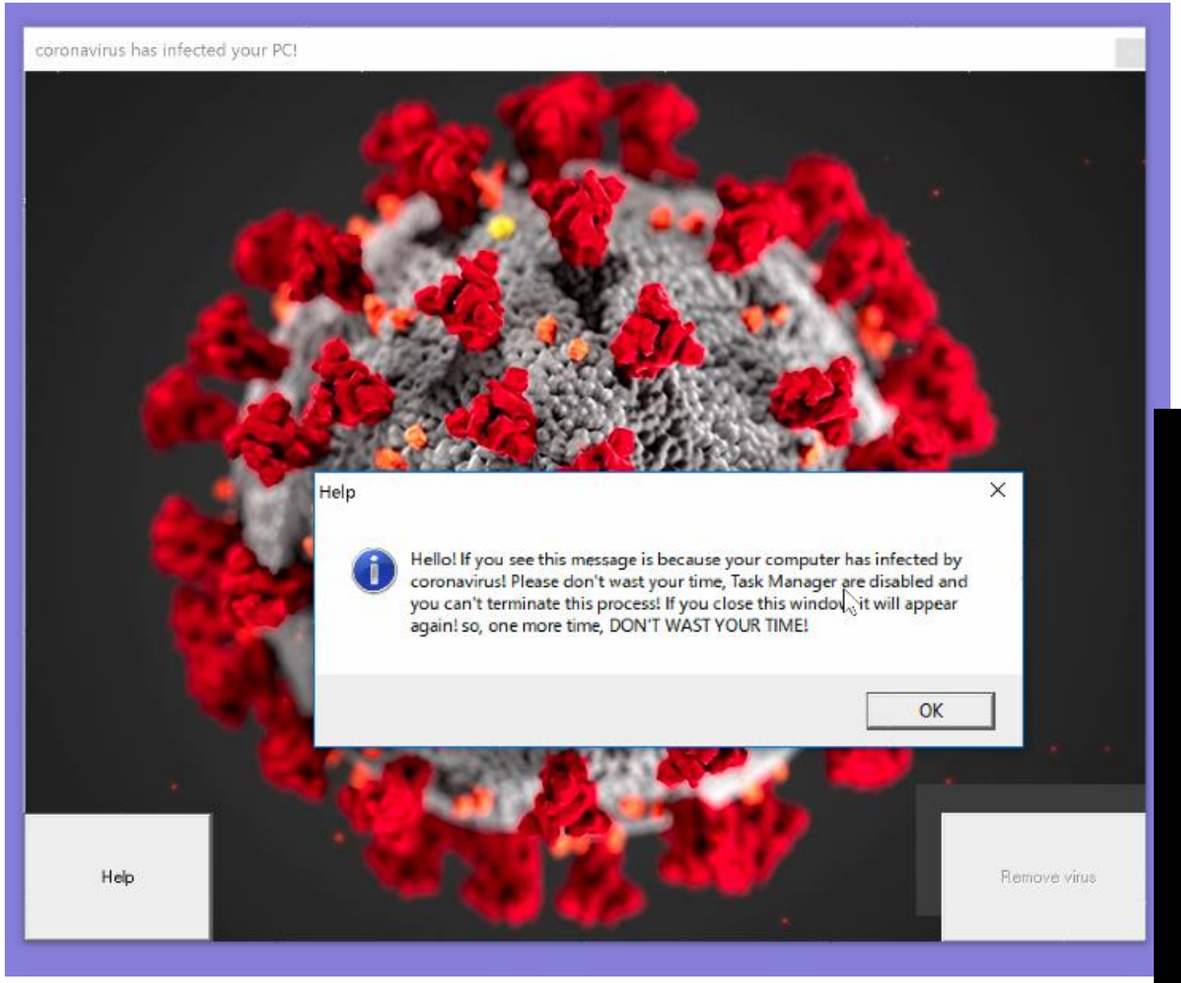
The infection

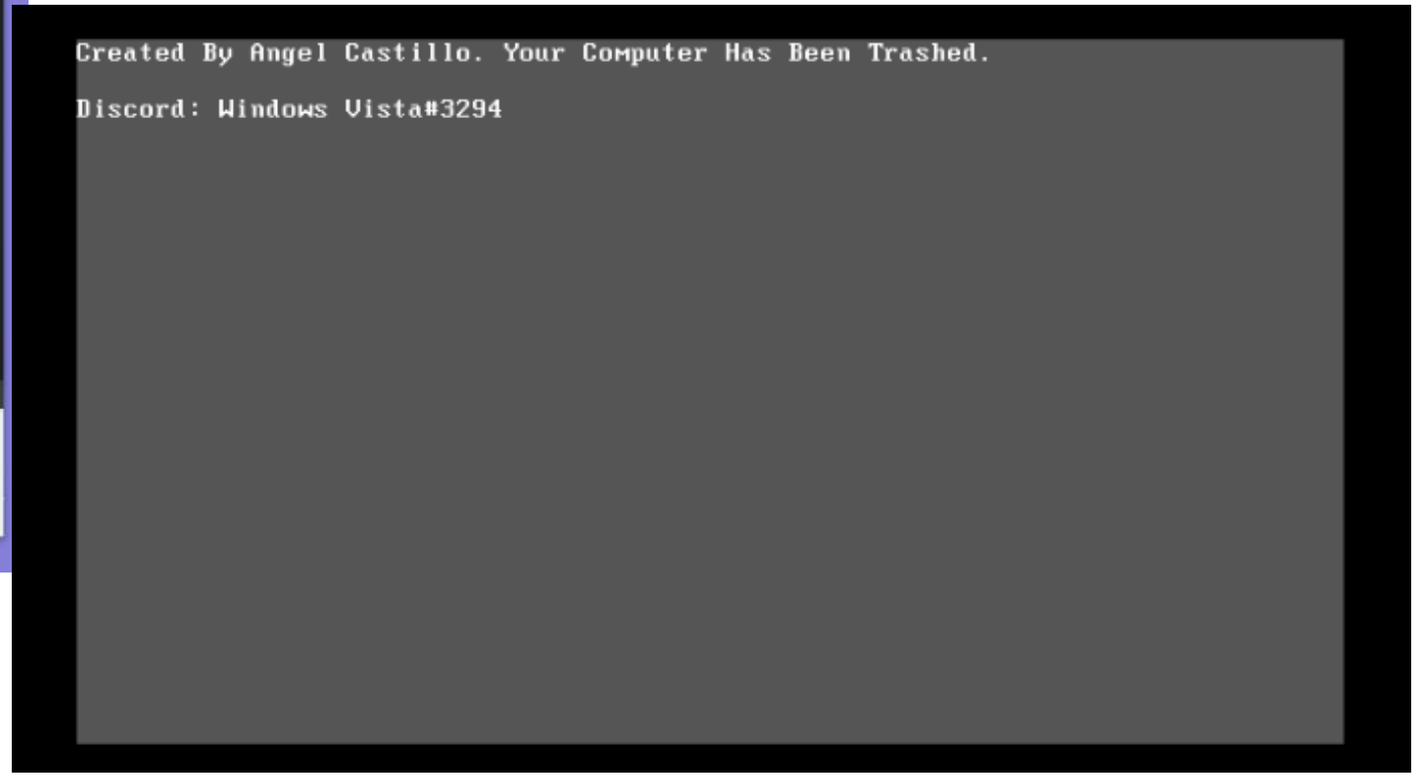






The infection





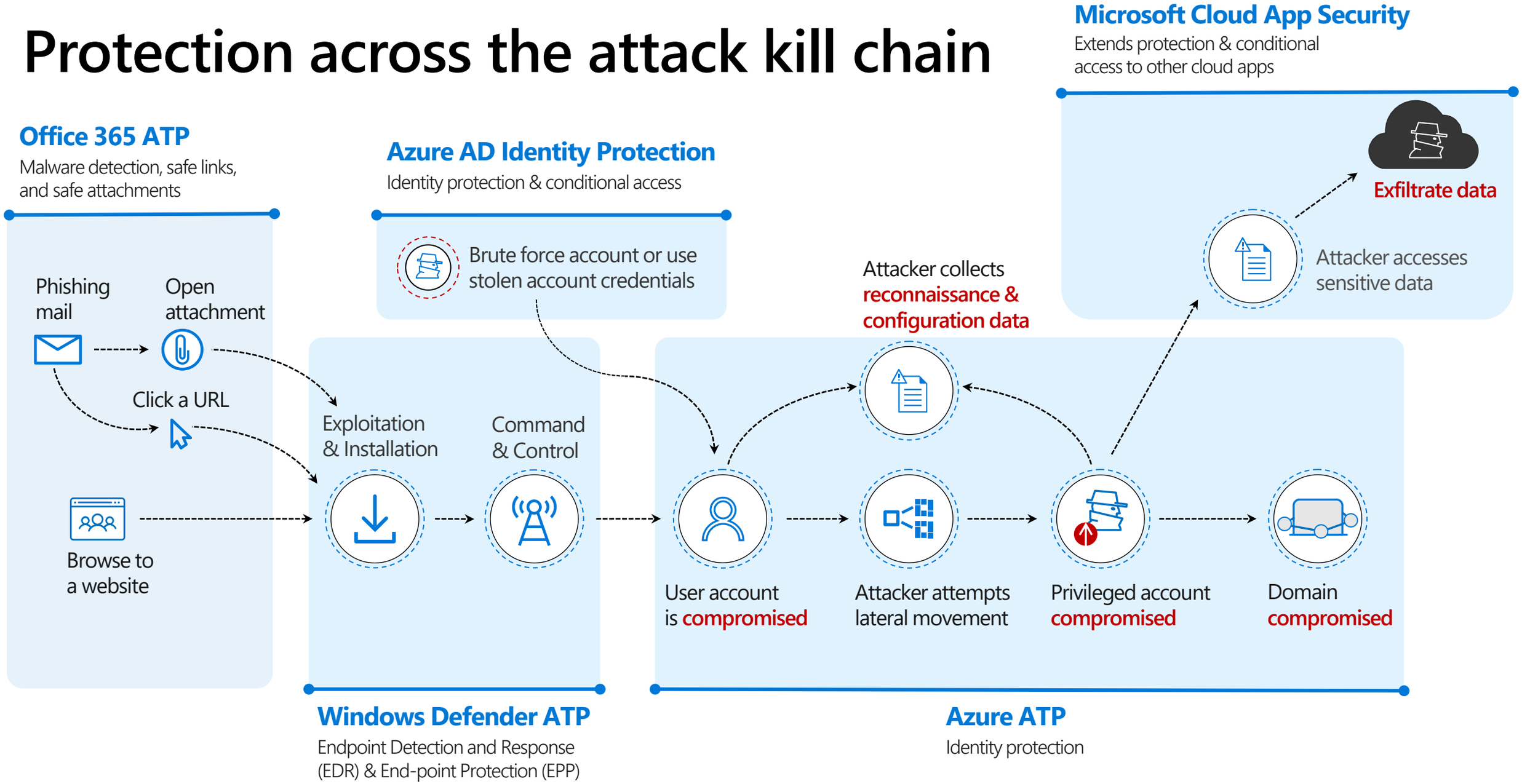
The ….. campaign

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



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.

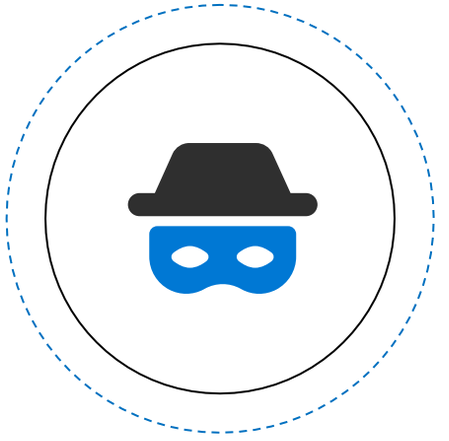
O365 ATP

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

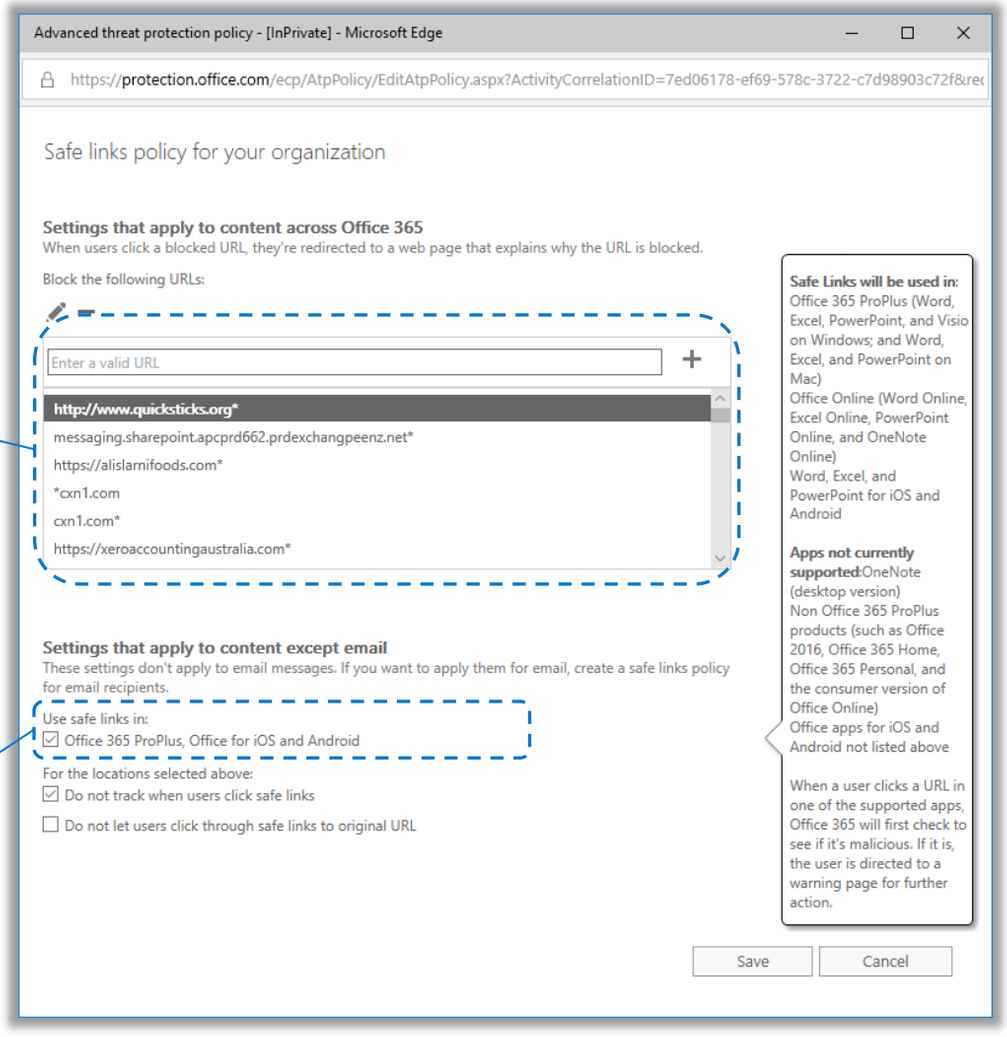
Safe Links for Office Clients

Zero-hour Auto-Purge

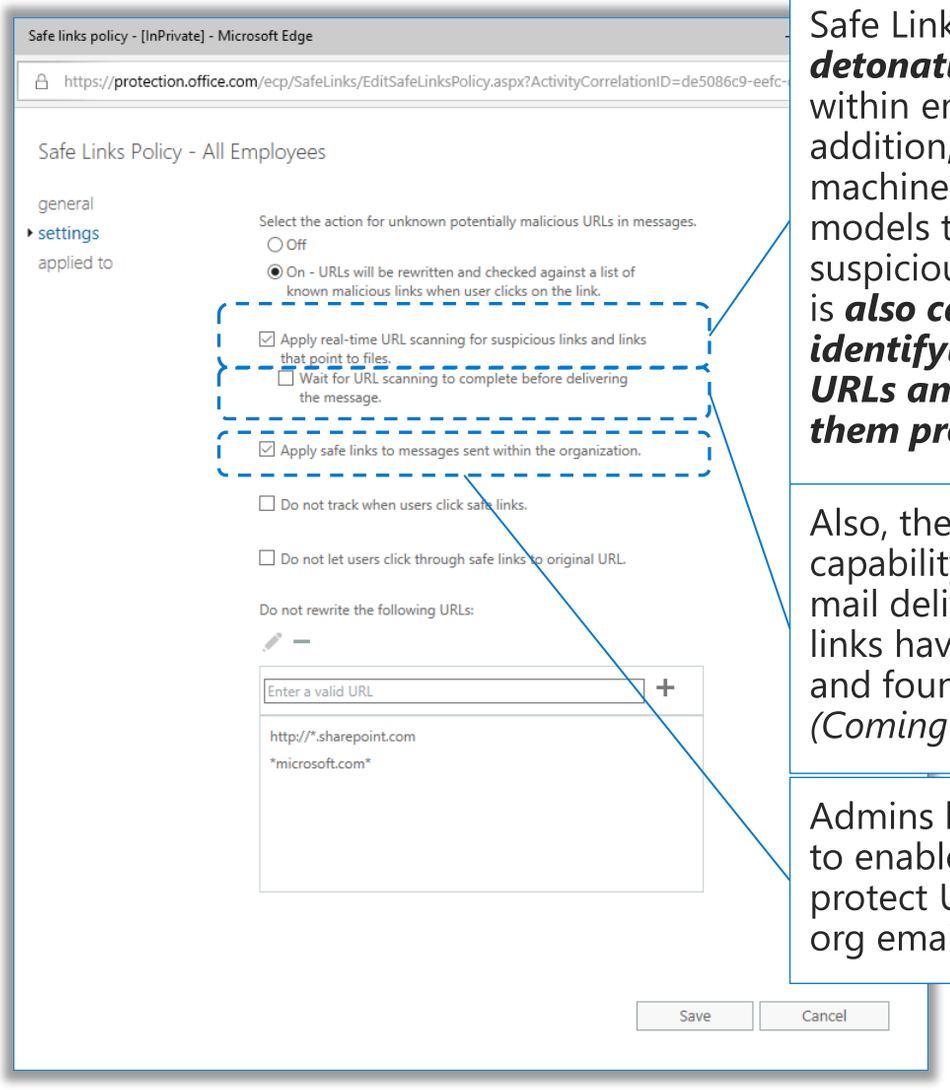
ATP Safe Links – Capabilities shown within policies

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

Safe Links can protect users from linked threats within Office.



ATP Safe Links – Organizational policy



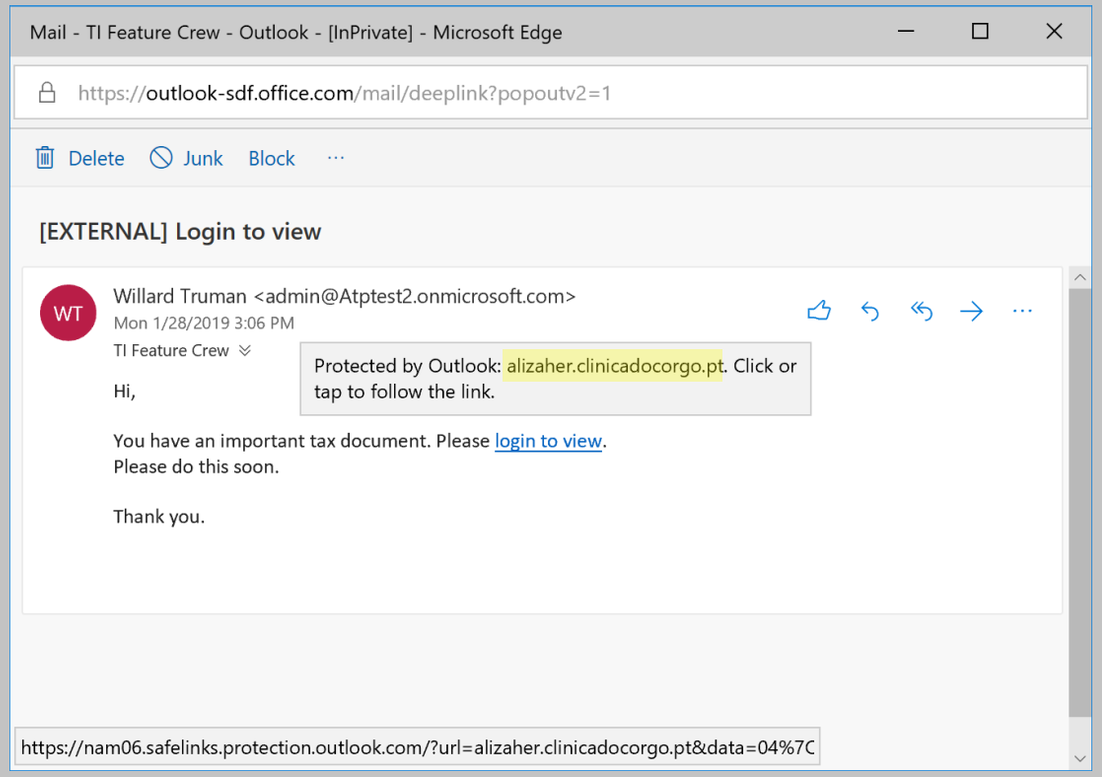
ATP Safe Links – Recipient-based policy

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***.

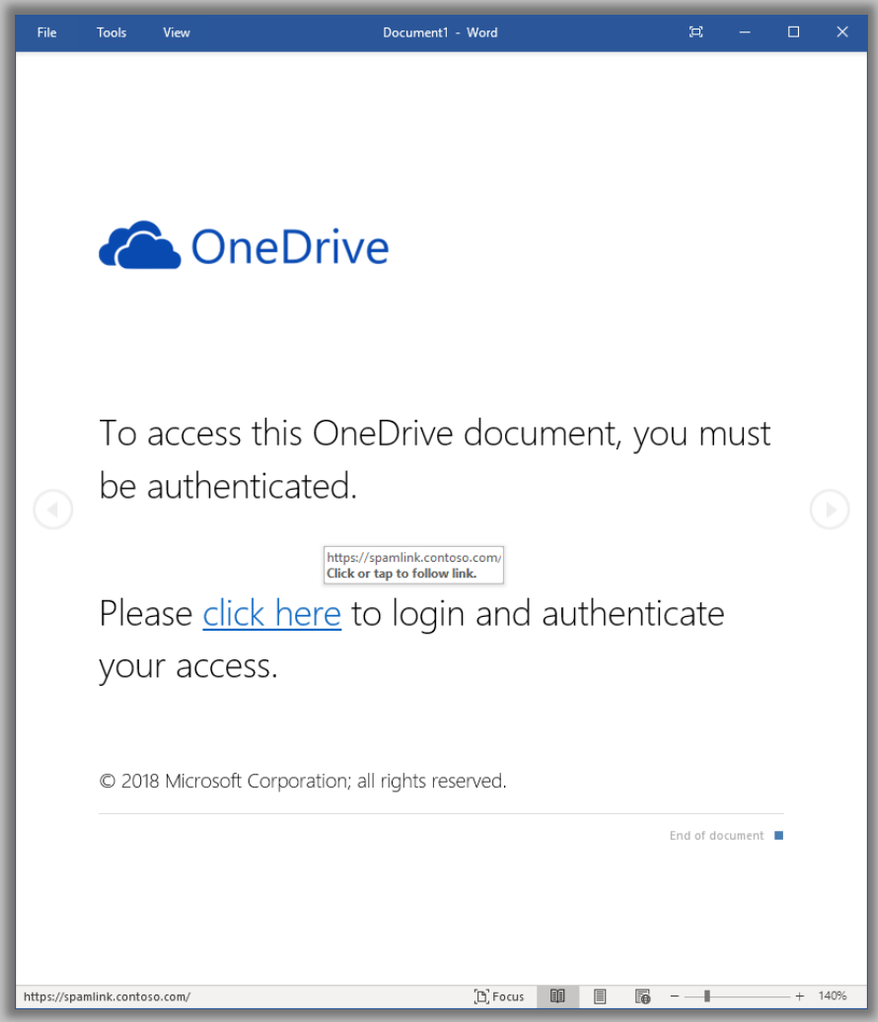
Also, there's the capability of holding off mail delivery until all links have been scanned and found to be safe. *(Coming soon!)*

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

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

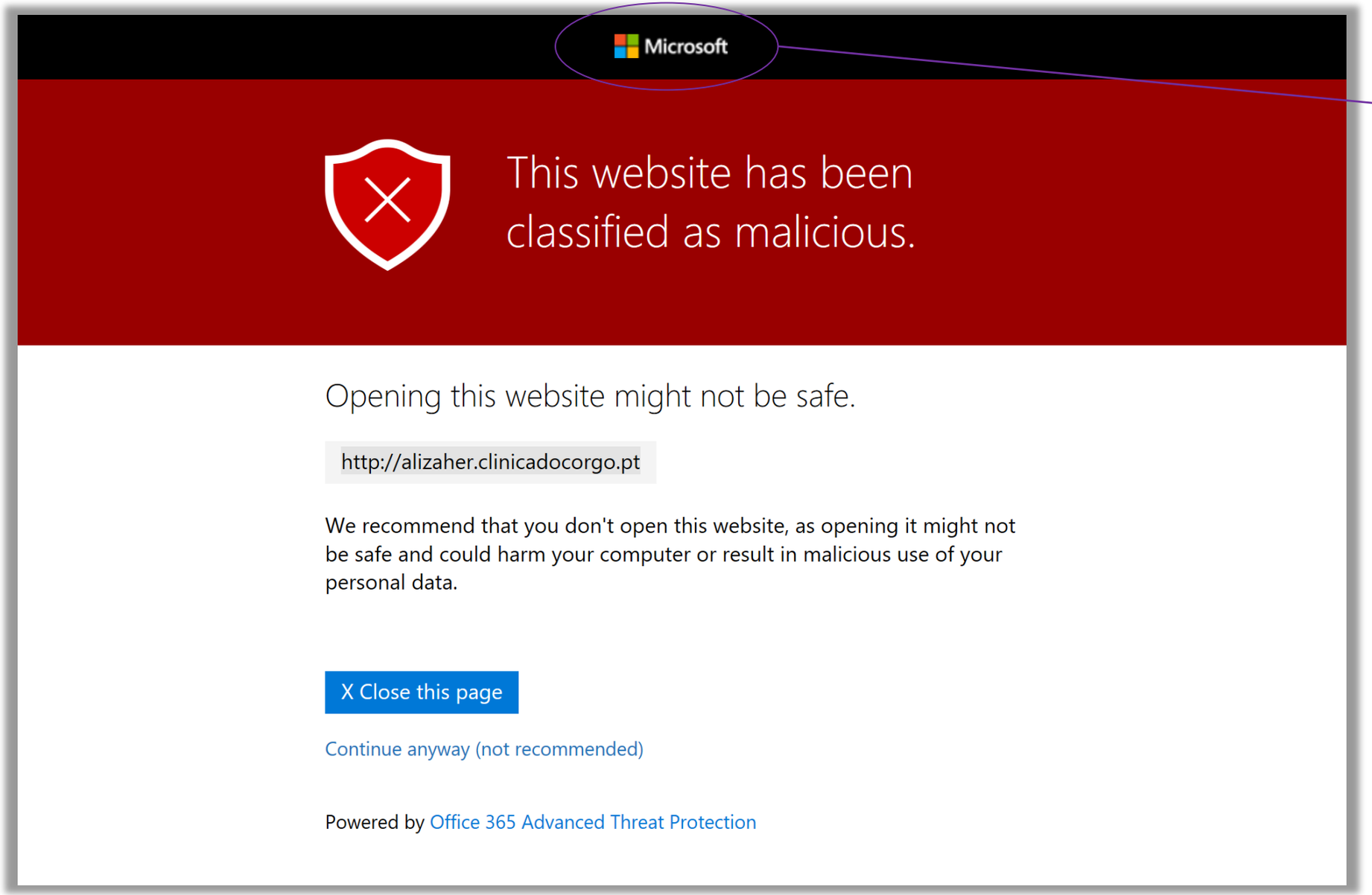


Inside emails, Safe Links rewrite the URL so users will go through our filters first. We try to *keep the original URL on hover* not only for a better end user experience, but we believe that, from a security perspective, the readability of links is very important.



Inside Office documents, Safe Links' protection is integrated into Office.

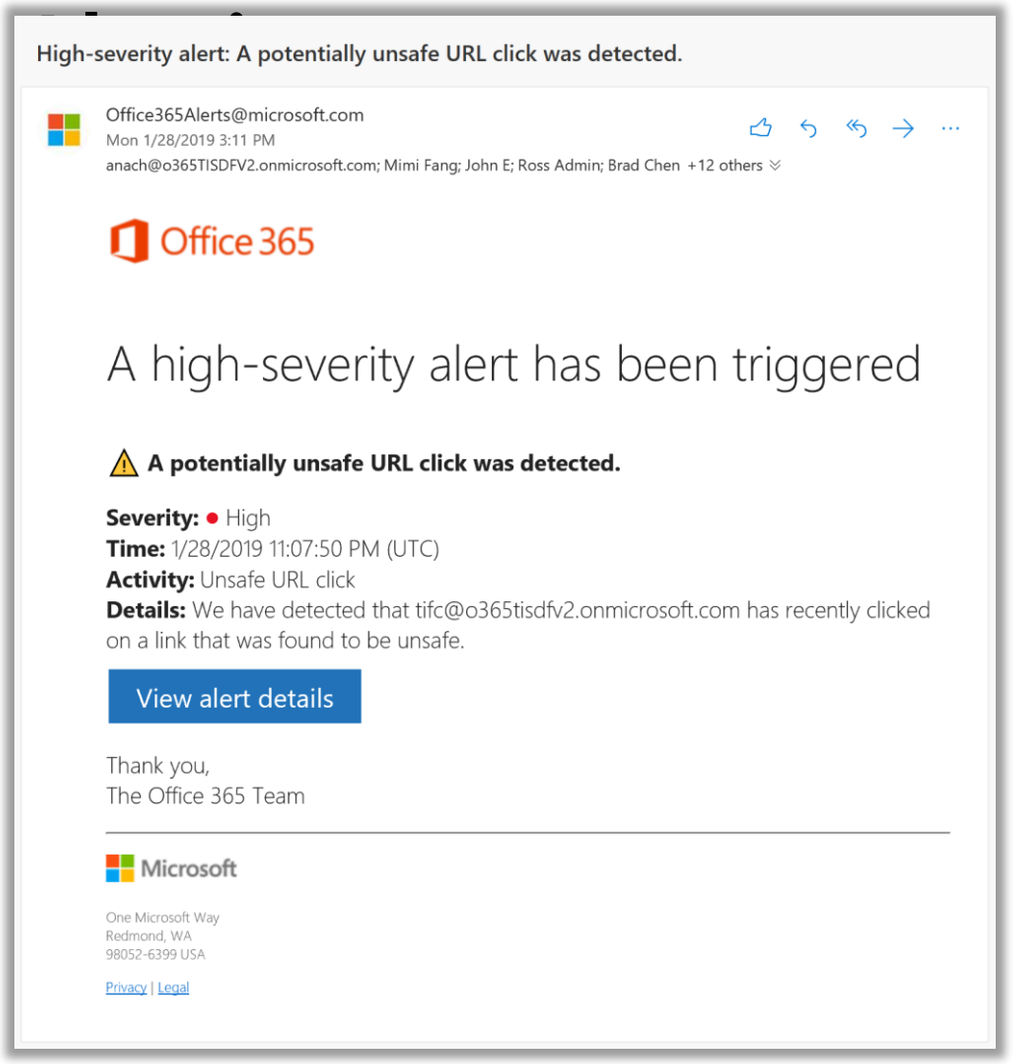
A malicious threat is blocked



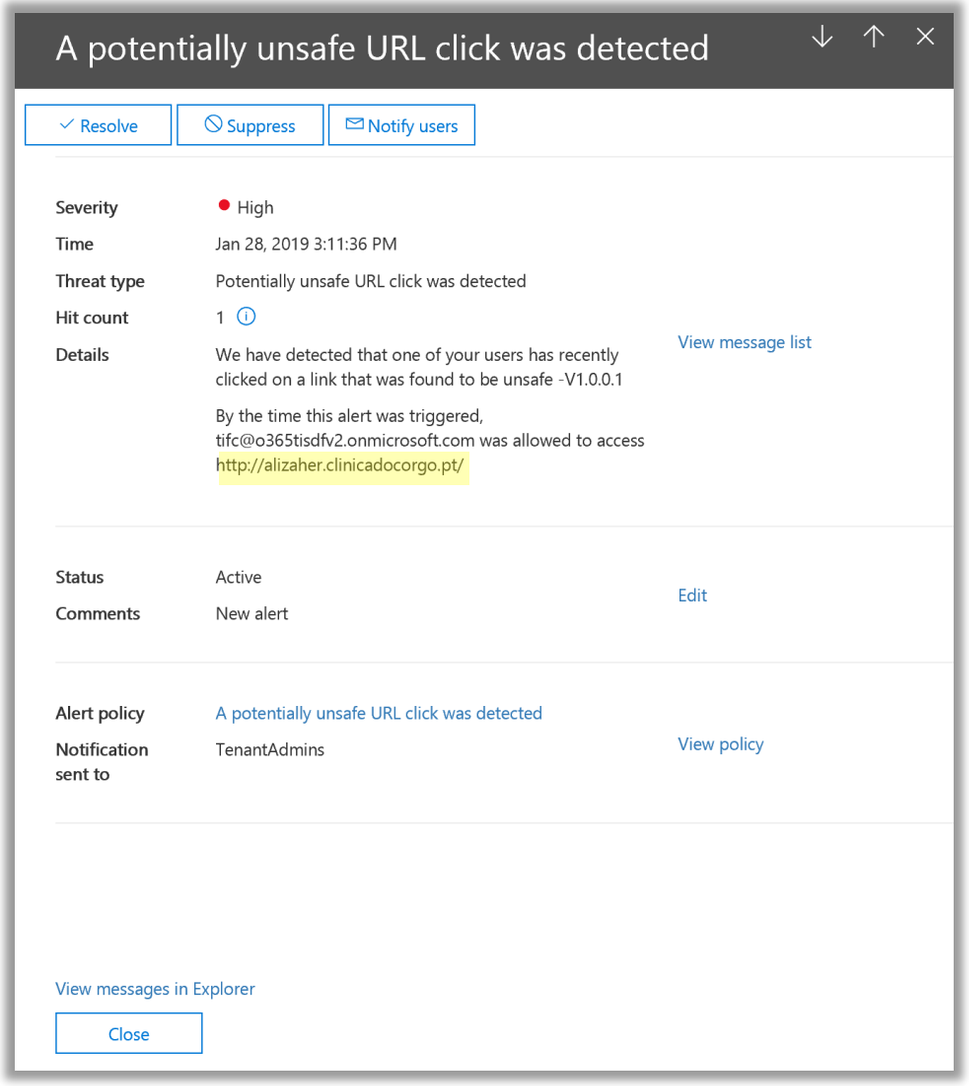
Customized branding

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

URL



Alert email



Alert details

Defender ATP

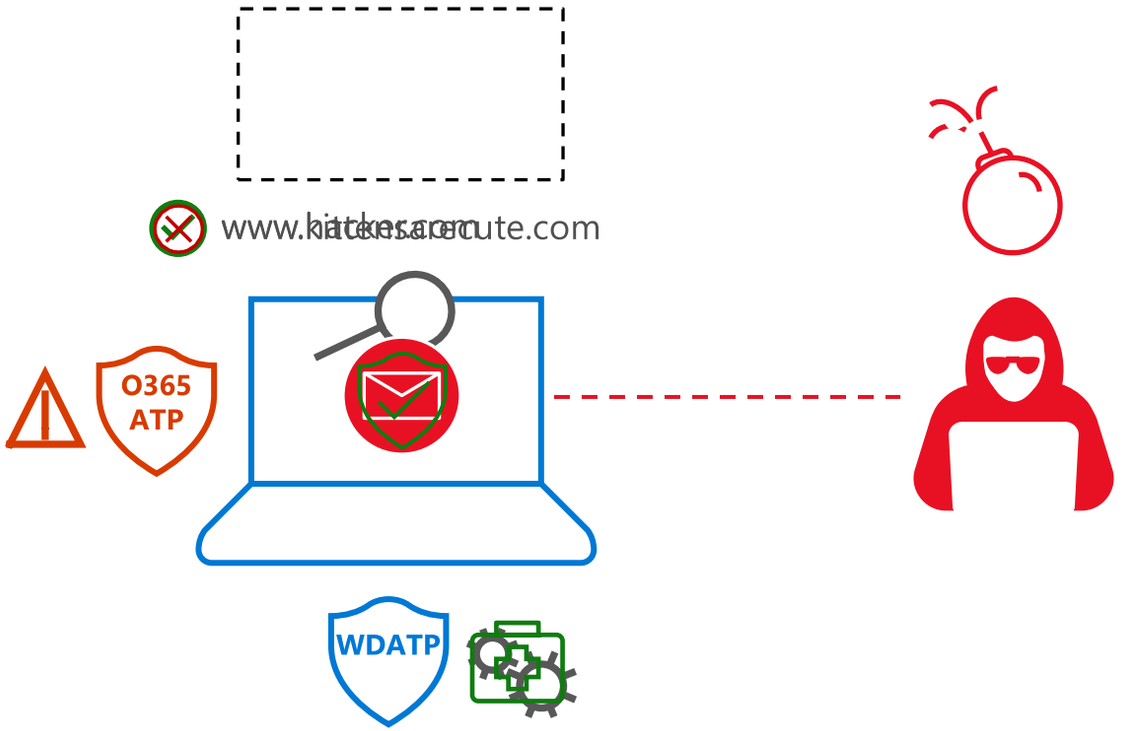
Protect endpoints with Microsoft Defender ATP, which covers licensed users for up to five concurrent devices that can be easily onboarded at any time. Microsoft Defender ATP monitors threats from across platforms, including macOS. Our tech community post includes additional guidance, best practices,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

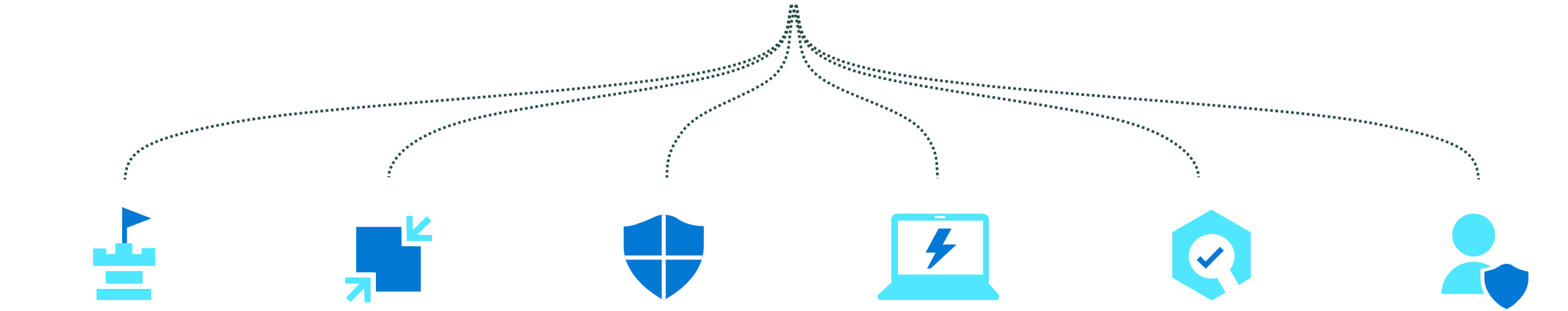
After 24 hours, the attacker “arms” the URL by redirecting to a malicious download which Office ATP detects and quarantines emails

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



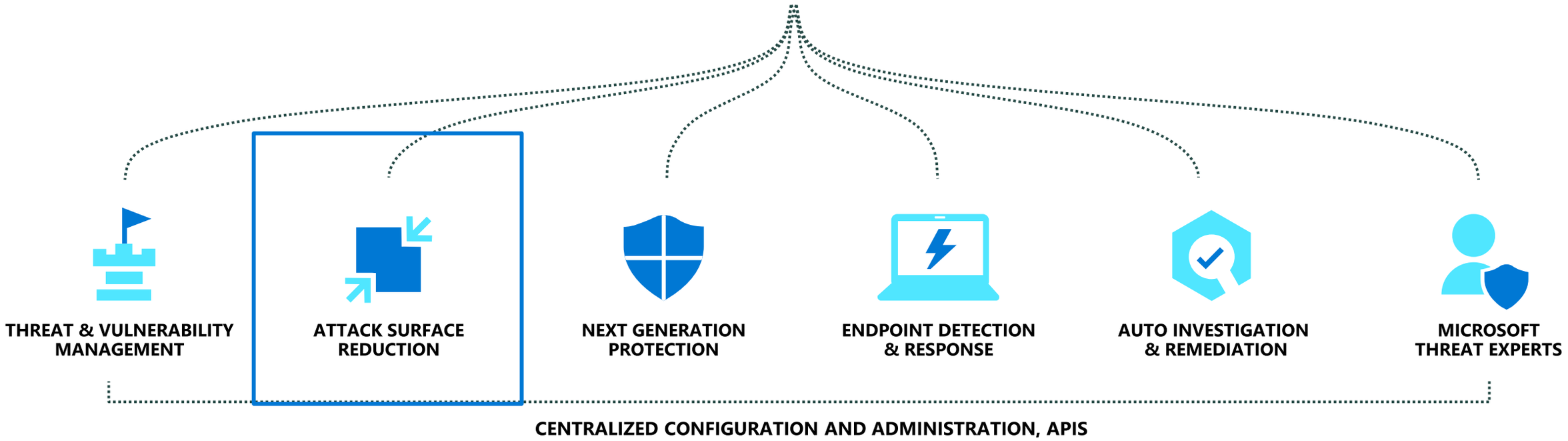
Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.



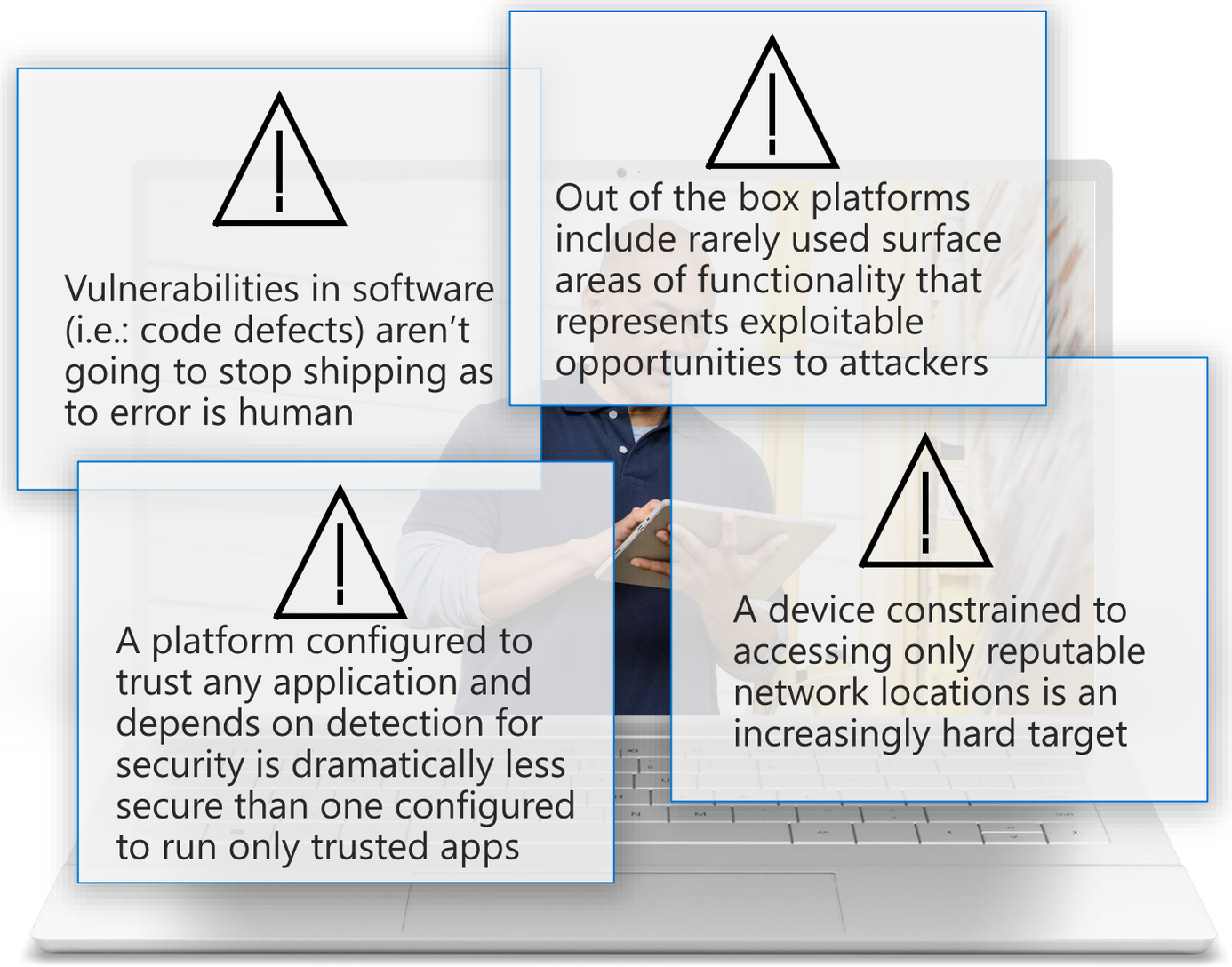
Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.



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

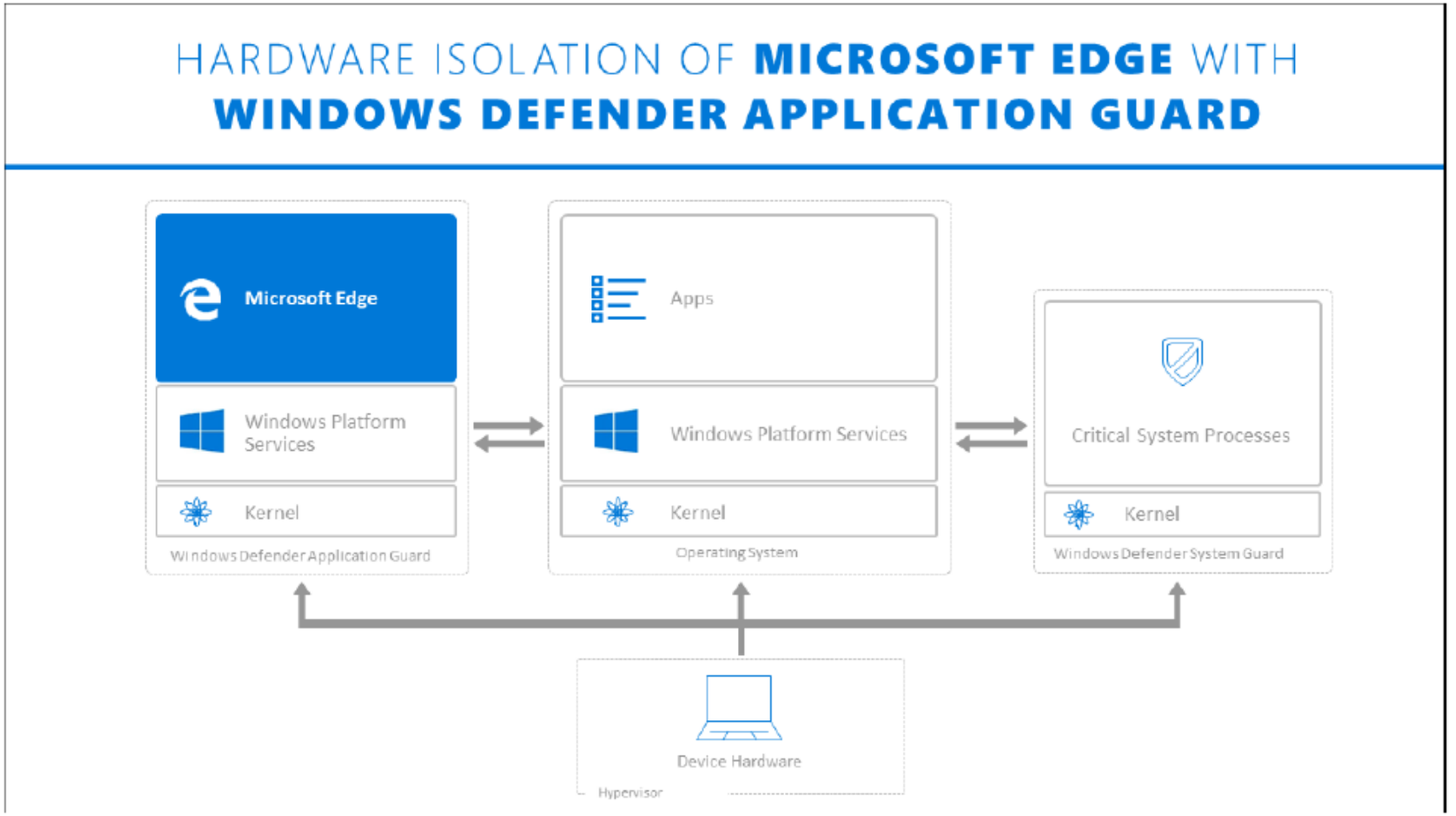
Only allow trusted applications to run

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.

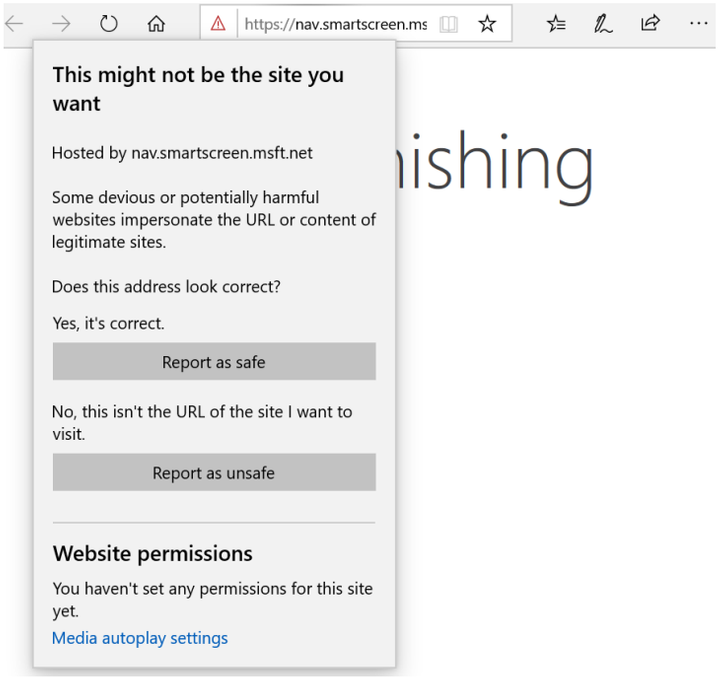
Attack Surface Reduction – Hardware based isolation

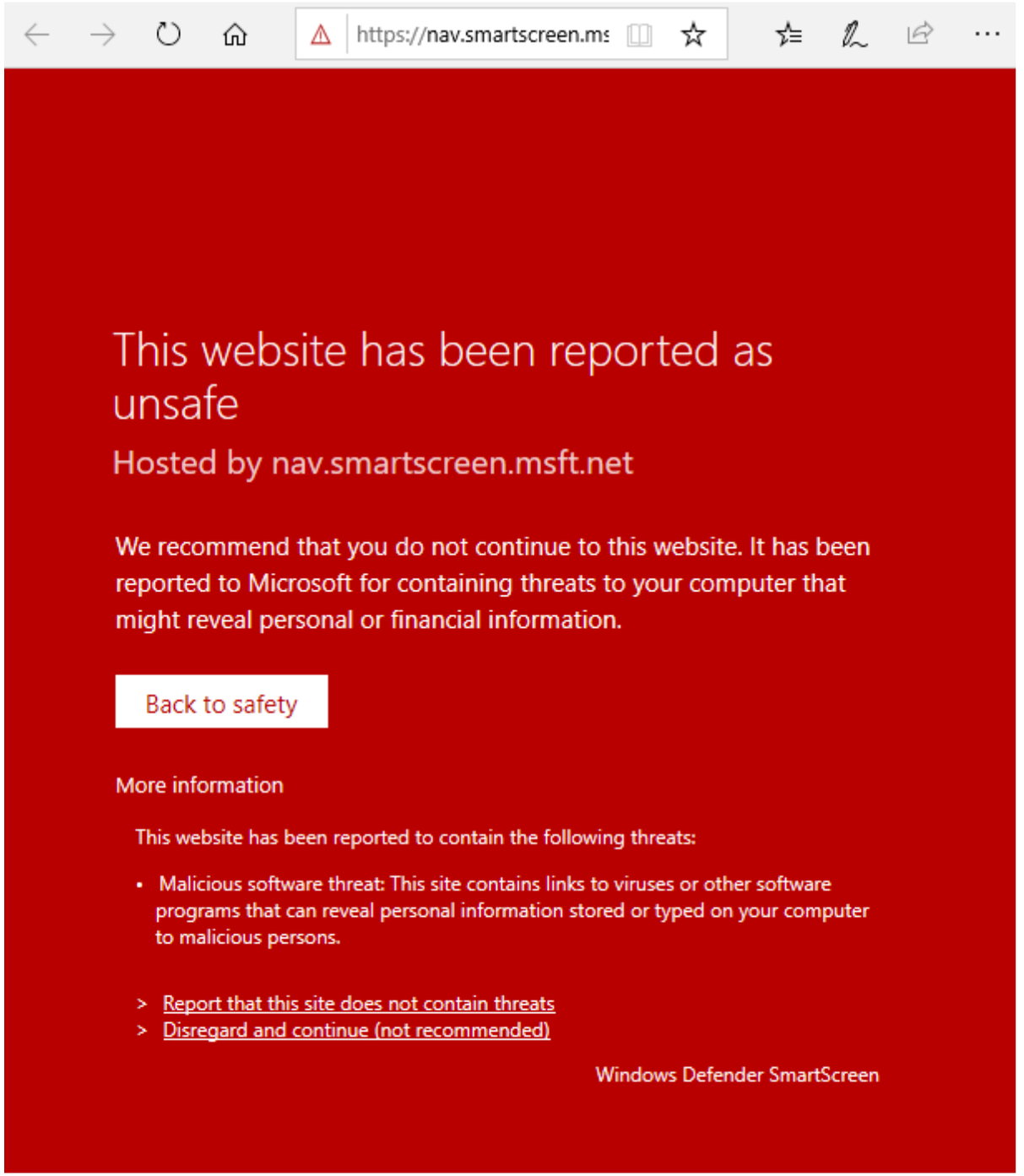
Windows Defender Application Guard

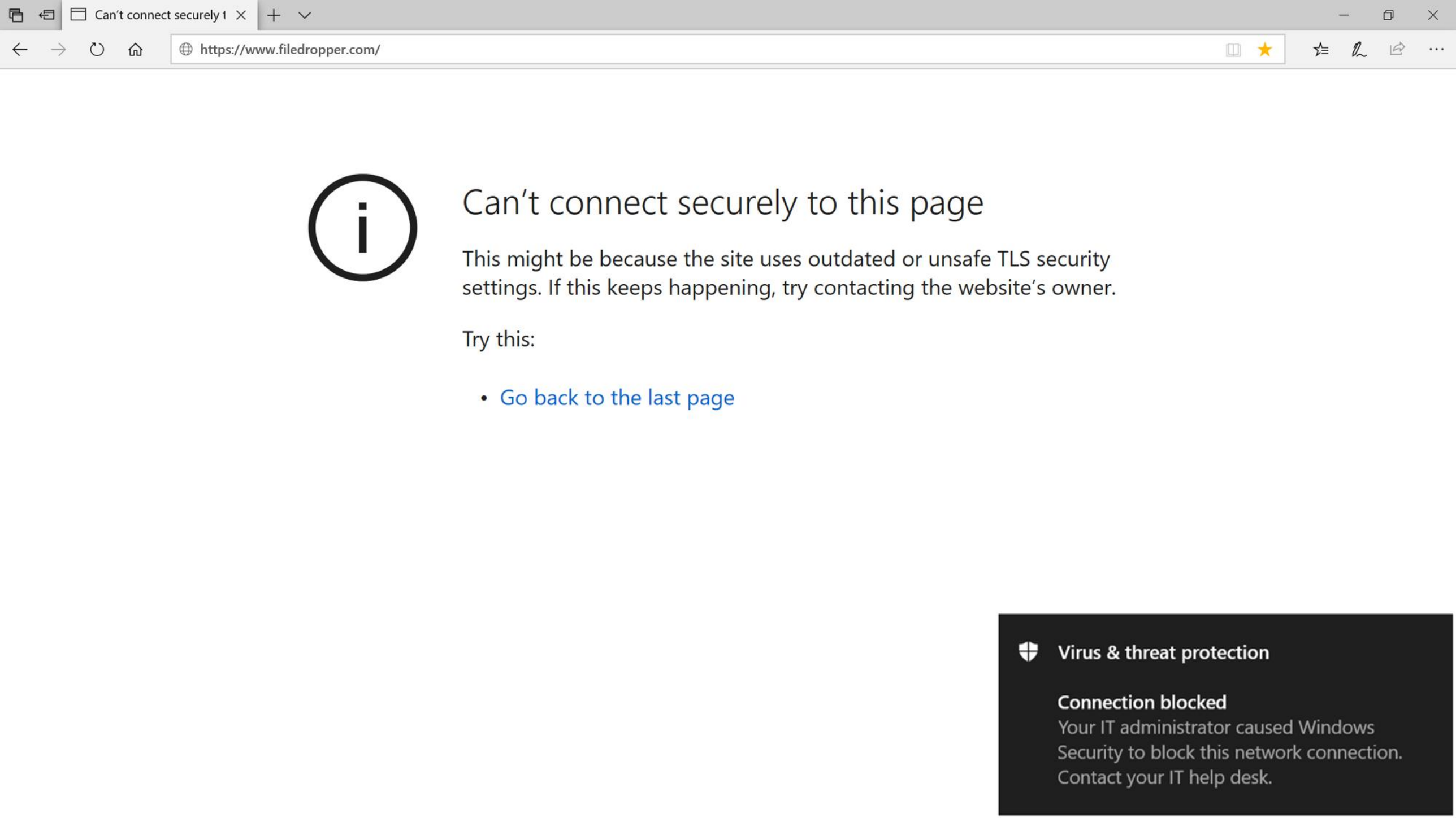


Web Threat Protection

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






Can’t connect securely t
https://www.filedropper.com/
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 t

https://www.gmail.com/

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

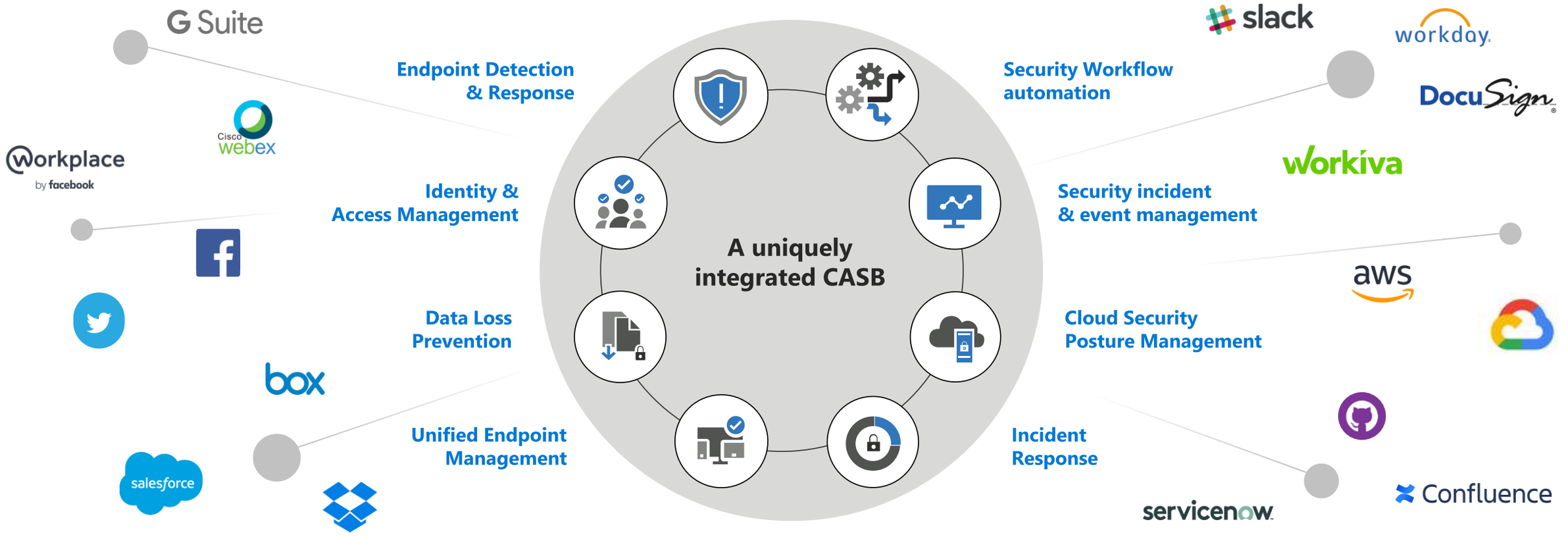
Microsoft Cloud App Security can help protect against shadow IT and unsanctioned app usage, identify and remediate cloud-native attacks, and control how data travels across cloud apps from Microsoft or third-party applications.

Microsoft

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



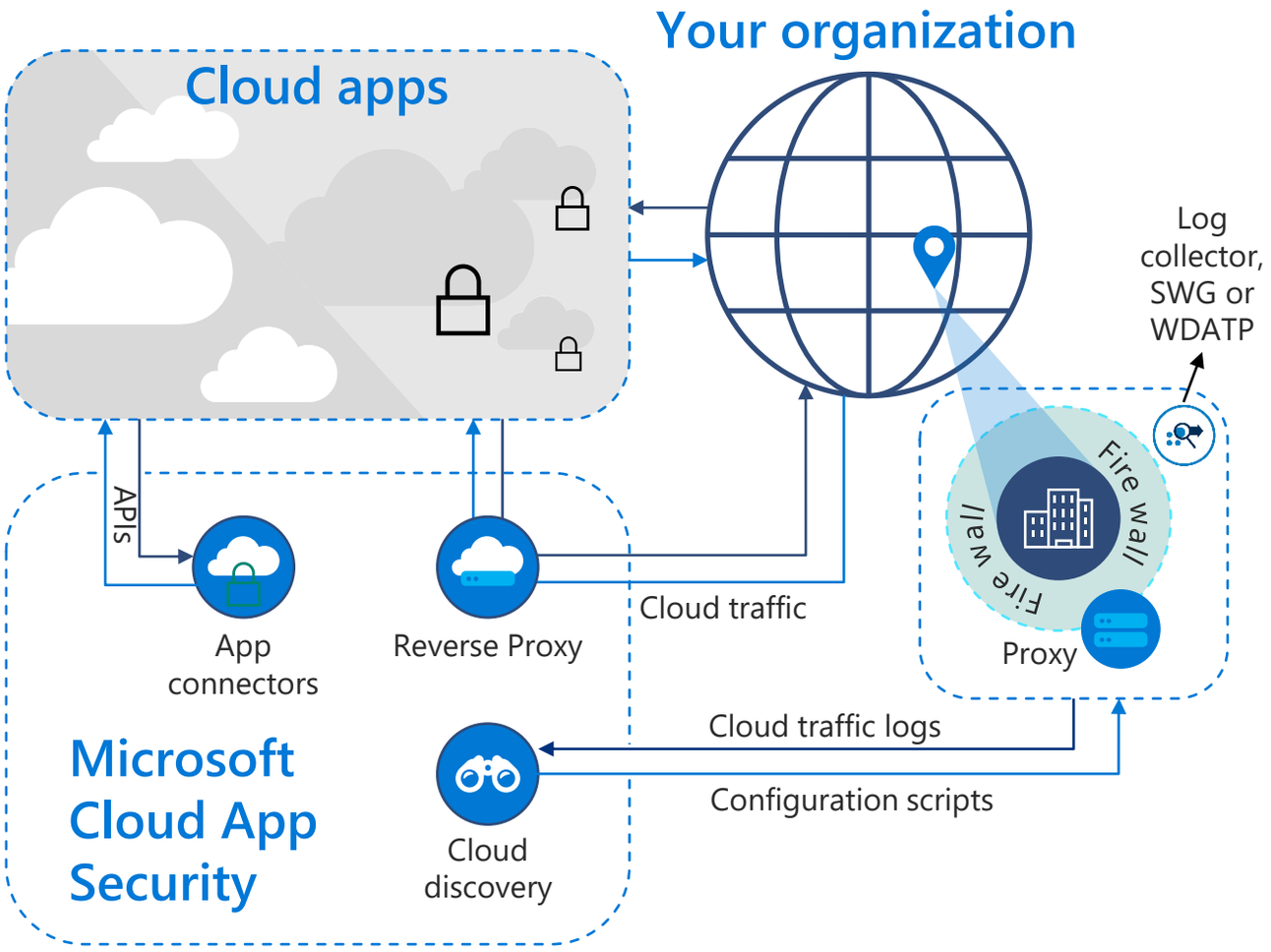
Microsoft Cloud App Security architecture

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

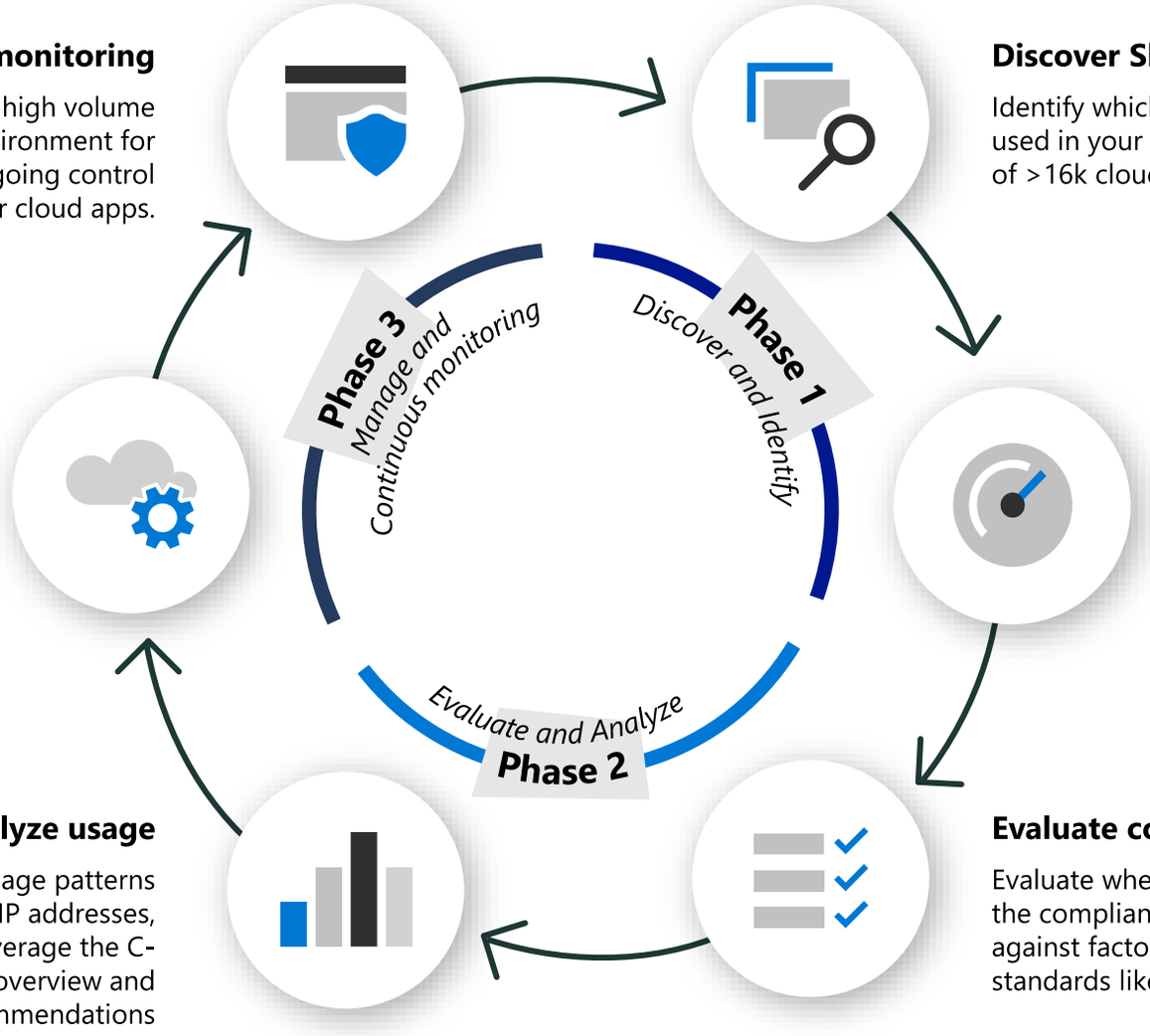
App connectors
Be alerted on user or file behavior anomalies and control the data stored in your cloud apps leveraging our API connectors

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



Discover Shadow IT

Identify which apps are being used in your organization from an app catalog of >16k cloud apps and custom apps.

Identify the risk levels of your apps

Understand the risk associated with discovered apps, based on more than 70 risk factors including, Security factors, industry- and legal regulations – with the ability to customize risk scoring

Evaluate compliance

Evaluate whether the discovered apps meet the compliance standards of your organization against factors like GDPR or industry-relevant standards like HIPAA readiness.

Analyze usage

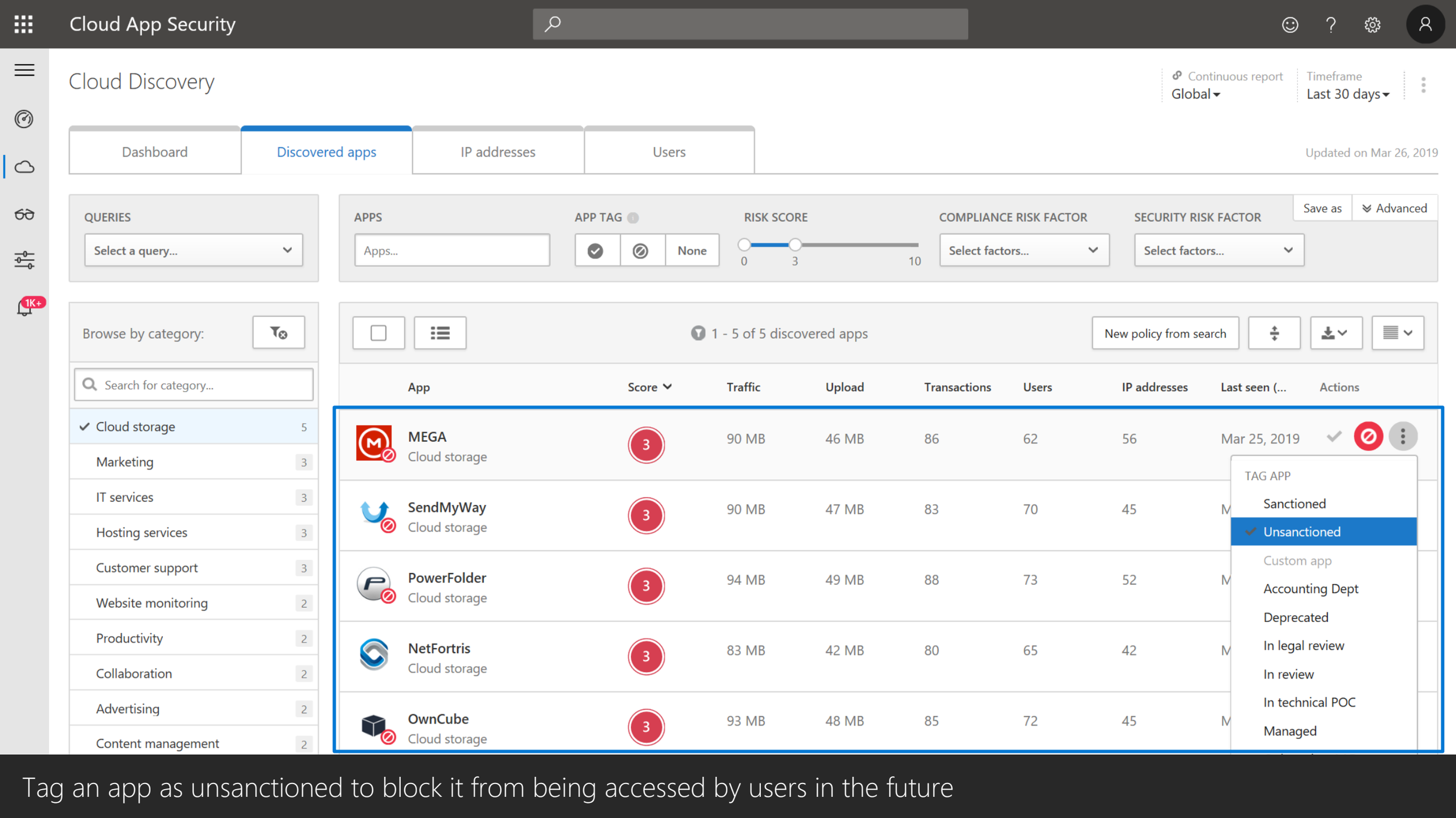
Understand the usage patterns based on traffic data, top users and IP addresses, app categories and machines. Leverage the C-level report for a high level overview and recommendations

Govern your cloud apps

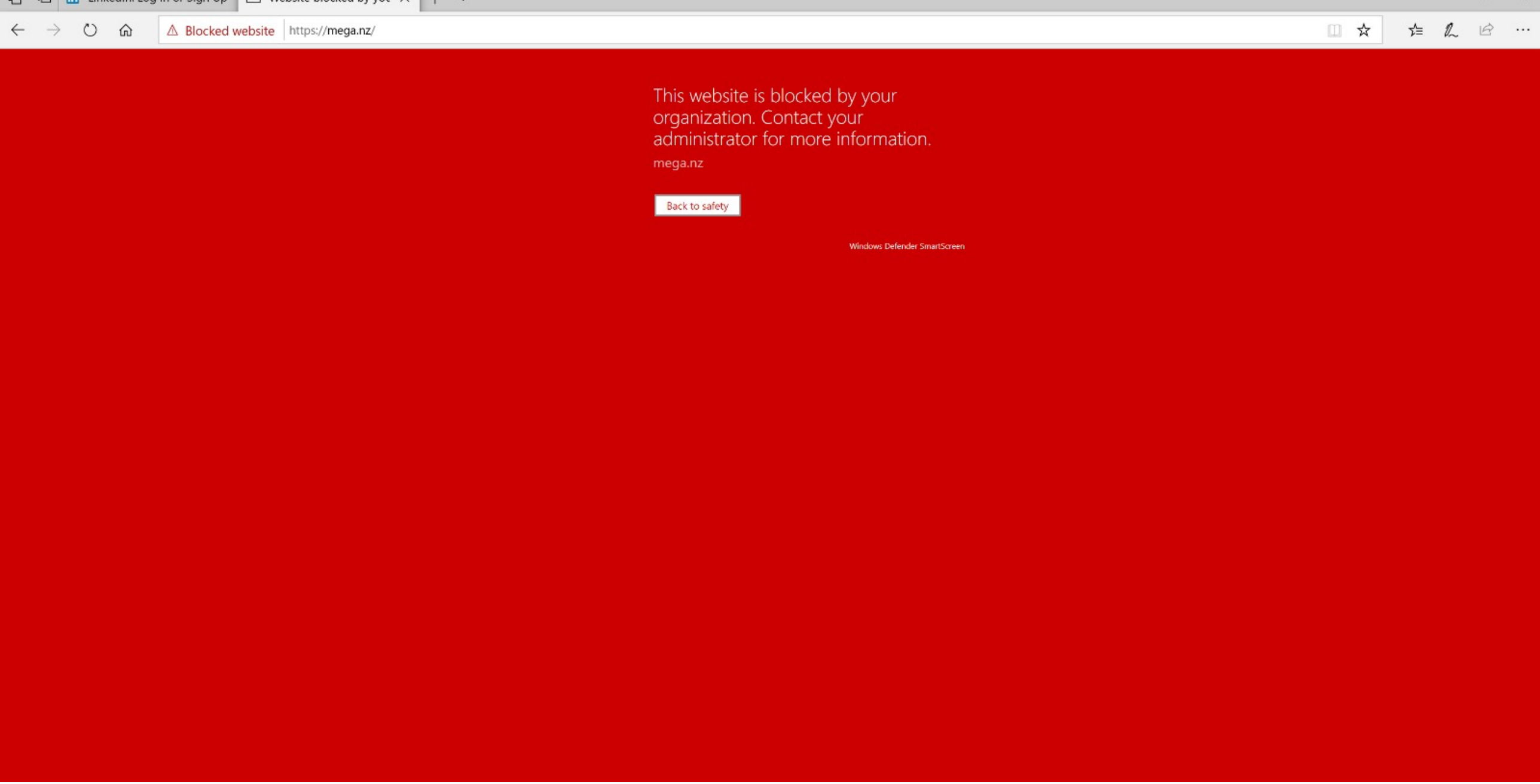
Start managing cloud apps and leverage one of several governance actions such as Sanction, Unsanction, onboarding an app to AAD to leverage SSO, marking them for review or blocking them from your network.

Continuous monitoring

Be alerted when new, risky or high volume apps are discovered in your environment for continuous monitoring and ongoing control over your cloud apps.



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



Endpoint based control over access to risky and non compliant apps via MDATP

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

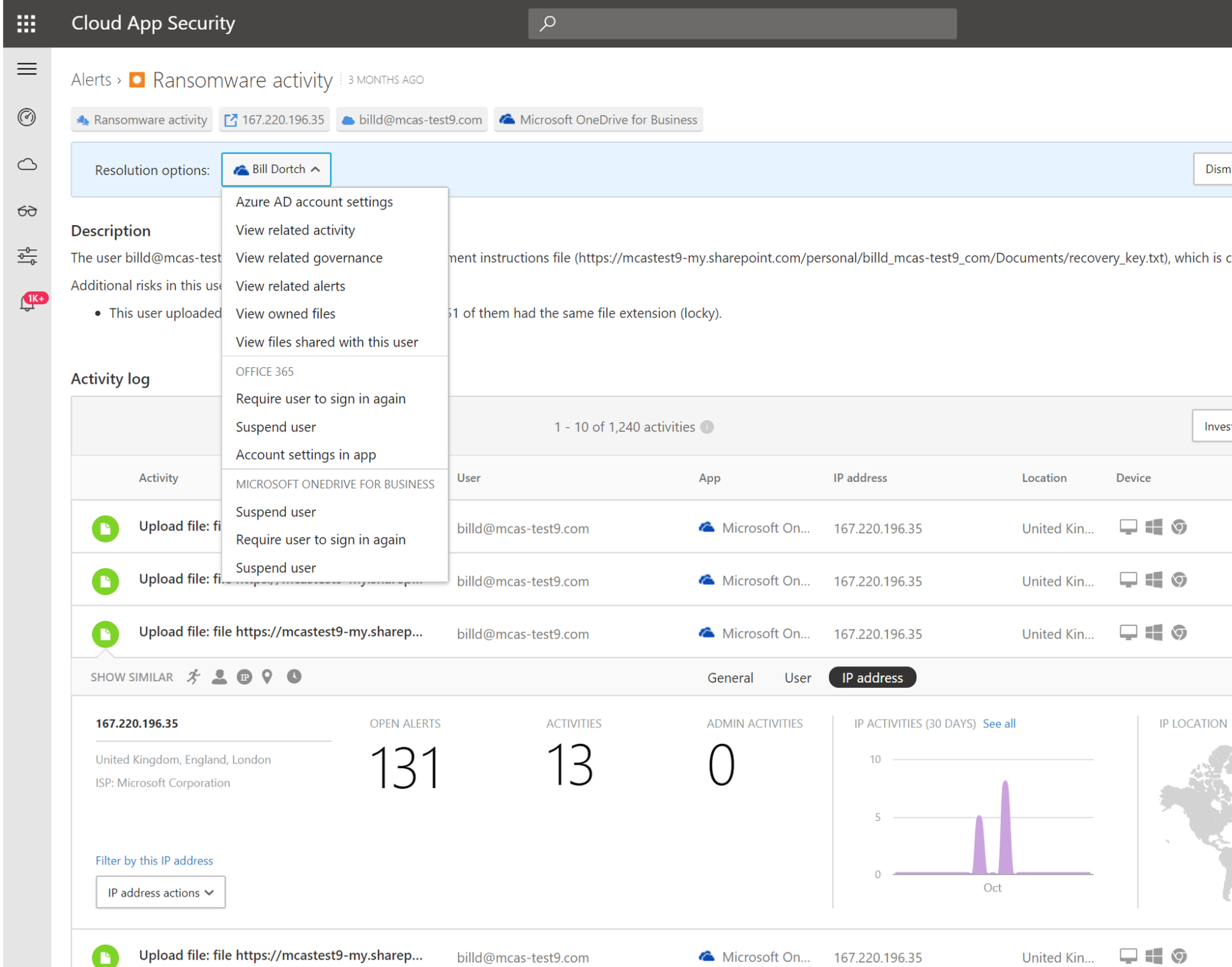
- Govern data in the cloud with granular DLP policies
- Leverage Microsoft's IP capabilities for classification
- Extend on-prem DLP solutions
- Automatically protect and encrypt your data using Azure Information Protection

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**

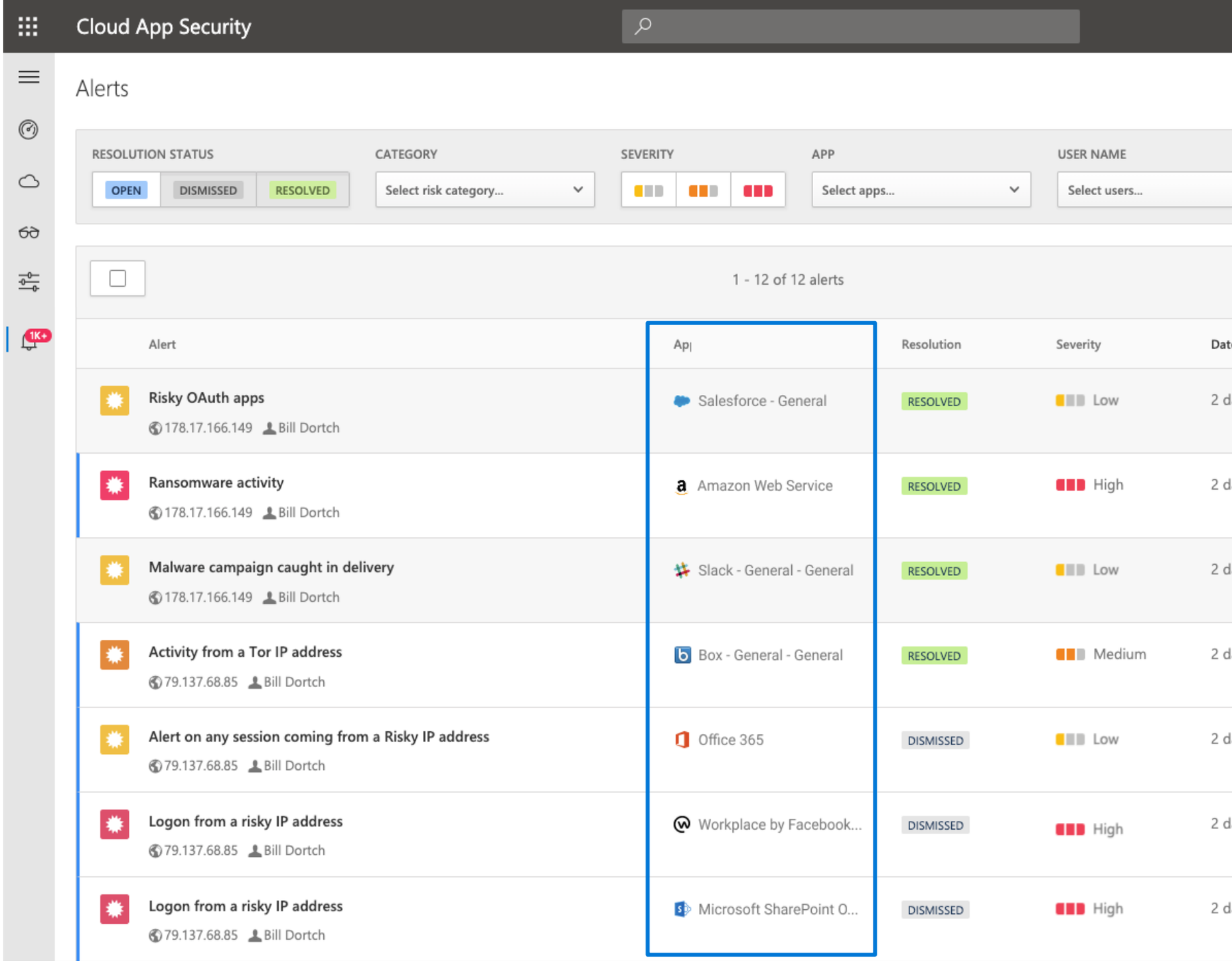


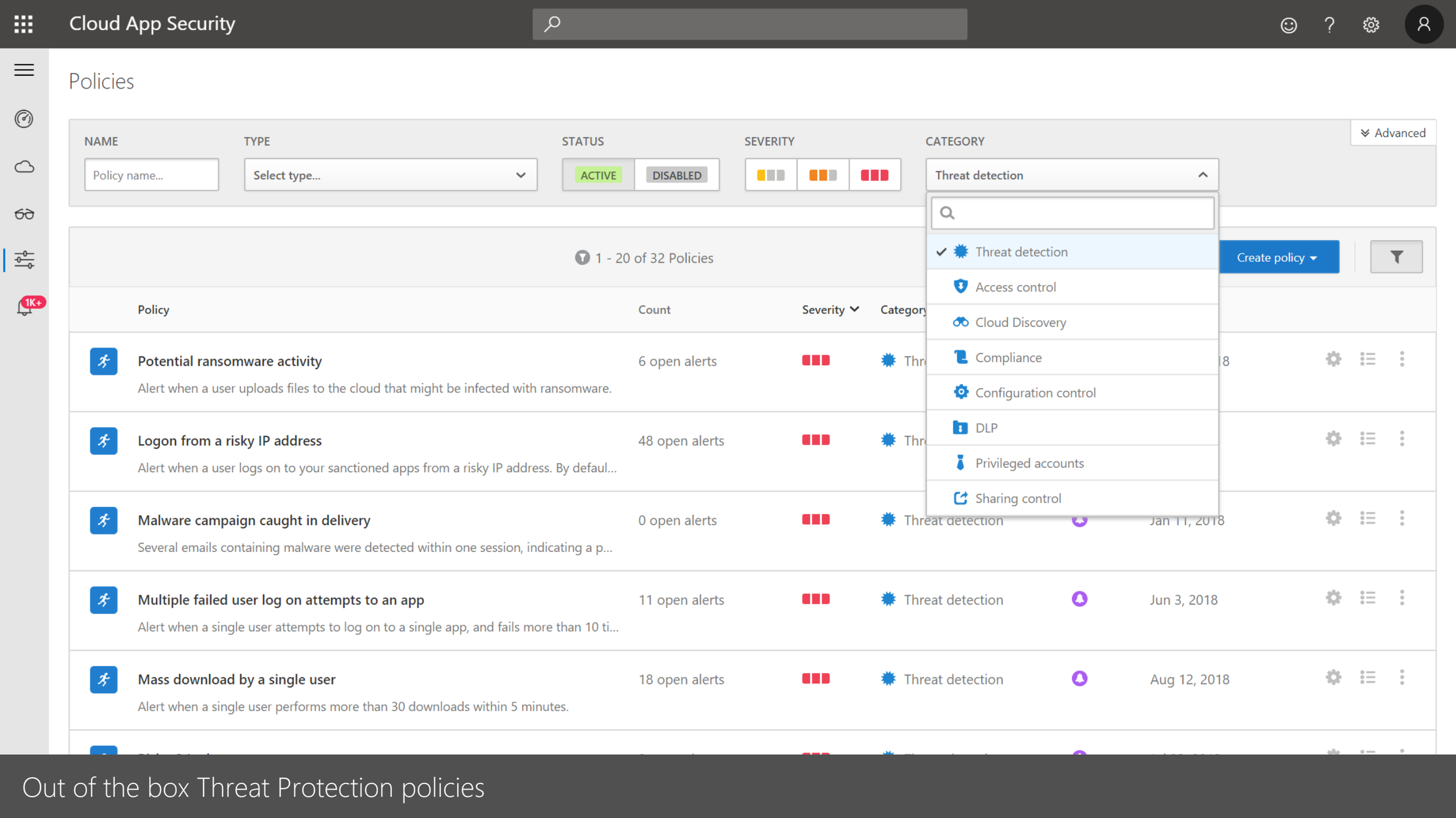
Comprehensive Threat Protection for your cloud apps

- **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

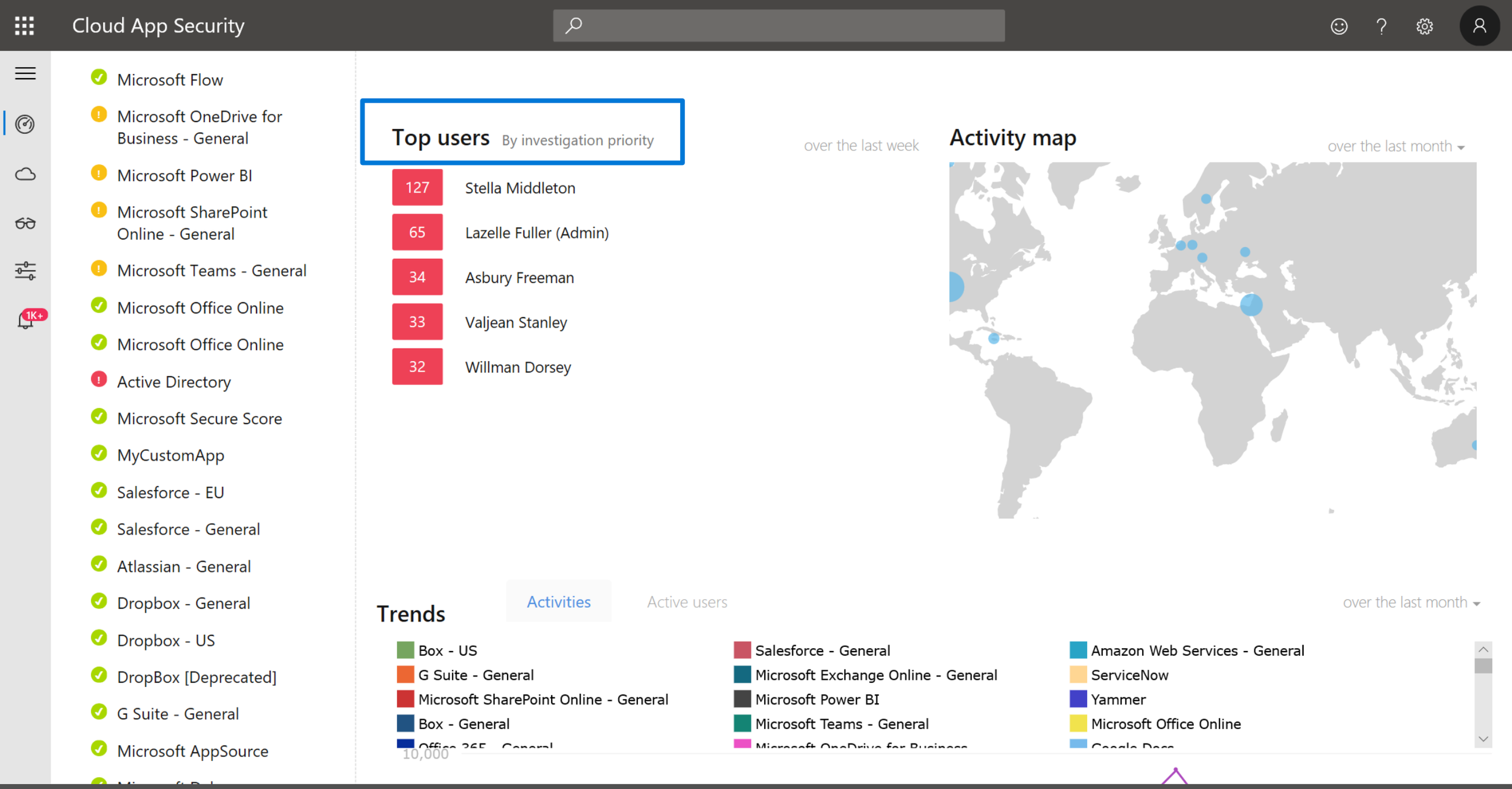
- **Malware Detonation**
- Intelligent heuristics identify potentially malicious files and detonate them in a sandbox environment - for existing and newly uploaded files

- **Customize policies to alert and remediate**
- Customize what you want to be alerted on to minimize noise and configure automatic remediation

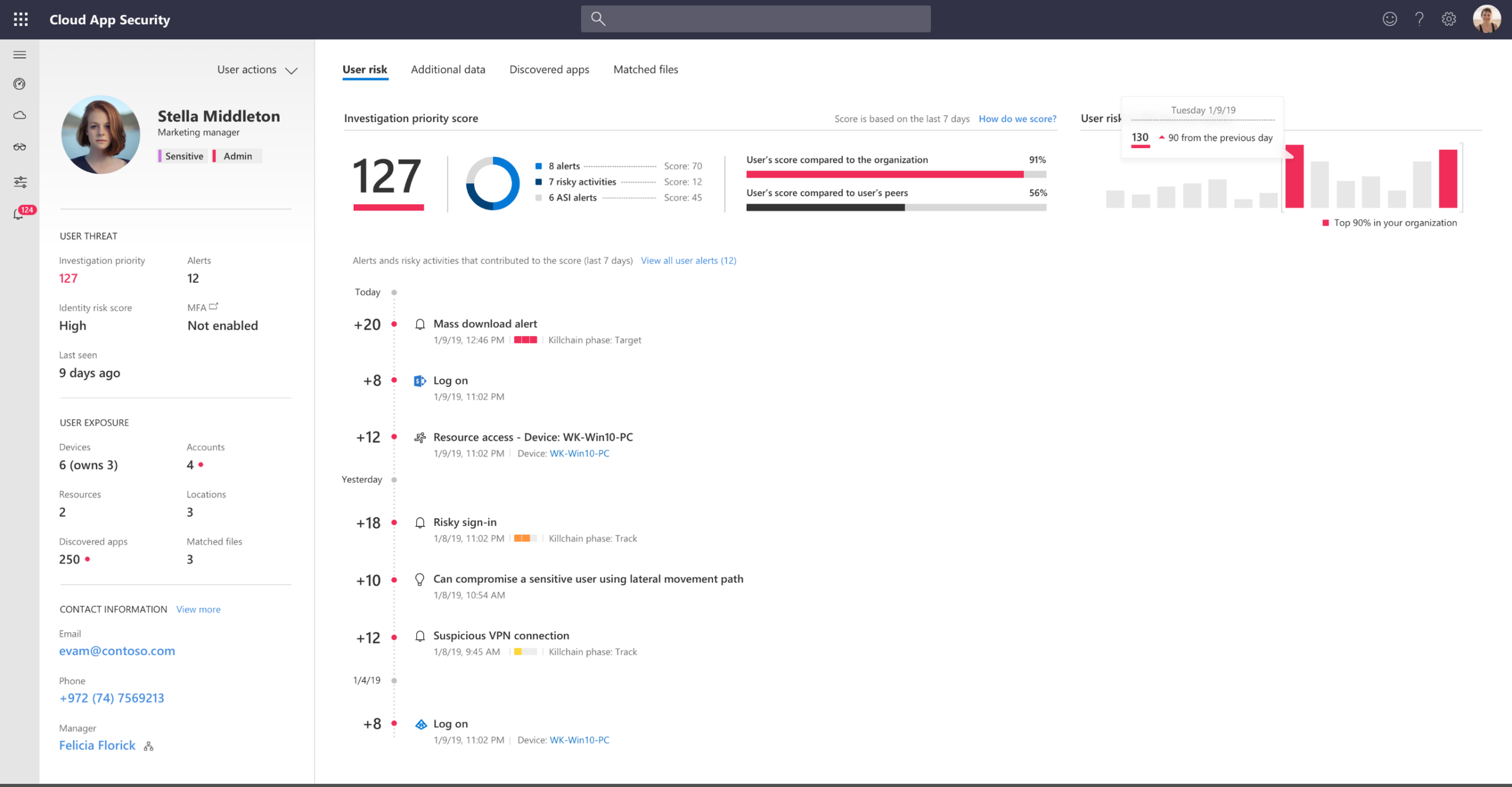




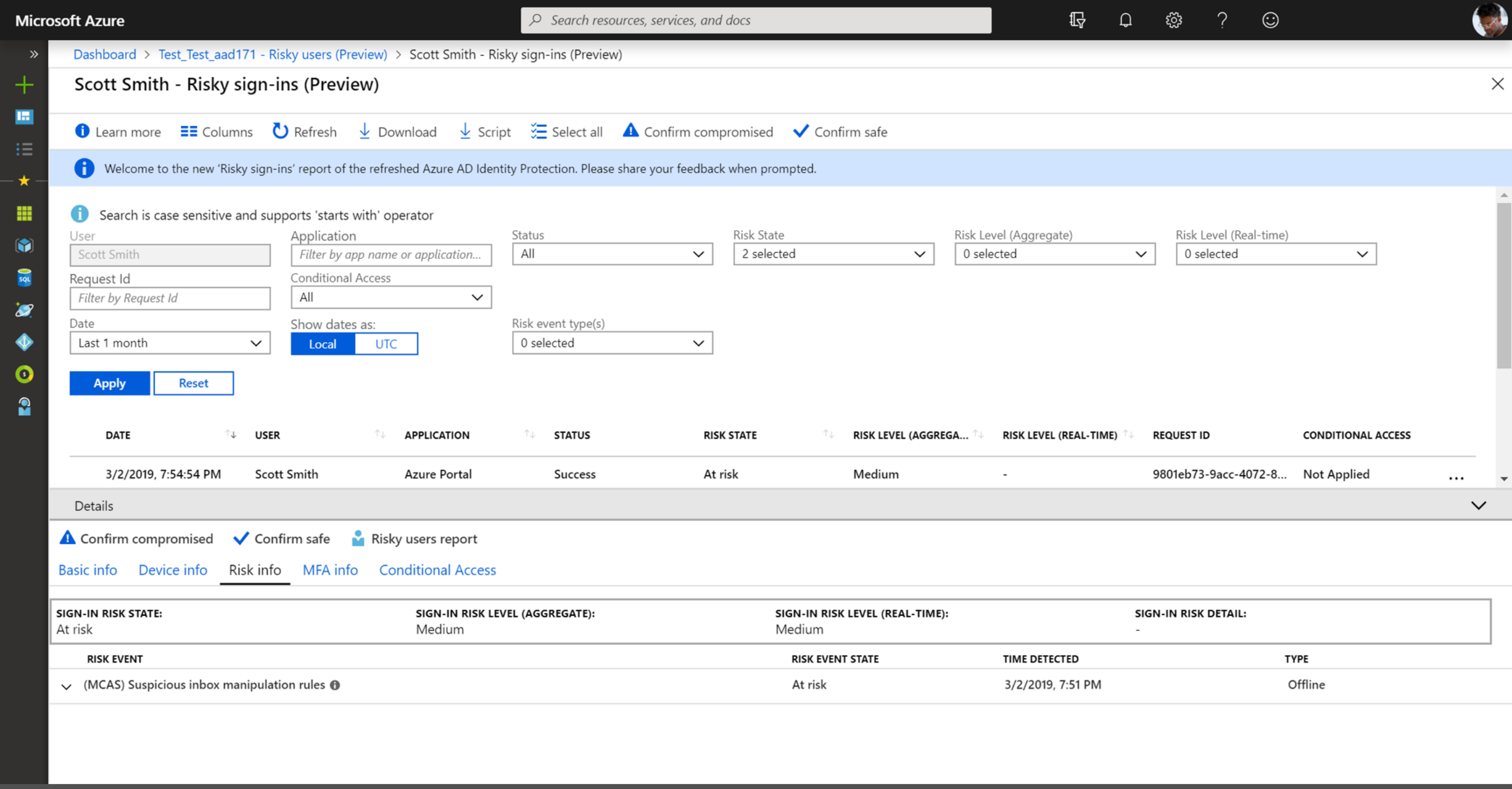
Out of the box Threat Protection policies



Top users by investigation priority on the Cloud App Security Dashboard

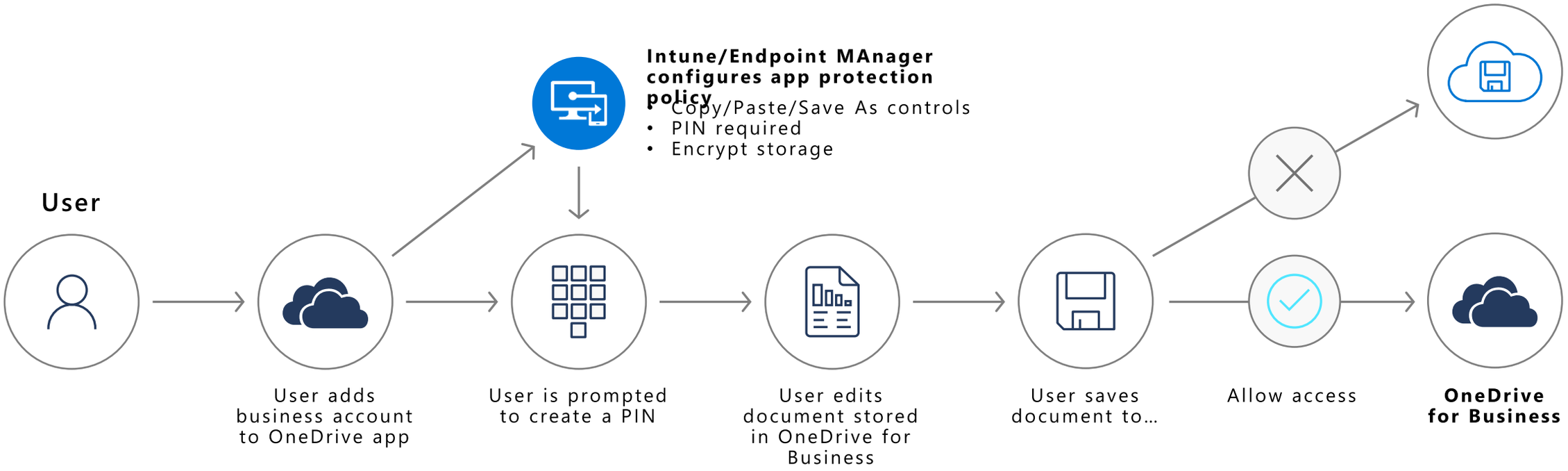


Hybrid UEBA for cloud and on-premise user activity – Investigation Priority



Hybrid UEBA for cloud and on-premise user activity – User Risk Score

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:

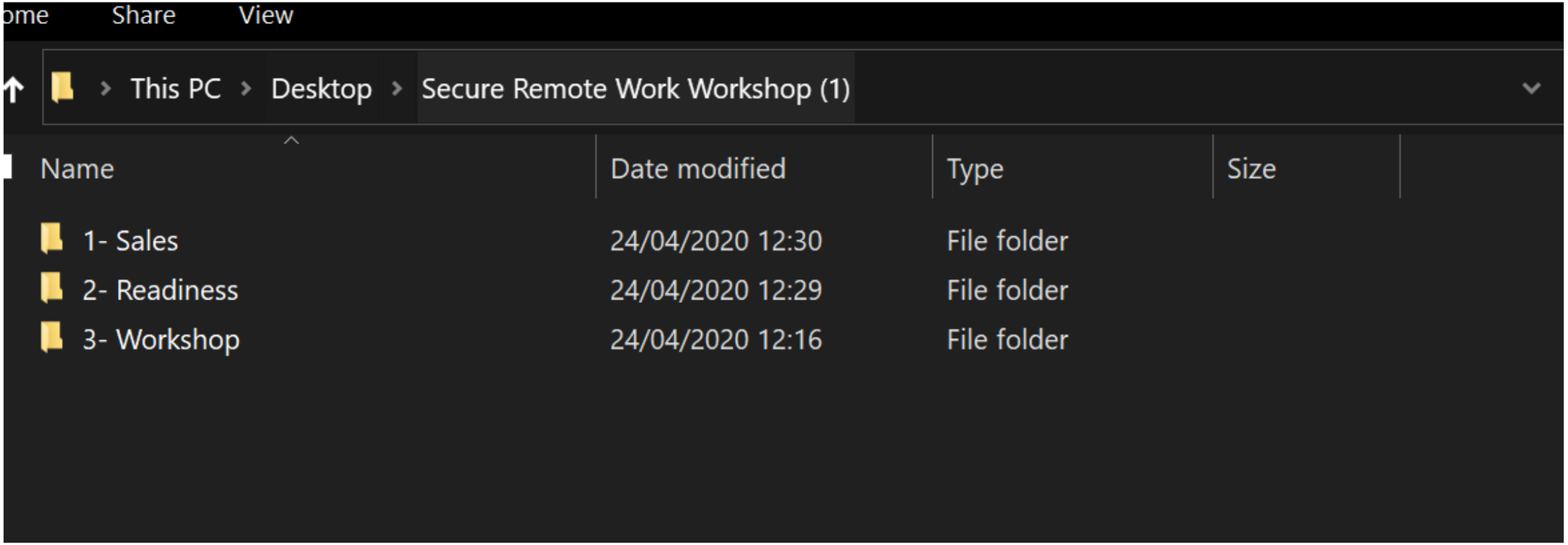
Enable Identity - Single Sign on & Self- Service Password Reset

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



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**

https://aka.ms/WE-TechOfficeHours-Materials

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

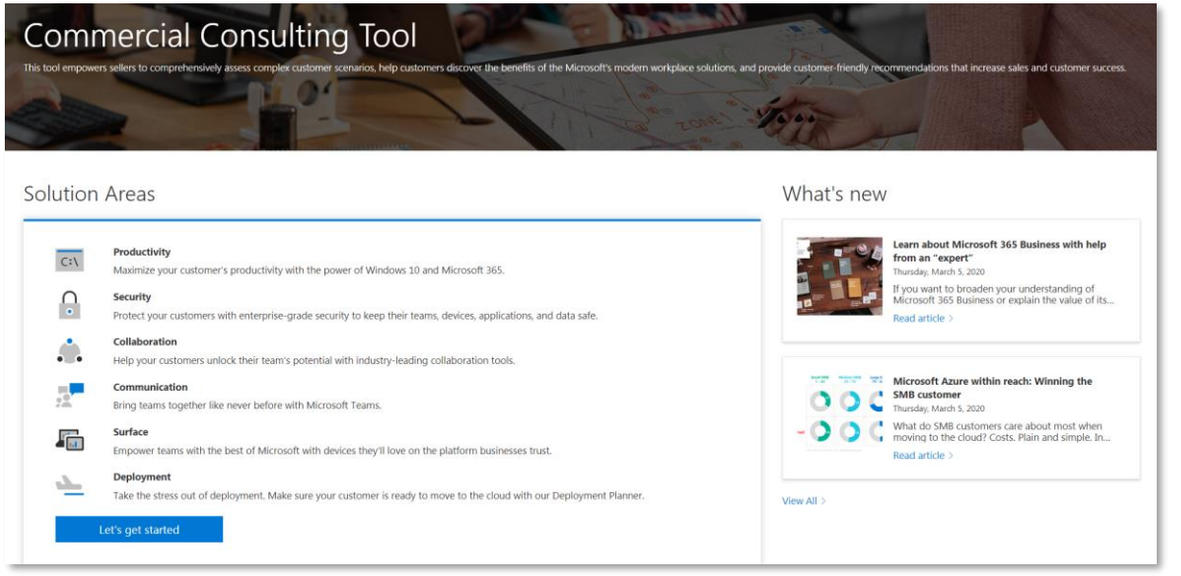
Develop joint deployment plan, including and timelines and next actions.

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



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

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

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

Microsoft

Thank You!