

How to fight phishing and optimise your Office 365 security



Paul Rouse

Senior Mobility & Security Consultant

paul.rouse@kocho.co.uk



Straw Poll



How many of you are using just Exchange Online Protection (EOP)?



How many of you are using a 3rd party email protection product today?



How many of you are using Microsoft Defender for Office 365 today?

The challenge of securing your environment



Current threat landscape



91%

Cyberattacks that start with email¹

30,720

Domains generated by criminals every three days²



\$1.8B

Loss attributed to business email compromise in 2020 alone³

168K

Phishing sites taken down by Microsoft in 2021²



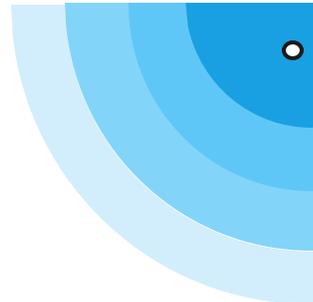
¹Verizon Data Breach Investigations Report | ²Microsoft 2021 Digital Defense Report [Learn More](#) | ³US Federal Bureau of Investigation, March 2021

Why do customers choose Microsoft?

Industry-leading email security

Forrester named
Microsoft a **Leader**
in 2021 Enterprise Email
Security Wave¹

FORRESTER®



SecOps efficiency and cost savings

Total Economic Impact study of moving from a
competitor to Defender for Office 365²

Improved blocking
of malicious links by

95%



Improved
investigation time by

92%



Reduced risk
of breach by

29%



¹The Forrester Wave™: Enterprise Email Security, Q2 2021, Joseph Blankenship, May 6, 2021. [Learn more](#)

²The Total Economic Impact™ Of Microsoft Defender For Office 365. [Learn more](#)

Why do customers choose Microsoft?

June 22, 2022 • 2 min read

Microsoft Defender for Office 365 receives highest award in SE Labs Enterprise Email Security Services test

Giulian Garruba Product Marketing Manager, Microsoft Defender for Office 365



Share ▾

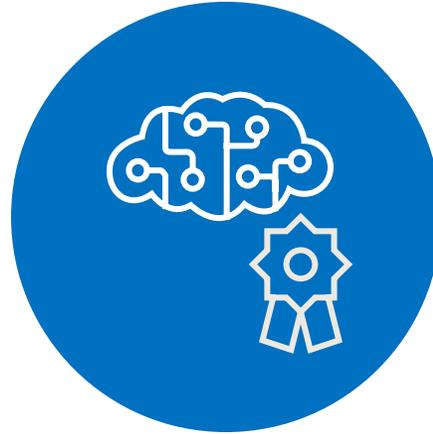


Why Microsoft?

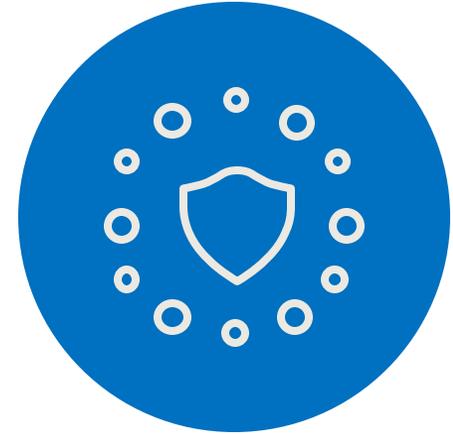
Our unique advantages.



Native protection
for Office 365



Industry-leading AI
and automation

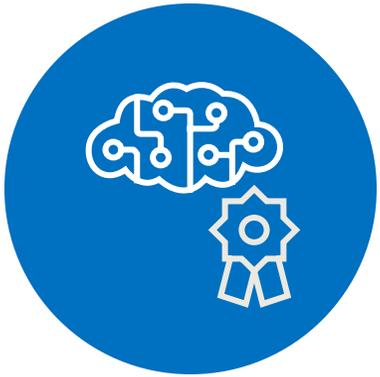


Comprehensive
approach

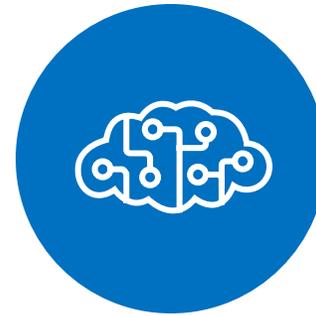


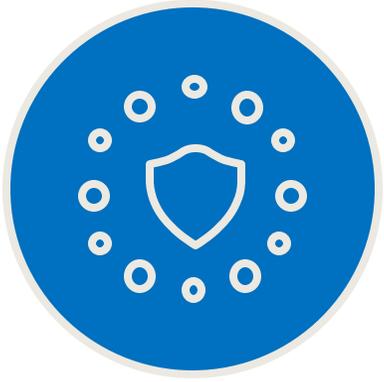
Native protection for Office 365





Industry-leading
AI and automation





Comprehensive approach



Microsoft 365 Defender

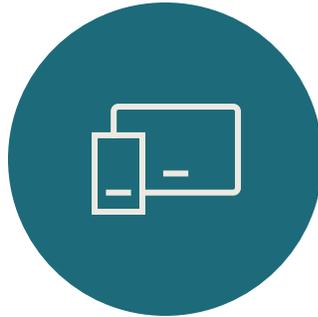


Automated cross-domain XDR security



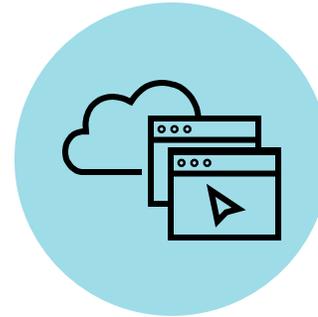
Identities

Microsoft Defender
for Identity



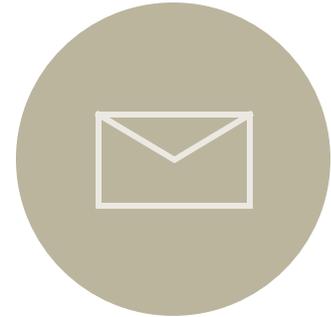
Endpoints

Microsoft Defender
for Endpoint



Cloud Apps

Microsoft Defender
for Cloud Apps



Email & collaboration

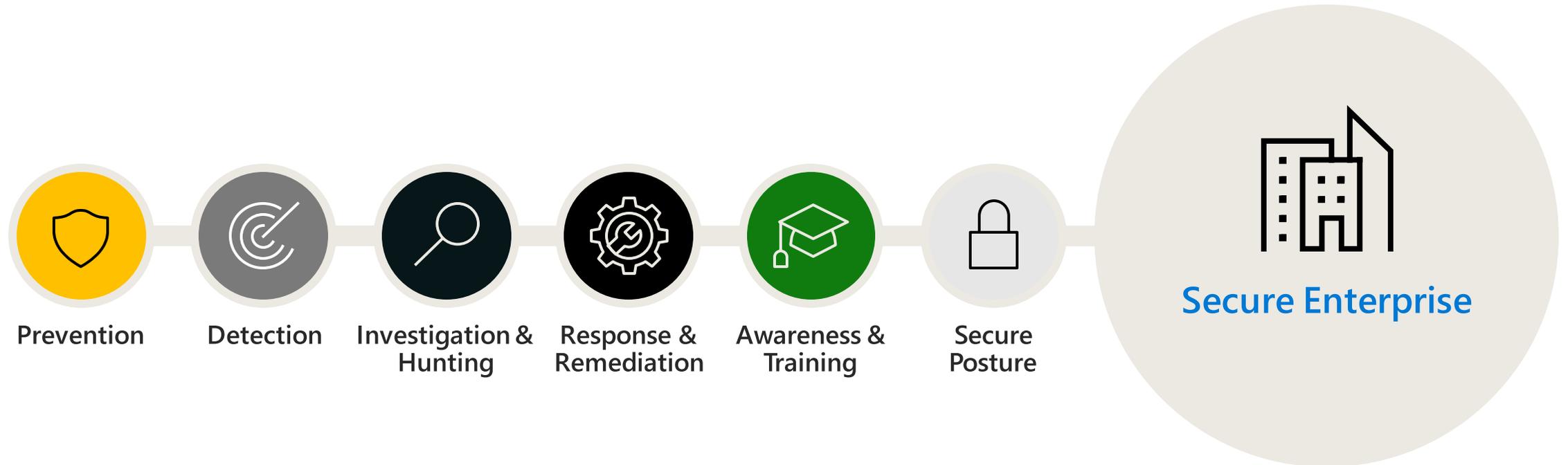
Microsoft Defender
for Office 365

SIEM

Microsoft Sentinel

Microsoft Defender for Office 365

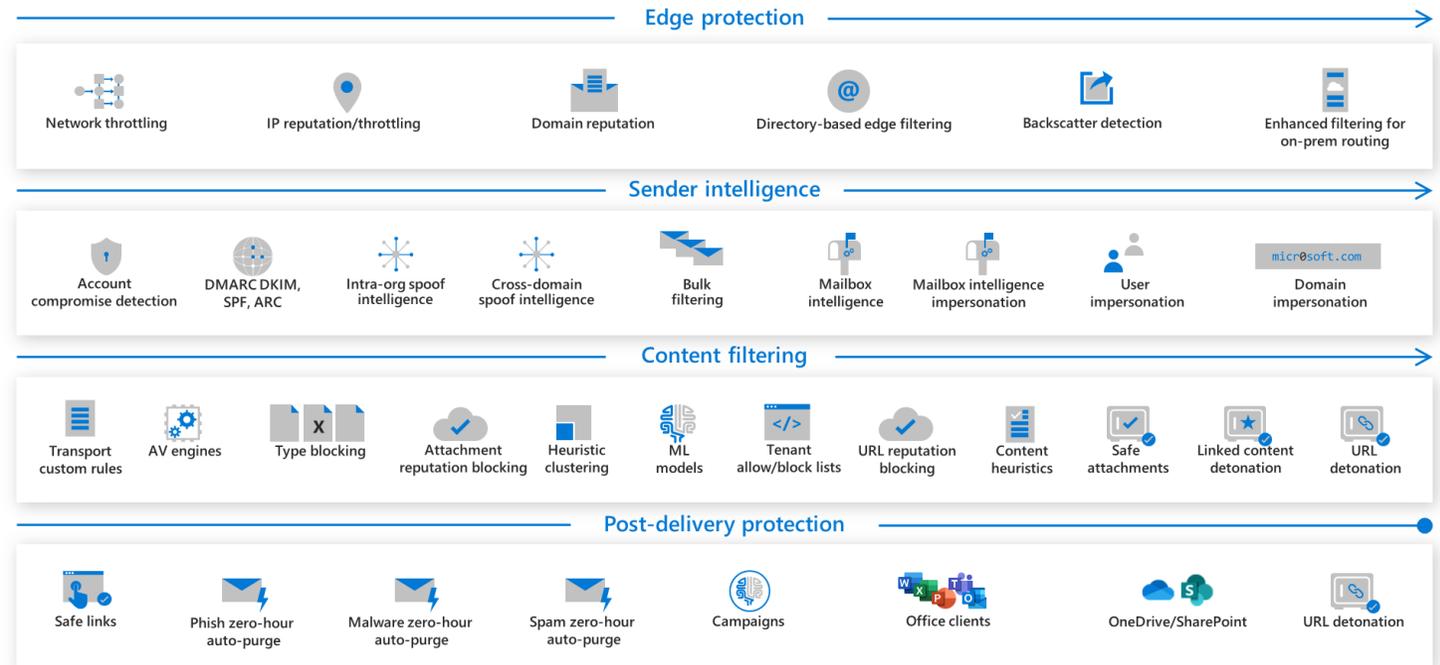
Securing your enterprise requires more than just prevention



Prevention

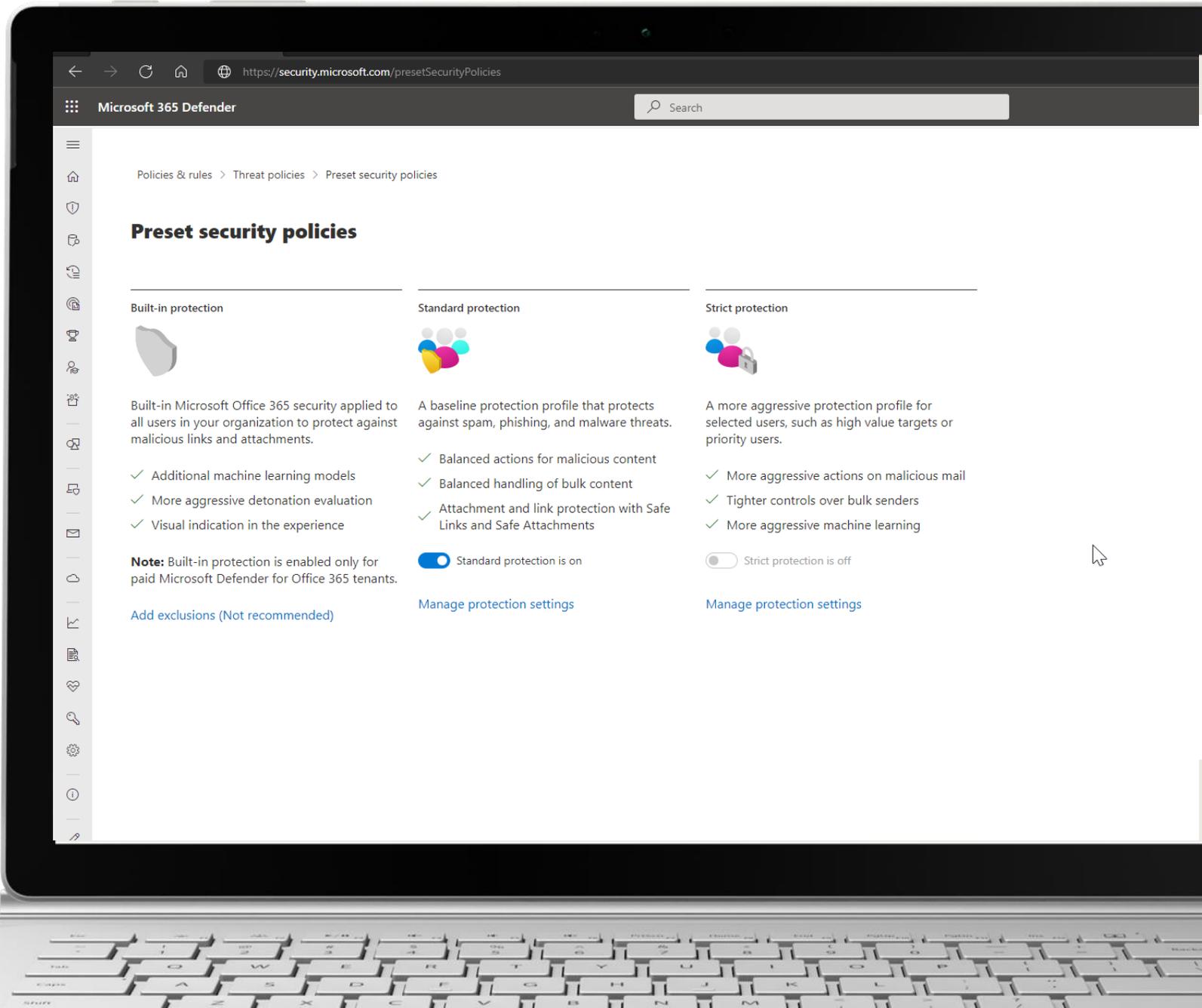
→ Multi-layered protection stack stops a wide variety of attacks

Multi-Layered protection stack



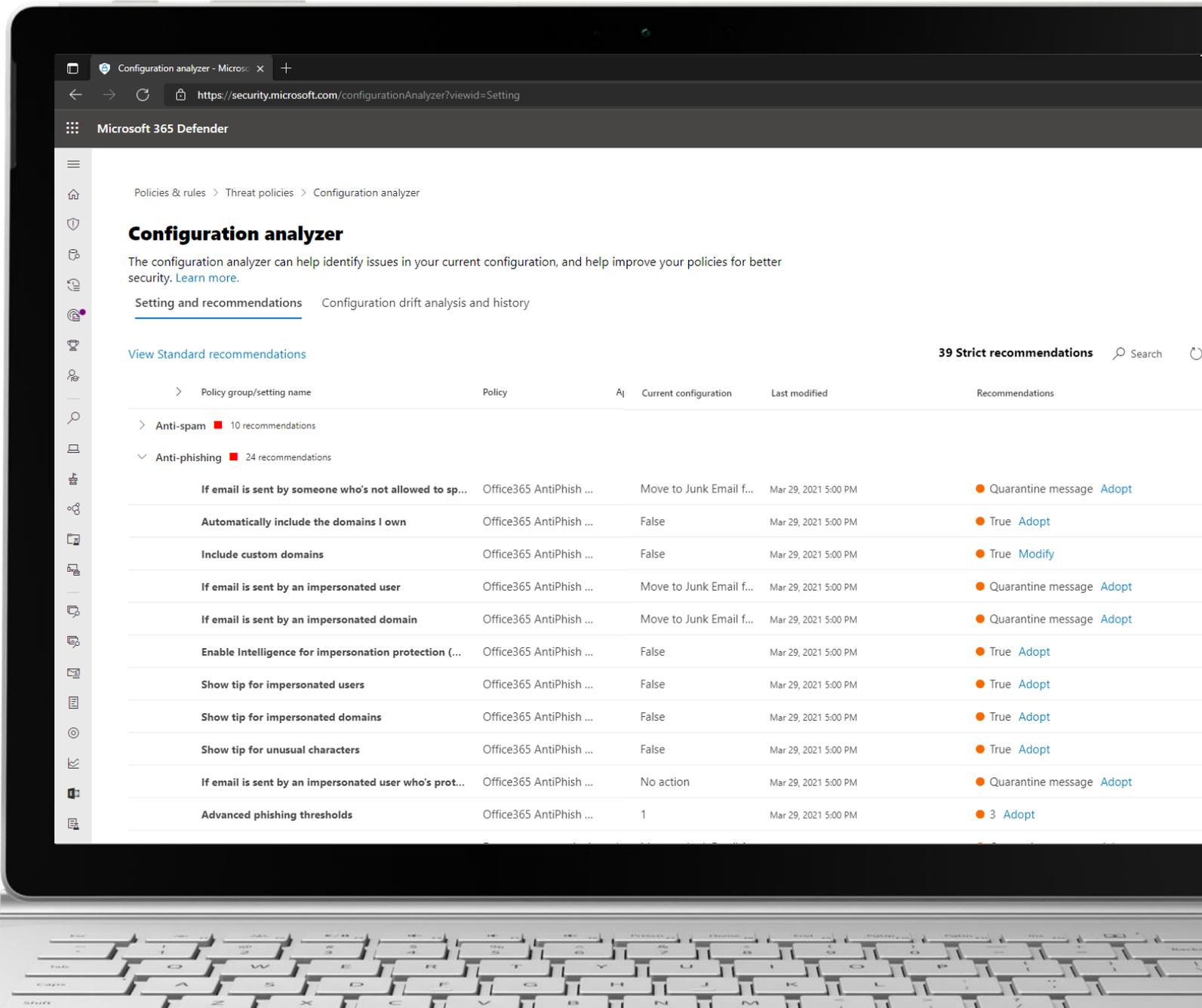
Prevention

- Multi-layered protection stack stops a wide variety of attacks
- Simplified configuration guidance



Prevention

- Multi-layered protection stack stops a wide variety of attacks
- Simplified configuration guidance





Policies & rules > Threat policies > Configuration analyzer

Configuration analyzer

The configuration analyzer can help identify issues in your current configuration, and help improve your policies for better security. [Learn more.](#)

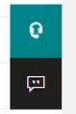
Standard recommendations | Strict recommendations | Configuration drift analysis and history

Anti-spam | 3
Anti-phishing | 15
Anti-malware | 1
Safe Attachments | 1

Refresh

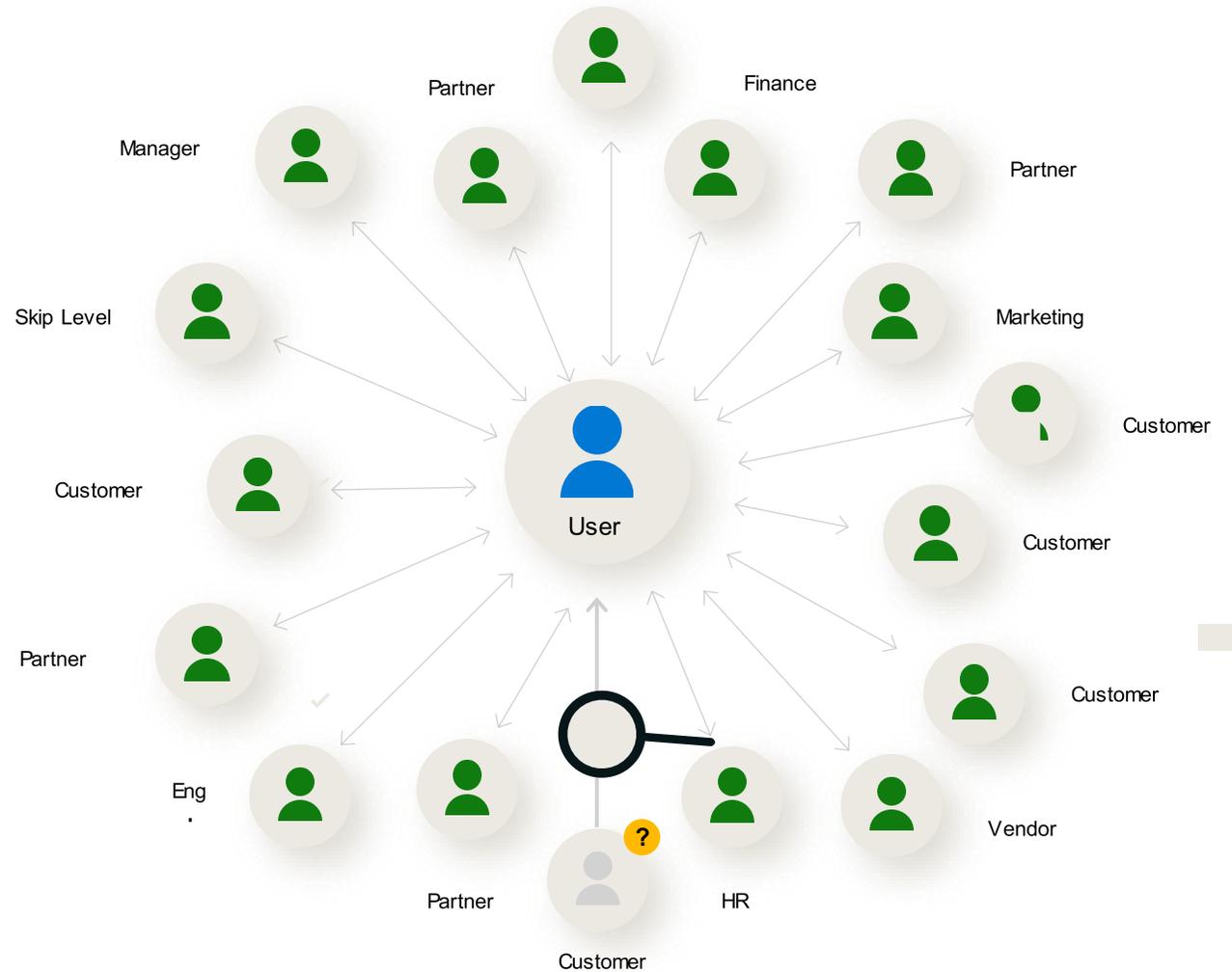
20 items Filter

Recommendations	Policy	Policy group/setting name	Policy type	Current configuration	Last modified	Status
<input type="checkbox"/> Quarantine message	Default	Phishing email detection action	Anti-spam	Move to Junk Email folder	Feb 24, 2022 11:47 AM	Not started
<input type="checkbox"/> Change 7 to 6	Default	Bulk email threshold	Anti-spam	7	Feb 24, 2022 11:47 AM	Not started
<input type="checkbox"/> Change False to True	Default	Enable end-user spam notifications	Anti-spam	False	Feb 24, 2022 11:47 AM	Not started
<input type="checkbox"/> Move to Junk Email folder	Office365 AntiPhish Default	If email is sent by someone who's not allowed to spoof your domain	Anti-phishing	Quarantine message	Feb 24, 2022 11:24 AM	Not started
<input type="checkbox"/> Change False to True	Office365 AntiPhish Default	Add users to protect	Anti-phishing	False	Feb 24, 2022 11:24 AM	Not started
<input type="checkbox"/> Change False to True	Office365 AntiPhish Default	Automatically include the domains I own	Anti-phishing	False	Feb 24, 2022 11:24 AM	Not started
<input type="checkbox"/> Change False to True	Office365 AntiPhish Default	Include custom domains	Anti-phishing	False	Feb 24, 2022 11:24 AM	Not started
<input type="checkbox"/> Quarantine message	Office365 AntiPhish Default	If email is sent by an impersonated user	Anti-phishing	No action	Feb 24, 2022 11:24 AM	Not started
<input type="checkbox"/> Quarantine message	Office365 AntiPhish Default	If email is sent by an impersonated domain	Anti-phishing	No action	Feb 24, 2022 11:24 AM	Not started
<input type="checkbox"/> Change False to True	Office365 AntiPhish Default	Show tip for impersonated users	Anti-phishing	False	Feb 24, 2022 11:24 AM	Not started
<input type="checkbox"/> Change False to True	Office365 AntiPhish Default	Show tip for impersonated domains	Anti-phishing	False	Feb 24, 2022 11:24 AM	Not started
<input type="checkbox"/> Change False to True	Office365 AntiPhish Default	Show tip for unusual characters	Anti-phishing	False	Feb 24, 2022 11:24 AM	Not started



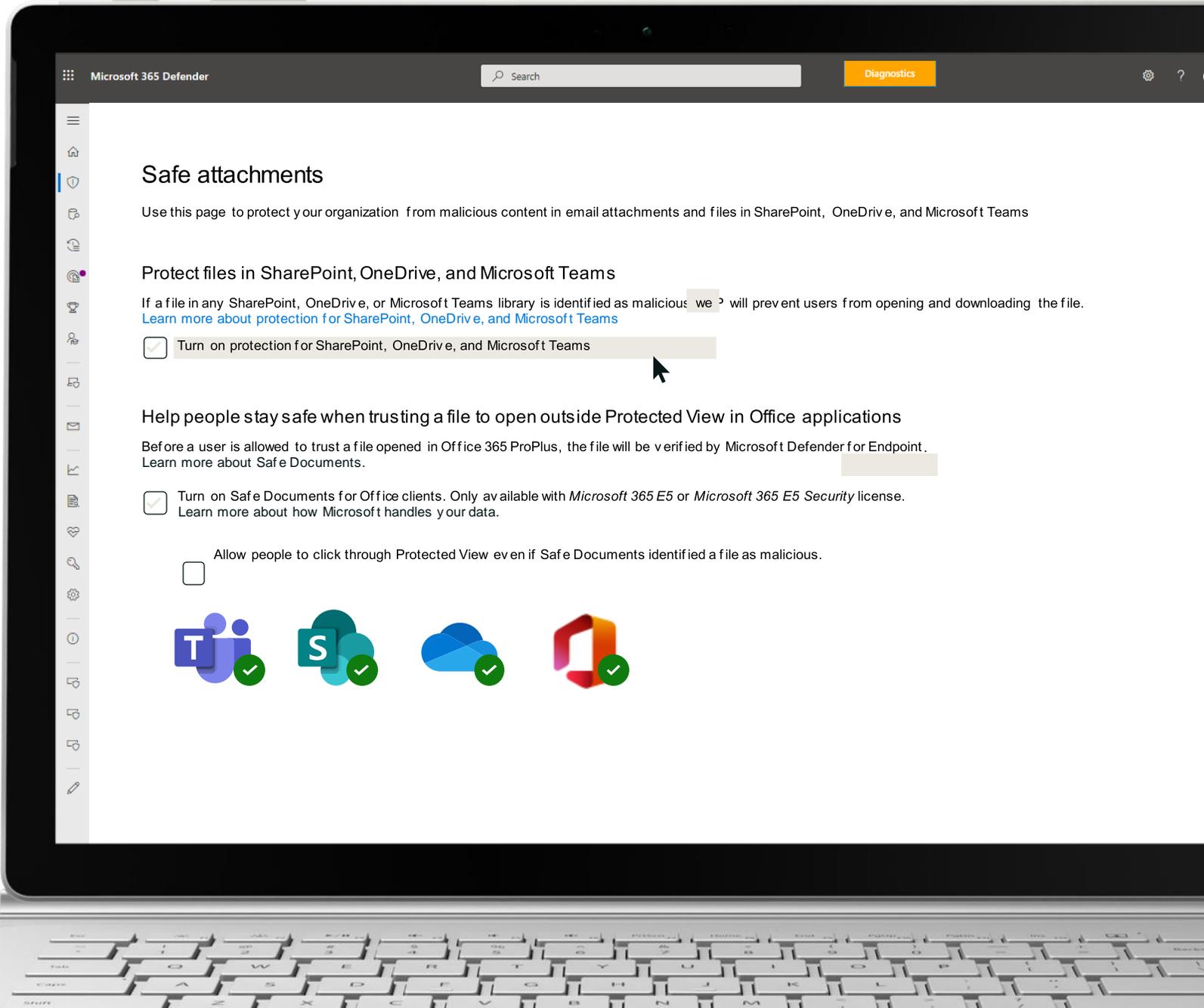
Prevention

- Multi-layered protection stack stops a wide variety of attacks
- Simplified configuration guidance
- Advanced protection against credential phishing, BEC, and account takeover



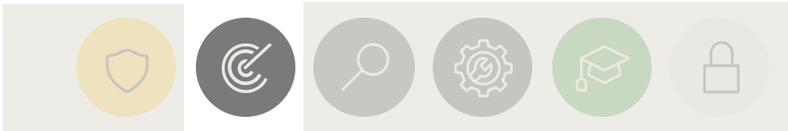
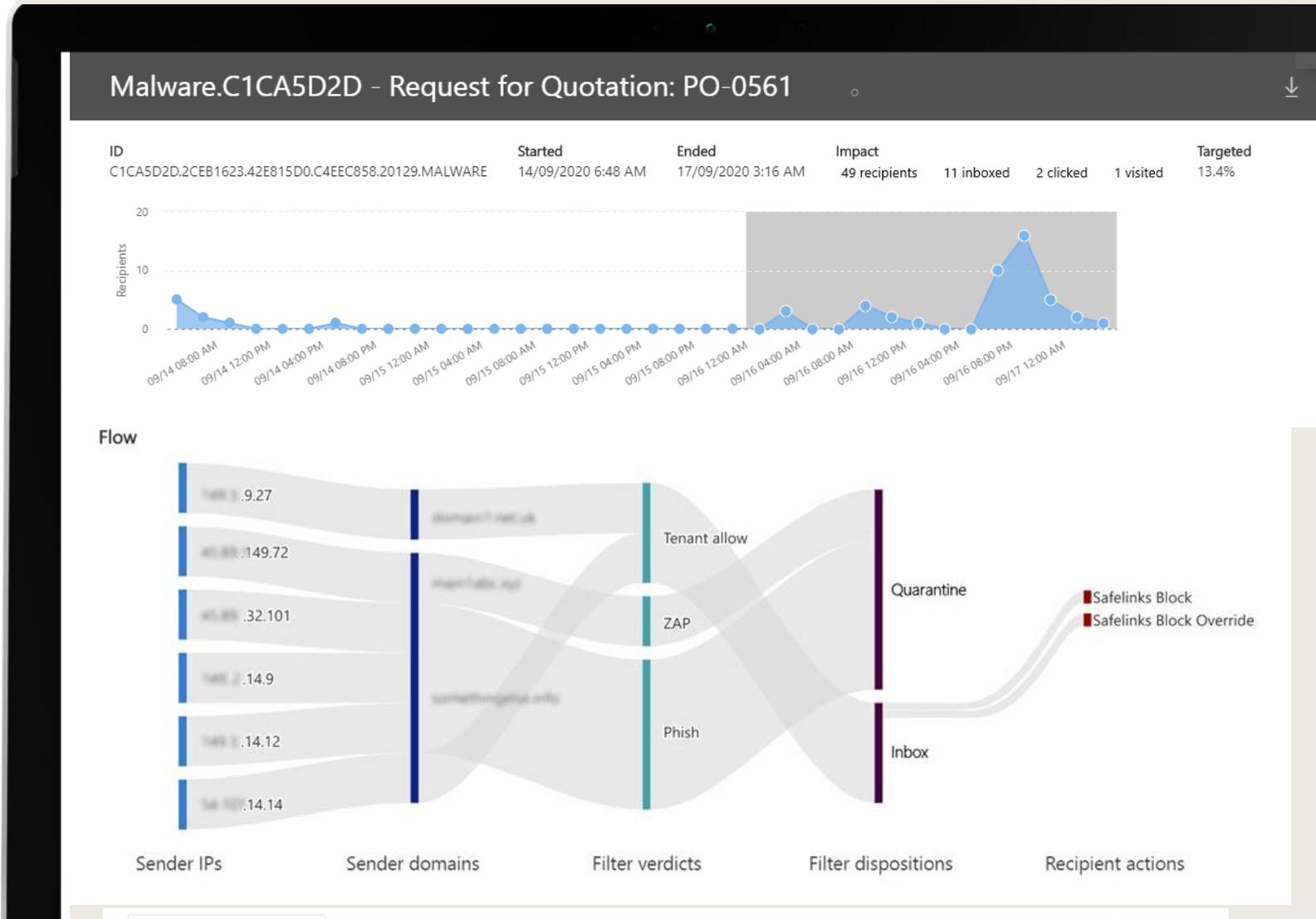
Prevention

- Multi-layered protection stack stops a wide variety of attacks
- Simplified configuration guidance
- Advanced protection against credential phishing, BEC, and account takeover
- Protection beyond email



Detection

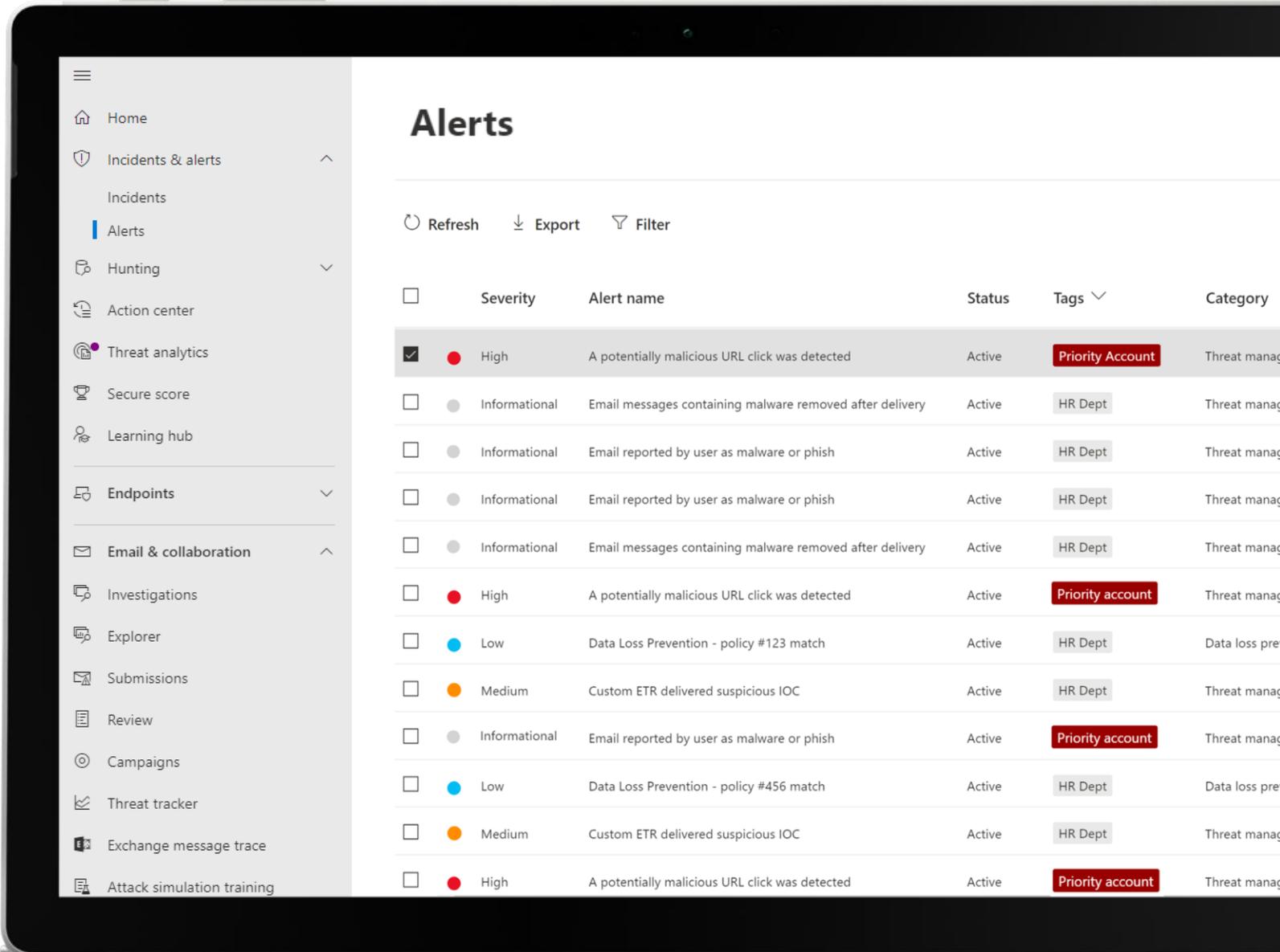
→ Campaign Views leverage AI to surface coordinated attacks designed to evade detection



Detection

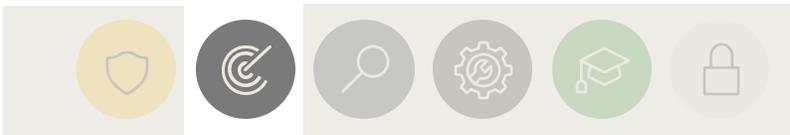
→ Campaign Views leverage AI to surface coordinated attacks designed to evade detection

→ Detailed alerts



The screenshot shows a security dashboard with a left-hand navigation menu and a main content area titled "Alerts". The navigation menu includes options like Home, Incidents & alerts, Alerts, Hunting, Action center, Threat analytics, Secure score, Learning hub, Endpoints, Email & collaboration, Investigations, Explorer, Submissions, Review, Campaigns, Threat tracker, Exchange message trace, and Attack simulation training. The "Alerts" section is currently selected. The main area displays a table of alerts with columns for checkboxes, Severity, Alert name, Status, Tags, and Category. The table contains 14 rows of alert data.

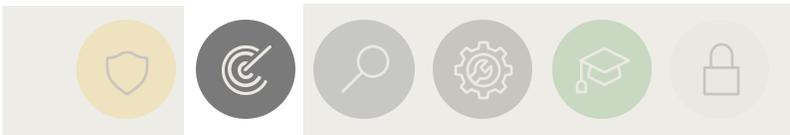
<input type="checkbox"/>	Severity	Alert name	Status	Tags	Category
<input checked="" type="checkbox"/>	High	A potentially malicious URL click was detected	Active	Priority Account	Threat manag
<input type="checkbox"/>	Informational	Email messages containing malware removed after delivery	Active	HR Dept	Threat manag
<input type="checkbox"/>	Informational	Email reported by user as malware or phish	Active	HR Dept	Threat manag
<input type="checkbox"/>	Informational	Email reported by user as malware or phish	Active	HR Dept	Threat manag
<input type="checkbox"/>	Informational	Email messages containing malware removed after delivery	Active	HR Dept	Threat manag
<input type="checkbox"/>	High	A potentially malicious URL click was detected	Active	Priority account	Threat manag
<input type="checkbox"/>	Low	Data Loss Prevention - policy #123 match	Active	HR Dept	Data loss pre
<input type="checkbox"/>	Medium	Custom ETR delivered suspicious IOC	Active	HR Dept	Threat manag
<input type="checkbox"/>	Informational	Email reported by user as malware or phish	Active	Priority account	Threat manag
<input type="checkbox"/>	Low	Data Loss Prevention - policy #456 match	Active	HR Dept	Data loss pre
<input type="checkbox"/>	Medium	Custom ETR delivered suspicious IOC	Active	HR Dept	Threat manag
<input type="checkbox"/>	High	A potentially malicious URL click was detected	Active	Priority account	Threat manag



Detection

- Campaign Views leverage AI to surface coordinated attacks designed to evade detection
- Detailed alerts
- Detection of content weaponized after delivery

The screenshot displays the Microsoft 365 Defender web interface. At the top, the title bar reads "Microsoft 365 Defender" with a search bar and a "Diagnostics" button. The main content area shows an alert titled "Alerts > A potentially malicious URL click was detected". Below the title, there is a "Part of incident: A potentially malicious URL click was detected" link and a user profile for "Jonathan Wolcott". The "ALERT STORY" section includes a "What happened" section with the text: "We have detected that one of your users has recently clicked on a link that was found to be malicious -V1.0.0.3". Below this is a "Messages list" section with a "View messages in Explorer" link and a table containing one message. The table has columns for "Received Date", "Recipient", "Subject", and "Sender". The message details are: Received Date: Mar 26, 2021 4:52 PM; Recipient: jwolcott@fabricam.onmicrosoft.com; Subject: Check this out!; Sender: badactor@contoso.com. On the right side, there is a detailed alert card for "A potentially malicious URL click was detected" with a "High" severity and "New" status. It includes options to "Manage alert" and "View messages in Explorer". Below the alert card is a "Classify this alert" section with "True alert" and "False alert" buttons. Further down, there are sections for "Alert state", "Alert details", "Alert Policy", and "Incident details". The "Alert state" section shows "Classification: Not Set" and "Assigned to: Unassigned". The "Alert details" section includes "Category: Initial access", "Detection source: MDO", "Detection technology: URL Detonation", "First activity: Mar 26, 2021 5:13:34 PM", and "Last activity: Mar 26, 2021 5:13:34 PM". The "Alert Policy" section shows "A potentially malicious URL click was detected". The "Incident details" section shows "Incident: A potentially malicious URL click was detected" and "Incident severity: High".



Protection Demo



End User Experience



Recycle Bin



Microsoft Edge



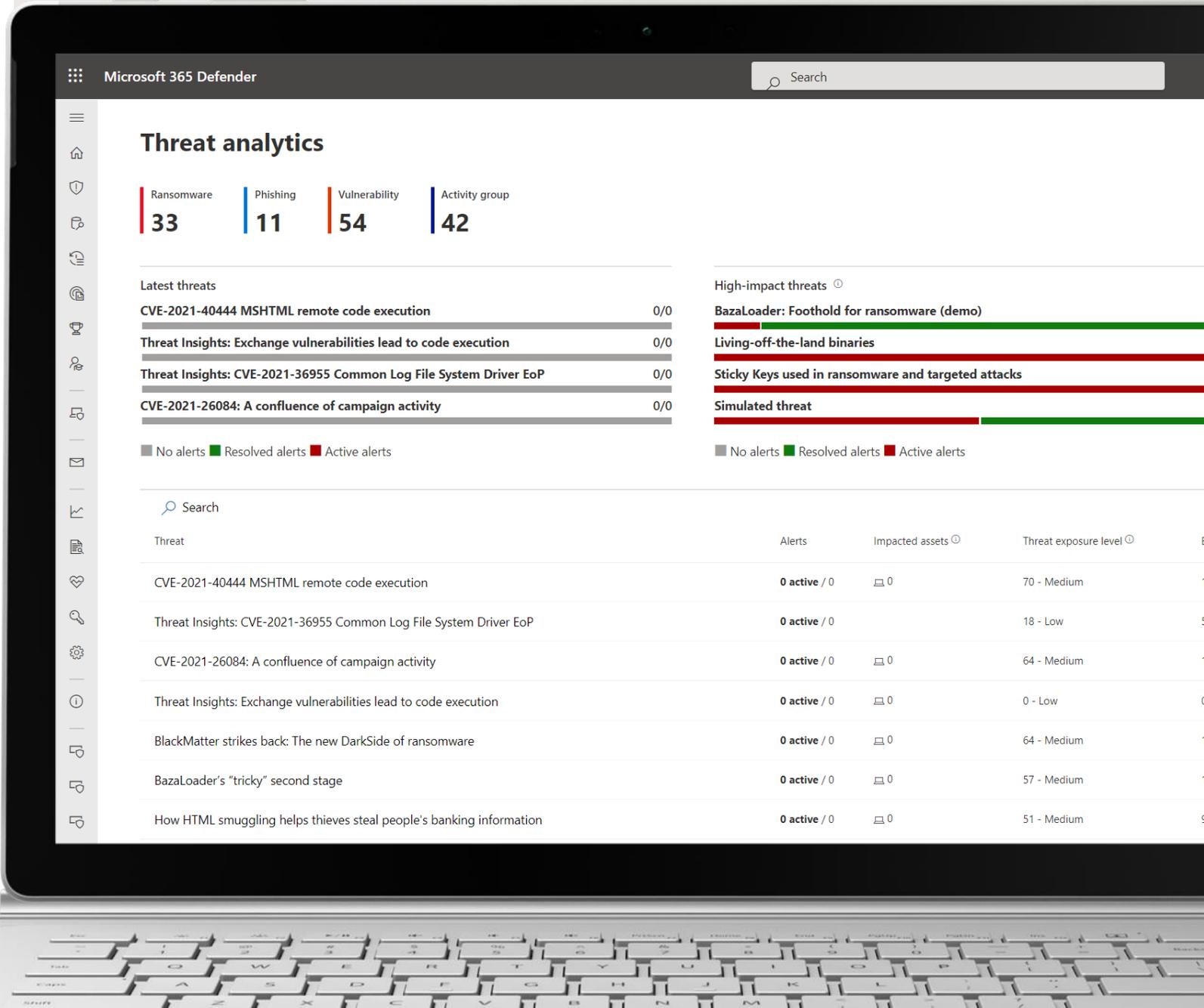
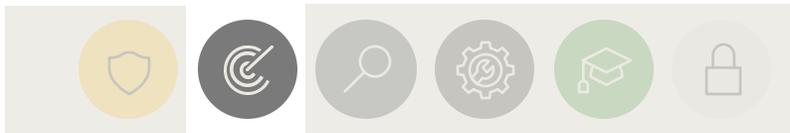
Type here to search



26°C Mostly cloudy ^ [display] [volume] ENG 3:33 PM 9/12/2022 [notifications]

Detection

- Campaign Views leverage AI to surface coordinated attacks designed to evade detection
- Detailed alerts
- Detection of content weaponized after delivery
- Threat Analytics reports from Microsoft Security Research



Threat analytics



Email notification settings Help resources

Latest threats

ZINC: Targeting IT, telecommunications, and media organizations	0/0
Threat Insights: Microsoft investigates Iranian attacks against the Albanian government	0/0
Azure subscription hijacking campaign facilitates credential stuffing attacks	0/0
OAuth consent phishing	0/0

■ No alerts ■ Resolved alerts ■ Active alerts

High-impact threats

Simulated threat	0/0
WannaCrypt	0/0
BadRabbit	0/0
Smoke Loader (Dofiol) mines coin	0/0

■ No alerts ■ Resolved alerts ■ Active alerts

Highest exposure threats

■ High 70-100 ■ Medium 30-69 ■ Low 0-29

Search 1-30 Choose columns 30 items per page Filters

Threat	Alerts	Impacted assets	Threat exposure level	Misconfigured devices	Vulnerable devices	Report type	Published
ZINC: Targeting IT, telecommunications, and media organizations	0 active /...		Not available	Not available	Not available	Activity groups	9/9/2022, 9:00 AM
Threat Insights: Microsoft investigates Iranian attacks against the Albanian government	0 active /...		Not available	Not available	Not available	Attack campaigns	9/8/2022, 1:00 AM
Azure subscription hijacking campaign facilitates credential stuffing attacks	0 active /...		Not available	Not available	Not available	Attack campaigns	9/1/2022, 9:22 AM
OAuth consent phishing	0 active /... 0		Not available	Not available	Not available	Tools & techniques	1/26/2021, 1:35 AM
CVE-2022-30190 Microsoft Support Diagnostic Tool remote code execution vulnerability	0 active /... 0		Not available	Not available	Not available	Vulnerabilities	6/8/2022, 1:33 PM
Business Email Compromise credential harvesting	0 active /...		Not available	Not available	Not available	Tools & techniques	8/28/2022, 11:45 PM
MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone	0 active /...		Not available	Not available	Not available	Tools & techniques	8/24/2022, 4:54 AM
Ransomware: A pervasive and ongoing threat	0 active /... 0		Not available	Not available	Not available	Attack campaigns	6/4/2021, 4:05 AM

Threat analytics

Ransomware **43** | Phishing **16** | Vulnerability **66** | Activity group **60**

Email notification settings Help resources

Latest threats

ZINC: Targeting IT, telecommunications, and media organizations	0/0
Threat Insights: Microsoft investigates Iranian attacks against the Albanian government	0/0
Azure subscription hijacking campaign facilitates credential stuffing attacks	0/0
OAuth consent phishing	0/0

No alerts Resolved alerts Active alerts

High-impact threats

Simulated threat	0/0
WannaCrypt	0/0
BadRabbit	0/0
Smoke Loader (Dofail) mines coin	0/0

No alerts Resolved alerts Active alerts

Highest exposure threats

High 70-100 Medium 30-69 Low 0-29

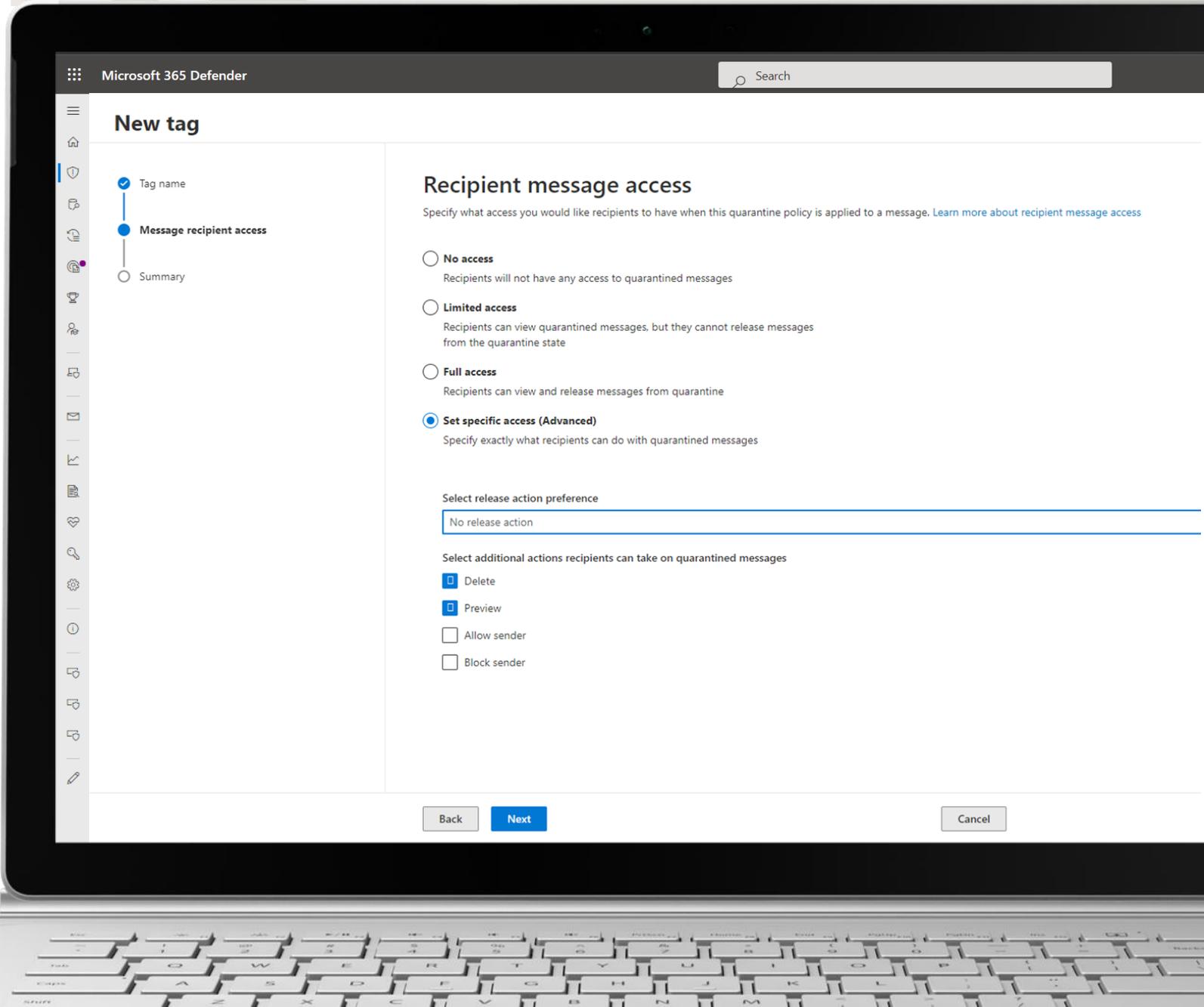
Search

1-30 Choose columns 30 items per page Filters

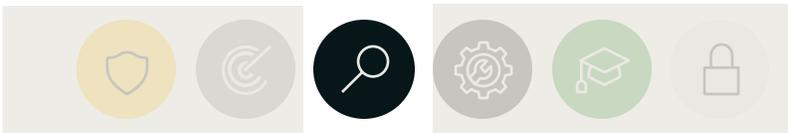
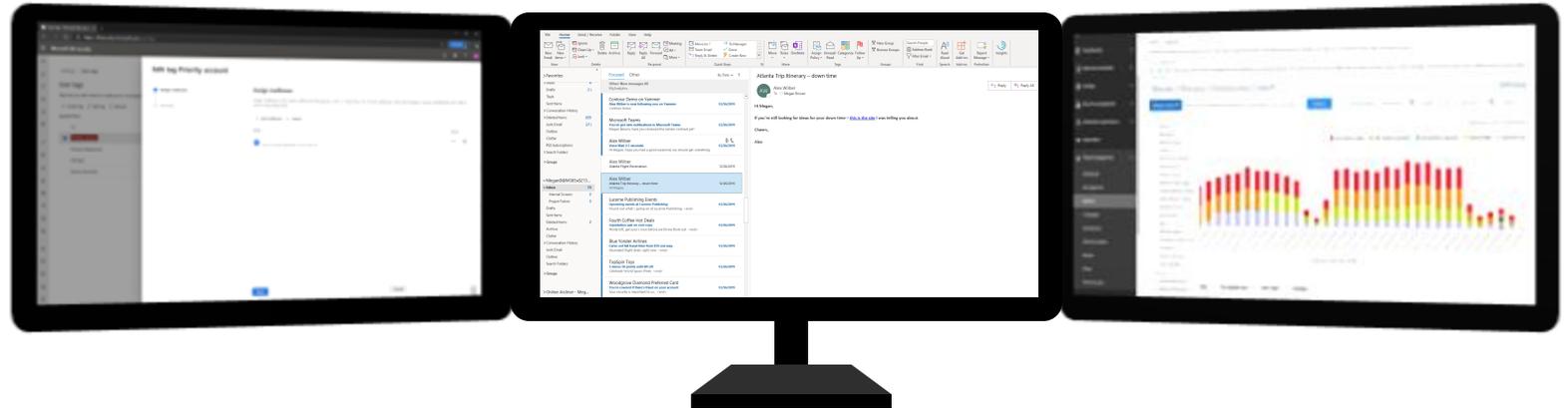
Threat	Alerts	Impacted assets	Threat exposure level	Misconfigured devices	Vulnerable devices	Report type	Published
ZINC: Targeting IT, telecommunications, and media organizations	0 active /...		Not available	Not available	Not available	Activity groups	9/9/2022, 9:00 AM
Threat Insights: Microsoft investigates Iranian attacks against the Albanian government	0 active /...		Not available	Not available	Not available	Attack campaigns	9/8/2022, 1:00 AM
Azure subscription hijacking campaign facilitates credential stuffing attacks	0 active /...		Not available	Not available	Not available	Attack campaigns	9/1/2022, 9:22 AM
OAuth consent phishing	0 active /...	0	Not available	Not available	Not available	Tools & techniques	1/26/2021, 1:35 AM
CVE-2022-30190 Microsoft Support Diagnostic Tool remote code execution vulnerability	0 active /...	0	Not available	Not available	Not available	Vulnerabilities	6/8/2022, 1:33 PM
Business Email Compromise credential harvesting	0 active /...		Not available	Not available	Not available	Tools & techniques	8/28/2022, 11:45 PM
MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone	0 active /...		Not available	Not available	Not available	Tools & techniques	8/24/2022, 4:54 AM
Ransomware: A pervasive and ongoing threat	0 active /...	0	Not available	Not available	Not available	Attack campaigns	6/4/2021, 4:05 AM

Detection

- Campaign Views leverage AI to surface coordinated attacks designed to evade detection
- Detailed alerts
- Detection of content weaponized after delivery
- Threat Analytics reports from Microsoft Security Research
- Dedicated end-user quarantine policy

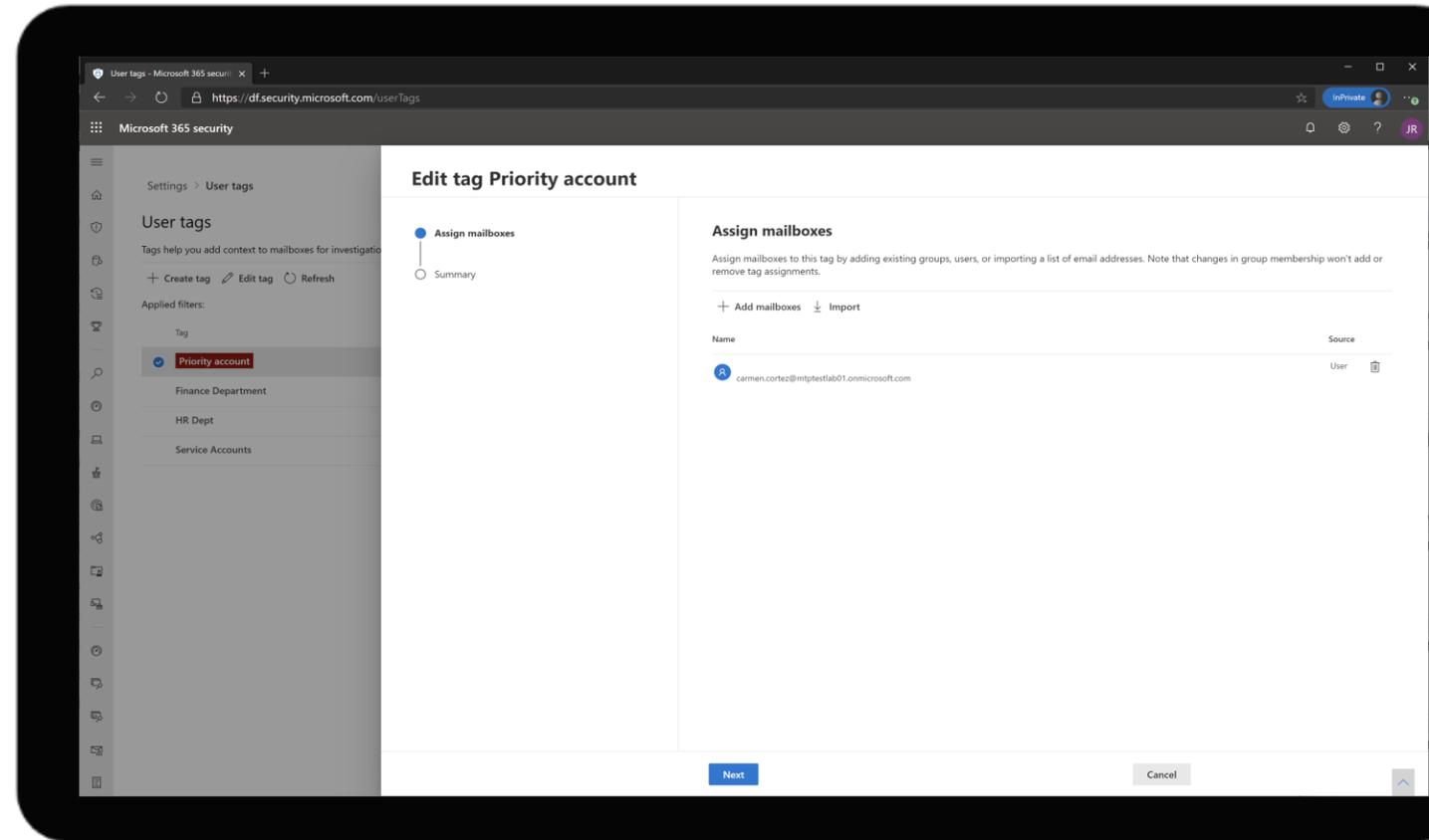


Investigation & Hunting



Investigation & Hunting

→ Prioritized focus through Priority accounts

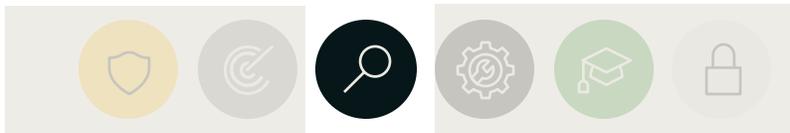


Investigation & Hunting

→ Prioritized focus through Priority accounts

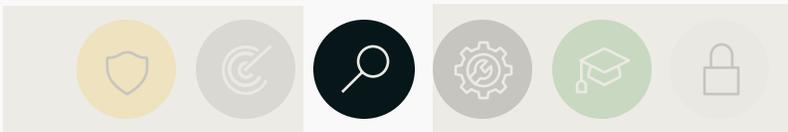
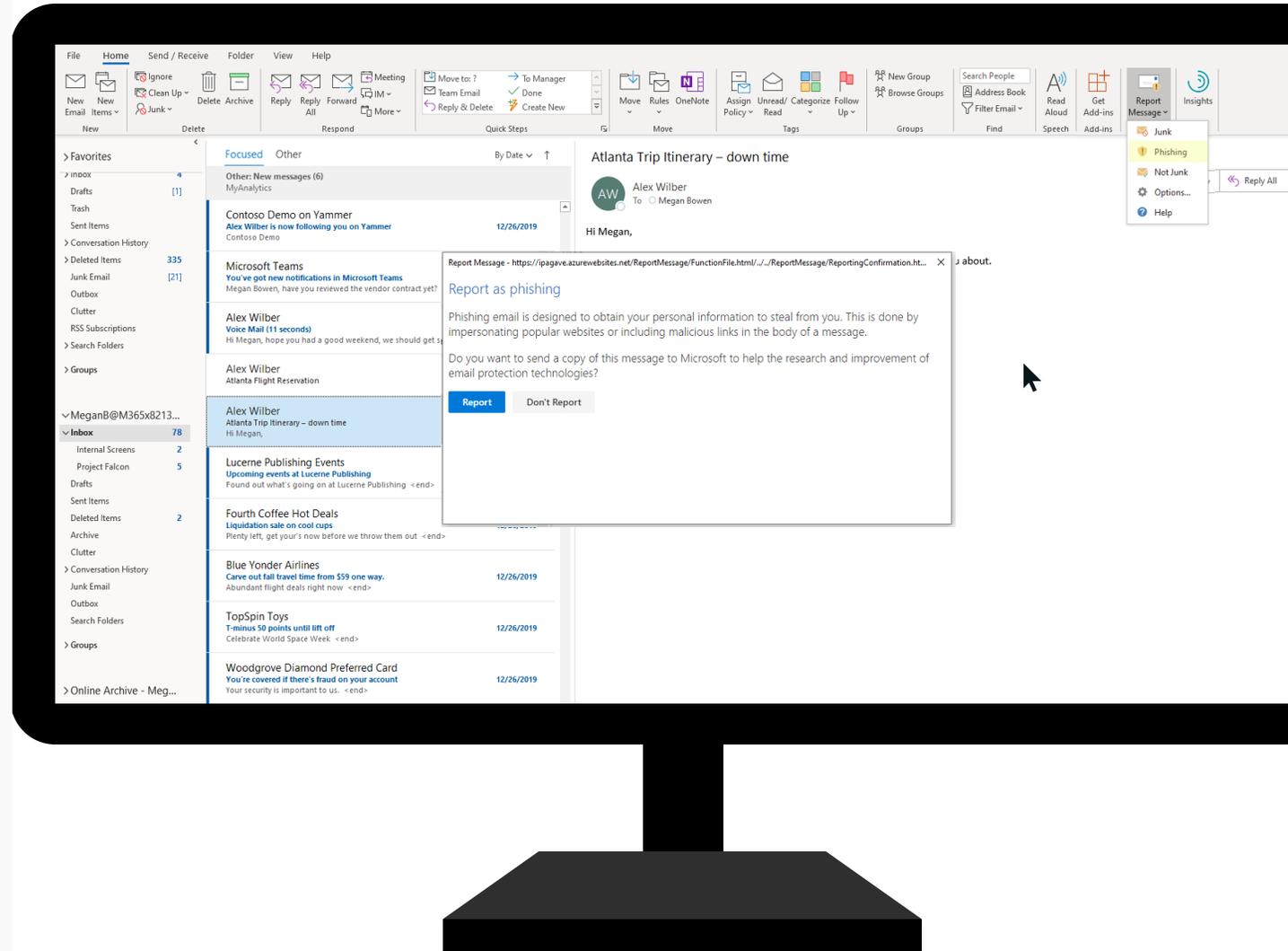
The screenshot displays the Microsoft 365 Defender Explorer interface. The top navigation bar includes 'Microsoft 365 Defender' and 'Diagnostics'. The main section is titled 'Explorer' and contains a search bar with the filter 'Priority Account'. Below the search bar, there are tabs for 'Email', 'URL clicks', 'URLs', 'Top targeted users', 'Email origin', and 'Campaign'. A table of email messages is shown, with columns for Date, Subject, Recipient, Tags, Sender, Additional actions, Latest delivery location, and Original delivery location. The 'Tags' column for several rows is highlighted with a red box and labeled 'Priority account'. The interface also includes a sidebar with various icons and a bottom status bar indicating '50 item(s) out of 8240 loaded'.

Date (UTC +05:30)	Subject	Recipient	Tags	Sender	Additional actions	Latest delivery location	Original delivery location
Sep 22, 2021 11:29 PM	The Drugstore with a Tender Lo...	johndoe@o365tisdflv2.onmicro...	Priority account	undearrelinquish90@vnnic.vn	-	Inbox/folder	Inbox/folder
Sep 22, 2021 11:29 PM	Could chewing this before bed ...	johndoe@o365tisdflv2.onmicro...	Priority account	+3 others RestoreHealthyTeeth@diabeta...	-	Inbox/folder	Inbox/folder
Sep 22, 2021 11:29 PM	云架梯...	johndoe@o365tisdflv2.onmicro...	Priority account	+3 others famesfms@yhotmail.com	-	Inbox/folder	Inbox/folder
Sep 22, 2021 11:29 PM	cheap whitehat monthly SEO PL...	johndoe@o365tisdflv2.onmicro...	Priority account	+3 others MatthewClay7162loy@gmail.com	-	Inbox/folder	Inbox/folder
Sep 22, 2021 11:28 PM	真稅票13530236312	johndoe@o365tisdflv2.onmicro...	Priority account	+3 others bnkvl@hotmail.com	-	Inbox/folder	Inbox/folder



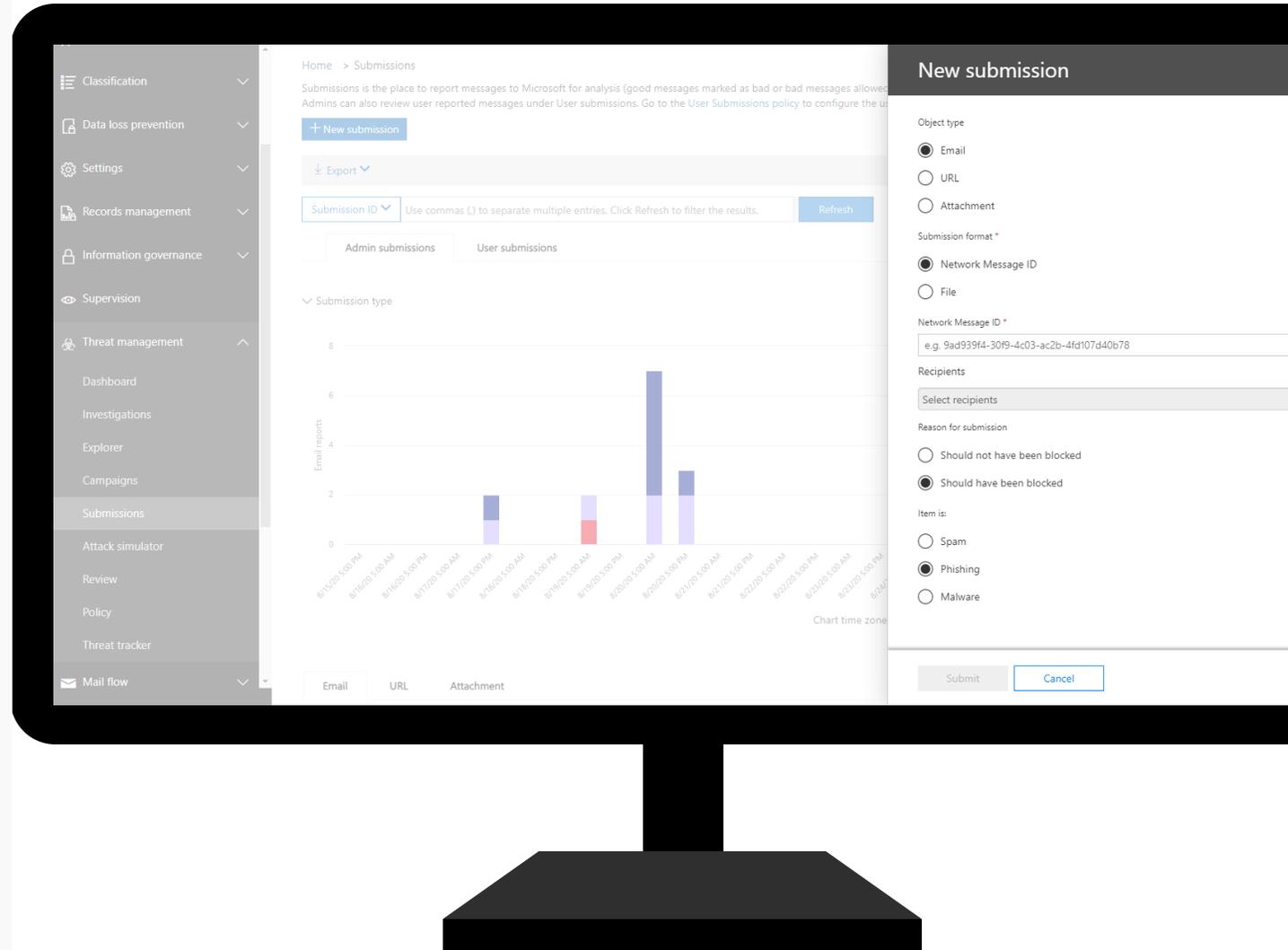
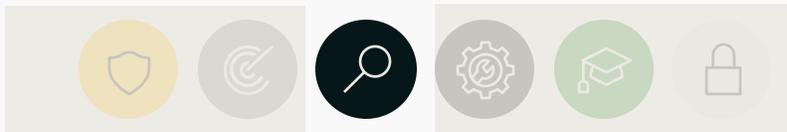
Investigation & Hunting

- Prioritized focus through Priority accounts
- User & Admin Submissions



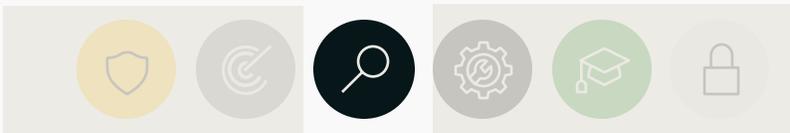
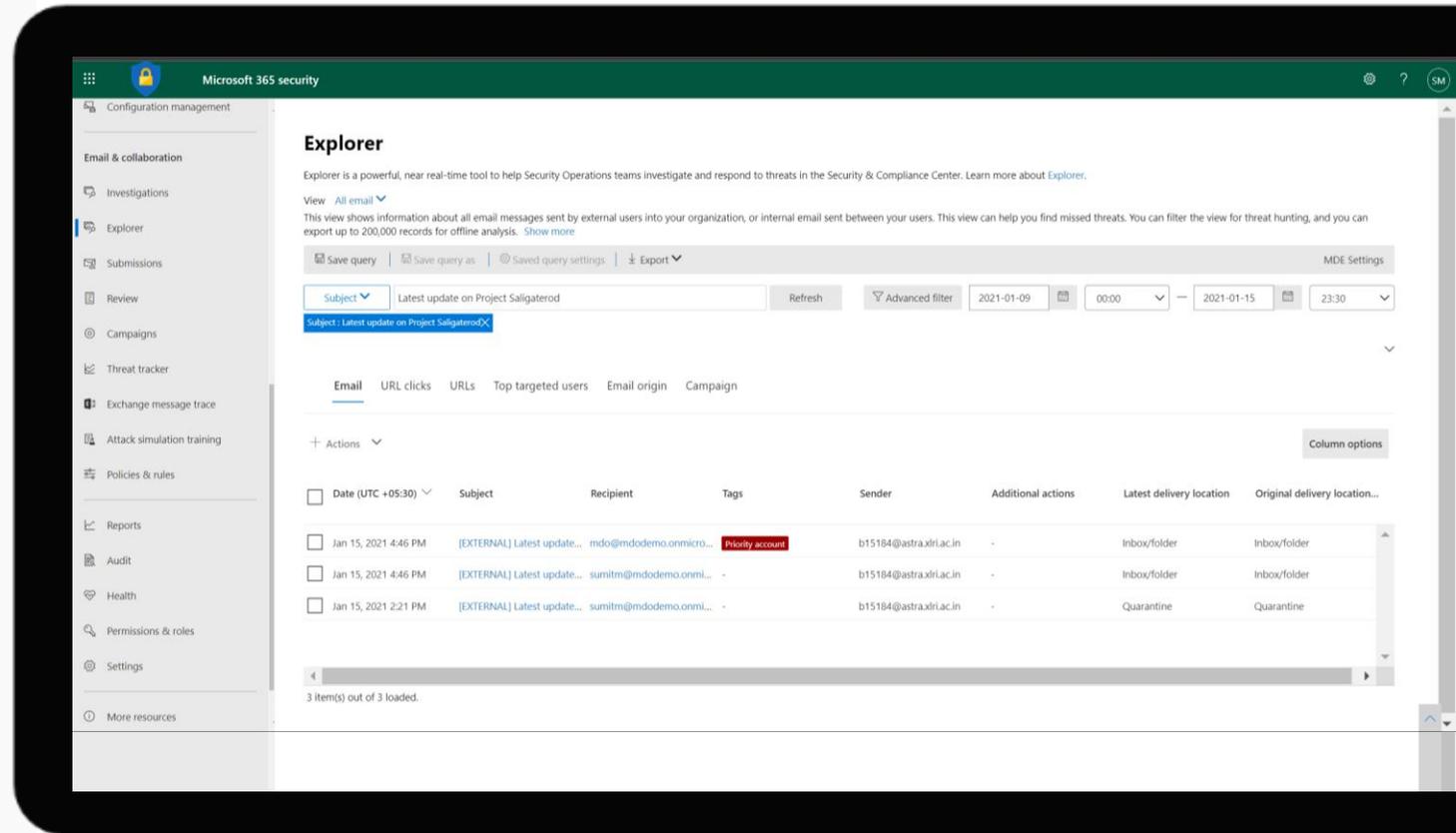
Investigation & Hunting

- Prioritized focus through Priority accounts
- User & Admin Submissions



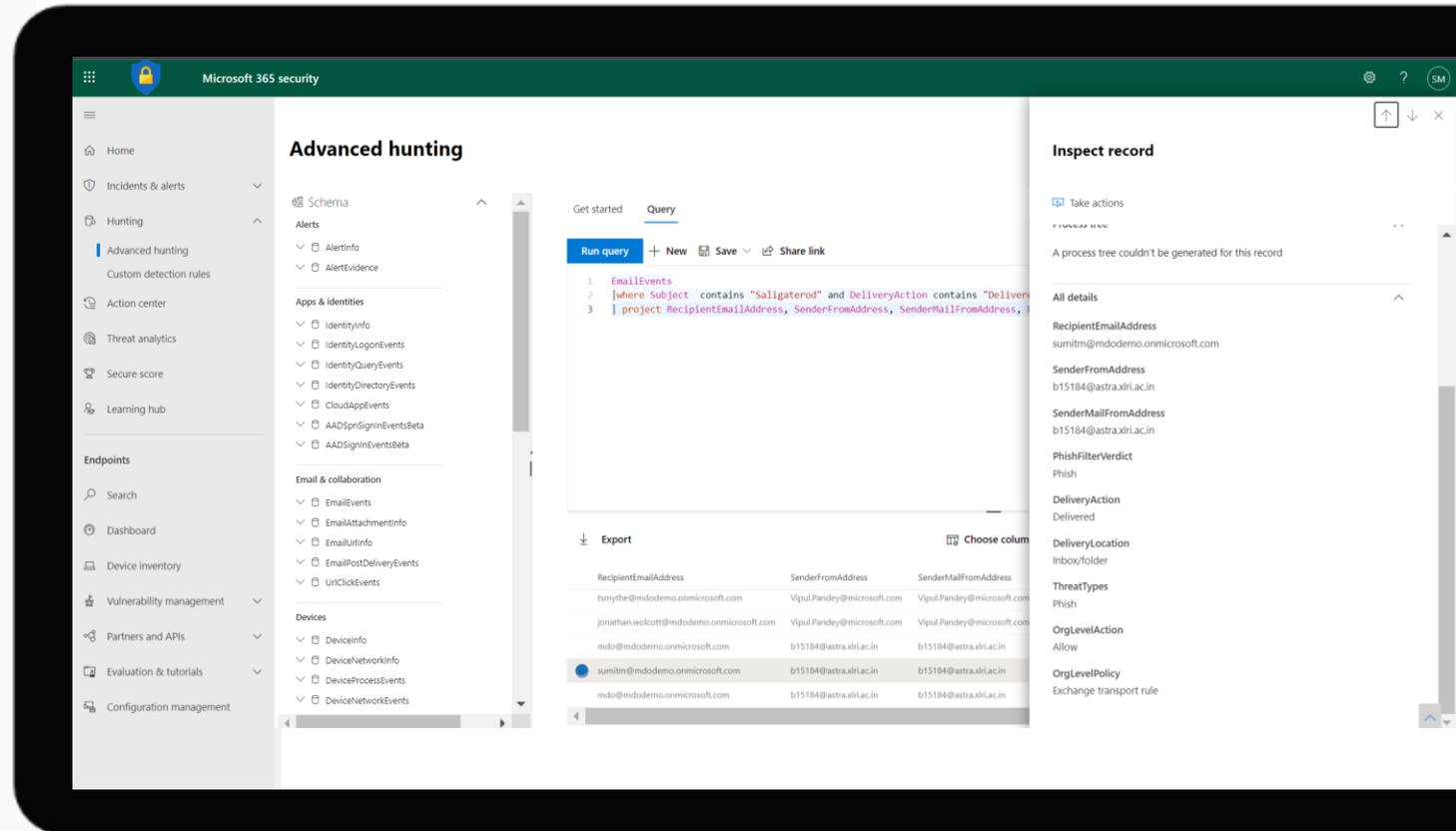
Investigation & Hunting

- Prioritized focus through Priority accounts
- User & Admin Submissions
- Threat Explorer



Investigation & Hunting

- Prioritized focus through Priority accounts
- User & Admin Submissions
- Threat Explorer
- Advanced Hunting for sophisticated queries



Microsoft 365 security

Advanced hunting

Schema

- Alerts
 - AlertInfo
 - AlertEvidence
- Apps & identities
 - IdentityInfo
 - IdentityLogonEvents
 - IdentityQueryEvents
 - IdentityDirectoryEvents
 - CloudAppEvents
 - AADSpnSignInEventsBeta
 - AADSignInEventsBeta
- Email & collaboration
 - EmailEvents
 - EmailAttachmentInfo
 - EmailUrlInfo
 - EmailPostDeliveryEvents
 - UrlClickEvents
- Devices
 - DeviceInfo
 - DeviceNetworkInfo
 - DeviceProcessEvents
 - DeviceNetworkEvents

Get started Query

Run query + New Save Share link

```
1 EmailEvents
2 | where Subject contains "Saligaterod" and DeliveryAction contains "Delivered"
3 | project RecipientEmailAddress, SenderFromAddress, SenderMailFromAddress,
```

Export Choose column

RecipientEmailAddress	SenderFromAddress	SenderMailFromAddress
sumitm@mdodemo.onmicrosoft.com	Vipul.Pandey@microsoft.com	Vipul.Pandey@microsoft.com
jonathan.walcott@mdodemo.onmicrosoft.com	Vipul.Pandey@microsoft.com	Vipul.Pandey@microsoft.com
mdo@mdodemo.onmicrosoft.com	b15184@astra.xiri.ac.in	b15184@astra.xiri.ac.in
sumitm@mdodemo.onmicrosoft.com	b15184@astra.xiri.ac.in	b15184@astra.xiri.ac.in
mdo@mdodemo.onmicrosoft.com	b15184@astra.xiri.ac.in	b15184@astra.xiri.ac.in

Inspect record

Take actions

A process tree couldn't be generated for this record

All details

- RecipientEmailAddress: sumitm@mdodemo.onmicrosoft.com
- SenderFromAddress: b15184@astra.xiri.ac.in
- SenderMailFromAddress: b15184@astra.xiri.ac.in
- PhishFilterVerdict: Phish
- DeliveryAction: Delivered
- DeliveryLocation: Inbox/folder
- ThreatTypes: Phish
- OrgLevelAction: Allow
- OrgLevelPolicy: Exchange transport rule



Advanced Hunting

Get Email Attachments | Emails Sent OoO Hours | PhishingEmailUrlRedirector | Create new

Schema Functions Queries

Alerts

- AlertInfo
- AlertEvidence

Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents

Email & collaboration

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents
- UrlClickEvents

Devices

- DeviceInfo
- DeviceNetworkInfo
- DeviceProcessEvents

Run query Save Share link

Last 7 days Create detection rule

Query

```

1 // get general email details
2 let emaildetails = EmailEvents
3 | project NetworkMessageId, Subject, SenderFromAddress, RecipientEmailAddress;
4 //get attachment details
5 EmailAttachmentInfo
6 | project NetworkMessageId, FileName
7 //join it to the email details
8 | join emaildetails on NetworkMessageId
9 // hide the following column

```

Getting Started Results

Run basic queries

Basic queries

Limit	Shows 10 rows from the specified table
Where	Apply filters to specific columns
Count	Counts the number of rows that match the specified filter
Top	Arranges results by event time and shows first 10 rows
Project	Shows only the file name, path, application and event time

Run advanced queries

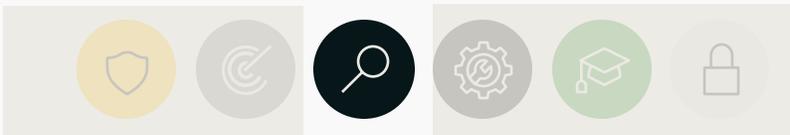
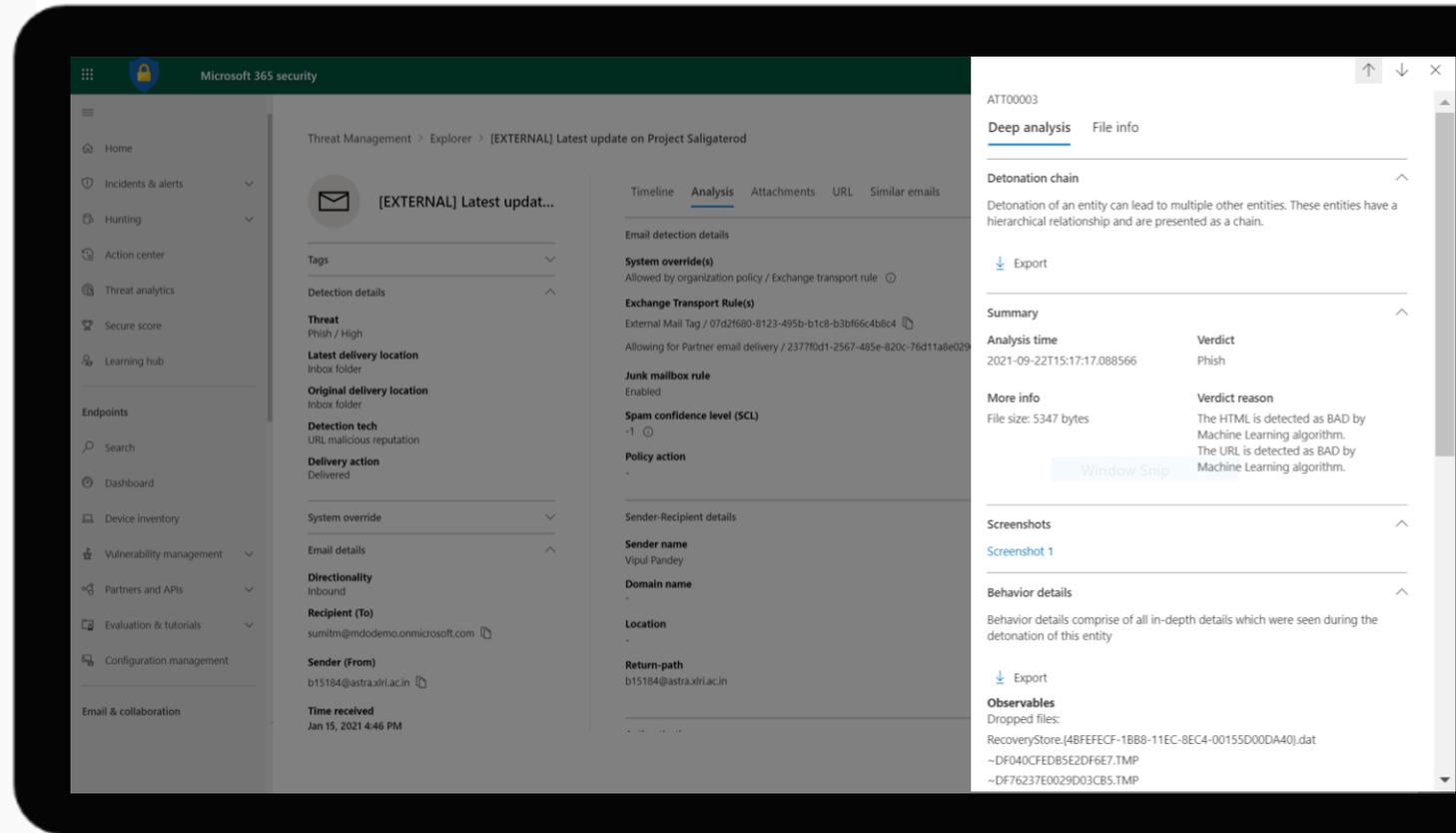
Advanced queries

Summarize	Shows the number of events each day in the past 7 days
Extend	Adds a column that combines user and domain values
Join	Merges file events and process events events on the same device
Makeset	Lists the files activity on each distinct application in the past hour
Find	Search for a value across multiple tables



Investigation & Hunting

- Prioritized focus through Priority accounts
- User & Admin Submissions
- Threat Explorer
- Advanced Hunting for sophisticated queries
- Detailed email analysis

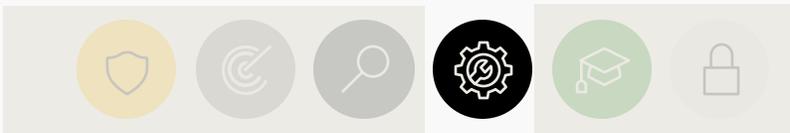


Response & Remediation

→ Guided hunting with inline actions

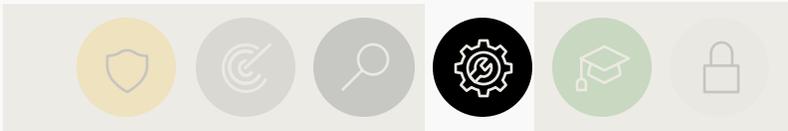
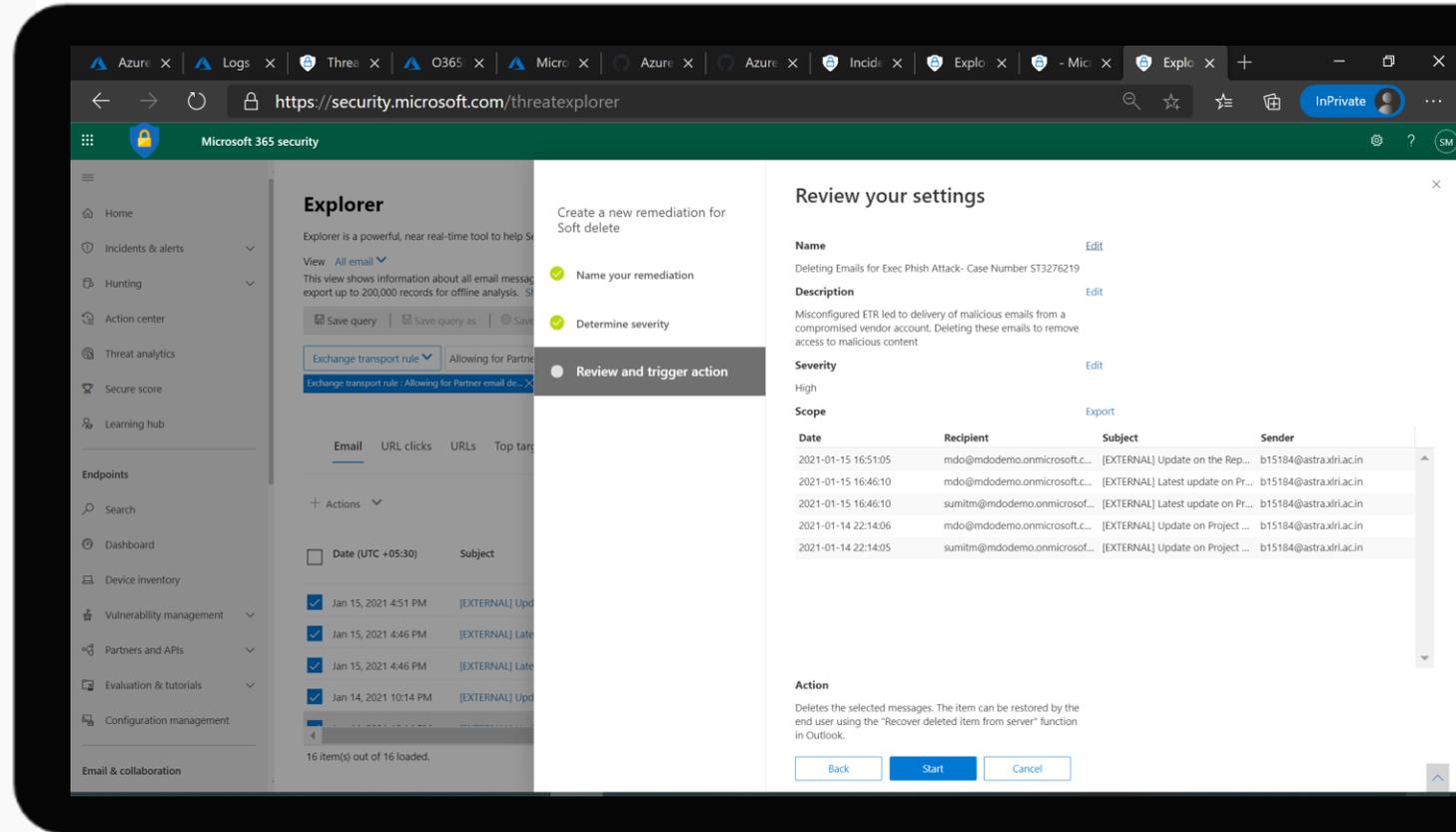
The screenshot displays the Microsoft 365 Security Explorer interface. The browser address bar shows the URL <https://security.microsoft.com/threatexplorer>. The page title is "Microsoft 365 security". The main content area is titled "Explorer" and includes a description: "Explorer is a powerful, near real-time tool to help Security Operations teams investigate and respond to threats in the Security & Compliance Center. Learn more about Explorer." Below this, there is a search bar with the query "Exchange transport rule: Allowing for Partner email delivery" and a date range filter from 2021-01-09 to 2021-01-15. A table of results is shown with columns for Subject, Recipient, Tags, Sender, Additional actions, Latest delivery location, and Original delivery location. An "Actions" menu is open over the table, listing options such as "Move & delete", "Move to junk folder", "Soft delete", "Hard delete", "Move to inbox", "Track & notify", "Trigger investigation", "Investigate Sender", "Investigate Recipient", and "Add to remediation".

Subject	Recipient	Tags	Sender	Additional actions	Latest delivery location	Original delivery location...
XTERNAL] Update on th...	mdo@mdodemo.onmicro...	Priority account	b15184@astraxri.ac.in	-	Inbox/folder	Inbox/folder
XTERNAL] Latest update...	mdo@mdodemo.onmicro...	Priority account	b15184@astraxri.ac.in	-	Inbox/folder	Inbox/folder
XTERNAL] Latest update...	sumitm@mdodemo.onmi...	-	b15184@astraxri.ac.in	-	Inbox/folder	Inbox/folder
XTERNAL] Update on Pr...	mdo@mdodemo.onmicro...	Priority account	b15184@astraxri.ac.in	-	Inbox/folder	Inbox/folder



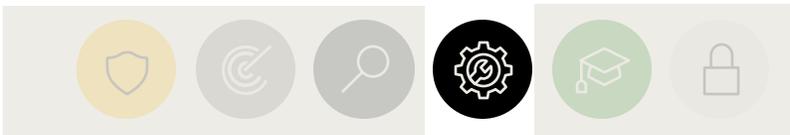
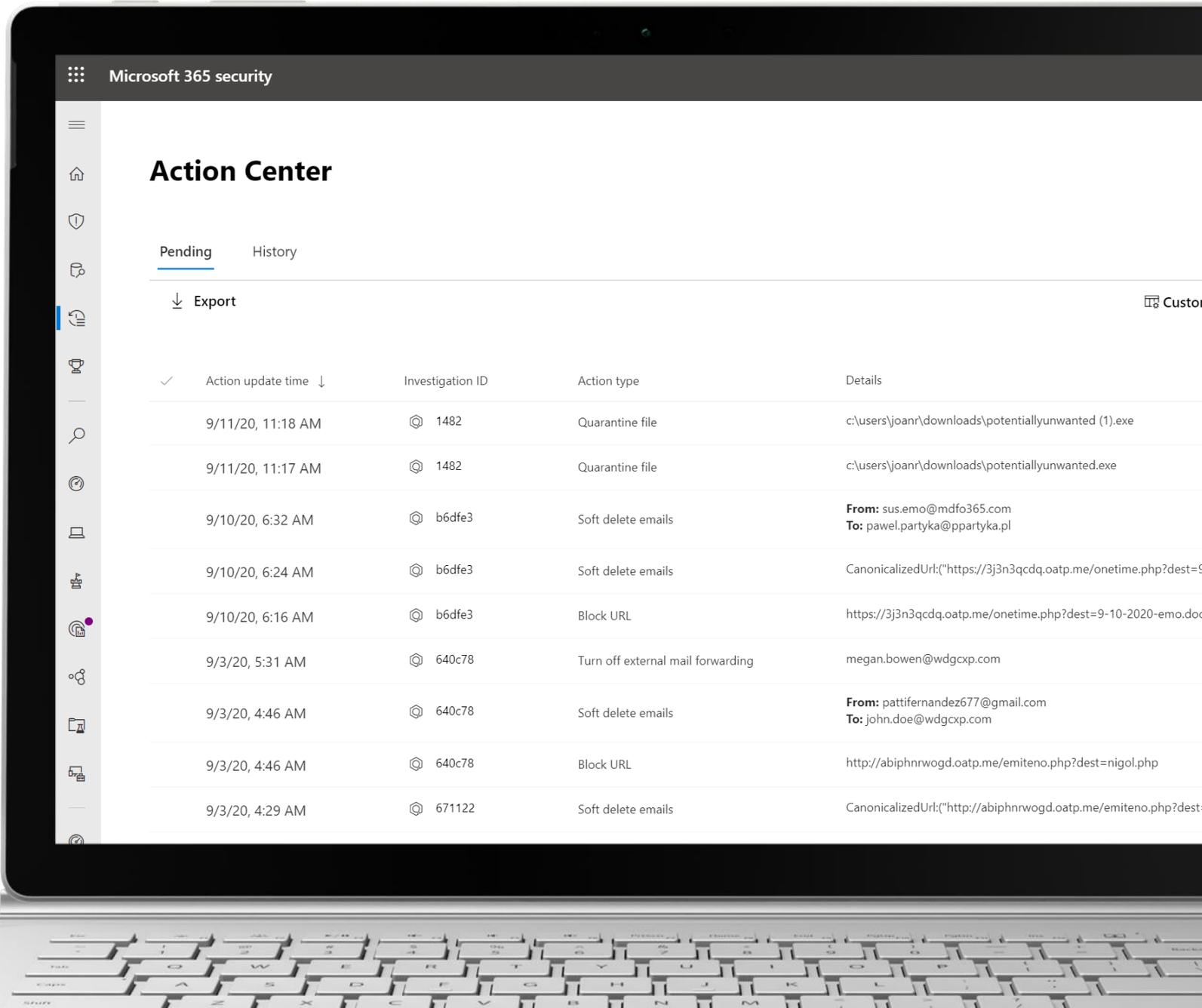
Response & Remediation

→ Guided hunting with inline actions



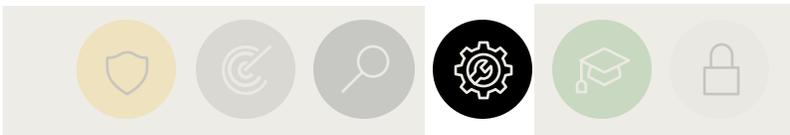
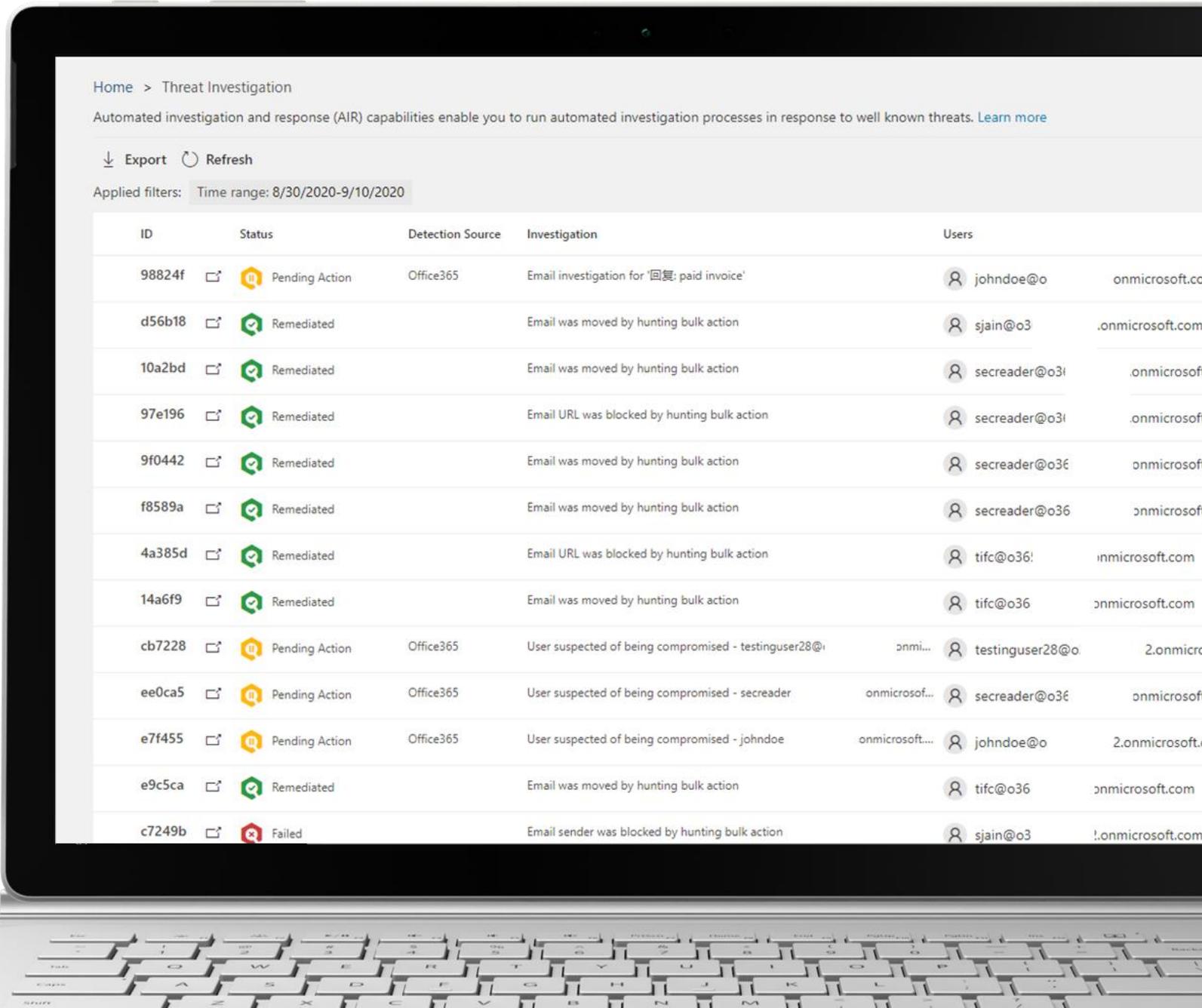
Response & Remediation

- Guided hunting with inline actions
- Centralized action queue



Response & Remediation

- Guided hunting with inline actions
- Centralized action queue
- Automated response playbooks



AIR - User Reported Phish Response



Root investigation Phase

- A determination about what type of threat it might be
- Who sent it
- Where the email was sent from (sending infrastructure)
- Whether other instances of the email were delivered or blocked
- An assessment from MS analysts
- Whether the email is associated with any known campaigns
- and more.

AIR - User Reported Phish Response

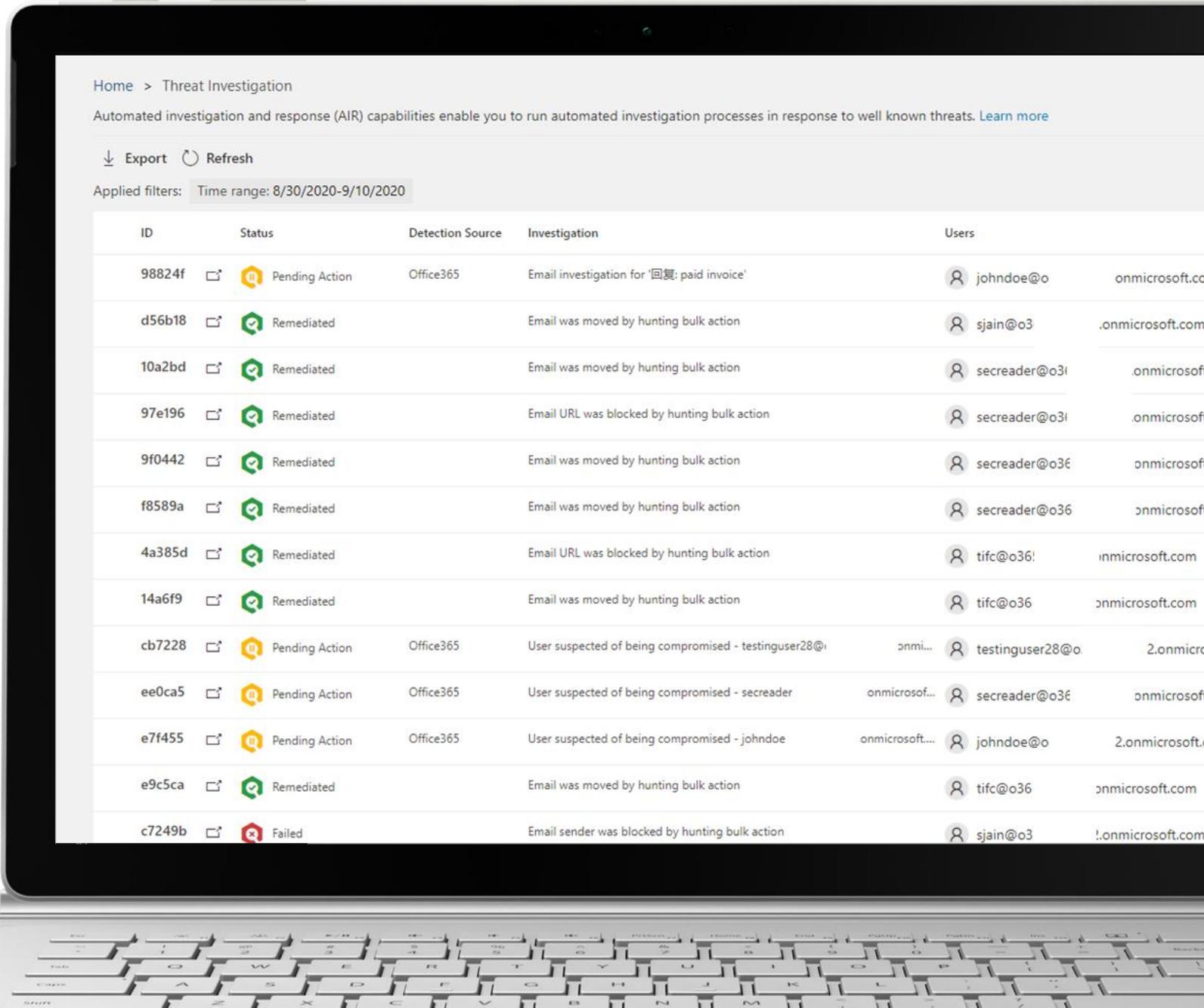


Threat Investigation and Hunting Phase

- Similar email messages are identified via email cluster searches.
- The signal is shared with other platforms, such as Microsoft Defender for Endpoint.
- A determination is made on whether any users have clicked through any malicious links in suspicious email messages.
- A check is done across Exchange Online Protection (EOP) and (Microsoft Defender for Office 365) to see if there are any other similar messages reported by users.
- A check is done to see if a user has been compromised. This check leverages signals across Office 365, Microsoft Defender for Cloud Apps, and Azure Active Directory, correlating any related user activity anomalies.

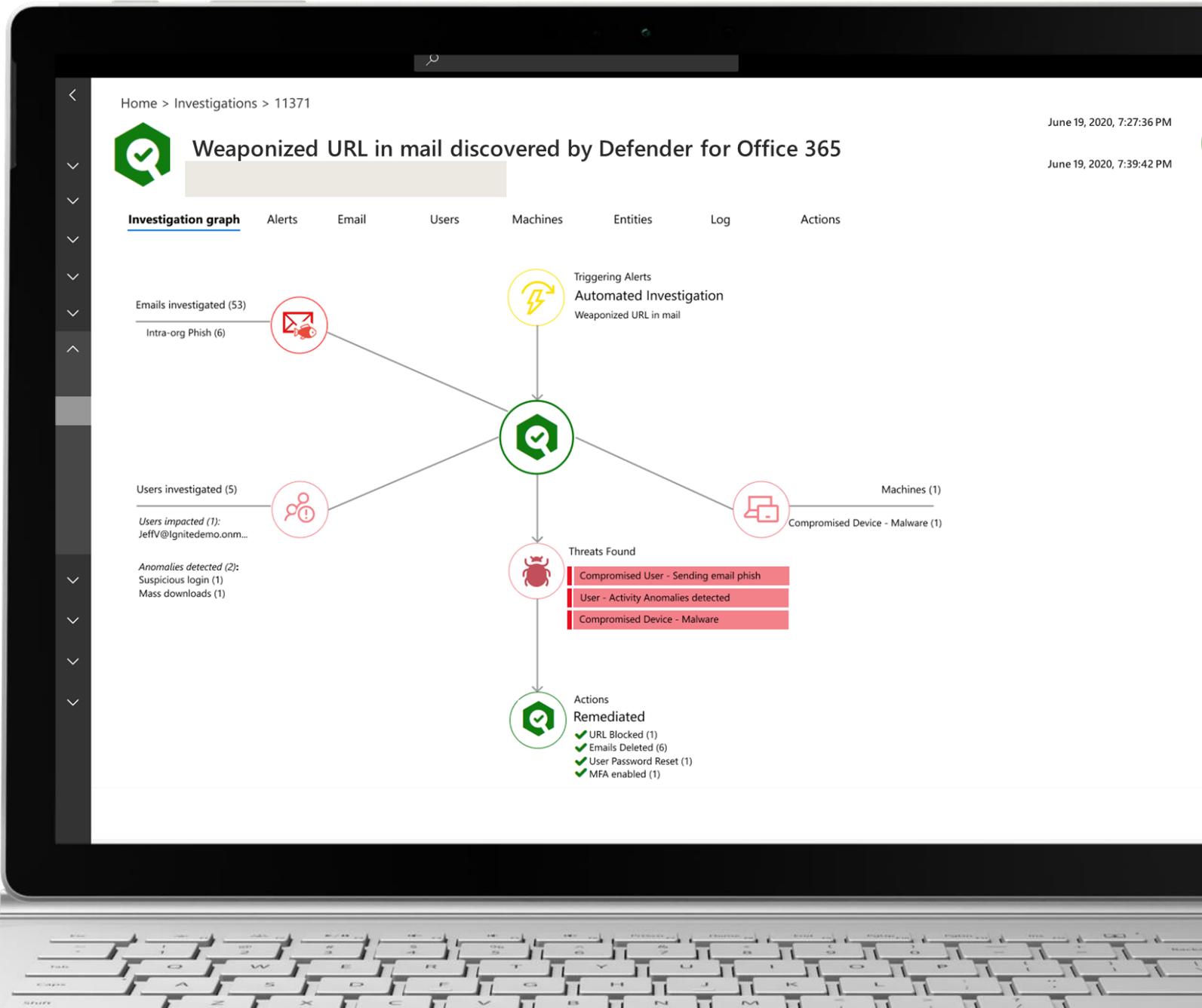
Remediation is the final phase of the playbook. During this phase, remediation steps are identified and surfaced for approval.

Response & Remediation



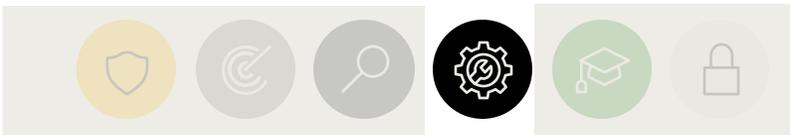
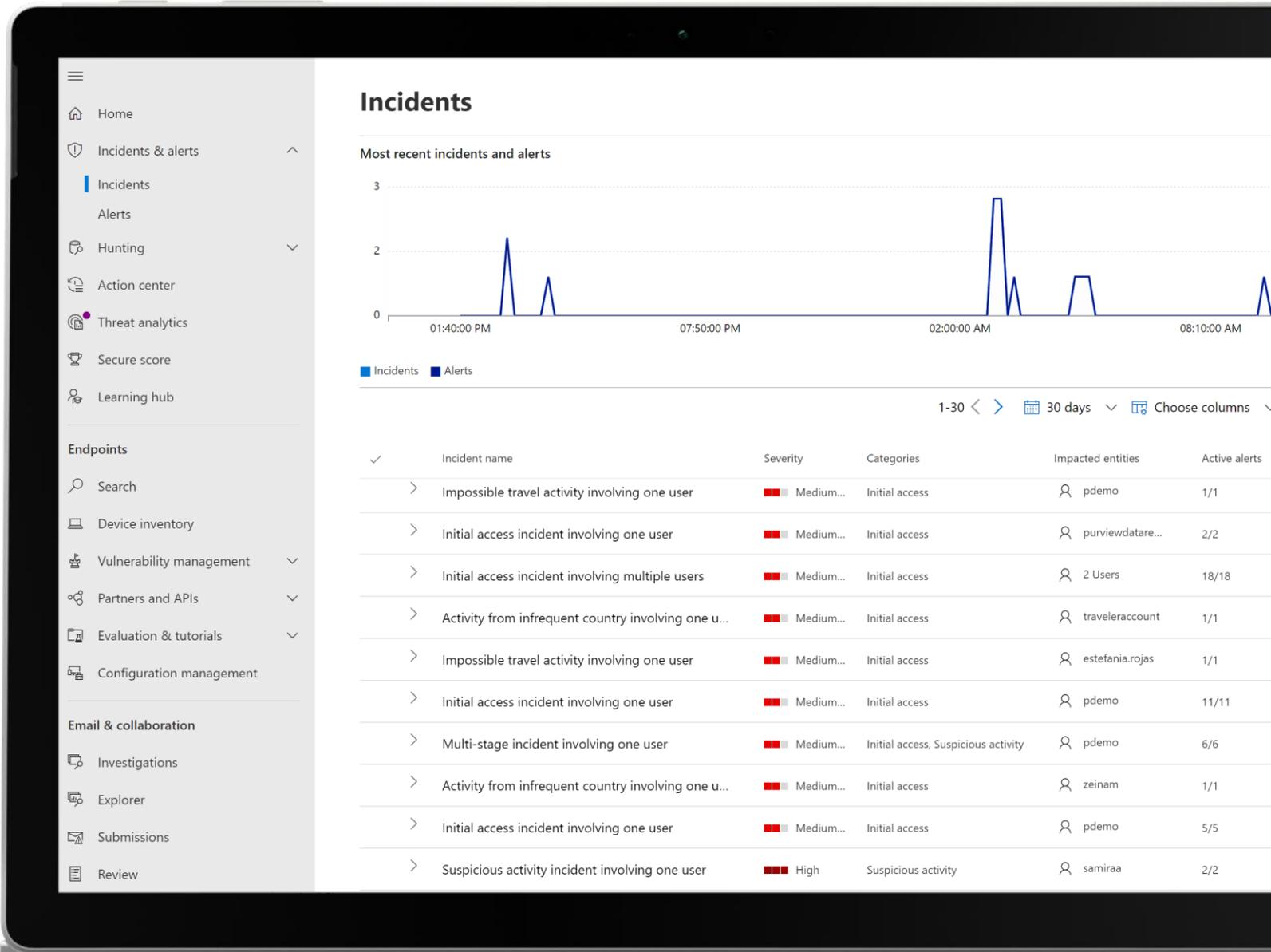
Response & Remediation

- Guided hunting with inline actions
- Centralized action queue
- Automated response playbooks



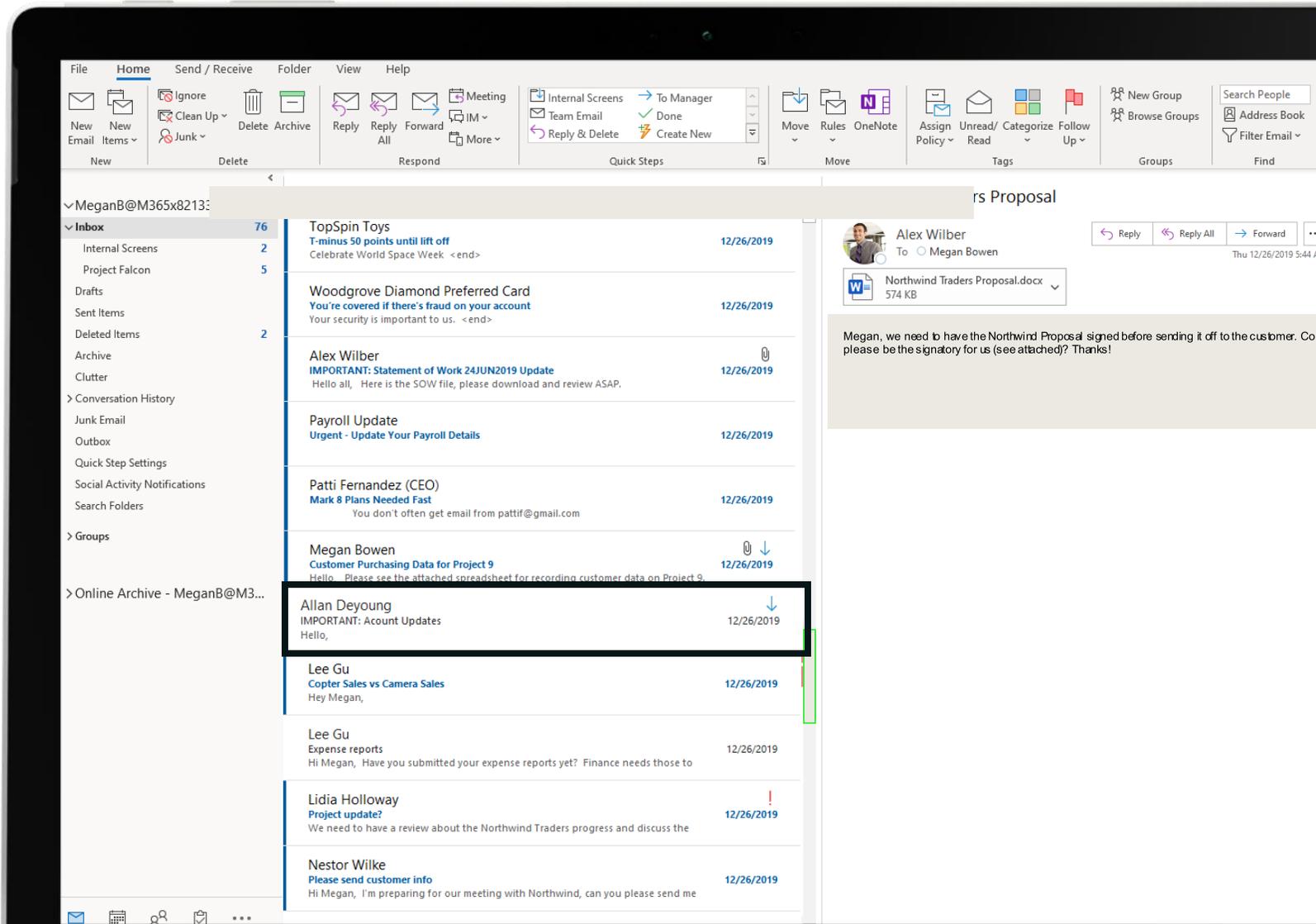
Response & Remediation

- Guided hunting with inline actions
- Centralized action queue
- Automated response playbooks
- Incidents



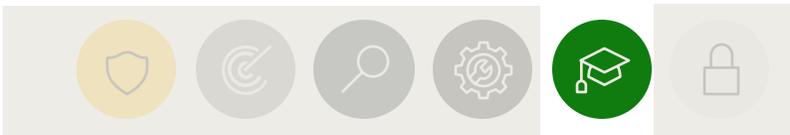
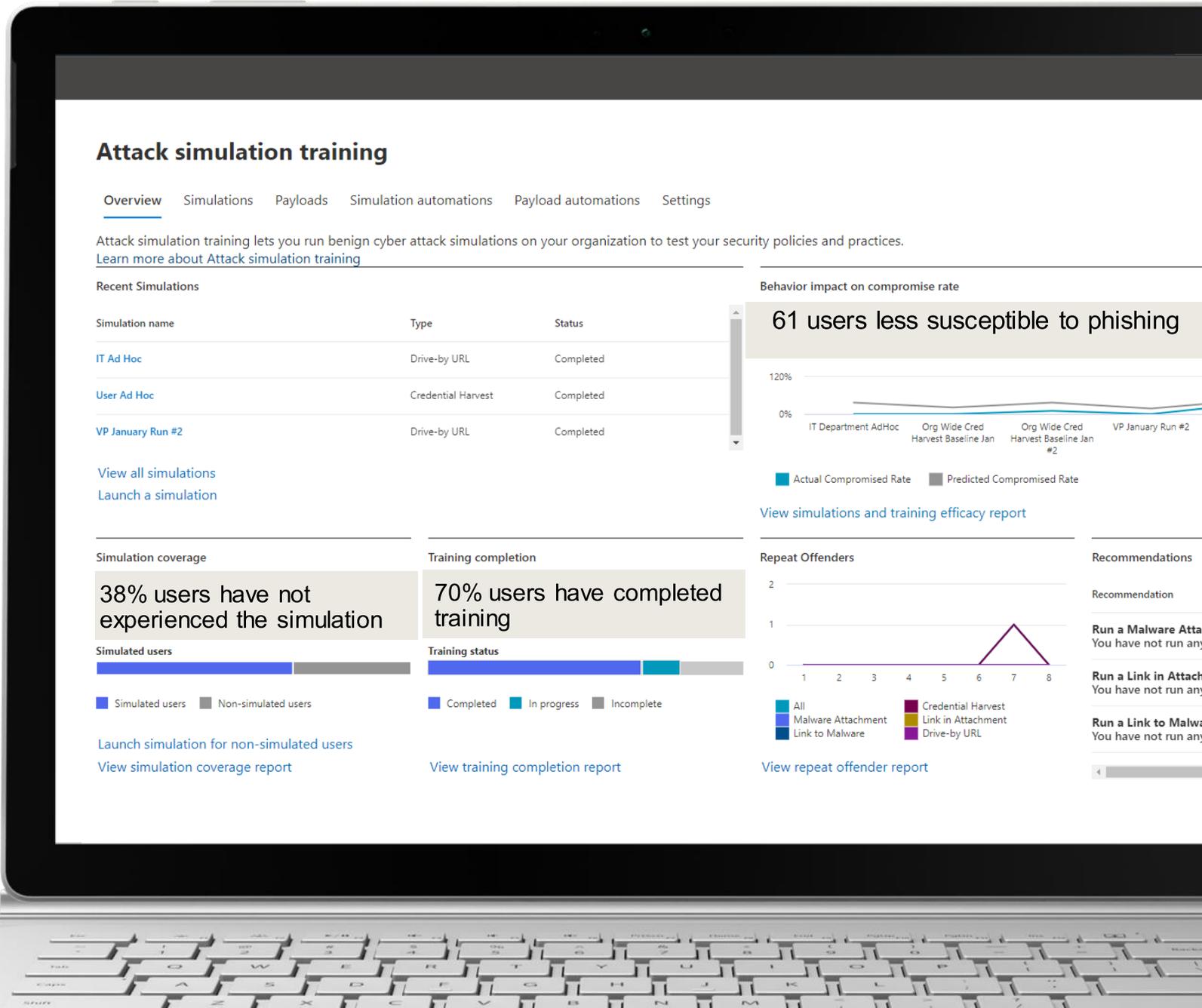
Response & Remediation

- Guided hunting with inline actions
- Centralized action queue
- Automated response playbooks
- Incidents
- Zero-Hour Auto-Purge (ZAP)



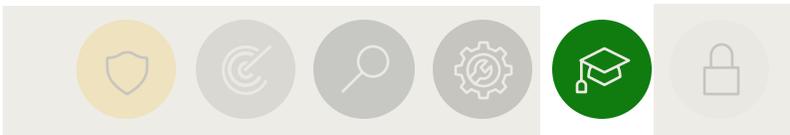
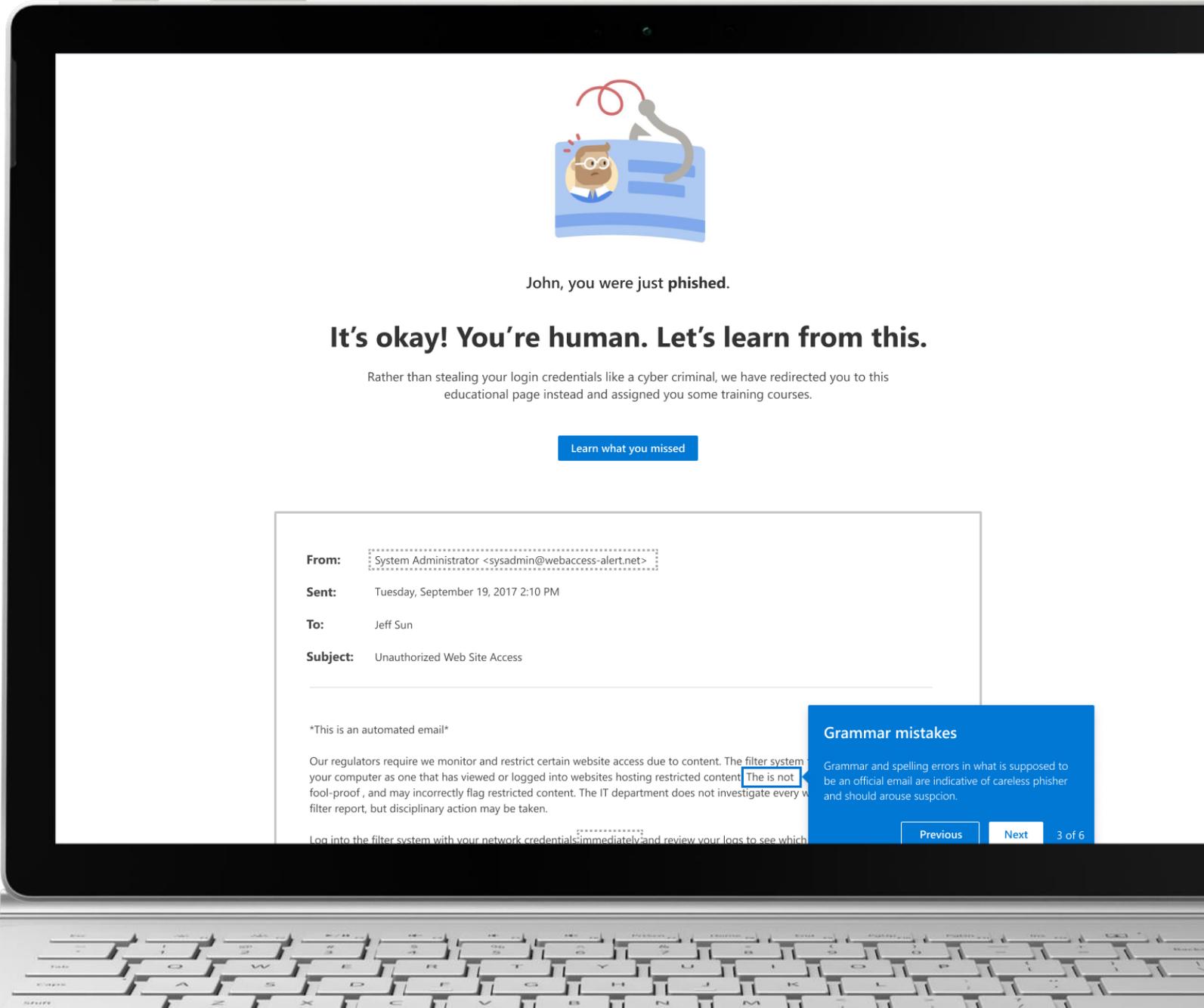
Awareness & Training

→ Enhanced simulation management



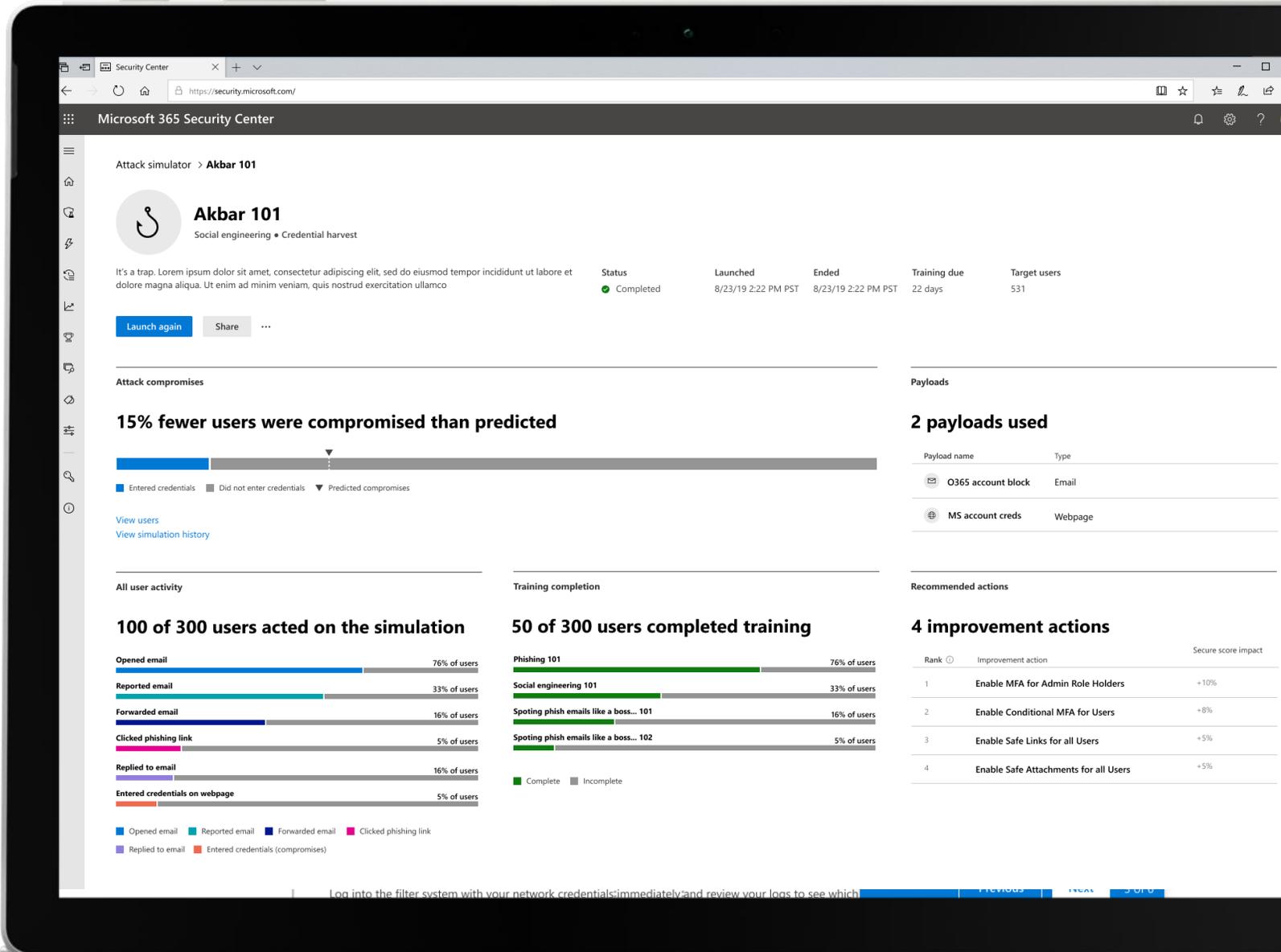
Awareness & Training

- Enhanced simulation management
- Dynamic end user training



Awareness & Training

- Enhanced simulation management
- Dynamic end user training
- Detailed reporting and insights



- Endpoints
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management
- Email & collaboration**
- Investigations
- Explorer
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training**
- Policies & rules
- Cloud apps
- Cloud discovery
- Cloud app catalog
- OAuth apps
- App governance
- Activity log
- Reports

Attack simulation training

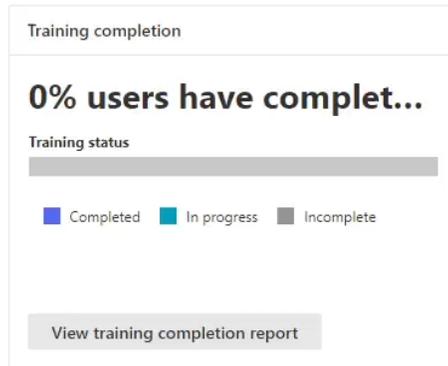
Overview Simulations Automations Content library Settings

Attack simulation training lets you run benign cyber attack simulations on your organization to test your security policies and practices. [Learn more about Attack simulation training](#)

Recent Simulations		
Simulation name	Type	Status
Cred Harvest	Credential Harvest	In progress
test	Malware Attachment	In progress
test	Malware Attachment	In progress

[View all simulations](#) [Launch a simulation](#)

Recommendations	
Recommendation	Action
Run a Drive-by URL simulation You have not run any recent simulations using this technique.	Launch now
Run a Link in Attachment simulation You have not run any recent simulations using this technique.	Launch now
Run a Link to Malware simulation You have not run any recent simulations using this technique.	Launch now



Home View

New email Delete Archive Report Sweep Move to Reply Reply all Forward Mark all as read

Favourites

- Inbox 1
- Sent Items
- Drafts
- Mark 8 Proj... 2
- Sales and ... 6
- Add favourite

Folders

- Inbox 1
- Drafts
- Sent Items
- Deleted I... 165
- Junk Email
- Archive
- Notes
- Conversation ...
- RSS Feeds
- Create new fol...

Groups

- U.S. Sales 1
- Digital Initia... 1

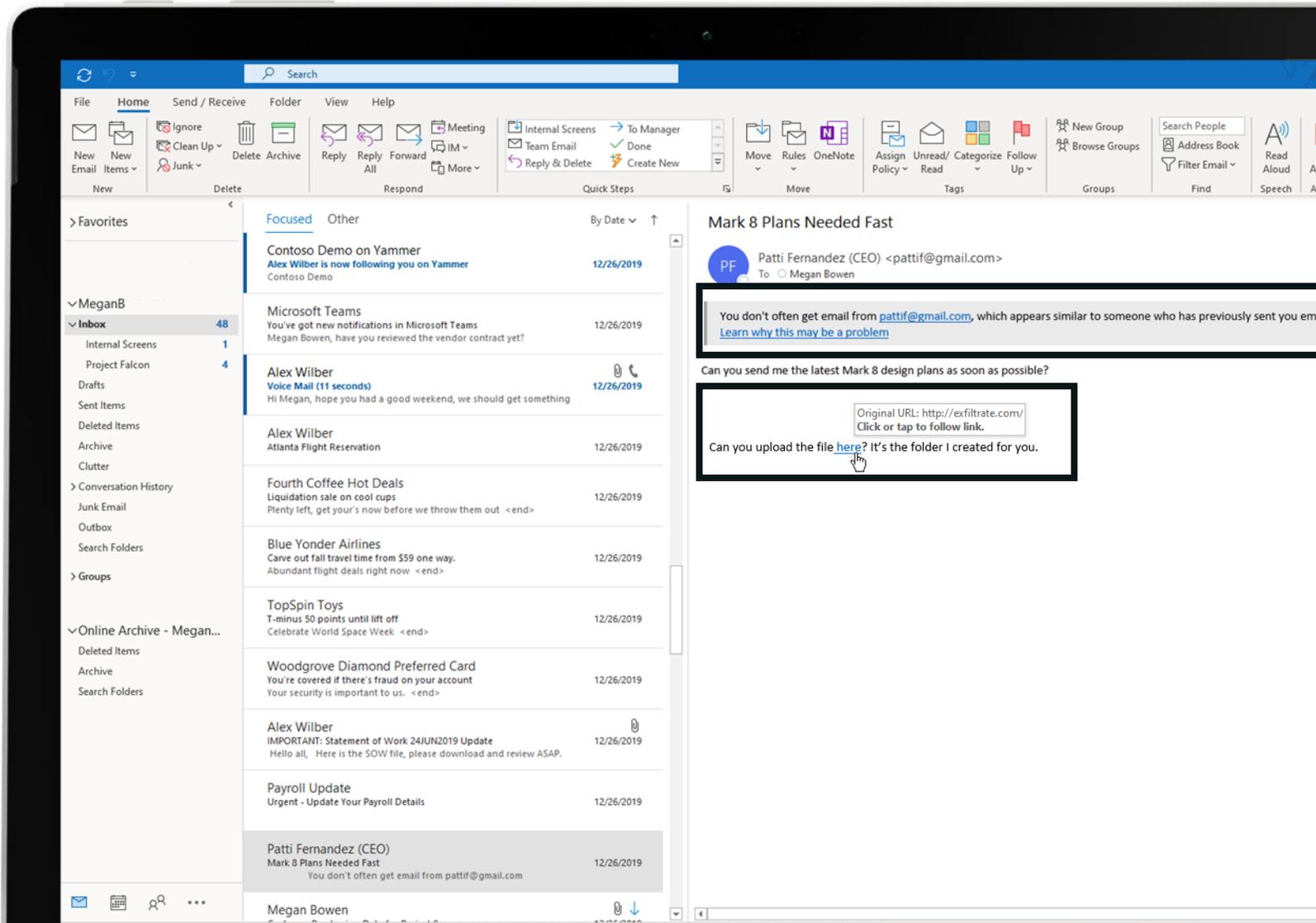
Focused Other Filter

- Microsoft email account activity notifi...
- Incoming emails quarantine... 7:32 PM
- Microsoft account Incoming email quar...

Select an item to read
Nothing is selected

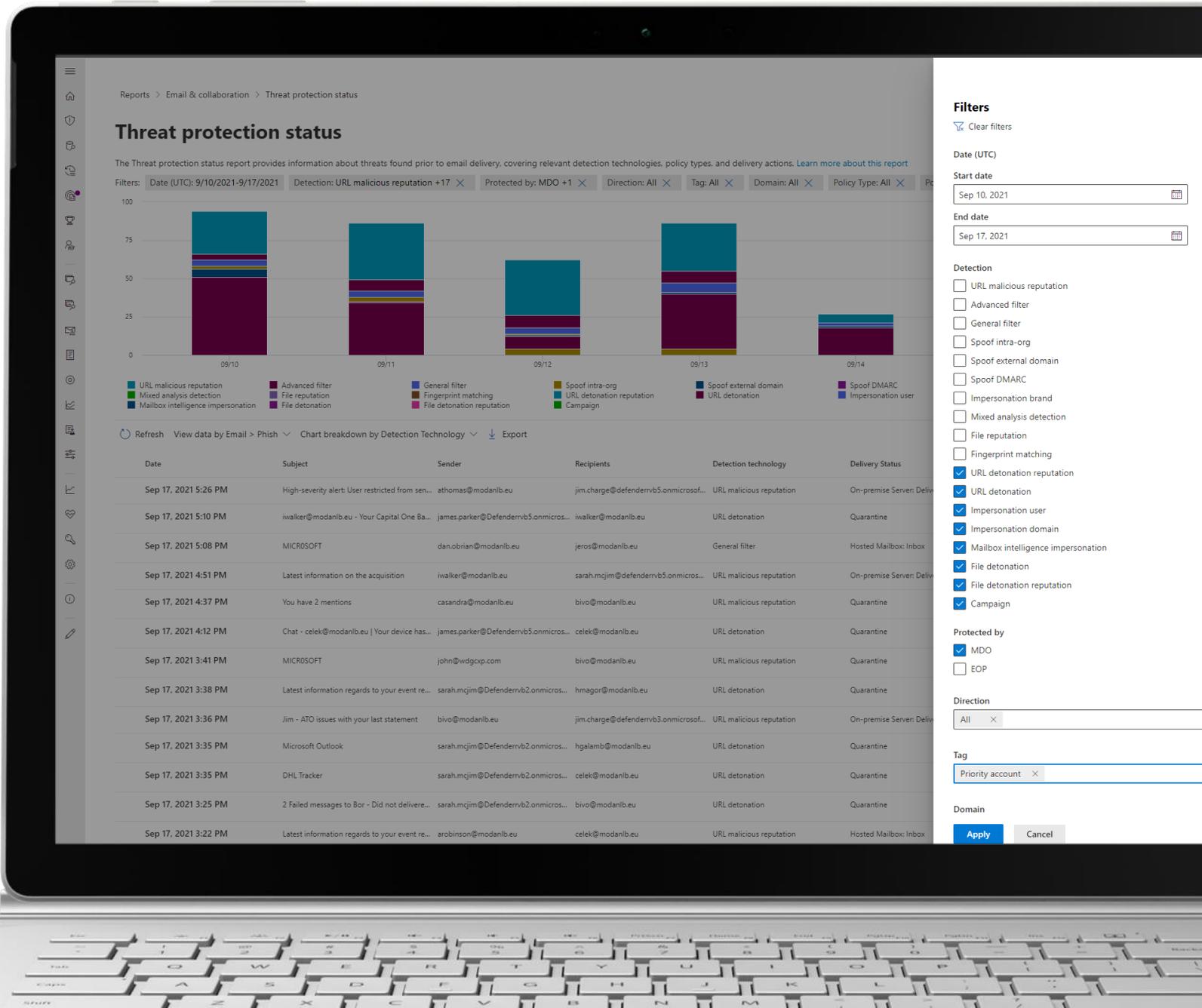
Awareness & Training

- Enhanced simulation management
- Dynamic end user training
- Detailed reporting and insights
- Native experiences foster user awareness



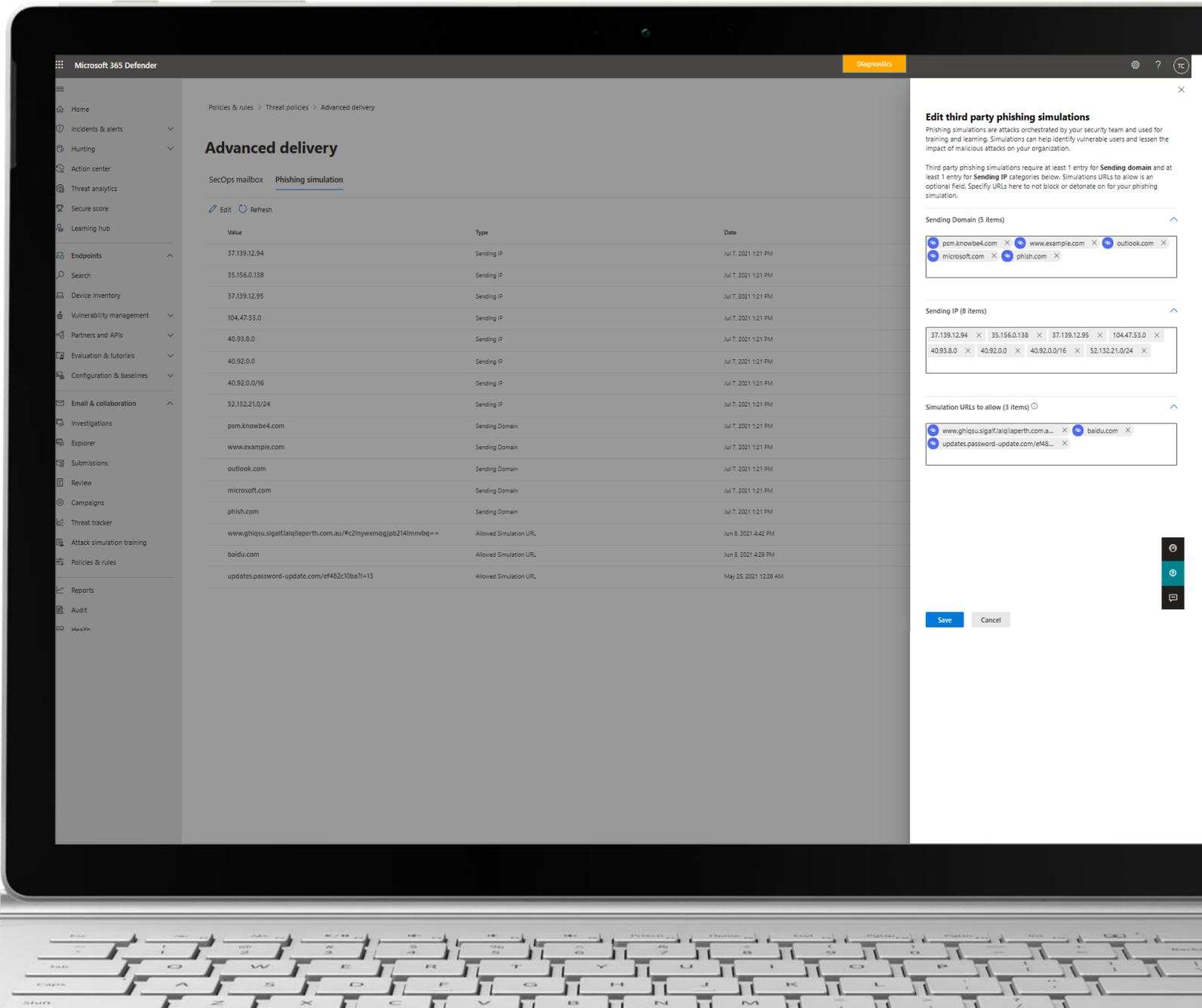
Secure Posture

→ Detailed reporting



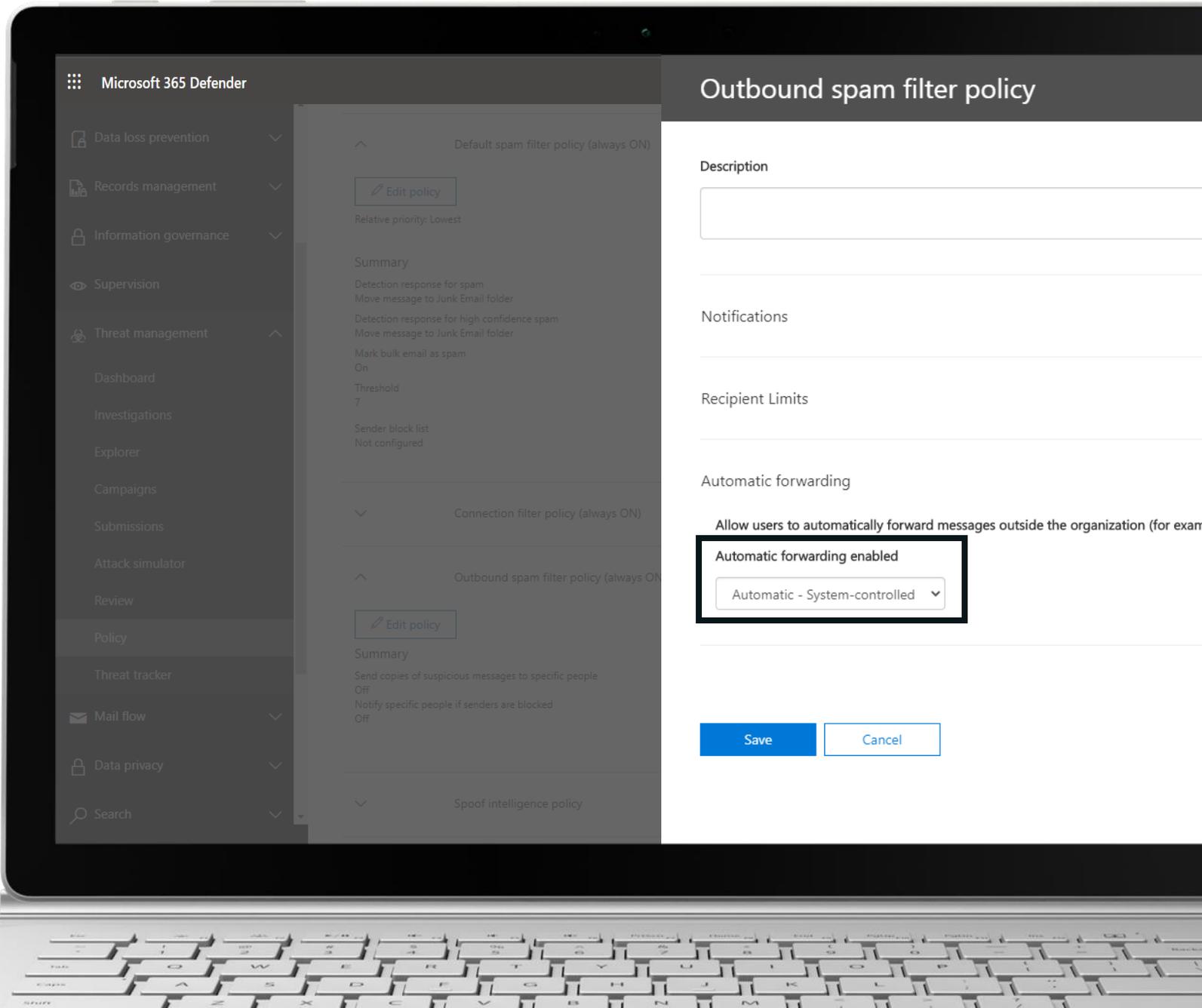
Secure Posture

- Detailed reporting
- Advanced Delivery for Phishing Simulations and Security Operation Mailboxes



Secure Posture

- Detailed reporting
- Advanced Delivery for Phishing Simulations and Security Operation Mailboxes
- Enhancing protection for our customers

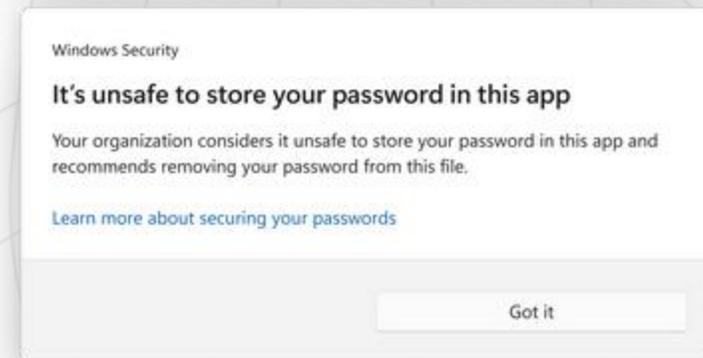
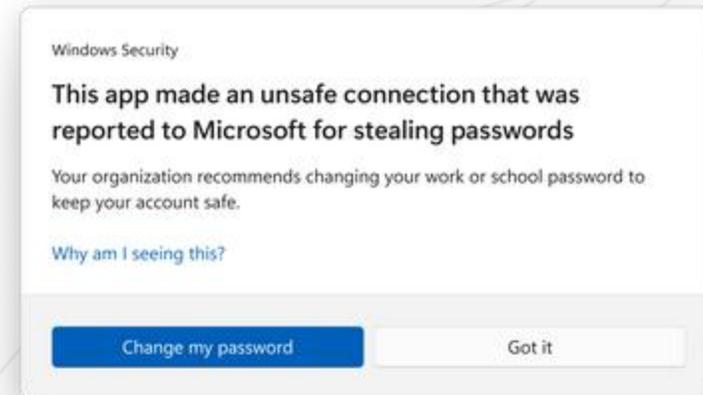


Enhanced Phishing Protection in Win11



- Enhanced phishing protection now baked into Windows 11
- Automatically detects when users type their password into any app or site. Windows understands in real-time whether that app or website has a secure connection to a trusted website; if not, Windows will let users know if they're in danger.
- SmartScreen identifies and protects against corporate password entry on reported phishing sites or apps connecting to phishing sites, password reuse on any app or site, and passwords typed into Notepad, Wordpad, or Microsoft 365 apps
- Automatically reports unsafe password usage to IT through the MDE portal
- Configured in MDM/CSP or Group Policy
- Relies on SmartScreen and Chromium Browser
- Requires Windows 11 version 22H2

Find out more: <https://techcommunity.microsoft.com/t5/windows-it-pro-blog/protect-passwords-with-enhanced-phishing-protection/ba-p/3631881>



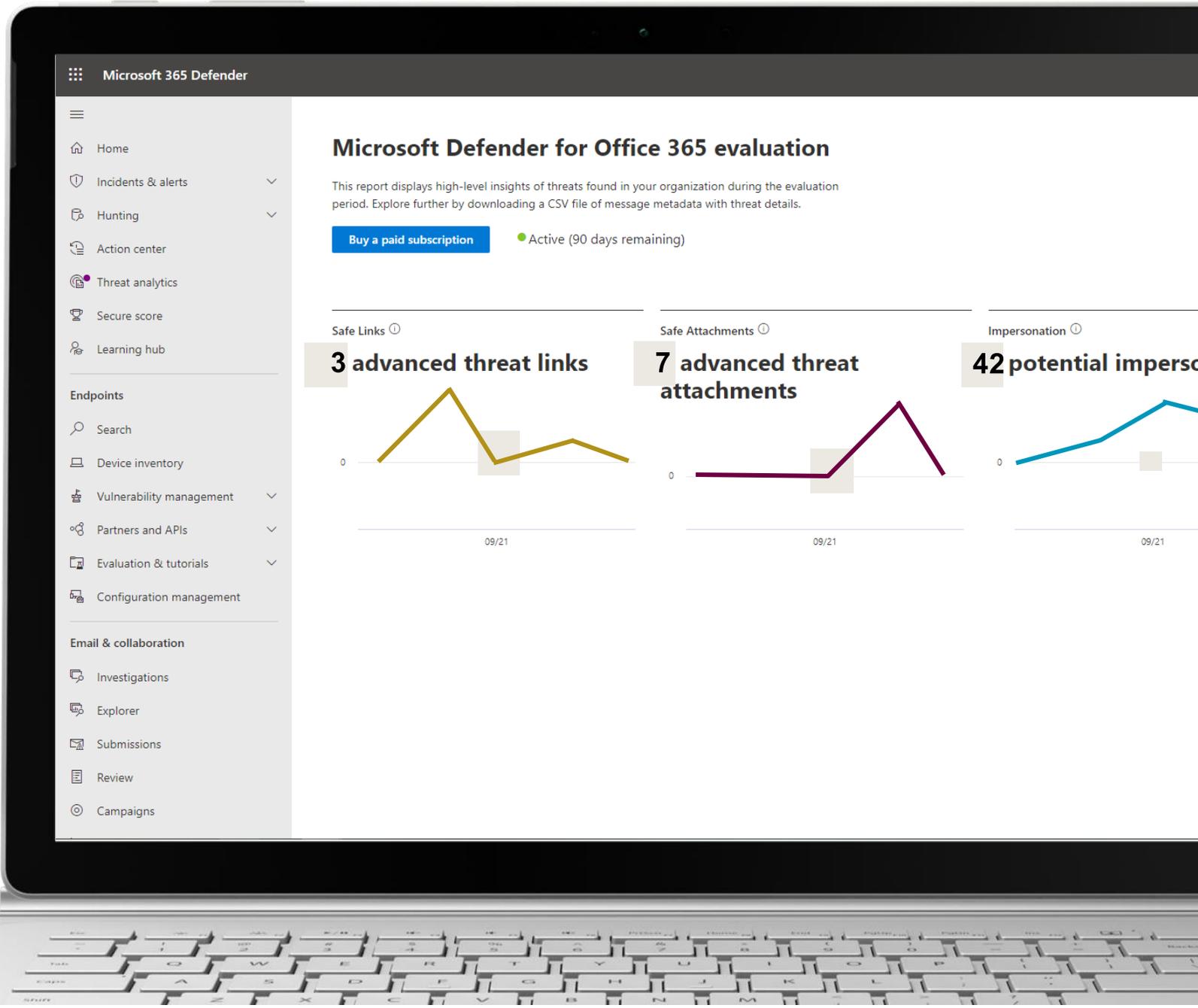
Microsoft Defender for Office 365

Securing your enterprise requires more than just prevention



Evaluation Mode

- Does not require changes to MX record
- Policies can be enabled in enforcement OR non-enforcement mode
- Investigate using Threat Explorer & Campaign Views
- Evaluation report updated daily for 90 days can help assess effectiveness



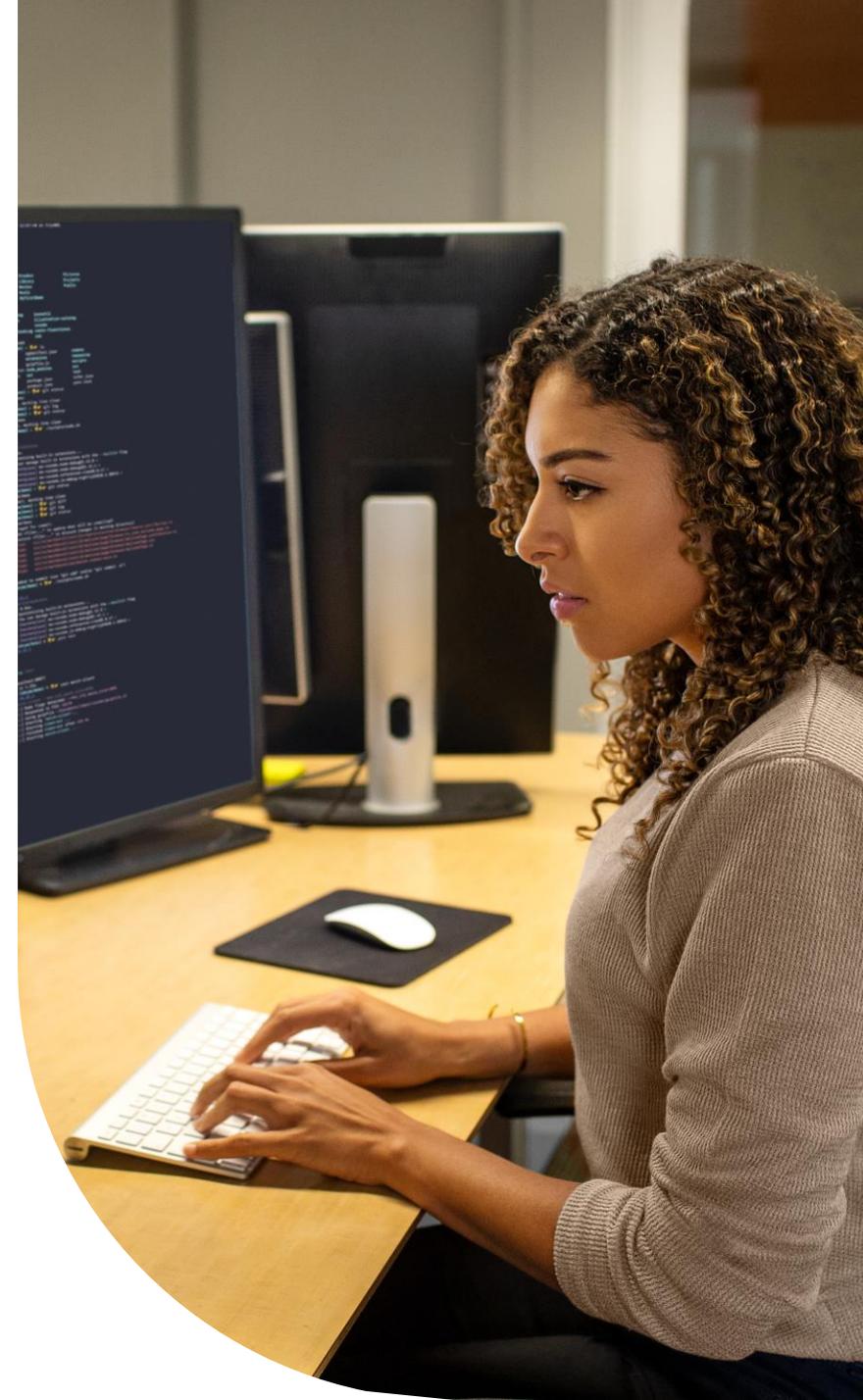
Next Steps & Resources

Arrange a Vision Call to discuss....

- Proof of concepts / Evaluations (90 day trial available)
- Funded Microsoft workshops
- Security Posture Assessments
- Your requirements

Learn more

- Product page: <https://aka.ms/DefenderO365>
- Blog: <https://aka.ms/MDOblog>
- Documentation: <https://aka.ms/MDOdocs>
- Defender for Office 365 – Sec Ops Guide: <http://aka.ms/opmdo>
- Microsoft Defender for Office 365 – SE Labs Evaluation: <https://www.microsoft.com/security/blog/2022/06/22/microsoft-defender-for-office-365-receives-highest-award-in-se-labs-enterprise-email-security-services-test/>





Thank you

→ Any questions?