Kocho
BECOME GREATER

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

The threat landscape continues to evolve

Correlation of signals is time-consuming and expensive

Disparate solutions cause inefficiencies

Current threat landscape

91%

Cyberattacks that start with email[1]

30,720

Domains generated by criminals every three days[2]

$1.8B

Loss attributed to business email compromise in 2020 alone[3]

168K

Phishing sites taken down by Microsoft in 2021[2]

[1]Verizon Data Breach Investigations Report | [2]Microsoft 2021 Digital Defense Report Learn More | [3]US 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 Wave[1]

SecOps efficiency and cost savings

Total Economic Impact study of moving from a competitor to Defender for Office 365[2]

Improved blocking of malicious links by **95%**

Improved investigation time by **92%**

Reduced risk of breach by **29%**

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

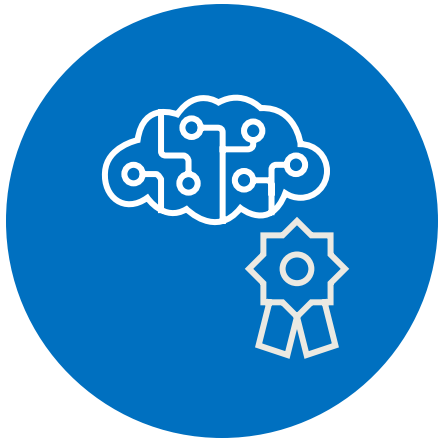
Share

SE labs – Microsoft Defender for Office 365 receives highest award in SE labs Enterprise Email Security Services Test Q1 2022 Learn more

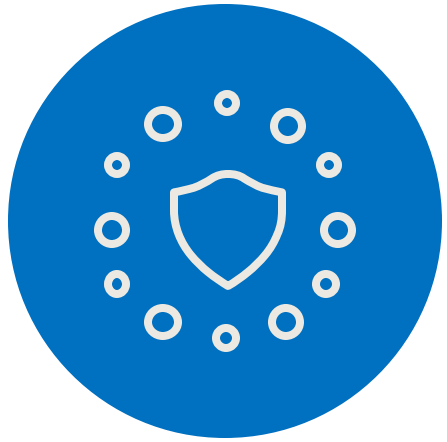
Why Microsoft?

Our unique advantages.

Native protection
for Office 365



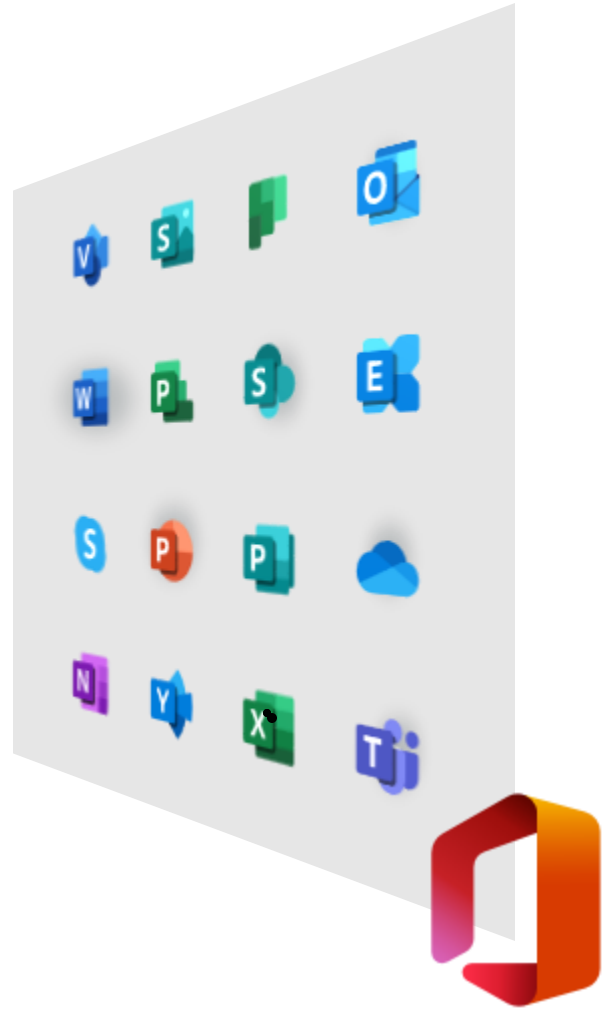
Industry-leading AI
and automation



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

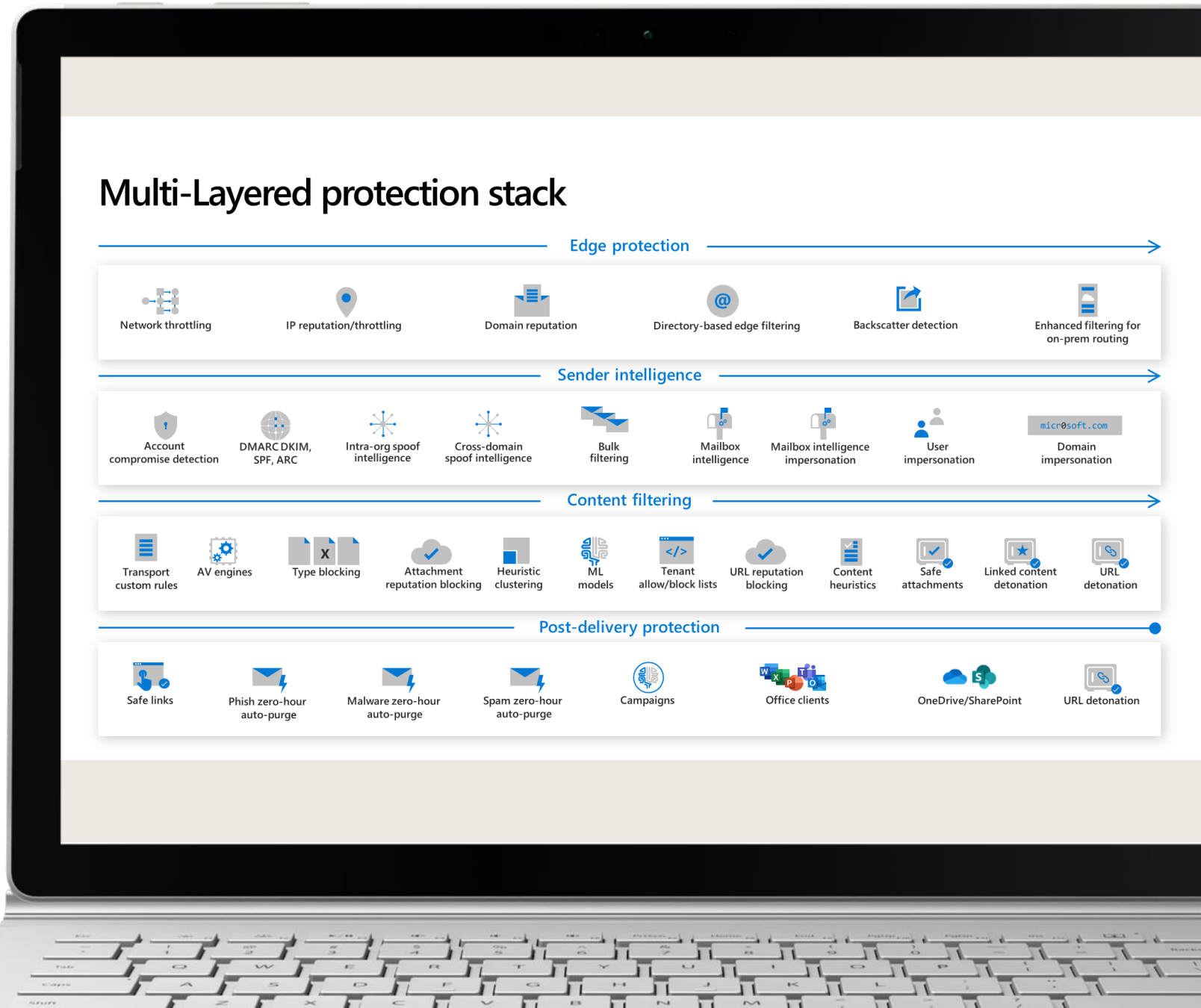
Microsoft Sentinel

Microsoft Defender for Office 365

Securing your enterprise requires more than just prevention

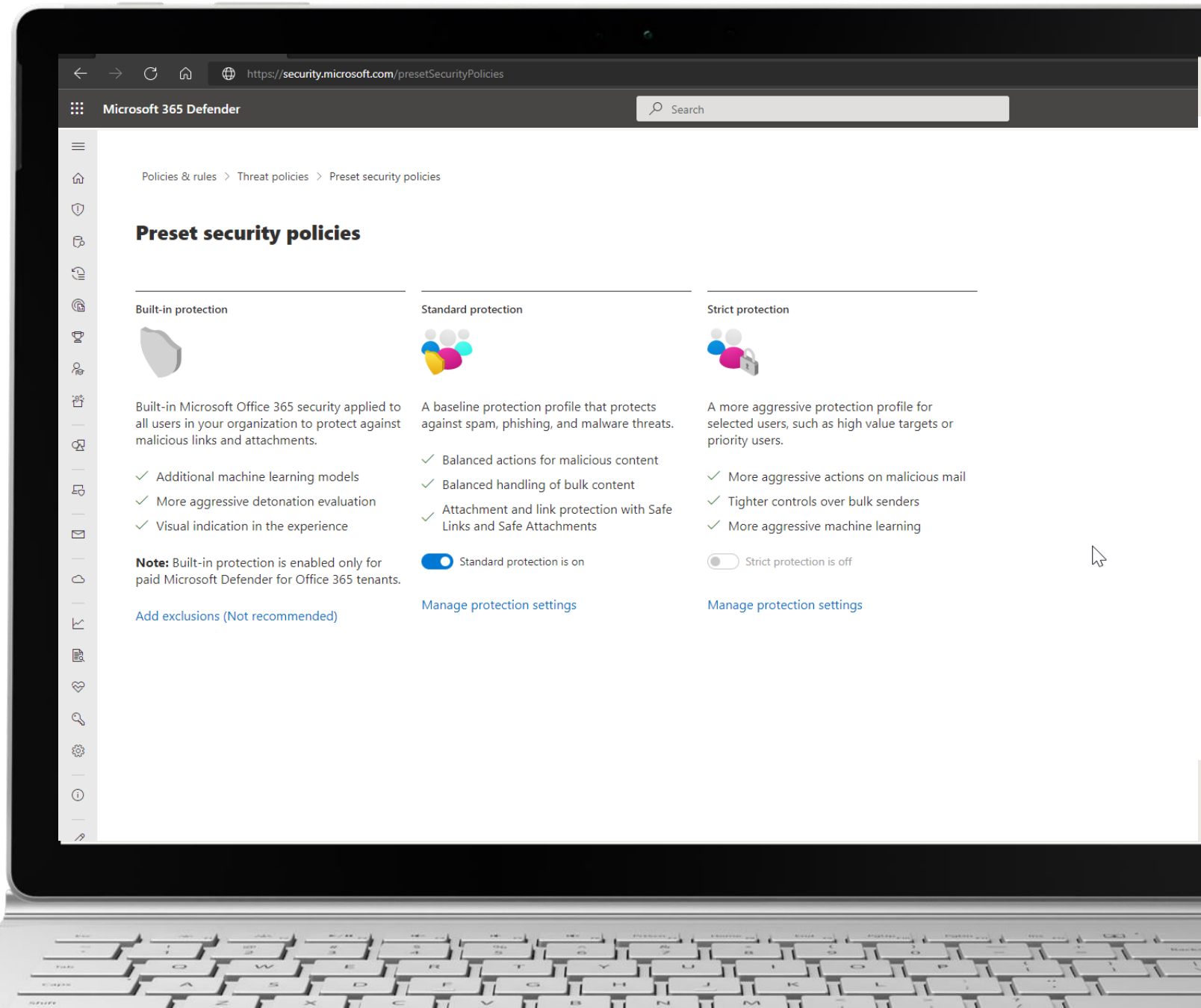
Prevention

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



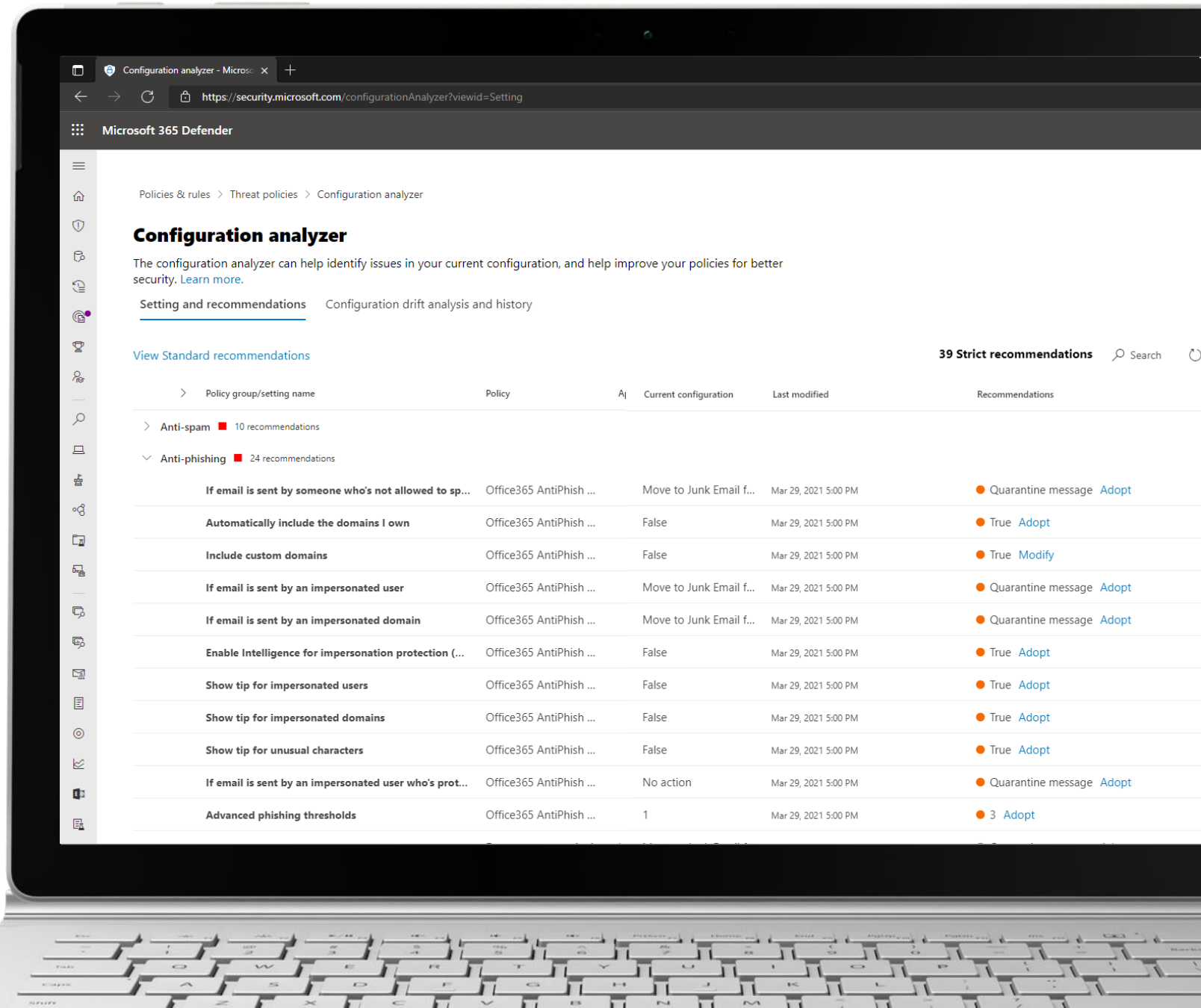
Prevention

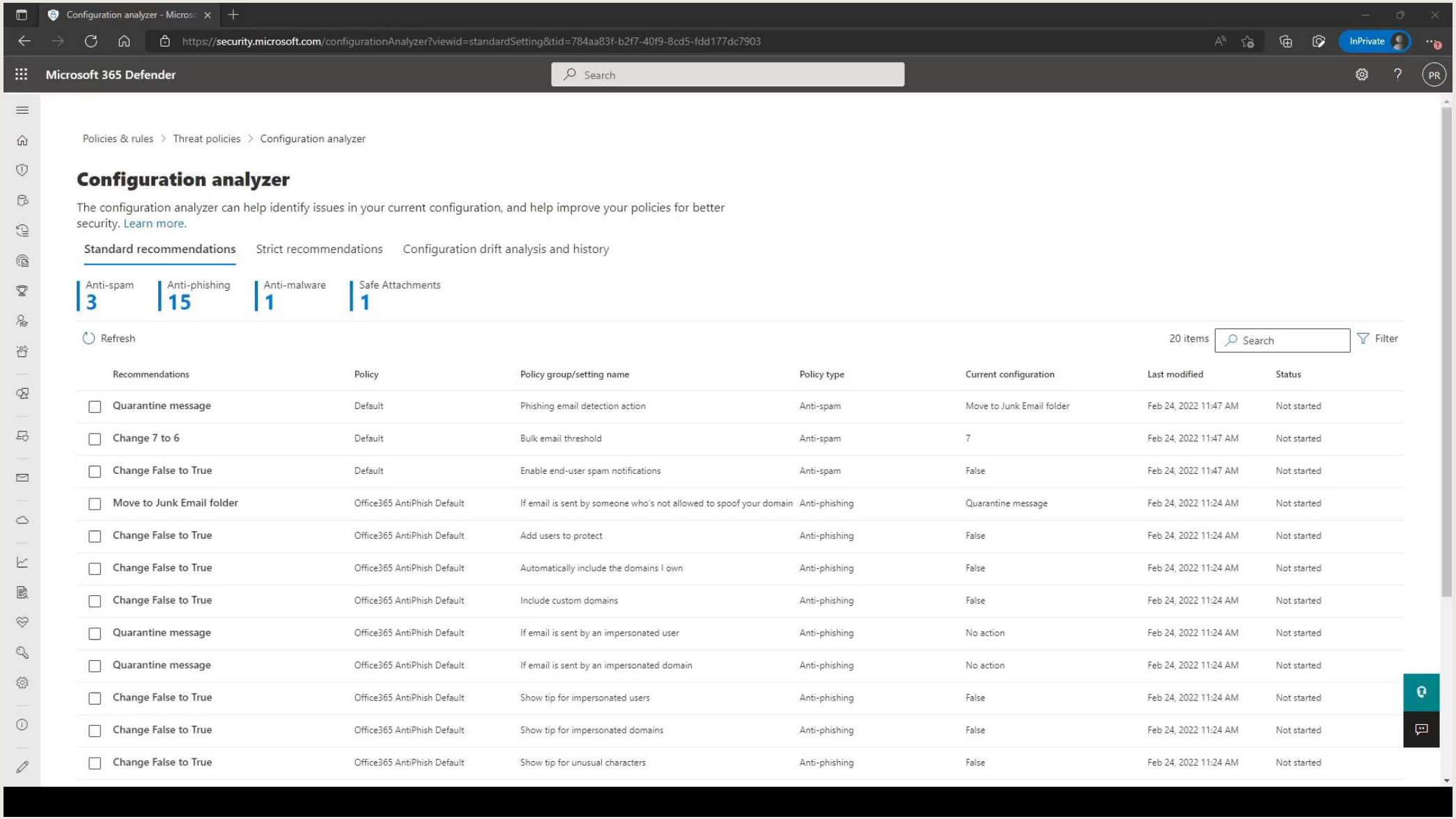
- Multi-layered protection stack stops a wide variety of attacks
- Simplified configuration guidance



Prevention

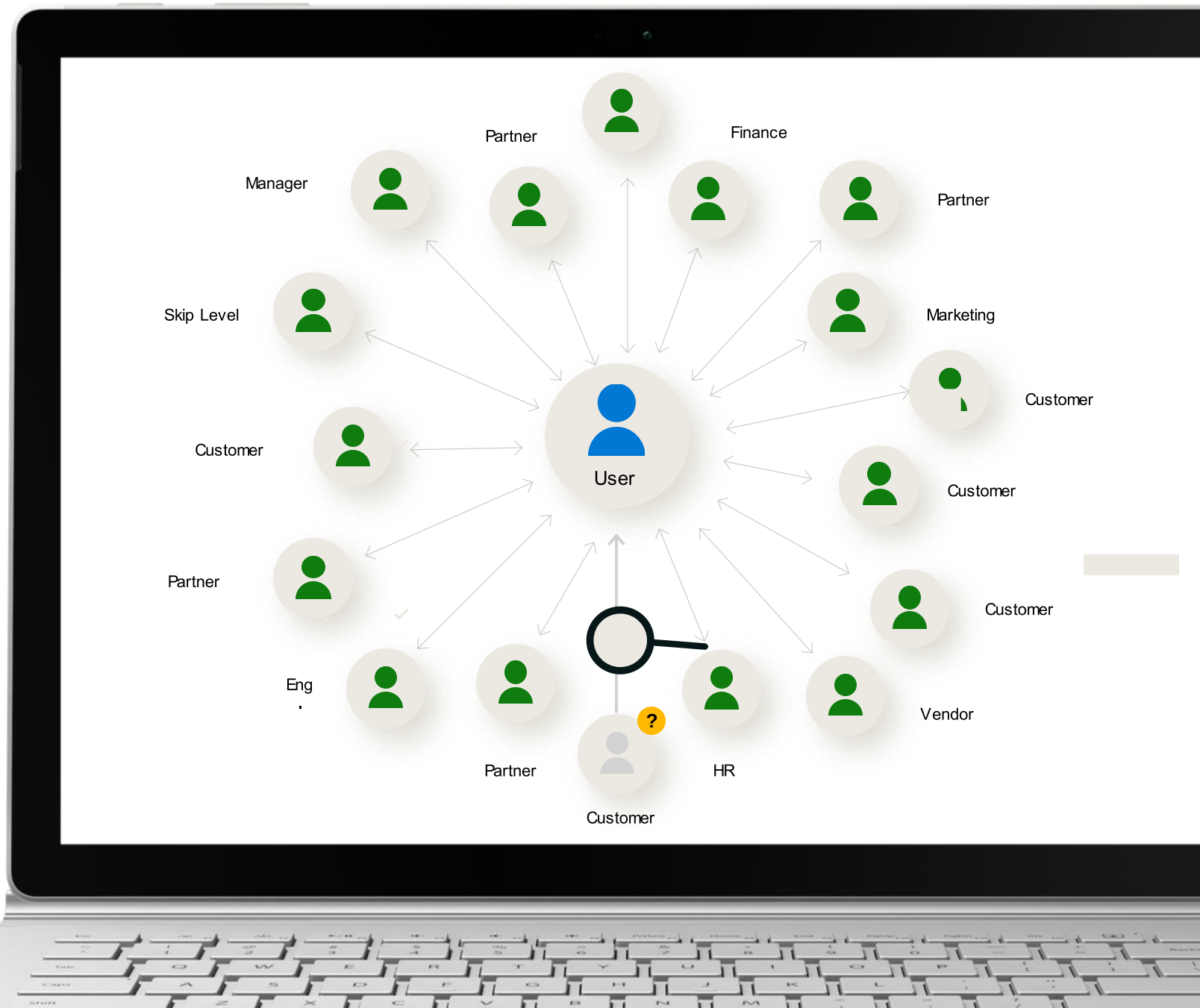
- Multi-layered protection stack stops a wide variety of attacks
- Simplified configuration guidance




Configuration analyzer - Microsc
https://security.microsoft.com/configurationAnalyzer?viewid=standardSetting&tid=784aa83f-b2f7-40f9-8cd5-fdd177dc7903
InPrivate
Microsoft 365 Defender
Search
PR
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
Search
Filter
Recommendations | Policy | Policy group/setting name | Policy type | Current configuration | Last modified | Status
Quarantine message | Default | Phishing email detection action | Anti-spam | Move to Junk Email folder | Feb 24, 2022 11:47 AM | Not started
Change 7 to 6 | Default | Bulk email threshold | Anti-spam | 7 | Feb 24, 2022 11:47 AM | Not started
Change False to True | Default | Enable end-user spam notifications | Anti-spam | False | Feb 24, 2022 11:47 AM | Not started
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
Change False to True | Office365 AntiPhish Default | Add users to protect | Anti-phishing | False | Feb 24, 2022 11:24 AM | Not started
Change False to True | Office365 AntiPhish Default | Automatically include the domains I own | Anti-phishing | False | Feb 24, 2022 11:24 AM | Not started
Change False to True | Office365 AntiPhish Default | Include custom domains | Anti-phishing | False | Feb 24, 2022 11:24 AM | Not started
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
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
Change False to True | Office365 AntiPhish Default | Show tip for impersonated users | Anti-phishing | False | Feb 24, 2022 11:24 AM | Not started
Change False to True | Office365 AntiPhish Default | Show tip for impersonated domains | Anti-phishing | False | Feb 24, 2022 11:24 AM | Not started
Change False to True | Office365 AntiPhish Default | Show tip for unusual characters | Anti-phishing | False | Feb 24, 2022 11:24 AM | Not started

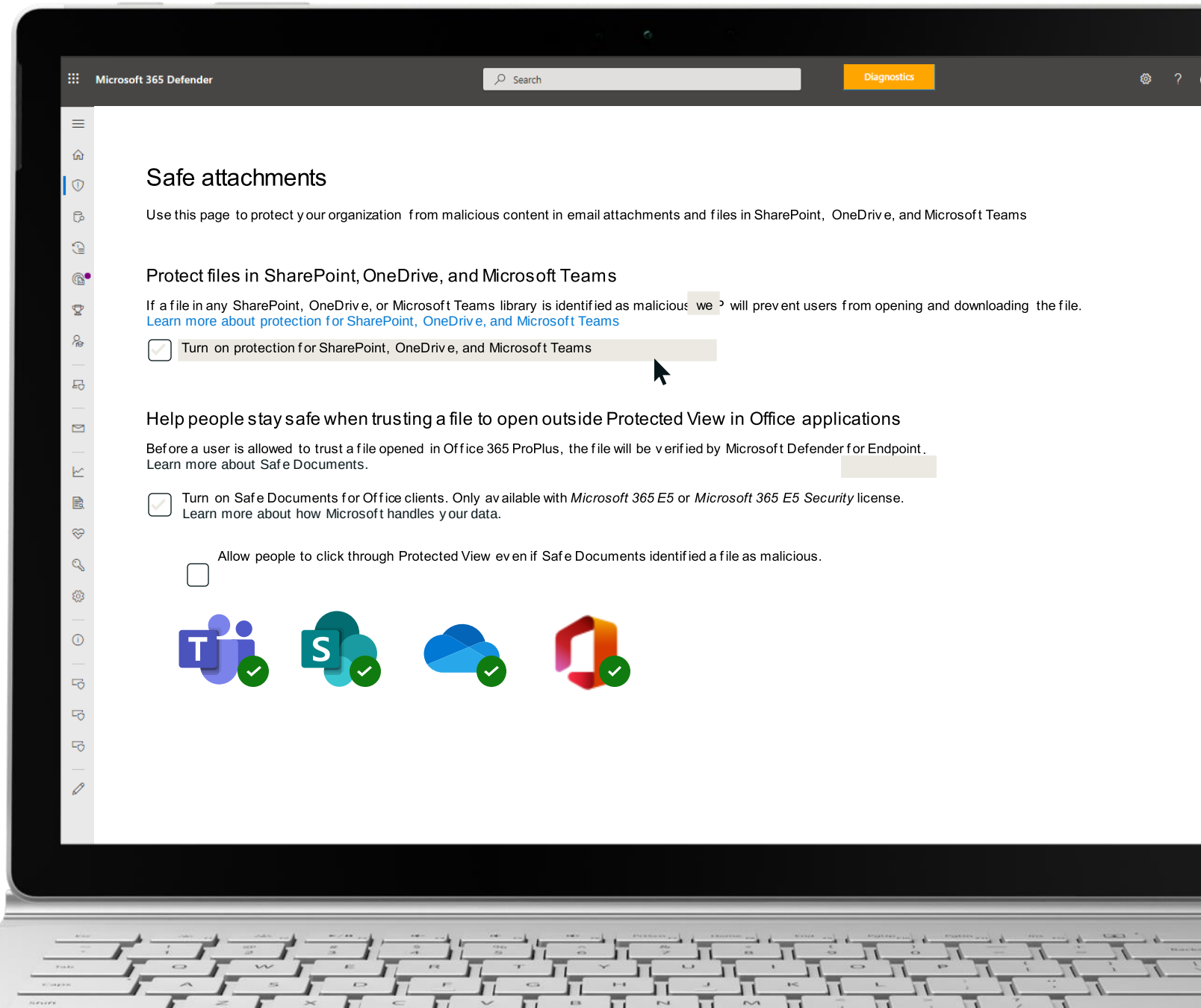
Prevention

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



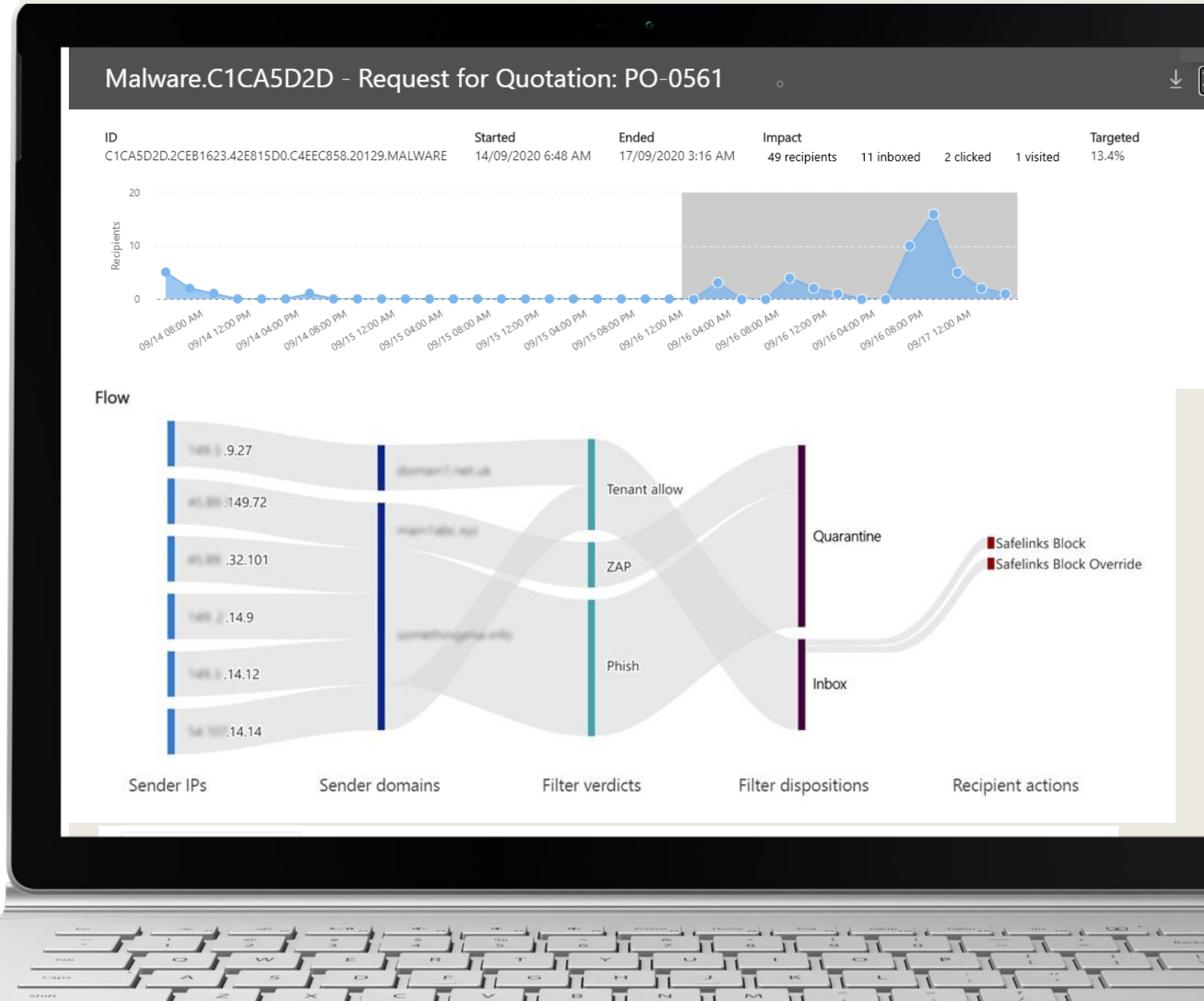
Prevention

- 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



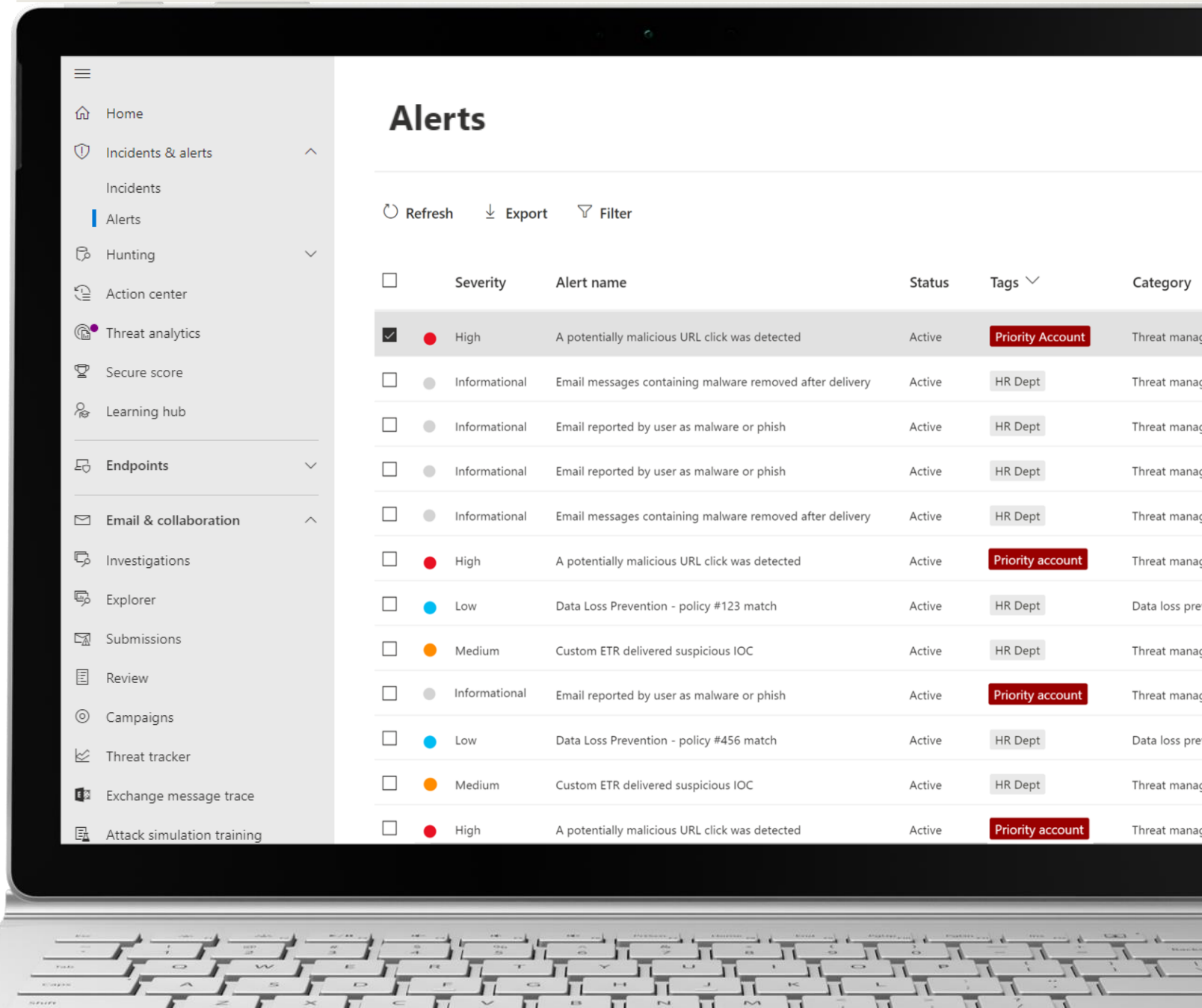
Detection

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



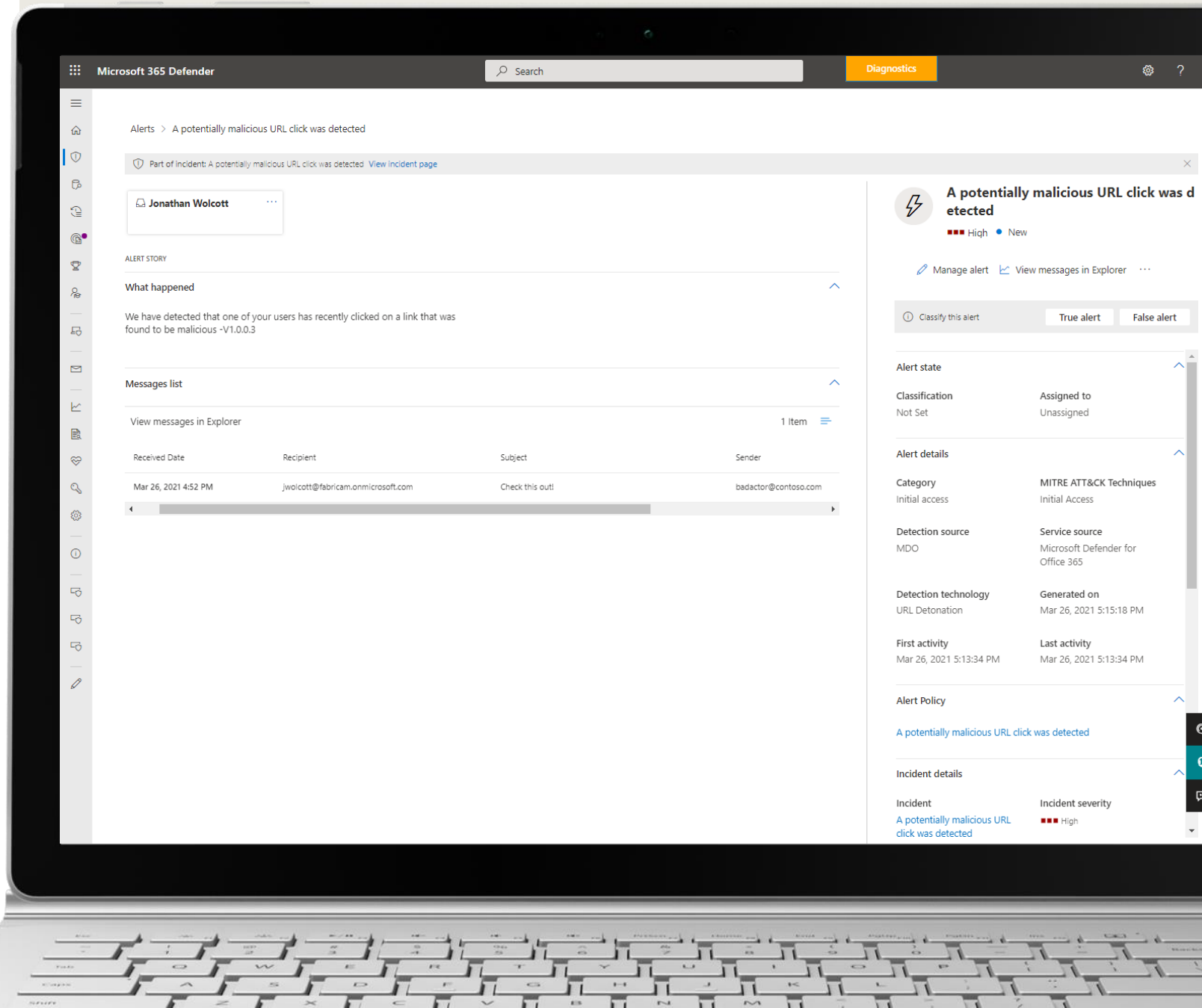
Detection

- Campaign Views leverage AI to surface coordinated attacks designed to evade detection
- Detailed alerts



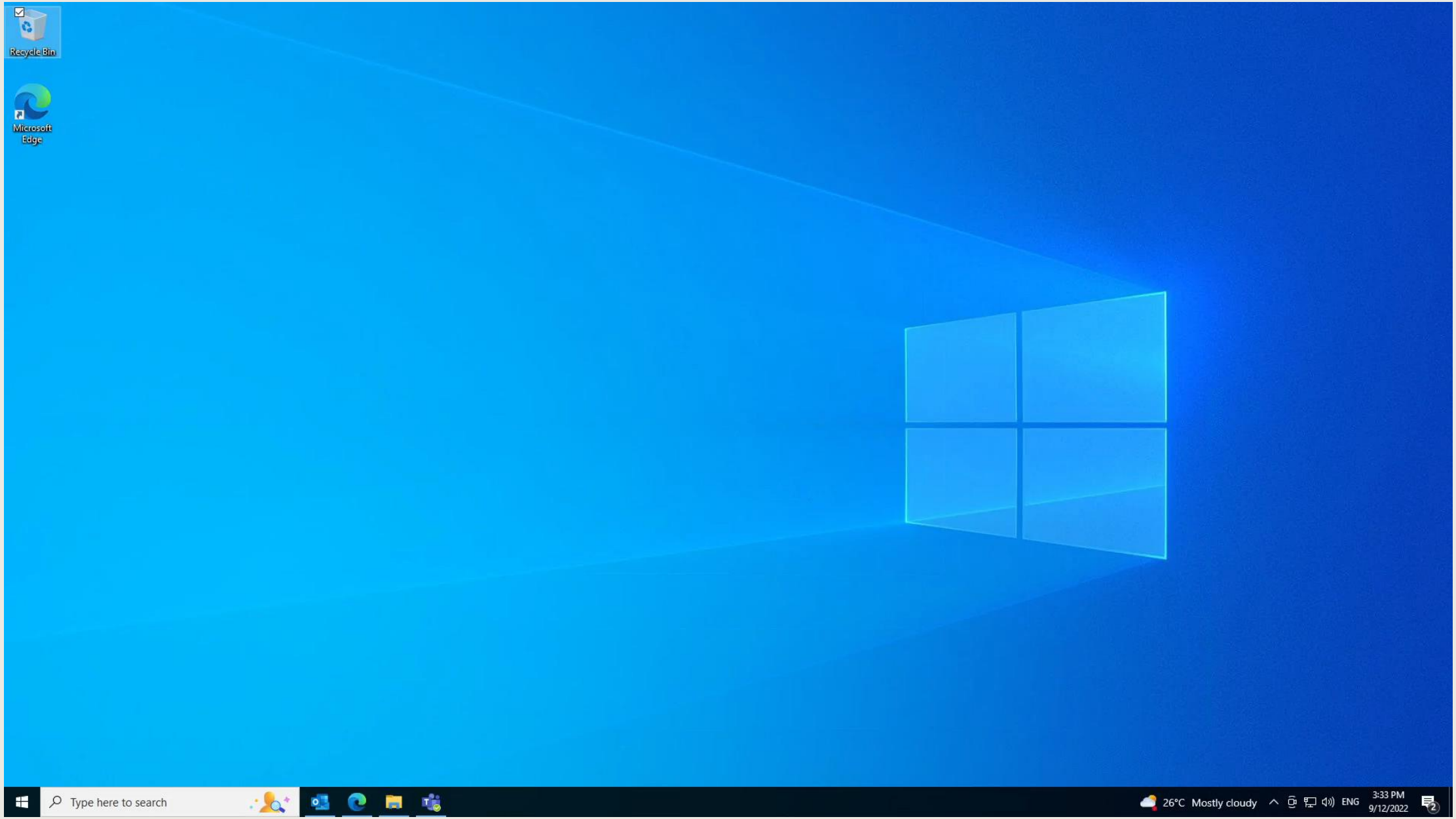
Detection

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



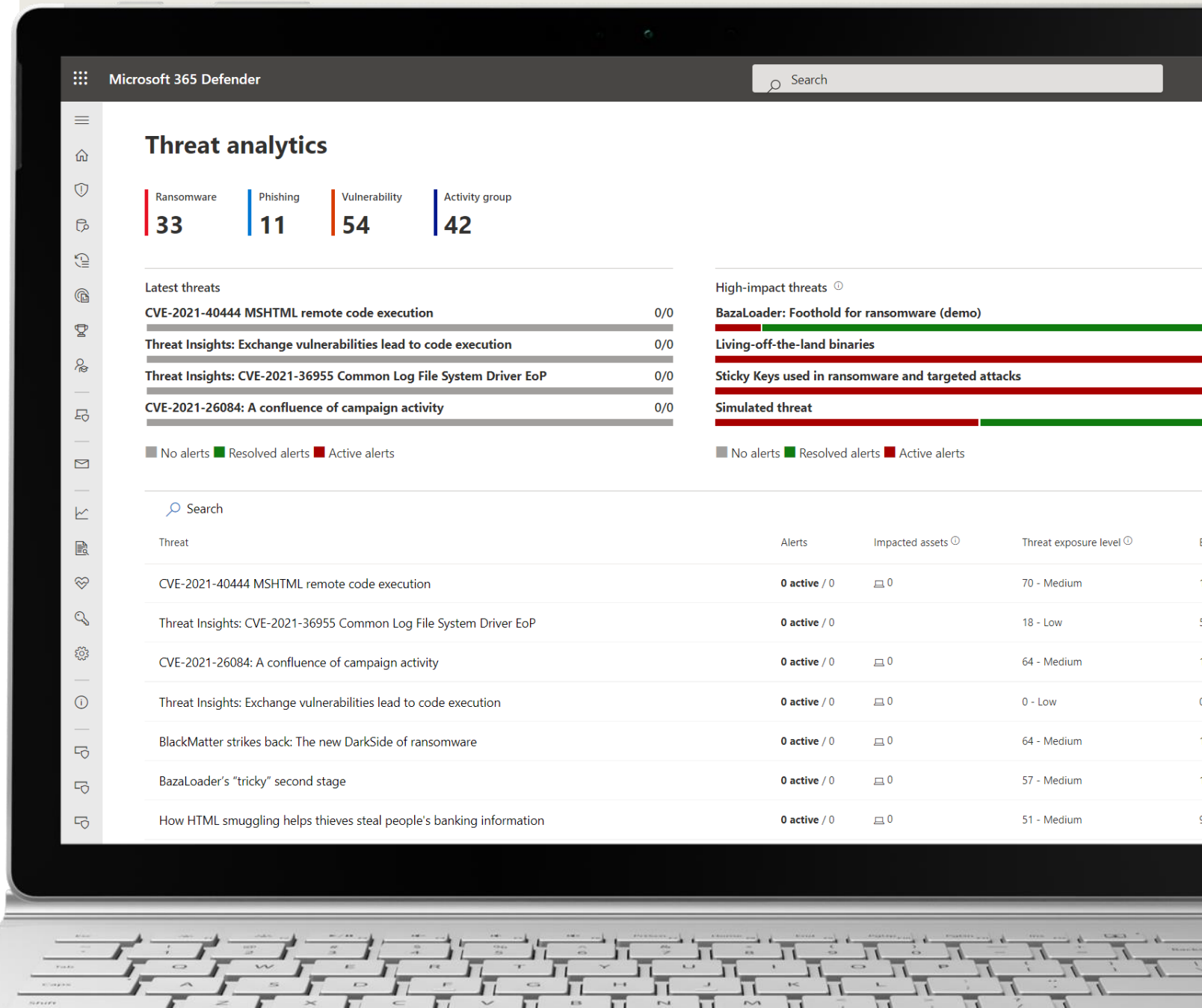
Protection Demo

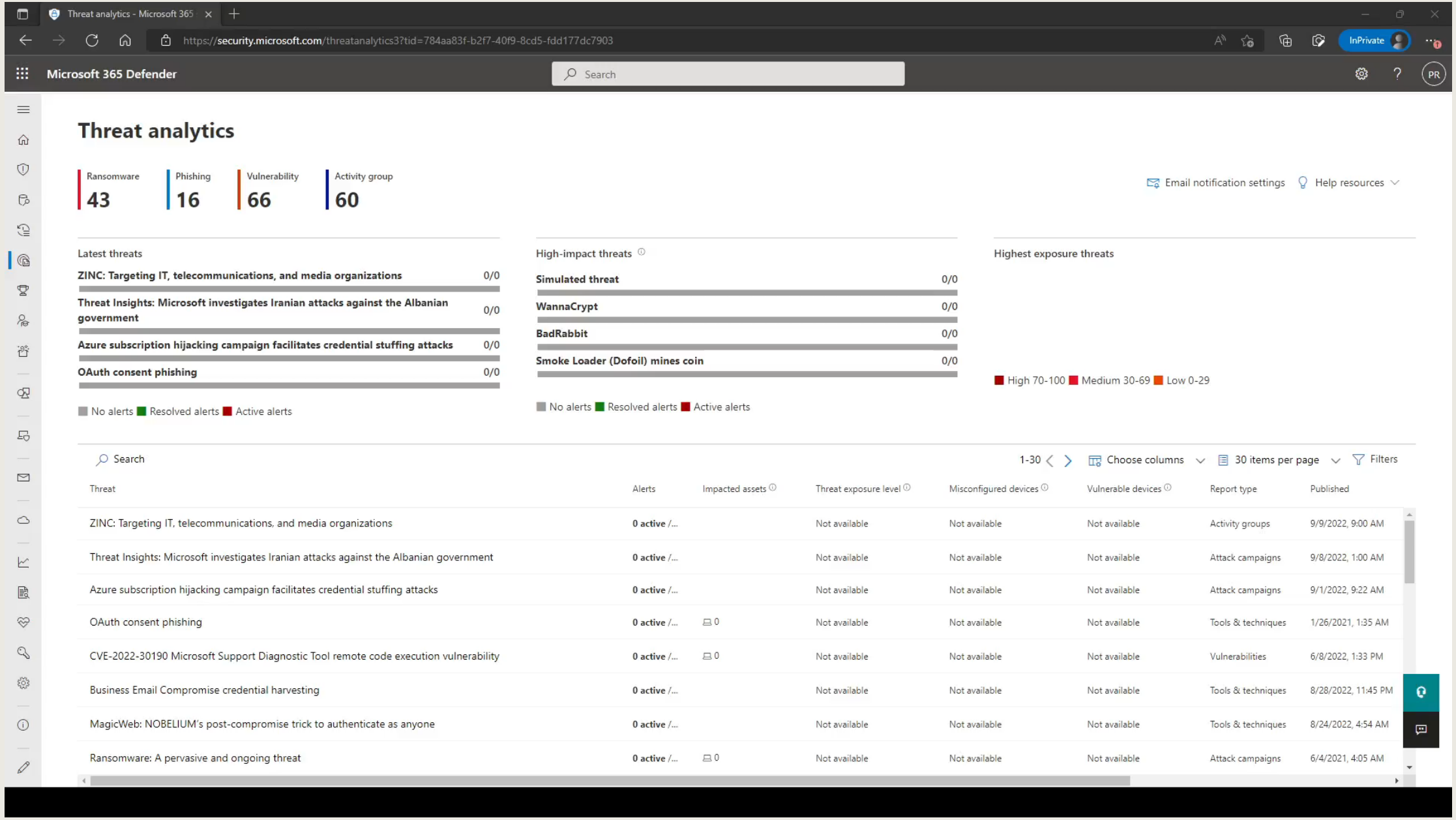
→ End User Experience

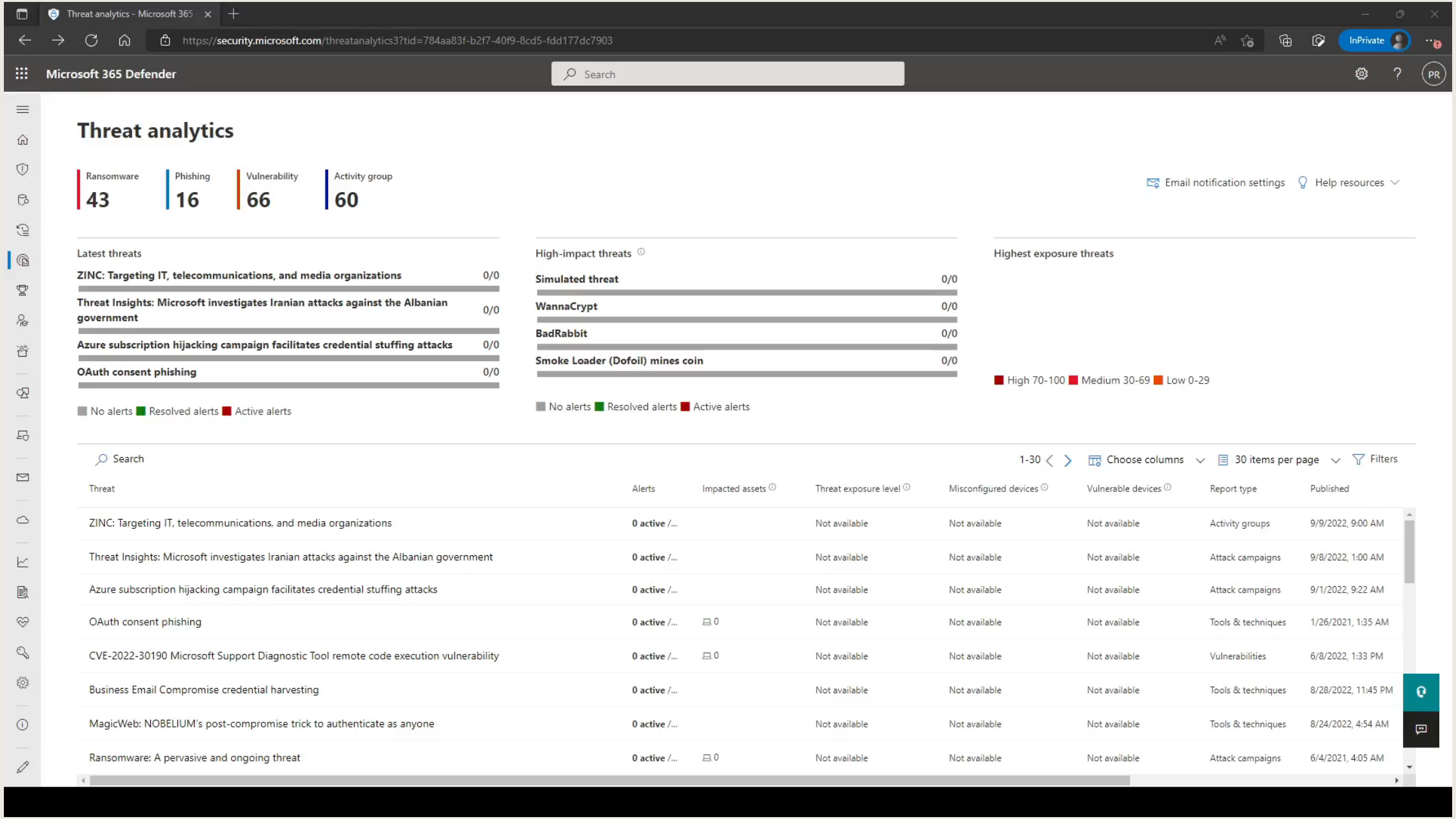

Recycle Bin
Microsoft Edge
Type here to search
26°C Mostly cloudy
ENG
3:33 PM
9/12/2022

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

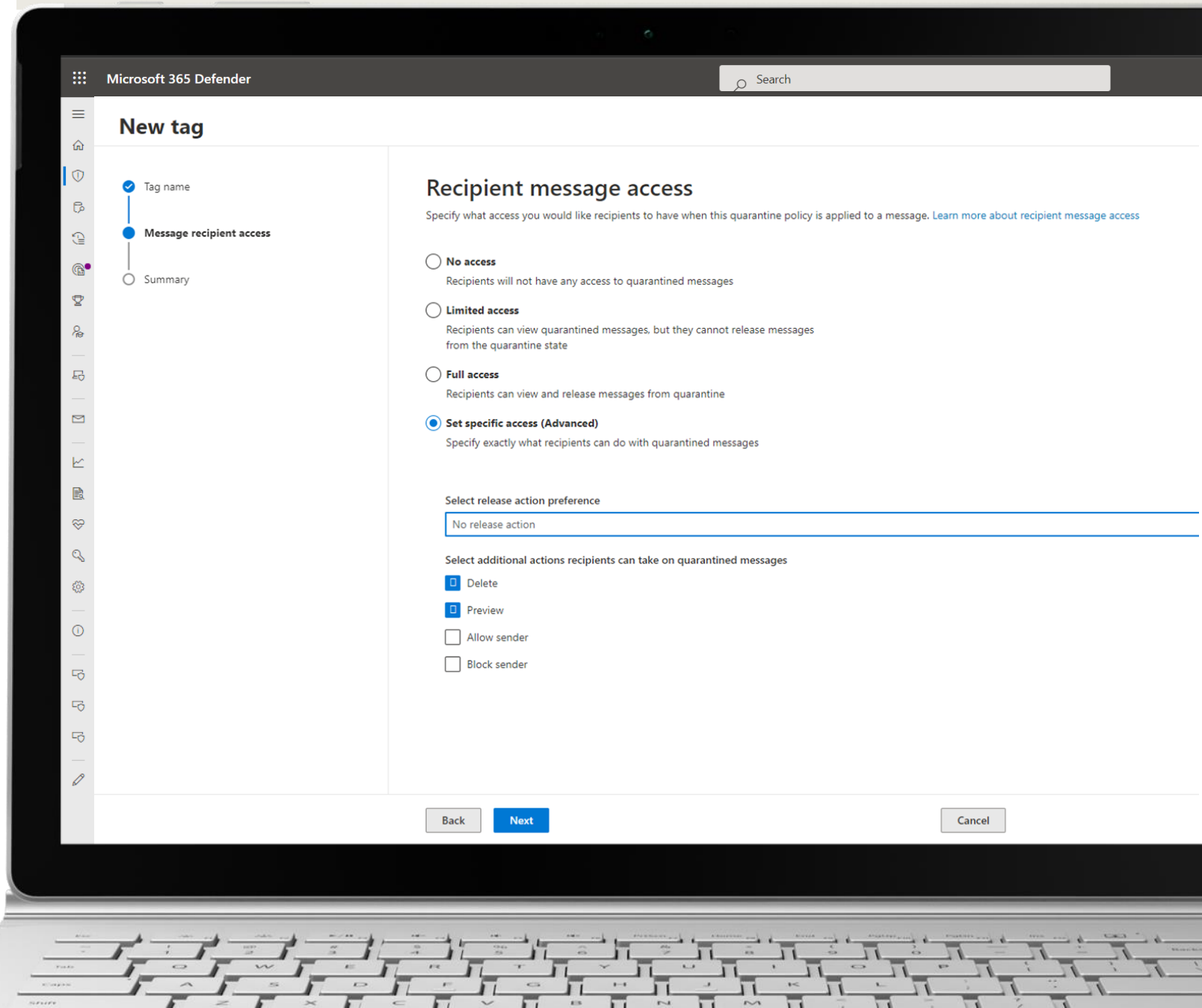



Threat analytics - Microsoft 365
https://security.microsoft.com/threatanalytics3?tid=784aa83f-b2f7-40f9-8cd5-fdd177dc7903
InPrivate
Microsoft 365 Defender
Search
PR
Threat analytics
Ransomware
43
Phishing
16
Vulnerability
66
Activity group
60
Email notification settings
Help resources
Latest threats
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 (Dofoil) 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

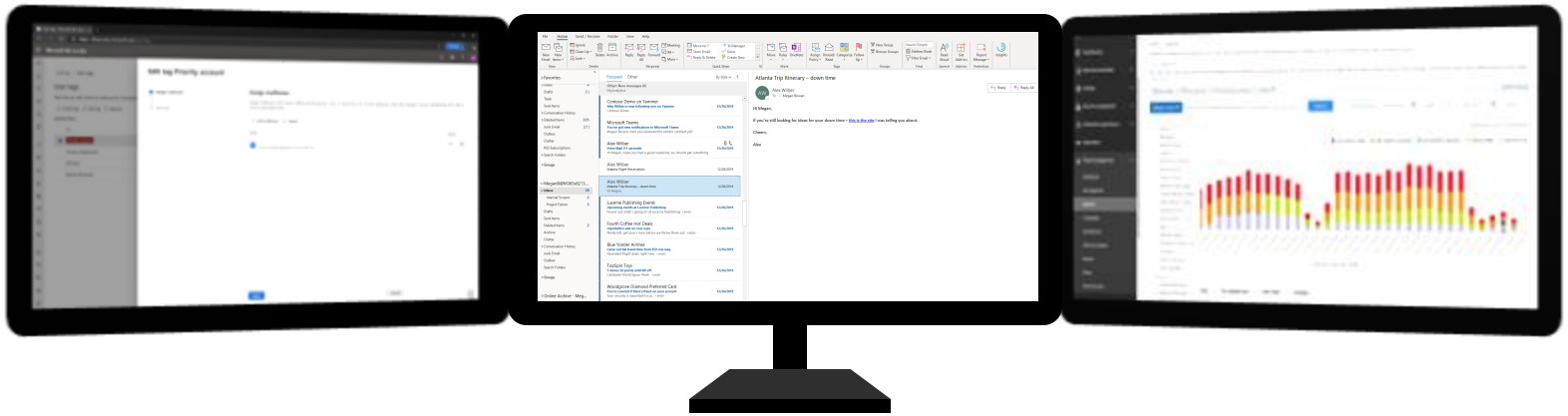

Threat analytics - Microsoft 365
https://security.microsoft.com/threatanalytics3?tid=784aa83f-b2f7-40f9-8cd5-fdd177dc7903
InPrivate
Microsoft 365 Defender
Search
PR
Threat analytics
Ransomware
43
Phishing
16
Vulnerability
66
Activity group
60
Email notification settings
Help resources
Latest threats
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 (Dofoil) 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

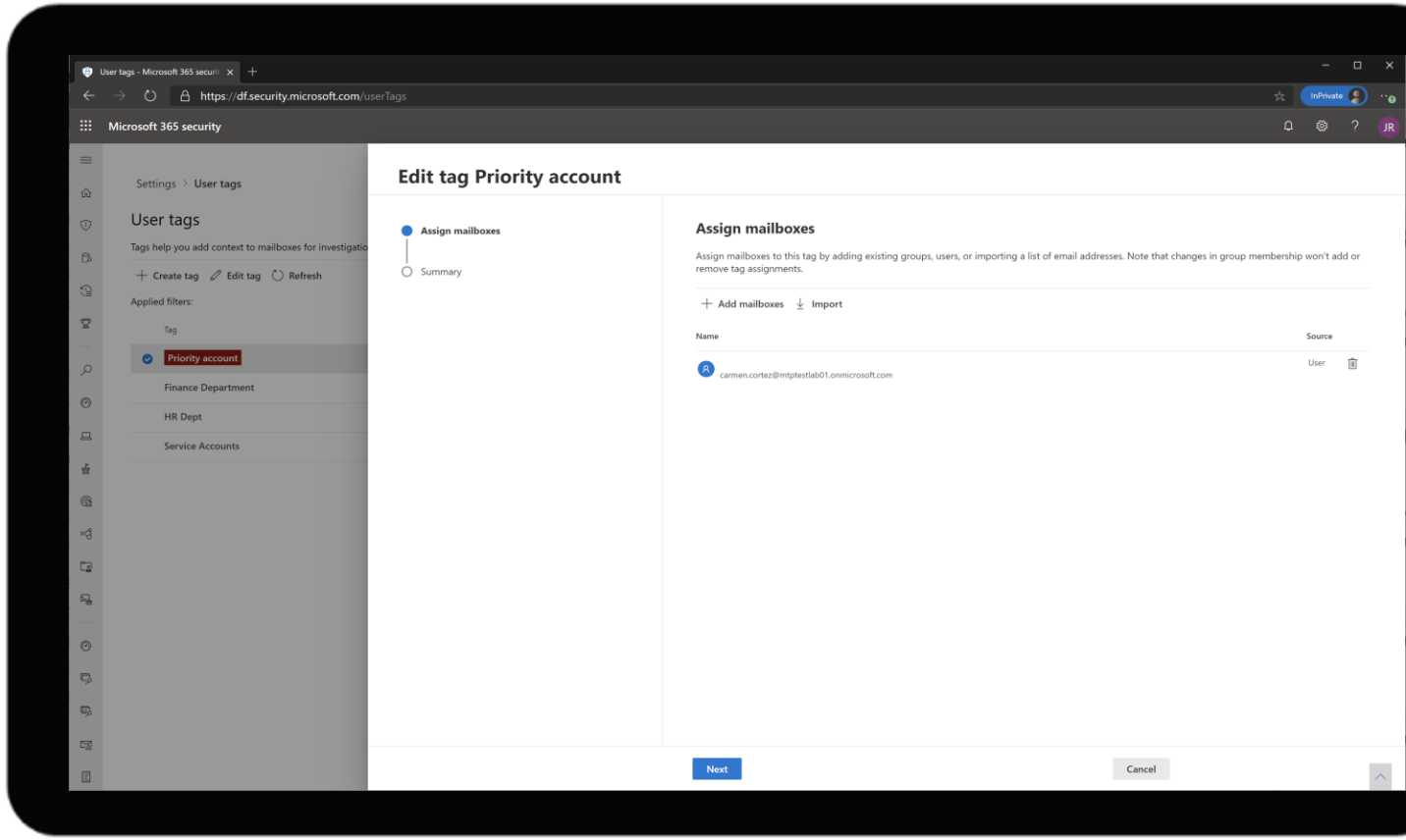


Investigation & Hunting



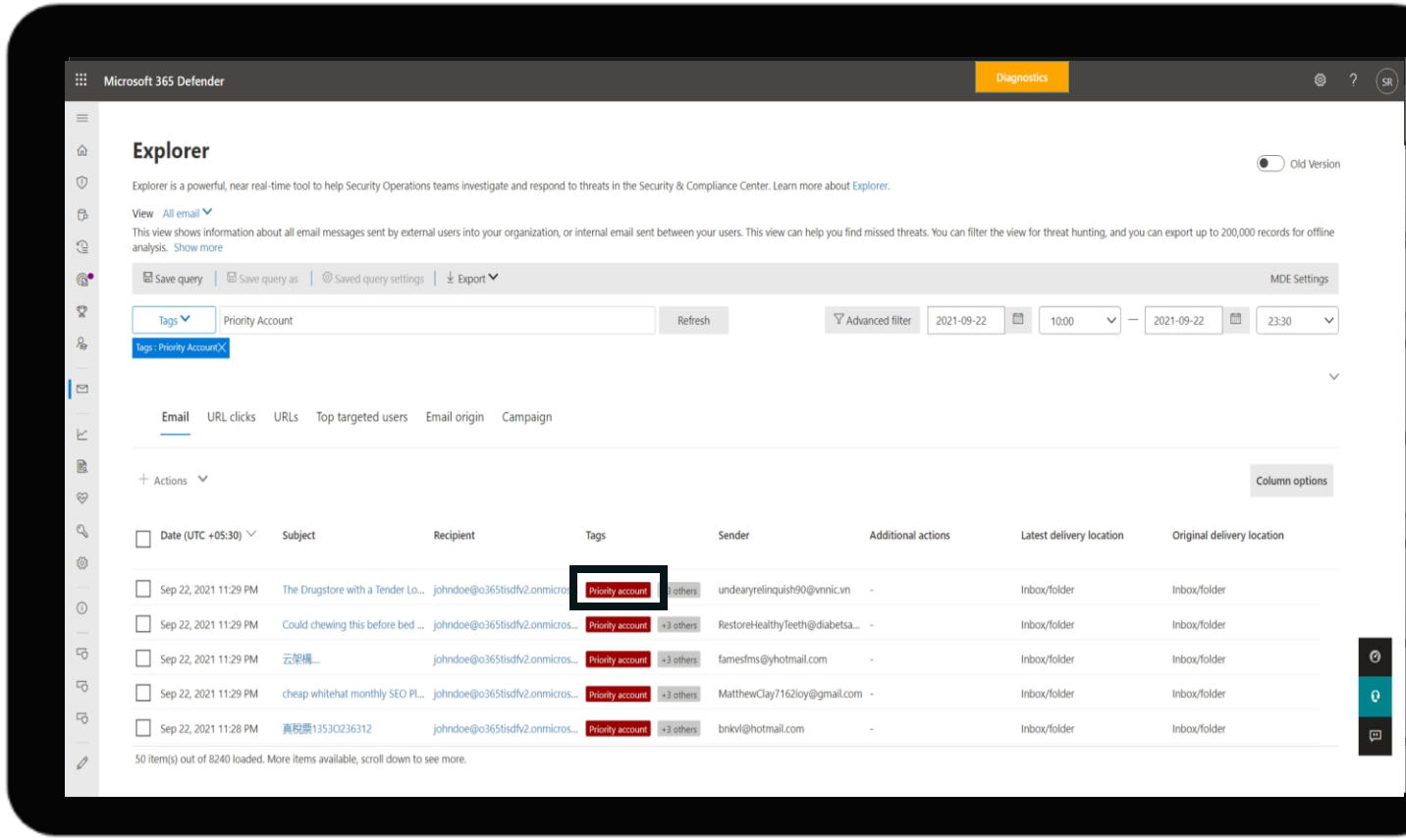
Investigation & Hunting

→ **Prioritized focus through Priority accounts**



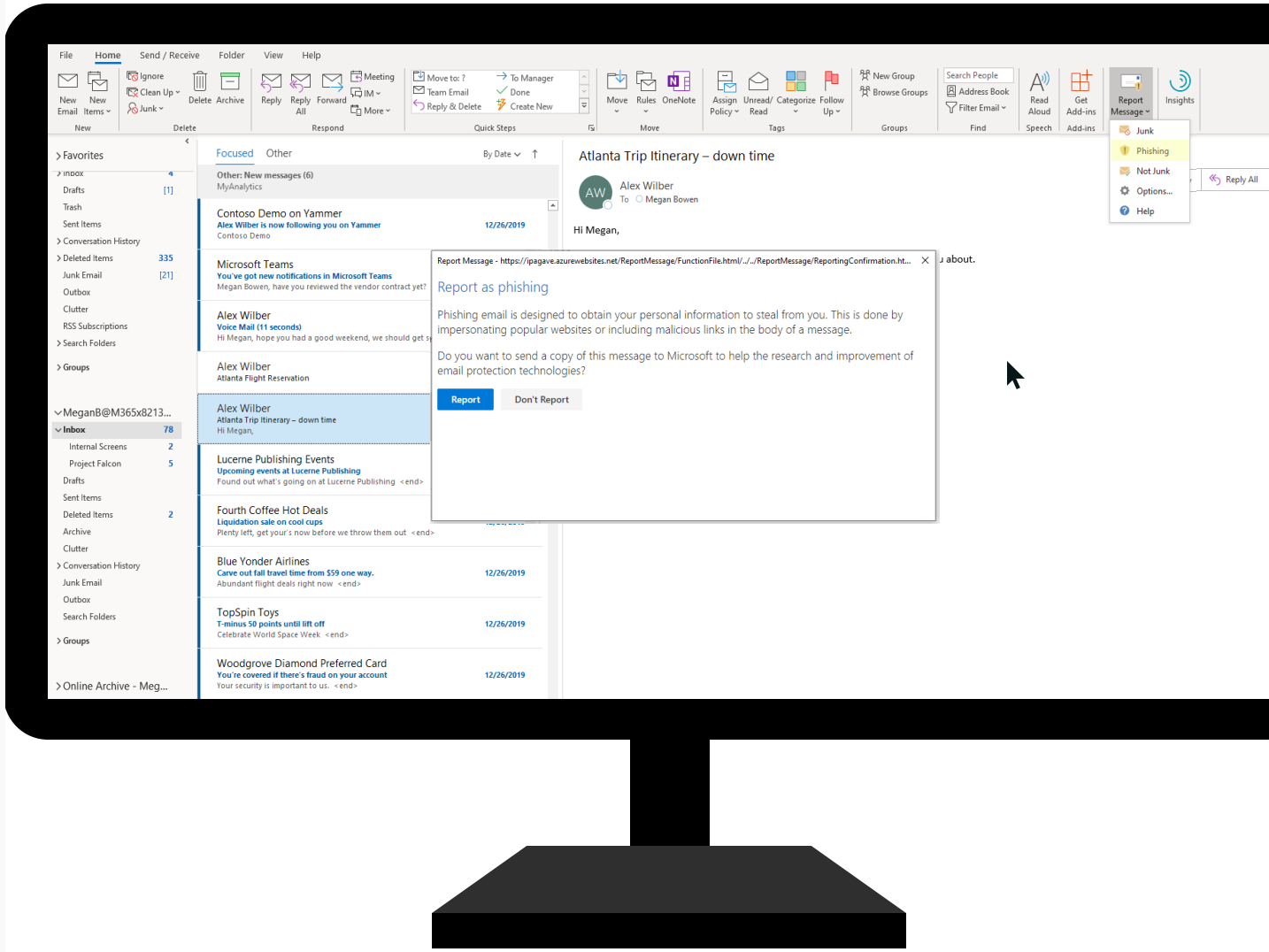
Investigation & Hunting

→ **Prioritized focus through Priority accounts**



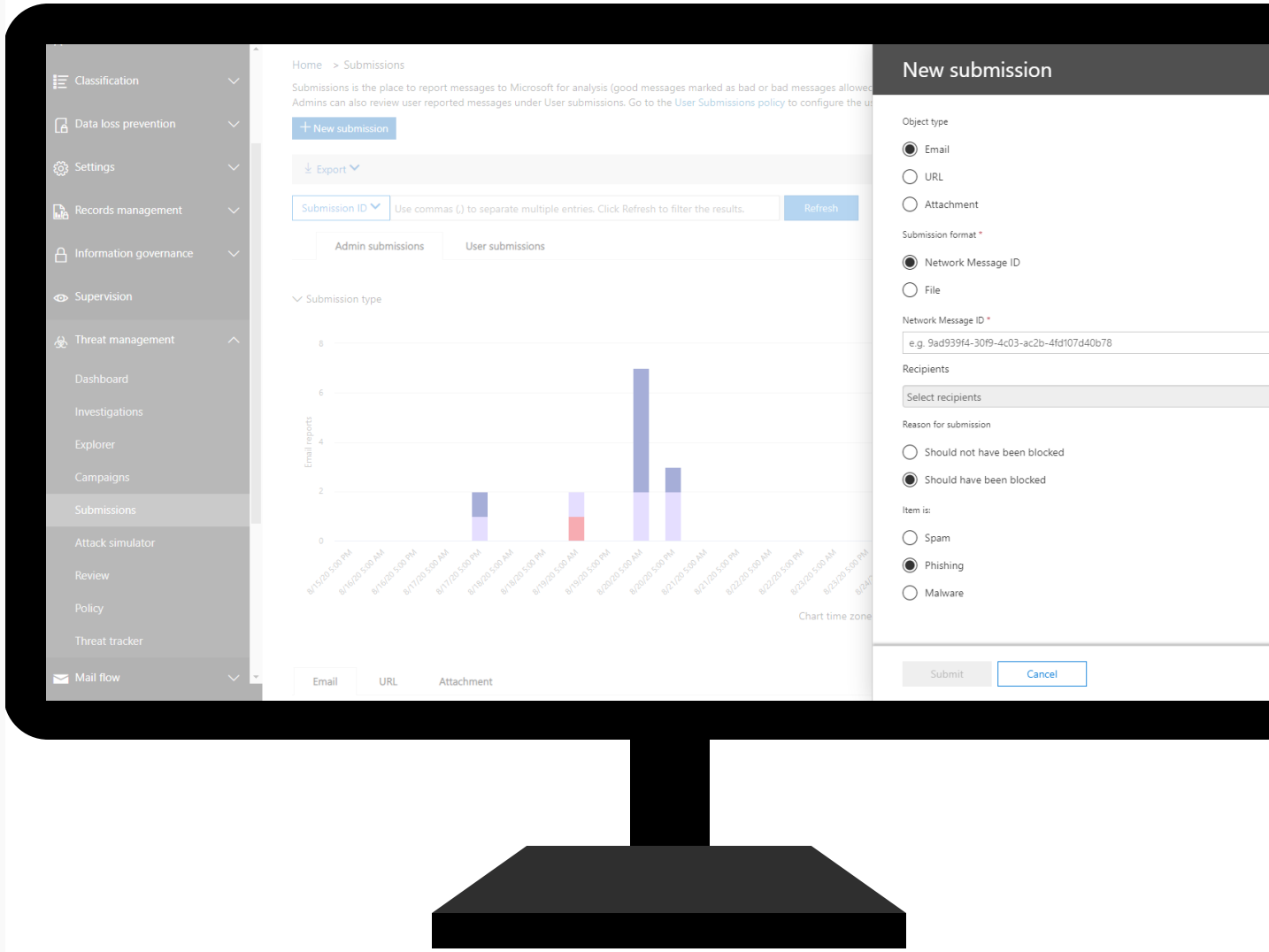
Investigation & Hunting

- Prioritized focus through Priority accounts
- User & Admin Submissions



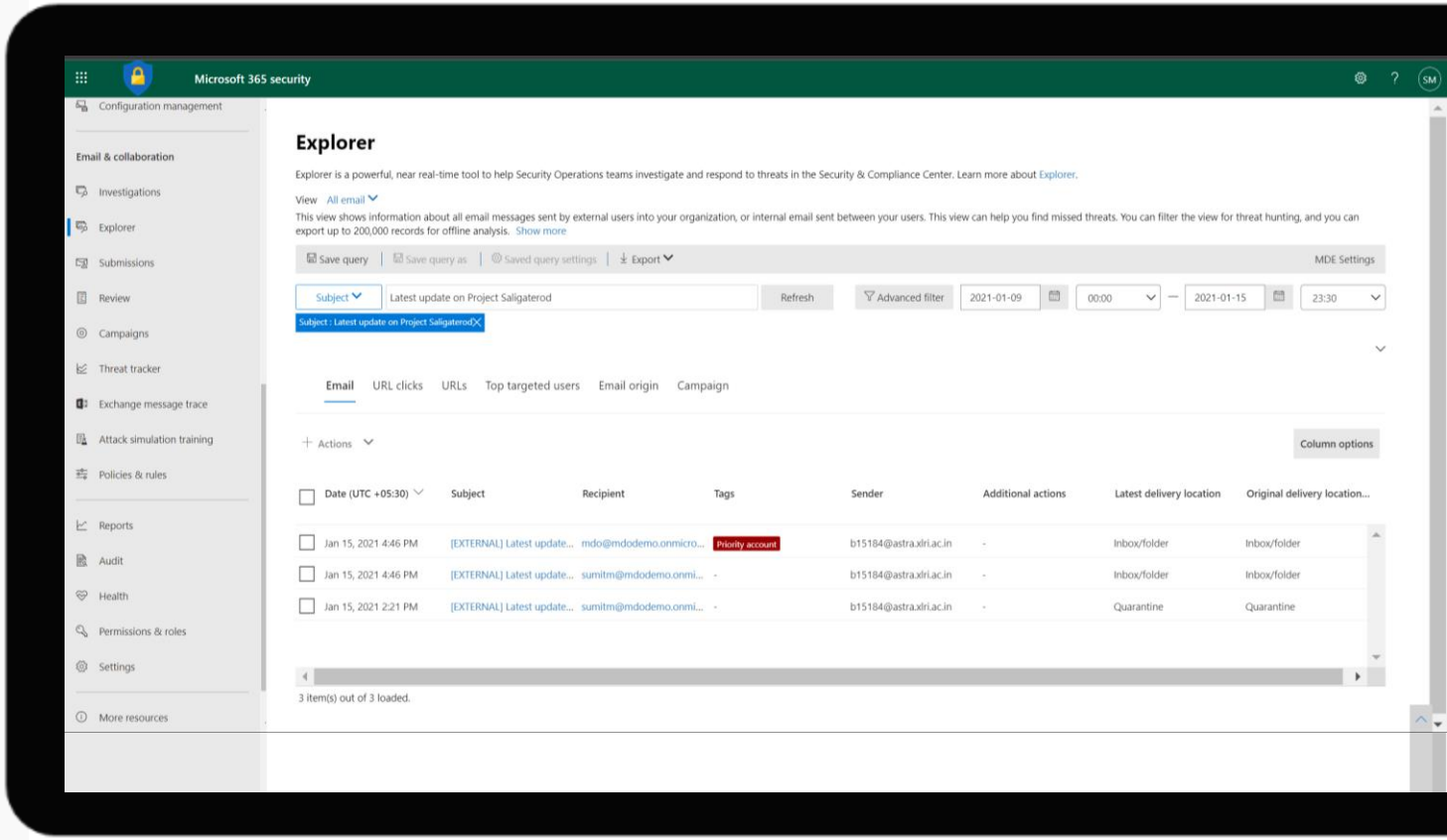
Investigation & Hunting

- Prioritized focus through Priority accounts
- User & Admin Submissions



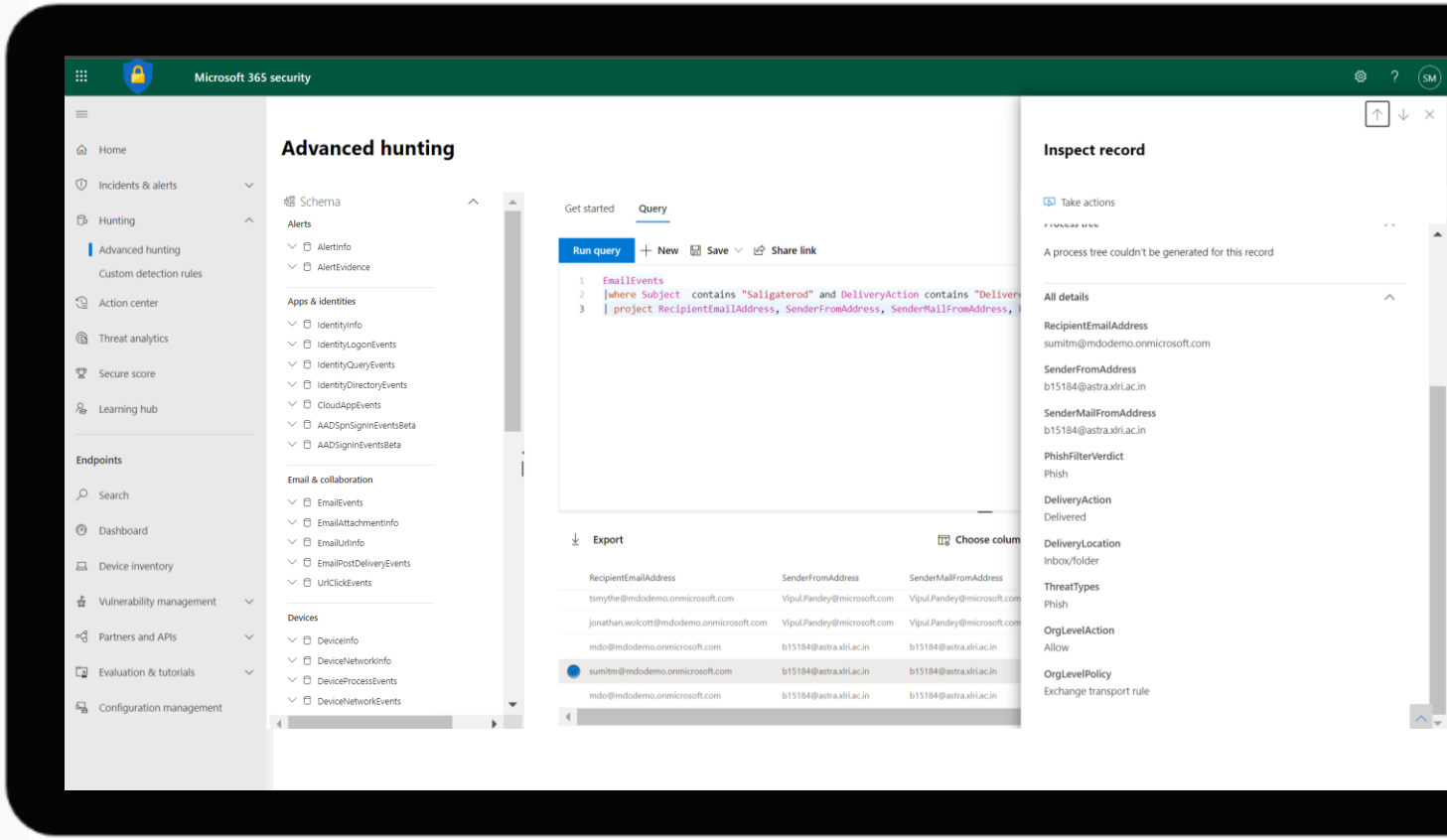
Investigation & Hunting

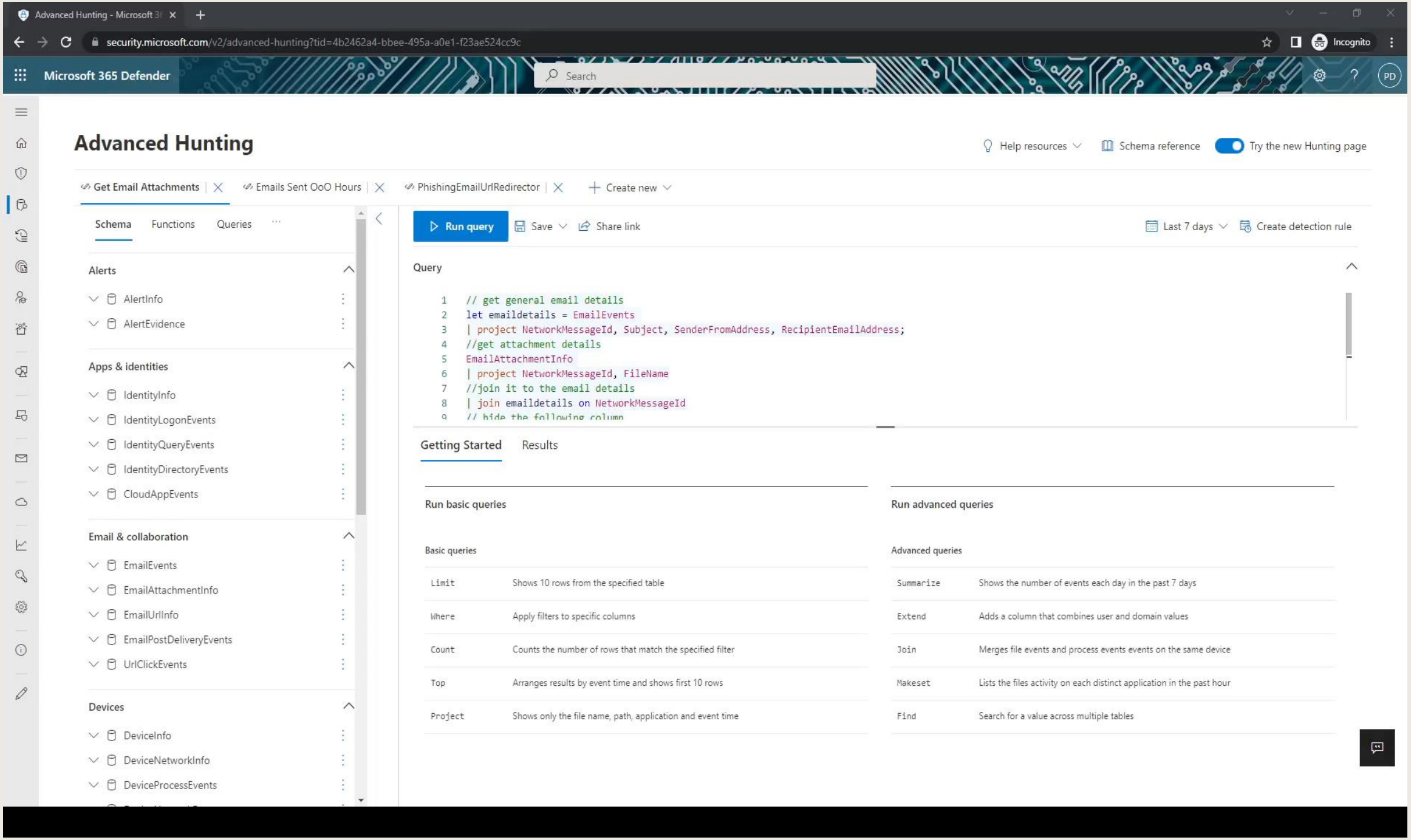
- **Prioritized focus through Priority accounts**
- **User & Admin Submissions**
- **Threat Explorer**



Investigation & Hunting

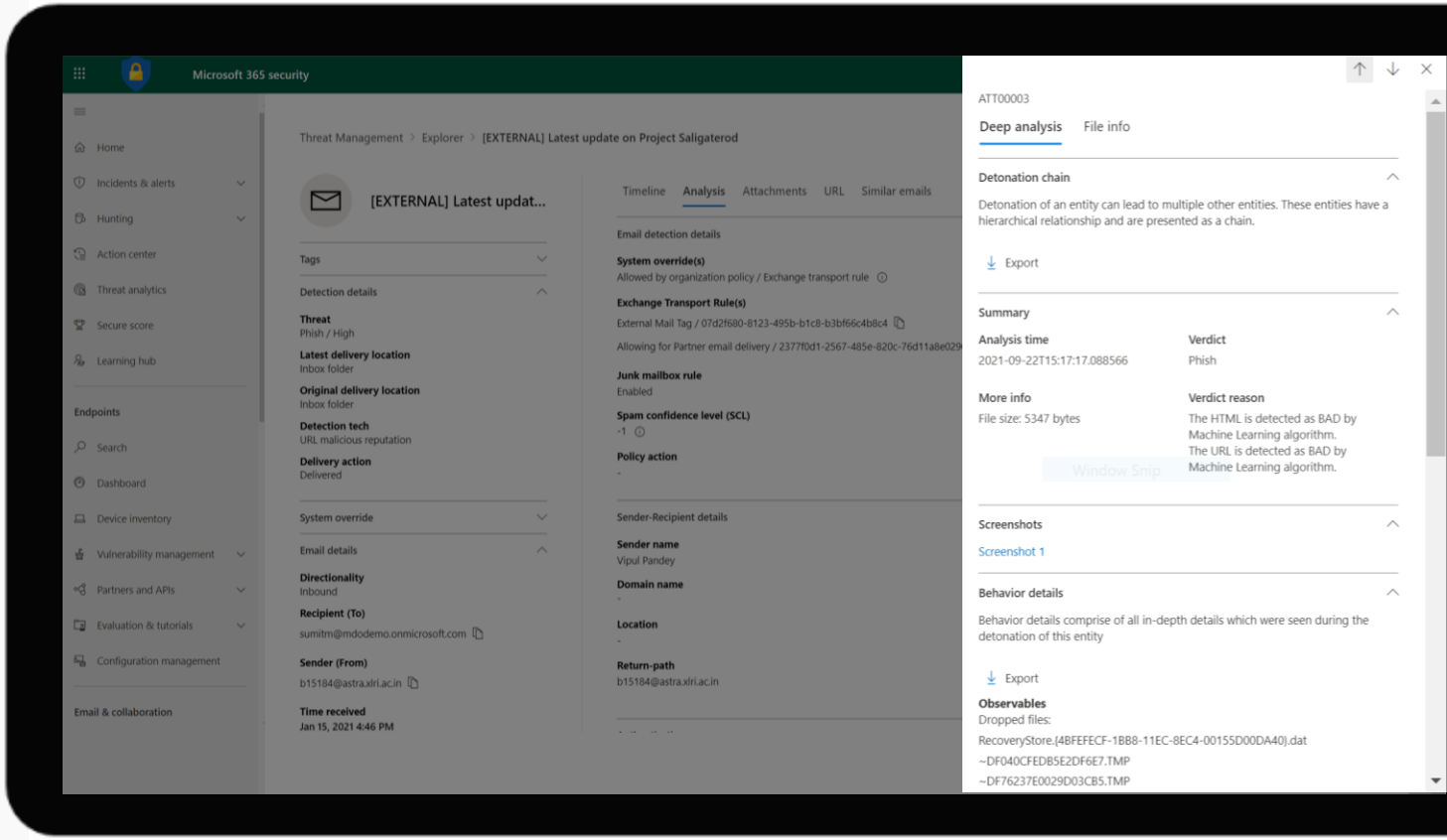
- Prioritized focus through Priority accounts
- User & Admin Submissions
- Threat Explorer
- Advanced Hunting for sophisticated queries




Advanced Hunting - Microsoft 3
security.microsoft.com/v2/advanced-hunting?tid=4b2462a4-bbee-495a-a0e1-f23ae524cc9c
Incognito
Microsoft 365 Defender
Search
PD
Advanced Hunting
Help resources
Schema reference
Try the new Hunting page
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
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

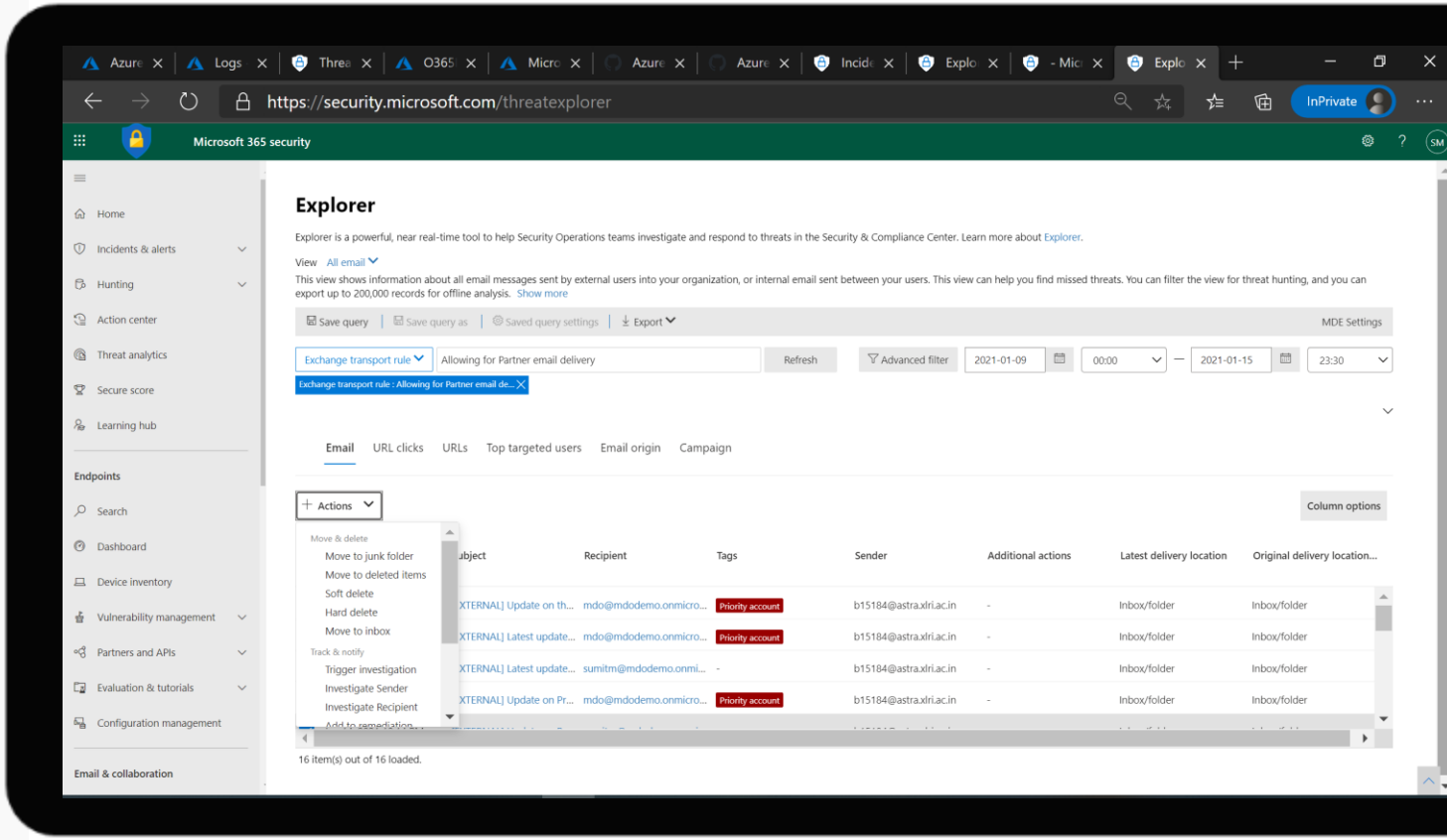
Investigation & Hunting

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



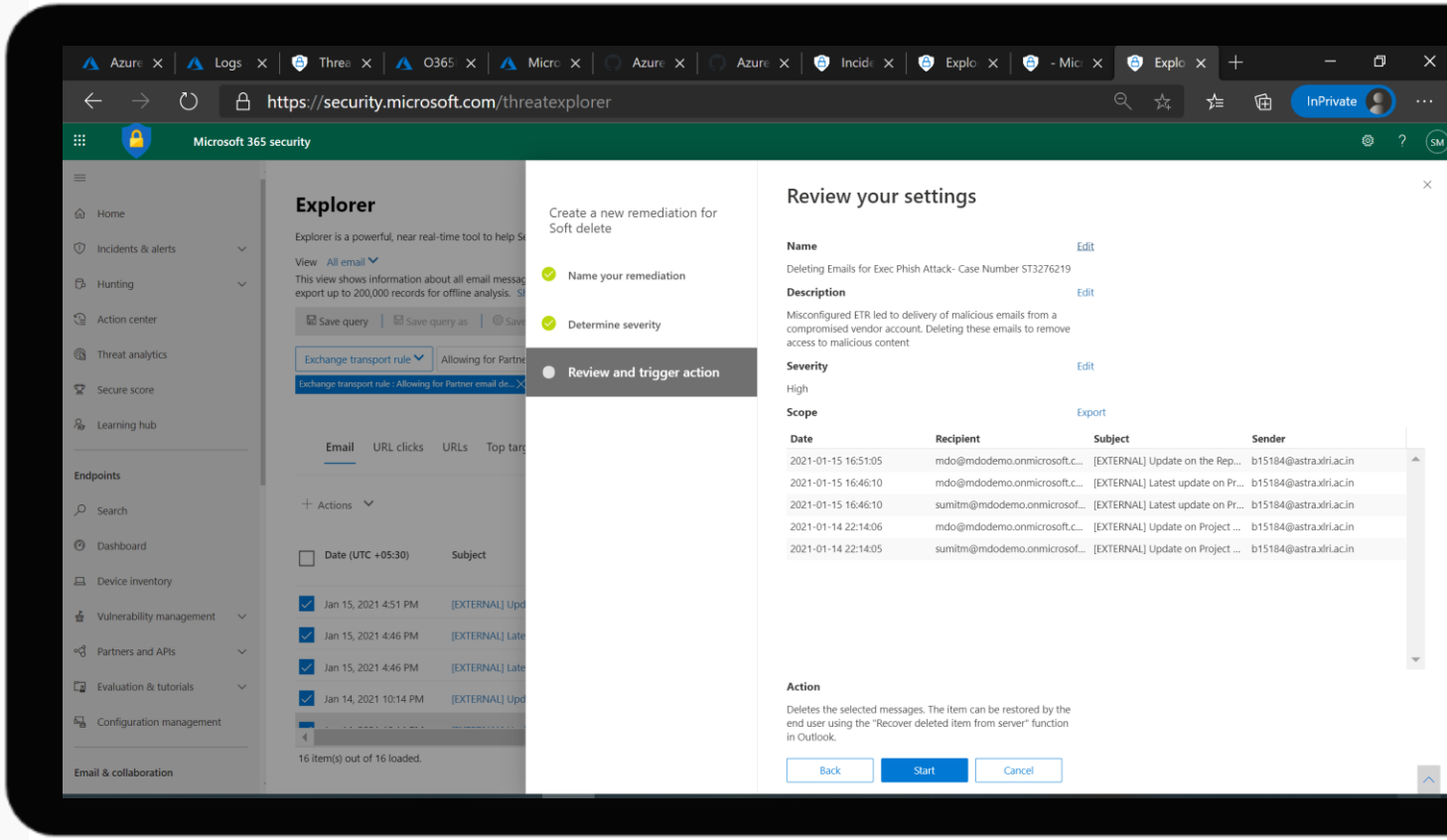
Response & Remediation

- **Guided hunting with inline actions**



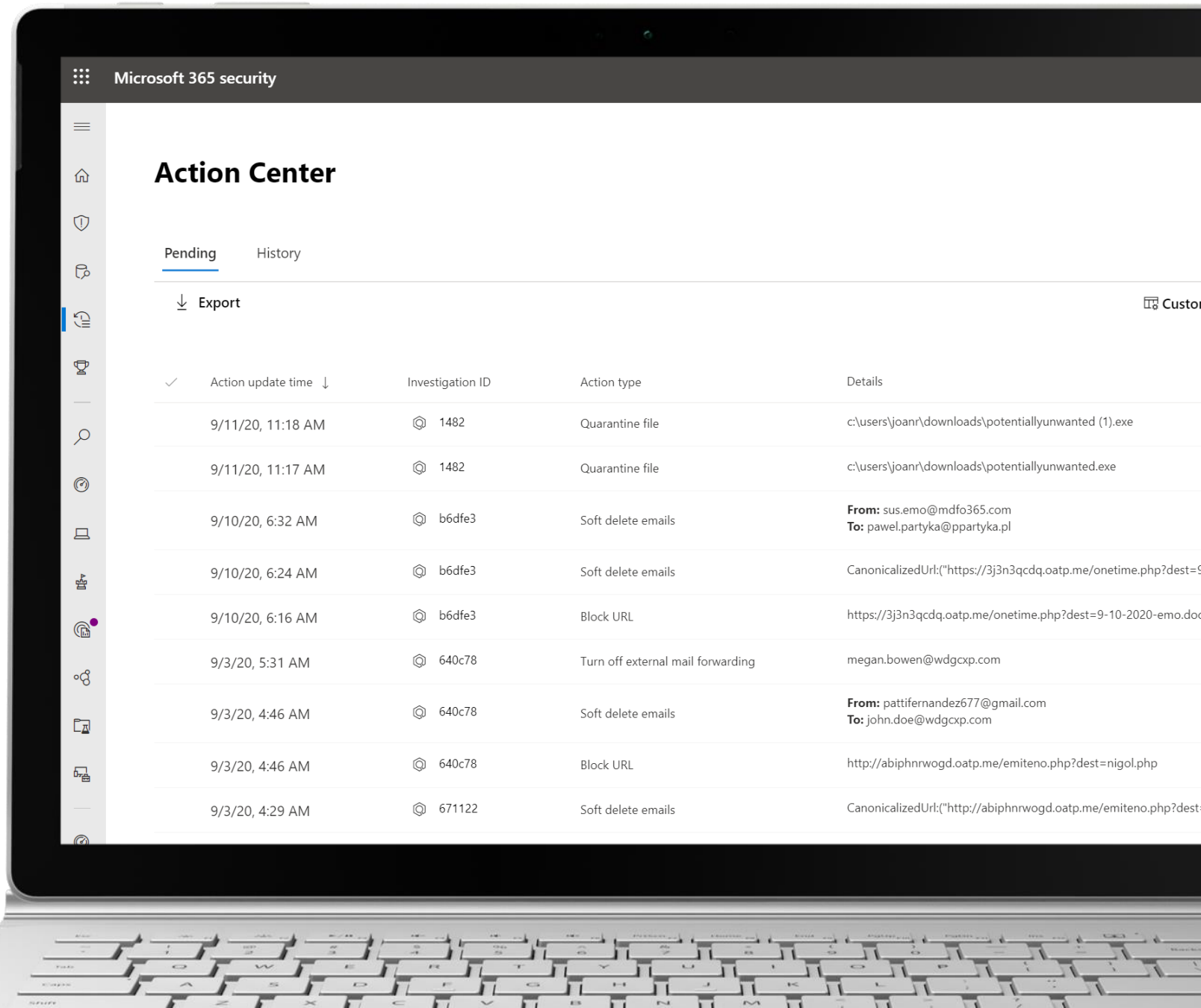
Response & Remediation

- **Guided hunting with inline actions**



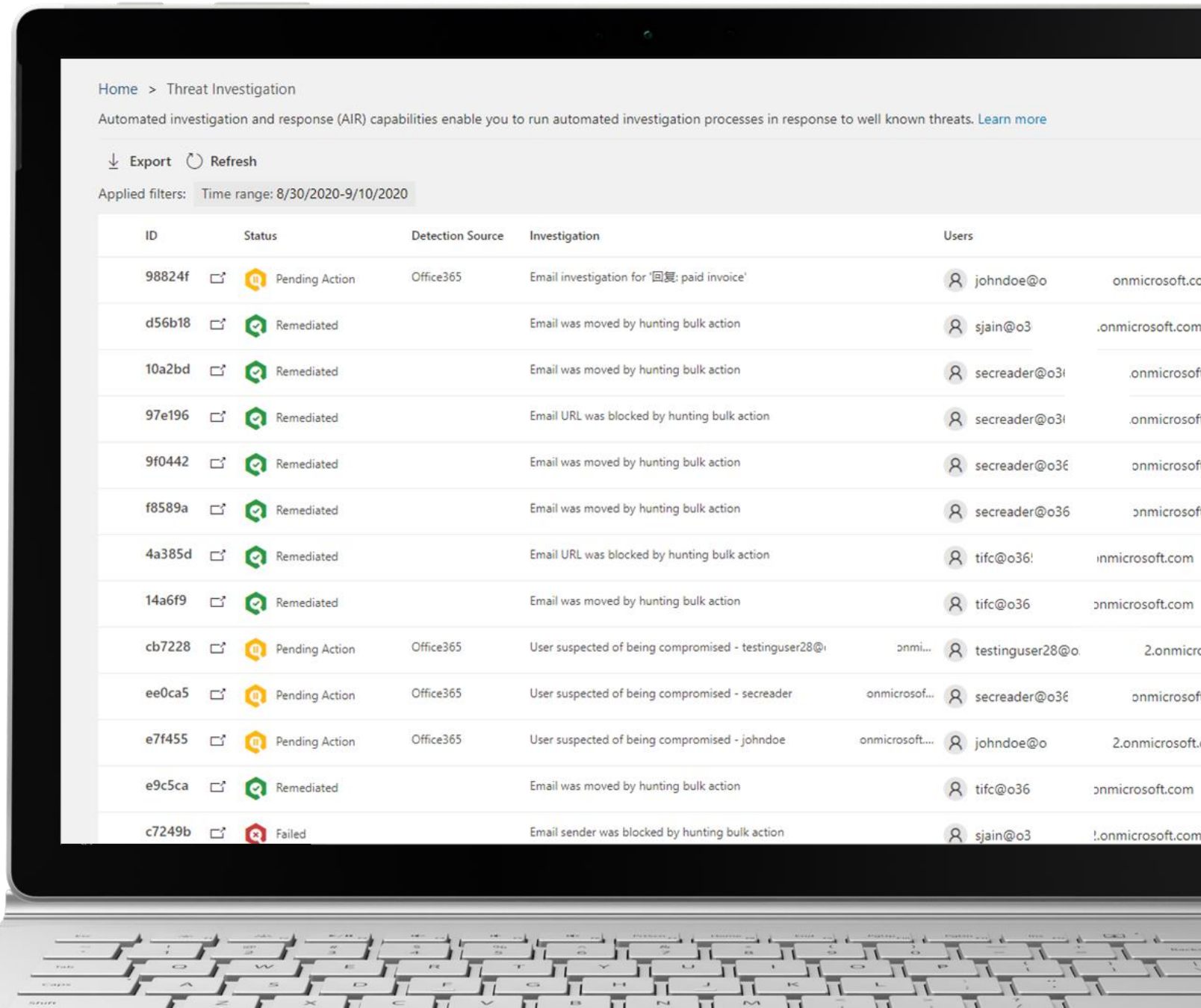
Response & Remediation

- 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.

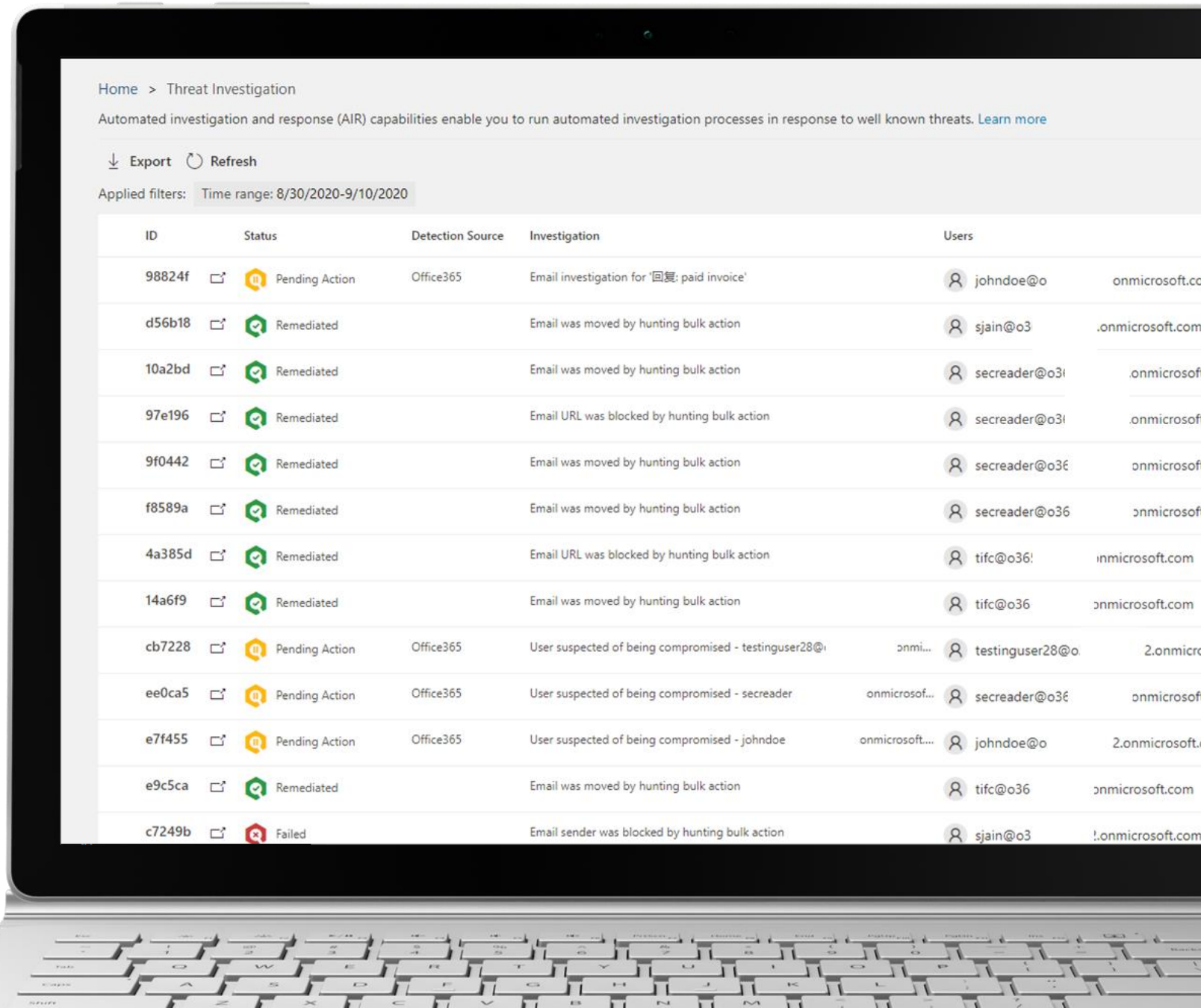
AIR - User Reported Phish Response

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.

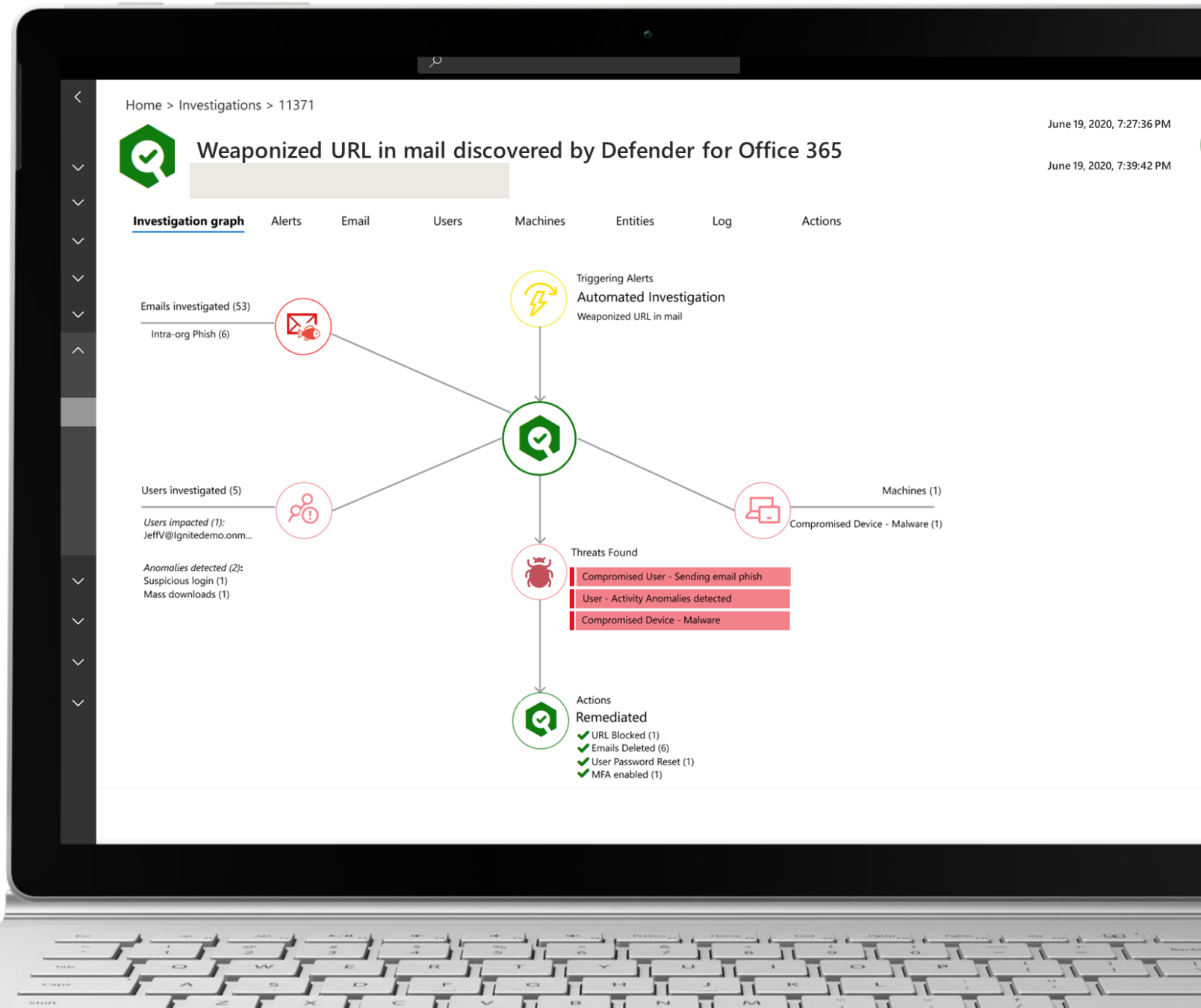
Remediation is the final phase of the playbook. During this phase, remediation steps are identified and surfaced for approval.

Response & Remediation



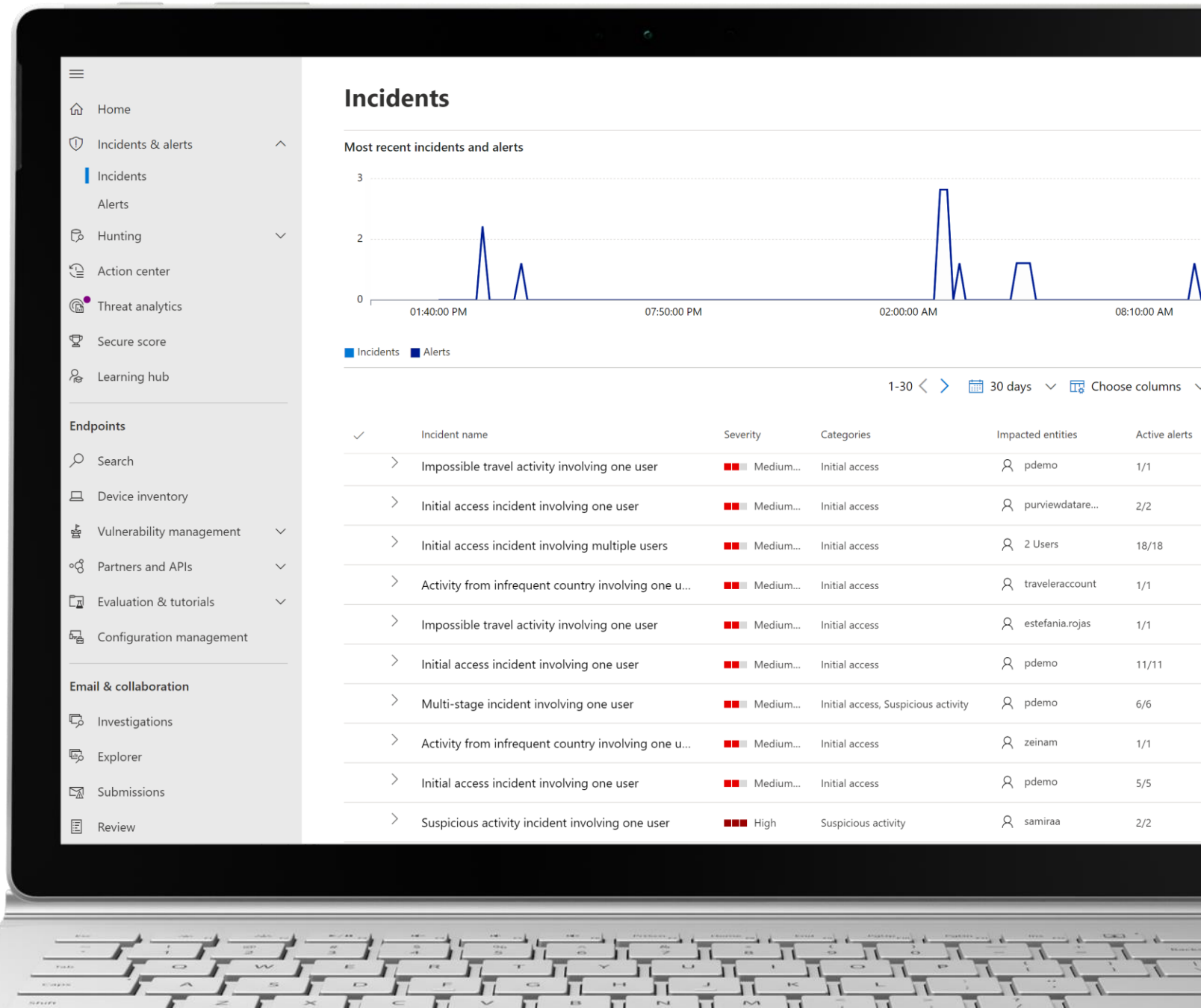
Response & Remediation

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



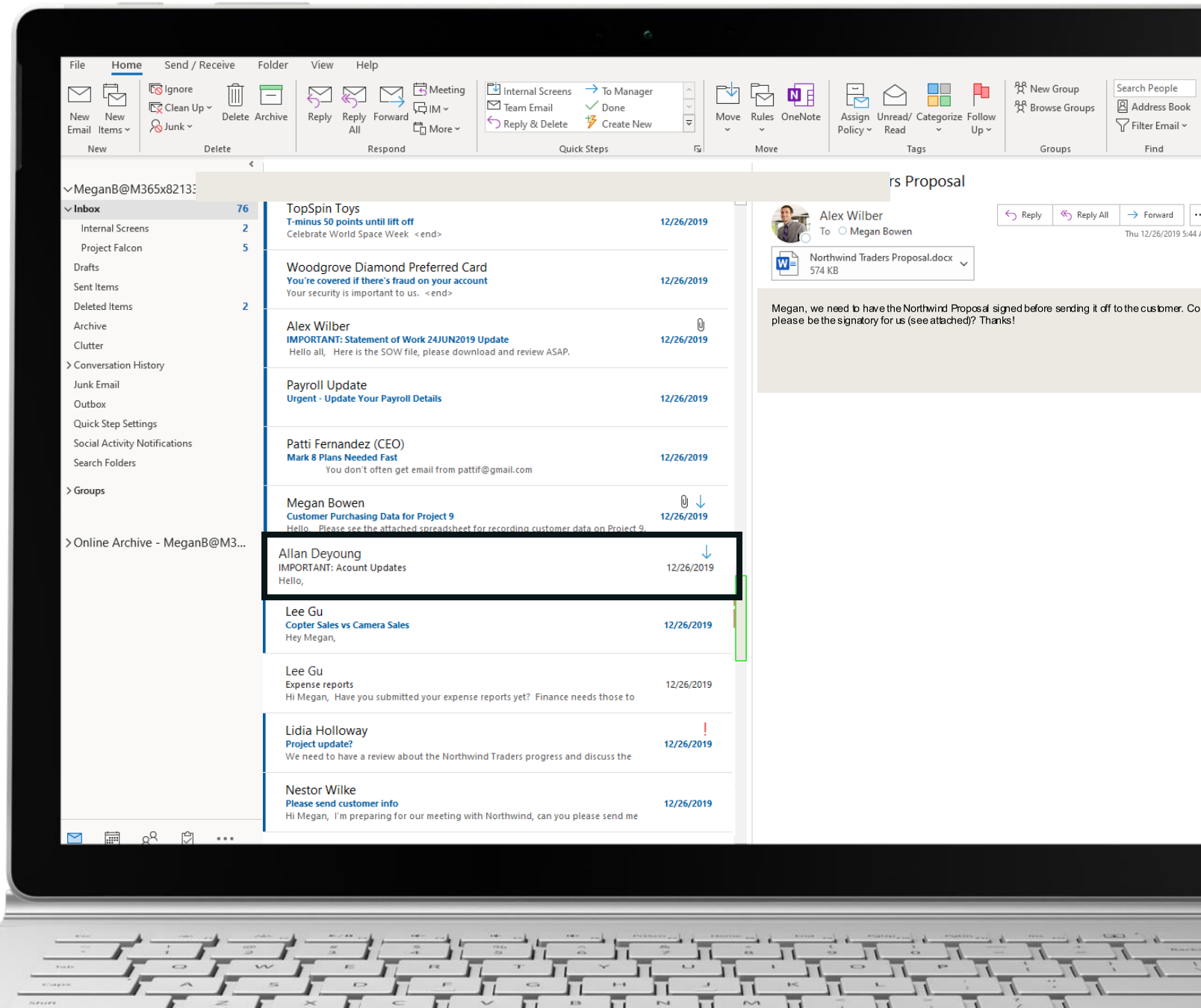
Response & Remediation

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



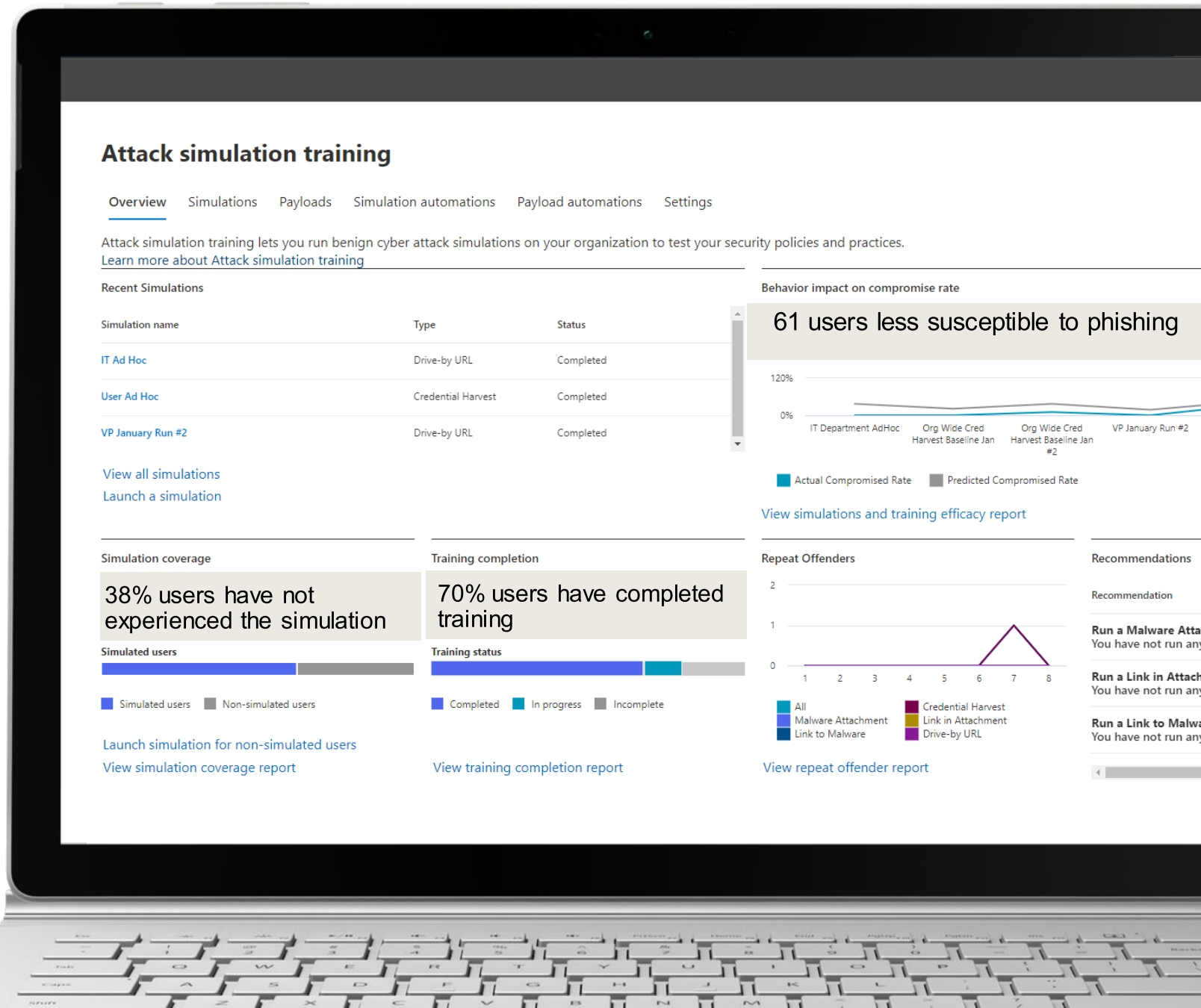
Response & Remediation

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



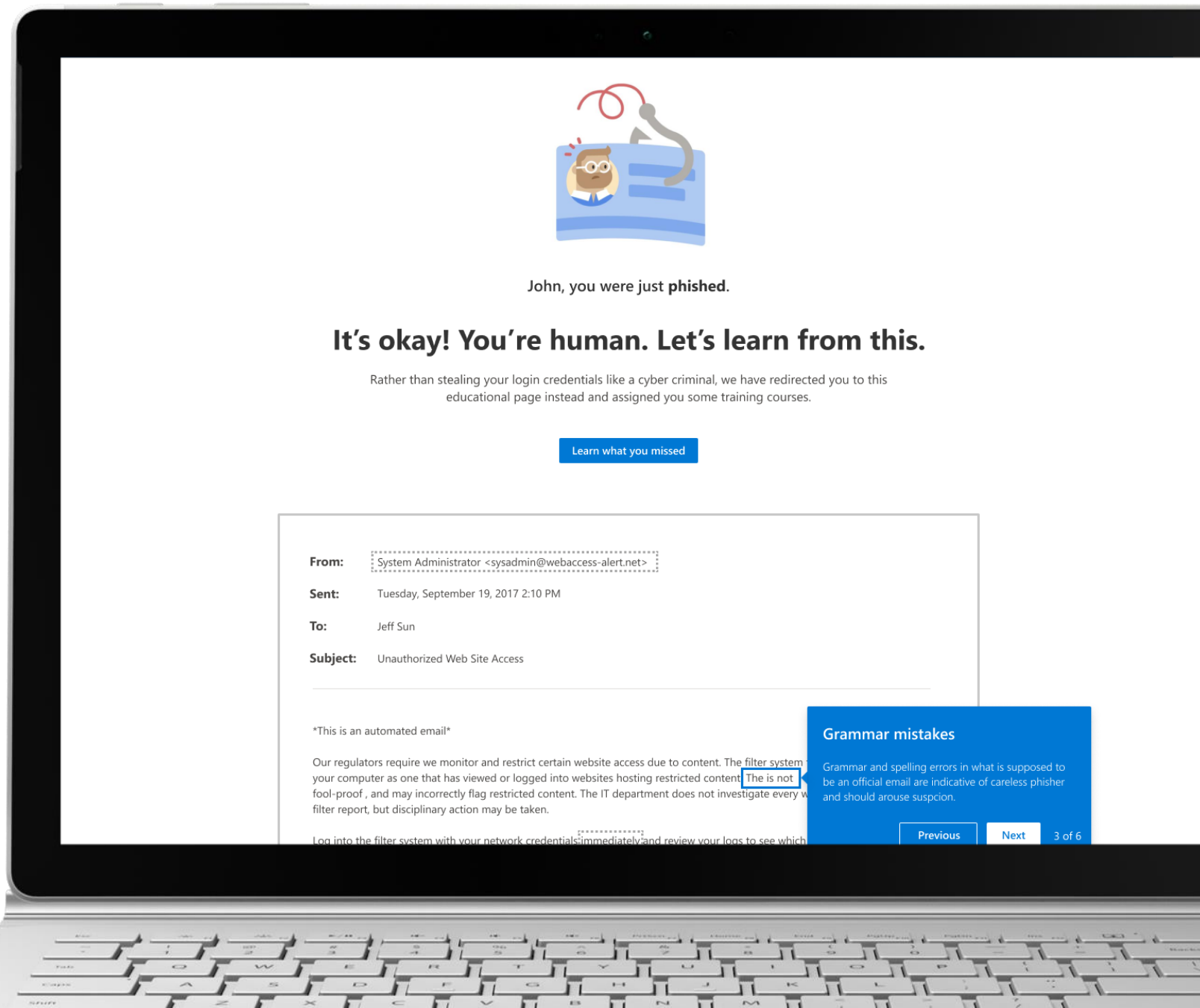
Awareness & Training

- Enhanced simulation management



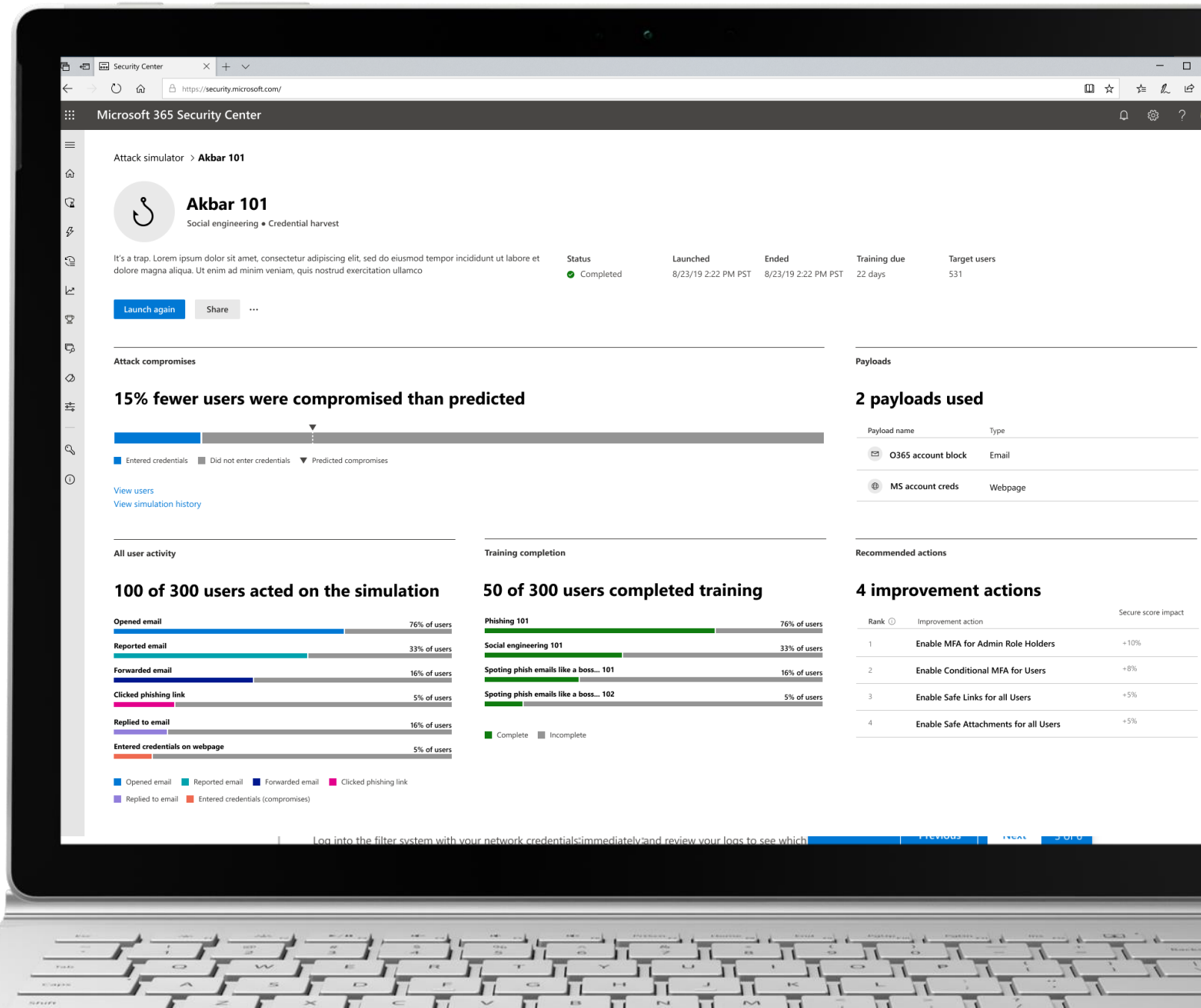
Awareness & Training

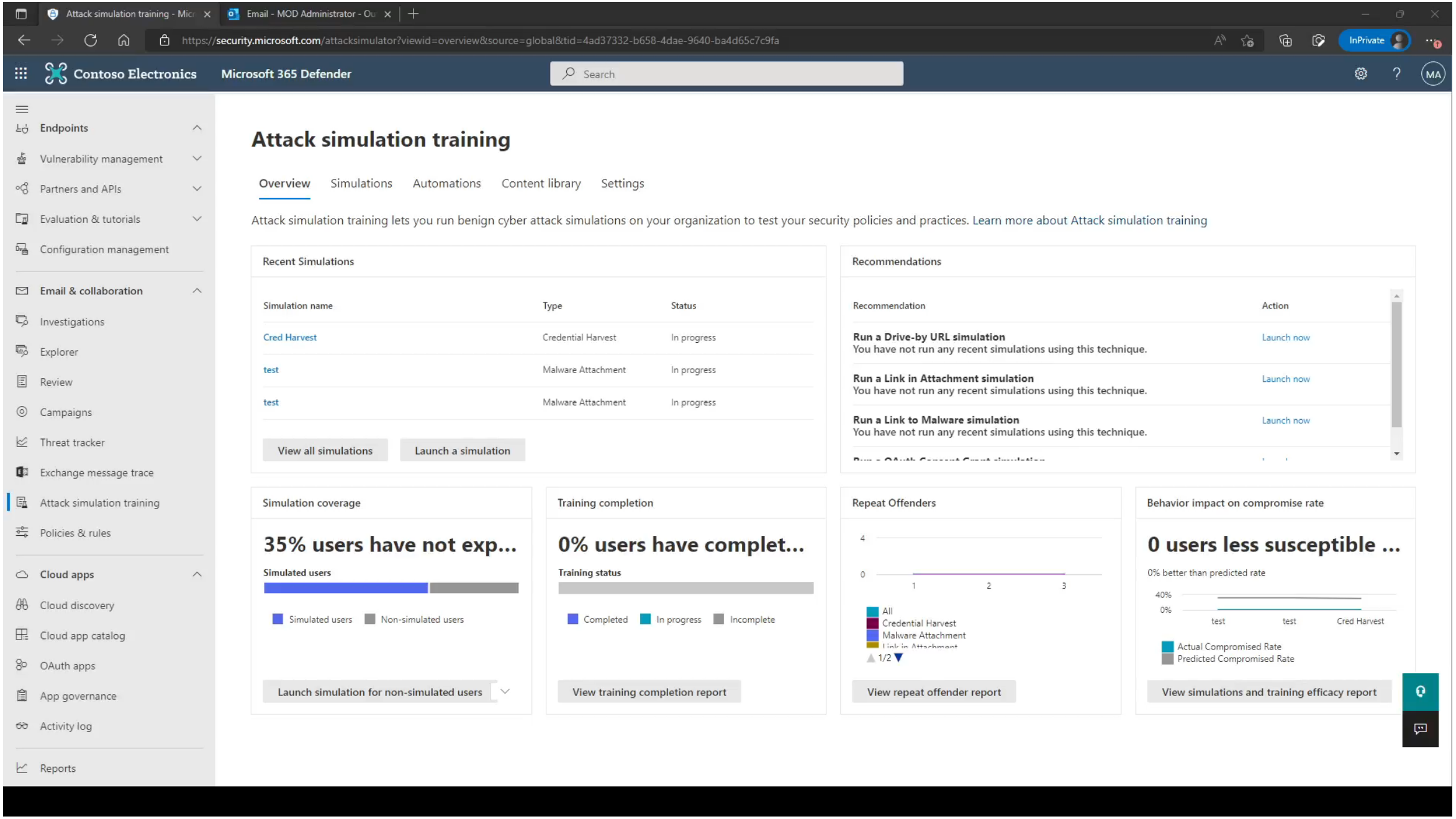
- Enhanced simulation management
- Dynamic end user training

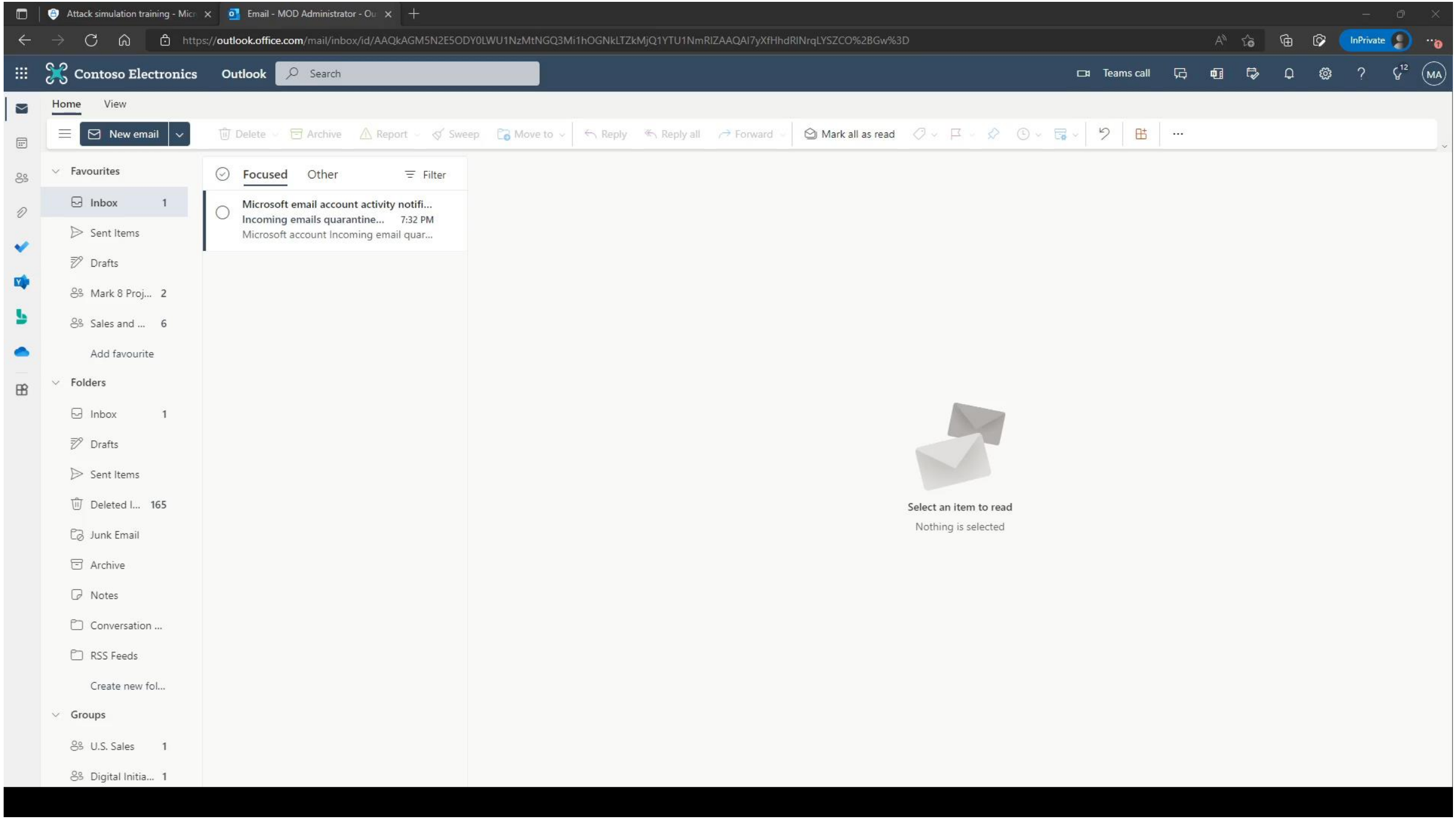


Awareness & Training

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

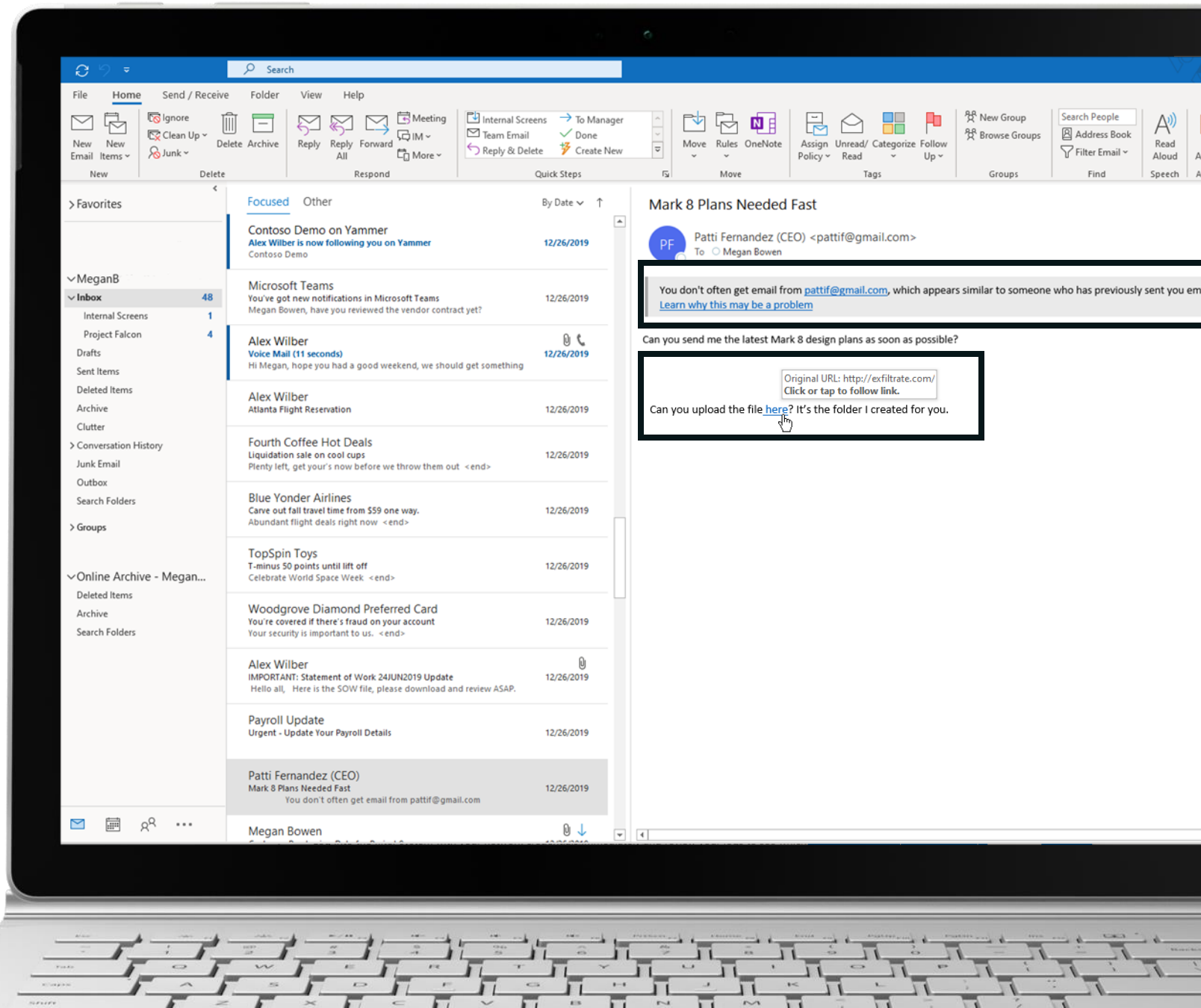



Attack simulation training - Micr
Email - MOD Administrator - Ou
https://security.microsoft.com/attacksimulator?viewid=overview&source=global&tid=4ad37332-b658-4dae-9640-ba4d65c7c9fa
InPrivate
Contoso Electronics
Microsoft 365 Defender
Search
MA
Endpoints
Vulnerability management
Partners and APIs
Evaluation & 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
Simulation coverage
35% users have not exp...
Simulated users
Simulated users
Non-simulated users
Launch simulation for non-simulated users
Training completion
0% users have complet...
Training status
Completed
In progress
Incomplete
View training completion report
Repeat Offenders
4
0
1
2
3
All
Credential Harvest
Malware Attachment
1/2
View repeat offender report
Behavior impact on compromise rate
0 users less susceptible ...
0% better than predicted rate
40%
0%
test
test
Cred Harvest
Actual Compromised Rate
Predicted Compromised Rate
View simulations and training efficacy report


Attack simulation training - Micr
Email - MOD Administrator - Ou
https://outlook.office.com/mail/inbox/id/AAQkAGM5N2E5ODY0LWU1NzMtNGQ3Mi1hOGNkLTZkMjQ1YTU1NmRlZAAQAI7yXfHhdRINrqLYSZCO%2BGw%3D
InPrivate
Contoso Electronics
Outlook
Search
Teams call
MA
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

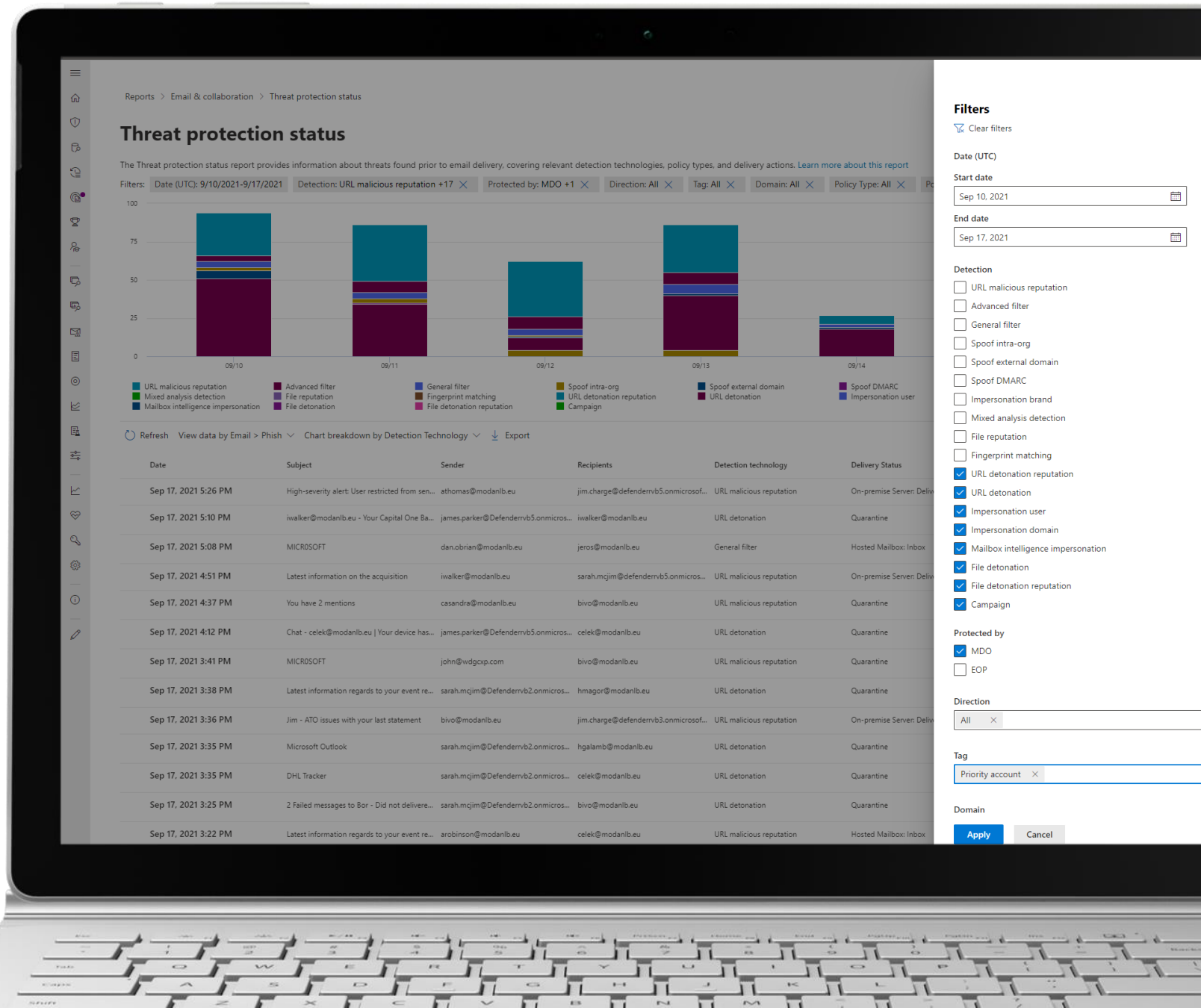
Awareness & Training

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



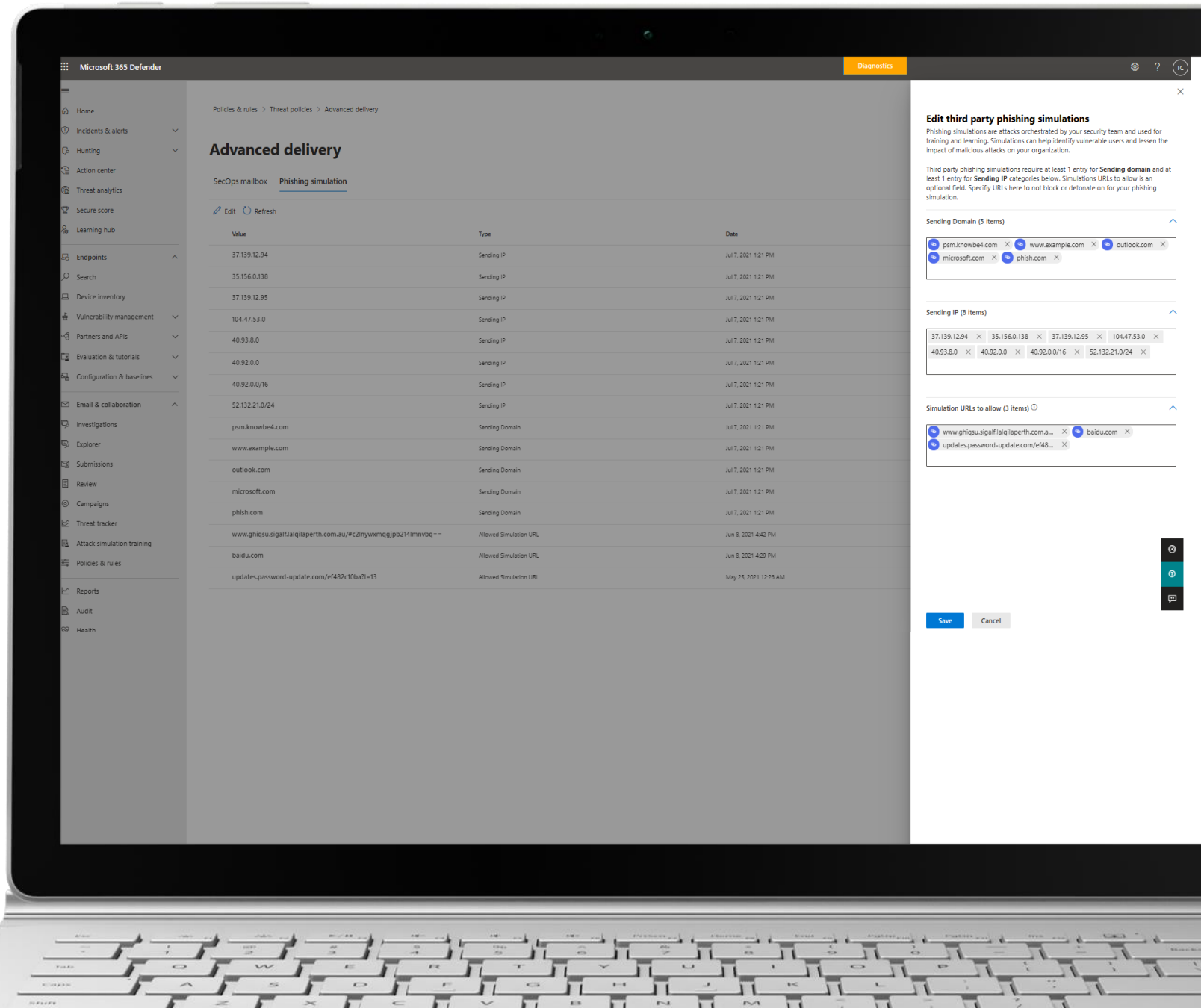
Secure Posture

- Detailed reporting



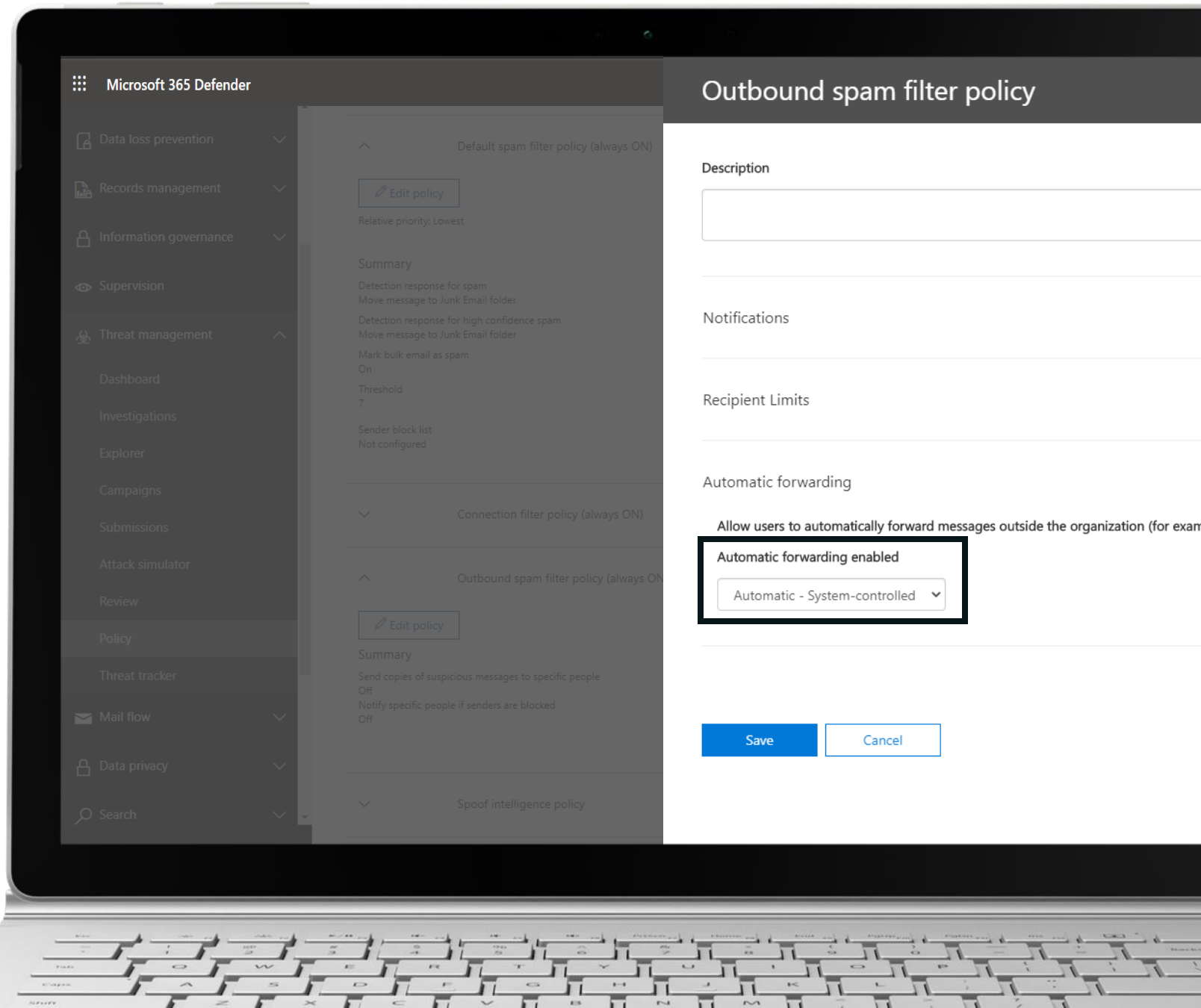
Secure Posture

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



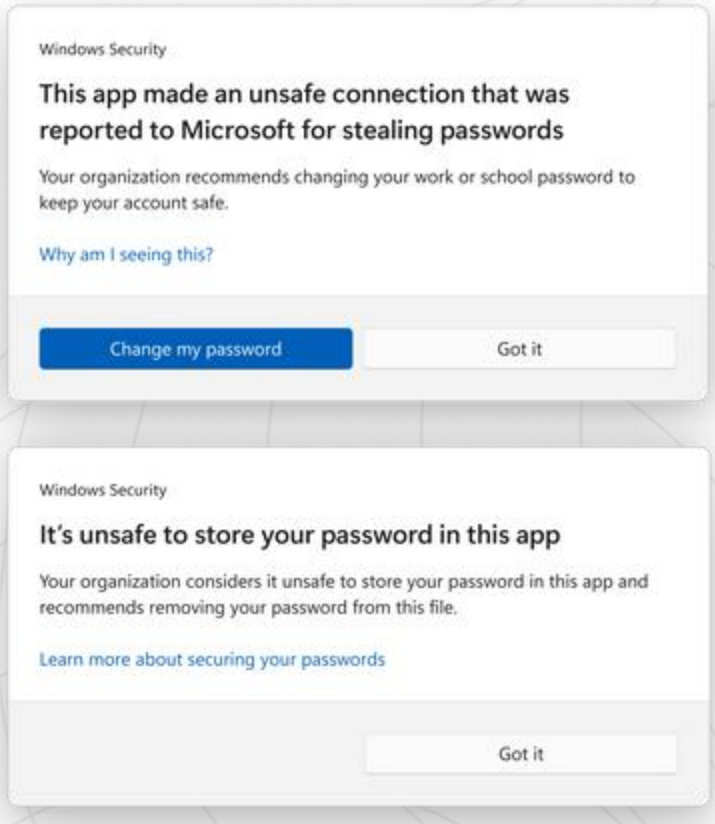
Secure Posture

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



Enhanced Phishing Protection in Win11

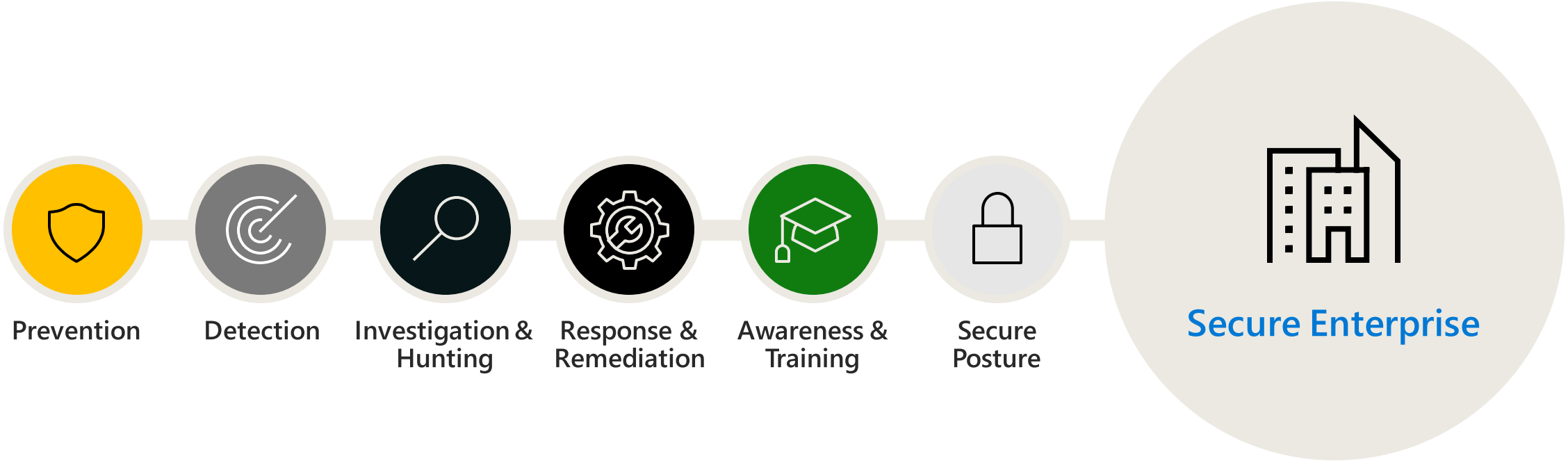
- Enhanced phishing protection now baked into Windows 11
- Automatically detects when users type their password into any app or site. Windows understands in real-time whether that app or website has a secure connection to a trusted website; if not, Windows will let users know if they're in danger.
- 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

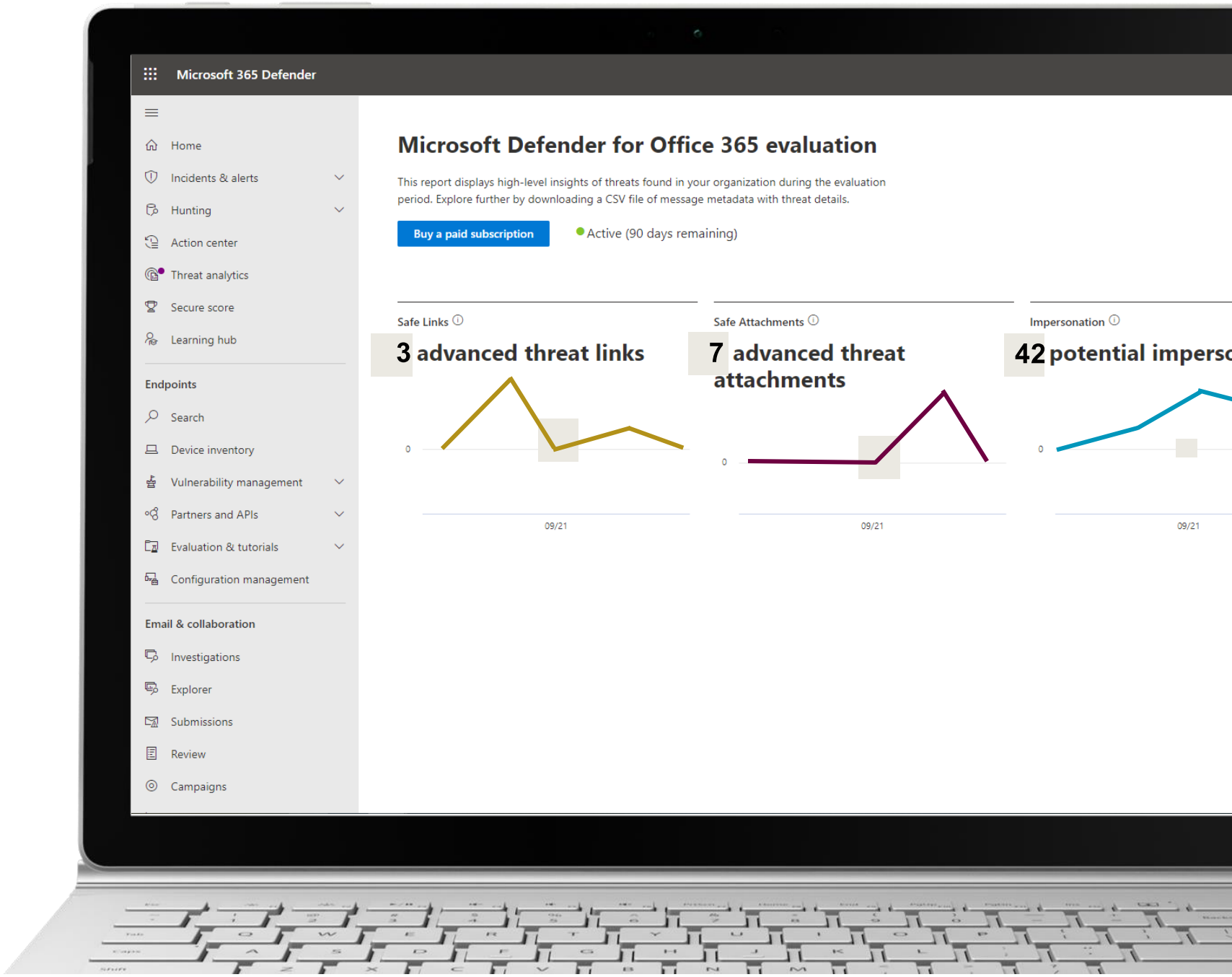
Microsoft Defender for Office 365

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

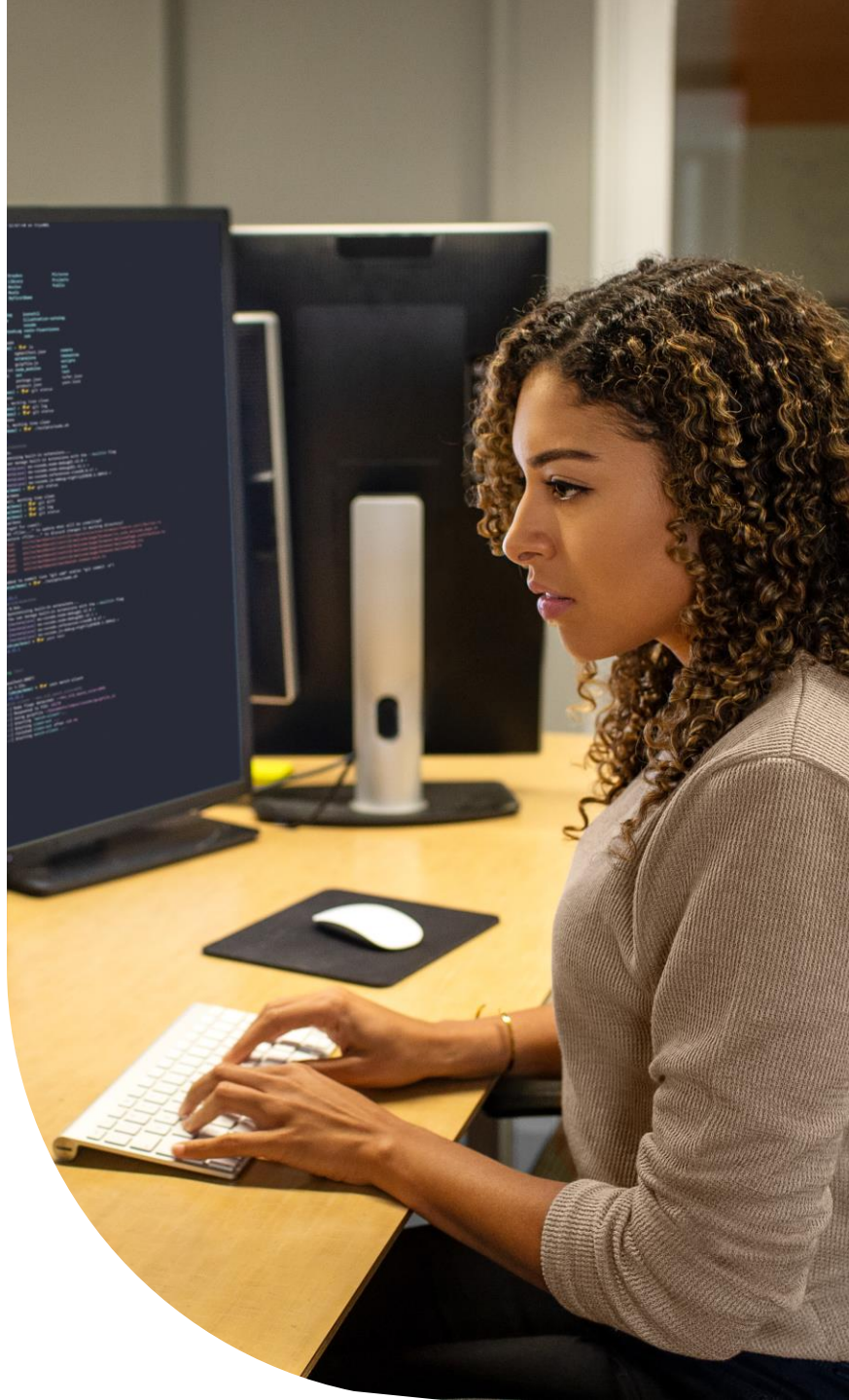
→ Product page: https://aka.ms/DefenderO365

→ 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/



Kocho

BECOME GREATER

Thank you

→ Any questions?