Microsoft

Microsoft Defender for Office 365

Integrated threat protection for all of Office 365

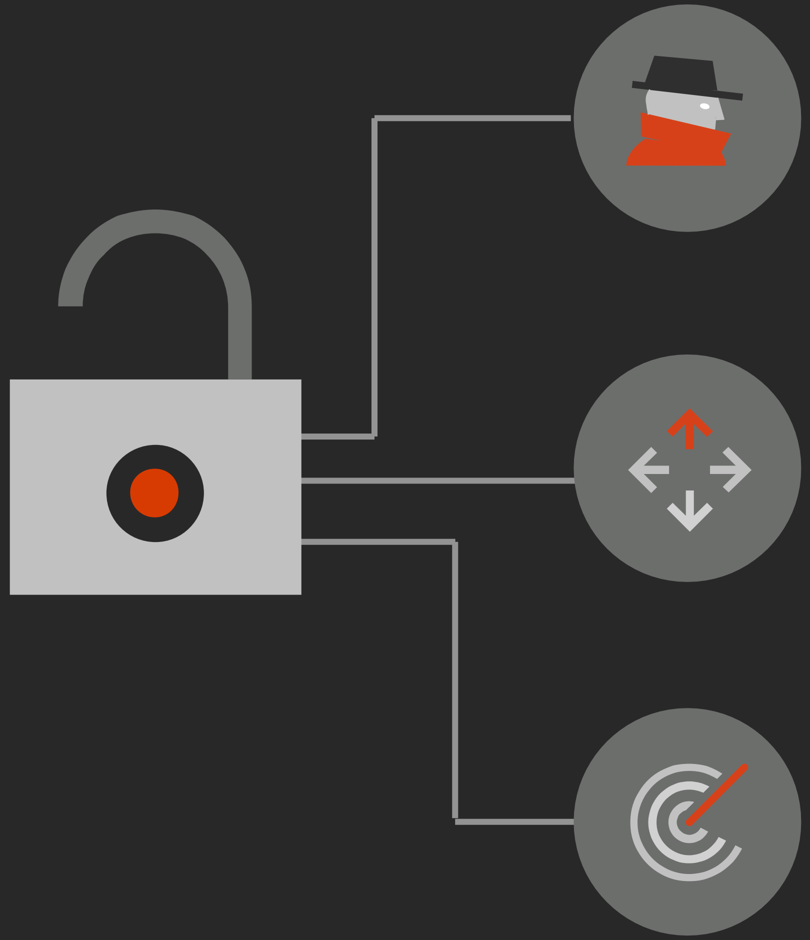
Product name changes

Microsoft Threat Protection	→	**Microsoft 365 Defender**
Azure Security Center (Cloud Workload Protection Platform)	→	**Azure Defender**
Microsoft Defender Advanced Threat Protection	→	**Microsoft Defender for Endpoint**
Office 365 Advanced Threat Protection	→	**Microsoft Defender for Office 365**
Azure Advanced Threat Protection	→	**Microsoft Defender for Identity**

Microsoft 365 Defender + Azure Defender = Microsoft Defender

Disclaimer:
On September 22, 2020 the new Microsoft Defender brand names were announced. Some information in this presentation may relate to the previous product names.
For more information on Microsoft Defender visit aka.ms/SIEMandXDR

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]

280 days

Average time to identify and contain a breach[2]

$26B

Loss attributed to business email compromise since 2016[3]

20%

Phish emails users click on within 5 mins[4]

[1] Verizon 2019 Data Breach Investigations Report | [2] IBM Cost of a Data Breach Report 2020 | [3] US Federal Bureau of Investigation, April 2019 | [4] Microsoft

Challenges with SecOps

$1.37M

Average that an organization spends annually in time wasted responding to erroneous malware alerts[1]

Over 80%

of data breaches involve use of stolen credentials or brute force[2]

70

Security products from 35 vendors Is the average for companies with over 1,000 employees[3]

Only 20%

of SecOps professionals feel their organization’s capabilities are mature[4]

[1]“The Cost of Insecure Endpoints” Ponemon Institute© Research Report [2]Verizon Data Breach Investigations Report 2020 [3]Nick McQuire, VP Enterprise Research CCS Insight. [4]The Road to Security Operations Maturity, Siemplify, 2019

Why Microsoft?

Our unique advantages.

Native protection
for Office 365

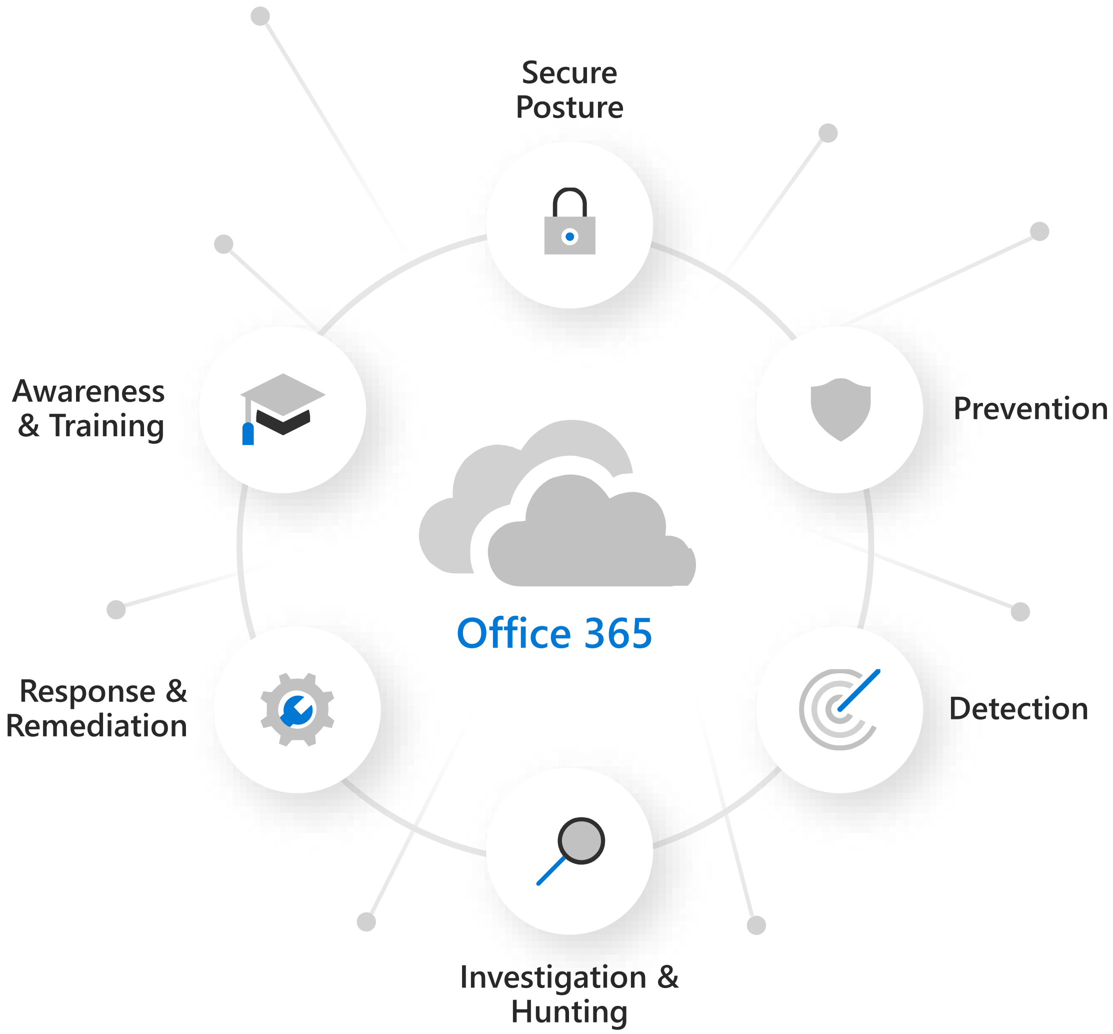
Industry-leading AI
and automation

Comprehensive
approach

Native protection for Office 365

Industry-leading
AI and automation

Comprehensive approach



Secure Posture

Awareness & Training

Prevention

Office 365

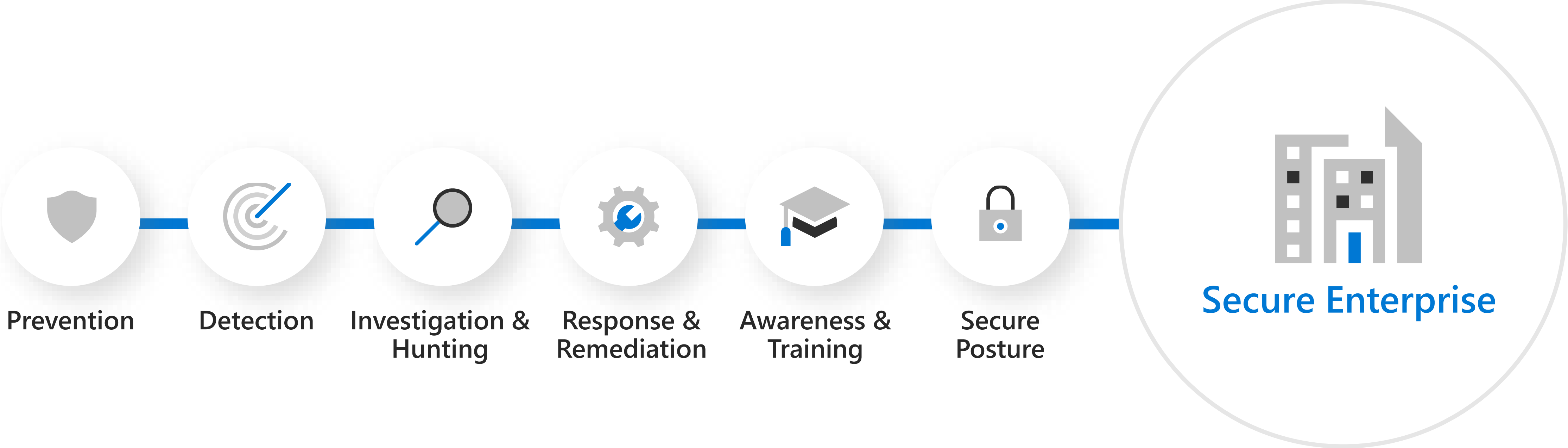
Response & Remediation

Detection

Investigation & Hunting

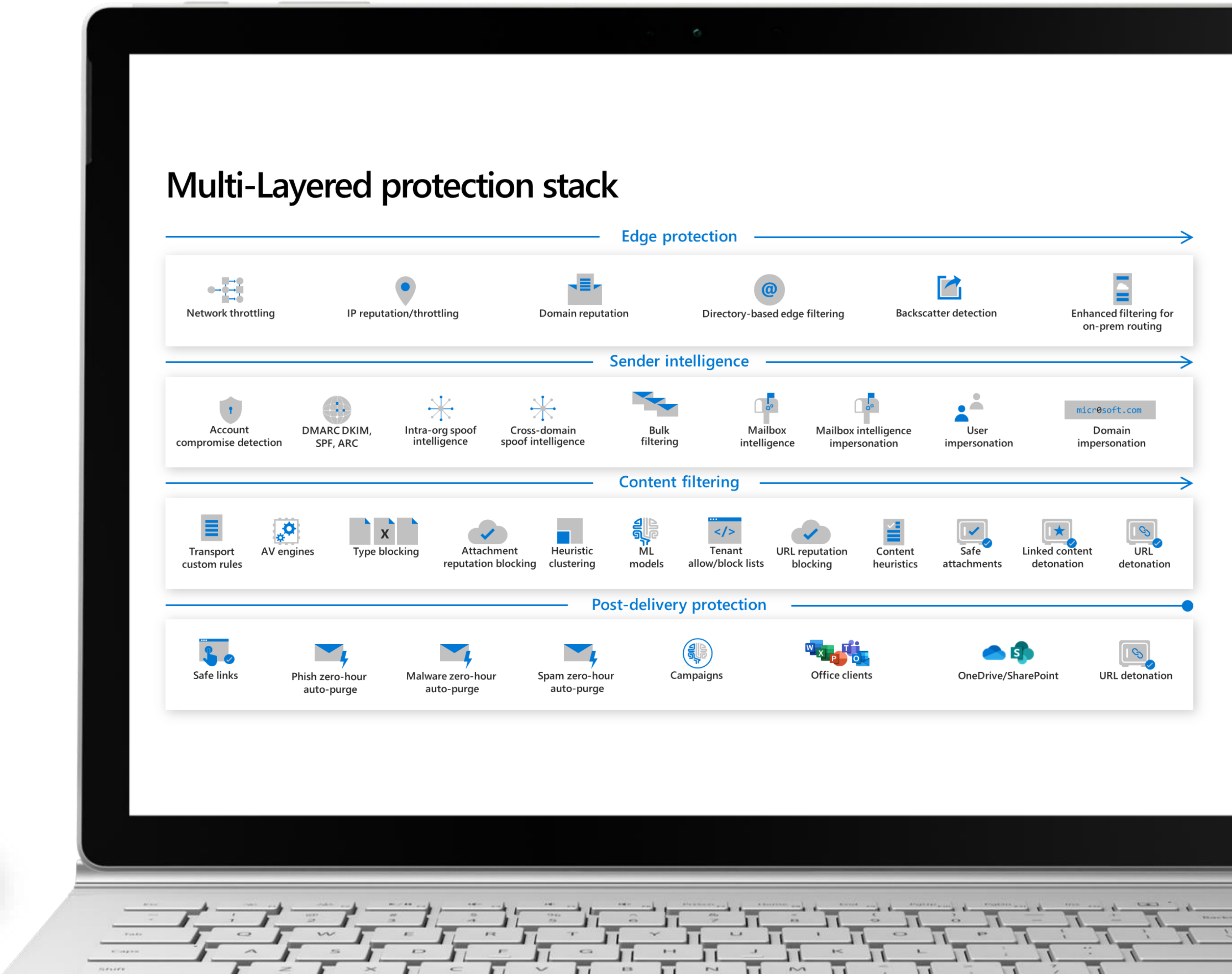
Microsoft Defender for Office 365

Securing your enterprise requires more than just prevention



Prevention

- → Multi-layered filtering stack to protects against wide variety of attacks



Multi-Layered protection stack

Edge protection

Network throttling | IP reputation/throttling | Domain reputation | Directory-based edge filtering | Backscatter detection | Enhanced filtering for on-prem routing

Sender intelligence

Account compromise detection | DMARC DKIM, SPF, ARC | Intra-org spoof intelligence | Cross-domain spoof intelligence | Bulk filtering | Mailbox intelligence | Mailbox intelligence impersonation | User impersonation | Domain impersonation

Content filtering

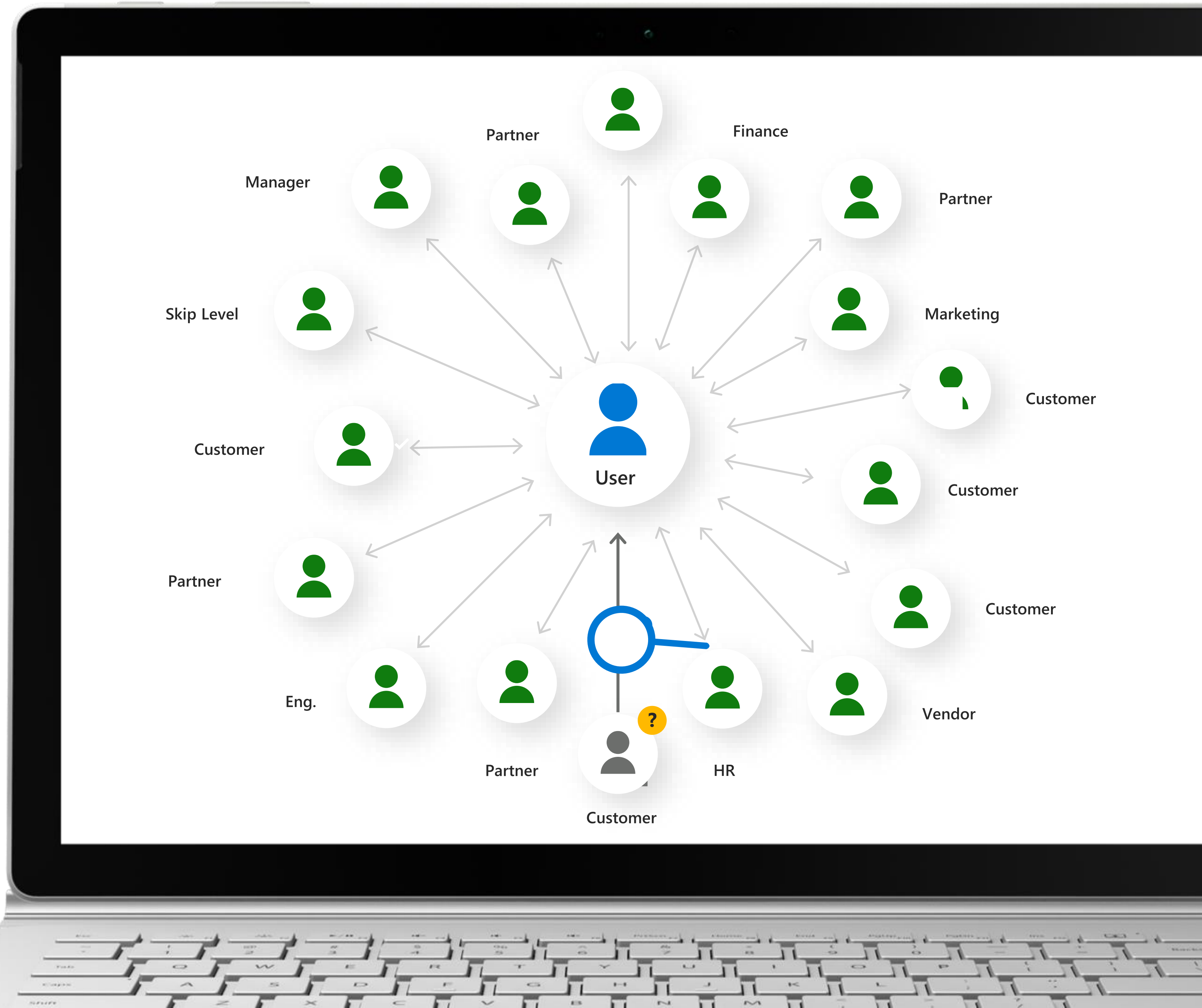
Transport custom rules | AV engines | Type blocking | Attachment reputation blocking | Heuristic clustering | ML models | Tenant allow/block lists | URL reputation blocking | Content heuristics | Safe attachments | Linked content detonation | URL detonation

Post-delivery protection

Safe links | Phish zero-hour auto-purge | Malware zero-hour auto-purge | Spam zero-hour auto-purge | Campaigns | Office clients | OneDrive/SharePoint | URL detonation

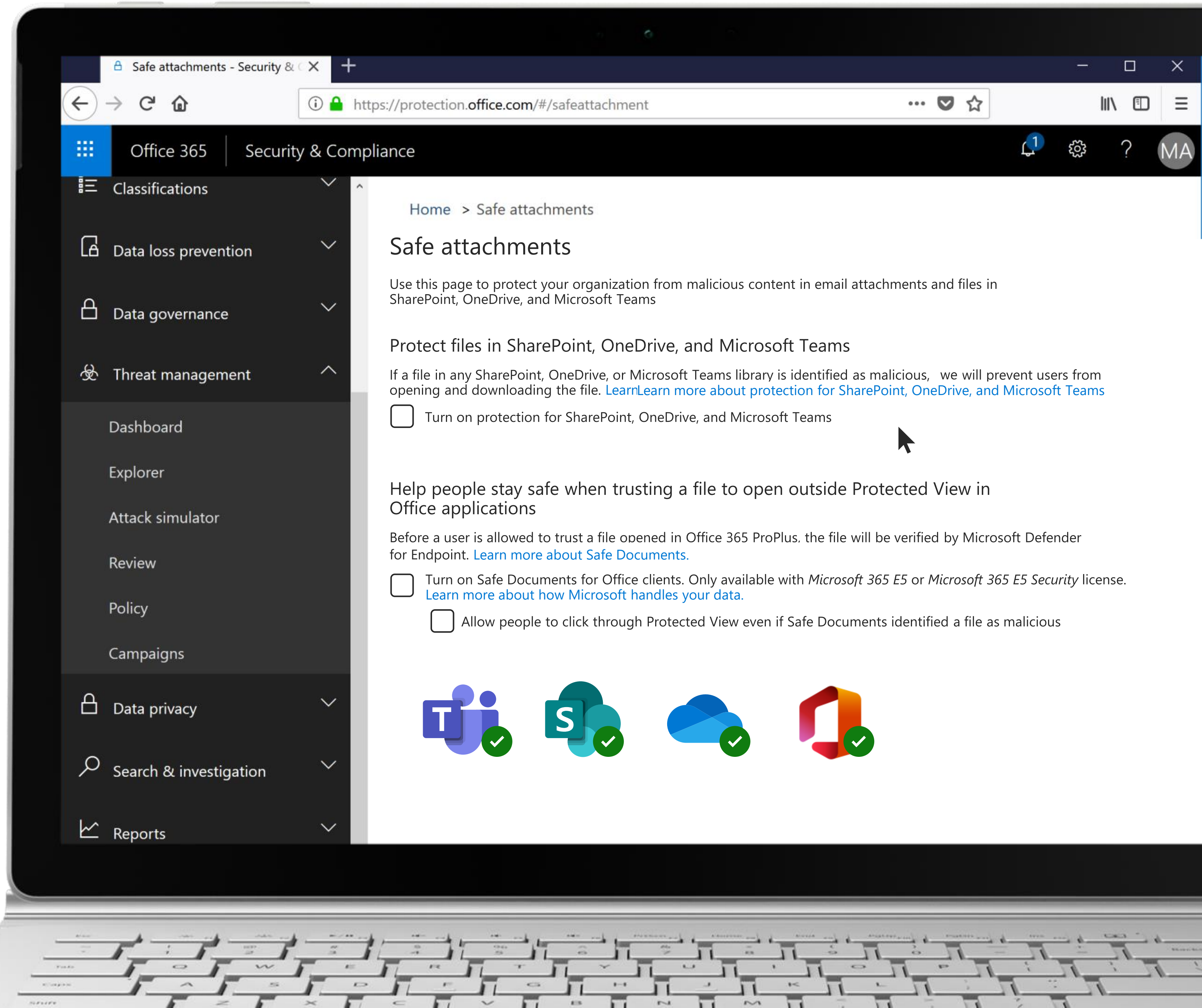
Prevention

- → Multi-layered filtering stack to protects against wide variety of attacks
- → Advanced protection against credential phishing, BEC, and account takeover



Prevention

- → Multi-layered filtering stack to protects against wide variety of attacks
- → Advanced protection against credential phishing, BEC, and account takeover
- → Protection beyond email



Home > Safe attachments

Safe attachments

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams

Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, we will prevent users from opening and downloading the file. LearnLearn more about protection for SharePoint, OneDrive, and Microsoft Teams

□ Turn on protection for SharePoint, OneDrive, and Microsoft Teams

Help people stay safe when trusting a file to open outside Protected View in Office applications

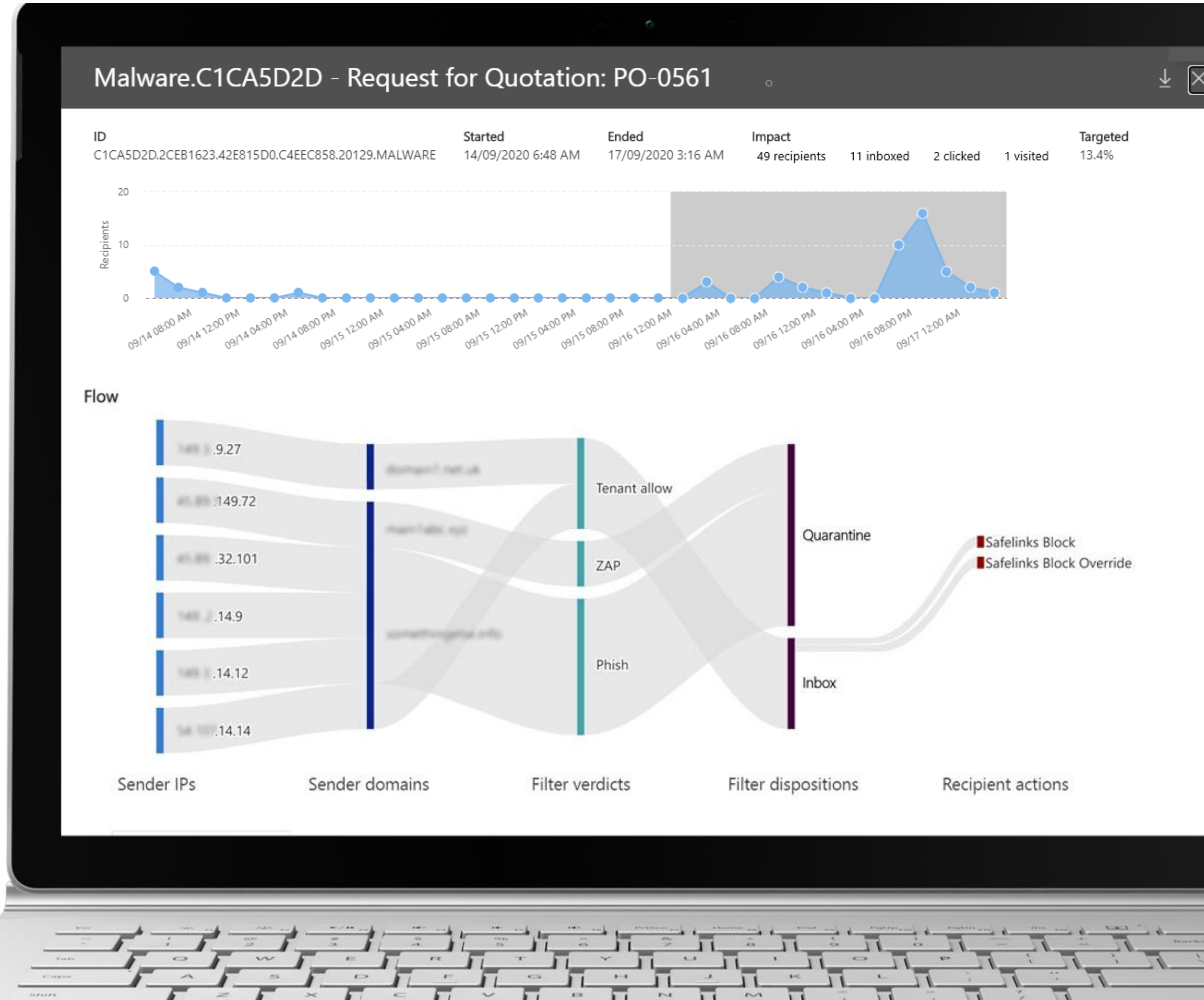
Before a user is allowed to trust a file opened in Office 365 ProPlus, the file will be verified by Microsoft Defender for Endpoint. Learn more about Safe Documents.

□ Turn on Safe Documents for Office clients. Only available with *Microsoft 365 E5* or *Microsoft 365 E5 Security* license. Learn more about how Microsoft handles your data.

□ Allow people to click through Protected View even if Safe Documents identified a file as malicious

Detection

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



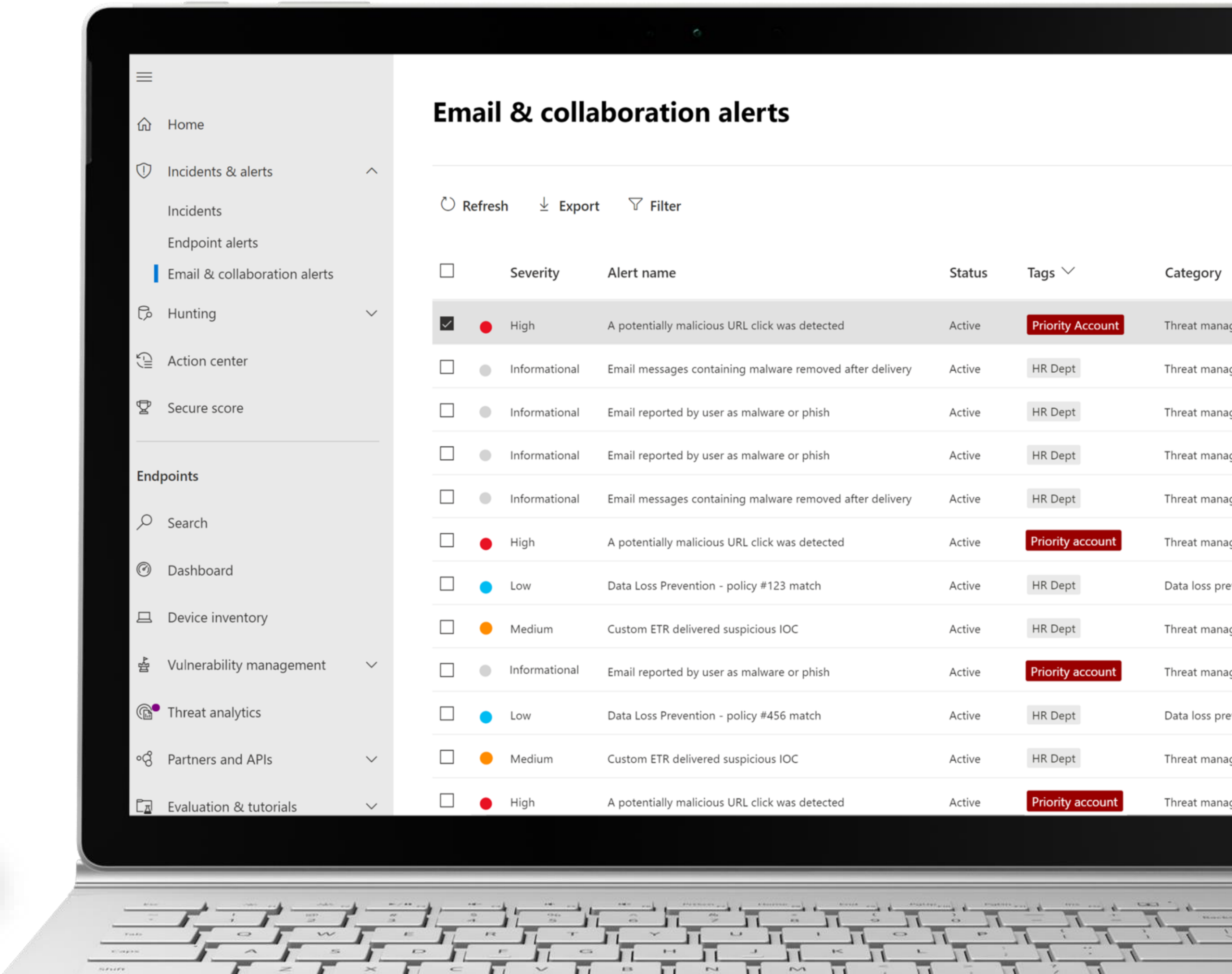
Malware.C1CA5D2D - Request for Quotation: PO-0561

ID	Started	Ended	Impact				Targeted
C1CA5D2D.2CEB1623.42E815D0.C4EEC858.20129.MALWARE	14/09/2020 6:48 AM	17/09/2020 3:16 AM	49 recipients	11 inboxed	2 clicked	1 visited	13.4%

Flow

Detection

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



Home

Incidents & alerts

Incidents

Endpoint alerts

Email & collaboration alerts

Hunting

Action center

Secure score

Endpoints

Search

Dashboard

Device inventory

Vulnerability management

Threat analytics

Partners and APIs

Evaluation & tutorials

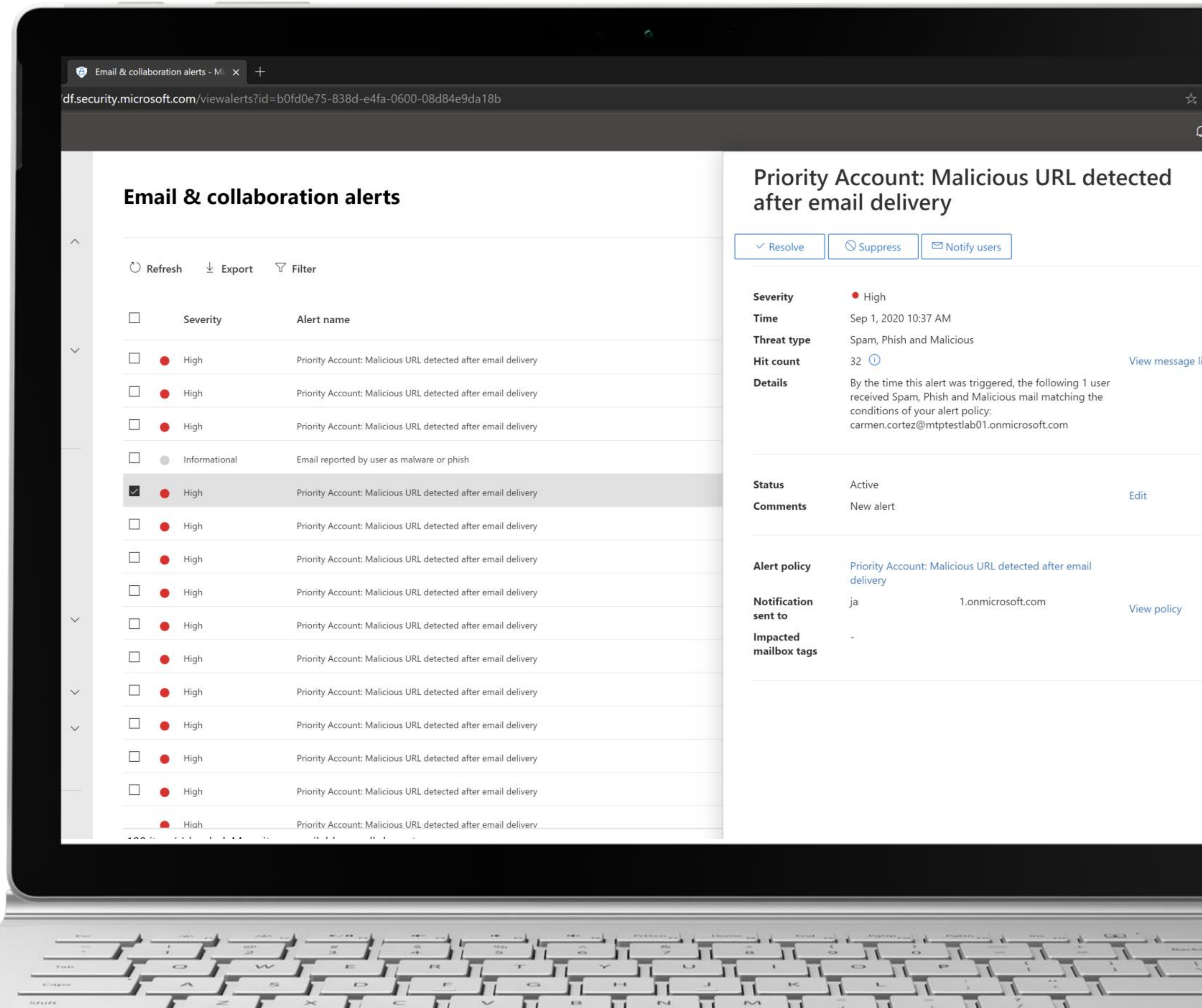
Email & collaboration alerts

Refresh Export Filter

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



Email & collaboration alerts - M ✕ +

df.security.microsoft.com/viewalerts?id=b0fd0e75-838d-e4fa-0600-08d84e9da18b

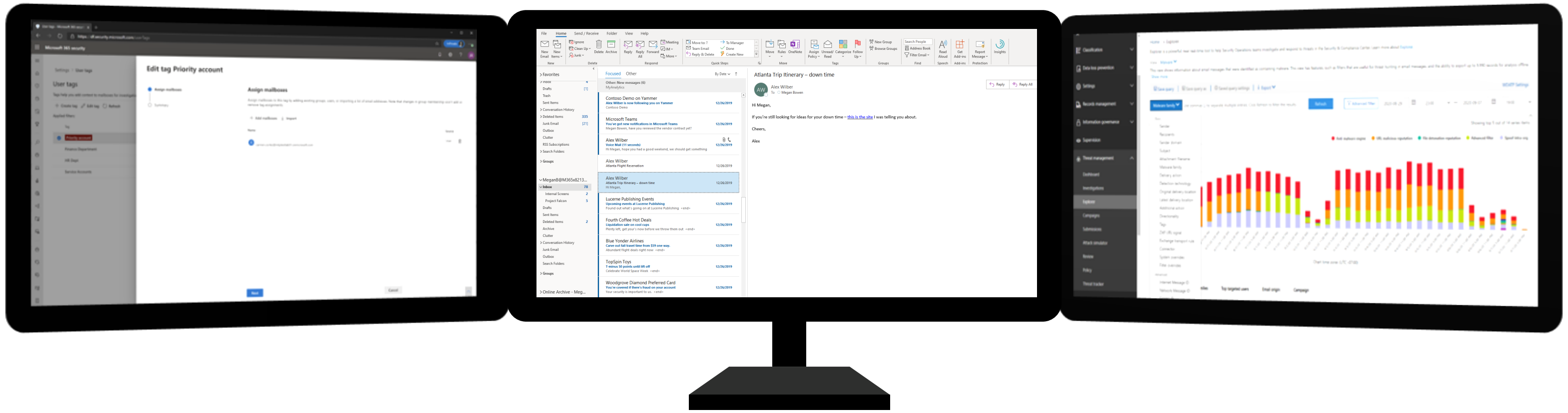
Email & collaboration alerts

□	Severity	Alert name
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● Informational	Email reported by user as malware or phish
☑	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
□	● High	Priority Account: Malicious URL detected after email delivery
	● High	Priority Account: Malicious URL detected after email delivery

Priority Account: Malicious URL detected after email delivery

Severity	● High
Time	Sep 1, 2020 10:37 AM
Threat type	Spam, Phish and Malicious
Hit count	32 ⓘ
Details	By the time this alert was triggered, the following 1 user received Spam, Phish and Malicious mail matching the conditions of your alert policy: carmen.cortez@mtptestlab01.onmicrosoft.com
Status	Active
Comments	New alert
Alert policy	Priority Account: Malicious URL detected after email delivery
Notification sent to	ja 1.onmicrosoft.com
Impacted mailbox tags	-

Investigation & Hunting



Other: New messages (6)
MyAnalytics

Contoso Demo on Yammer
Alex Wilber is now following you on Yammer 12/26/2019
Contoso Demo

Microsoft Teams
You've got new notifications in Microsoft Teams 12/26/2019
Megan Bowen, have you reviewed the vendor contract yet?

Alex Wilber
Voice Mail (11 seconds) 12/26/2019
Hi Megan, hope you had a good weekend, we should get something

Alex Wilber
Atlanta Flight Reservation 12/26/2019

Alex Wilber
Atlanta Trip Itinerary – down time 12/26/2019
Hi Megan,

Lucerne Publishing Events
Upcoming events at Lucerne Publishing 12/26/2019
Found out what's going on at Lucerne Publishing <end>

Fourth Coffee Hot Deals
Liquidation sale on cool cups 12/26/2019
Plenty left, get your's now before we throw them out <end>

Blue Yonder Airlines
Carve out fall travel time from $59 one way. 12/26/2019
Abundant flight deals right now <end>

TopSpin Toys
T-minus 50 points until lift off 12/26/2019
Celebrate World Space Week <end>

Woodgrove Diamond Preferred Card
You're covered if there's fraud on your account 12/26/2019
Your security is important to us. <end>

Atlanta Trip Itinerary – down time

AW Alex Wilber
To Megan Bowen

Reply Reply All

Hi Megan,

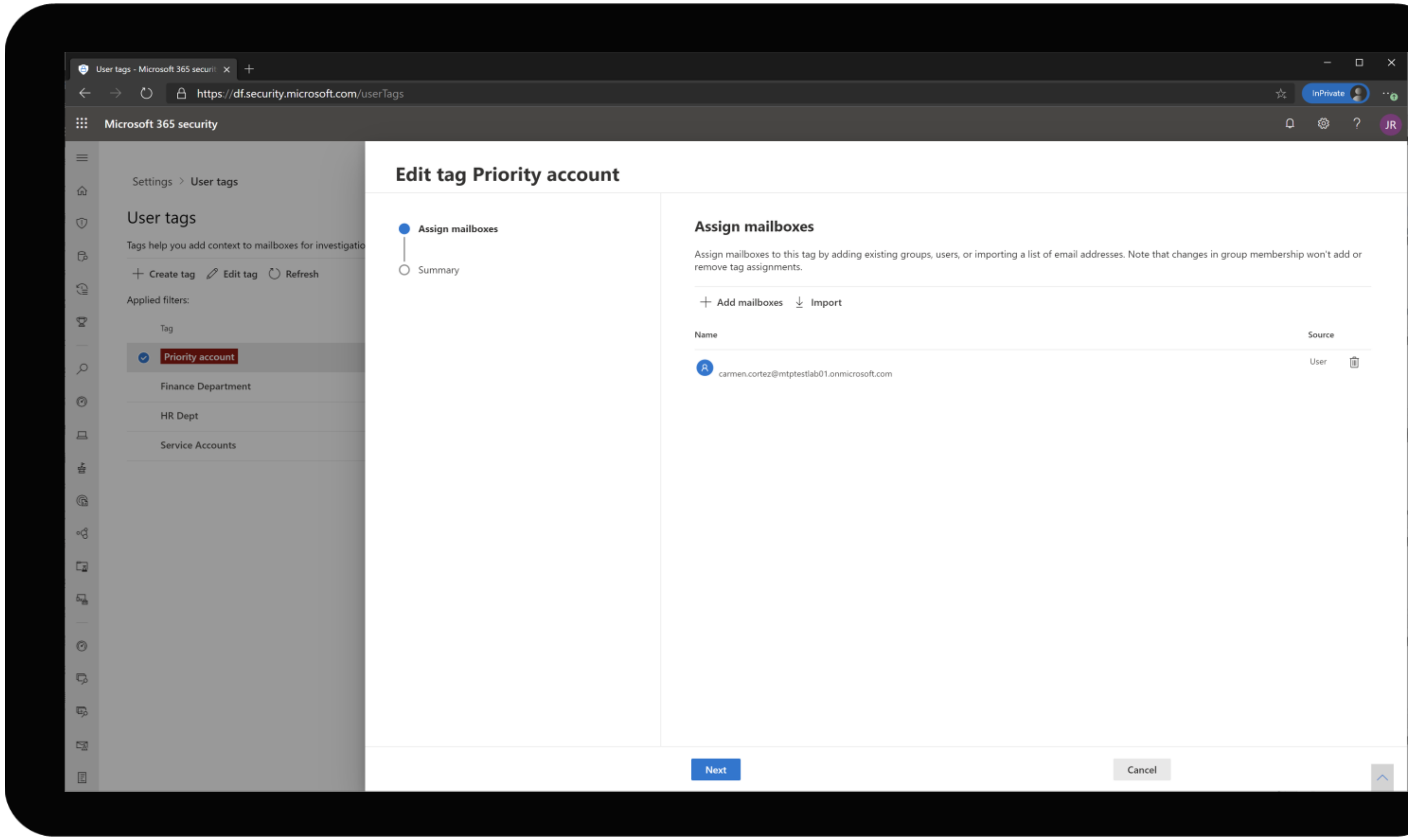
If you're still looking for ideas for your down time – this is the site I was telling you about.

Cheers,

Alex

Investigation & Hunting

→ Prioritized focus through Priority accounts



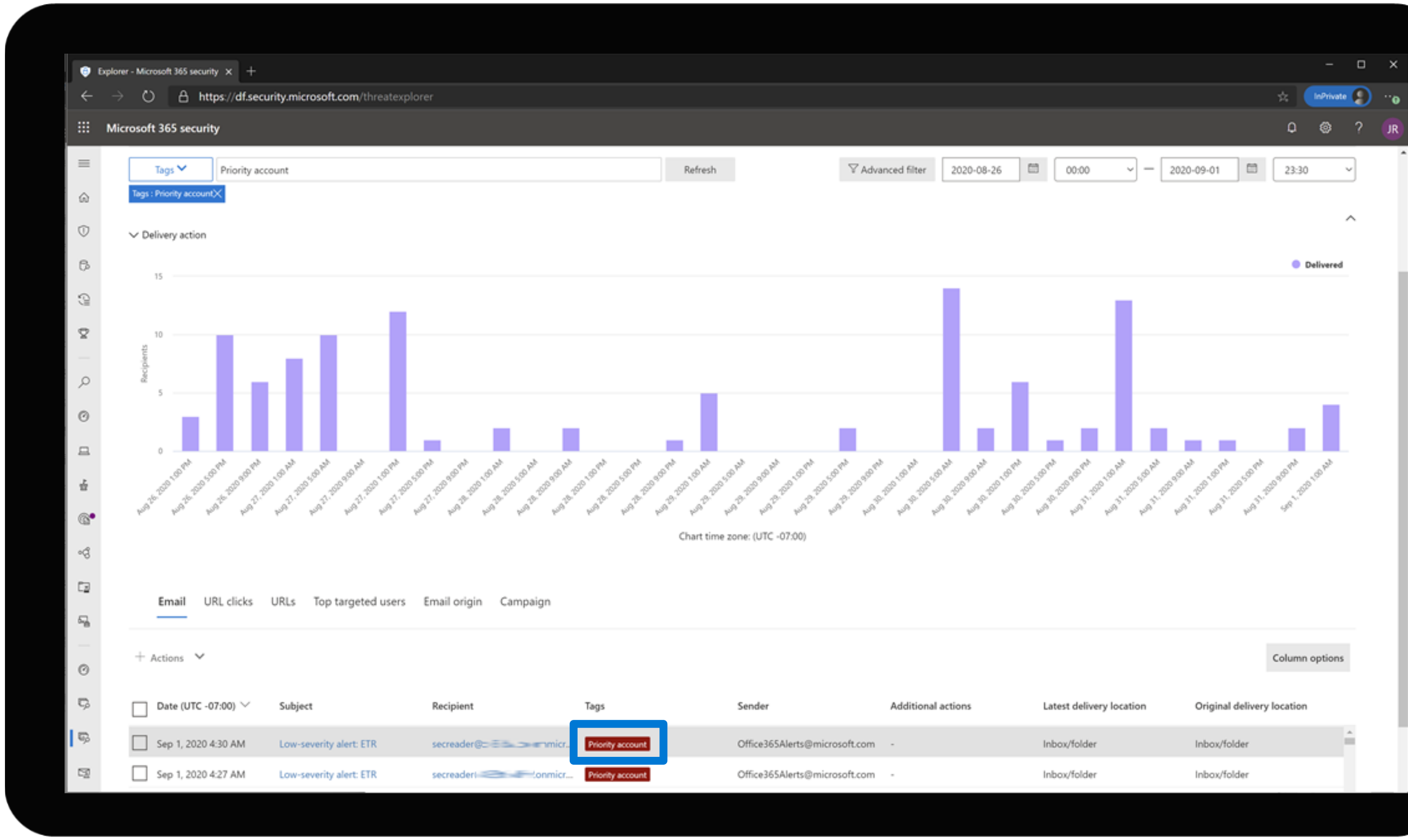
Tags help you add context to mailboxes for investigatio

Assign mailboxes to this tag by adding existing groups, users, or importing a list of email addresses. Note that changes in group membership won't add or remove tag assignments.

Name	Source
carmen.cortez@mtptestlab01.onmicrosoft.com	User

Investigation & Hunting

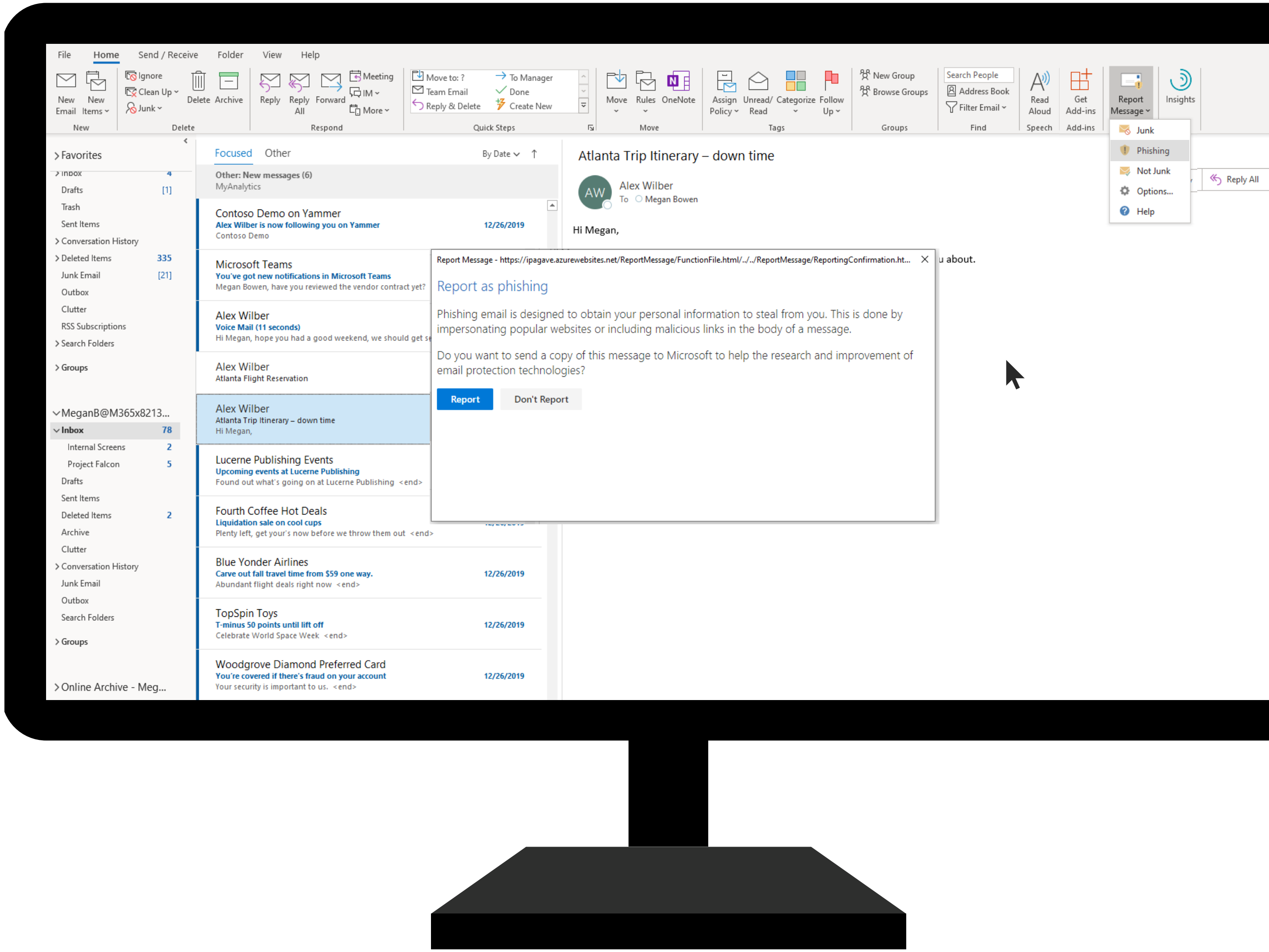
→ Prioritized focus through Priority accounts



□ Date (UTC -07:00)	Subject	Recipient	Tags	Sender	Additional actions	Latest delivery location	Original delivery location
□ Sep 1, 2020 4:30 AM	Low-severity alert: ETR	secreader@[redacted]micr...	Priority account	Office365Alerts@microsoft.com	-	Inbox/folder	Inbox/folder
□ Sep 1, 2020 4:27 AM	Low-severity alert: ETR	secreader[redacted]onmicr...	Priority account	Office365Alerts@microsoft.com	-	Inbox/folder	Inbox/folder

Investigation & Hunting

- → Prioritized focus through Priority accounts
- → User & Admin Submissions



Other: New messages (6)
MyAnalytics

Contoso Demo on Yammer
Alex Wilber is now following you on Yammer 12/26/2019
Contoso Demo

Microsoft Teams
You've got new notifications in Microsoft Teams
Megan Bowen, have you reviewed the vendor contract yet?

Alex Wilber
Voice Mail (11 seconds)
Hi Megan, hope you had a good weekend, we should get s

Alex Wilber
Atlanta Flight Reservation

Alex Wilber
Atlanta Trip Itinerary – down time
Hi Megan,

Lucerne Publishing Events
Upcoming events at Lucerne Publishing
Found out what's going on at Lucerne Publishing <end>

Fourth Coffee Hot Deals
Liquidation sale on cool cups
Plenty left, get your's now before we throw them out <end>

Blue Yonder Airlines
Carve out fall travel time from $59 one way. 12/26/2019
Abundant flight deals right now <end>

TopSpin Toys
T-minus 50 points until lift off 12/26/2019
Celebrate World Space Week <end>

Woodgrove Diamond Preferred Card
You're covered if there's fraud on your account 12/26/2019
Your security is important to us. <end>

Atlanta Trip Itinerary – down time

AW Alex Wilber
To Megan Bowen

Hi Megan,

u about.

Report Message - https://ipagave.azurewebsites.net/ReportMessage/FunctionFile.html/../../ReportMessage/ReportingConfirmation.ht... ✕

Report as phishing

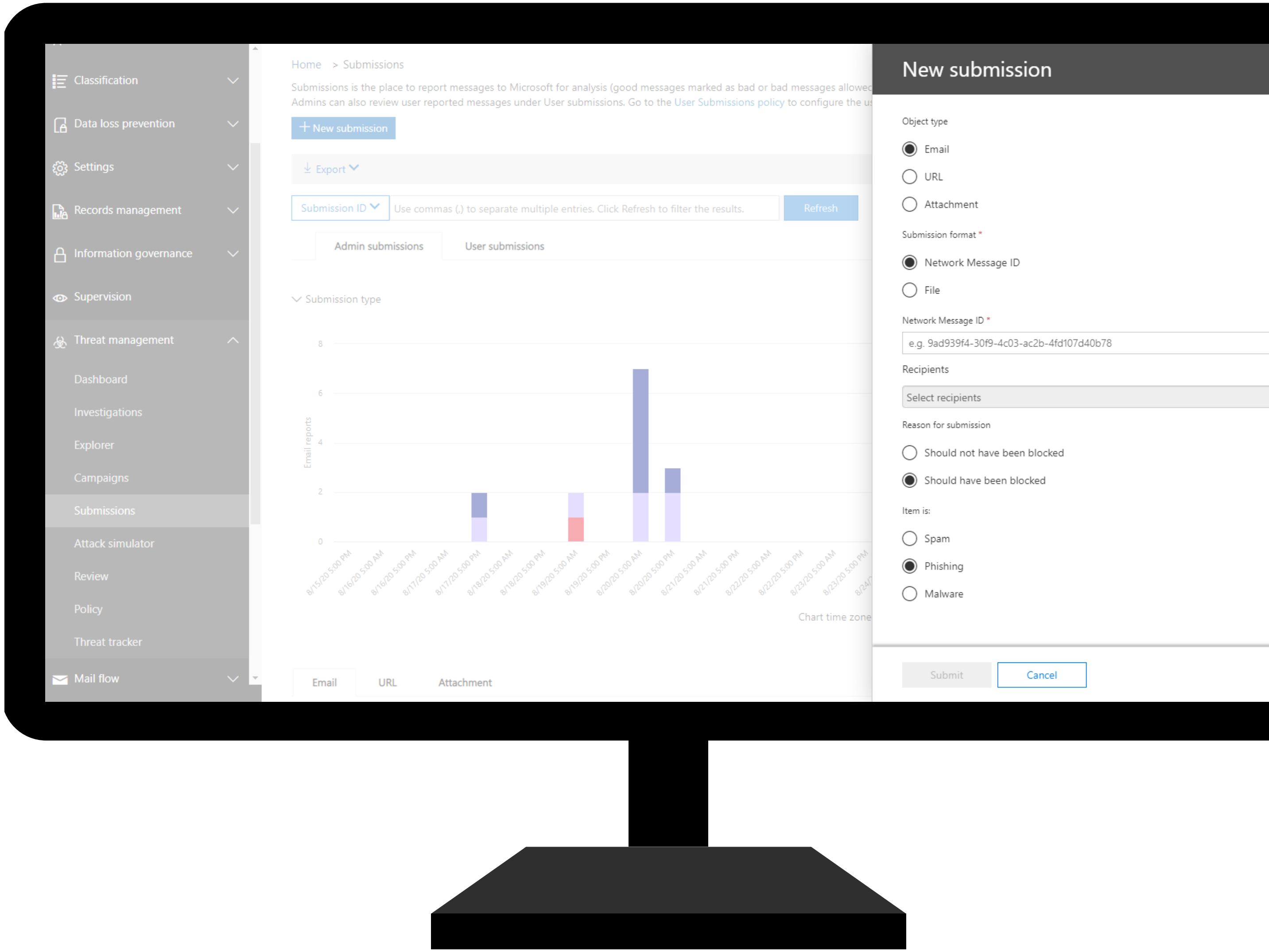
Phishing email is designed to obtain your personal information to steal from you. This is done by impersonating popular websites or including malicious links in the body of a message.

Do you want to send a copy of this message to Microsoft to help the research and improvement of email protection technologies?

Report | Don't Report

Investigation & Hunting

- → Prioritized focus through Priority accounts
- → User & Admin Submissions



Submissions is the place to report messages to Microsoft for analysis (good messages marked as bad or bad messages allowed
Admins can also review user reported messages under User submissions. Go to the User Submissions policy to configure the u

Use commas (,) to separate multiple entries. Click Refresh to filter the results.

New submission

Object type

- ● Email
- ○ URL
- ○ Attachment

Submission format *

- ● Network Message ID
- ○ File

Network Message ID *

e.g. 9ad939f4-30f9-4c03-ac2b-4fd107d40b78

Recipients

Select recipients

Reason for submission

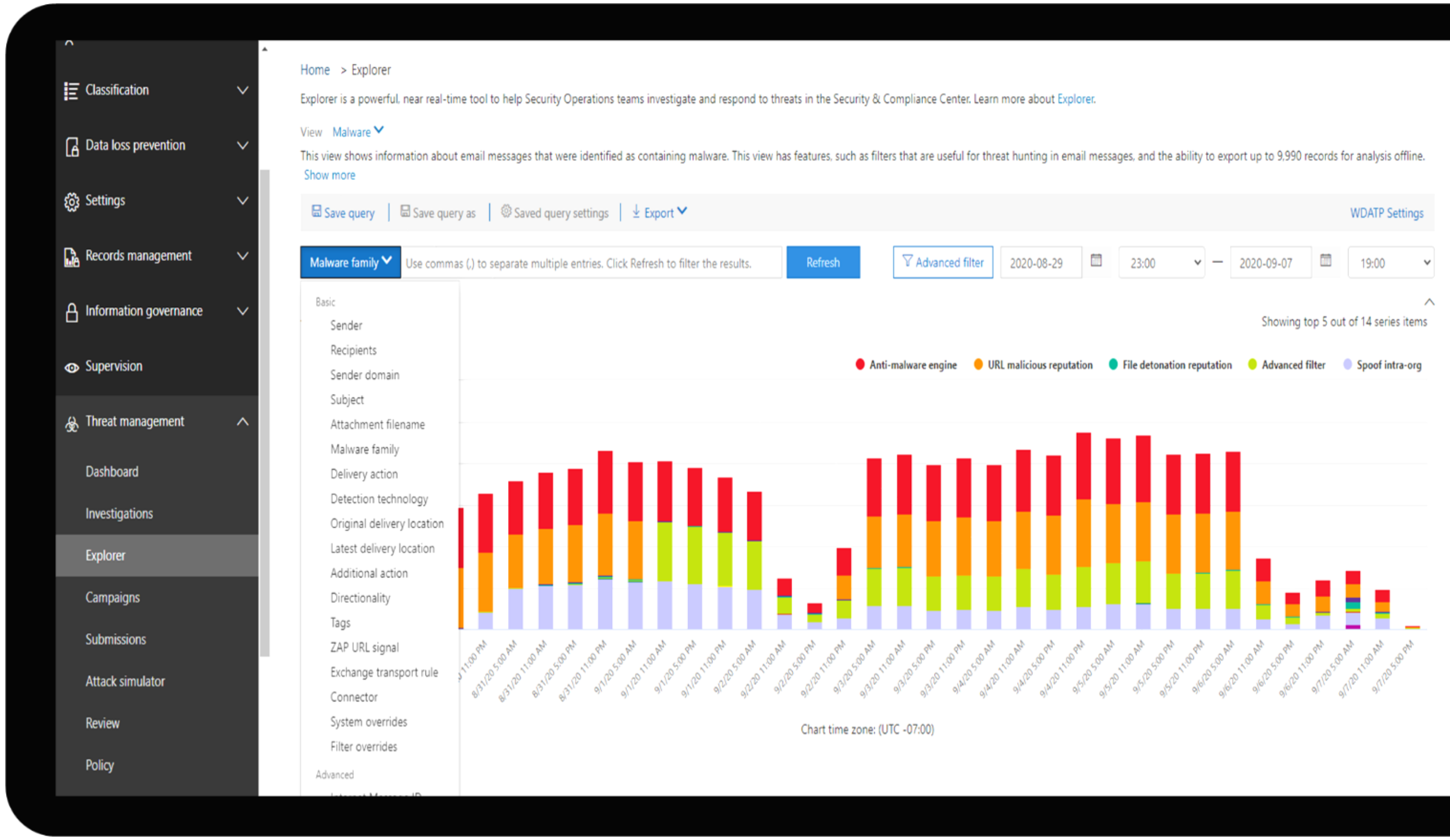
- ○ Should not have been blocked
- ● Should have been blocked

Item is:

- ○ Spam
- ● Phishing
- ○ Malware

Investigation & Hunting

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



Home > Explorer

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.

View Malware

This view shows information about email messages that were identified as containing malware. This view has features, such as filters that are useful for threat hunting in email messages, and the ability to export up to 9,990 records for analysis offline.

Malware family: Use commas (,) to separate multiple entries. Click Refresh to filter the results.

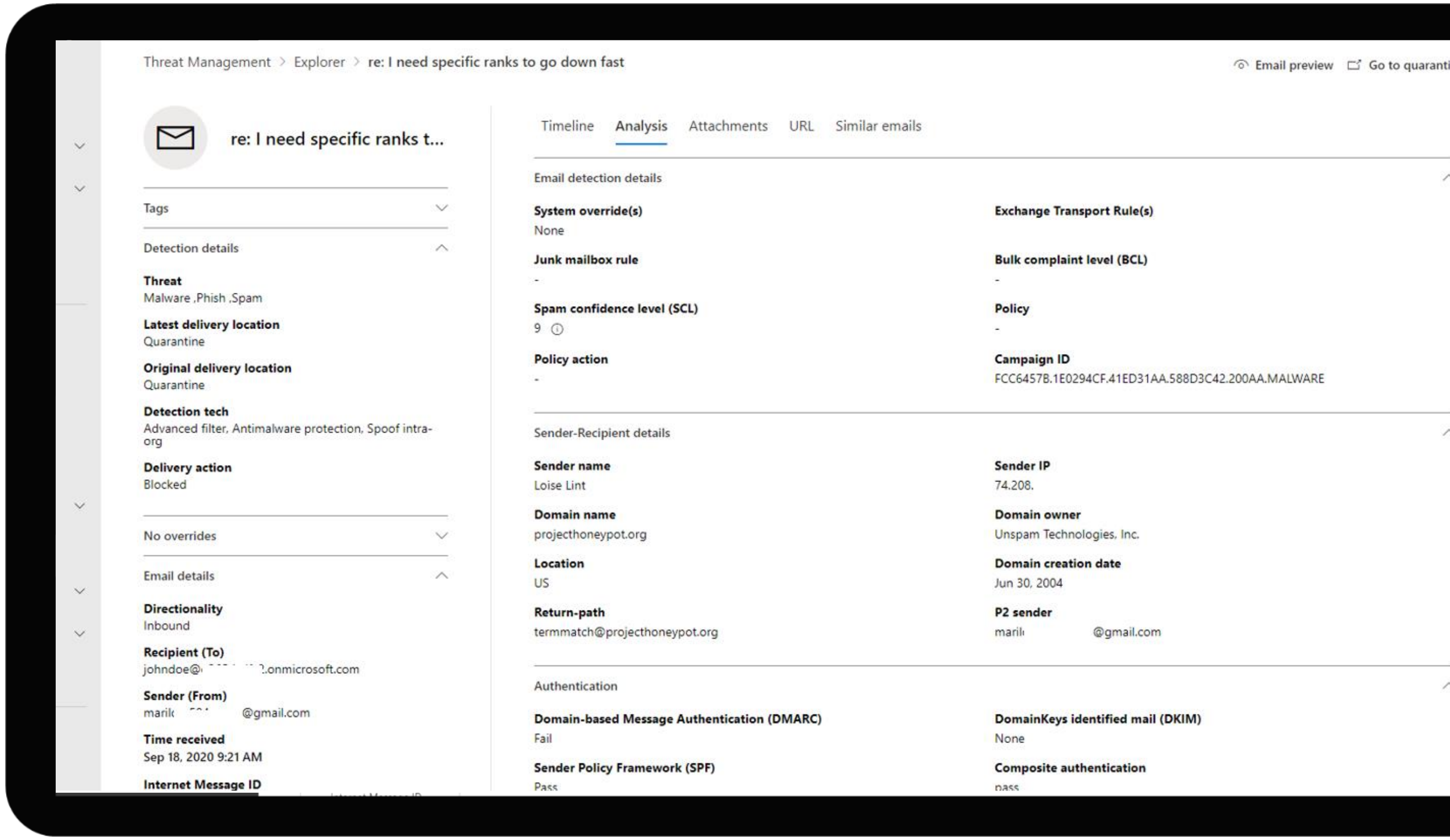
2020-08-29 23:00 — 2020-09-07 19:00

Showing top 5 out of 14 series items

Chart time zone: (UTC -07:00)

Investigation & Hunting

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



Threat Management > Explorer > re: I need specific ranks to go down fast

re: I need specific ranks t...

Detection details

Threat
Malware ,Phish ,Spam

Latest delivery location
Quarantine

Original delivery location
Quarantine

Detection tech
Advanced filter, Antimalware protection, Spoof intra-org

Delivery action
Blocked

No overrides

Email details

Directionality
Inbound

Recipient (To)
johndoe@ .onmicrosoft.com

Sender (From)
marik @gmail.com

Time received
Sep 18, 2020 9:21 AM

Internet Message ID

Email detection details

System override(s)
None

Exchange Transport Rule(s)

Junk mailbox rule
-

Bulk complaint level (BCL)
-

Spam confidence level (SCL)
9 ⓘ

Policy
-

Policy action
-

Campaign ID
FCC6457B.1E0294CF.41ED31AA.588D3C42.200AA.MALWARE

Sender-Recipient details

Sender name
Loise Lint

Sender IP
74.208.

Domain name
projecthoneypot.org

Domain owner
Unspam Technologies, Inc.

Location
US

Domain creation date
Jun 30, 2004

Return-path
termmatch@projecthoneypot.org

P2 sender
marik @gmail.com

Authentication

Domain-based Message Authentication (DMARC)
Fail

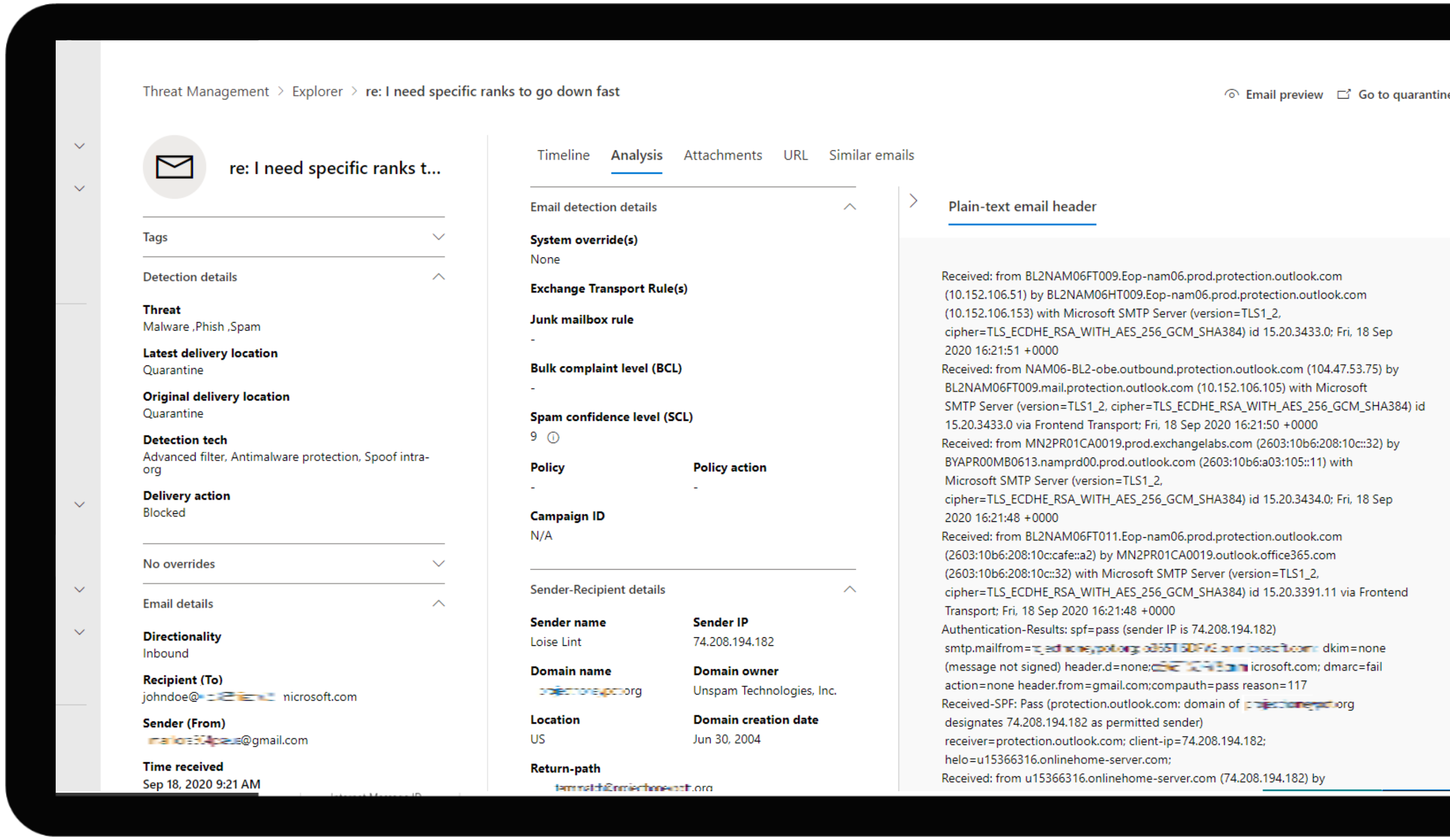
DomainKeys identified mail (DKIM)
None

Sender Policy Framework (SPF)
Pass

Composite authentication
pass

Investigation & Hunting

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



Threat Management > Explorer > re: I need specific ranks to go down fast

re: I need specific ranks t...

Threat
Malware ,Phish ,Spam

Latest delivery location
Quarantine

Original delivery location
Quarantine

Detection tech
Advanced filter, Antimalware protection, Spoof intra-org

Delivery action
Blocked

Directionality
Inbound

Recipient (To)
johndoe@[redacted] nicrosoft.com

Sender (From)
[redacted]@gmail.com

Time received
Sep 18, 2020 9:21 AM

System override(s)
None

Exchange Transport Rule(s)

Junk mailbox rule
-

Bulk complaint level (BCL)
-

Spam confidence level (SCL)
9 ⓘ

Policy
-

Policy action
-

Campaign ID
N/A

Sender name
Loise Lint

Sender IP
74.208.194.182

Domain name
[redacted]org

Domain owner
Unspam Technologies, Inc.

Location
US

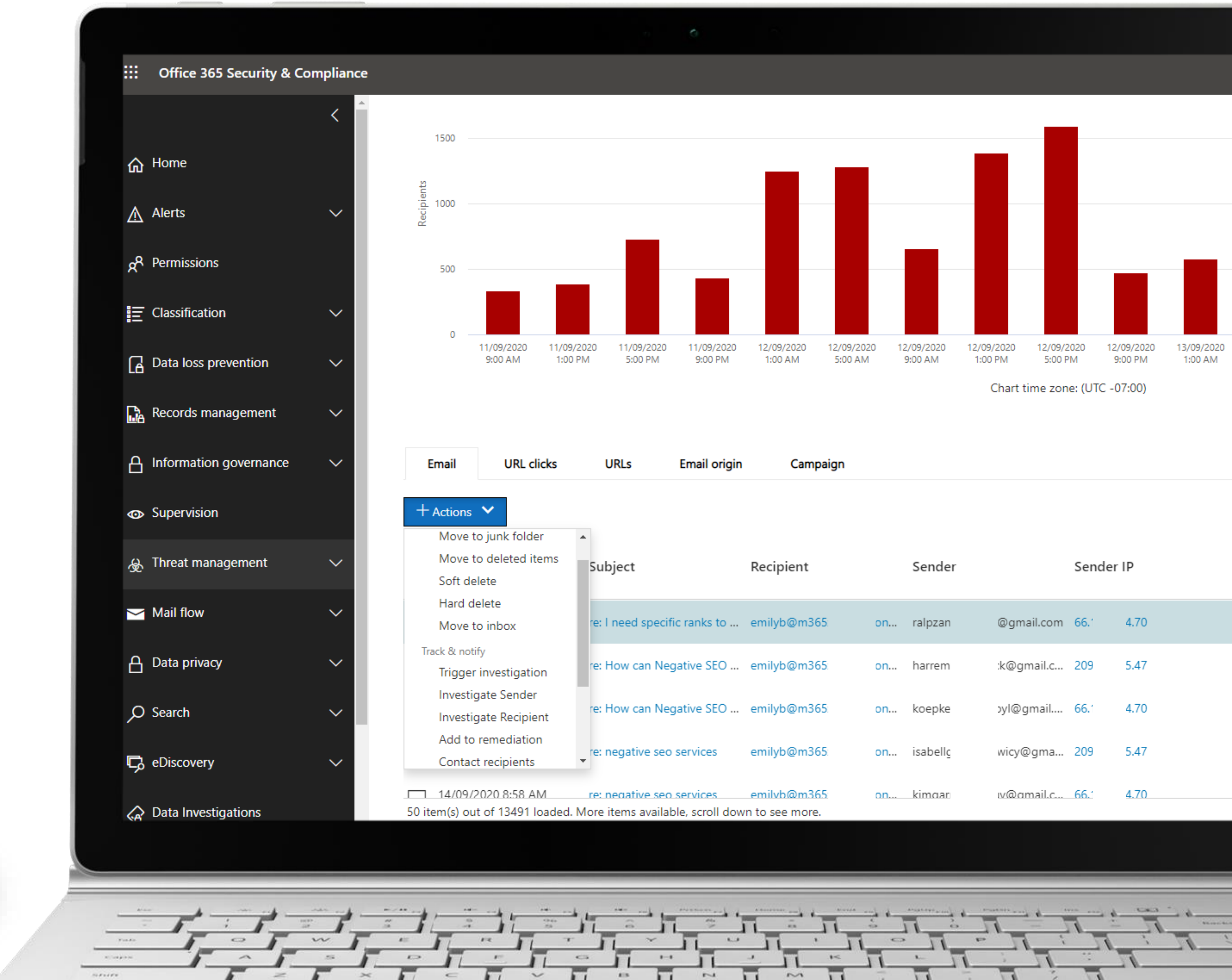
Domain creation date
Jun 30, 2004

Return-path
[redacted].org

```
Received: from BL2NAM06FT009.Eop-nam06.prod.protection.outlook.com
 (10.152.106.51) by BL2NAM06HT009.Eop-nam06.prod.protection.outlook.com
 (10.152.106.153) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3433.0; Fri, 18 Sep
 2020 16:21:51 +0000
Received: from NAM06-BL2-obe.outbound.protection.outlook.com (104.47.53.75) by
 BL2NAM06FT009.mail.protection.outlook.com (10.152.106.105) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.3433.0 via Frontend Transport; Fri, 18 Sep 2020 16:21:50 +0000
Received: from MN2PR01CA0019.prod.exchangelabs.com (2603:10b6:208:10c::32) by
 BYAPR00MB0613.namprd00.prod.outlook.com (2603:10b6:a03:105::11) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3434.0; Fri, 18 Sep
 2020 16:21:48 +0000
Received: from BL2NAM06FT011.Eop-nam06.prod.protection.outlook.com
 (2603:10b6:208:10c:cafe::a2) by MN2PR01CA0019.outlook.office365.com
 (2603:10b6:208:10c::32) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3391.11 via Frontend
 Transport; Fri, 18 Sep 2020 16:21:48 +0000
Authentication-Results: spf=pass (sender IP is 74.208.194.182)
 smtp.mailfrom=[redacted] dkim=none
 (message not signed) header.d=none;[redacted] icrosoft.com; dmarc=fail
 action=none header.from=gmail.com;compauth=pass reason=117
Received-SPF: Pass (protection.outlook.com: domain of [redacted]org
 designates 74.208.194.182 as permitted sender)
 receiver=protection.outlook.com; client-ip=74.208.194.182;
 helo=u15366316.onlinehome-server.com;
Received: from u15366316.onlinehome-server.com (74.208.194.182) by
```

Response & Remediation

→ Guided hunting with inline actions

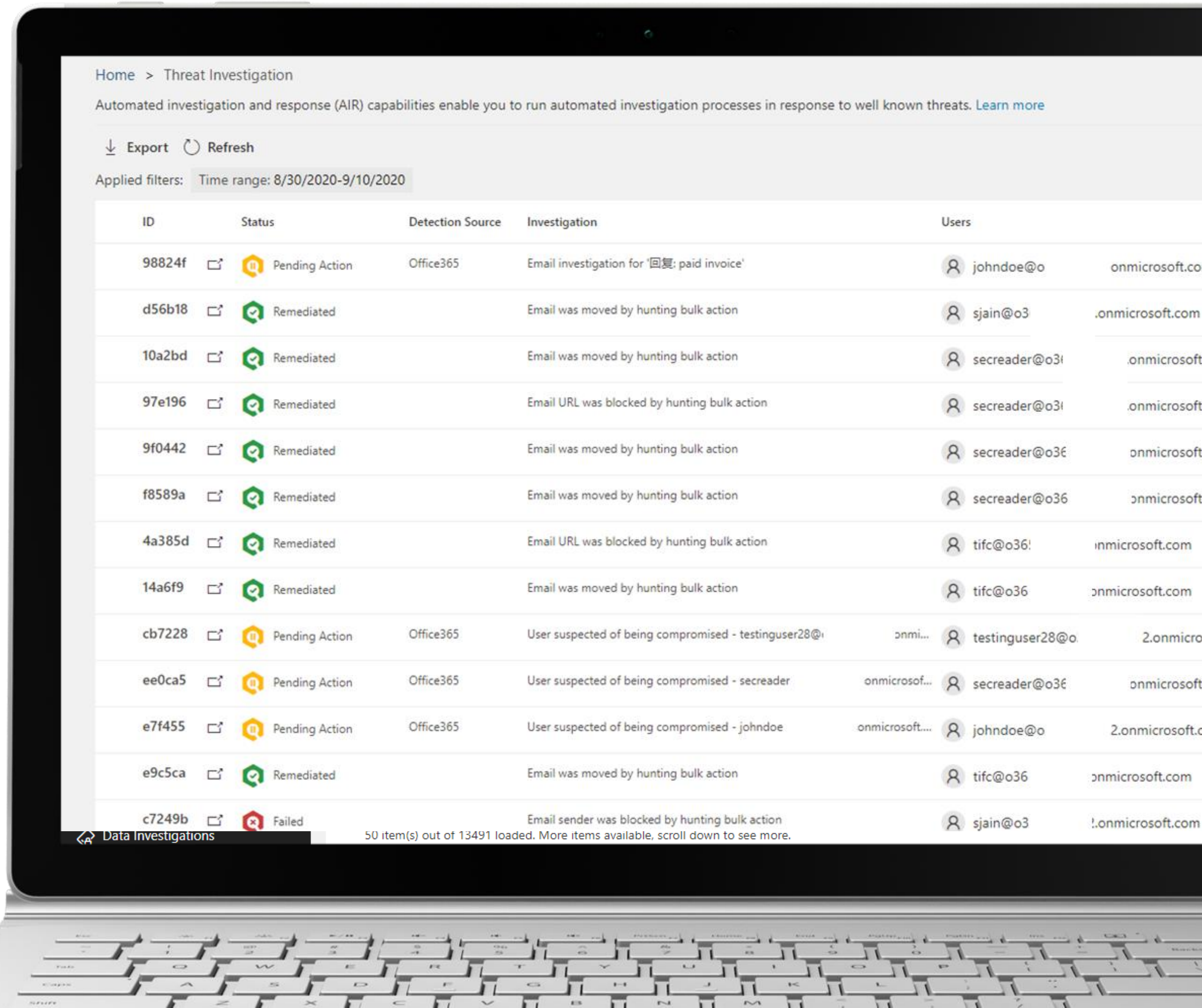


	Subject	Recipient		Sender		Sender IP	
	re: I need specific ranks to ...	emilyb@m365:	on...	ralpzan	@gmail.com	66.1	4.70
	re: How can Negative SEO ...	emilyb@m365:	on...	harrem	:k@gmail.c...	209	5.47
	re: How can Negative SEO ...	emilyb@m365:	on...	koepke	yl@gmail....	66.1	4.70
	re: negative seo services	emilyb@m365:	on...	isabellg	wicy@gma...	209	5.47
□ 14/09/2020 8:58 AM	re: negative seo services	emilyb@m365:	on...	kimgar	v@gmail.c...	66.1	4.70

50 item(s) out of 13491 loaded. More items available, scroll down to see more.

Response & Remediation

- → Guided hunting with inline actions
- → Automated response playbooks



Home > Threat Investigation

Automated investigation and response (AIR) capabilities enable you to run automated investigation processes in response to well known threats. Learn more

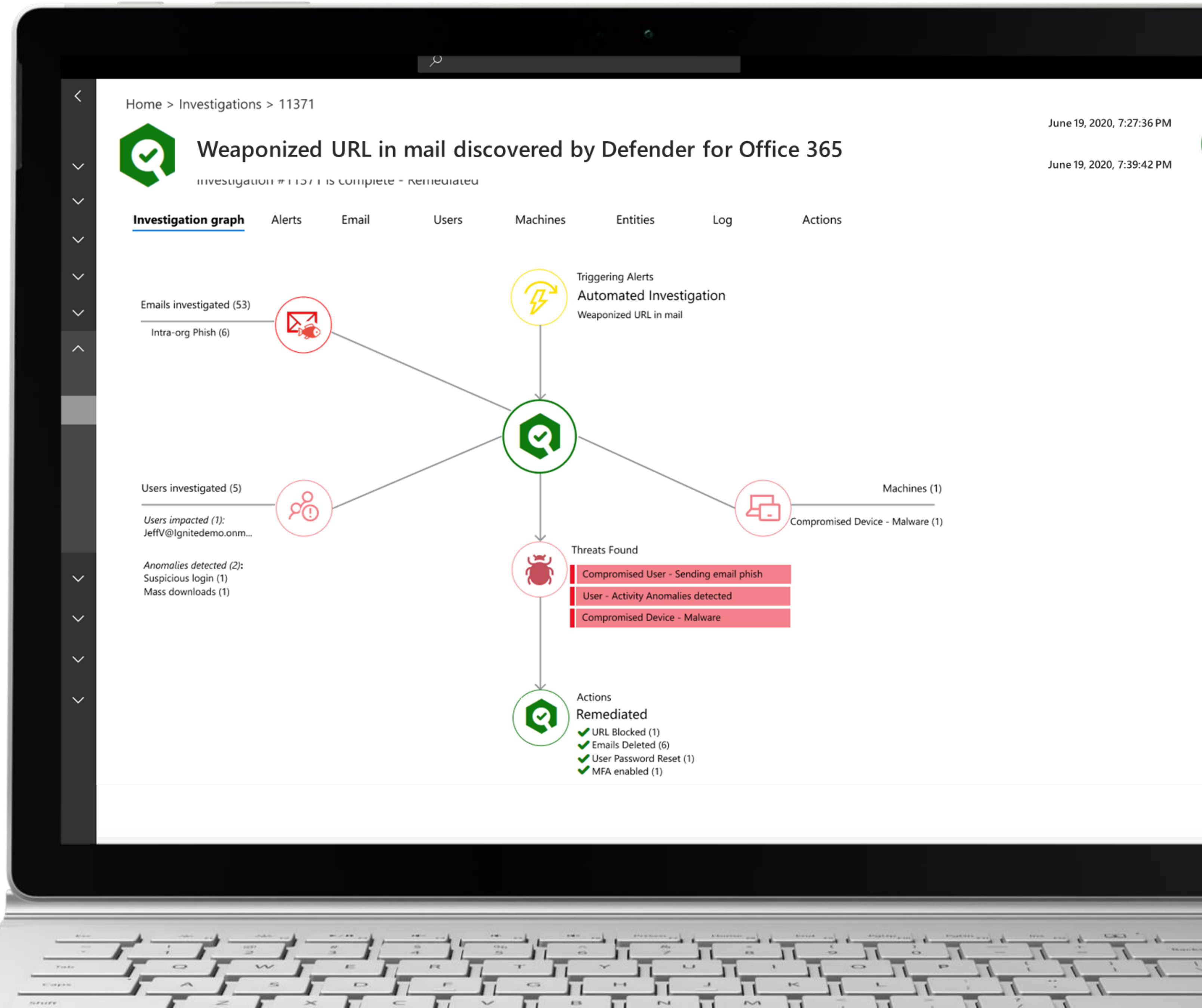
Applied filters: Time range: 8/30/2020-9/10/2020

ID	Status	Detection Source	Investigation		Users
98824f	Pending Action	Office365	Email investigation for '回复: paid invoice'		johndoe@o onmicrosoft.co
d56b18	Remediated		Email was moved by hunting bulk action		sjain@o3 .onmicrosoft.com
10a2bd	Remediated		Email was moved by hunting bulk action		secreader@o3 .onmicrosoft
97e196	Remediated		Email URL was blocked by hunting bulk action		secreader@o3 .onmicrosoft
9f0442	Remediated		Email was moved by hunting bulk action		secreader@o36 onmicrosoft
f8589a	Remediated		Email was moved by hunting bulk action		secreader@o36 onmicrosoft
4a385d	Remediated		Email URL was blocked by hunting bulk action		tifc@o36 nmicrosoft.com
14a6f9	Remediated		Email was moved by hunting bulk action		tifc@o36 onmicrosoft.com
cb7228	Pending Action	Office365	User suspected of being compromised - testinguser28@	onmi...	testinguser28@o 2.onmicro
ee0ca5	Pending Action	Office365	User suspected of being compromised - secreader	onmicrosof...	secreader@o36 onmicrosoft
e7f455	Pending Action	Office365	User suspected of being compromised - johndoe	onmicrosoft....	johndoe@o 2.onmicrosoft.c
e9c5ca	Remediated		Email was moved by hunting bulk action		tifc@o36 onmicrosoft.com
c7249b	Failed		Email sender was blocked by hunting bulk action		sjain@o3 .onmicrosoft.com

50 item(s) out of 13491 loaded. More items available, scroll down to see more.

Response & Remediation

- → Guided hunting with inline actions
- → Automated response playbooks



Home > Investigations > 11371

Weaponized URL in mail discovered by Defender for Office 365

Investigation #11371 is complete - Remediated

June 19, 2020, 7:27:36 PM

June 19, 2020, 7:39:42 PM

Triggering Alerts
Automated Investigation
Weaponized URL in mail

Emails investigated (53)
Intra-org Phish (6)

Users investigated (5)
Users impacted (1):
JeffV@Ignitedemo.onm...
Anomalies detected (2):
Suspicious login (1)
Mass downloads (1)

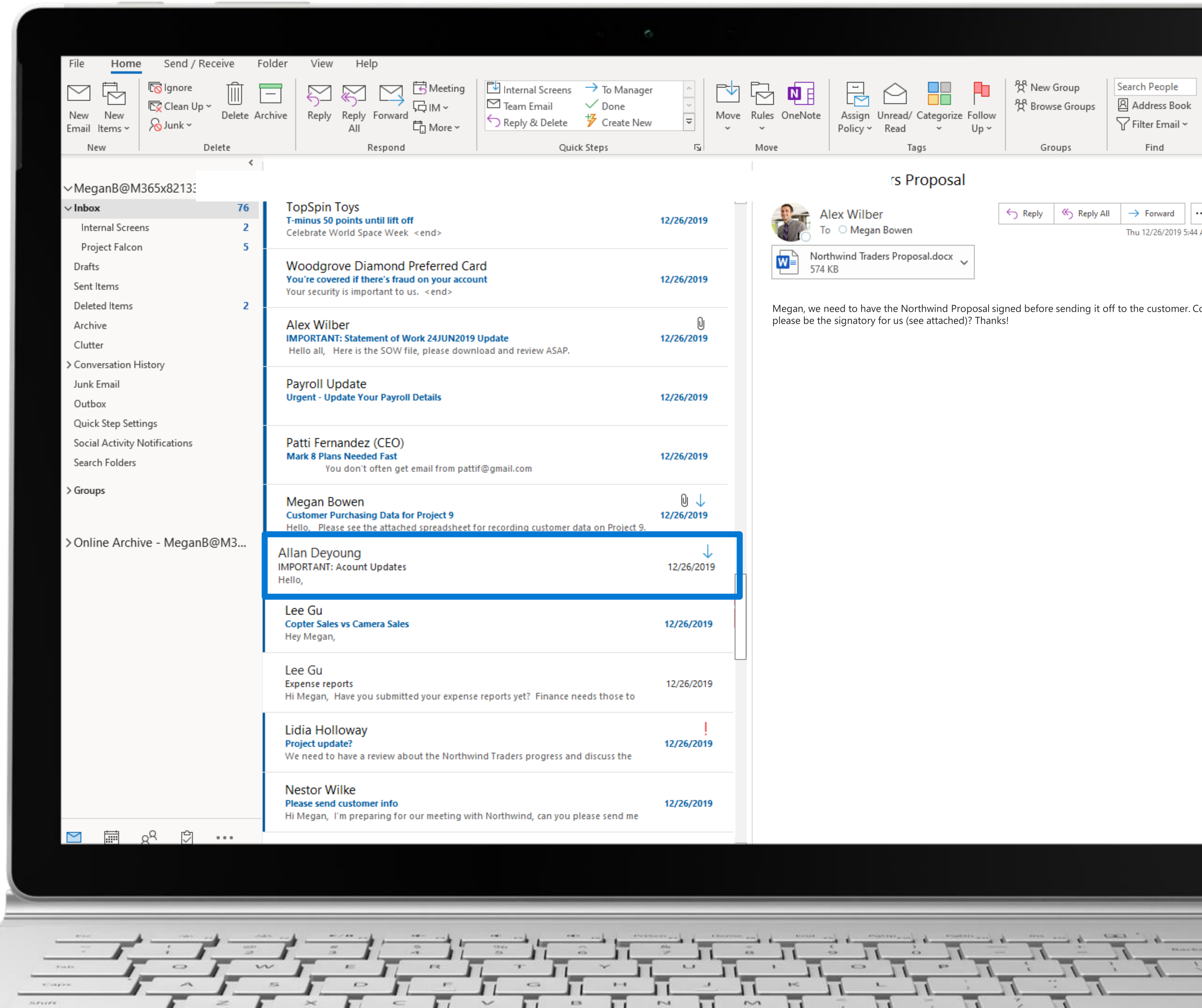
Machines (1)
Compromised Device - Malware (1)

Threats Found
Compromised User - Sending email phish
User - Activity Anomalies detected
Compromised Device - Malware

Actions
Remediated
✓ URL Blocked (1)
✓ Emails Deleted (6)
✓ User Password Reset (1)
✓ MFA enabled (1)

Response & Remediation

- → Guided hunting with inline actions
- → Automated response playbooks
- → Zero-Hour Auto-Purge (ZAP)



TopSpin Toys
T-minus 50 points until lift off 12/26/2019
Celebrate World Space Week <end>

Woodgrove Diamond Preferred Card
You're covered if there's fraud on your account 12/26/2019
Your security is important to us. <end>

Alex Wilber
IMPORTANT: Statement of Work 24JUN2019 Update 12/26/2019
Hello all, Here is the SOW file, please download and review ASAP.

Payroll Update
Urgent - Update Your Payroll Details 12/26/2019

Patti Fernandez (CEO)
Mark 8 Plans Needed Fast 12/26/2019
You don't often get email from pattif@gmail.com

Megan Bowen
Customer Purchasing Data for Project 9 12/26/2019
Hello, Please see the attached spreadsheet for recording customer data on Project 9.

Allan Deyoung
IMPORTANT: Acount Updates 12/26/2019
Hello,

Lee Gu
Copter Sales vs Camera Sales 12/26/2019
Hey Megan,

Lee Gu
Expense reports 12/26/2019
Hi Megan, Have you submitted your expense reports yet? Finance needs those to

Lidia Holloway
Project update? 12/26/2019
We need to have a review about the Northwind Traders progress and discuss the

Nestor Wilke
Please send customer info 12/26/2019
Hi Megan, I'm preparing for our meeting with Northwind, can you please send me

rs Proposal

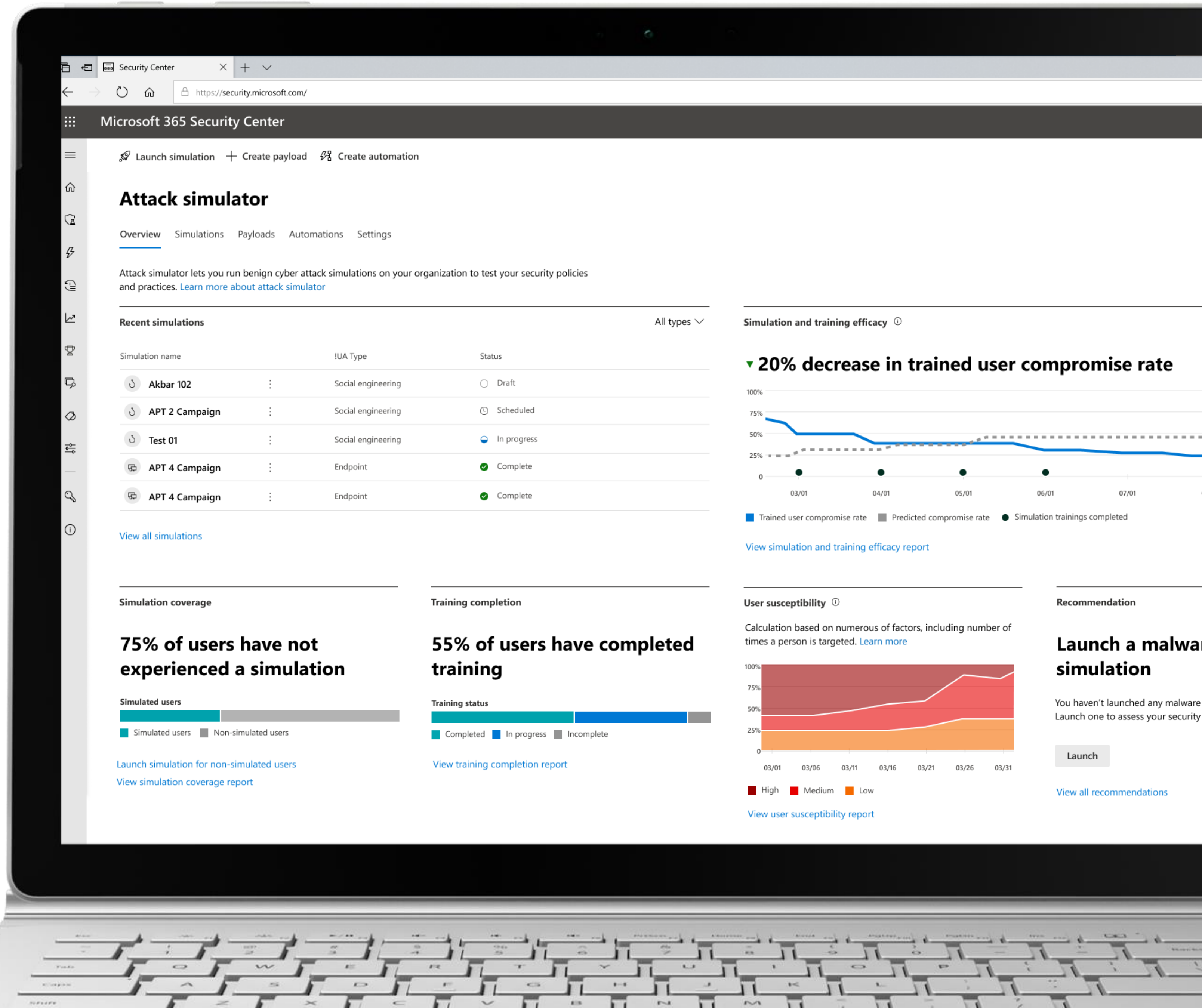
Alex Wilber
To Megan Bowen
Thu 12/26/2019 5:44

Northwind Traders Proposal.docx
574 KB

Megan, we need to have the Northwind Proposal signed before sending it off to the customer. C
please be the signatory for us (see attached)? Thanks!

Awareness & Training

→ Enhanced simulation management



Security Center

https://security.microsoft.com/

Microsoft 365 Security Center

Launch simulation + Create payload Create automation

Attack simulator

Overview Simulations Payloads Automations Settings

Attack simulator lets you run benign cyber attack simulations on your organization to test your security policies and practices. Learn more about attack simulator

Recent simulations All types

Simulation name	!UA Type	Status
Akbar 102	Social engineering	○ Draft
APT 2 Campaign	Social engineering	Scheduled
Test 01	Social engineering	In progress
APT 4 Campaign	Endpoint	✓ Complete
APT 4 Campaign	Endpoint	✓ Complete

View all simulations

Simulation and training efficacy

▼ 20% decrease in trained user compromise rate

100%
75%
50%
25%
0
03/01
04/01
05/01
06/01
07/01
Trained user compromise rate
Predicted compromise rate
Simulation trainings completed

View simulation and training efficacy report

Simulation coverage

75% of users have not experienced a simulation

Launch simulation for non-simulated users

View simulation coverage report

Training completion

55% of users have completed training

View training completion report

User susceptibility

Calculation based on numerous of factors, including number of times a person is targeted. Learn more

View user susceptibility report

Recommendation

Launch a malwa simulation

You haven't launched any malware

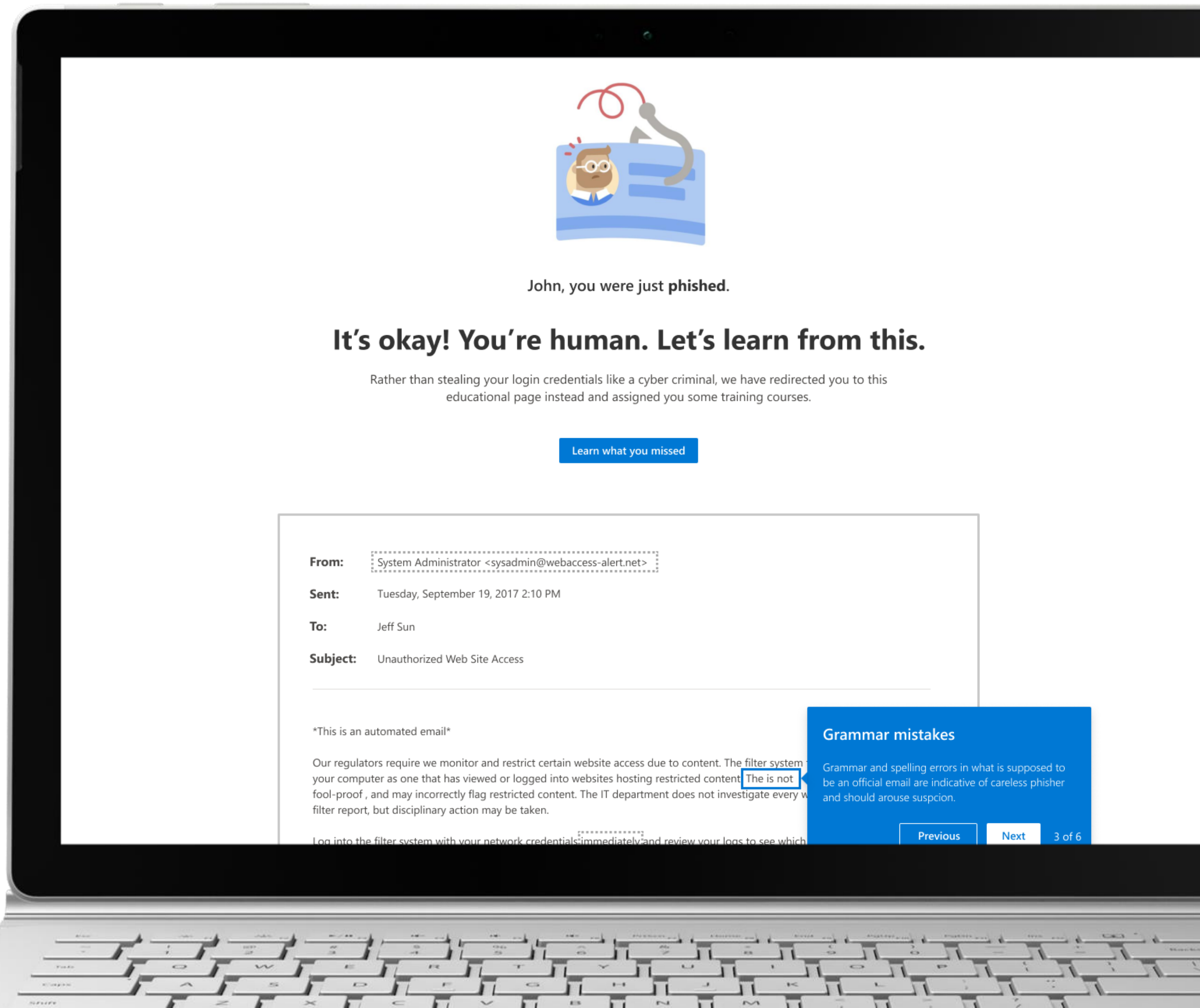
Launch one to assess your security

Launch

View all recommendations

Awareness & Training

- → Enhanced simulation management
- → Dynamic end user training



John, you were just **phished**.

It's okay! You're human. Let's learn from this.

Rather than stealing your login credentials like a cyber criminal, we have redirected you to this educational page instead and assigned you some training courses.

From: System Administrator <sysadmin@webaccess-alert.net>

Sent: Tuesday, September 19, 2017 2:10 PM

To: Jeff Sun

Subject: Unauthorized Web Site Access

This is an automated email

Our regulators require we monitor and restrict certain website access due to content. The filter system
your computer as one that has viewed or logged into websites hosting restricted content The is not
fool-proof , and may incorrectly flag restricted content. The IT department does not investigate every
filter report, but disciplinary action may be taken.

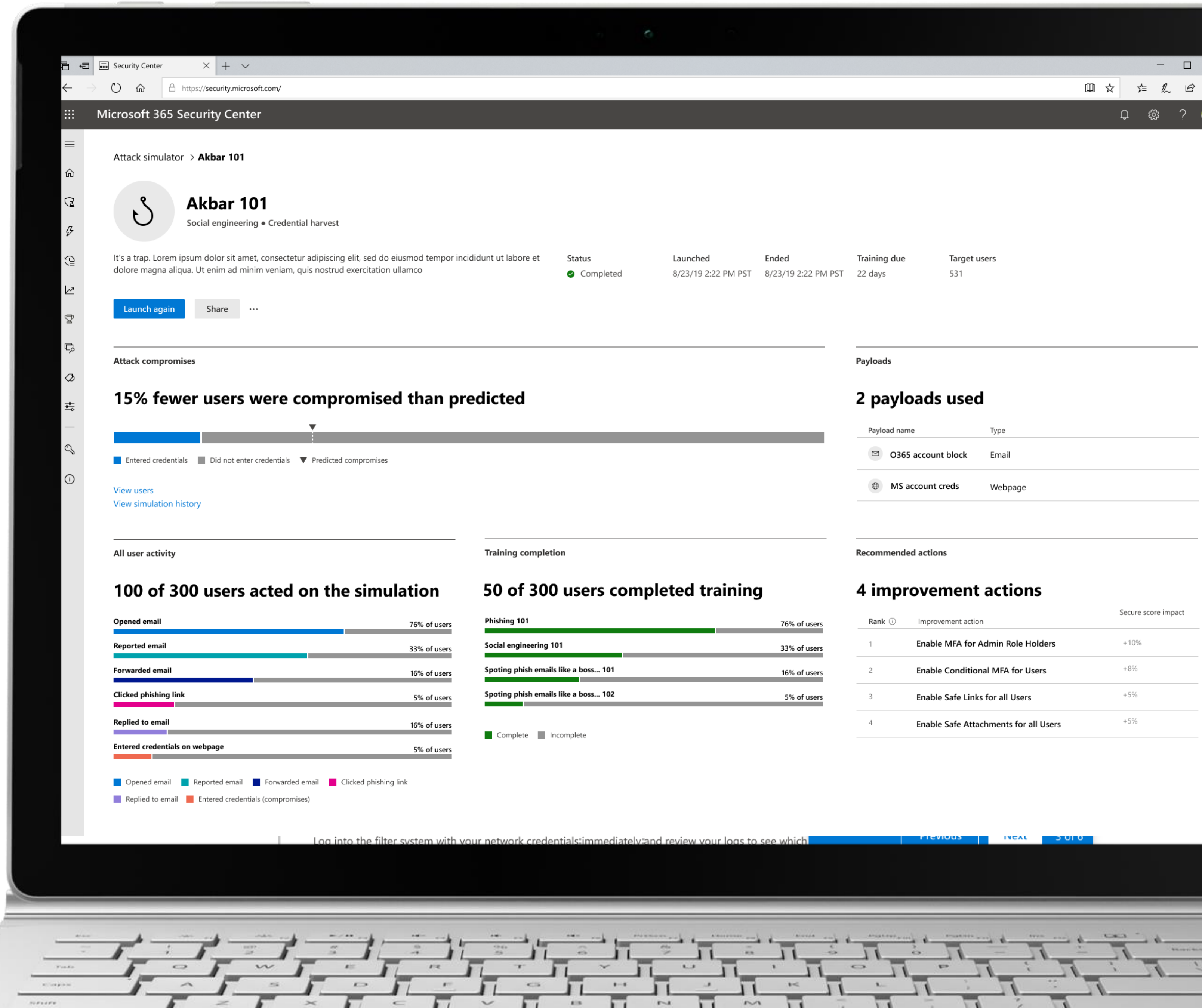
Log into the filter system with your network credentials immediately and review your logs to see which

Grammar mistakes

Grammar and spelling errors in what is supposed to be an official email are indicative of careless phisher and should arouse suspcion.

Awareness & Training

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



Security Center
https://security.microsoft.com/
Microsoft 365 Security Center

Attack simulator > **Akbar 101**

Akbar 101

Social engineering • Credential harvest

It's a trap. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco

Status	Launched	Ended	Training due	Target users
Completed	8/23/19 2:22 PM PST	8/23/19 2:22 PM PST	22 days	531

Attack compromises

15% fewer users were compromised than predicted

View users
View simulation history

Payloads

2 payloads used

Payload name	Type
O365 account block	Email
MS account creds	Webpage

All user activity

100 of 300 users acted on the simulation

Opened email	76% of users
Reported email	33% of users
Forwarded email	16% of users
Clicked phishing link	5% of users
Replied to email	16% of users
Entered credentials on webpage	5% of users

Training completion

50 of 300 users completed training

Phishing 101	76% of users
Social engineering 101	33% of users
Spoting phish emails like a boss... 101	16% of users
Spoting phish emails like a boss... 102	5% of users

Recommended actions

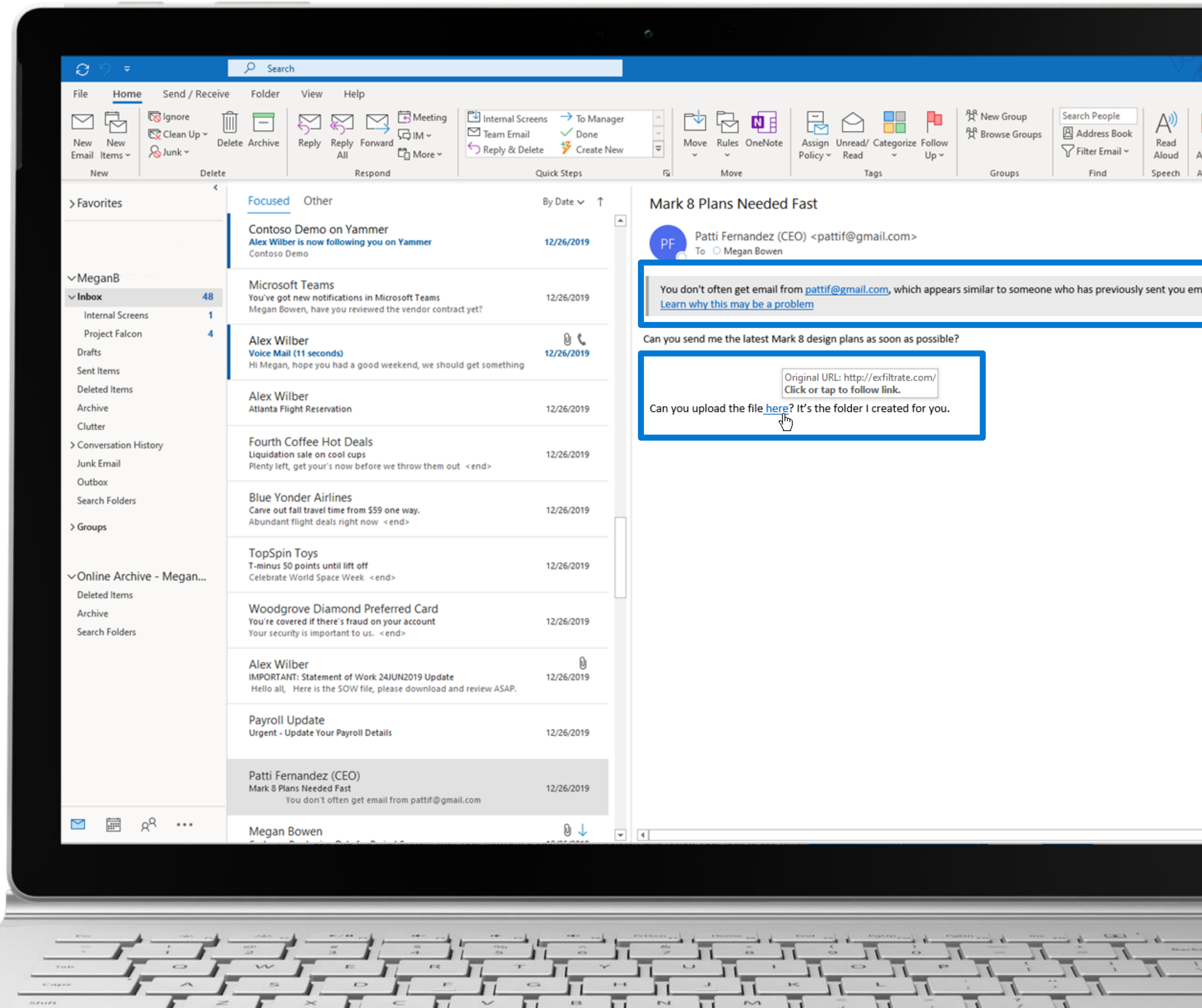
4 improvement actions

Rank	Improvement action	Secure score impact
1	Enable MFA for Admin Role Holders	+10%
2	Enable Conditional MFA for Users	+8%
3	Enable Safe Links for all Users	+5%
4	Enable Safe Attachments for all Users	+5%

Log into the filter system with your network credentials immediately and review your logs to see which

Awareness & Training

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



Contoso Demo on Yammer
Alex Wilber is now following you on Yammer
Contoso Demo
12/26/2019

Microsoft Teams
You've got new notifications in Microsoft Teams
Megan Bowen, have you reviewed the vendor contract yet?
12/26/2019

Alex Wilber
Voice Mail (11 seconds)
Hi Megan, hope you had a good weekend, we should get something
12/26/2019

Alex Wilber
Atlanta Flight Reservation
12/26/2019

Fourth Coffee Hot Deals
Liquidation sale on cool cups
Plenty left, get your's now before we throw them out <end>
12/26/2019

Blue Yonder Airlines
Carve out fall travel time from $59 one way.
Abundant flight deals right now <end>
12/26/2019

TopSpin Toys
T-minus 50 points until lift off
Celebrate World Space Week <end>
12/26/2019

Woodgrove Diamond Preferred Card
You're covered if there's fraud on your account
Your security is important to us. <end>
12/26/2019

Alex Wilber
IMPORTANT: Statement of Work 24JUN2019 Update
Hello all, Here is the SOW file, please download and review ASAP.
12/26/2019

Payroll Update
Urgent - Update Your Payroll Details
12/26/2019

Patti Fernandez (CEO)
Mark 8 Plans Needed Fast
You don't often get email from pattif@gmail.com
12/26/2019

Megan Bowen

Mark 8 Plans Needed Fast

PF Patti Fernandez (CEO) <pattif@gmail.com>
To ○ Megan Bowen

You don't often get email from pattif@gmail.com, which appears similar to someone who has previously sent you em
Learn why this may be a problem

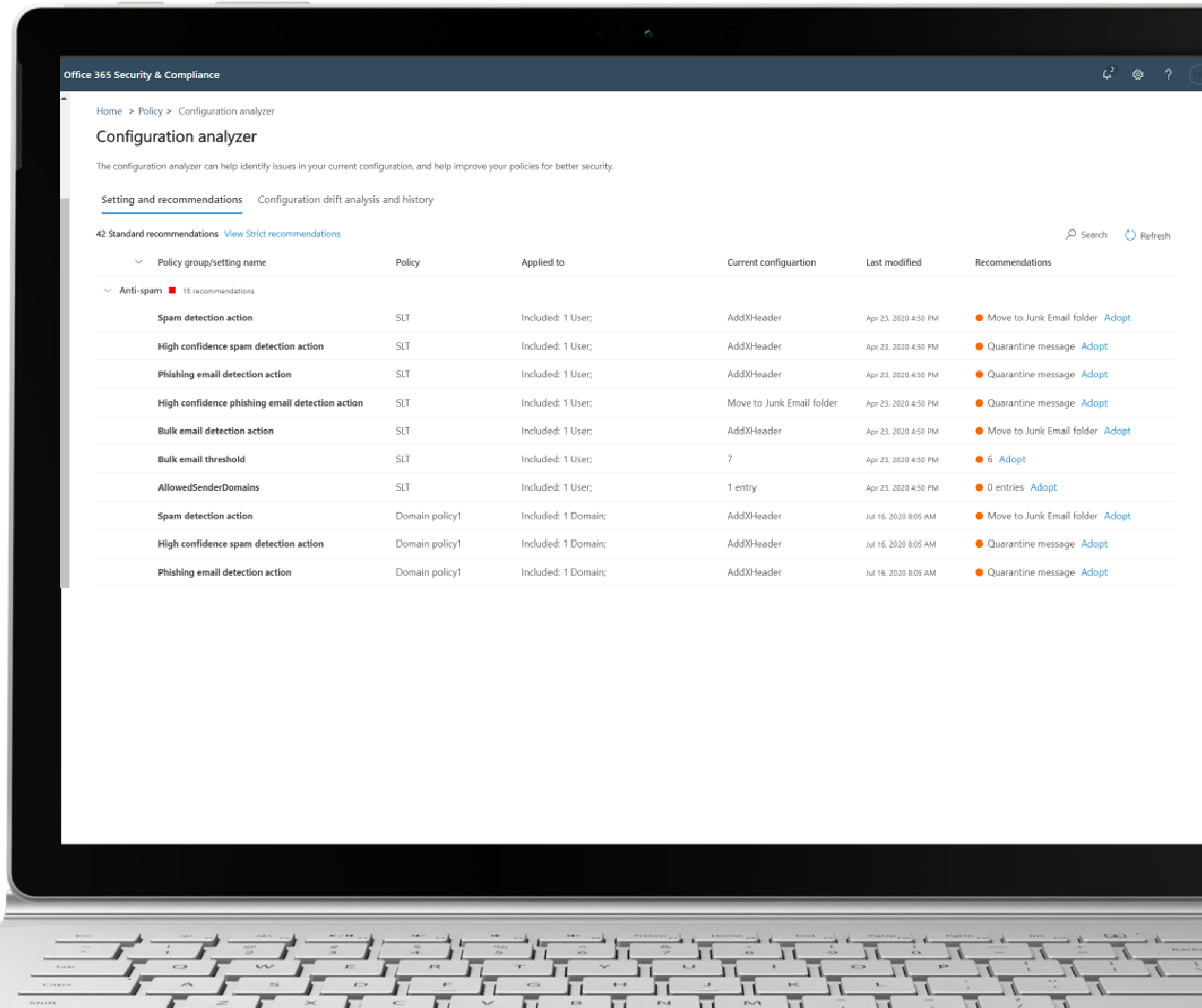
Can you send me the latest Mark 8 design plans as soon as possible?

Original URL: http://exfiltrate.com/
Click or tap to follow link.

Can you upload the file here? It's the folder I created for you.

Secure Posture

→ Understand policy gaps



Office 365 Security & Compliance

Home > Policy > Configuration analyzer

Configuration analyzer

The configuration analyzer can help identify issues in your current configuration, and help improve your policies for better security.

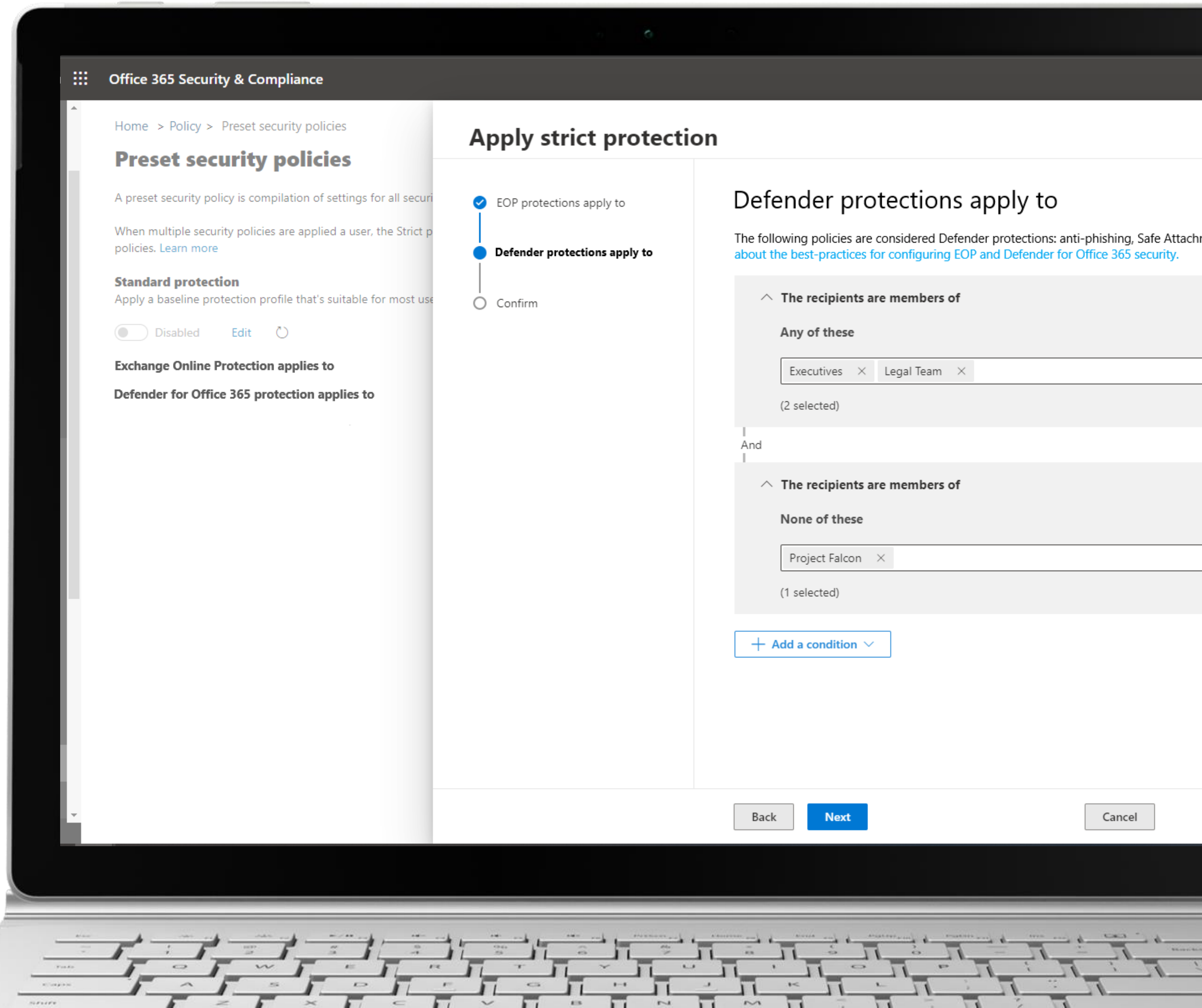
Setting and recommendations
Configuration drift analysis and history

42 Standard recommendations View Strict recommendations

Policy group/setting name	Policy	Applied to	Current configuartion	Last modified	Recommendations
Anti-spam 🟥 18 recommendations					
Spam detection action	SLT	Included: 1 User;	AddXHeader	Apr 23, 2020 4:50 PM	● Move to Junk Email folder Adopt
High confidence spam detection action	SLT	Included: 1 User;	AddXHeader	Apr 23, 2020 4:50 PM	● Quarantine message Adopt
Phishing email detection action	SLT	Included: 1 User;	AddXHeader	Apr 23, 2020 4:50 PM	● Quarantine message Adopt
High confidence phishing email detection action	SLT	Included: 1 User;	Move to Junk Email folder	Apr 23, 2020 4:50 PM	● Quarantine message Adopt
Bulk email detection action	SLT	Included: 1 User;	AddXHeader	Apr 23, 2020 4:50 PM	● Move to Junk Email folder Adopt
Bulk email threshold	SLT	Included: 1 User;	7	Apr 23, 2020 4:50 PM	● 6 Adopt
AllowedSenderDomains	SLT	Included: 1 User;	1 entry	Apr 23, 2020 4:50 PM	● 0 entries Adopt
Spam detection action	Domain policy1	Included: 1 Domain;	AddXHeader	Jul 16, 2020 8:05 AM	● Move to Junk Email folder Adopt
High confidence spam detection action	Domain policy1	Included: 1 Domain;	AddXHeader	Jul 16, 2020 8:05 AM	● Quarantine message Adopt
Phishing email detection action	Domain policy1	Included: 1 Domain;	AddXHeader	Jul 16, 2020 8:05 AM	● Quarantine message Adopt

Secure Posture

- → Understand policy gaps
- → Simplified configuration



Office 365 Security & Compliance

Home > Policy > Preset security policies

Preset security policies

A preset security policy is compilation of settings for all securi

When multiple security policies are applied a user, the Strict p policies. Learn more

Standard protection

Apply a baseline protection profile that's suitable for most use

Disabled Edit

Exchange Online Protection applies to

Defender for Office 365 protection applies to

Apply strict protection

- ✓ EOP protections apply to
- ● **Defender protections apply to**
- ○ Confirm

Defender protections apply to

The following policies are considered Defender protections: anti-phishing, Safe Attachi about the best-practices for configuring EOP and Defender for Office 365 security.

The recipients are members of

Any of these

Executives ✕ Legal Team ✕

(2 selected)

And

The recipients are members of

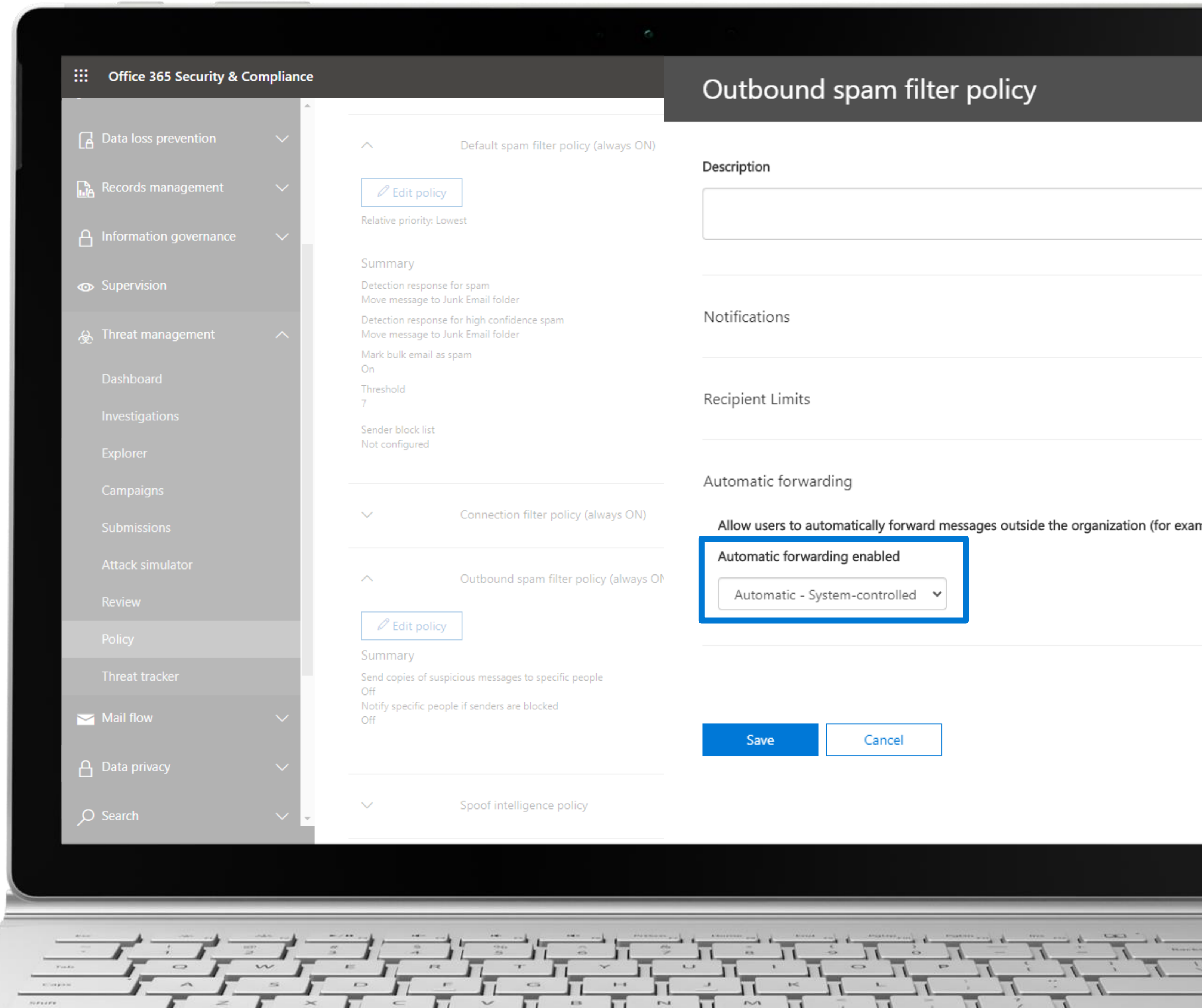
None of these

Project Falcon ✕

(1 selected)

Secure Posture

- → Understand policy gaps
- → Simplified configuration
- → Enhancing protection for our customers



Default spam filter policy (always ON)

Relative priority: Lowest

Summary

Detection response for spam
Move message to Junk Email folder

Detection response for high confidence spam
Move message to Junk Email folder

Mark bulk email as spam
On

Threshold
7

Sender block list
Not configured

Connection filter policy (always ON)

Outbound spam filter policy (always ON

Summary

Send copies of suspicious messages to specific people
Off
Notify specific people if senders are blocked
Off

Spoof intelligence policy

Outbound spam filter policy

Description

Notifications

Recipient Limits

Automatic forwarding

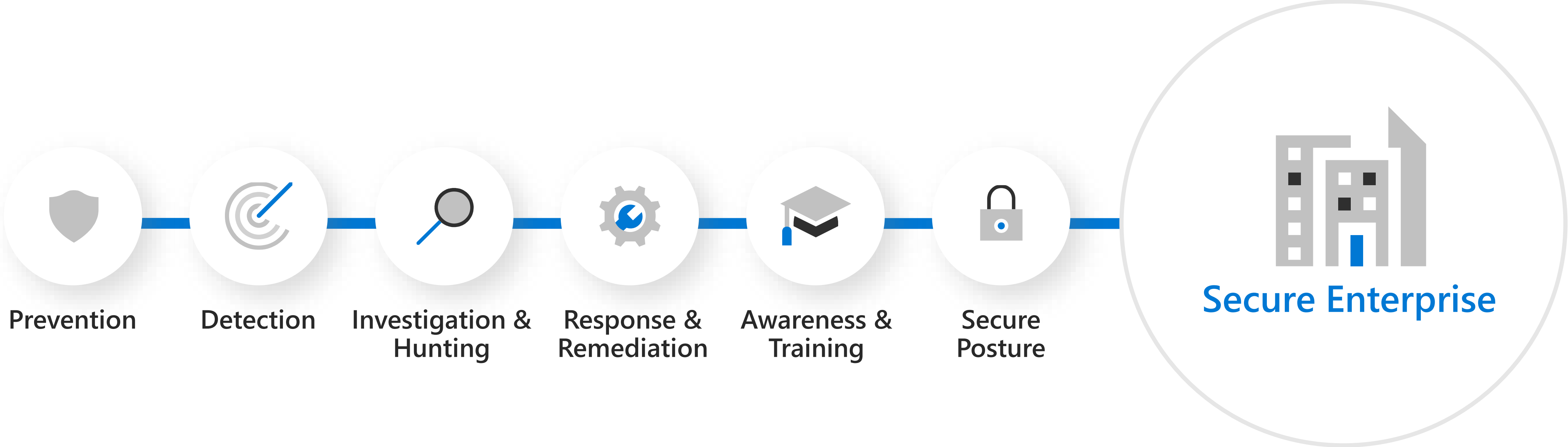
Allow users to automatically forward messages outside the organization (for exam

Automatic forwarding enabled

Automatic - System-controlled

Microsoft Defender for Office 365

Securing your enterprise requires more than just prevention



Prevention

Detection

Investigation & Hunting

Response & Remediation

Awareness & Training

Secure Posture

Secure Enterprise

Microsoft 365 Defender

Automated cross-domain XDR security

Identities

Microsoft Defender for Identity

Endpoints

Microsoft Defender for Endpoint

Cloud Apps

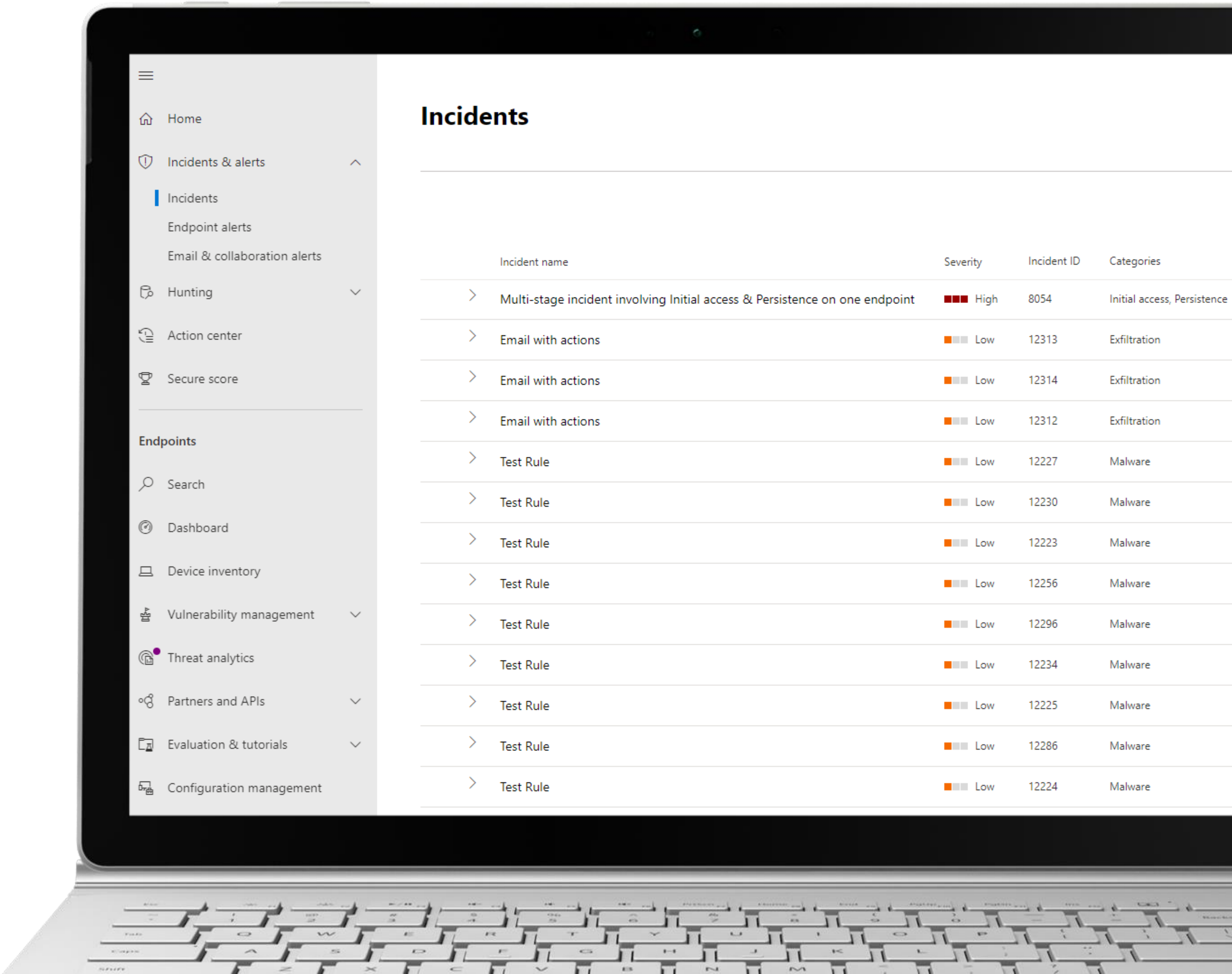
Microsoft Cloud App Security

User Data

Microsoft Defender for Office 365

Microsoft 365 Defender

→ Incidents consolidate alerts and investigations

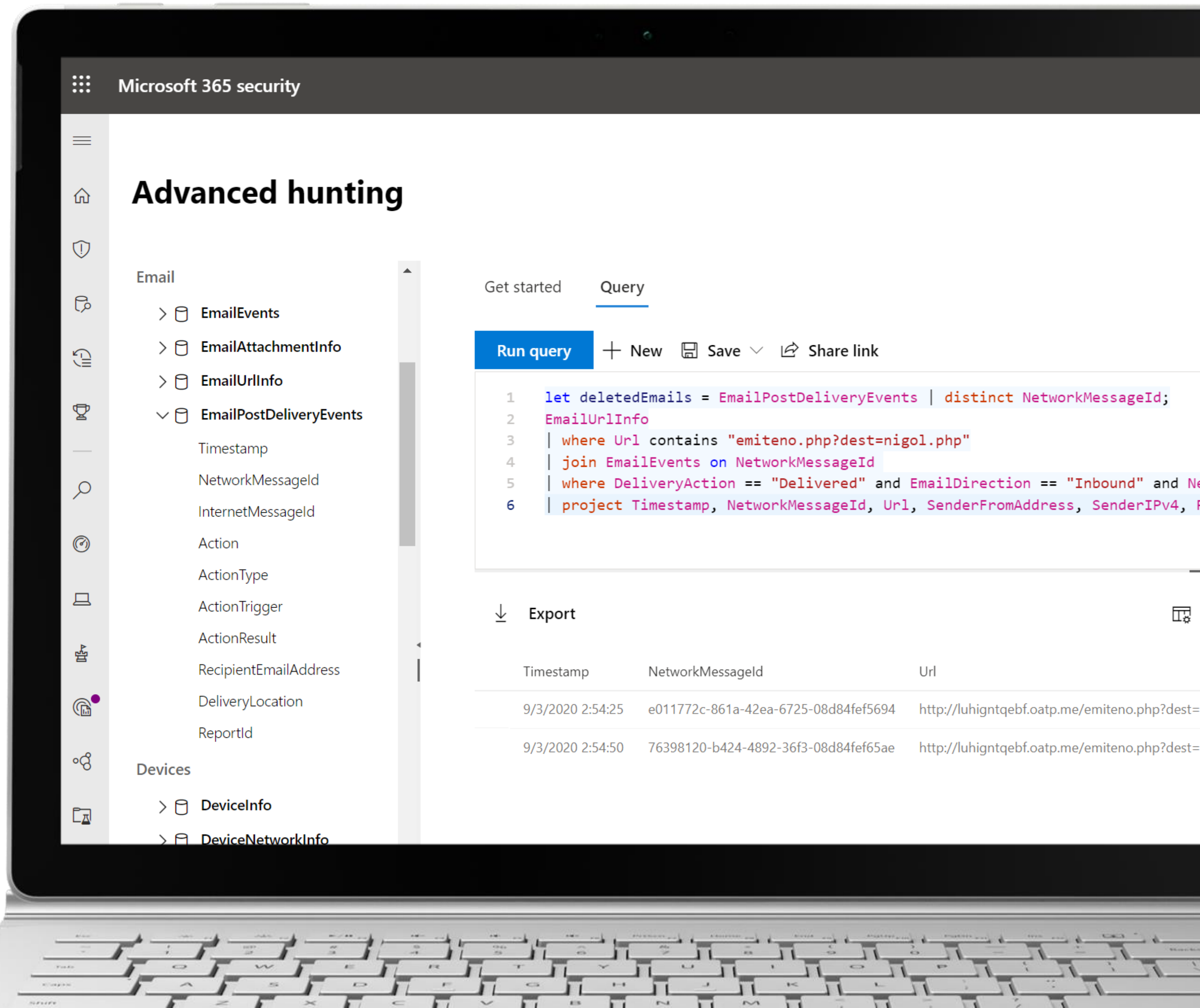


Incidents

Incident name	Severity	Incident ID	Categories
Multi-stage incident involving Initial access & Persistence on one endpoint	High	8054	Initial access, Persistence
Email with actions	Low	12313	Exfiltration
Email with actions	Low	12314	Exfiltration
Email with actions	Low	12312	Exfiltration
Test Rule	Low	12227	Malware
Test Rule	Low	12230	Malware
Test Rule	Low	12223	Malware
Test Rule	Low	12256	Malware
Test Rule	Low	12296	Malware
Test Rule	Low	12234	Malware
Test Rule	Low	12225	Malware
Test Rule	Low	12286	Malware
Test Rule	Low	12224	Malware

Microsoft 365 Defender

- → Incidents consolidate alerts and investigations
- → Advanced hunting for sophisticated queries



Advanced hunting

Email

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents
  - Timestamp
  - NetworkMessageId
  - InternetMessageId
  - Action
  - ActionType
  - ActionTrigger
  - ActionResult
  - RecipientEmailAddress
  - DeliveryLocation
  - ReportId

Devices

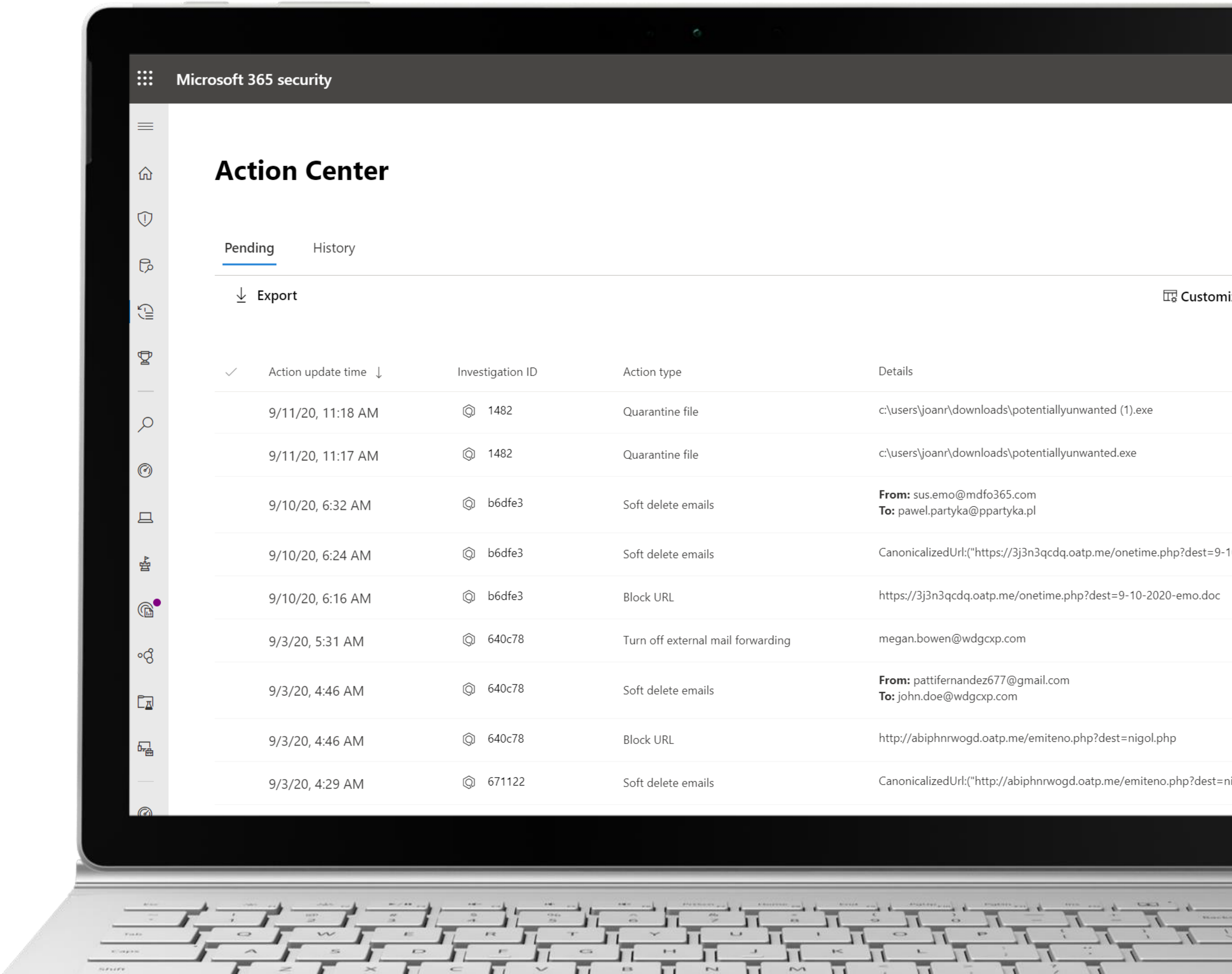
- DeviceInfo
- DeviceNetworkInfo

```
let deletedEmails = EmailPostDeliveryEvents | distinct NetworkMessageId;
EmailUrlInfo
| where Url contains "emiteno.php?dest=nigol.php"
| join EmailEvents on NetworkMessageId
| where DeliveryAction == "Delivered" and EmailDirection == "Inbound" and Ne
| project Timestamp, NetworkMessageId, Url, SenderFromAddress, SenderIPv4, F
```

Timestamp	NetworkMessageId	Url
9/3/2020 2:54:25	e011772c-861a-42ea-6725-08d84fef5694	http://luhigntqebf.oatp.me/emiteno.php?dest=
9/3/2020 2:54:50	76398120-b424-4892-36f3-08d84fef65ae	http://luhigntqebf.oatp.me/emiteno.php?dest=

Microsoft 365 Defender

- → Incidents consolidate alerts and investigations
- → Advanced hunting for sophisticated queries
- → Centralized action queue



Action Center

✓	Action update time ↓	Investigation ID	Action type	Details
	9/11/20, 11:18 AM	1482	Quarantine file	c:\users\joanr\downloads\potentiallyunwanted (1).exe
	9/11/20, 11:17 AM	1482	Quarantine file	c:\users\joanr\downloads\potentiallyunwanted.exe
	9/10/20, 6:32 AM	b6dfe3	Soft delete emails	**From:** sus.emo@mdfo365.com **To:** pawel.partyka@ppartyka.pl
	9/10/20, 6:24 AM	b6dfe3	Soft delete emails	CanonicalizedUrl:("https://3j3n3qcdq.oatp.me/onetime.php?dest=9-1
	9/10/20, 6:16 AM	b6dfe3	Block URL	https://3j3n3qcdq.oatp.me/onetime.php?dest=9-10-2020-emo.doc
	9/3/20, 5:31 AM	640c78	Turn off external mail forwarding	megan.bowen@wdgcxp.com
	9/3/20, 4:46 AM	640c78	Soft delete emails	**From:** pattifernandez677@gmail.com **To:** john.doe@wdgcxp.com
	9/3/20, 4:46 AM	640c78	Block URL	http://abiphnrwogd.oatp.me/emiteno.php?dest=nigol.php
	9/3/20, 4:29 AM	671122	Soft delete emails	CanonicalizedUrl:("http://abiphnrwogd.oatp.me/emiteno.php?dest=ni

For more information:
https://aka.ms/DefenderO365

Microsoft Defender for Office 365

Integrated threat protection for all of Office 365

Microsoft Security