Microsoft Security

Do More with Less with Microsoft Security Solution

Mr. Paul Tsang CCSP CISSP CISA
Security Specialist
Microsoft Hong Kong

Three problems on Cybersecurity Landscape for HK

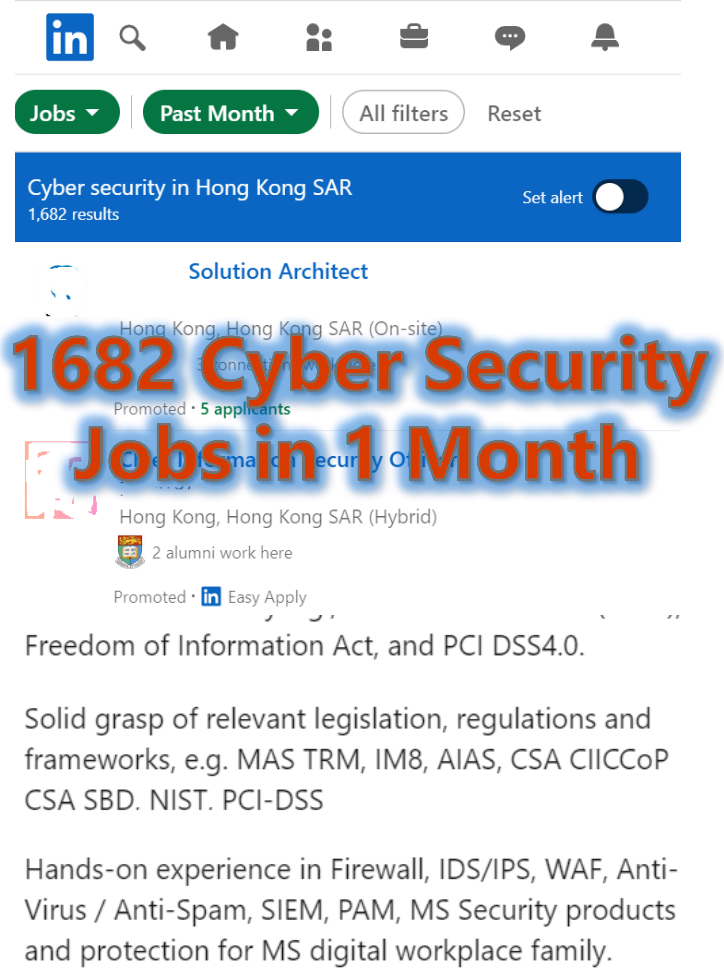
Conventional security tools have not kept pace

- Finger pointing on compatibility
- Unlimited Mesh API to maintain

Cost of security breaches is rising

- Complexity of breaches
- Cost of investigations
- Data Leakage penalty
- Reputations

Resources are constrained



Cyber security in Hong Kong SAR
1,682 results

Solution Architect
Hong Kong, Hong Kong SAR (On-site)
Promoted · 5 applicants

Hong Kong, Hong Kong SAR (Hybrid)
2 alumni work here
Promoted · Easy Apply

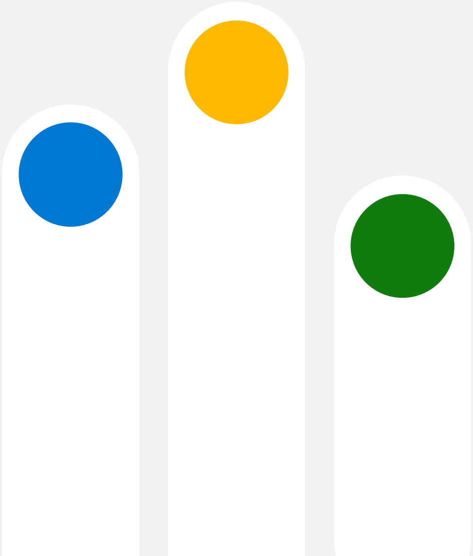
1682 Cyber Security Jobs in 1 Month

Freedom of Information Act, and PCI DSS4.0.

Solid grasp of relevant legislation, regulations and frameworks, e.g. MAS TRM, IM8, AIAS, CSA CIICCoP CSA SBD. NIST. PCI-DSS

Hands-on experience in Firewall, IDS/IPS, WAF, Anti-Virus / Anti-Spam, SIEM, PAM, MS Security products and protection for MS digital workplace family.

Microsoft Security helps you do more with less



Simplify Vendor Management

Reduce threats with AI and Automation

Improve Operational Efficiency

Microsoft

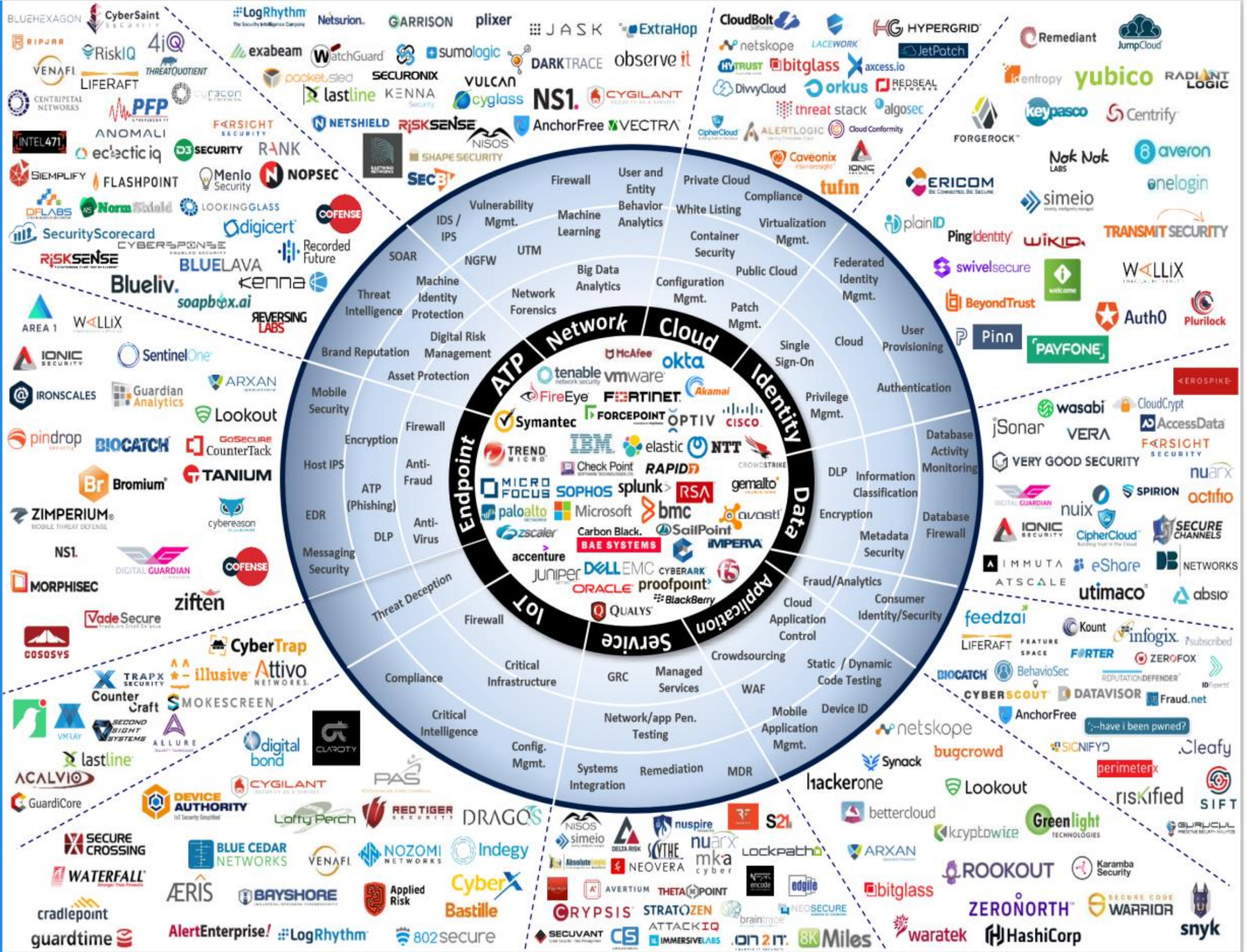
Simplify Vendor Management

How Many Security products are you managing today?

Gartner found in the 2020 CISO Effectiveness Survey that 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more.

Gartner the Top 8 Security and Risk Trends We're Watching
Contributor: Kasey Panetta

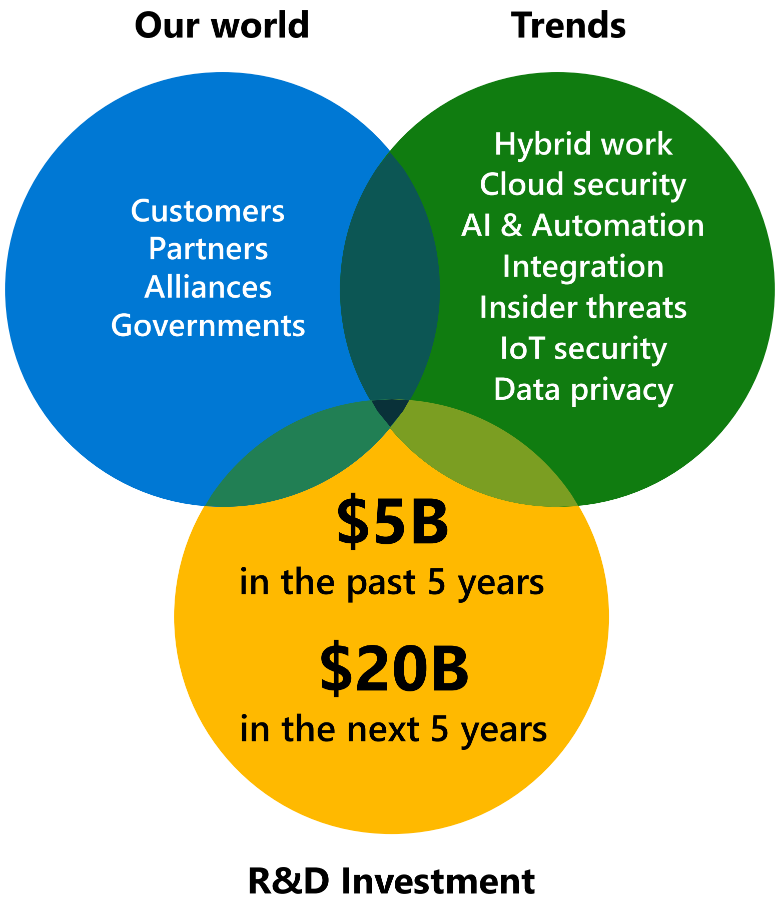
Information security landscape



Source: Boston Meridian Partners

We’re investing where security is going

To help you keep pace with change



Our world

Customers
Partners
Alliances
Governments

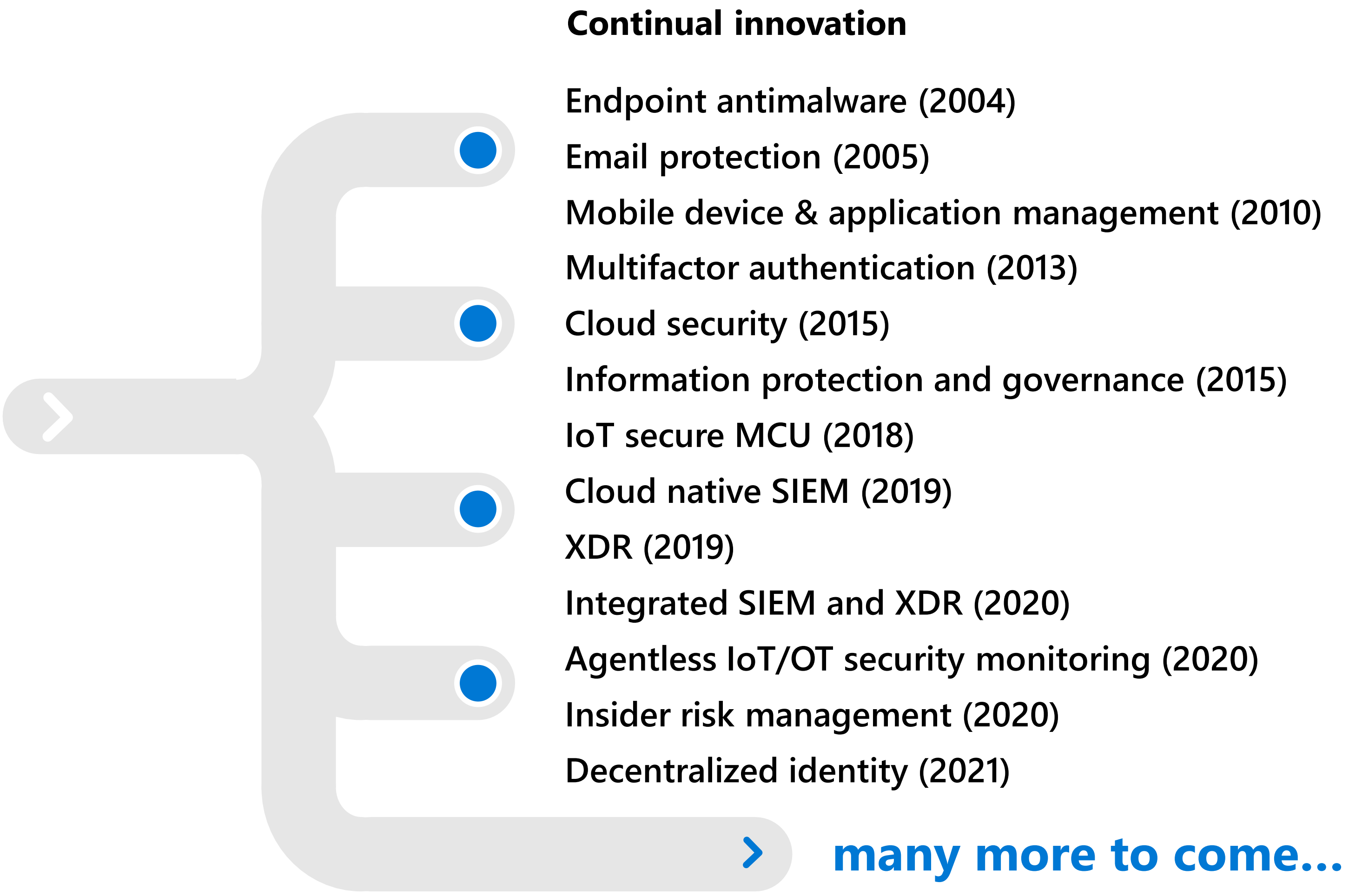
Trends

Hybrid work
Cloud security
AI & Automation
Integration
Insider threats
IoT security
Data privacy

$5B
in the past 5 years

$20B
in the next 5 years

R&D Investment



Continual innovation

Endpoint antimalware (2004)
Email protection (2005)
Mobile device & application management (2010)
Multifactor authentication (2013)
Cloud security (2015)
Information protection and governance (2015)
IoT secure MCU (2018)
Cloud native SIEM (2019)
XDR (2019)
Integrated SIEM and XDR (2020)
Agentless IoT/OT security monitoring (2020)
Insider risk management (2020)
Decentralized identity (2021)

many more to come…

Protection aligned to where you're going

Solutions to support your digital journey

Protect identity & access for strong **Zero Trust** foundations

Modernize security & **defend against threats**

Secure **multi-cloud** environments

Protect & govern sensitive data

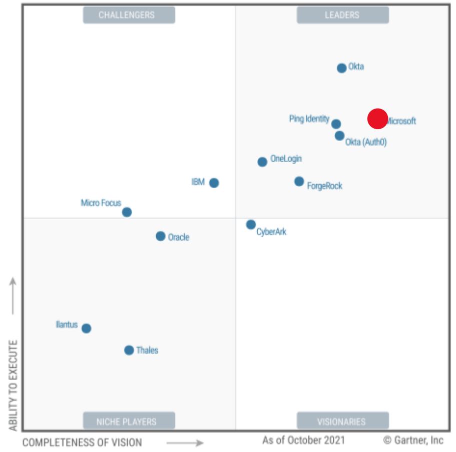
Mitigate compliance & privacy **risk**

Gartner®

Microsoft Security a Leader in 6 Gartner Magic Quadrant reports

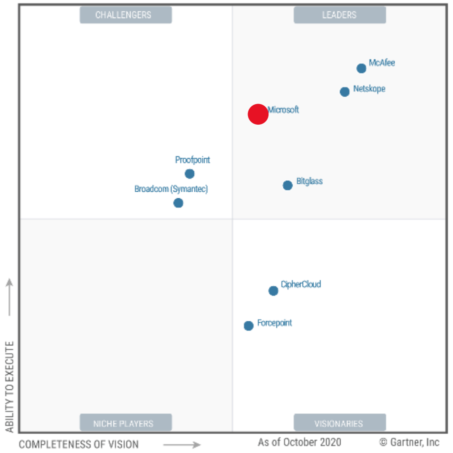
*Gartner “Magic Quadrant for Access Management,” by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021
*Gartner “Magic Quadrant for Cloud Access Security Brokers,” by Craig Lawson, Steve Riley, October 2020
*Gartner “Magic Quadrant for Enterprise Information Archiving,” by Michael Hoech, Jeff Vogel, October 2020
*Gartner “Magic Quadrant for Endpoint Protection Platforms,” by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021
*Gartner “Magic Quadrant for Unified Endpoint Management,” by Dan Wilson, Chris Silva, Tom Cipolla, August 2021
*Gartner “2022 Gartner® Magic QuadrantTM for Security Information and Event Management”

These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

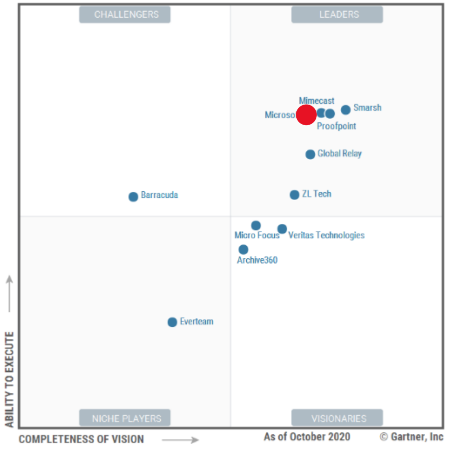


Source: Gartner (November 2021)

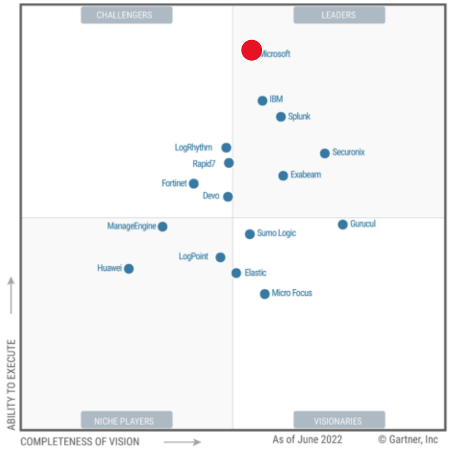
Access Management



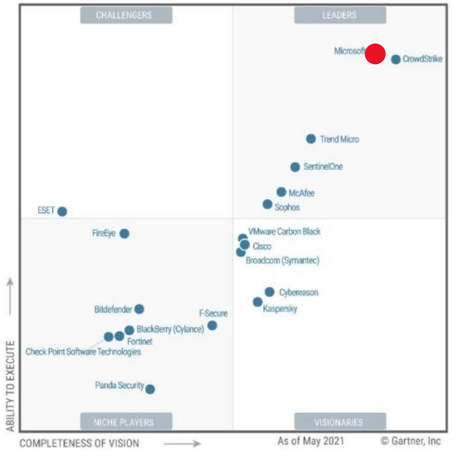
Cloud Access Security Brokers



Enterprise Information Archiving

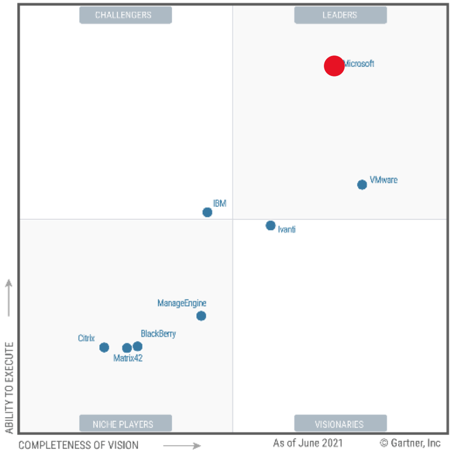


Security Information And Event Management



Source: Gartner (May 2021)

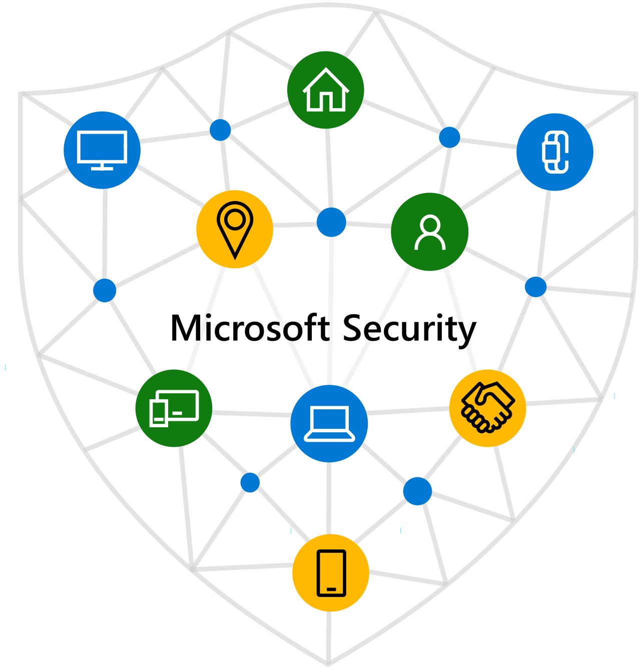
Endpoint Protection Platforms



Source: Gartner (August 2021)

Unified Endpoint Management

Simplify vendor management



Replace up to

50

product categories

Up to

60%

savings with Microsoft 365 E5 Security and Microsoft 365 E5 Compliance[1]

$0

built in Cloud Security Posture Management with Microsoft Defender for Cloud

30%

savings from unifying cloud security tools with Microsoft Defender for Cloud[2]

[1] Savings based on publicly available estimated pricing for other vendor solutions and Web Direct/Base Price shown for Microsoft offerings

[2] Forrester Consulting, "The Total Economic Impact ™ Of Microsoft Azure Security Center," June, 2021, commissioned by Microsoft

Microsoft

Reduce threats with AI and Automation

Microsoft Security

Insights from 43 trillion daily security signals

Microsoft security experts illuminate today’s threat landscape, providing insights on emerging trends as well as historically persistent threats.

Microsoft Digital Defense Report

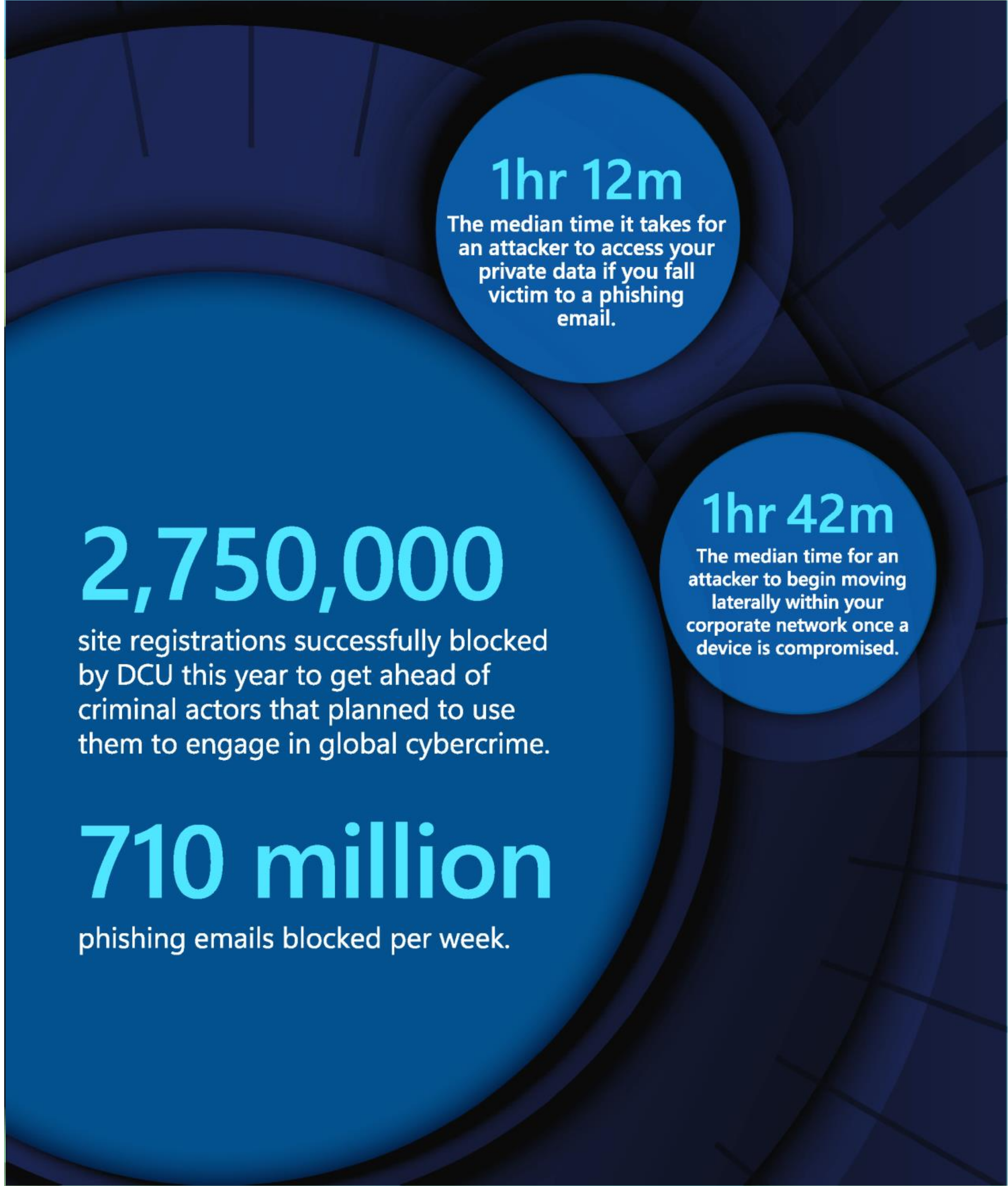
November 2022

The state of cybercrime

Attackers are compromising businesses to **host phishing campaigns, malware, or use their computing power to mine cryptocurrency**. This year saw a significant increase in indiscriminate phishing and credential theft to gain information.

Additionally, **homoglyph domains are being used to deceive viewers** into thinking the homoglyph domain is a genuine domain. Homoglyph domains impersonate legitimate domain names by utilizing characters that are identical or nearly identical in appearance to another character.

Internet of Things (IoT) devices are also becoming an increasingly popular target for cybercriminals using widespread botnets. When routers are unpatched and left exposed directly to the internet, threat actors can abuse them to gain access to networks, execute malicious attacks, and even support their operations.



1hr 12m

The median time it takes for an attacker to access your private data if you fall victim to a phishing email.

2,750,000

site registrations successfully blocked by DCU this year to get ahead of criminal actors that planned to use them to engage in global cybercrime.

1hr 42m

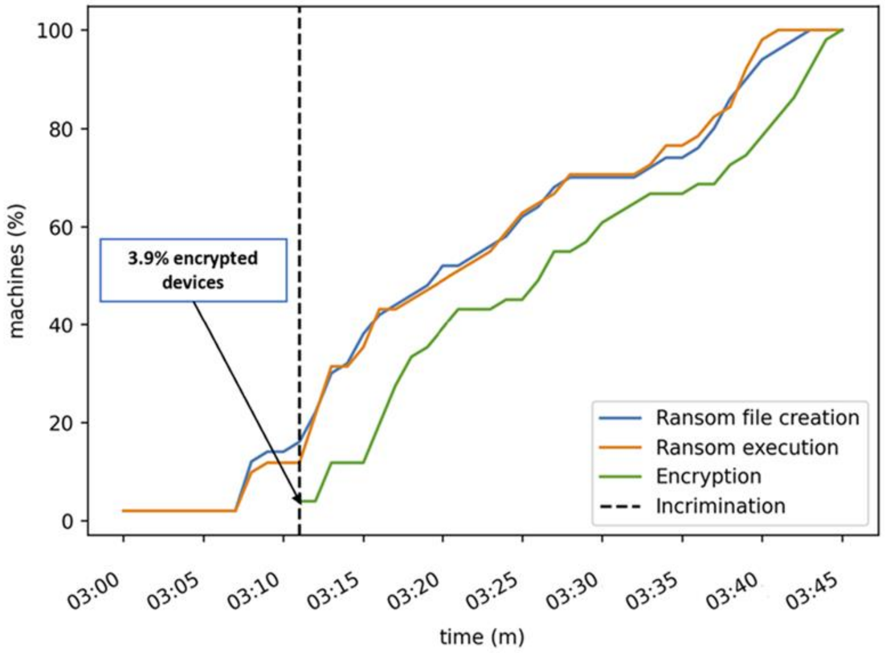
The median time for an attacker to begin moving laterally within your corporate network once a device is compromised.

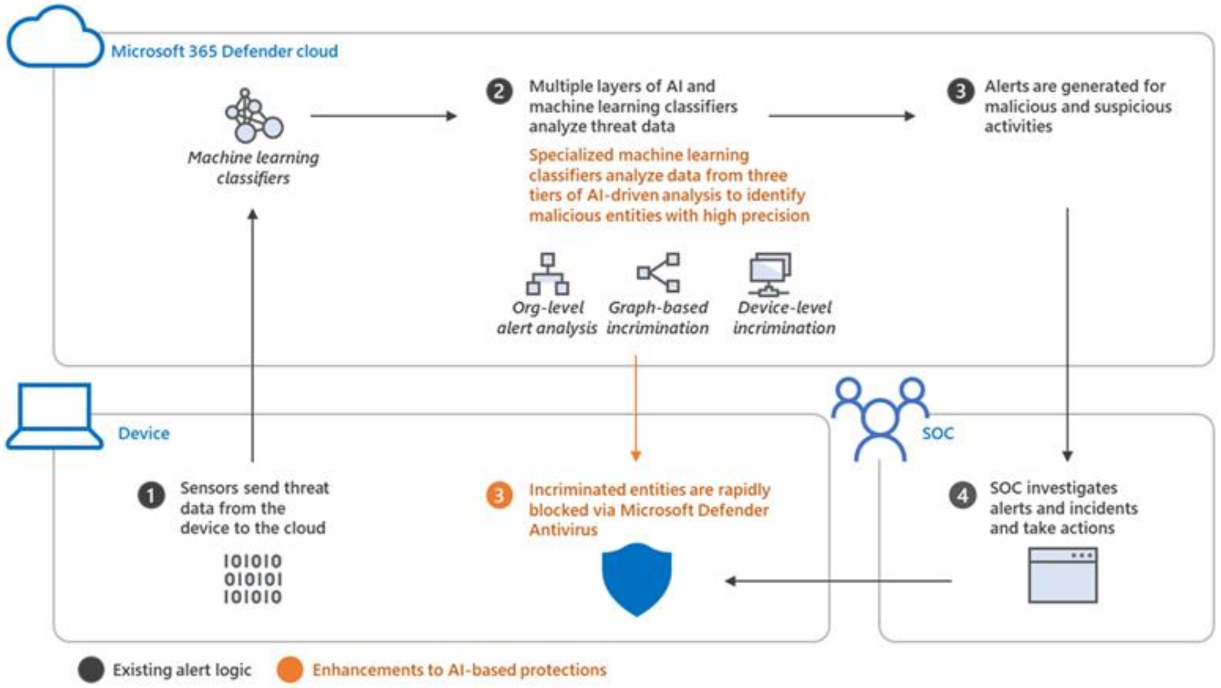
710 million

phishing emails blocked per week.

Improving AI-based defenses to disrupt human-operated ransomware

- A time-series and statistical analysis of alerts to look for anomalies at the organization level
- Graph-based aggregation of suspicious events across devices within the organization to identify malicious activity across a set of devices
- Device-level monitoring to identify suspicious activity with high confidence





Microsoft 365 Defender cloud
Machine learning classifiers
Org-level alert analysis
Graph-based incrimination
Device-level incrimination
Device
SOC
101010
010101
101010

1 Sensors send threat data from the device to the cloud

2 Multiple layers of AI and machine learning classifiers analyze threat data

Specialized machine learning classifiers analyze data from three tiers of AI-driven analysis to identify malicious entities with high precision

3 Alerts are generated for malicious and suspicious activities

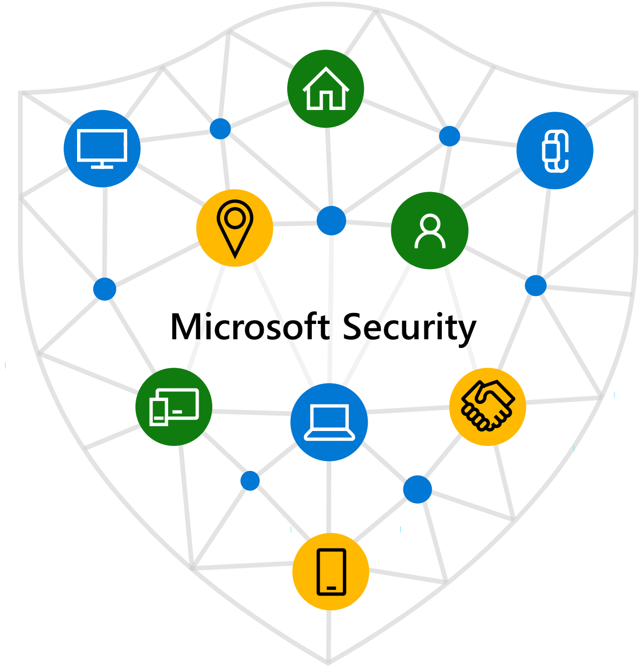
3 Incriminated entities are rapidly blocked via Microsoft Defender Antivirus

4 SOC investigates alerts and incidents and take actions

● Existing alert logic ● Enhancements to AI-based protections

[Improving AI-based defenses to disrupt human-operated ransomware - Microsoft Security Blog]

Reduce threats with AI and Automation



60%
reduced risk of material breach

65%
less time to investigate threats

88%
less time responding to threats with Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud[1]

$10.5
million additional end user productivity from automation and process improvements in Microsoft 365 Defender[2]

96%
less time spent monitoring potential suspicious activity with Microsoft Purview[3]

90%
reduction in noise, elevating the most critical issues with Microsoft Sentinel[4]

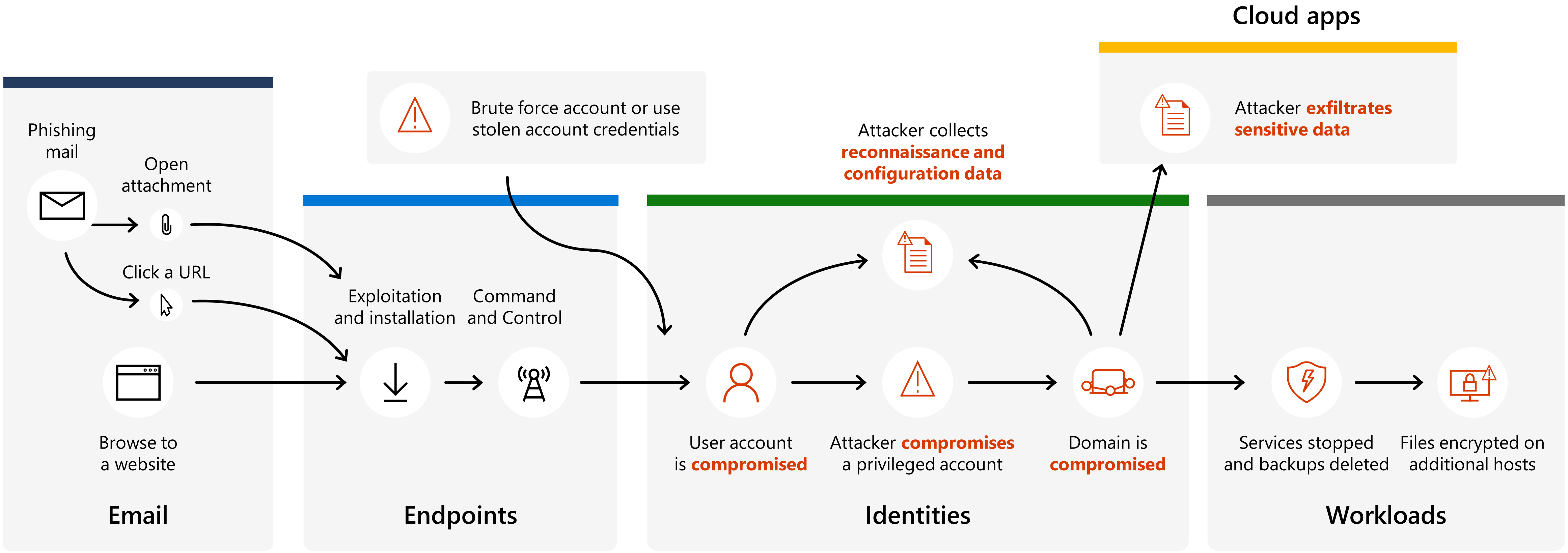
[1] Forrester Consulting, "The Total Economic Impact™ Of Microsoft SIEM and XDR", August 2022, commissioned by Microsoft
[2] Forrester Consulting, "The Total Economic Impact™ Of Microsoft 365 Defender", April 2022, commissioned by Microsoft
[3] Forrester Consulting, "The Total Economic Impact ™ Of Microsoft 365 E5 Compliance," February, 2021, commissioned by Microsoft
[4] Microsoft blog: Azure Sentinel uncovers the real threats hidden in billions of low fidelity signals, Feb 2020

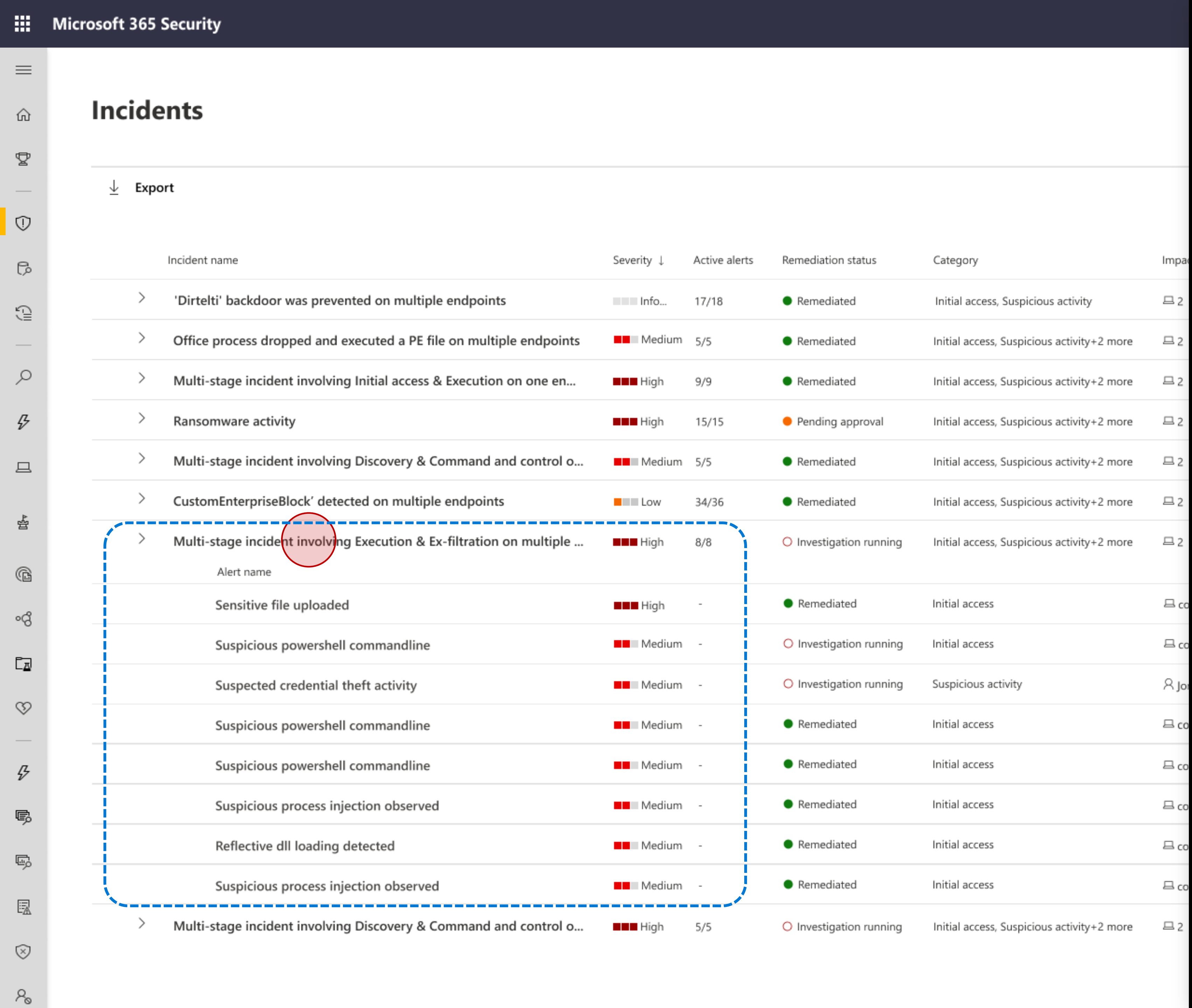
Microsoft

Improve Operational Efficiency

Attacks are crossing modalities

Typical human-operated ransomware campaign


Cloud apps
Attacker exfiltrates sensitive data
Brute force account or use stolen account credentials
Attacker collects reconnaissance and configuration data
Phishing mail
Open attachment
Click a URL
Browse to a website
Email
Exploitation and installation
Command and Control
Endpoints
User account is compromised
Attacker compromises a privileged account
Domain is compromised
Identities
Services stopped and backups deleted
Files encrypted on additional hosts
Workloads



Microsoft 365 Security

Incidents

Export

Incident name	Severity ↓	Active alerts	Remediation status	Category	Impa
'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	co
Suspicious powershell commandline	Medium	-	○ Investigation running	Initial access	co
Suspected credential theft activity	Medium	-	○ Investigation running	Suspicious activity	Jo
Suspicious powershell commandline	Medium	-	● Remediated	Initial access	co
Suspicious powershell commandline	Medium	-	● Remediated	Initial access	co
Suspicious process injection observed	Medium	-	● Remediated	Initial access	co
Reflective dll loading detected	Medium	-	● Remediated	Initial access	co
Suspicious process injection observed	Medium	-	● Remediated	Initial access	co
Multi-stage incident involving Discovery & Command and control o...	High	5/5	○ Investigation running	Initial access, Suspicious activity+2 more	2

Protection first

→ Microsoft 365 Defender is a full protection stack!

1,000 Encounters

↓

300 Alerts

Alerts to Incidents

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

300 Alerts

↓

40 Incidents

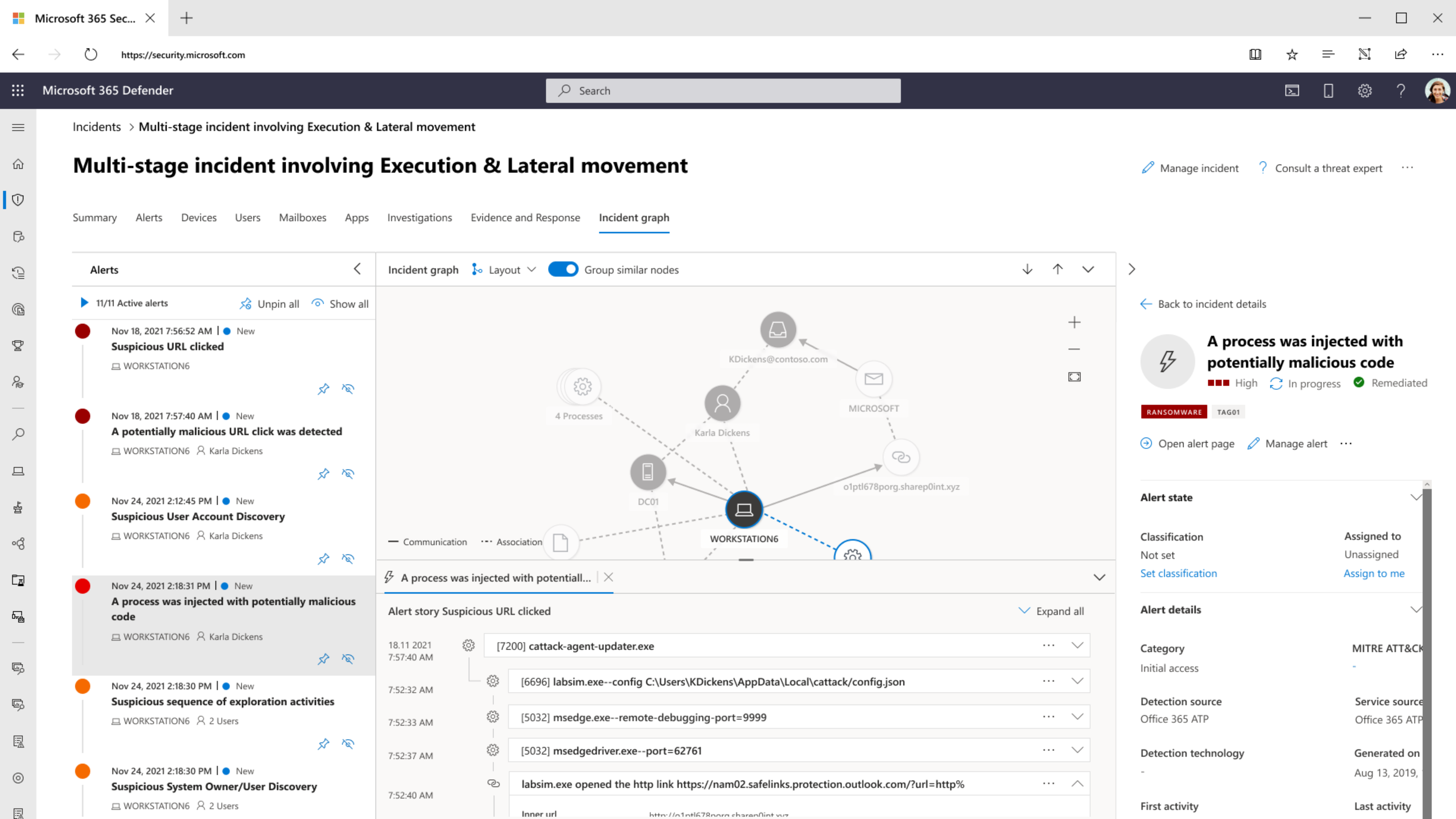
Automated Self-healing

→ Automatically resolves 75% of incidents

40 Incidents

↓

10 Incidents



Incidents > Multi-stage incident involving Execution & Lateral movement

Multi-stage incident involving Execution & Lateral movement

Nov 18, 2021 7:56:52 AM | New
Suspicious URL clicked
WORKSTATION6

Nov 18, 2021 7:57:40 AM | New
A potentially malicious URL click was detected
WORKSTATION6 Karla Dickens

Nov 24, 2021 2:12:45 PM | New
Suspicious User Account Discovery
WORKSTATION6 Karla Dickens

Nov 24, 2021 2:18:31 PM | New
A process was injected with potentially malicious code
WORKSTATION6 Karla Dickens

Nov 24, 2021 2:18:30 PM | New
Suspicious sequence of exploration activities
WORKSTATION6 2 Users

Nov 24, 2021 2:18:30 PM | New
Suspicious System Owner/User Discovery
WORKSTATION6 2 Users

A process was injected with potentiall...

Alert story Suspicious URL clicked

18.11 2021 7:57:40 AM [7200] cattack-agent-updater.exe

7:52:32 AM [6696] labsim.exe--config C:\Users\KDickens\AppData\Local\cattack/config.json

7:52:33 AM [5032] msedge.exe--remote-debugging-port=9999

7:52:37 AM [5032] msedgedriver.exe--port=62761

7:52:40 AM labsim.exe opened the http link https://nam02.safelinks.protection.outlook.com/?url=http%

Inner url http://o1ptl678porg.sharep0int.xyz

A process was injected with potentially malicious code

High In progress Remediated

RANSOMWARE TAG01

Alert state

Classification: Not set
Set classification

Assigned to: Unassigned
Assign to me

Alert details

Category: Initial access

MITRE ATT&CK: -

Detection source: Office 365 ATP

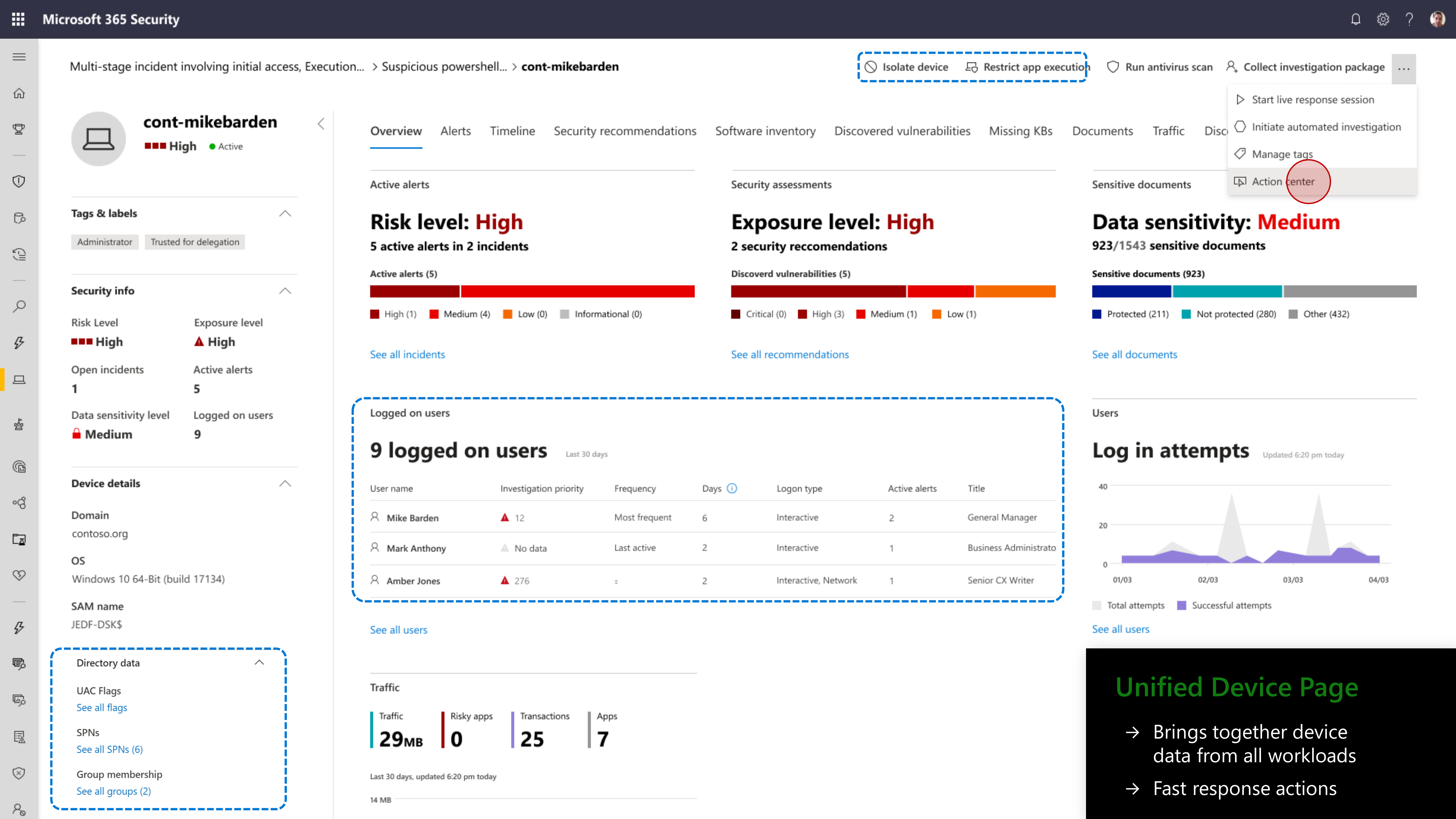
Service source: Office 365 ATP

Detection technology: -

Generated on: Aug 13, 2019,

First activity

Last activity



Microsoft 365 Security

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

Isolate device
Restrict app executio
Run antivirus scan
Collect investigation package
...
Start live response session
Initiate automated investigation
Manage tags
Action center

cont-mikebarden

High ● Active

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)

See all incidents

Security assessments

Exposure level: High

2 security reccomendations

Discoverd vulnerabilities (5)

See all recommendations

Sensitive documents

Data sensitivity: Medium

923/1543 sensitive documents

Sensitive documents (923)

See all documents

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

Users

Log in attempts Updated 6:20 pm today

See all users

Traffic

Traffic	Risky apps	Transactions	Apps
29MB	0	25	7

Last 30 days, updated 6:20 pm today

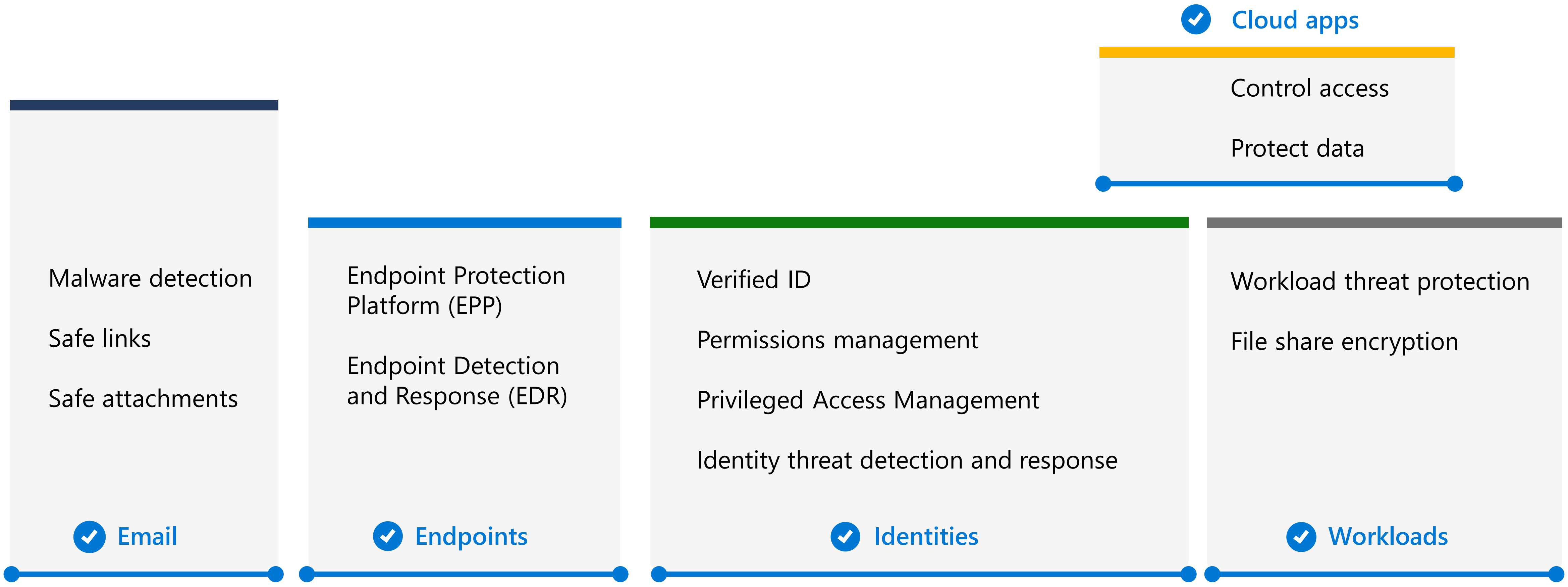
Unified Device Page

→ Brings together device data from all workloads

→ Fast response actions

Protection across the entire kill chain

With Microsoft SIEM and XDR



Malware detection

Safe links

Safe attachments

Email

Endpoint Protection Platform (EPP)

Endpoint Detection and Response (EDR)

Endpoints

Verified ID

Permissions management

Privileged Access Management

Identity threat detection and response

Identities

Cloud apps

Control access

Protect data

Workload threat protection

File share encryption

Workloads

Uncover the attack end to end and take action to completely evict the attacker.

Do more with less – Microsoft 365 Defender reduces costs and improves the SOC's efficiency

$17.1M

Average savings* compared to point solutions

>80%

alert reduction in the SOC queue

>75%

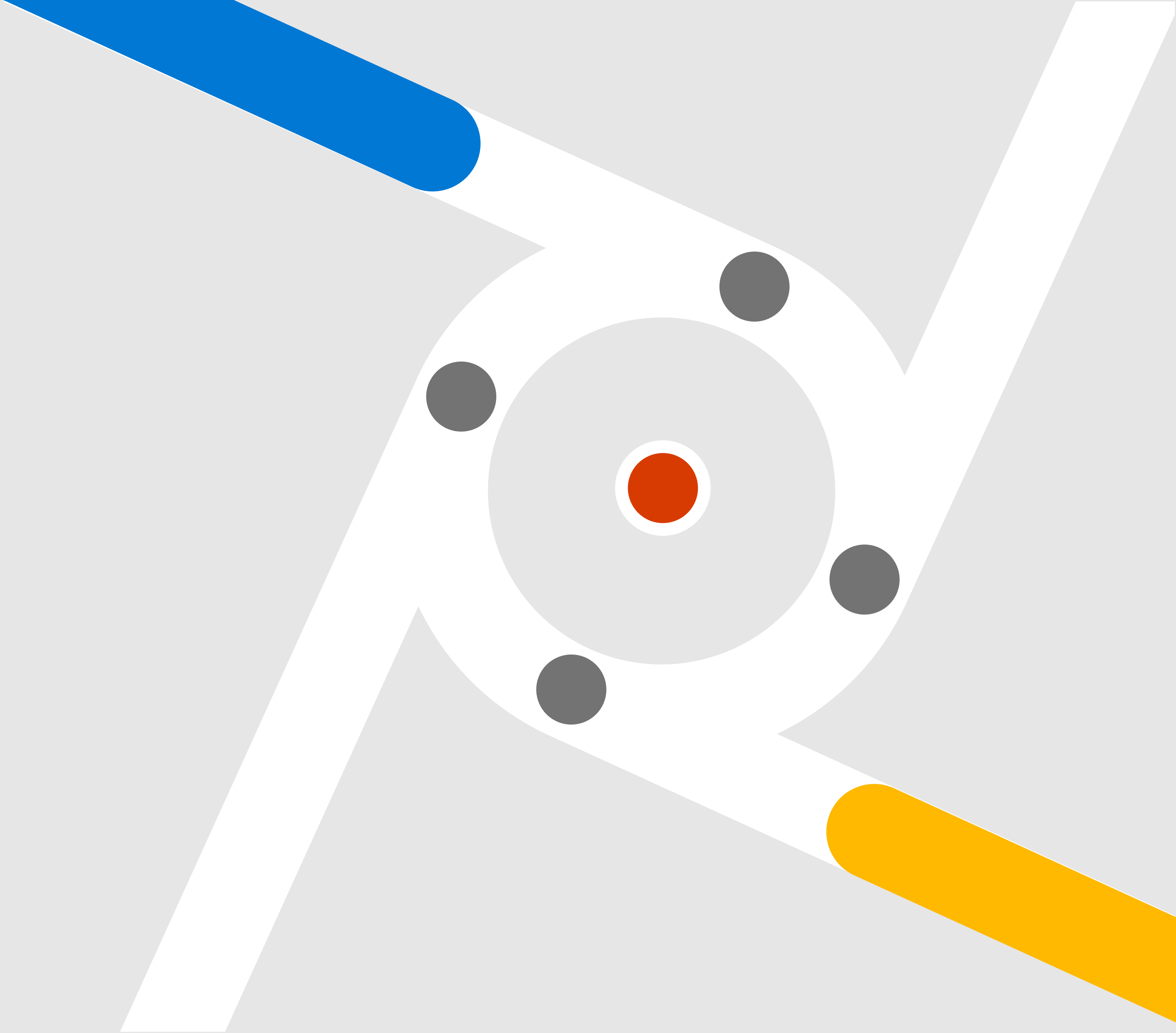
of work items resolved with automation

*over three years

1. Forrester Consulting, "The Total Economic Impact of Microsoft 365 Defender

Microsoft Security

Summary & Recommendations



Microsoft Security

The cyber resilience bell curve

98%

Basic security hygiene still protects against 98% of attacks

- Enable multifactor authentication
- Apply Zero Trust principles
- Use modern anti-malware
- Keep up to date
- Protect data

Microsoft Security

Thank you