



Incidentes cibernéticos em tempos de pandemia

Nycholas Szucko

Diretor Cybersecurity LATAM

nyszucko@microsoft.com

Cybersecurity: in the News, in the Boardroom

\$8 trillion

Cost (USD) of cybercrime to global economy by 2022

750+%

Growth in # of ransomware families in 2016

99 days

Median # of days between infiltration and detection

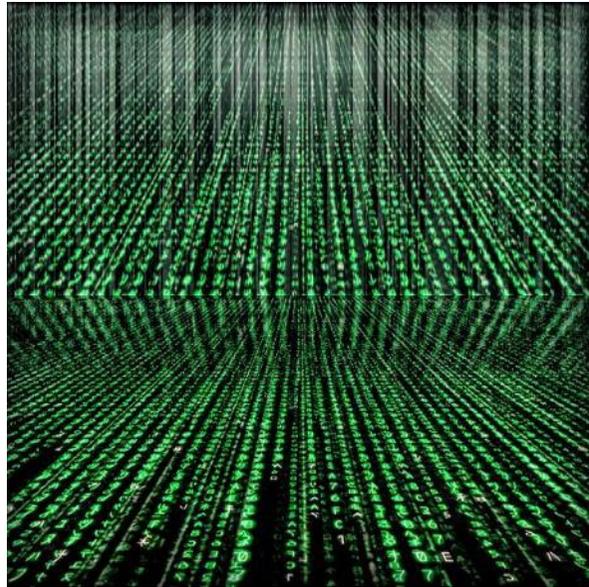
\$4M

Average cost of a data breach in 2017

88%

Of companies concerned about cyberattacks in 2017

Criminals are **smart, creative, well-financed** and **not limited by borders.**



Cybercrime challenges law enforcement



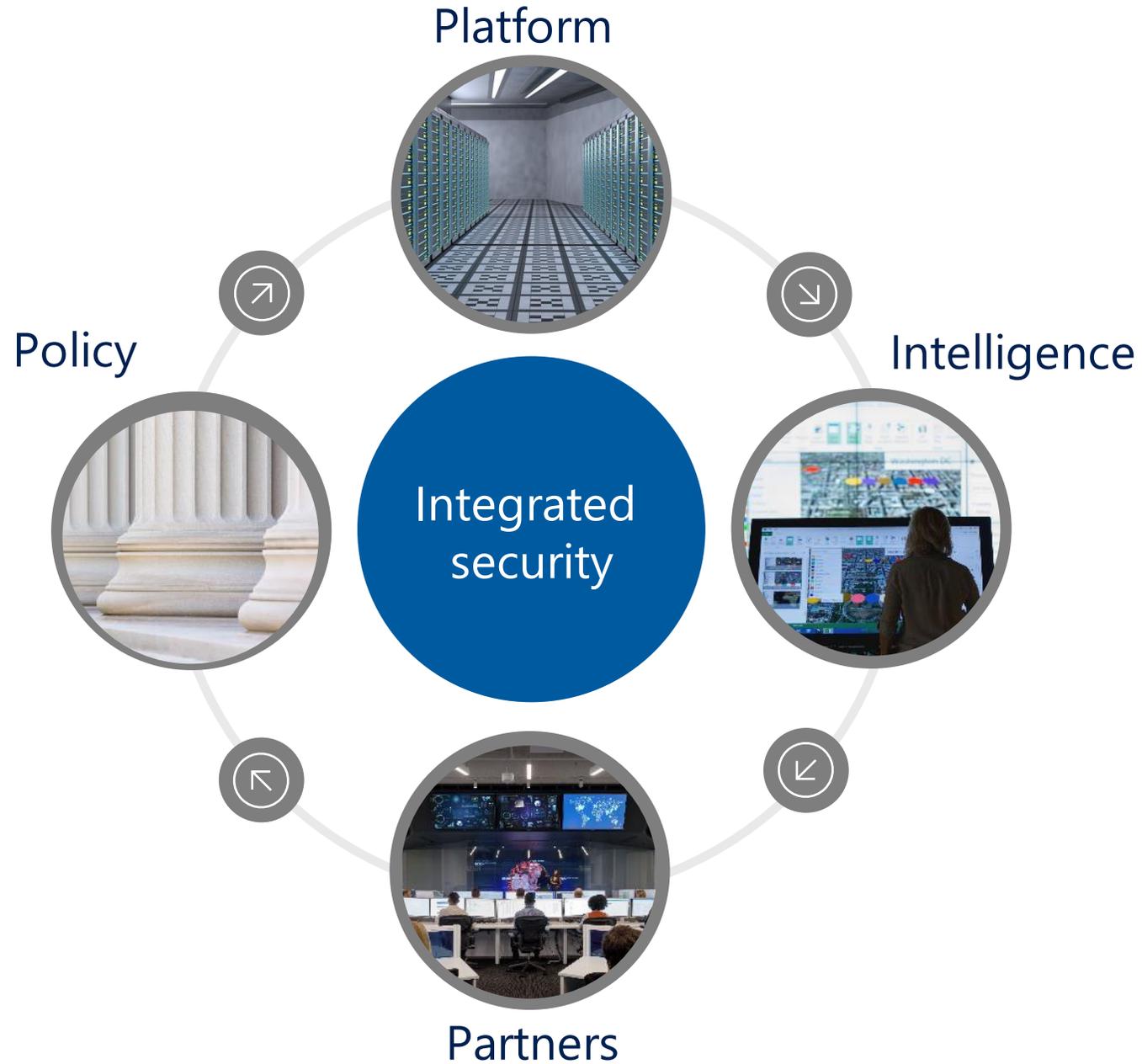
The Internet grants anonymity

Cybercrime disregards geopolitical borders

Crimes span multiple enforcement jurisdictions

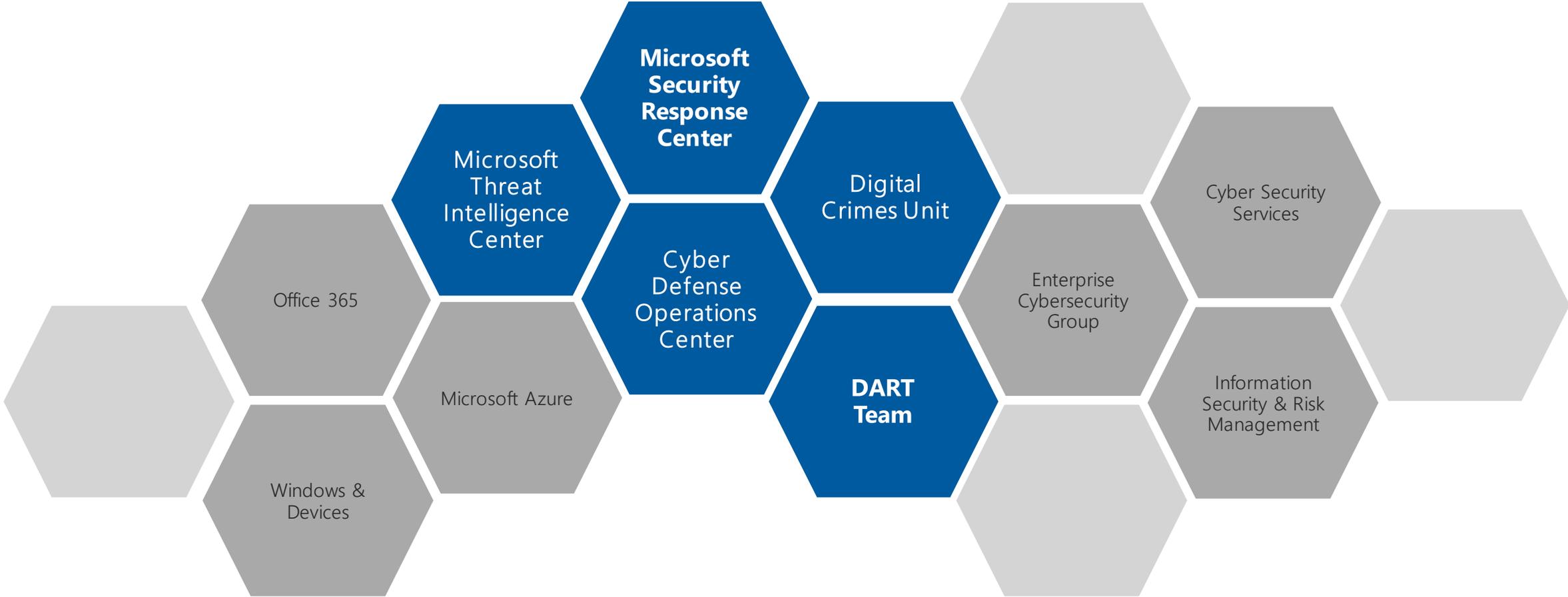
Need for cross-agency collaboration

Microsoft's Unique Approach

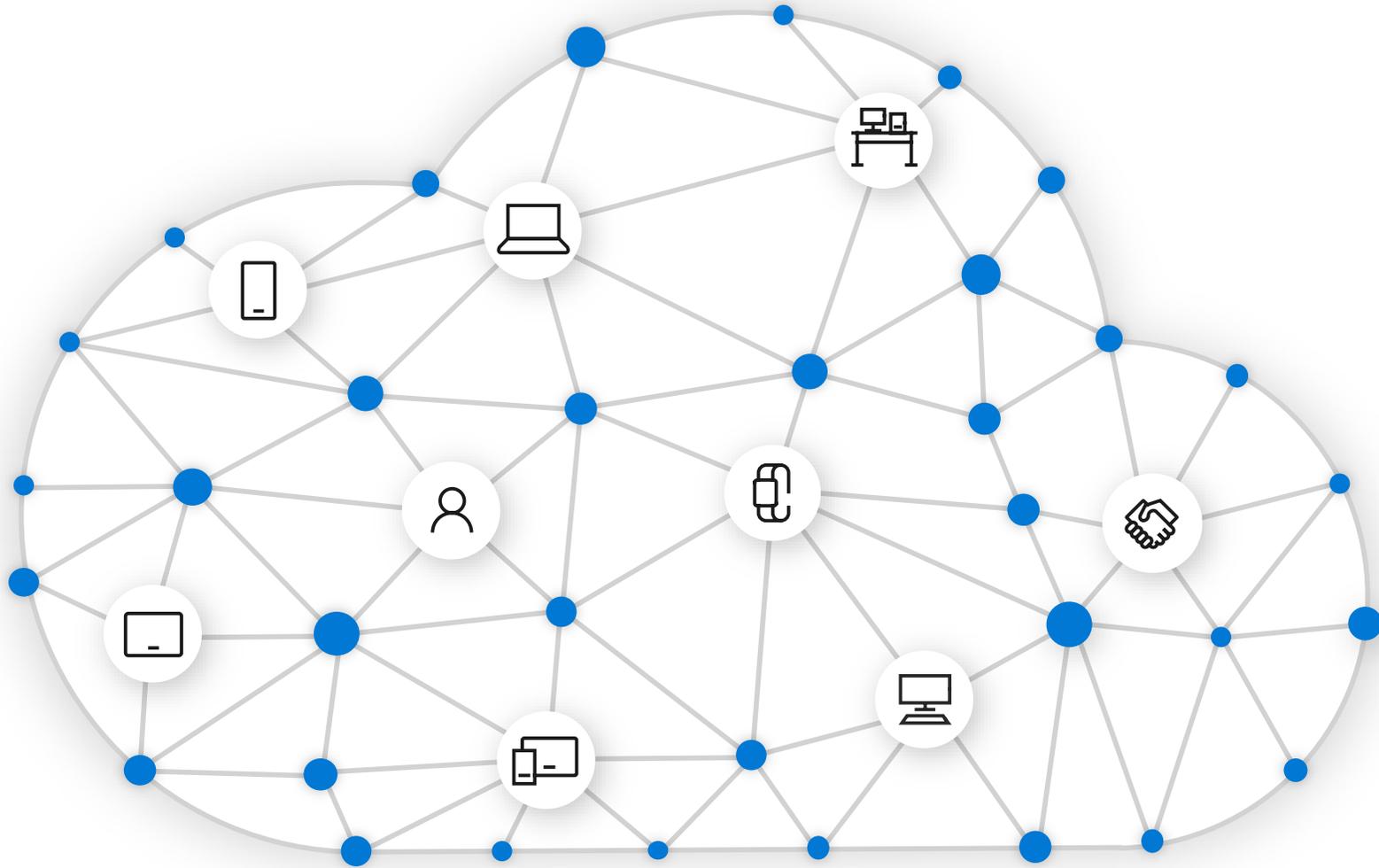


Working Together: Coordinated Response

Using intelligence gained, Microsoft security teams work together to secure our platform





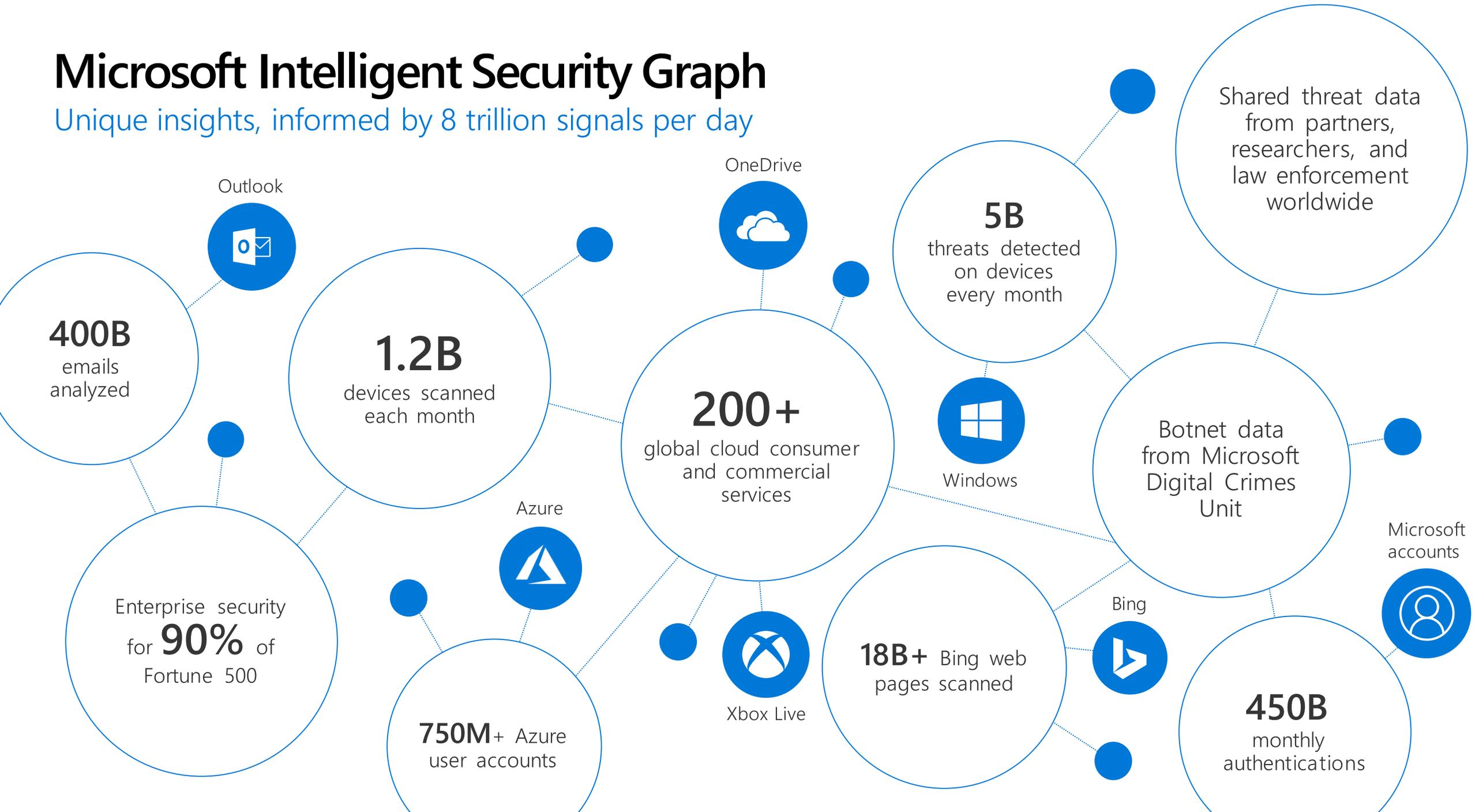


“The future of cybersecurity...is in the cloud.”¹

¹ <https://go.forrester.com/blogs/tech-titans-google-and-microsoft-are-transforming-cybersecurity/>

Microsoft Intelligent Security Graph

Unique insights, informed by 8 trillion signals per day

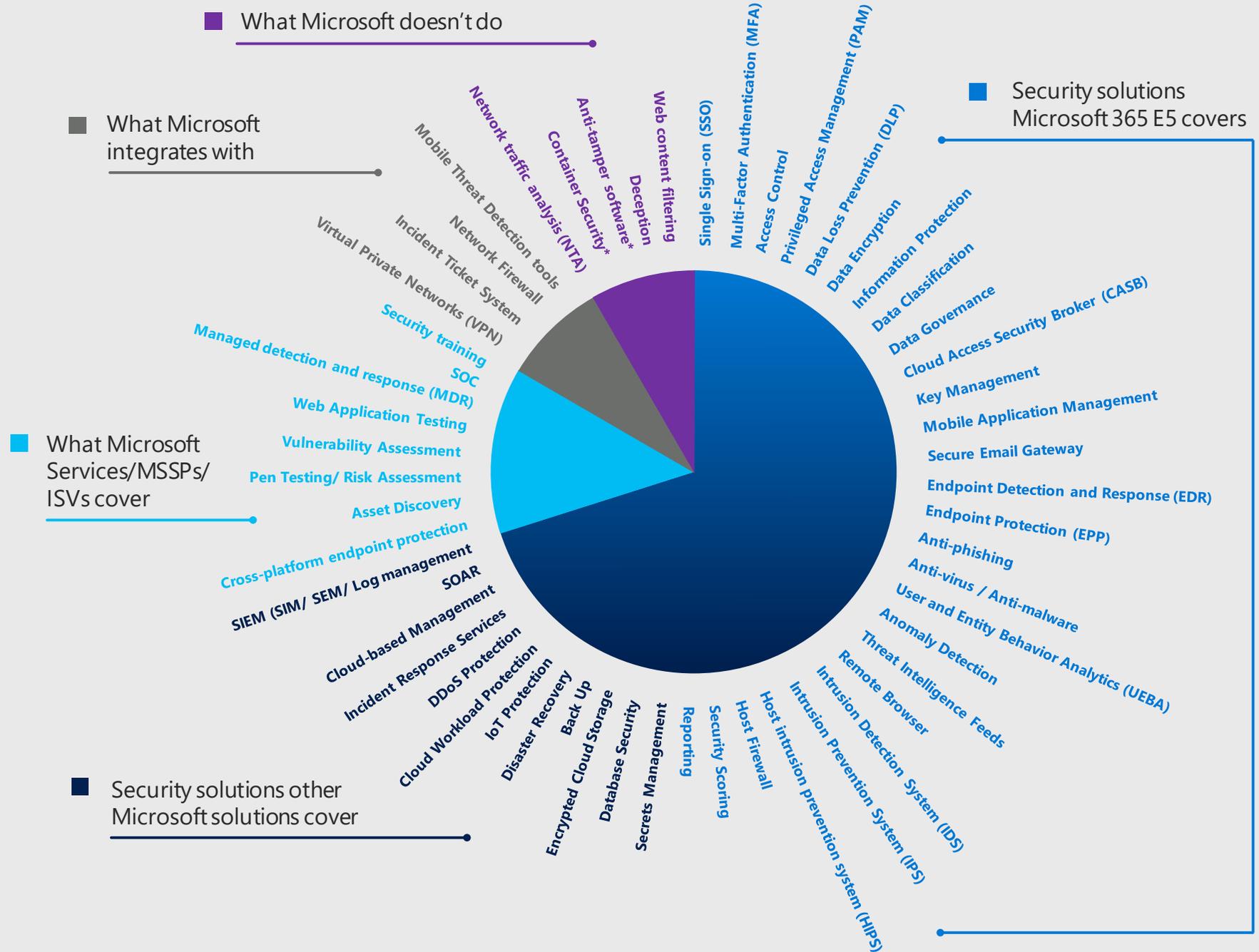




“ We have dozens of 3rd party solutions stitched together with duck tape and bail wire. ”

- CSO, General Atomics

Customers that have Microsoft 365 E5 Security can replace up to 26 other security vendors



Our unique approach



**Built-in experiences that
work across platforms**



**AI and automation
to secure your future**



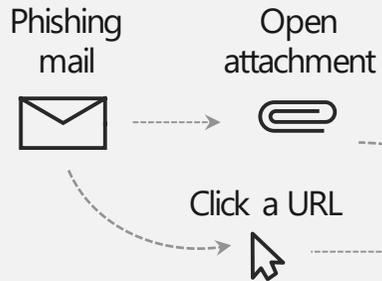
**Integrated across people,
devices, apps, and data**

Simplify security, improve threat protection



Office 365 ATP

Malware detection, safe links, and safe attachments



Azure AD Identity Protection

Identity protection & conditional access

 Brute force account or use stolen account credentials

Attacker collects reconnaissance & configuration data

Microsoft Cloud App Security

Extends protection & conditional access to other cloud apps



Microsoft Defender ATP

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

Exploitation & Installation

Command & Control

User account is **compromised**

Attacker attempts lateral movement

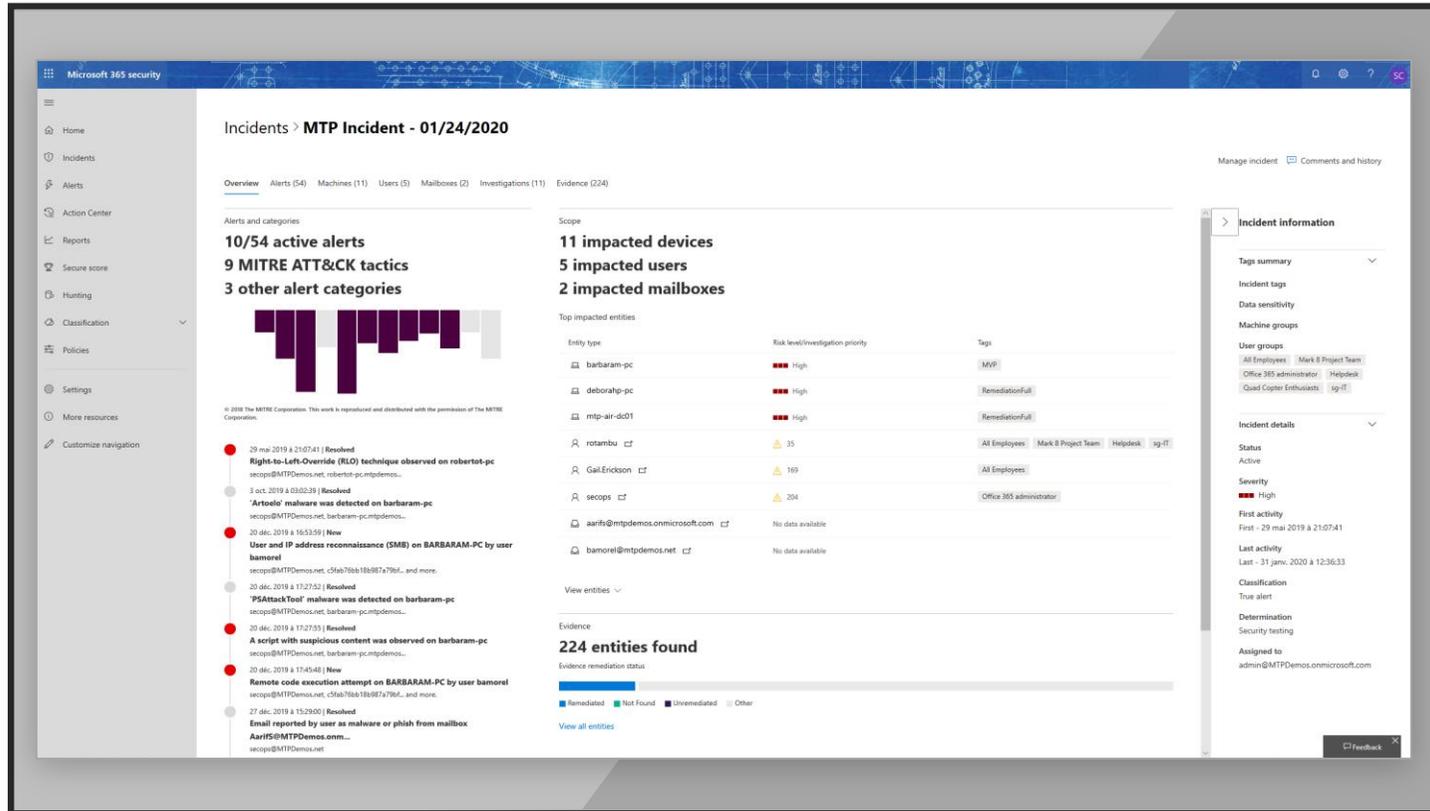
Privileged account **compromised**

Domain **compromised**

Azure ATP

Identity protection

Simplify security, improve threat protection

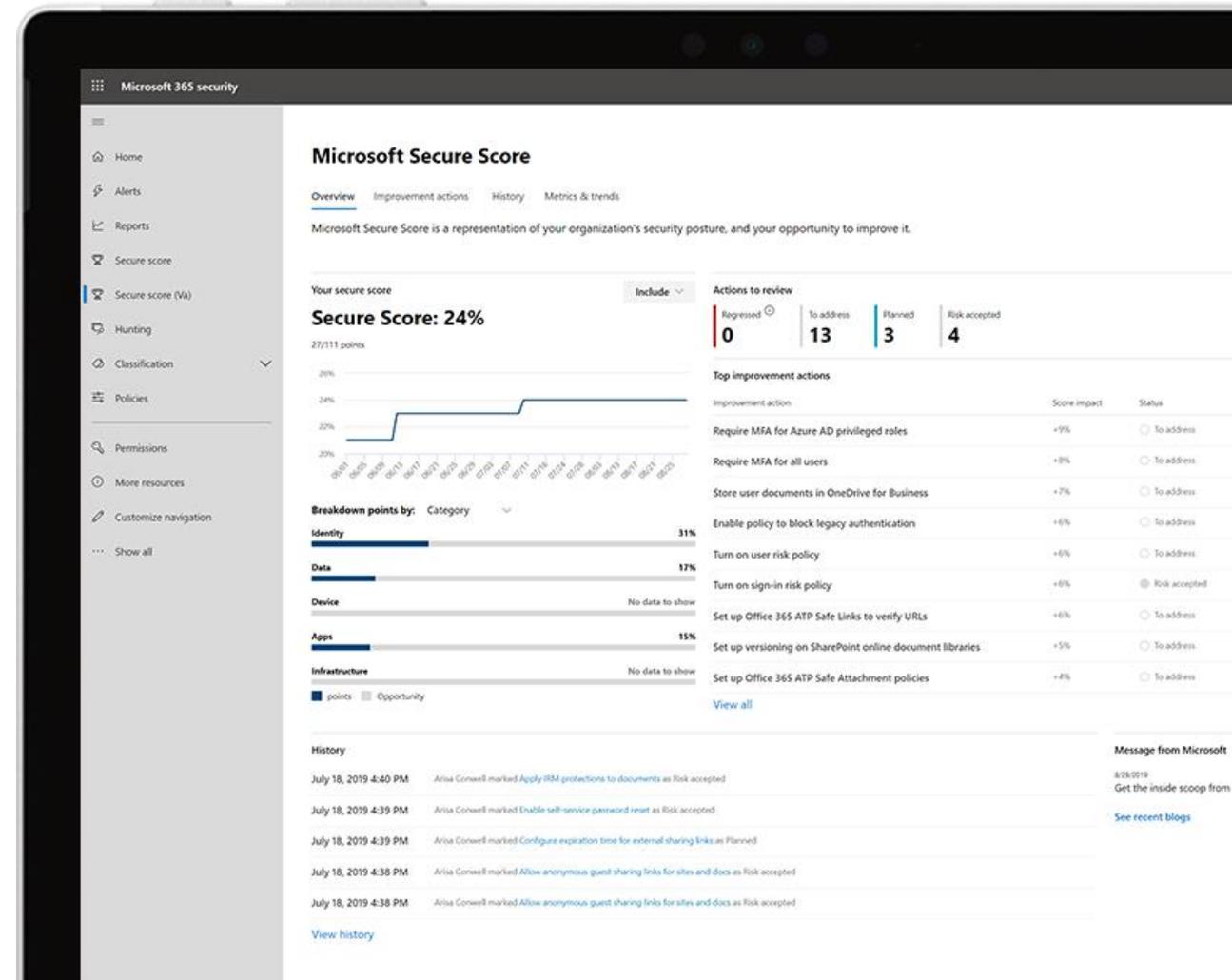


Integrated & coordinated threat protection:

- Correlated incidents
- Centralized view of automated workflows
- Advanced hunting across email and endpoints

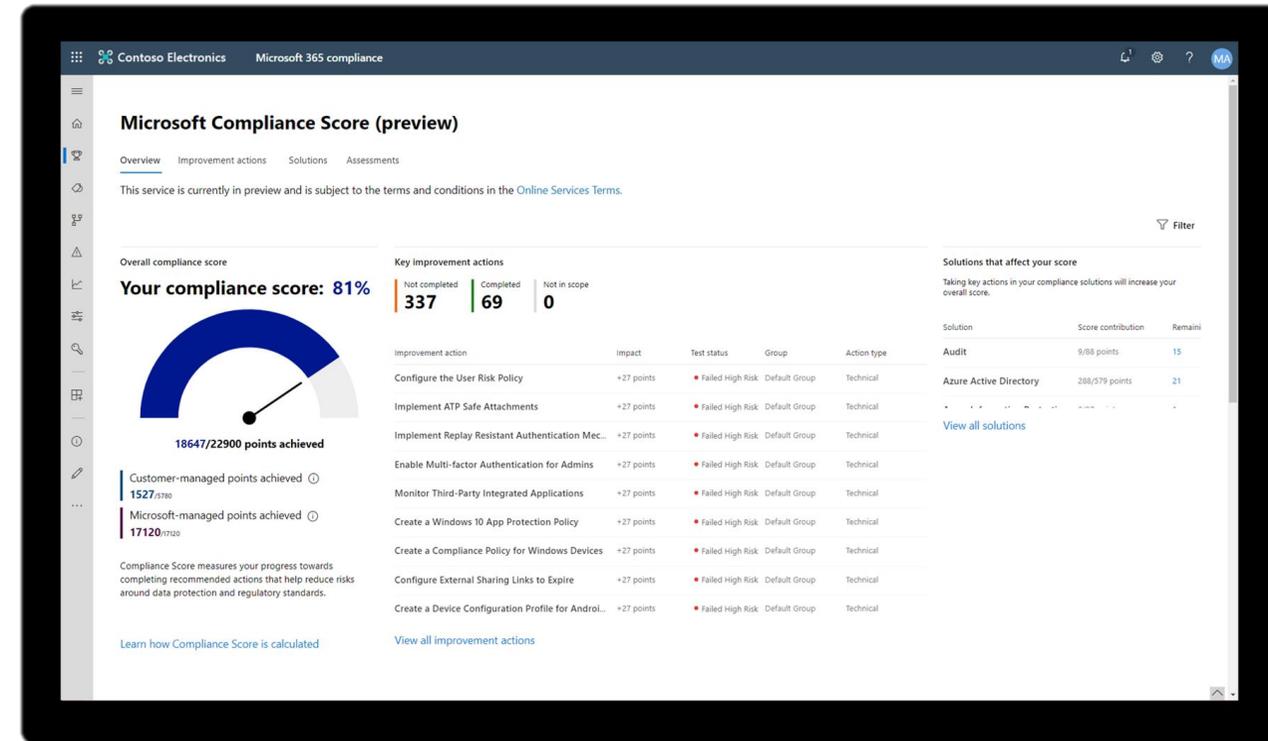
Microsoft Secure Score

Use intelligent insights and guidance to strengthen your organization's security posture with Microsoft Secure Score.



Compliance Manager - LGPD

Microsoft Compliance Score helps address the ever-changing data privacy landscape



- Overview
- Getting started
- Pricing & settings
- POLICY & COMPLIANCE**
- Coverage
- Secure score
- Security policy
- Regulatory compliance
- RESOURCE SECURITY HYGIENE**
- Recommendations
- Compute & apps
- Networking
- IoT Hubs & resources
- Data & storage
- Identity & access
- Security solutions
- ADVANCED CLOUD DEFENSE**
- Adaptive application controls
- Just in time VM access
- Adaptive network hardening
- File Integrity Monitoring

Subscriptions What's new

Policy & compliance

Secure score



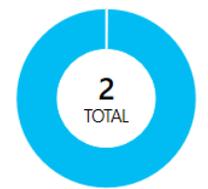
508 OF 950

[Review your secure score >](#)

Regulatory compliance

SOC TSP	1 of 13 passed controls
ISO 27001	2 of 20 passed controls
PCI DSS 3.2.1	5 of 41 passed controls

Subscription coverage



2 TOTAL

655 Covered resources

- Fully covered: 2
- Partially covered: 0
- Not covered: 0

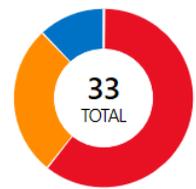
Make alert data available to your SIEM

You can make Security Center alert data available to your SIEM connector

[Set up SIEM connector >](#)

Resource security hygiene

Recommendations



33 TOTAL

- High Severity: 20
- Medium Severity: 9
- Low Severity: 4

310 Unhealthy resources

Resource health by severity

322 Compute & apps resources	310 Data & storage resources
19 Networking resources	4 Identity & access resources

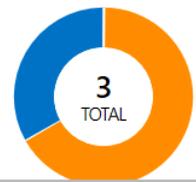
Review and improve your secure score

Review and resolve security issues to improve your secure score and secure your resources

[Learn more >](#)

Threat protection

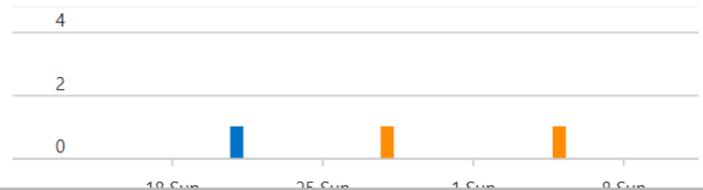
Security alerts by severity



3 TOTAL

- High Severity: 0
- Medium Severity: 2
- Low Severity: 1

Security alerts over time



High severity	0
Medium severity	2
Low severity	1

New - Advanced threat protection

Security Center can now proactively detect unusual and potentially malicious activity or exploit Storage accounts

Simplify security. Save 52%

Let's get started



Microsoft security workshop

Threat check

Security discovery

Security immersion experience



Thank you.