



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

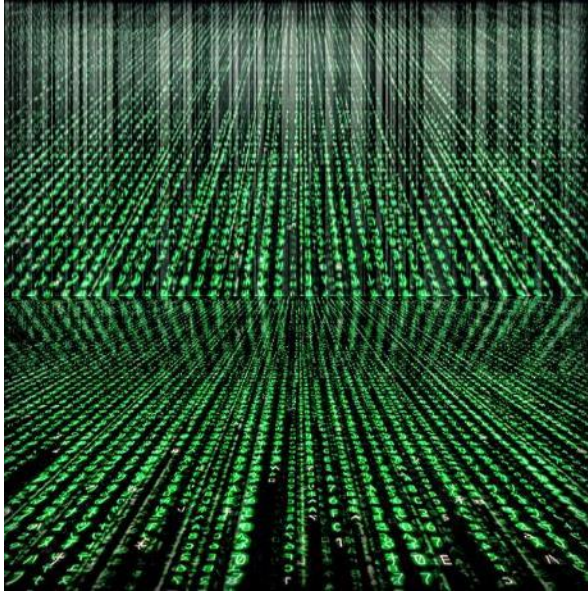
\$4M

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



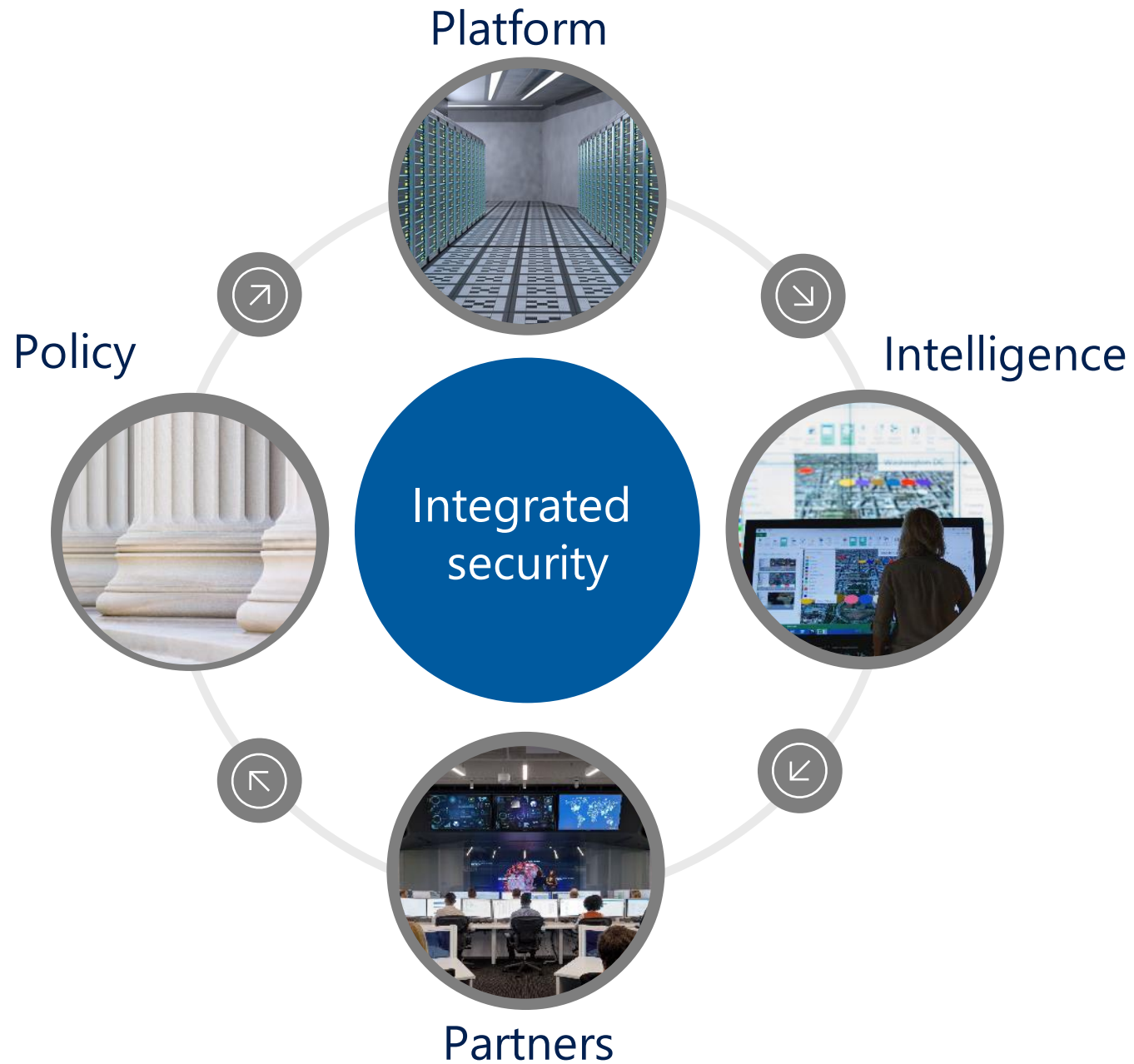
The Internet grants anonymity

Cybercrime disregards geopolitical borders

Crimes span multiple enforcement jurisdictions

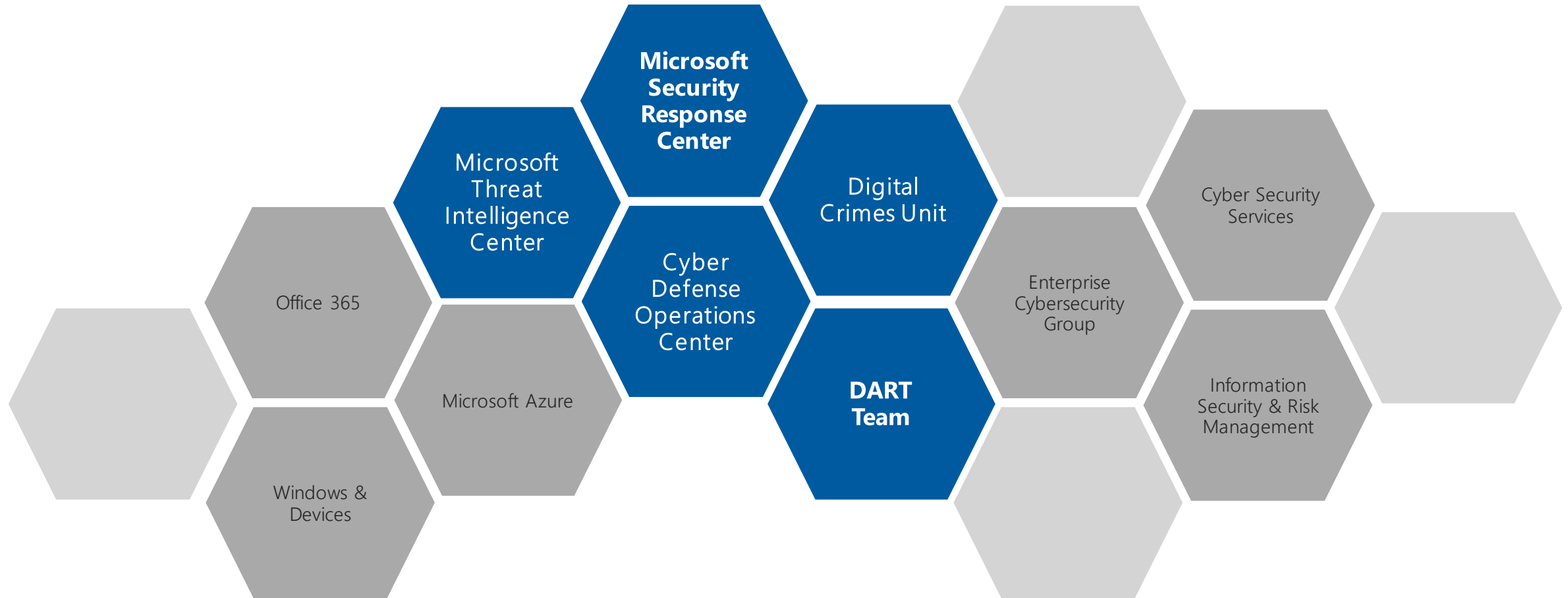
Need for cross-agency collaboration

Microsoft's Unique Approach

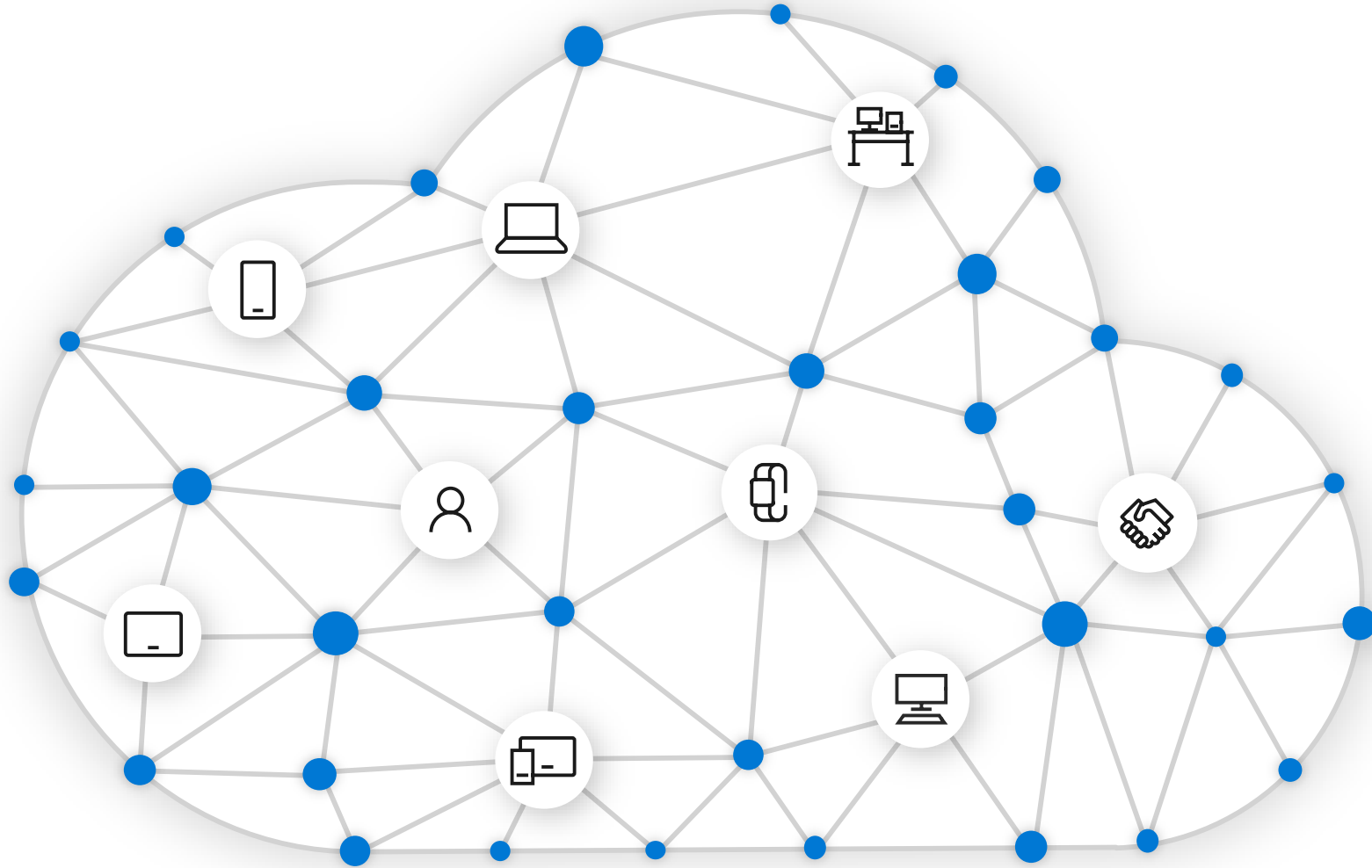


Working Together: Coordinated Response

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





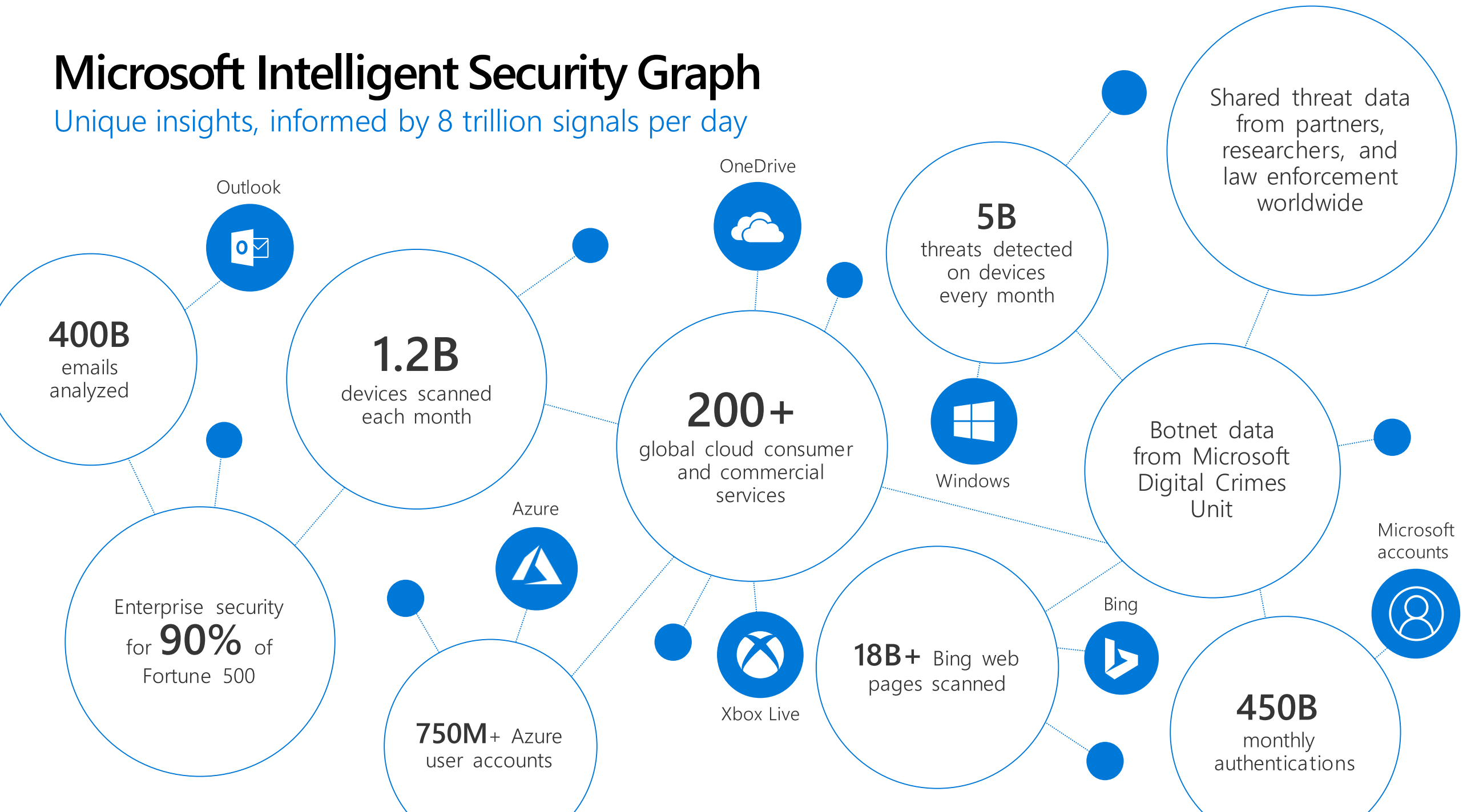


“The future of cybersecurity...is in the cloud.”¹

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



Application Security

Advanced Threat Protection

Palo Alto Networks
 BluVector
 Check Point
 Cisco
 CorSA
 FireEye
 Fortinet
 Huawei
 Hysolate

JoeSecurity
 Juniper
 Lastline
 McAfee
 Metasploit
 Mimecast
 Opswat
 Qualys
 Reversing Labs

RESEC
 Sunar Software
 SonicWall
 Sophos
 Spirinix
 Symantec
 Veeva
 Votiro
 WatchGuard

NAC

Aruba
 Baucor
 Cisco
 Ardus
 Extreme
 ForeScout
 Fortinet
 Genixis
 Portnox
 Trustwave

SDN

BlackBridge
 Certo
 Cybera
 Cylance
 Cyberark
 Cybertronics
 Skyport Systems
 Tempered
 Versa
 Zentao
 Zscaler

DDoS Protection

Alcamal
 Check Point
 Fortinet
 Imperva
 Neustar
 Neuroguard
 Refocus
 Oracle
 Secure64
 StackPath

DNS Security

Bluecat
 Cisco
 Infoblox
 Efficient IP
 Infoblox
 Neustar
 Secure64
 ThreatSTOP
 Veeva

Network Firewall

Alcamal
 Cisco
 Check Point
 Cisco
 Clovis
 Endian
 FireEye
 ForeScout
 Fortinet
 Hysolate
 Huawei
 OPAG
 Sangfor
 Secured
 SonicWall
 Sophos
 Stormshield
 Tufin
 Veeva

Decryption

Acavallo
 Active
 CyberTrap
 Cymmetria
 Fidelis
 Mokescree
 Viper
 WatchGuard

A collage of logos for various companies, including APERIO, MCS + CIT, BELDEN, GIGALOG, CYPRESS, CYBERX, COMBUSTOR, DRAGON, endian, FORTINET, FORESCOUT, HALO, Inology, dimension, NextView, PPF, OWL, radwin, RHEBO, and others.

[illegible]

The collage features logos for various cybersecurity and application security companies, organized into three main categories:

- WAF & Application Security:** Includes logos for Acunetix, AIO, Akamai, Allot, Cloudflare, Contrast, CyberArk, DigiNotar, Fortinet, Imperva, Netspi, OnePass, Oracle, Penta, PortShift, PureSec, Qualys, Rapid7, Reblaze, Riverbed, Scuri, Synopsys, Tenable, Trend Micro, Trustwave, Veracode, Vicarius, Wallarm, Wazark, and Whitelabel.
- Application Security Testing:** Includes logos for Acunetix, Beyond, Bugcrowd, BugPanda, Checkmarx, ERPScan, Fasoo, Hackerone, IBM, MicroFocus, NewSecure, Parasoft, Performe, PortSwigger, Qualys, Rapid7, Security Compass, SiteLock, Snyk, Sonarsource, Synack, Synopsys, Tenable, Trustwave, Veracode, Whitelabel, and WhiteSource.
- Cloud Security:** Includes logos for AWS, Azure, Google Cloud, IBM, Microsoft, Oracle, SAP, Salesforce, ServiceNow, VMware, and Workday.

MSSP

[illegible]

BlueTalon CODE42 Dextel dataphy
 DECRYPTHERN CIPHERLOCK egress global security
 IONIC opentext PRIVITAR SECURE
 SPINSON StorageCraft TINKER VANDIVE VERA

Risk & Compliance

[illegible]

Security Ops & Incident Response

Threat Intelligence

IoT

[illegible]

Messaging Security

Identity & Access Management

The collage displays a wide array of logos from companies in the cybersecurity and identity space. The logos are organized into several horizontal rows, each representing a different category:

























- Authentication:** Includes logos for Accepto, Auth0, Averaon, BehavioSec, Biocatch, CallSign, Centrify, CLEF Security, CORE Security, EXOSTAR, FUDU Products, Google, HPR, IEE, Imprivata, INTRINSIC ID, JUMIO, NOK, PENDING, plainID, SAASPASS, SaferPass, SECRET KEY, SECUREPUSH, ShoCard, SILVERFORT, tascant, ThreatMetrix, TRUSONA, UNBEBOUND, UNIFY YTD, UNIKEY, V-KEY, and VIRGIL.
- Privileged Management:** Includes logos for VAVEN, okta, Centrify, onelogin, IBM, idaptive, iNtens, CRACLE, RSA, Microsoft, and THALES.
- Identity Governance:** Includes logos for BeyondTrust, ManageEngine, Centrify, MICRO FOCUS, CYBERARK, ONE IDENTITY, FUDU Remediant, HITACHI, IBM thyrotic, ADDOMATICS, Datto, helpsystems, ScailPoint, SAVVYNT, and simeio.
- Consumer Identity:** Includes logos for Akamai, Auth0, BEIRAN, FORRESTER, IDExperts, IDME, JUMIO, loginradius, Microsoft, PINE, PIREAN, SECURE, Trulook, vchain, verato, and VERACLOUD.

Security Analytics

Blockchain

Security Consulting & Services

Fraud & Transaction Security

Cloud Security

[illegible]

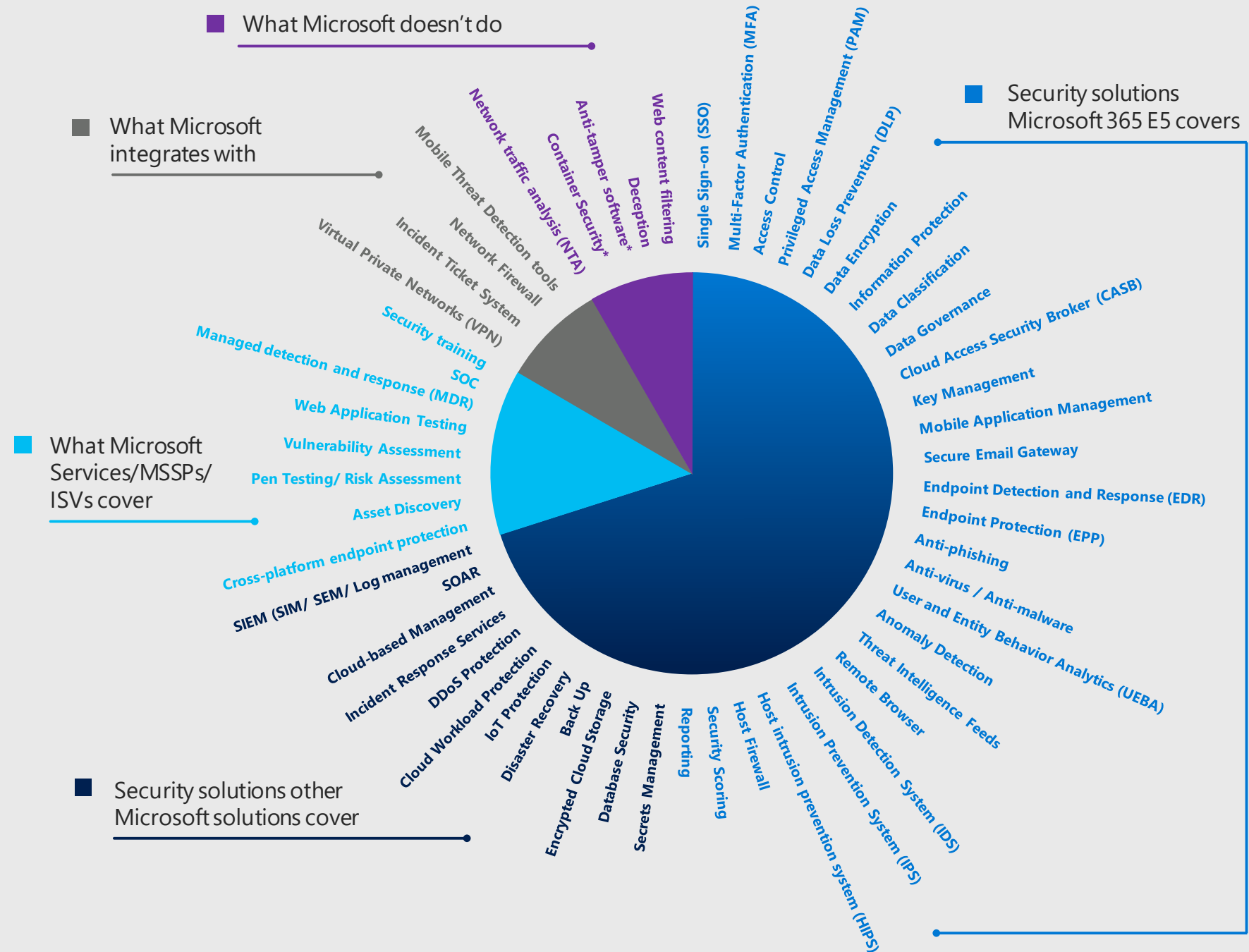
CASE

The background image shows two cars parked on a grassy field. On the left, a blue car has a large, jagged hole in its rear window. On the right, a red car has a large, jagged hole in its rear door. In the background, there is a chain-link fence and some trees.

“ 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**



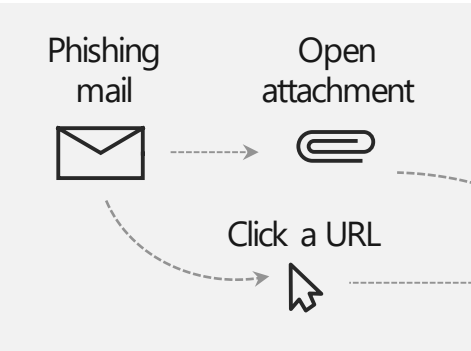
**Integrated across people,
devices, apps, and data**

Simplify security, improve threat protection



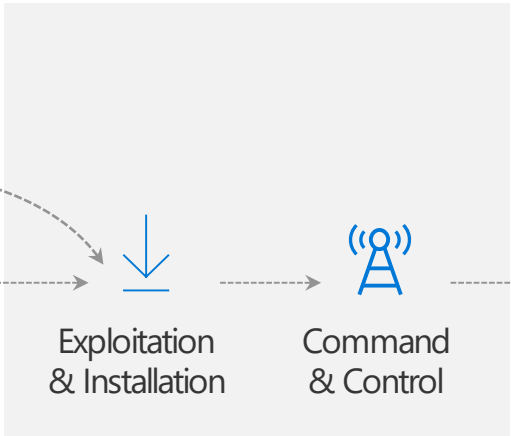
Office 365 ATP

Malware detection, safe links, and safe attachments



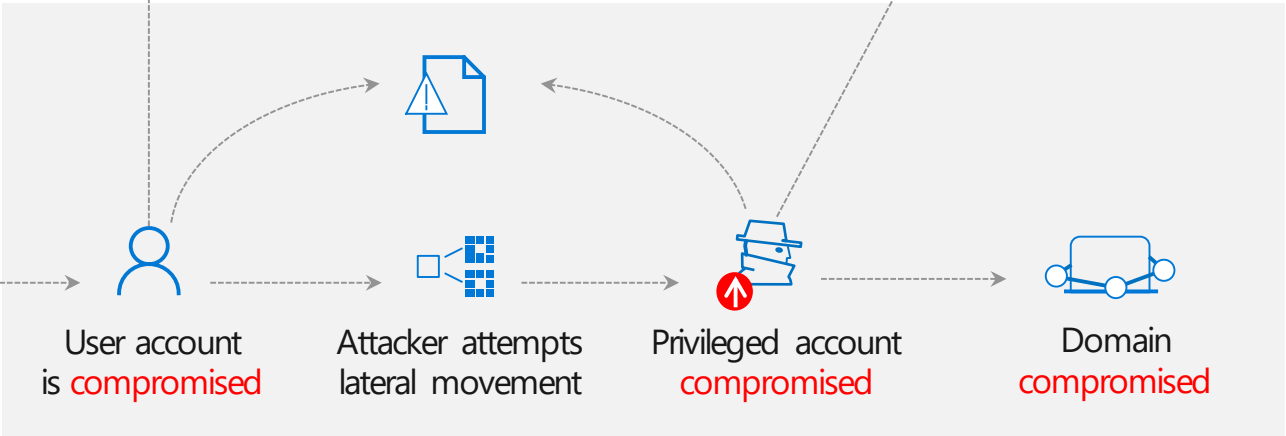
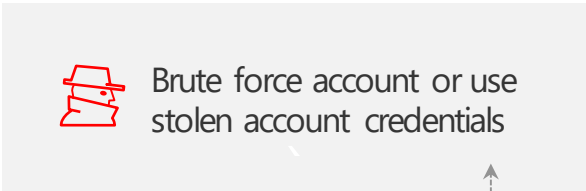
Microsoft Defender ATP

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



Azure AD Identity Protection

Identity protection & conditional access



Azure ATP

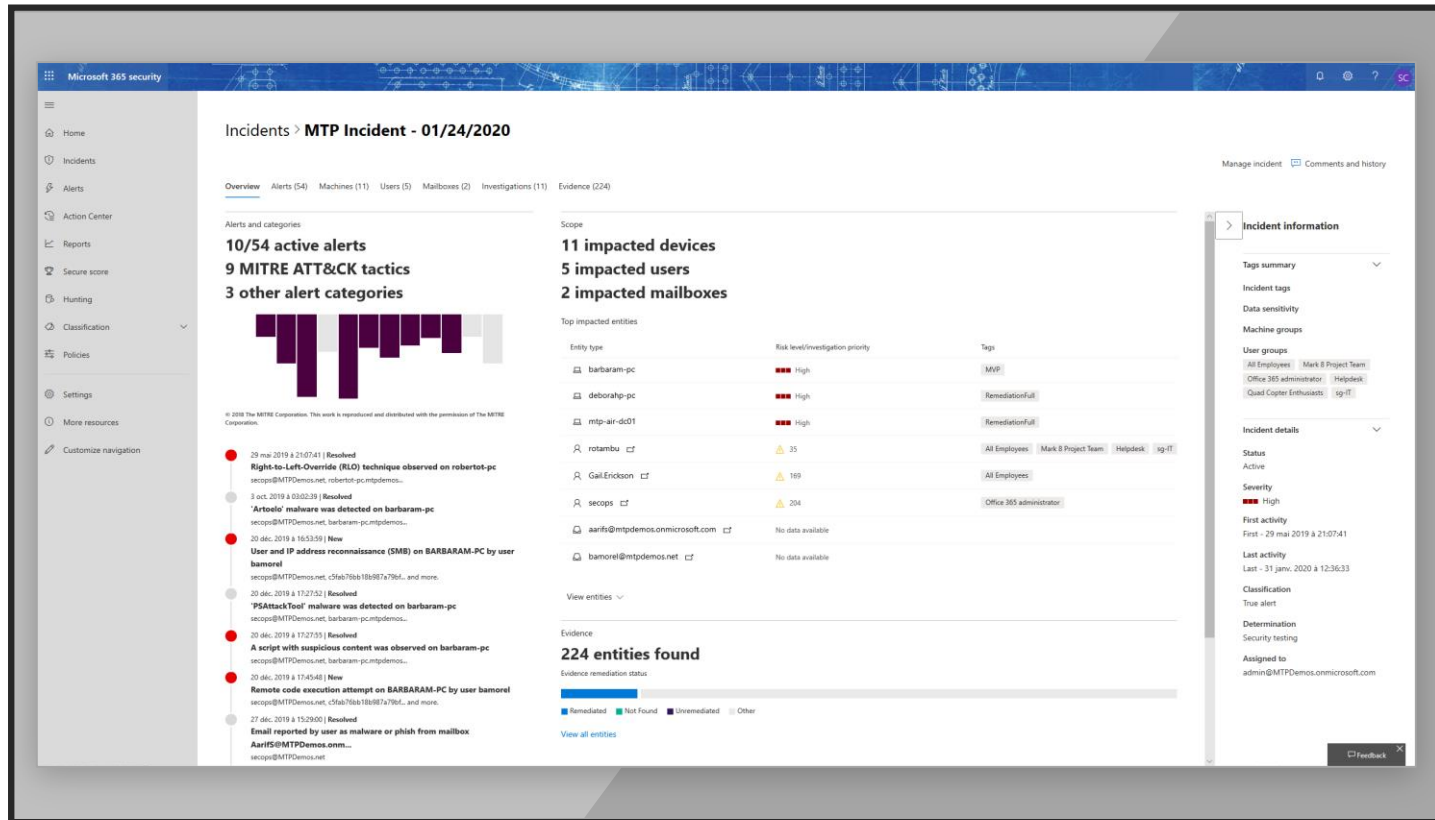
Identity protection

Microsoft Cloud App Security

Extends protection & conditional access to other cloud apps



Simplify security, improve threat protection

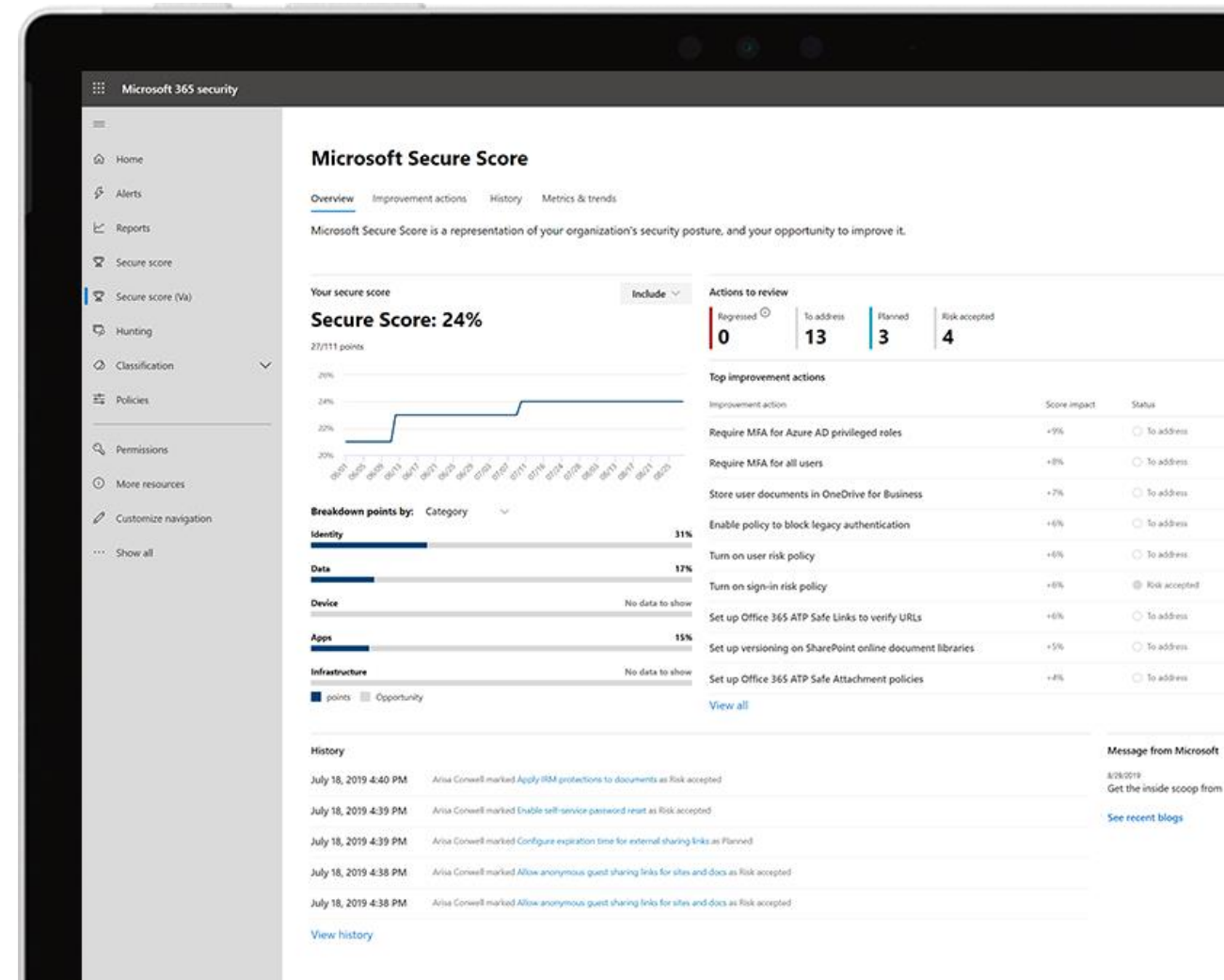


Integrated & coordinated threat protection:

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

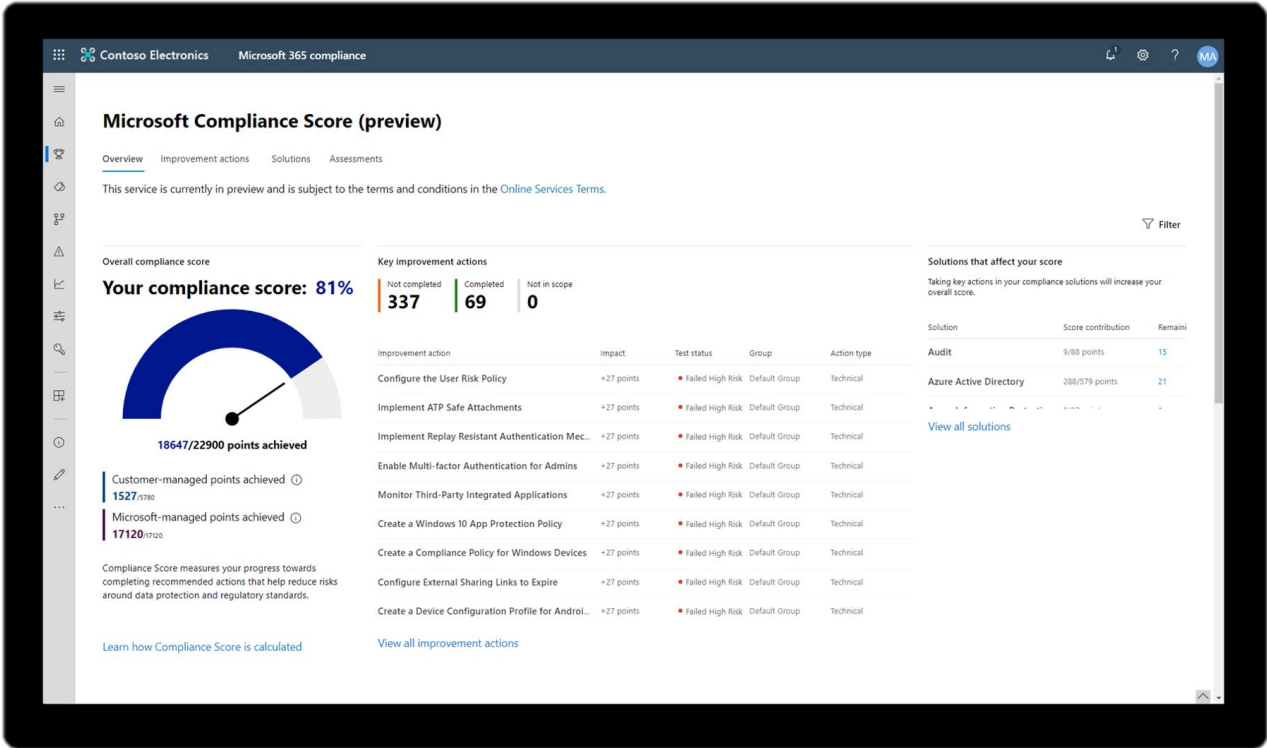
Microsoft Secure Score

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



[Subscriptions](#) [What's new](#)

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](#)

Policy & compliance

Secure score



508 OF 950

[Review your secure score >](#)

Regulatory compliance

SOC TSP

1 of 13 passed controls

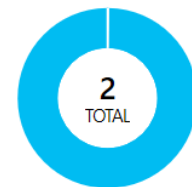
ISO 27001

2 of 20 passed controls

PCI DSS 3.2.1

5 of 41 passed controls

Subscription coverage



655 Covered resources

Fully covered
2

Partially covered
0

Not covered
0

Make alert data available to your SIEM

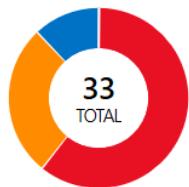


You can make Security Center data available to your SIEM connector

[Set up SIEM connector >](#)

Resource security hygiene

Recommendations



310 Unhealthy resources

High Severity
20

Medium Severity
9

Low Severity
4

Resource health by severity



322 Compute & apps resources



19 Networking resources



310 Data & storage resources



4 Identity & access resources

Review and improve your secure score

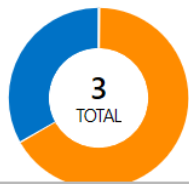


Review and resolve security alerts, improve your secure score and secure your resources

[Learn more >](#)

Threat protection

Security alerts by severity

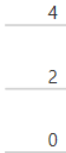


High Severity
0

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 in your Storage accounts

Simplify security. Save 52%

Let's get started



Microsoft security workshop

Threat check

Security discovery

Security immersion experience



Thank you.