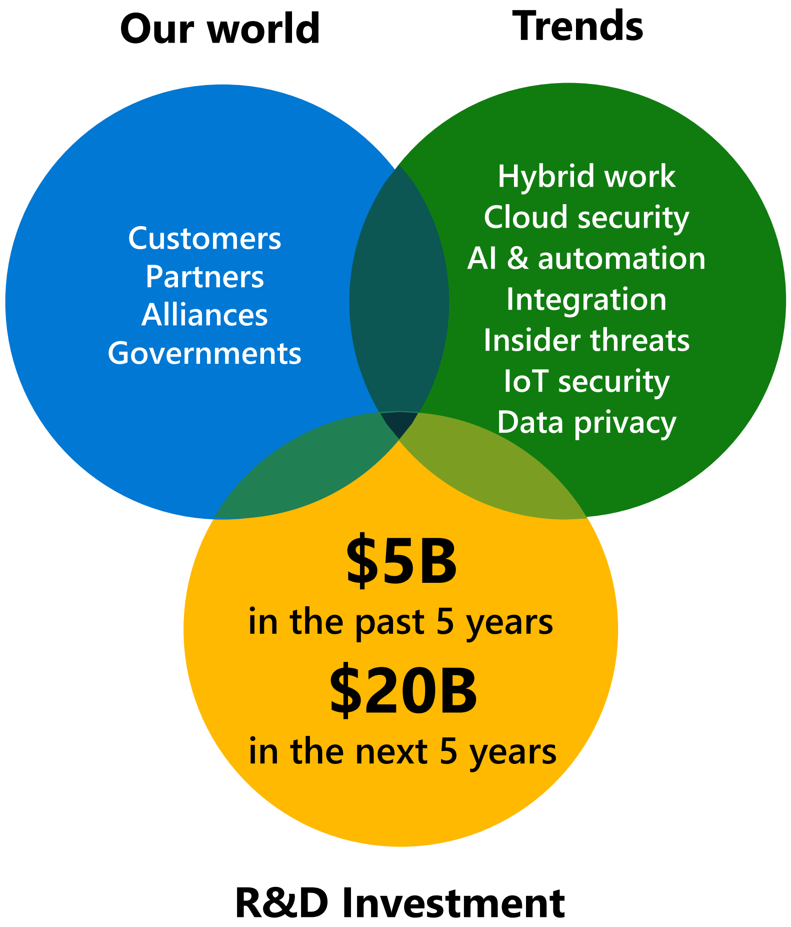
Microsoft Security

Microsoft Security

Building a safer world together

Dag Nyrud
Director – Security & Modern Work
Microsoft Norway

May 2023


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

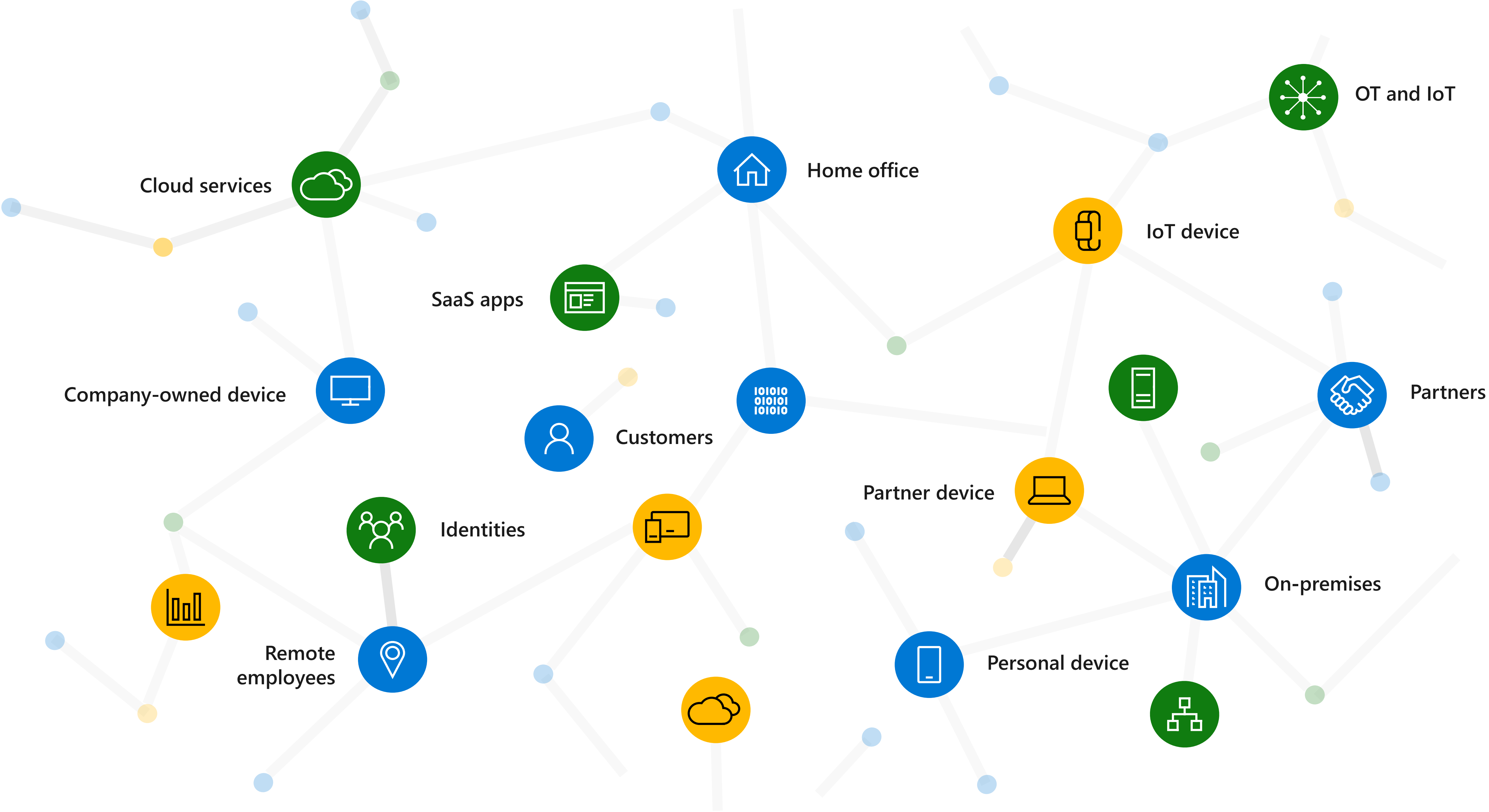
$20B
in the next 5 years

R&D Investment

> *"Security is our top priority, and we are committed to working with others across the industry to protect our customers."*
>
> Satya Nadella
> *Chief Executive Officer, Microsoft Corporation*

Security has never been more critical

The technology environment has never been so complex



Cloud services
Home office
OT and IoT
IoT device
SaaS apps
Company-owned device
Customers
Partners
Partner device
Identities
On-premises
Remote employees
Personal device

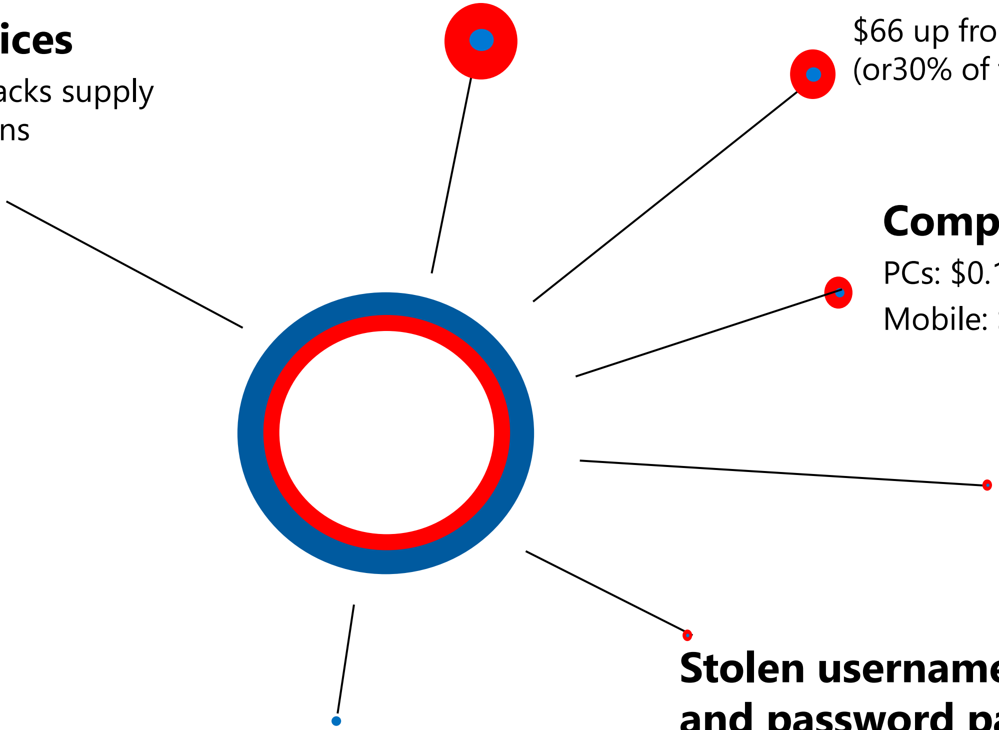
Navigating a shifting world

Attacks growing
more sophisticated

Conventional security tools
have not kept pace

Regulatory landscape
becoming **more complex**

The cybercrime economy and services



Attacker for hire (per job)

$250 per job (and up)

Randsomeware kits)

$66 up front

(or30% of the profit / affiliate money)

Other Services

Continuous attacks supply chain innovations

Compromised PCs/Devices

PCs: $0.13 to $0.89

Mobile: $0.87 to $2.78

Spearfishing for hire

$100 to $1.000

(per successful account takeover)

Stolen username and password pairs

$0.97 per 1,000 (average)

(Bulk: $150 for 400M)

Denial of Service

$311.88 per month

WITH NO TECHNICAL KNOWLEDGE OF HOW TO CONDUCT A CYBERCRIME ATTACK, AN AMATEUR THREAT ACTOR CAN PURCHASE A RANGE OF SERVICES TO CONDUCT THEIR ATTACKS WITH ONE CLICK.

100M

password attacks took place globally everyday

+667% increase

in phishing attacks

Security Snapshot

Business Email Compromise

attempts detected and investigated
by Microsoft Threat Intelligence
Digital Crimes Unit (DCU)
from April '22 to April '23

Cyber signals report – May 23:

Blogpost:
https://aka.ms/CyberSignals4SecurityPost

Insider article:
https://aka.ms/CyberSignals-4

35 Million
Annual

156,000
Daily

417,678
Phishing URL
Takedowns

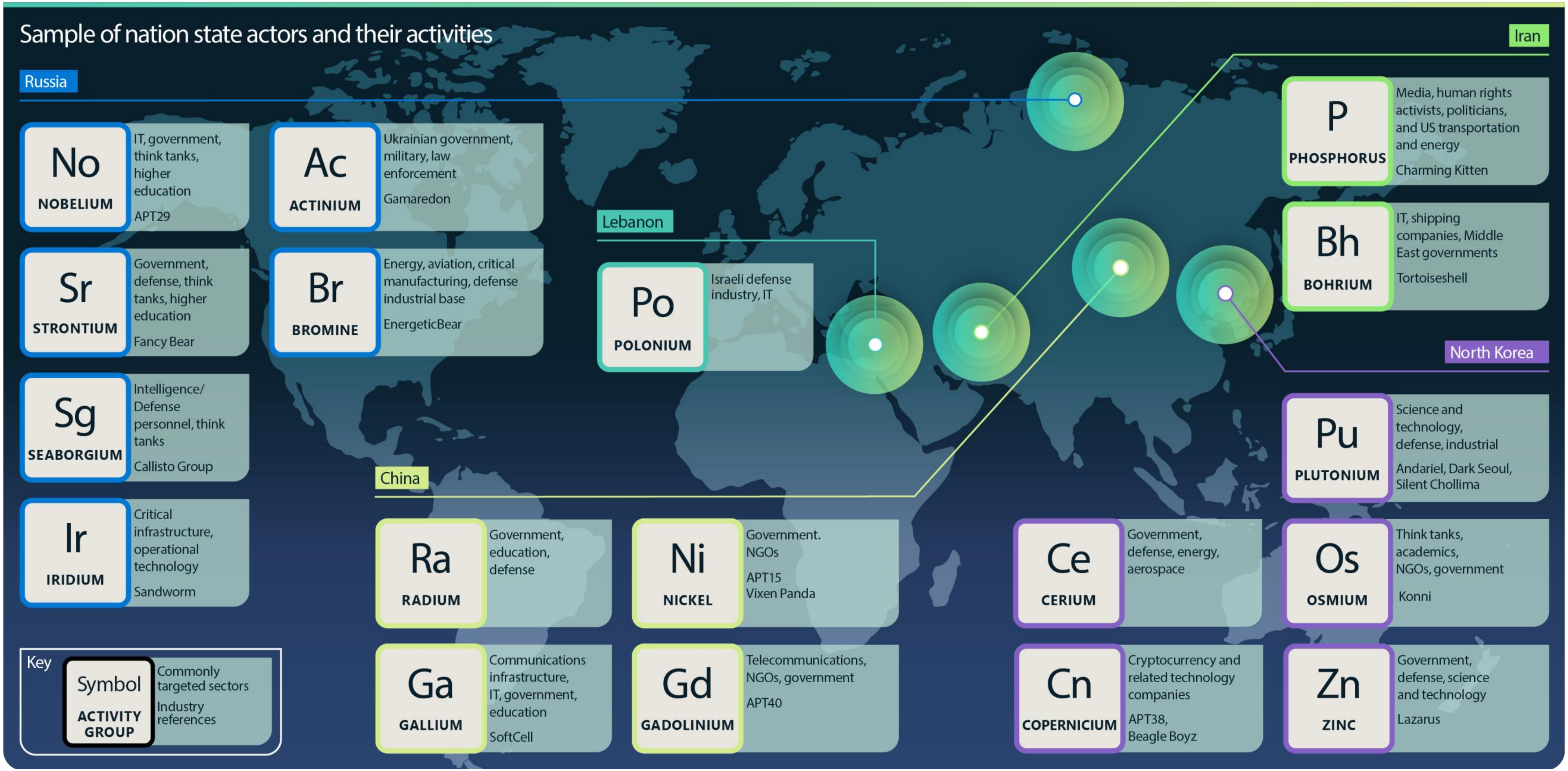
Microsoft

Microsoft Digital Defense Report 2022

Illuminating the threat landscape
and empowering a digital defense.

Aka.ms/MDDR

About our nation state data



Sample of nation state actors and their activities

Russia

No NOBELIUM — IT, government, think tanks, higher education — APT29

Ac ACTINIUM — Ukrainian government, military, law enforcement — Gamaredon

Sr STRONTIUM — Government, defense, think tanks, higher education — Fancy Bear

Br BROMINE — Energy, aviation, critical manufacturing, defense industrial base — EnergeticBear

Sg SEABORGIUM — Intelligence/ Defense personnel, think tanks — Callisto Group

Ir IRIDIUM — Critical infrastructure, operational technology — Sandworm

Lebanon

Po POLONIUM — Israeli defense industry, IT

China

Ra RADIUM — Government, education, defense

Ni NICKEL — Government. NGOs — APT15 Vixen Panda

Ga GALLIUM — Communications infrastructure, IT, government, education — SoftCell

Gd GADOLINIUM — Telecommunications, NGOs, government — APT40

Iran

P PHOSPHORUS — Media, human rights activists, politicians, and US transportation and energy — Charming Kitten

Bh BOHRIUM — IT, shipping companies, Middle East governments — Tortoiseshell

North Korea

Pu PLUTONIUM — Science and technology, defense, industrial — Andariel, Dark Seoul, Silent Chollima

Ce CERIUM — Government, defense, energy, aerospace

Os OSMIUM — Think tanks, academics, NGOs, government — Konni

Cn COPERNICIUM — Cryptocurrency and related technology companies — APT38, Beagle Boyz

Zn ZINC — Government, defense, science and technology — Lazarus

Key

Symbol ACTIVITY GROUP — Commonly targeted sectors — Industry references

Coordinated Russian cyber and military operations in Ukraine

April 19
IRIDIUM launches destructive attack on Lviv-based logistics provider

April 29
IRIDIUM conducts reconnaissance against transportation sector network in Lviv

May 3
Russian missiles strike railway substations, disrupting transport service

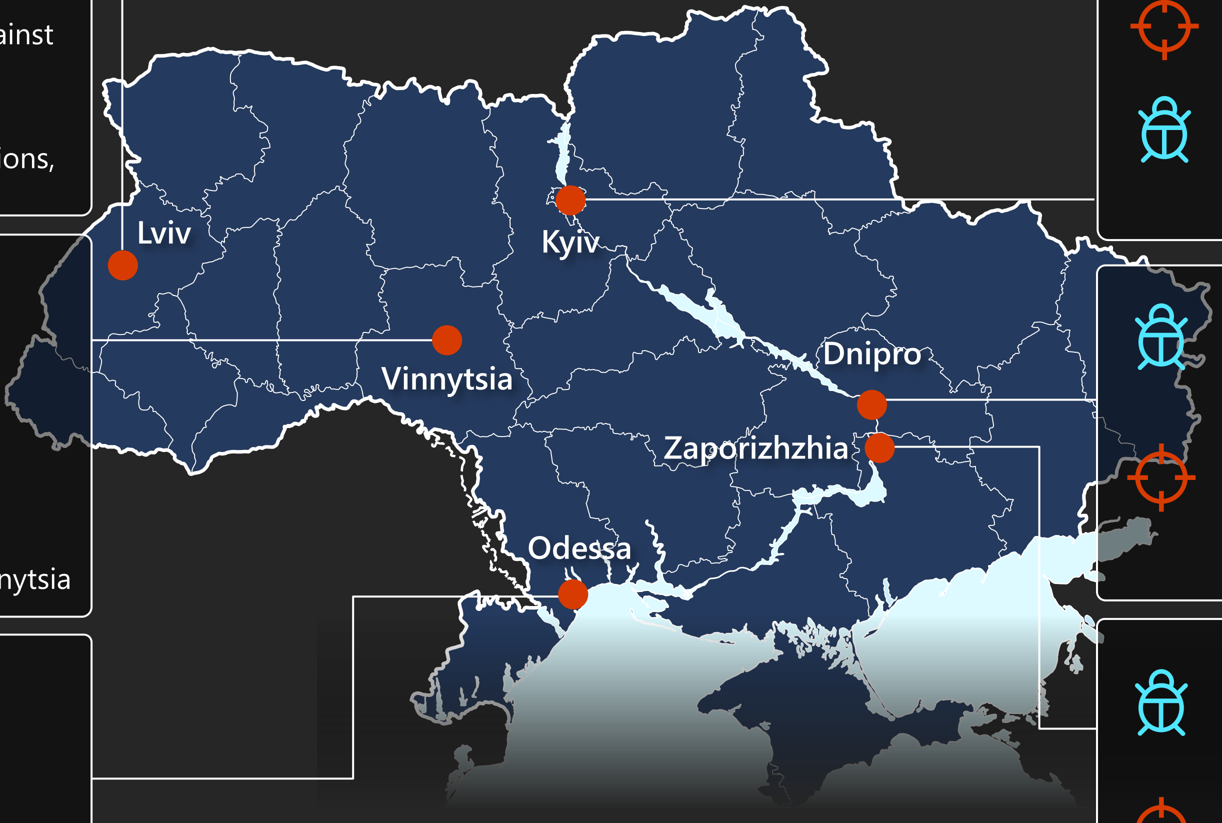
March 4
STRONTIUM targets government network in Vinnytsia

March 6
Russian forces launch eight missiles at Vinnytsia airport[3]

March 16
Russian rockets strike TV tower in Vinnytsia

February 14
Odessa-based critical infrastructure compromised by likely Russian actors

April 3
Russian airstrikes hit fuel depots and processing plants around Odessa



February 28
Threat actor compromises a Kyiv-based media company

March 1
Missile strikes Kyiv TV tower

March 1
Kyiv-based media companies face destructive attacks and data exfiltration

March 11
Dnipro government agency targeted with destructive implant

March 11
First direct Russian strikes hit Dnipro government buildings, among others

March 2
Russian group moves laterally on network of Ukrainian nuclear power company

March 3
Russia's military occupies Ukraine's largest nuclear power station

LEGEND Cyber Kinetic

Microsoft on the front lines

Protecting

860K organizations in 120 countries

Analyzing

65T threat signals every day

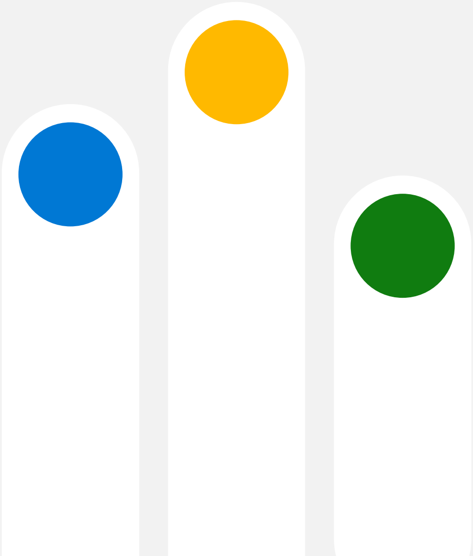
Tracking

250+ unique nation-states, cybercriminals, and other threat actors

Blocked

70B attacks last year

Microsoft Security helps you do more with less



Simplify Vendor Management

Reduce threats with AI and Automation

Improve Operational Efficiency

Infrastructure Security

Network Firewall

Check Point, Cisco, Barracuda, Dell SonicWALL, Juniper, Hewlett Packard Enterprise, Hillstone, Stormshield, McAfee, Fortinet, Sangfor, AhnLab, Bluecat, paloalto, WatchGuard, Huawei, Sophos

Network Monitoring

Blue Coat, Cisco, Ixia, ProtectWise, Netscout, Juniper, DeepNines, solarwinds, Gigamon, Spiceworks, ForeScout, Bradford Networks, EMC RSA, riverbed

Intrusion Prevention Systems

IBM, Cisco, corero, Sophos, Check Point, Hewlett Packard Enterprise, paloalto, Fortinet, DeepNines, Extreme, Huawei, McAfee, FireEye, Juniper, NSFocus, radware, AirTight

Unified Threat Management

Fortinet, Juniper, paloalto, FireEye, Dell, Hillstone, Cisco, Check Point, WatchGuard, Clavister, gateprotect, Sophos, Huawei, endian, Barracuda, Stormshield

Endpoint Security

Endpoint Protection

McAfee, Cylance, Kaspersky, Microsoft, LANDesk, Morphisec, ThreatTrack, PSafe, F-Secure, Barkly, HEATsoftware, eset, invincea, Stormshield, SentinelOne, CrowdStrike, panda, Bromium, Fortinet, Fixme Stick, Bitdefender, AVG, Confer, Trend Micro, Ensilo, Webroot, Malwarebytes, Symantec

Endpoint Detection & Response

red canary, Tanium, Cynet, certego, Outlier, LightCyber, Confer, Triumfant, Cyphort, ZoneFox, morphick, Hexis, CrowdStrike, Bromium, Topspin, CounterTack, Hexadite, QinetiQ, Fluency, 2tex, Guidance, FireEye, ziften, invincea, SentinelOne, EMC RSA, Carbon Black, cybereason, lastline, Digital Guardian, nexthink, Hexis, Endgame

Application Security

WAF & Application Security

Pentasecurity, Qualys, Sucuri, F5, Alert Logic, Shape, Trustwave, Akamai, AIO Networks, waratek, NSFocus, Zenedge, Citrix, ergon, SOHA, denyall, Arxan, Fireblade, netsparker, DBAPPSecurity, Fortinet, Seworks, Barracuda, radware, Positive Technologies, Imperva

Vulnerability Assessment

bugcrowd, WhiteHat Security, Rapid7, Trustwave, Checkmarx, nccgroup, SRC:CLR, McAfee, Flexera, Hewlett Packard Enterprise, Core Security, BeyondTrust, hackerone, IBM, RandomStorm, Veracode, Cigital, snyk, Outpost24, Qualys

Managed Security Service Provider

at&t, Solutionary, verizon, Trustwave, Optiv, Alert Logic, Symantec, Clone Systems, nuspire networks, MegaPath, CenturyLink, IBM, CSC, Dell SecureWorks, Hewlett Packard Enterprise, BT, orange Business Services, Wipro, BAE Systems

Messaging Security

proofpoint, Forcepoint, Microsoft, EdgeWave, FireEye, Cisco, Trustwave, morphick, Symantec, Cloudmark, GWAVA, WatchGuard, BAE Systems, Cyren, Spamina, Fortinet, AstraID, McAfee, appriver, Barracuda, clearswift, Agari, Sophos, Trend Micro, Dell, mimecast

Web Security

Blue Coat, distil networks, Cisco, Sophos, Trustwave, Cloudflare, Shape, zscaler, ZenMate, Fortinet, appriver, F5, ContentKeeper, Check Point, EasySolutions, Barracuda, OpenDNS, FireEye, Cyren, Forcepoint, Webroot, Symantec, Trend Micro, GWAVA, iboss, Bluecat, Venafi, Spamina

IoT Security

Mocana, cryptosoft, Bastille, utimaco, Webroot, endian, Argus, Rubicon, riscure, ZingBox, Arilou, ARM, Cyberbit, SecuriThings, Imubit, Bayshore, Device Authority, Icon Labs, Cloudwear, Infineon, IOActive

Security Operations & Incident Response

SIEM

IBM, LogRhythm, logentries, EventTracker, Alien Vault, EIQ, splunk, Alert Logic, tenable, EMC RSA, Huntsman, sumologic, NetIQ, Skybox, TIBCO, Trustwave, Logscape, Netmonastery, accelops, logz.io, Hewlett Packard Enterprise, CorreLog, Fluency, BlackStratus, logpoint, solarwinds

Security Incident Response

PhantomCyber, Hexadite, Invotas, Skybox, proofpoint, resilient, cybereason, Raytheon Foreground Security, DFLabs, ayehu, Click, Cyber Triage, Rapid7, nuix, Demisto, Guidance, Paladion, Syncurity, experts, Cyberbit, CyberSponse, Hexis, swimlane

Risk & Compliance

Redseal, Firemon, Allgress, Anliance, RSAM, Prevalent, kenna, IBM, MetricStream, RSA Archer, cytegic, bringa, SecurityScorecard, Paladion, BitSight, tufin

Threat Intelligence

BrightPoint Security, DomainTools, ThreatConnect, Anomali, Verisign, Farsight Security, iSight Partners, PhishLabs, ZeroFox, IID, Webroot, SenseCy, Cisco, RiskIQ, ThreatMetrix, Recorded Future, Blueliv, malwarepatrol, OpenDNS, Flashpoint, digital shadows, surveda, SurfWatch, LookingGlass, CrowdStrike, Securonix, Bluecat, proofpoint, ThreatQuotient

Mobile Security

lookout, MobileIron, AppDome, wandera, Mocana, airwatch, nuro, silent circle, InAuth, tigertext, Check Point, Better, LaunchKey, bitglass, SnoopWall, Kaspersky, AVG, TrustLook, IBM, V-Key, Fortinet, Trend Micro, apthority, AirTight, Optiolabs, Koolspan, tascent, Wickr, NowSecure, BlackBerry, pindrop, PSafe, Zimperium, Sophos

Data Security

Hewlett Packard Enterprise, Vormetric, harvest.ai, nuro, Thinair, Vera, Ensilo, Microsoft, Ionic Security, BB Networks, Wickr, Privitar, BlueTalon, globalvelocity, Winmagic, Somansa, CipherCloud, identityfinder, Digital Guardian

Transaction Security

feedzai, Cardinal Commerce, ethoca, Forter, sift science, Early Warning, riskified, ThreatMetrix, NuData Security, Acculynk, iovation, Kount, Brighterion, Socure, Au10tix, IdenTrust, Signifyd, MaxMind, Guardian Analytics

Specialized Threat Analysis & Protection

IronNet Cybersecurity, Fortscale, Bay Dynamics, invincea, Trapx Security, exabeam, LightCyber, Damballa, nyotron, SS8, Invision Mobile System, Avecto, Cymmetria, Area 1, Vectra, Palantir, sqrrl, prelert, niara, deepinstinct, Networks, ProtectWise, fireglass, Seculert, utimaco, Securonix, Spikes, Redowl, Darktrace, Novetta, E8 Security, Endgame, Cylance, Bromium, Datavisor, Menlo Security, Cyphort, Gurucul, Ionic Security, esentire, illusive

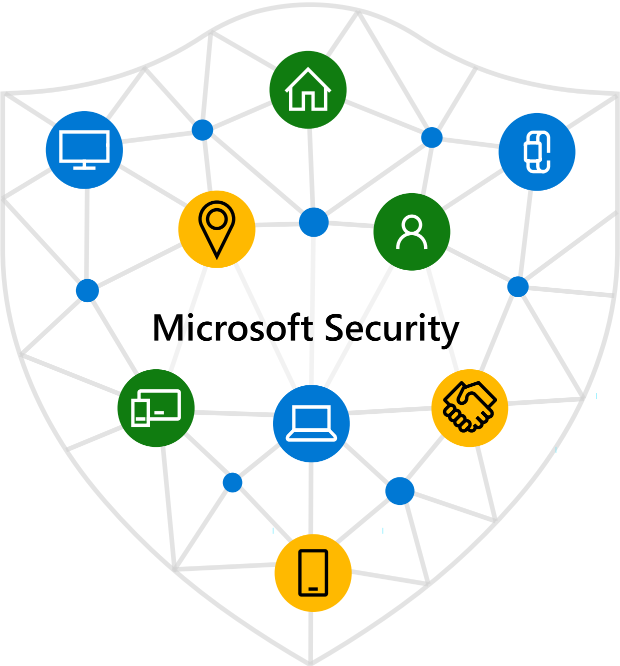
Identity & Access Management

covisint, Clef, Nok Nok Labs, Oracle, PingIdentity, Courion, EMC RSA, Cloudiway, imprivata, Bitium, SaferPass, ForgeRock, ca, Saaspass, okta, WISeKey, SailPoint, Microsoft, onelogin, Trulioo, BeyondTrust, simeio, SecureKey, Auth0, DeepIdentity, IDme, Device Authority, Duo Security, Avecto, Exostar, welcome, verato, tascent, SecureAuth, LaunchKey, ilantus, IBM, Pirean, janrain, gemalto, CyberArk, Centrify, thycotic

Cloud Security

illumio, CloudPassage, bitglass, Bracket, elastica, panda, adallom, AnCrypted Cloud, zscaler, evident.io, ManagedMethods, Code42, WhiteHat, SOHA, Cloudiway, covata, threat stack, Vaultive, harvest.ai, CloudLock, Microsoft, Firelayers, HyTrust, palerra, Fortycloud, Cato Networks, Dome9, guardtime, Twistlock, ClearDATA, Qualys, vArmour, skyhigh, netskope, BetterCloud, boxcryptor, Blue Coat, Vera, CipherCloud

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

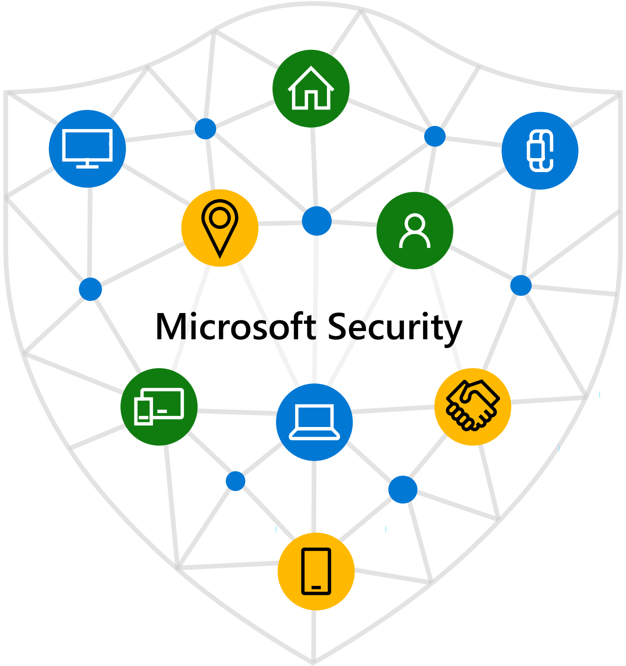
30%

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

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]

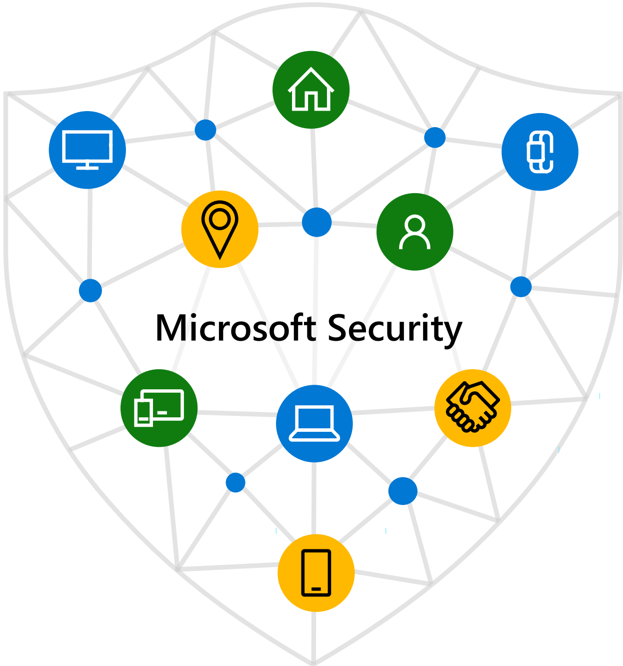
$10.5
million additional end user productivity from automation and process improvements in Microsoft 365 Defender[2]

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

Improve Operational Efficiency



67%

reduced time to deployment with Microsoft Sentinel[1]

73%

improved efficiency of network-related IT work with Azure Network Security[2]

75%

reduction in password requests after introducing Self-service Single-Sign-On (SSO) with Azure Active Directory[3]

$479k

in human capital freed up by redeploying IT time with Microsoft Endpoint Manager[4]

[1] Forrester Consulting, "The Total Economic Impact ™ Of Microsoft Azure Sentinel," November, 2020, commissioned by Microsoft

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

[3] Forrester Consulting, "The Total Economic Impact™ Of Zero Trust Solutions From Microsoft", December 2021, commissioned by Microsoft

[4] Forrester Consulting, "The Total Economic Impact ™ Of Microsoft Endpoint Manager," April 2021, commissioned by Microsoft

A leader in security, compliance, identity, & management

Gartner

A Leader in six

Gartner® Magic
Quadrant™ reports

FORRESTER®

A Leader in eight

Forrester Wave™ categories

IDC

A Leader in seven

IDC MarketScape reports

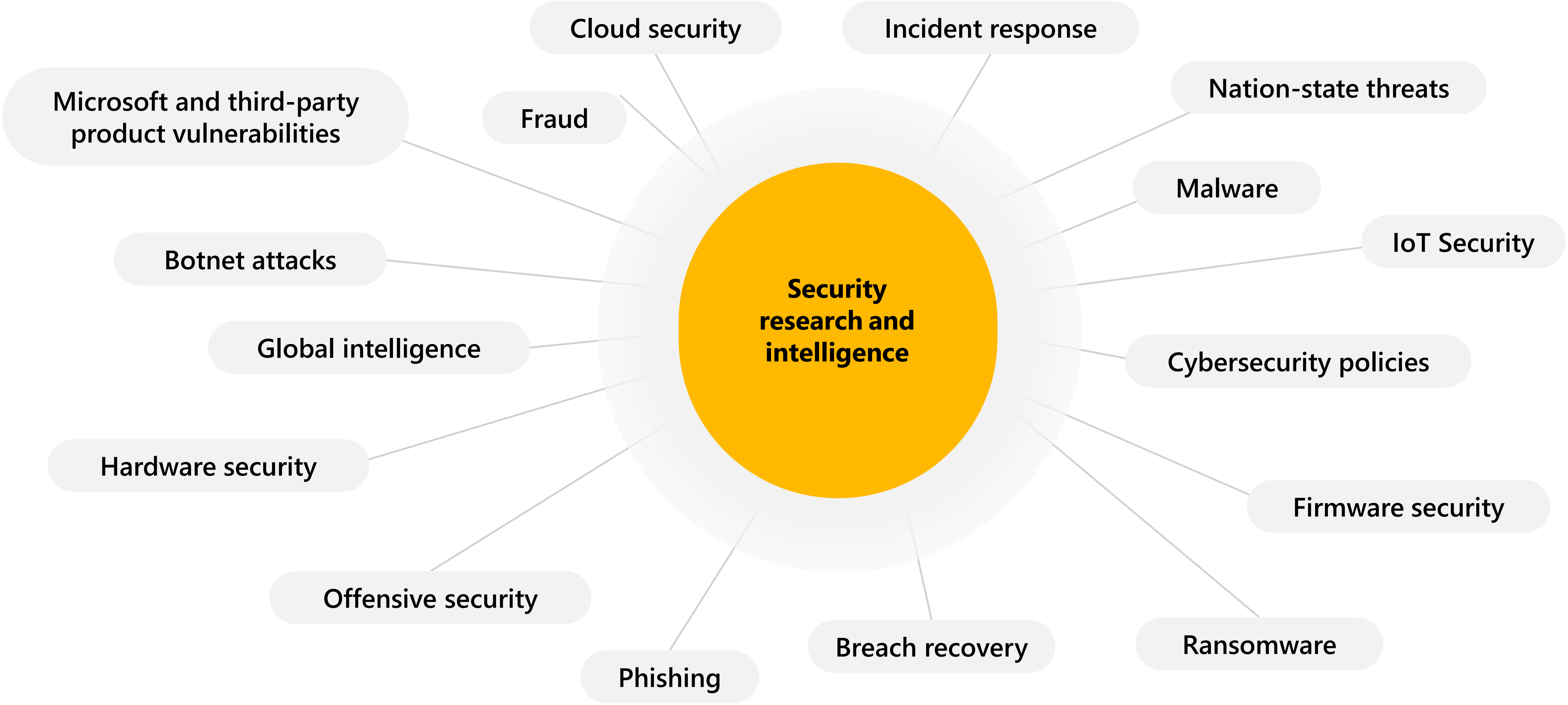
Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The Gartner content described herein (the "Gartner Content") represent(s) research opinion or viewpoints published, as part of a syndicated subscription service, by Gartner, Inc. ("Gartner"), and are not representations of fact. Gartner Content speaks as of its original publication date (and not as of the date of this [type of filing]), and the opinions expressed in the Gartner Content are subject to change without notice. GARTNER and MAGIC QUADRANT are registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment, Doc #US48306021. November 2021
IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment, Doc #48304721. November 2021
IDC MarketScape: Worldwide Advanced Authentication for Identity Security 2021 Vendor Assessment, Doc #US46178720, July 2021
IDC MarketScape: Worldwide eDiscovery Early Case Assessment Software 2022 Vendor Assessment, Doc #US48970222, October 2022

IDC MarketScape: Worldwide Unified Endpoint Management Software 2022 Vendor Assessment
IDC MarketScape: Worldwide Unified Endpoint Management Software for Small and Medium-Sized Businesses 2022 Vendor Assessment
IDC MarketScape: Worldwide Unified Endpoint Management Software for Ruggedized/Internet of Things Deployment 2022 Vendor Assessment

Your enhanced security team



Security research and intelligence

Cloud security

Incident response

Nation-state threats

Microsoft and third-party product vulnerabilities

Fraud

Malware

IoT Security

Botnet attacks

Global intelligence

Cybersecurity policies

Hardware security

Firmware security

Offensive security

Breach recovery

Ransomware

Phishing

Protection aligned to what's ahead

Solutions to support your digital journey

Defend against threats with SIEM plus XDR

Secure multicloud environments

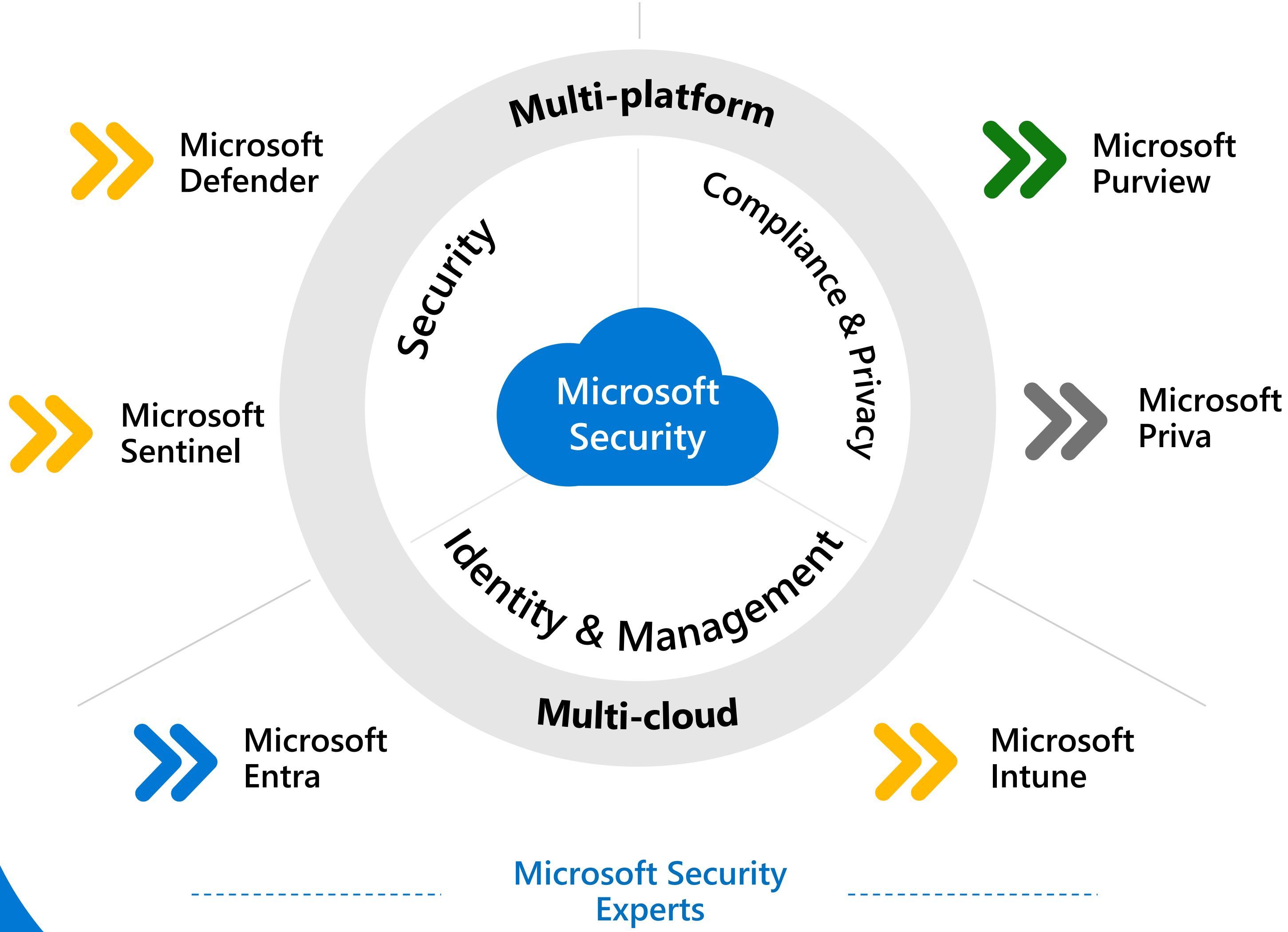
Secure identities and access

Protect and govern sensitive data

Mitigate compliance and privacy risk

Portfolio overview

Six product families integrating over 50 product categories



Microsoft

Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

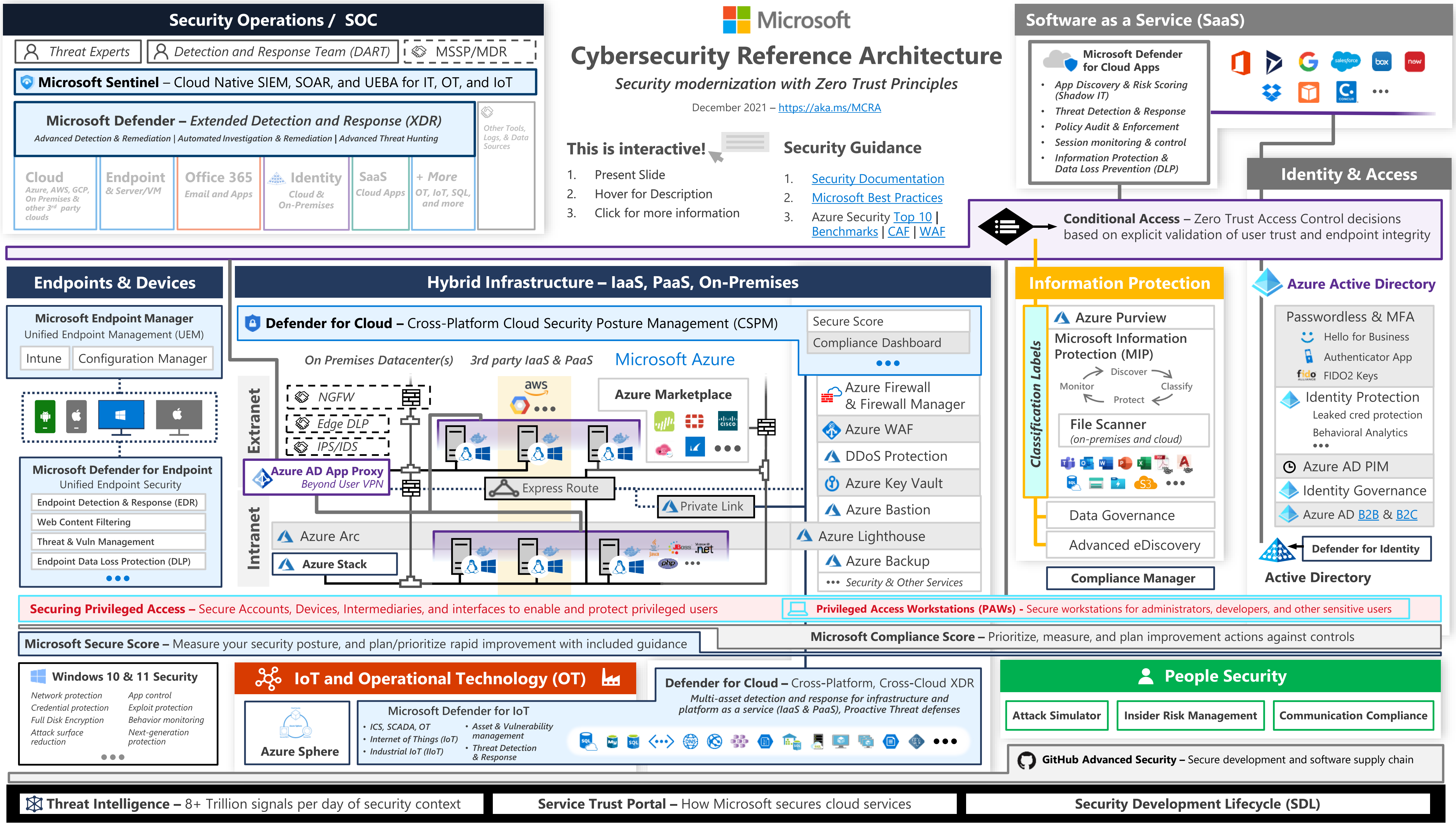
December 2021 – https://aka.ms/MCRA

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF



Security Operations / SOC

Threat Experts | Detection and Response Team (DART) | MSSP/MDR

Microsoft Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Microsoft Defender – *Extended Detection and Response (XDR)*

Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

- Cloud – *Azure, AWS, GCP, On Premises & other 3rd party clouds*
- Endpoint – *& Server/VM*
- Office 365 – *Email and Apps*
- Identity – *Cloud & On-Premises*
- SaaS – *Cloud Apps*
- + More – *OT, IoT, SQL, and more*
- *Other Tools, Logs, & Data Sources*

Software as a Service (SaaS)

Microsoft Defender for Cloud Apps

- *App Discovery & Risk Scoring (Shadow IT)*
- *Threat Detection & Response*
- *Policy Audit & Enforcement*
- *Session monitoring & control*
- *Information Protection & Data Loss Prevention (DLP)*

Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

Microsoft Endpoint Manager

Unified Endpoint Management (UEM)

Intune | Configuration Manager

Microsoft Defender for Endpoint

Unified Endpoint Security

- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)
- •••

Hybrid Infrastructure – IaaS, PaaS, On-Premises

Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)

- Secure Score
- Compliance Dashboard
- •••

On Premises Datacenter(s) | *3rd party IaaS & PaaS* | Microsoft Azure

Extranet: NGFW | Edge DLP | IPS/IDS

Azure AD App Proxy – *Beyond User VPN*

Azure Marketplace

Express Route | Private Link

Intranet: Azure Arc | **Azure Stack**

- Azure Firewall & Firewall Manager
- Azure WAF
- DDoS Protection
- Azure Key Vault
- Azure Bastion
- Azure Lighthouse
- Azure Backup
- ••• *Security & Other Services*

Information Protection

Classification Labels

- Azure Purview
- Microsoft Information Protection (MIP) – Discover, Classify, Protect, Monitor
- File Scanner *(on-premises and cloud)*
- Data Governance
- Advanced eDiscovery

Compliance Manager

Azure Active Directory

- Passwordless & MFA
  - Hello for Business
  - Authenticator App
  - FIDO2 Keys
- Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
  - •••
- Azure AD PIM
- Identity Governance
- Azure AD B2B & B2C

Defender for Identity

Active Directory

Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users

Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls

Windows 10 & 11 Security

Network protection	*App control*
Credential protection	*Exploit protection*
Full Disk Encryption	*Behavior monitoring*
Attack surface reduction	*Next-generation protection*

•••

IoT and Operational Technology (OT)

Azure Sphere

Microsoft Defender for IoT

- *ICS, SCADA, OT*
- *Internet of Things (IoT)*
- *Industrial IoT (IIoT)*
- *Asset & Vulnerability management*
- *Threat Detection & Response*

Defender for Cloud – Cross-Platform, Cross-Cloud XDR

Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

GitHub Advanced Security – Secure development and software supply chain

Threat Intelligence – 8+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Control at scale

Security

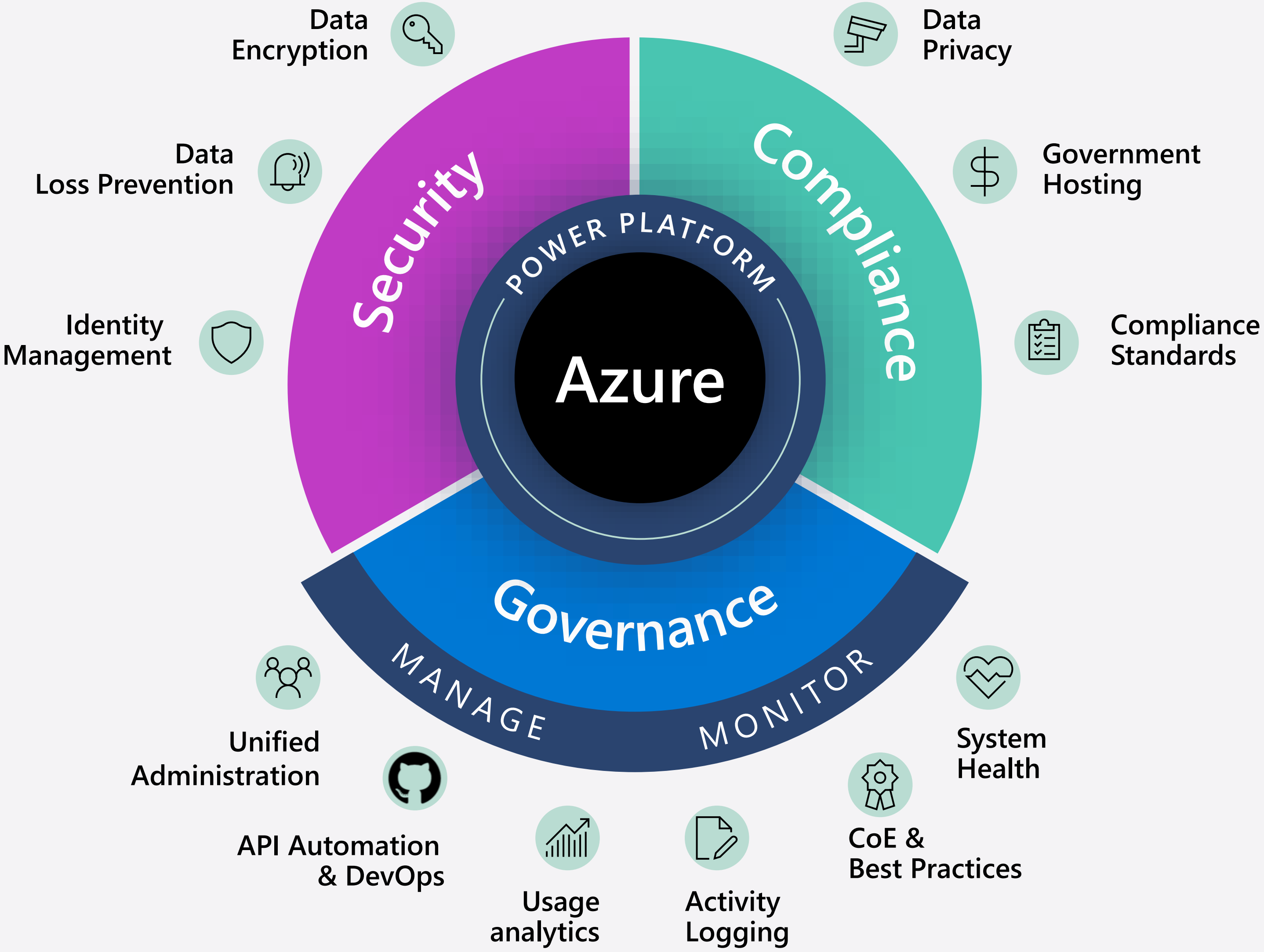
20B+ USD investment in security R&D and 3,500 cyber security experts

Compliance

Hosted in Azure and globally available with 90+ compliance offerings including CIS Benchmark, CSA STAR Self-Assessment, SOC 1 Type 2.

Governance

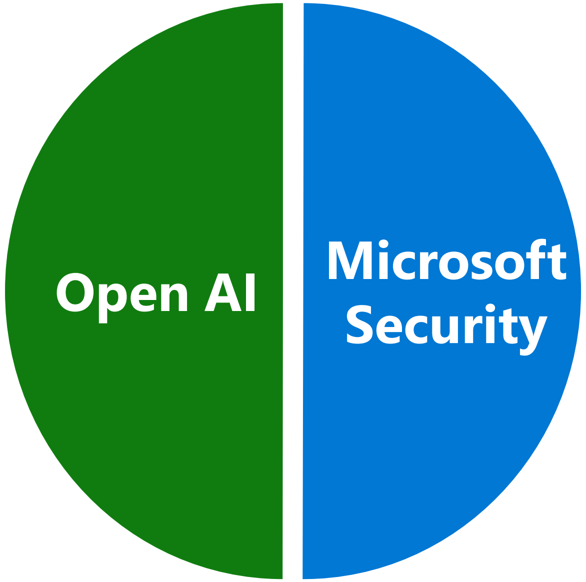
Enterprise scale governance capabilities native part of the platform



Microsoft Security

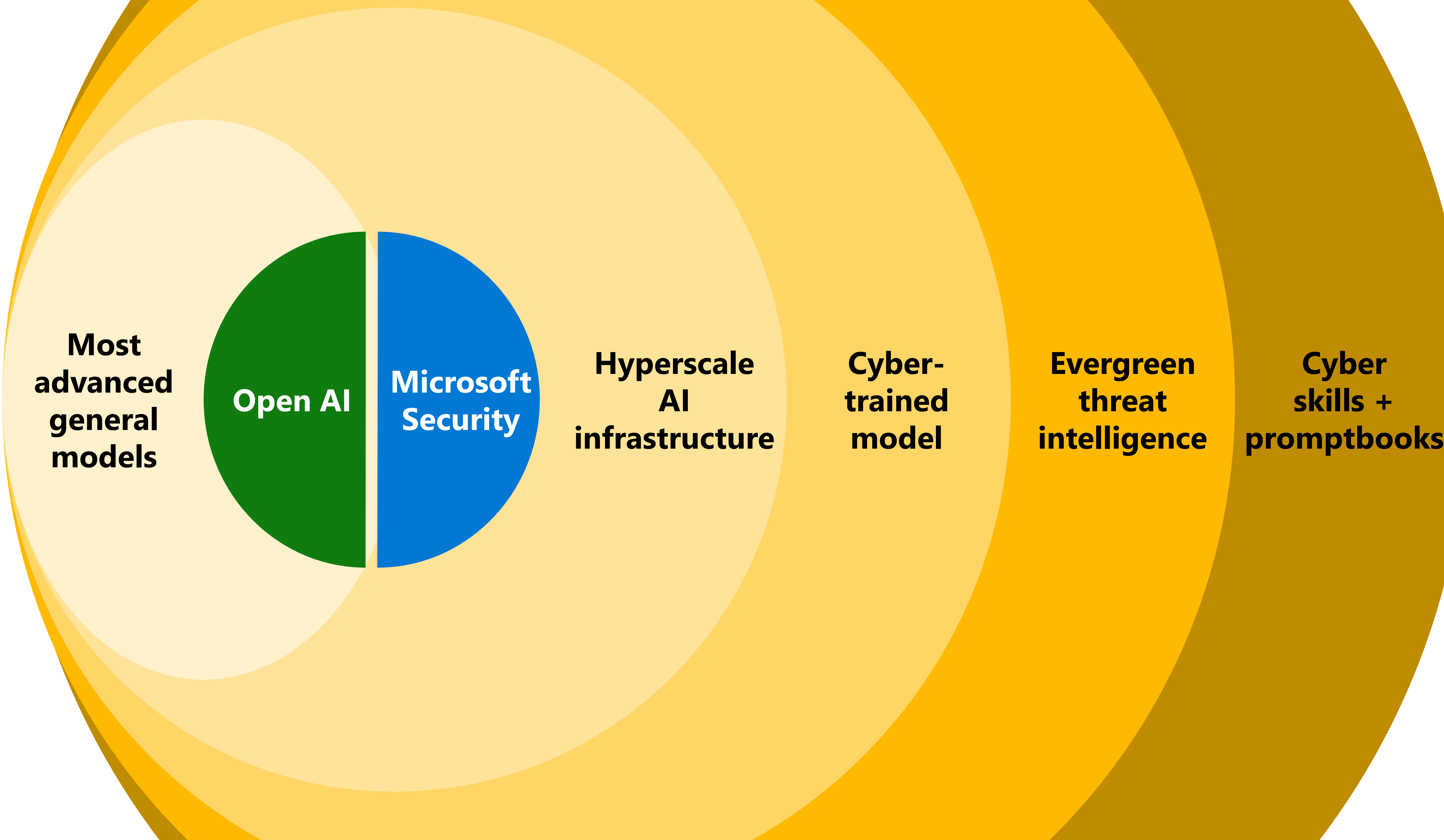
Microsoft Security Copilot

Briefing



Open AI

Microsoft Security



Most advanced general models

Open AI

Microsoft Security

Hyperscale AI infrastructure

Cyber-trained model

Evergreen threat intelligence

Cyber skills + promptbooks

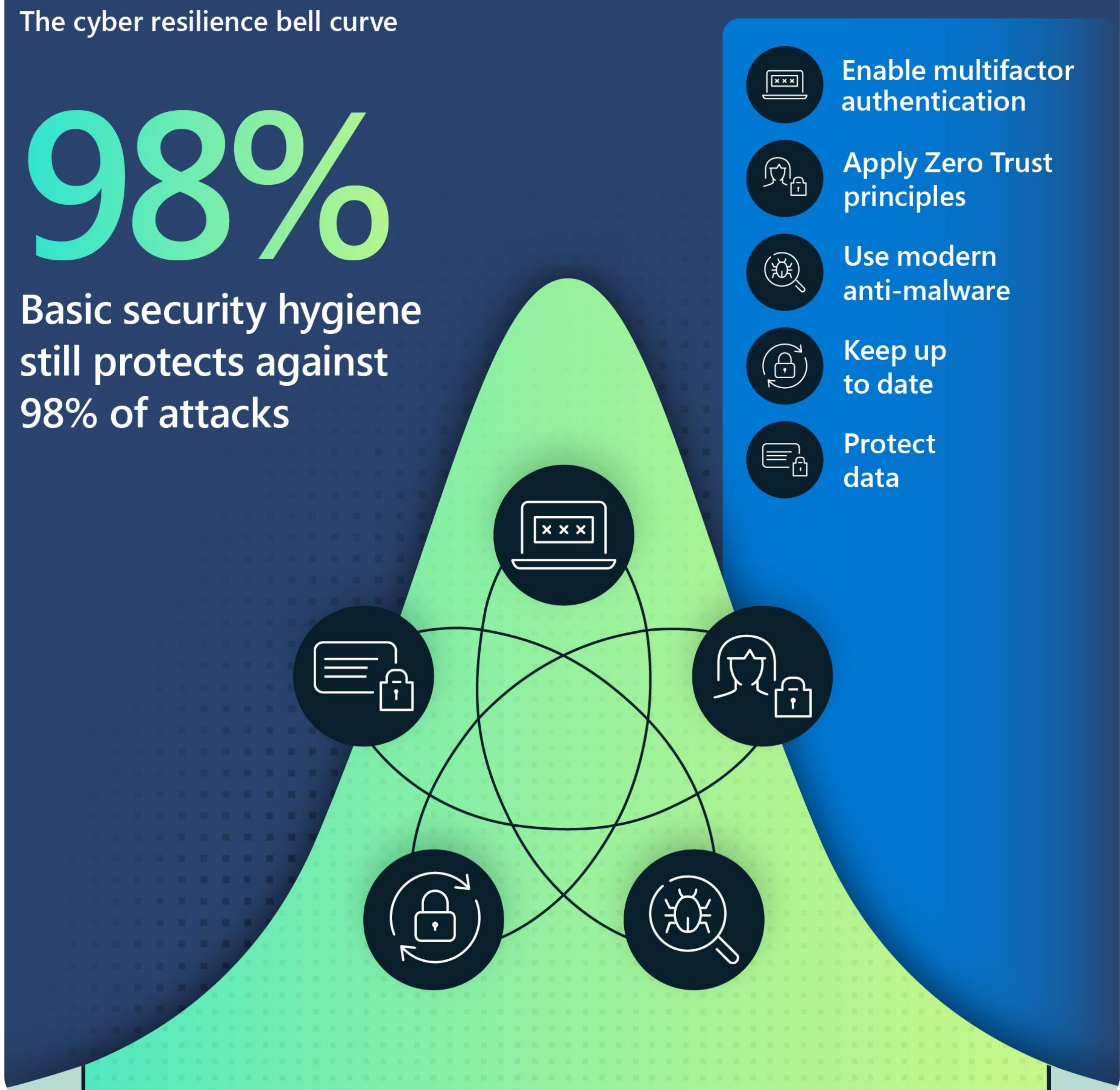
Microsoft

Announcing

Microsoft Security Copilot

Calls to action for cyber resilience

Resilience success factors every organization should adopt



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

More information

Microsoft | Microsoft Sikkerhet

Start kostnadsfri prøveversjon

Sikkerhet for små eller mellomstore bedrifter

Arbeid sikkert fra hvor som helst med enkle, kostnadseffektive og brukervennlige løsninger, spesielt utviklet for virksomheter med opptil 300 ansatte.

Vis abonnementer og priser

Sikkerhet er vitalt for bedriften din

Bedrifter opplever en økning i både volum og sofistikering av nettangrep. Med rask teknologiadopsjon og økt hybridarbeid er risikoen større for små og mellomstore kunder som sliter med budsjettbegrensninger og null i spesialiserte sikkerhetskunnskaper. Microsofts omfattende løsninger motarbeider disse truslene som er under stadig utvikling.

300 %

Økning i angrep med løsepengevirus

Løsepengevirus er en vanlig trussel for små bedrifter og utgjør halvparten til tre fjerdedeler av ofrene. Angrep med løsepengevirus har økt med nesten 300 % det siste året.[1]

23 %

Opplevde et sikkerhetsbrudd

23 prosent av små og mellomstore kunder sier at de hadde et sikkerhetsbrudd det siste året.[2] Forbli på nettet ved å ta i bruk omfattende sikkerhet med automatisering for raskt å oppdage og svare på trusler.

108 000 USD

Gjennomsnittlige kostnader for virksomheter

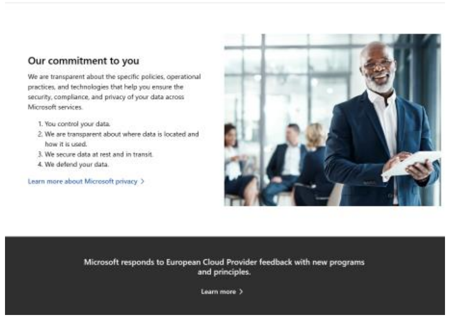
Det er anslått at gjennomsnittskostnaden for et databrudd for en bedrift er USD 108 000.[3] Du trenger ikke å inngå kompromisser bare fordi du er en liten bedrift – sikkerhet som holder deg produktiv er en kritisk investering.

aka.ms/security

Introducing Microsoft Security Copilot: Empowering defenders at the speed of AI

Mar 28, 2023 | Vasu Jakkal, Corporate Vice President, Security, Compliance, Identity, and Management

Security Copilot blogg
aka.ms/securitycopilo
Watch the Secure event keynote



Our commitment to you

We are transparent about the specific policies, operational practices, and technologies that help you ensure the security, compliance, and privacy of your data across Microsoft services.

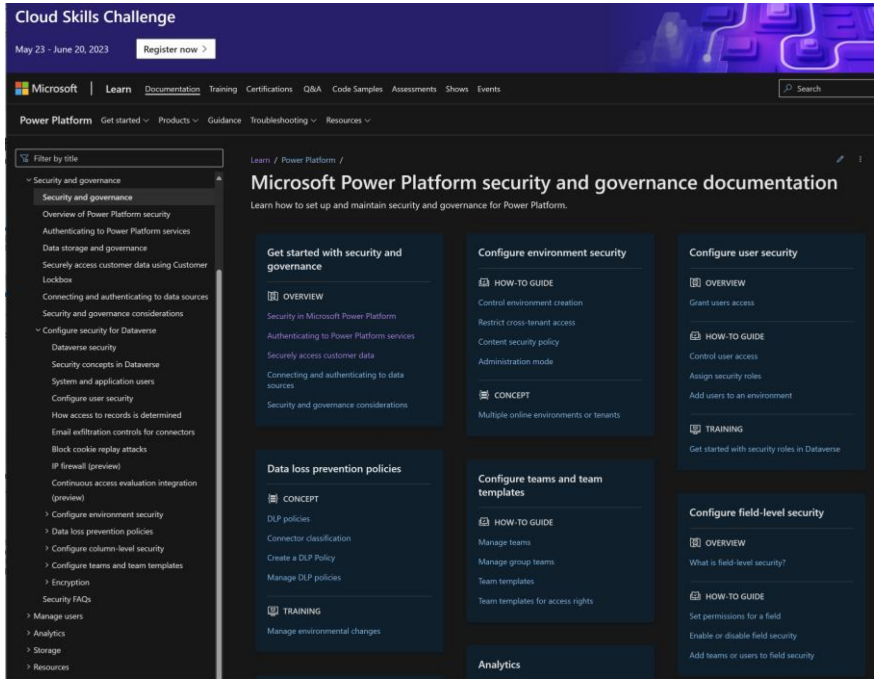
1. You control your data.
2. We are transparent about where data is located and how it is used.
3. We secure data at rest and in transit.
4. We defend your data.

Learn more about Microsoft privacy >

Microsoft responds to European Cloud Provider feedback with new programs and principles.

Learn more >

aka.ms/trustcenter



Cloud Skills Challenge

May 23 - June 20, 2023

Register now >

- Security and governance
  - Security and governance
  - Overview of Power Platform security
  - Authenticating to Power Platform services
  - Data storage and governance
  - Securely access customer data using Customer Lockbox
  - Connecting and authenticating to data sources
  - Security and governance considerations
  - Configure security for Dataverse
    - Dataverse security
    - Security concepts in Dataverse
    - System and application users
    - Configure user security
    - How access to records is determined
    - Email exfiltration controls for connectors
    - Block cookie replay attacks
    - IP firewall (preview)
    - Continuous access evaluation integration (preview)
    - Configure environment security
    - Data loss prevention policies
    - Configure column-level security
    - Configure teams and team templates
    - Encryption
  - Security FAQs
- Manage users
- Analytics
- Storage
- Resources

Learn / Power Platform /

Microsoft Power Platform security and governance documentation

Learn how to set up and maintain security and governance for Power Platform.

Get started with security and governance

OVERVIEW
Security in Microsoft Power Platform
Authenticating to Power Platform services
Securely access customer data
Connecting and authenticating to data sources
Security and governance considerations

Configure environment security

HOW-TO GUIDE
Control environment creation
Restrict cross-tenant access
Content security policy
Administration mode

CONCEPT
Multiple online environments or tenants

Configure user security

OVERVIEW
Grant users access

HOW-TO GUIDE
Control user access
Assign security roles
Add users to an environment

TRAINING
Get started with security roles in Dataverse

Data loss prevention policies

CONCEPT
DLP policies
Connector classification
Create a DLP Policy
Manage DLP policies

TRAINING
Manage environmental changes

Configure teams and team templates

HOW-TO GUIDE
Manage teams
Manage group teams
Team templates
Team templates for access rights

Analytics

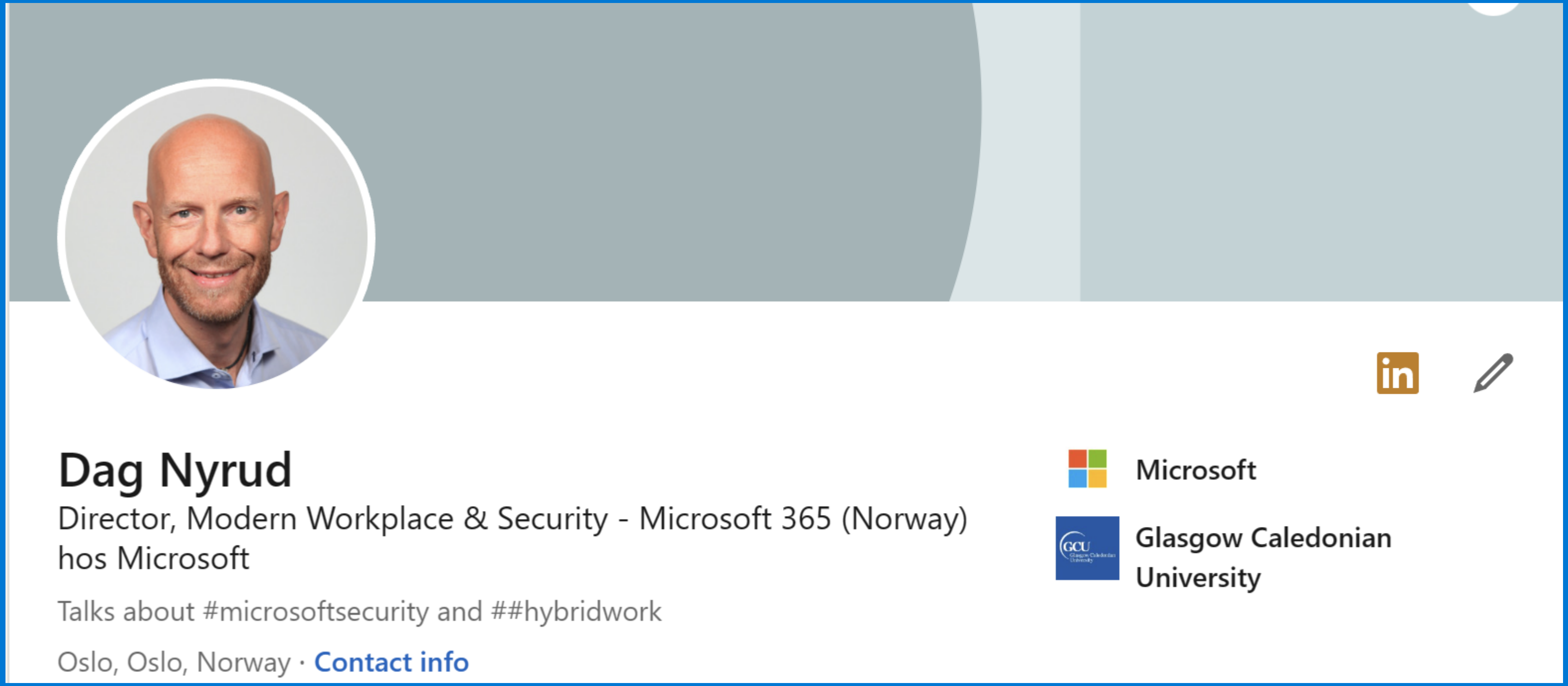
Configure field-level security

OVERVIEW
What is field-level security?

HOW-TO GUIDE
Set permissions for a field
Enable or disable field security
Add teams or users to field security

learn.microsoft.com
or
https://learn.microsoft.com/en-us/power-platform/admin/security

Tusen takk!



Dag Nyrud

Director, Modern Workplace & Security - Microsoft 365 (Norway) hos Microsoft

Talks about #microsoftsecurity and ##hybridwork

Oslo, Oslo, Norway · Contact info

Microsoft

Glasgow Caledonian University

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