

# Microsoft Security

**Abbas Kudrati**

APAC Lead Chief Cybersecurity Advisor

[Abbas.Kudrati@Microsoft.Com](mailto:Abbas.Kudrati@Microsoft.Com)

<https://aka.ms/abbas>

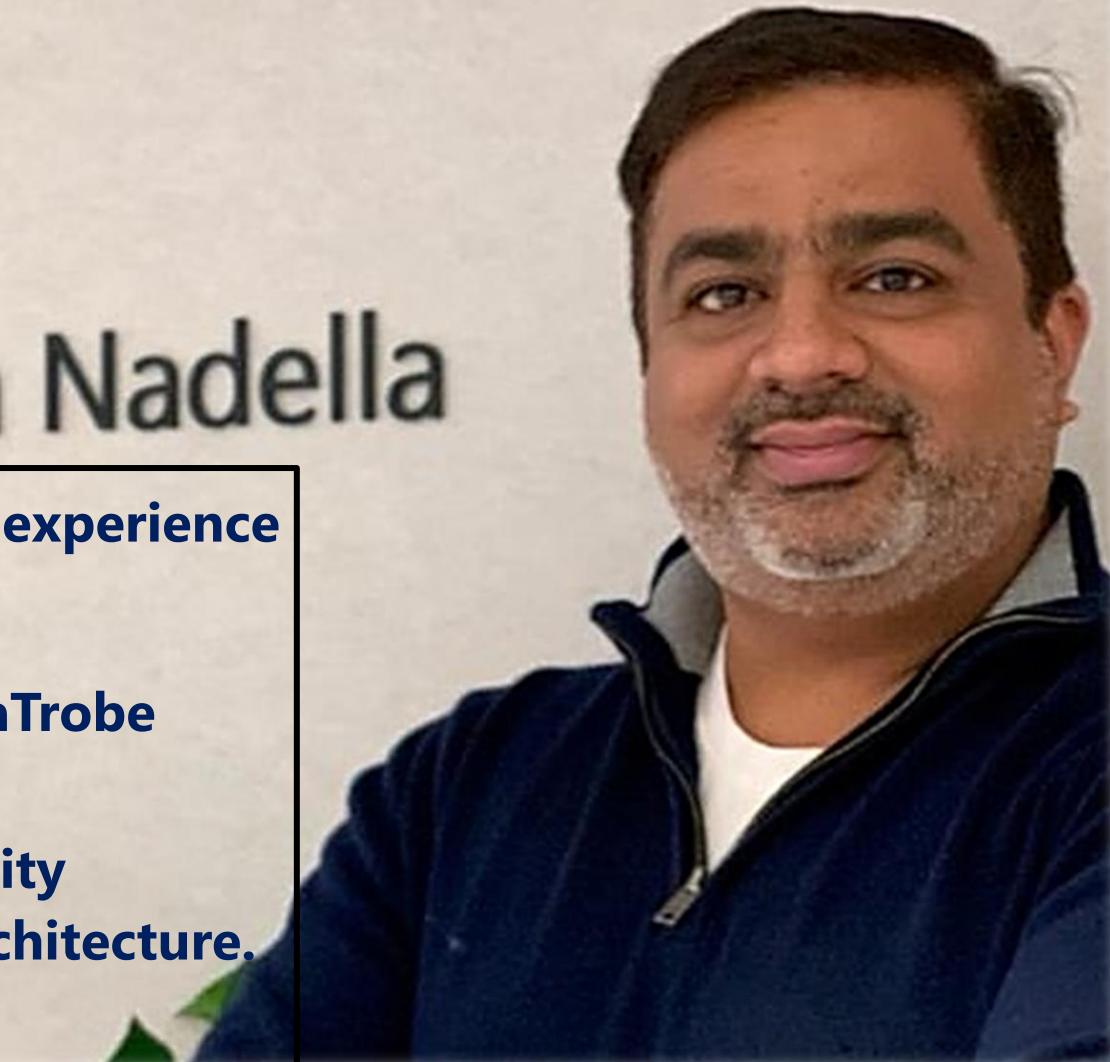


# About me

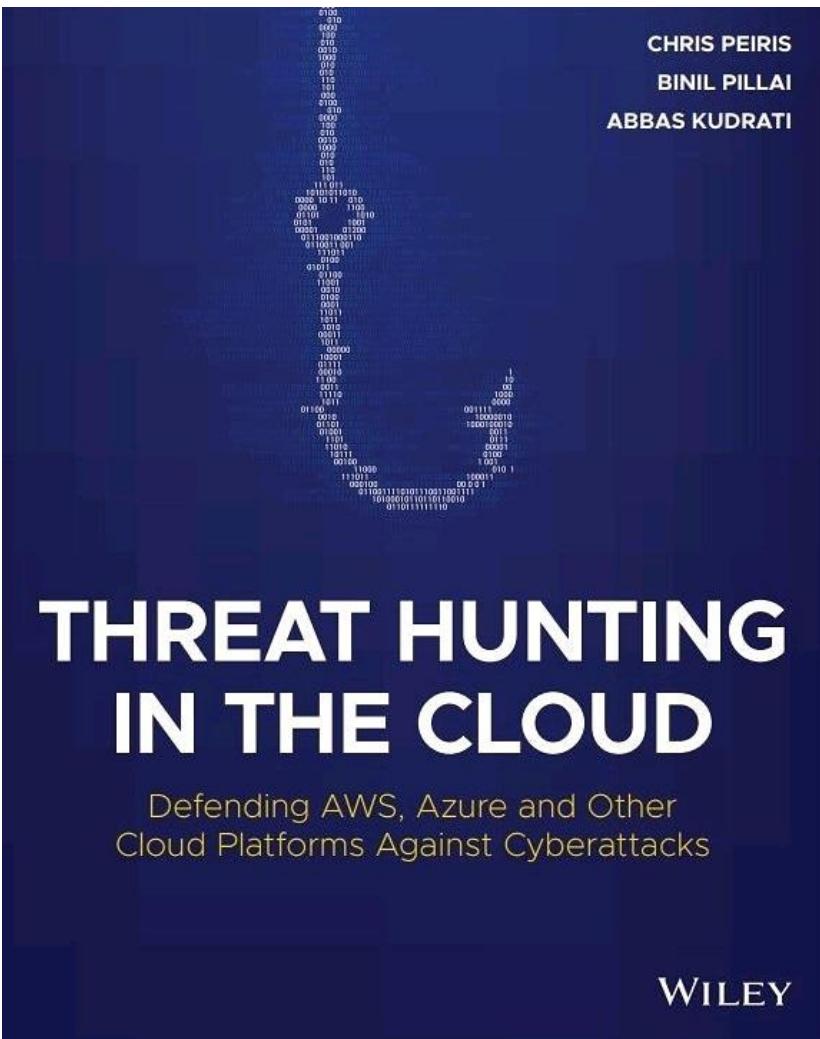
"You join Microsoft, not to be cool  
but to make others cool"

Satya Nadella

- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**



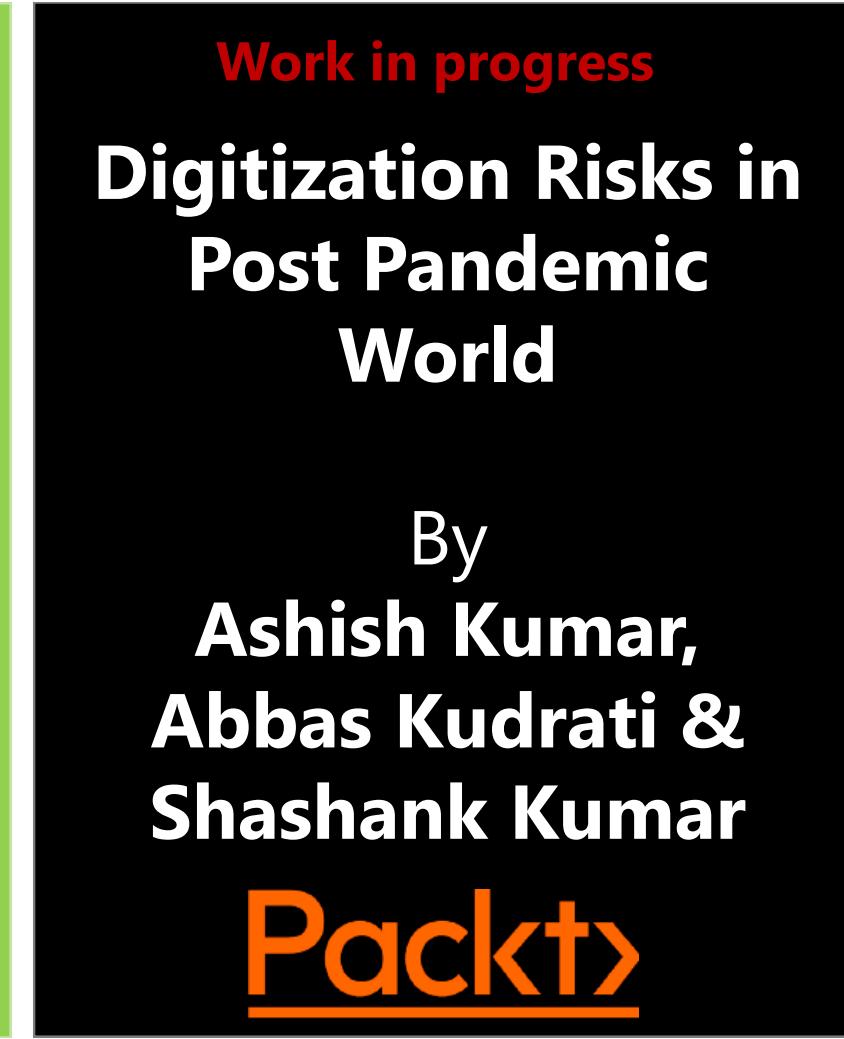
# My publications



Available now on [Amazon](#).



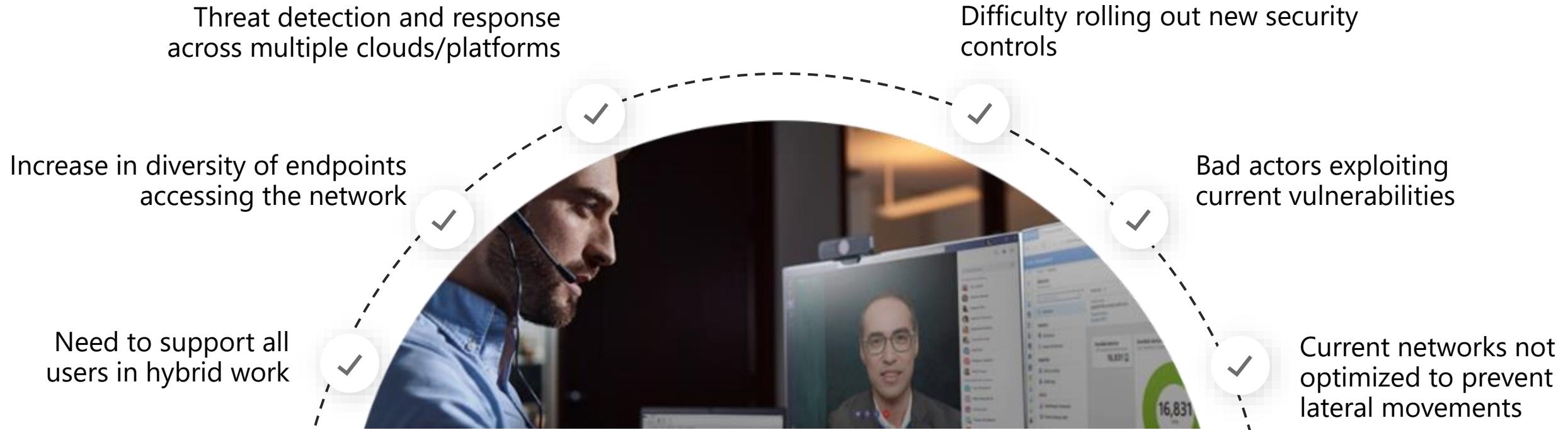
Target release by May 2022.



Target release by March 2022.

# Our new reality intensifies security challenges

How do we drive operational resiliency while strengthening cybersecurity?

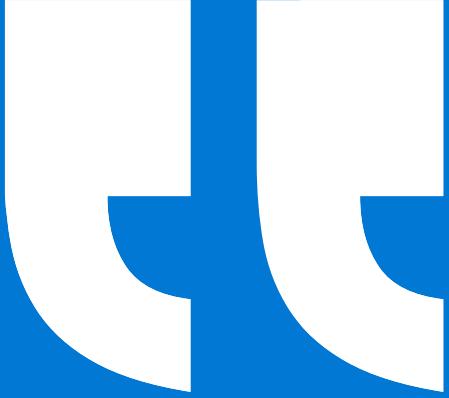


***"Security is our top priority and we are committed to working with others across the industry to protect our customers."***

**Satya Nadella**  
*Chief Executive Officer, Microsoft Corporation*

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships





To empower every person and every organization on the planet to achieve more

Microsoft's Mission



**To empower every person and every organization on the planet to achieve more**

Microsoft's Mission

**To keep customer safe and secure - and they can trust their digital fabric they build upon – hybrid and multi-cloud.**

Microsoft Security



# Microsoft Are Transforming Cybersecurity

[Joseph Blankenship](#), VP, Research Director  
[Jeff Pollard](#), VP, Principal Analyst



Qualys. All from a single a



## Make No Mistake — Microsoft Is A Security Company Now

[Josh Zelonis](#), Principal Analyst MAR 22 2019

[Microsoft has announced support for macOS](#) in its rebranded Microsoft Defender ATP product, taking this product from being an offering that could be considered an add-on for hardening its own operating system to a multipurpose security solution. While this is an early release, it is a clear signal of the investment Microsoft is making to be a security company and should not be ignored.

**What Is The Efficacy Of The Microsoft Defender ATP Product?**

[Home](#) » [Cybersecurity](#) » [Analytics & Intelligence](#) » [Make No Mistake — Microsoft Is A Security Company Now](#)



**Make No Mistake — Microsoft Is A Security Company Now**

by Roger Halbeer on March 26, 2019

That's not a bad start of the day, reading such a headline from a Forrester analyst. I am often asked, how far we are going to drive security within Microsoft. Well, I guess here you have an answer from an outsider:

[Make No Mistake — Microsoft Is A Security Company Now](#). Even though the author mainly focuses on Windows Defender, Windows Defender ATP and the Mac integration, it is still a strong statement:



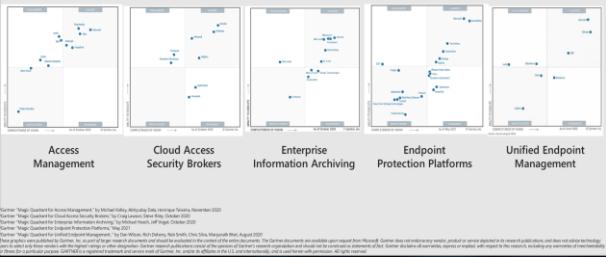
Microsoft has the ability to hire and retain the best talent out there, and this announcement certainly demonstrates that it is making the necessary investments to be a multipurpose security vendor. The endpoint security industry has been put on notice: Microsoft is a security company now, and it's coming for your business.

But that's not the only one. There was another Forrester article

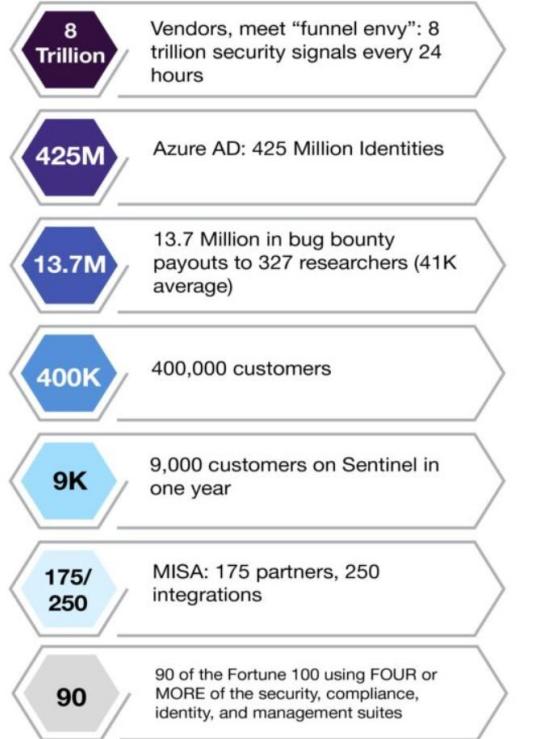
[Tech Titans Alphabet And Microsoft Are Transforming Cybersecurity](#) pointing in a similar direction. Even if I disagree that what we have seen from Google in the security analytics space at RSA can be compared with [Azure Sentinel](#), both companies definitely have the ability to significantly change the security world. One big challenge we often face is, that security professionals are still very reluctant to bring their information (mainly the logs) to the cloud. I would just give you two quotes from the blog post I just mentioned:

Gartner®

Microsoft—a Leader in 5 Gartner Magic Quadrant reports



## Microsoft Security Highlights 2020



# Gartner®

“Microsoft is now a security vendor”



# Deutsche Bank

“Largest Security Vendor in the world”

# FORRESTER®

“Microsoft Is Now A Cybersecurity Behemoth”

“Multi-cloud, multi-platform and the world’s largest cybersecurity company by revenue, Microsoft can boast that over the past four quarters it has done nearly as much cybersecurity revenue as McAfee, Symantec , and Palo Alto Networks — combined.”

Daniel Newman, Futurum Research

# Scale and Protection of Microsoft Security

Over 24 trillion daily security signals

AI powered detections and automated actions

8,500+ security engineers & researchers

**9B**

Endpoint threats  
blocked

**31B**

Identity threats  
blocked

**32B**

Email threats  
blocked

Protecting

**715K**

organizations  
in 120 countries

July 1, 2020, through June 30, 2021

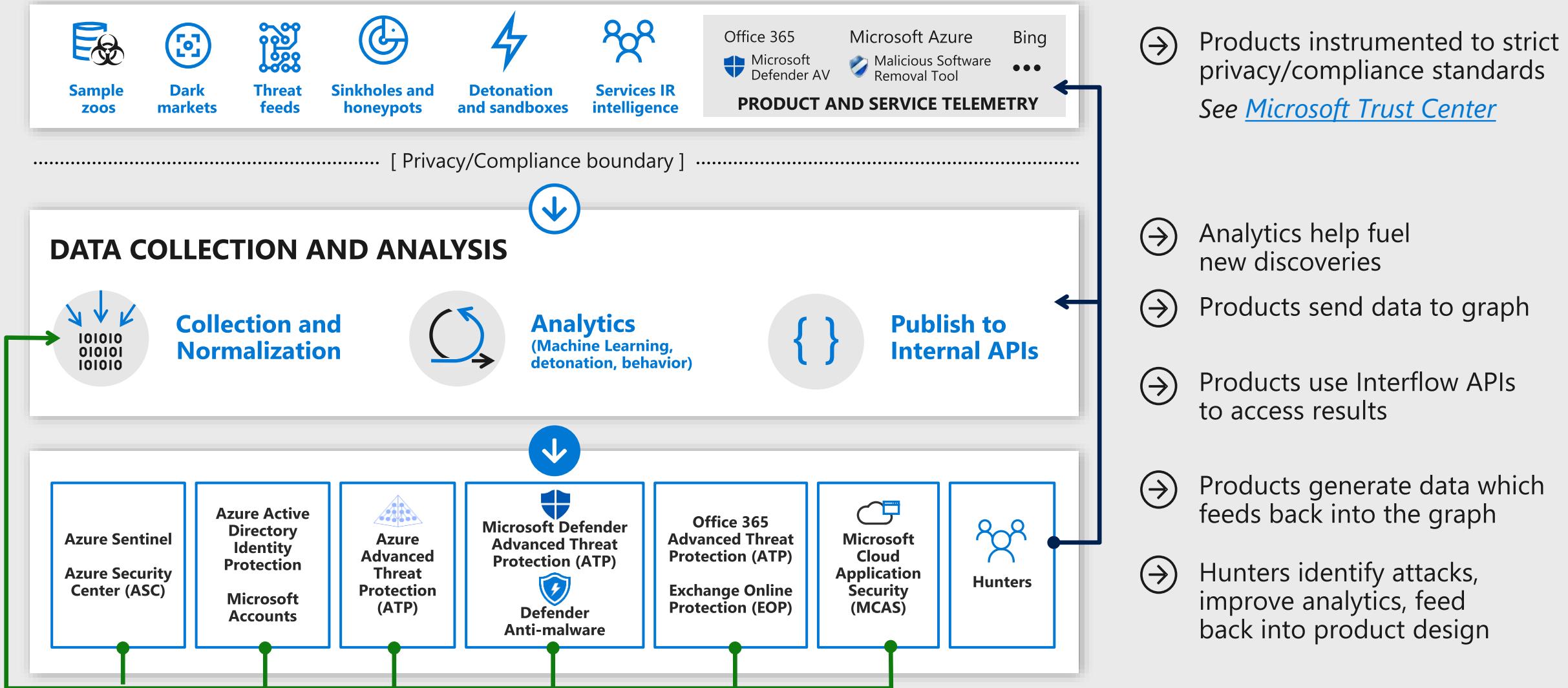
Source: [Microsoft Digital Defense Report](#)

# THE MICROSOFT CYBER DEFENSE OPERATIONS CENTER



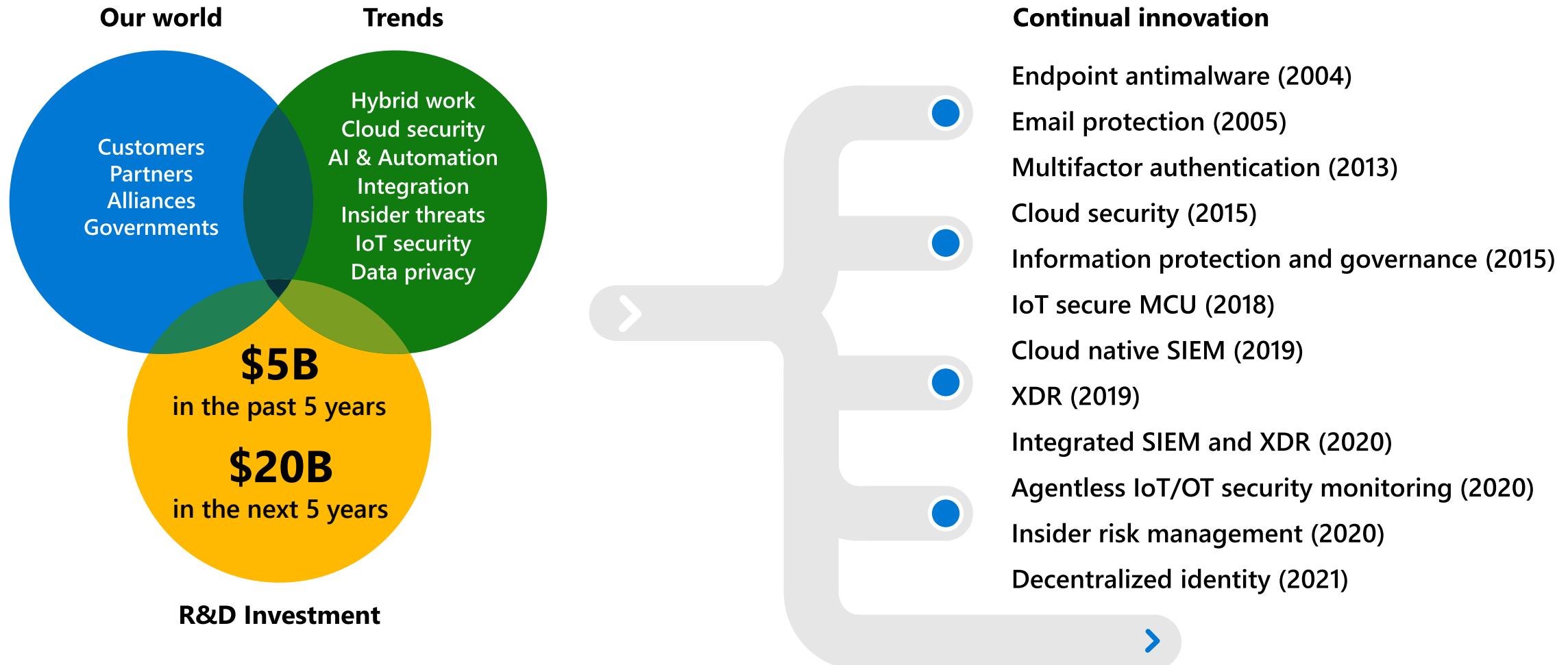
- Protect Microsoft cloud infrastructure and services 24 x 7 x 365
- Unite personnel, technology, and analytics in a central hub
- Provide world-class security monitoring, defense, and response
- More than 150 Security Experts and Data Scientists
- Connected to 8,500+ Security Professionals across Microsoft
- Tight partnerships with Microsoft Research and the Security Development Lifecycle (SDL) team

# Inside View of Microsoft Threat Intelligence



# We're investing where security is going

To help you keep pace with change



# Empower your security teams to protect employees and resources

How CISOs are navigating the challenges of COVID-19

82%

feel pressured to lower costs.

67%

identified pandemic-themed phishing attacks.

#1

priority to reduce cost is improved threat protection.



## More Than 70% of SOC Analysts Experiencing Burnout

Nearly 65% of security operations center (SOC) analysts are likely to change jobs in the next year, survey shows.



Dark Reading Staff

Dark Reading

March 05, 2022

**Stress and frustration continue to plague the security operations center (SOC):**

**nearly 70% report understaffed teams, and 60% say their workloads have spiked over the past year.**

**Some 64% of SOC analysts say manual work eats up more than half of their time, and reporting and monitoring are their least favorite parts of the job.**

**More than 65% say half of their security tasks could be automated, leaving them time to do deeper security work.**

**And 64% are considering leaving the organization for a new position somewhere else.**

# Gartner Cybersecurity Prediction 2021-2022

1. By the end of 2023, modern privacy laws will cover the personal information of 75% of the world's population – strong need to automate Privacy Mgt
2. By 2024, 30% of enterprises will adopt cloud-delivered Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) and Firewall As A Service (FWaaS) capabilities **from the same vendor.** – tools consolidation
3. By 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements. – Cyber readiness becoming a KPI

[The Top 8 Cybersecurity Predictions for 2021-2022 \(gartner.com\)](#)

[Gartner Top Security and Risk Trends for 2021](#)

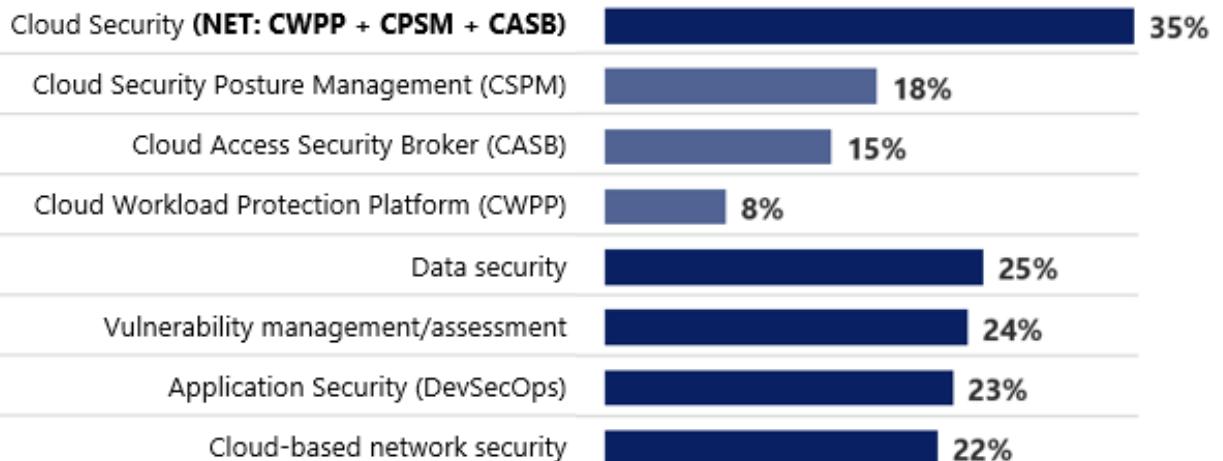
## Top Security and Risk Trends for 2021

01	Cybersecurity mesh		02	Cyber-savvy boards	
03	Vendor consolidation		04	Identity-first security	
05	Managing machine identities becoming a critical security capability				
06	“Remote work” now just “work”		07	Breach and attack simulation	
08	Privacy-enhancing computation techniques				

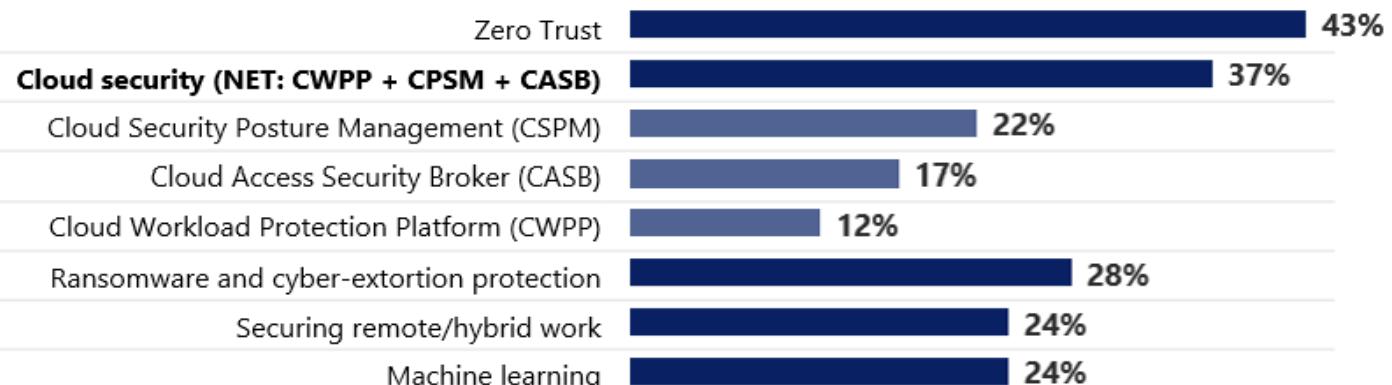
## Top 5 cybersecurity challenges



## Most Interested in Investing in Next 12 Months

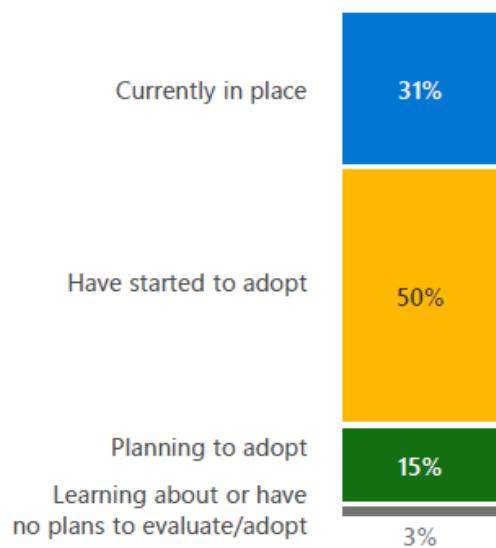


## Security Topics of Interest



[How CISOs are preparing to tackle 2022 - Microsoft Security Blog](#)

### EXHIBIT 3. HYBRID WORKPLACE INTENT



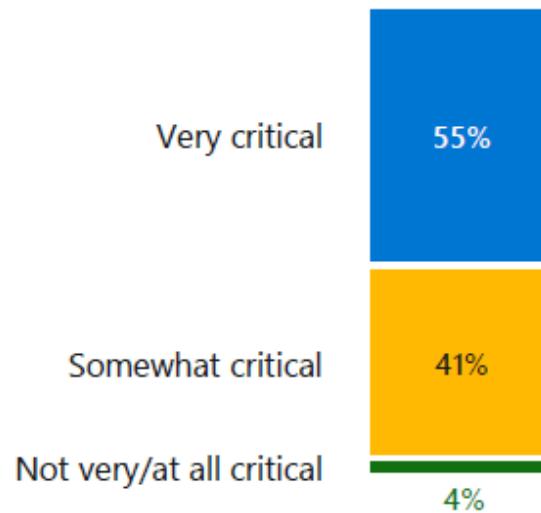
### EXHIBIT 4. HYBRID WORKPLACE CONCERN

Employees downloading unsafe apps	37%
An increase to IT workload	37%
Ransomware attacks	36%
Phishing attacks	35%
Improper use of personal devices	34%
Unauthorized access to data	31%
Inability to manage all devices	30%
Use of personal email accounts	30%
Non-compliance with data regulations	24%

# Zero Trust Adaption report 2020 /21

### EXHIBIT 1. ZERO TRUST IS CRITICAL

Very + Somewhat ▶ 96%



### EXHIBIT 2. ZERO TRUST MOTIVATORS

#### Top Motivators

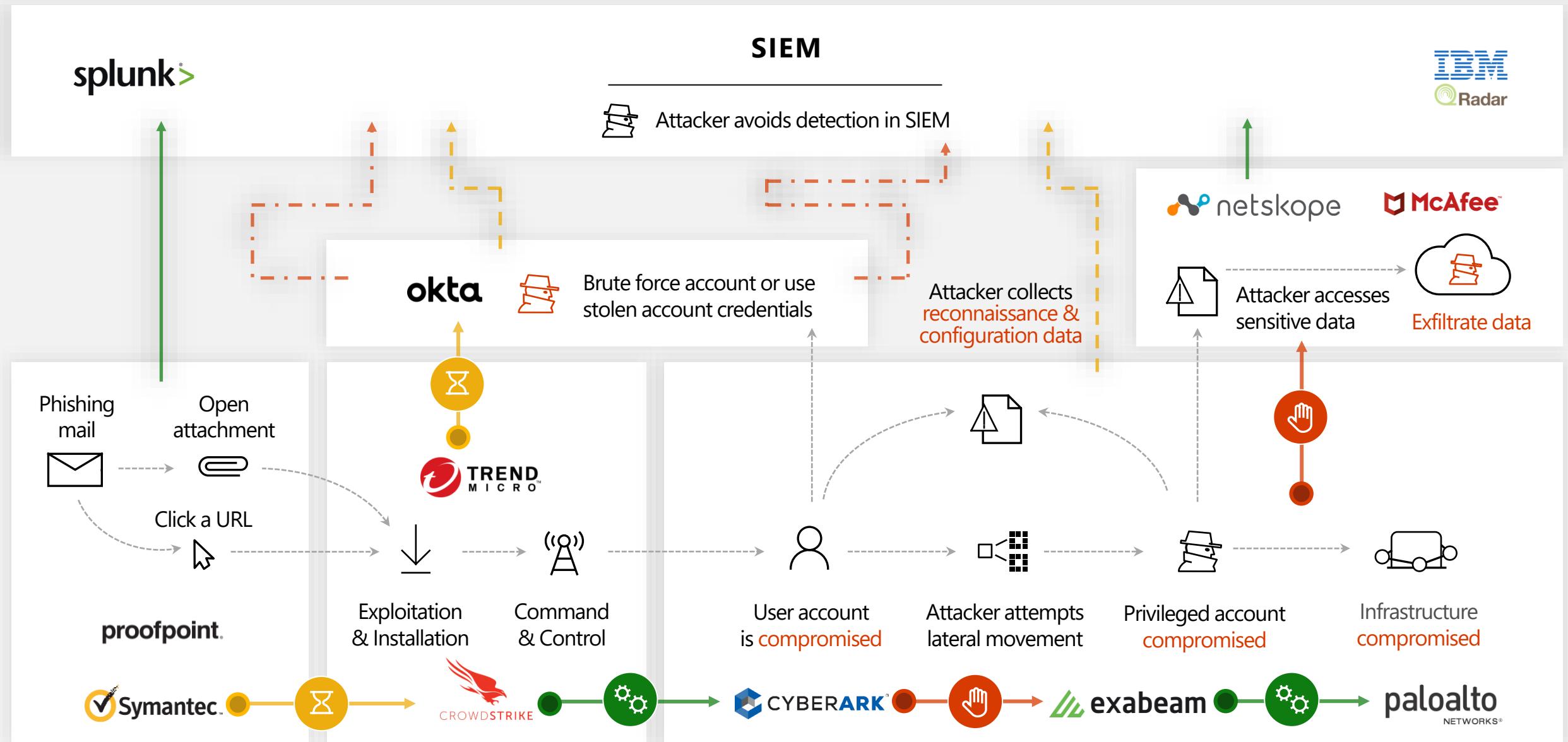
Improve overall security posture	47%
Improve end user experience and productivity	44%
Transform the way security teams work together	38%
Simplify security stack	35%
Reduce security costs	35%

## EXHIBIT 7. ZERO TRUST COMPONENT IMPLEMENTATION (TOP 3) – RANKED #1 (IMPLEMENTED FIRST)

Identities		Endpoints	
Apps		Network	
Strong authentication (i.e., multi-factor authentication, passwordless authentication)	32%	Data Loss Prevention policies/controls for all unmanaged and managed devices	27%
Automated risk detection and remediation	27%	Real-time device risk evaluation / endpoint threat detection	26%
Adaptive access policies to gate access to resources	22%	Devices are registered with identity provider	24%
Ongoing Shadow IT Discovery and risk assessment	23%	Secure access controls to protect networks	25%
Granular access control to your apps (such as limited visibility or read only)	22%	Threat protection and filtering with context-based signals	24%
Policy-based access control for apps	20%	All traffic is encrypted	20%

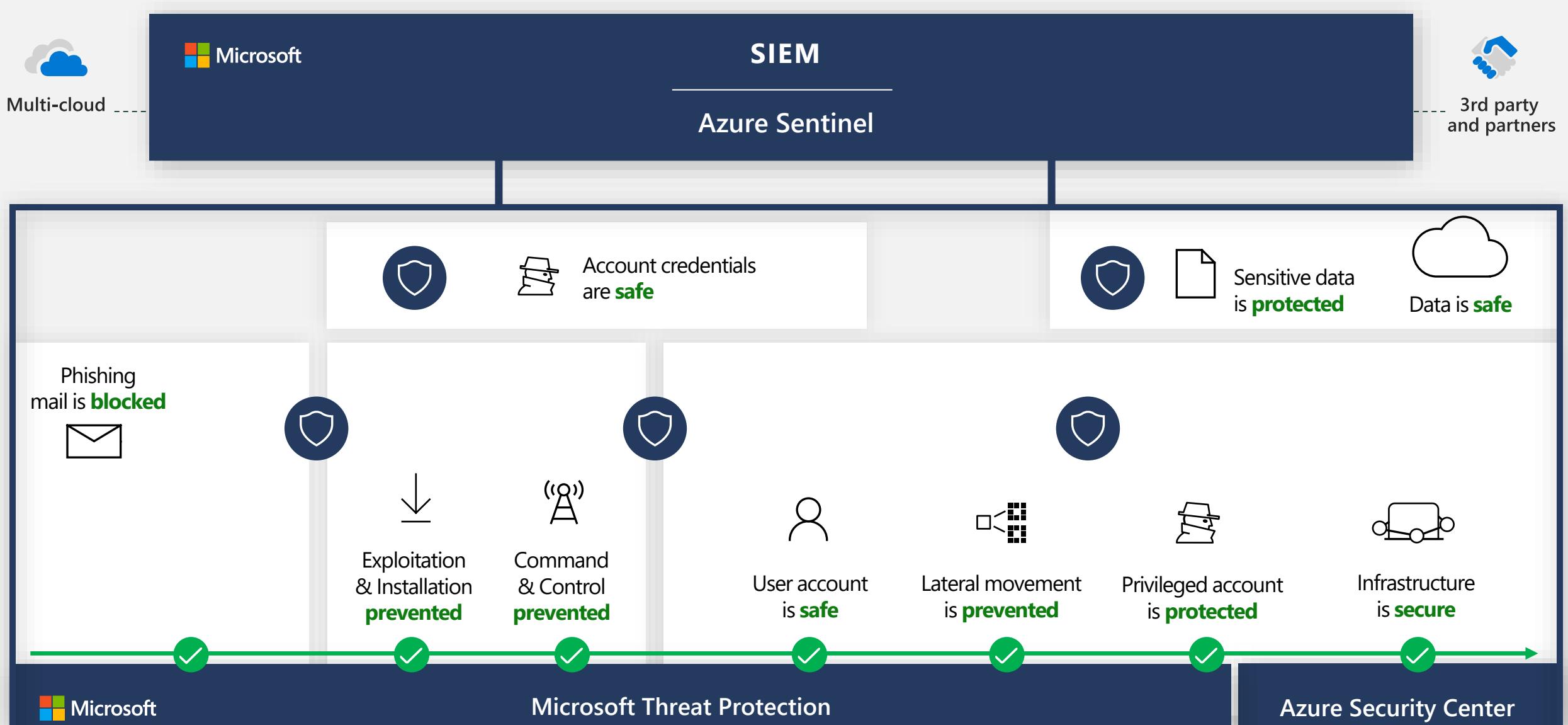
Reduce cyber risk

# Siloed security leads to gaps in coverage



Reduce cyber risk

# Microsoft Security closes the gaps



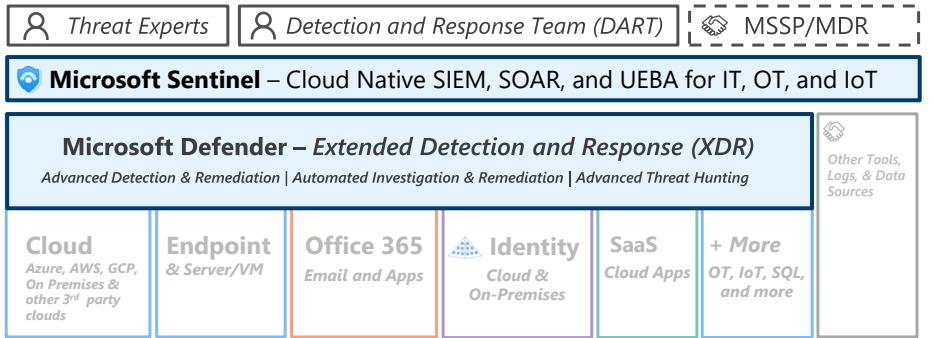
# Reduce cyber risk with integrated, best-in-class protection

Integrated threat protection powered  
by AI and automation

- Detect and respond faster and more accurately to attacks.
- Increase SecOps efficiency.
- Reduce the number and cost of breaches.



## Security Operations / SOC



# Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

December 2021 – <https://aka.ms/MCRA>

This is interactive!

## Security Guidance

1. Present Slide
  2. Hover for Description
  3. Click for more information
1. [Security Documentation](#)
  2. [Microsoft Best Practices](#)
  3. Azure Security [Top 10 | Benchmarks | CAF | WAF](#)

## Software as a Service (SaaS)



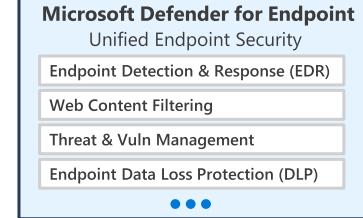
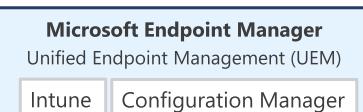
- App Discovery & Risk Scoring (Shadow IT)
- Threat Detection & Response
- Policy Audit & Enforcement
- Session monitoring & control
- Information Protection & Data Loss Prevention (DLP)



## Identity & Access

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

## Endpoints & Devices



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

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

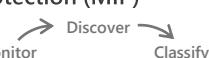


- Azure Firewall & Firewall Manager
- Azure WAF
- DDoS Protection
- Azure Key Vault
- Azure Bastion
- Azure Lighthouse
- Azure Backup
- ... Security & Other Services

## Information Protection



Microsoft Information Protection (MIP)



File Scanner (on-premises and cloud)



Data Governance

Advanced eDiscovery

Compliance Manager

## Azure Active Directory

Passwordless & MFA

Hello for Business

Authenticator App

fido ALLIANCE FIDO2 Keys

Identity Protection

Leaked cred protection

Behavioral Analytics

Azure AD PIM

Identity Governance

Azure AD B2B & B2C

Defender for Identity

Active Directory

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

## Windows 10 & 11 Security

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

## IoT and Operational Technology (OT)



### 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)**

microsoft.com/en-au/security/business/forrester-tei-study



# Cost savings and benefits of Microsoft Security solutions

Read a collection of Forrester Consulting Total Economic Impact™ (TEI) studies commissioned by Microsoft, including Cloud App Security and Azure Active Directory studies.

## Microsoft Security solutions

Deliver a best-in-class, end-to-end solution for cost-effective security. Read these Forrester TEI studies to learn more.



**Forrester TEI of Zero Trust solutions from Microsoft**

[Download study >](#)  
[Learn more >](#)

**Forrester TEI of Microsoft 365 E5 Compliance**

[Download study >](#)  
[Learn more >](#)

**Forrester TEI of Microsoft Azure Network Security**

[Download study >](#)  
[Learn more >](#)

**Forrester TEI of Modernizing Endpoints**

[Download study >](#)  
[Learn more >](#)

**Forrester TEI of Microsoft Endpoint Manager**

[Download study >](#)  
[Learn more >](#)

<https://www.microsoft.com/en-au/security/business/forrester-tei-study>

# Annual estimated cost savings

COST SAVINGS CATEGORIES	20,000 seats	1,000 seats	50 seats
Vendor license cost consolidation	\$4,300,000	\$220,000	\$11,000
IT administration and deployment savings	\$6,100,000	\$330,000	\$41,000
Reduce total cost of risk	\$2,200,000	\$390,000	\$290,000
Save on automation and process improvements	\$12,000,000	\$600,000	\$30,000
POTENTIAL COST SAVINGS PER YEAR	Up to <b>\$25M</b>	Up to <b>\$1.5M</b>	Up to <b>\$380K</b>

Rounded estimates based on commissioned Forrester TEI studies and Microsoft Value Calculator and illustrate first year cost estimates. Contact your Microsoft representative for estimates for your organization.



# Microsoft Security technology

## Identity and access management

Secure access for a connected world



## Threat protection

Stop threats across your entire organization



## Cloud security

Comprehensive protection for multi-cloud resources, apps and data



## Information protection and governance

Safeguard sensitive data across clouds, apps, and endpoints



## Risk management

Identify and remediate critical data risks within your organization



## Compliance management

Assess compliance and respond to regulatory requirements



# Identity and access management

Secure access for a connected world



Unified identity management



Seamless user experiences



Secure adaptive access



Simplified identity governance



# Threat protection

Stop threats across your entire organization



Secure all clouds, all platforms



Get leading integrated protection



Deliver rapid, intelligent response



# Cloud security

Comprehensive protection for  
multi-cloud resources, apps, and data



Strengthen cloud security posture



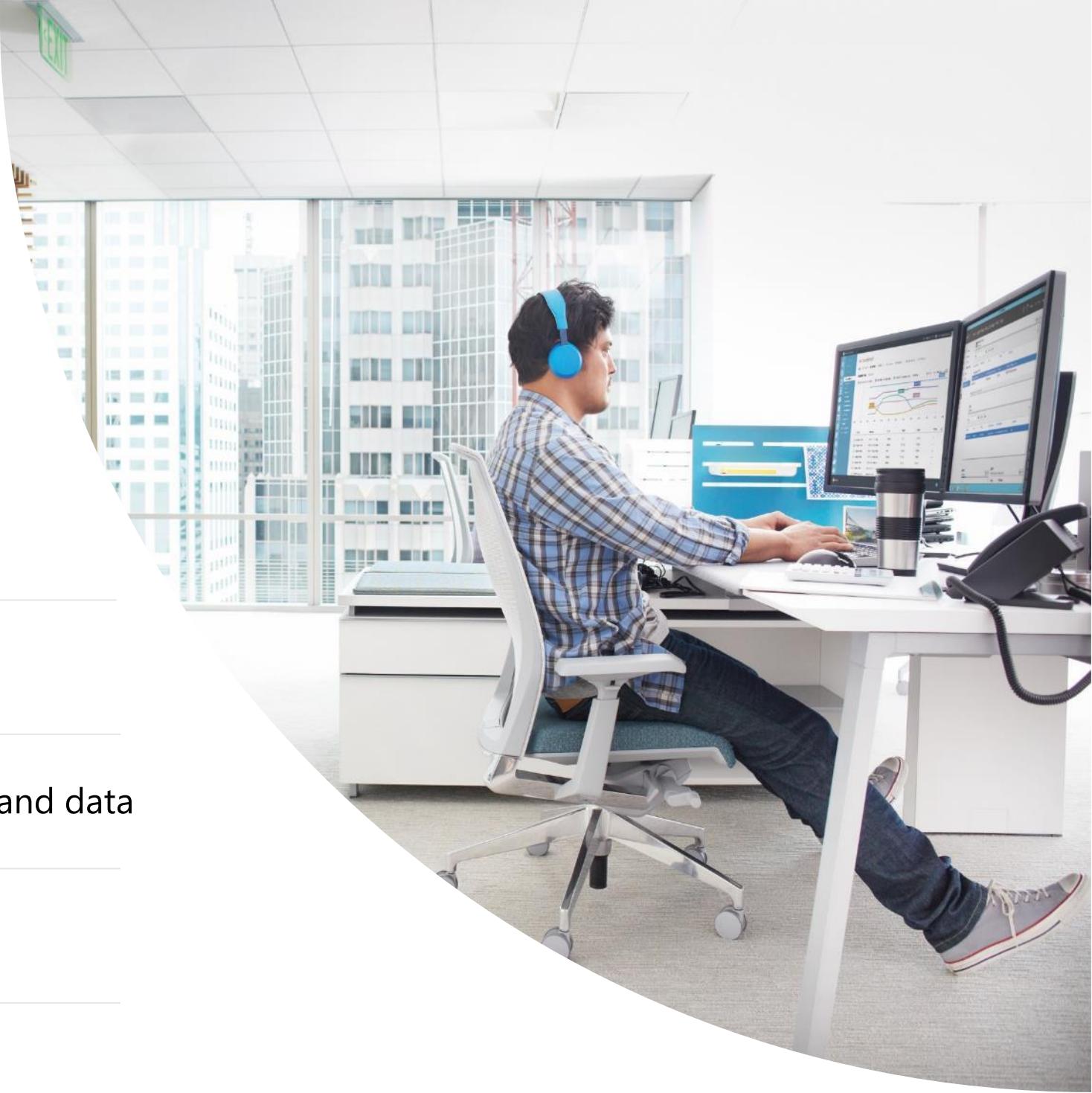
Protect cloud workloads from threats



Control access to cloud resources, apps, and data



Enable secure development in the cloud



# Information protection and governance

Safeguard sensitive data across  
clouds, apps, and endpoints



Know and protect sensitive data  
wherever it is



Prevent accidental or inappropriate  
sharing of sensitive data



Classify and govern data at scale



# Risk management

Identify and remediate critical risks within your organization



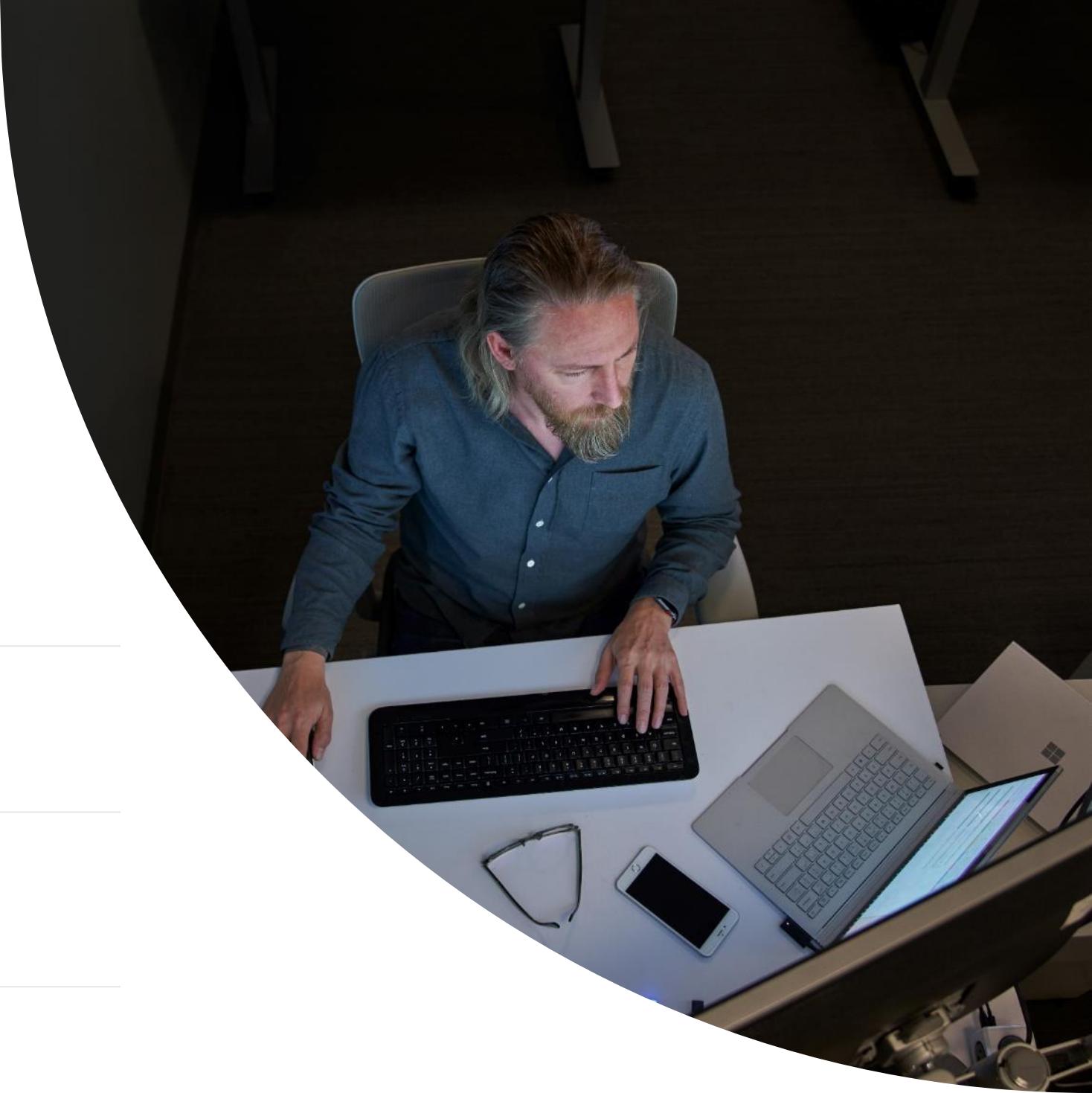
Manage insider risks with an end-to-end approach



Leverage ML to identify potential risks in communications



Escalate policy violations via seamless investigation handoff



# Compliance management

Assess compliance and respond  
to regulatory requirements



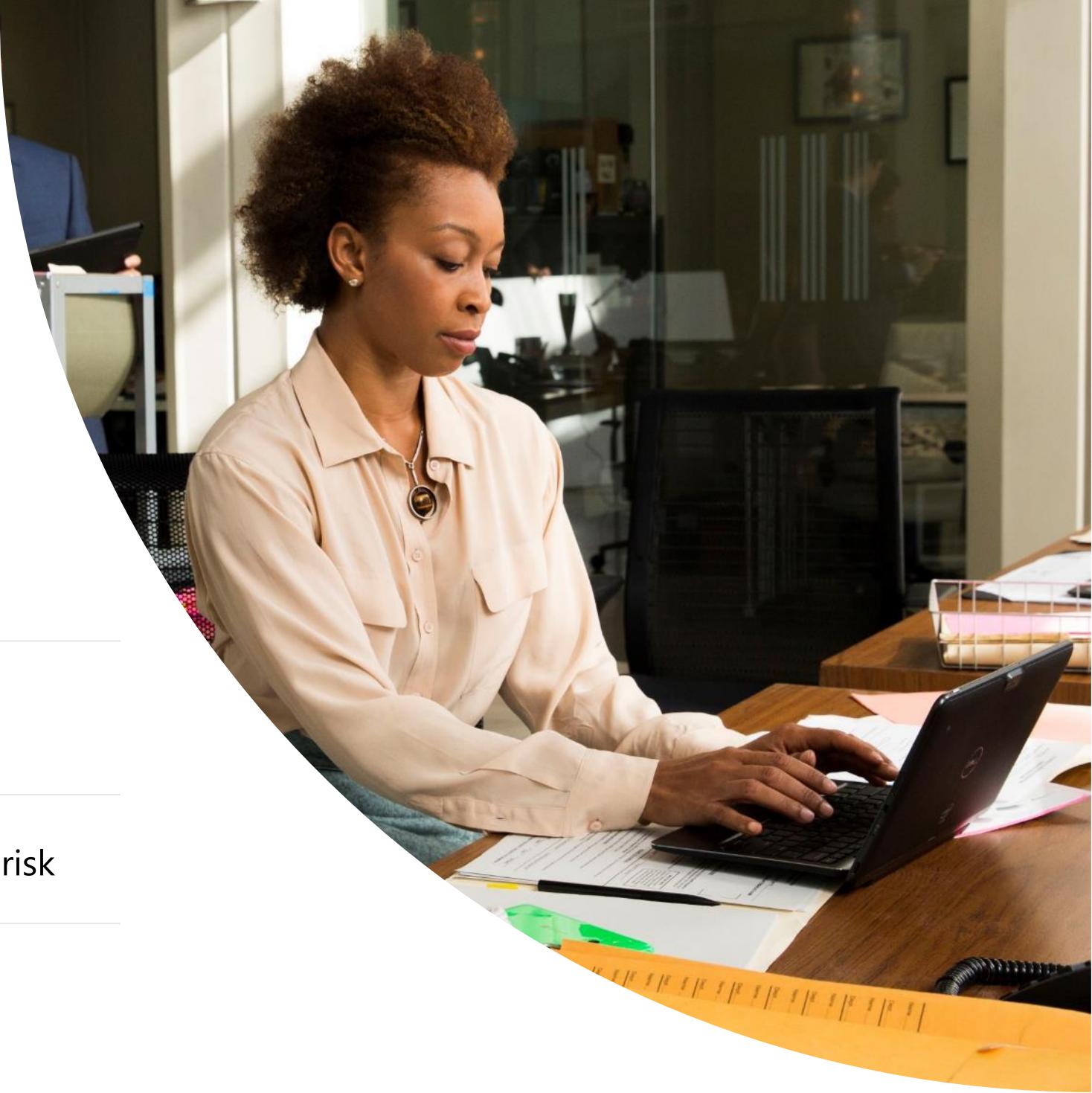
Intuitive end-to-end  
compliance management



Vast out-of-the-box assessment library  
to meet your unique requirements



Built-in intelligent automation to reduce risk



# Visibility, assessment, and guidance to strengthen your security posture

Identity  
and access  
management



Threat  
protection



Cloud  
security



Information  
protection  
and governance



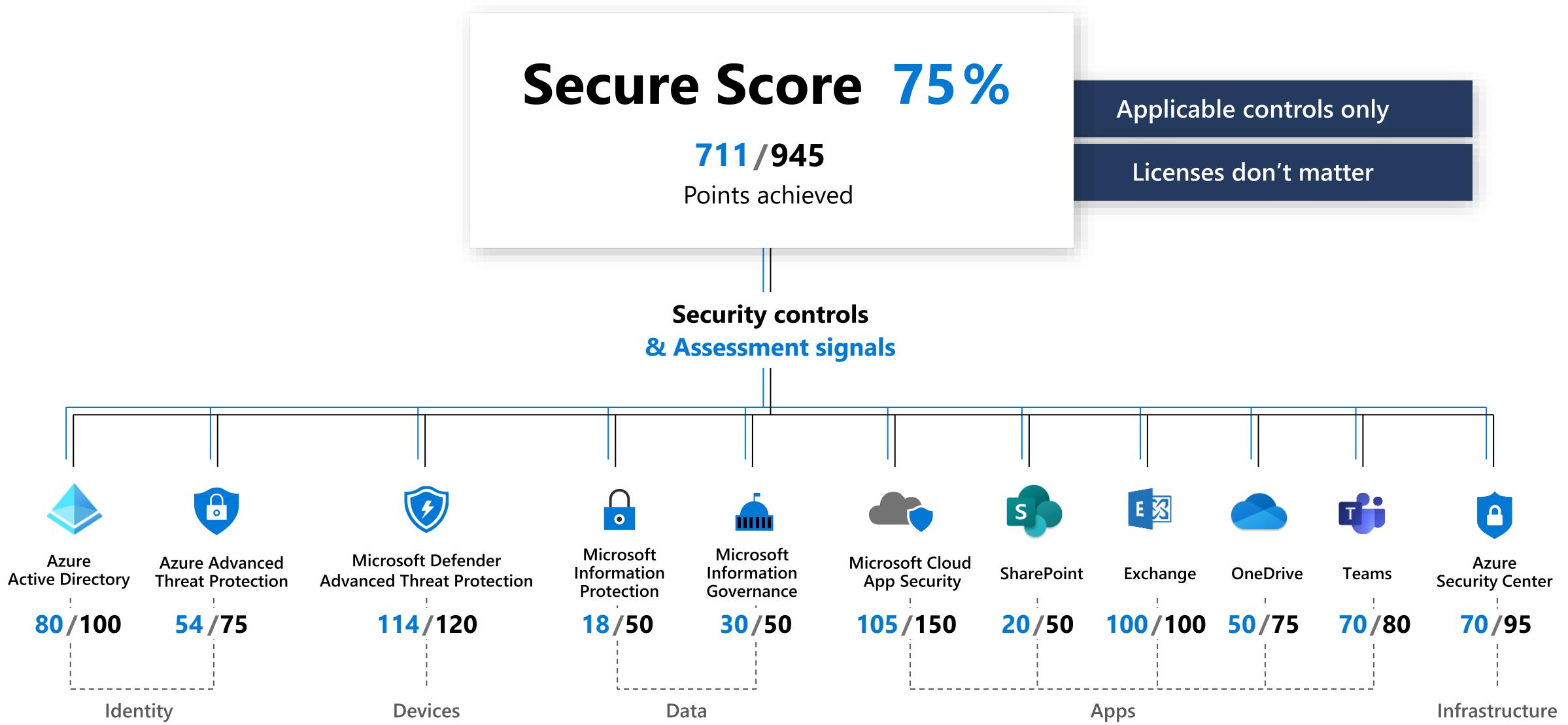
Risk  
management



Secure Score



# How does it work?

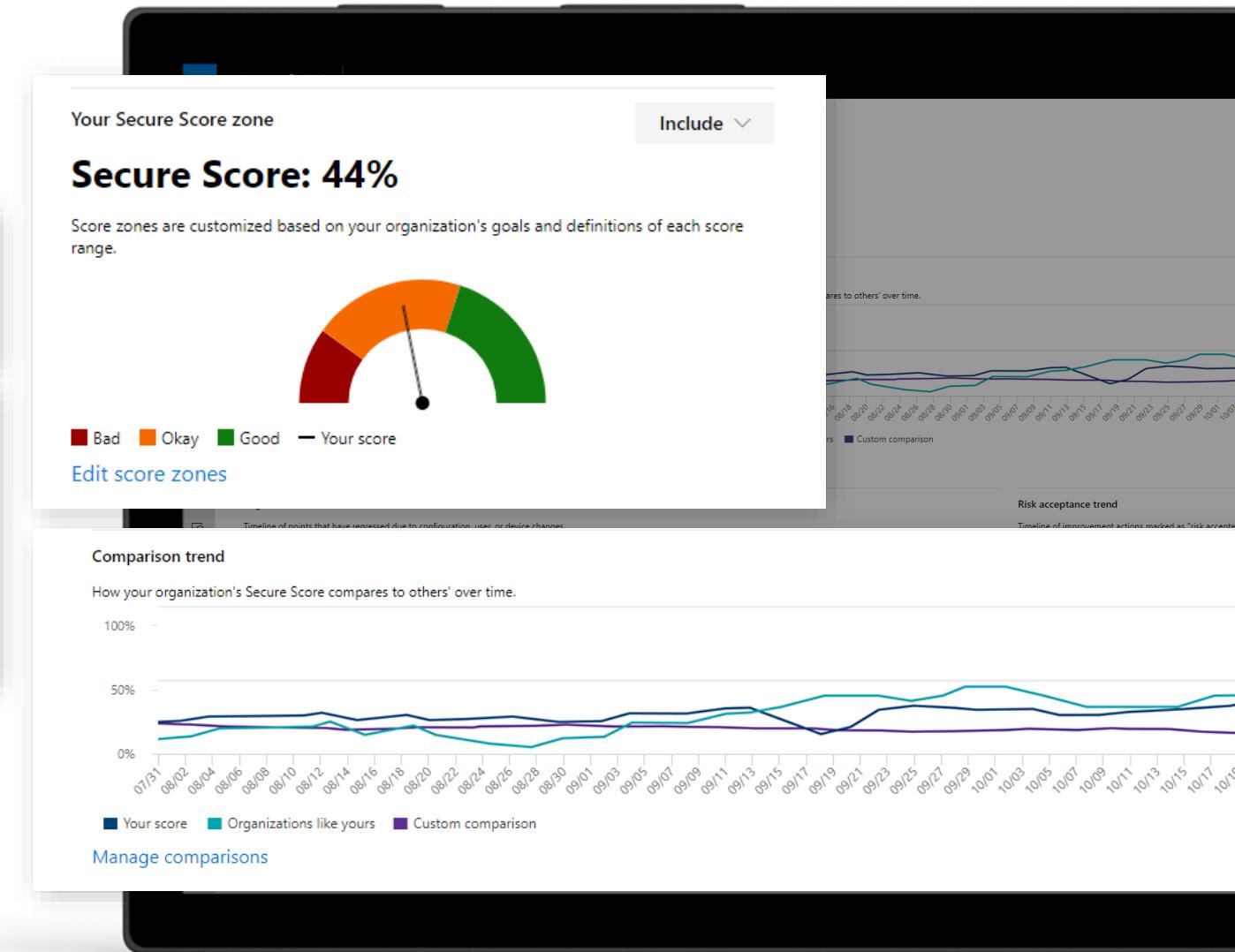


# Microsoft Secure Score is your tool to drive ongoing posture improvement

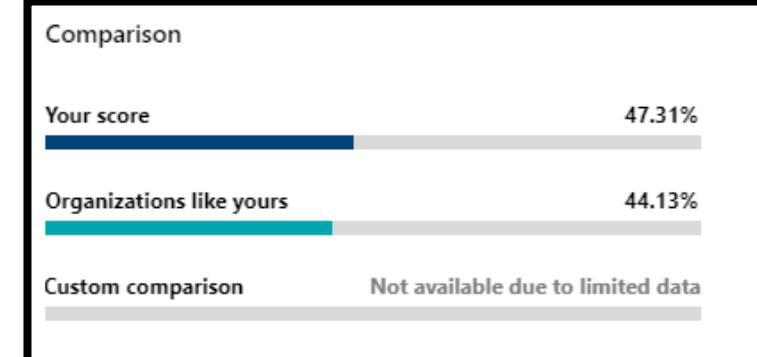
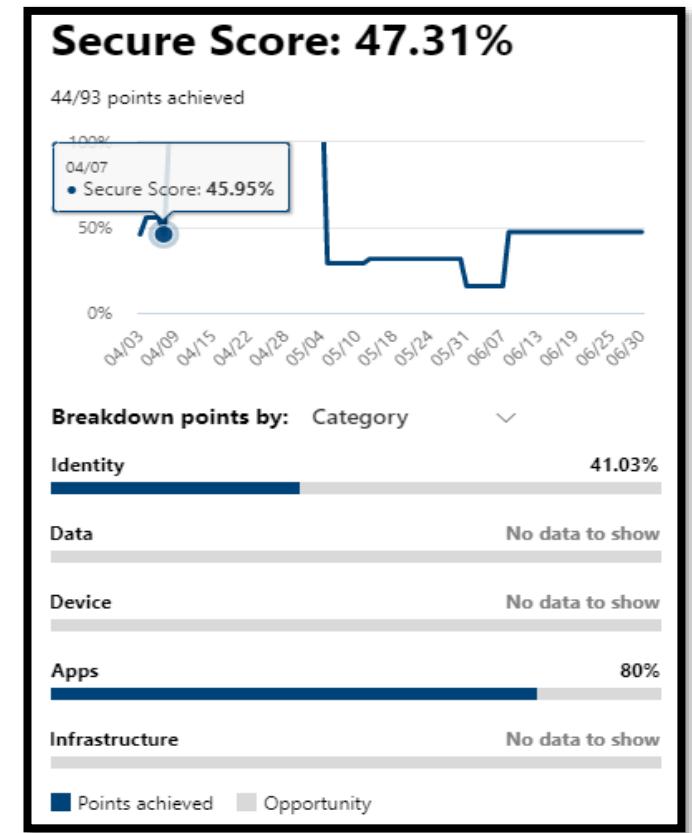
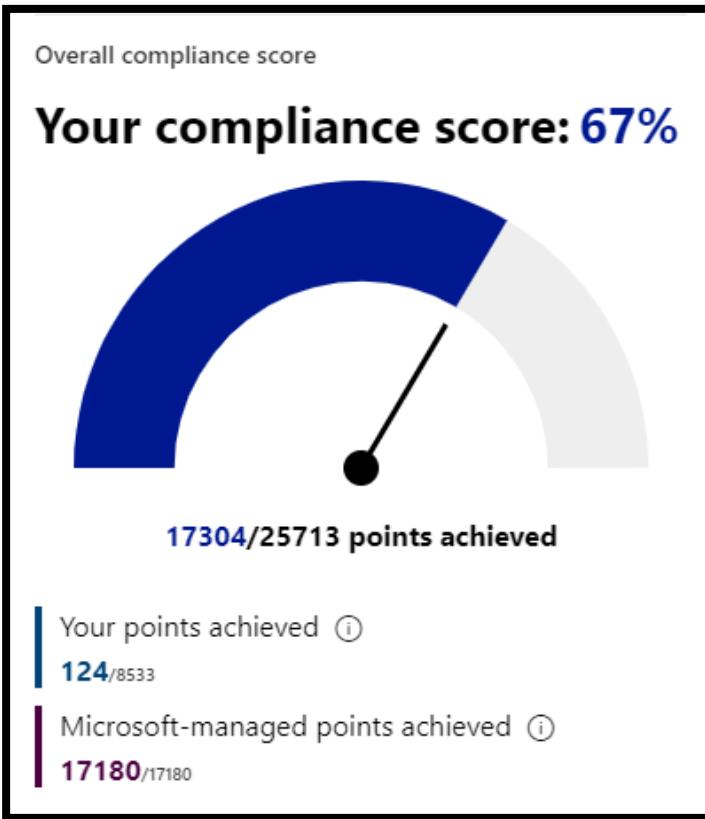
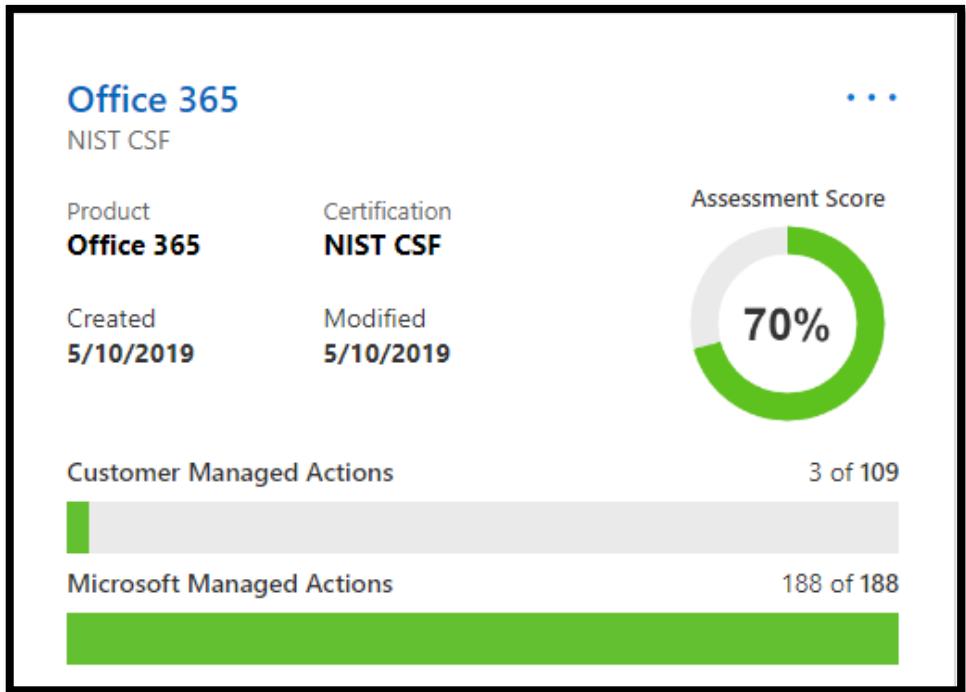
## How can I report to my CISO?

Enables security teams to demonstrate

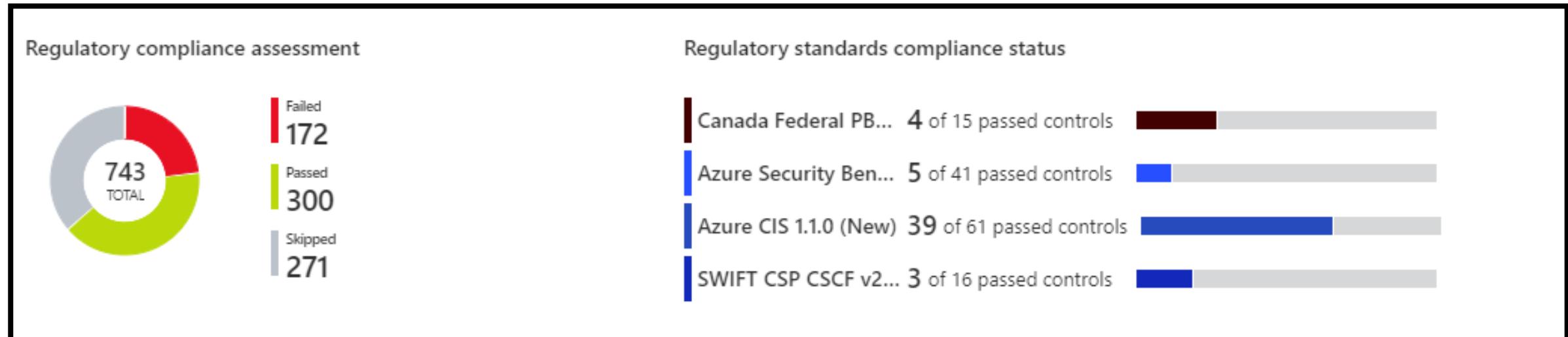
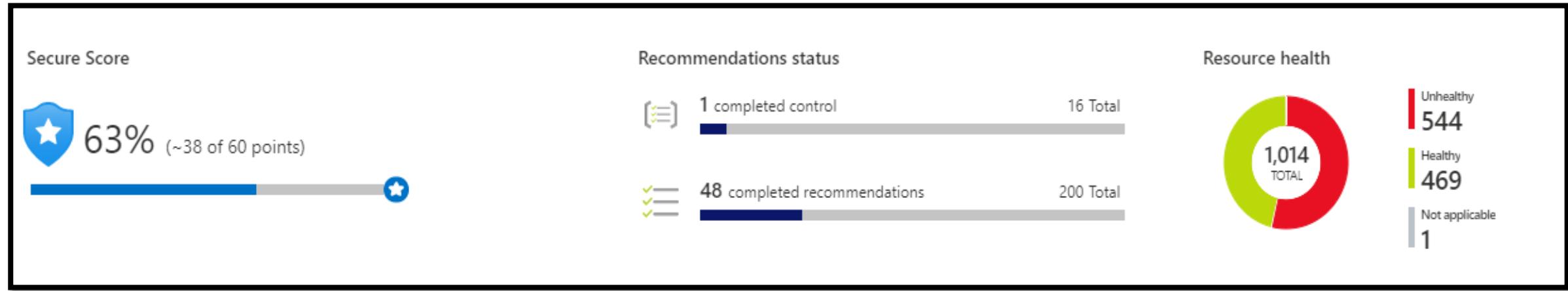
- Progress to CISO
- Benchmark



# CISO Reporting Dashboard (Microsoft 365)

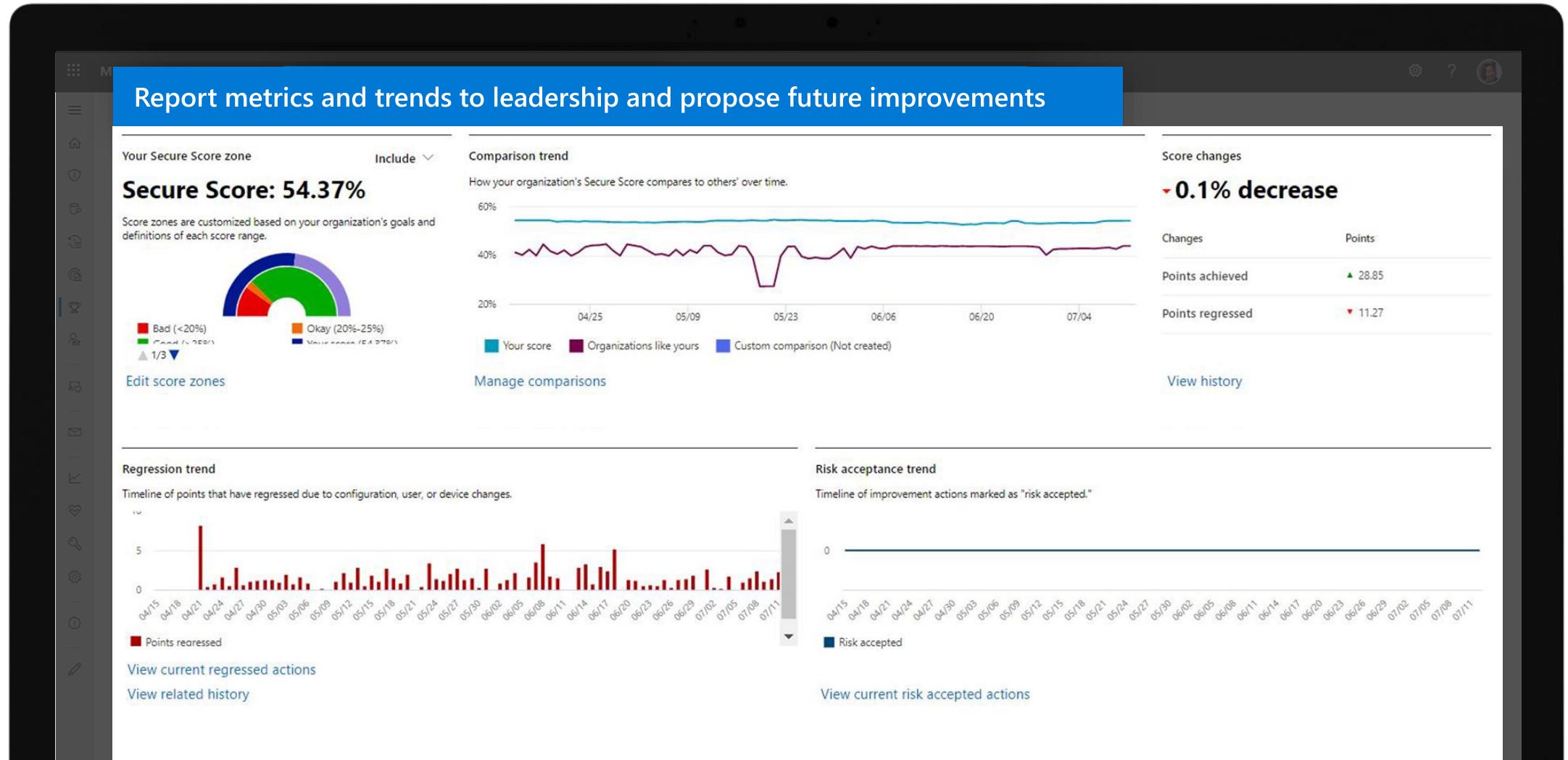


# CISO Reporting Dashboard (Microsoft Azure)



# Next step: Strengthen your security posture

Visibility and guidance will help you take full advantage of your security platform



# A Leader in Security, Compliance, Identity & Management



[A Leader in five Gartner®  
Magic Quadrant™ reports](#)

[A Leader in eight Forrester  
Wave™ categories](#)

[A Leader in six IDC  
MarketScape reports](#)

[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 Unified Endpoint Management Software 2021 Vendor Assessment](#)

[IDC MarketScape: Worldwide Unified Endpoint Management Software for Small and Medium-Sized Businesses 2021 Vendor Assessment](#)

[IDC MarketScape: Worldwide Unified Endpoint Management Software for Ruggedized/Internet of Things Deployment 2021 Vendor Assessment](#)

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.



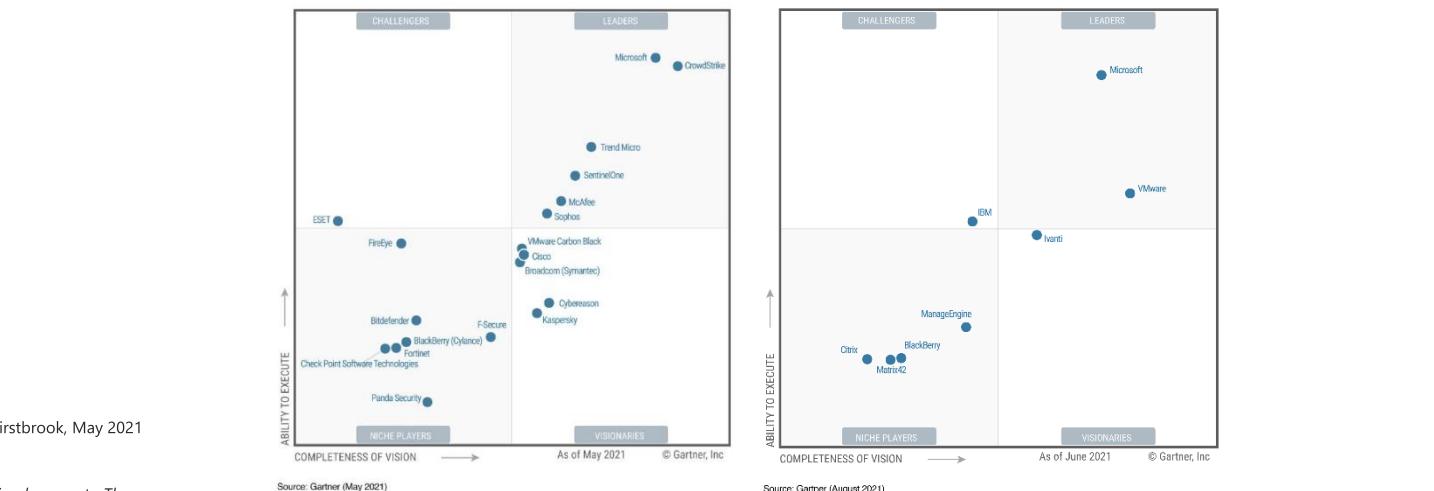
# Microsoft Security— a Leader in 5 Gartner Magic Quadrant reports



Access  
Management

Cloud Access  
Security Brokers

Enterprise  
Information Archiving



Endpoint  
Protection Platforms

Unified Endpoint  
Management

\*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

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.

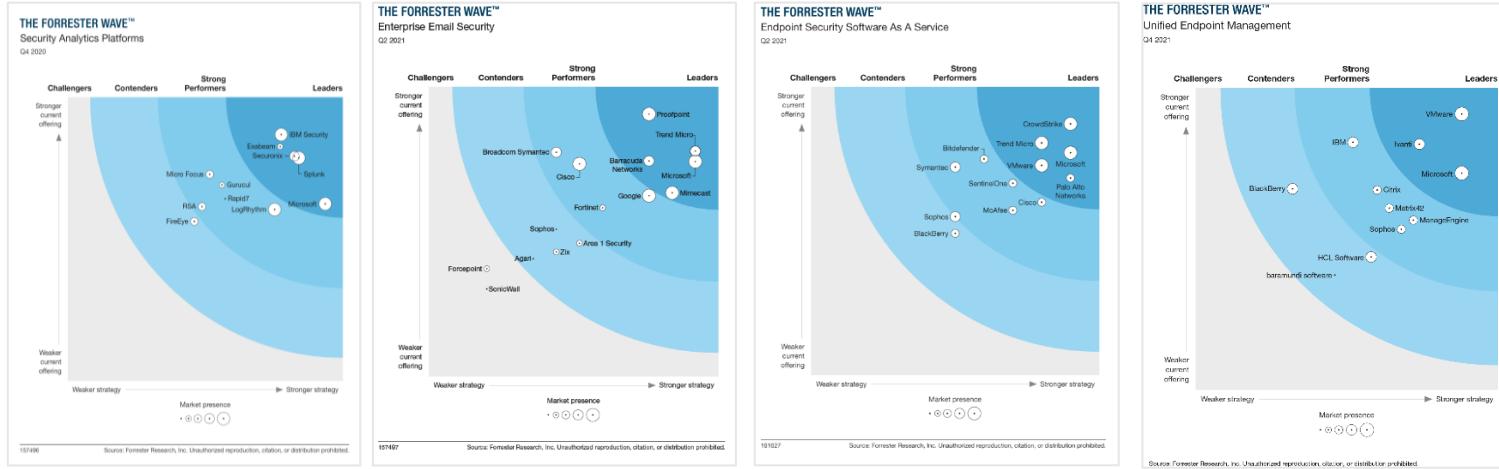


# Microsoft Security— a Leader in 8 Forrester Wave and New Wave reports

1. The Forrester Wave™: Security Analytics Platforms, Q4 2020, Joseph Blankenship, Claire O'Malley, December 2020
2. The Forrester Wave™: Enterprise Email Security Q2 2021 Joseph Blankenship, Claire O'Malley, April 2021
3. The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021, Chris Sherman, May 2021
4. The Forrester Wave™: Unified Endpoint Management, Q4 2019, Andrew Hewitt, November 2021
5. The Forrester Wave™: Unstructured Data Security Platforms, Q2 2021, Heidi Shey, May 2021
6. The Forrester Wave™: Cloud Security Gateways, Q2 2021, Andras Cser, May 2021
7. The Forrester Wave: Identity As A Service (IDaaS) For Enterprise, Q3 2021 Sean Ryan, August 2021
8. The Forrester New Wave™: Extended Detection And Response (XDR), Q4 2021, Allie Mellen, October 2021

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.

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

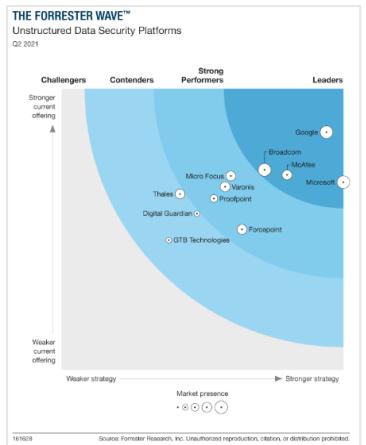


Security  
Analytics  
Platform

Enterprise  
Email  
Security

Endpoint  
Security  
Software as a  
Service

Unified Endpoint  
Management



Unstructured  
Data Security  
Platforms

Cloud Security  
Gateways

Identity As  
a Service

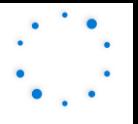
Extended  
Detection And  
Response  
(XDR)

# Way Ahead

Delivering a seamless and secure experience for every employee in a hybrid world



Managing costs and where to consolidate



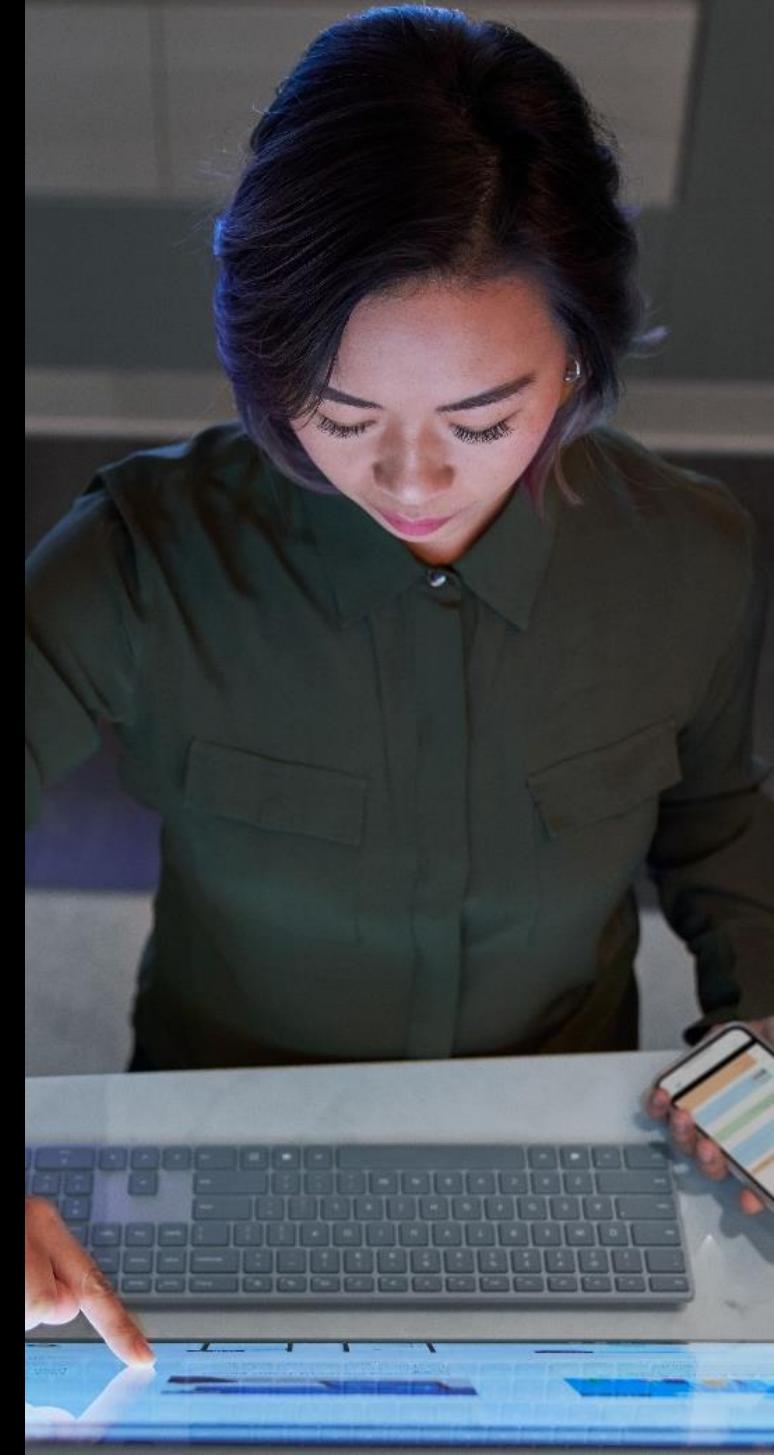
Modernizing security operations for faster resolution and risk remediation



Developing a compliance posture to address growing privacy concerns and complex regulations



Establishing a strategy to acquire and develop security talent in a competitive and scarce skills market



# **Next Step**

# Next steps

Let us help you get started.

Request a **Security Workshop** to learn how Microsoft can help improve your security posture.

The dashboard displays the following key information:

- Incident queue > Credential theft phishing campaign**
- 11/11 Active alerts**:
  - 1 Active alert from 04/05/2019 06:44:45 AM
  - 1 Active alert from 04/05/2019 06:12:22 AM
  - 1 Active alert from 04/05/2019 06:10:40 AM
- 8 MITRE attack categories**:
  - Exploit
  - Discovery
  - Execution
  - Delivery
  - Collection
  - Lateral Movement
  - Privilege Escalation
  - Defense Evasion
- Scope**:
  - 2 impacted devices**: com.milebarden, EU-Primary-DC
  - 2 impacted users**: Jonathan-Wolcott, Mike Borden
  - 2 impacted mailboxes**: Tracie Huber, Haley Stevens
- Top impacted assets**: com.milebarden (Risk level: high), EU-Primary-DC (Risk level: high)
- Incident details**:
  - Incident status: Active
  - First activity: Nov 5, 2018 06:32 AM
  - Last activity: Nov 4, 2019 06:53 AM
  - Classification: Not set
  - Determination: Not set
  - Assigned to: Not assigned
- Evidence and pending actions**: 23 evidence found

Get a customized **Total Cost of Risk** report for your organization.

The interface includes several sections:

- About**: Describes the tool's purpose and features:
  - Identifies the starting point of the attack, captures basic information about the customer - such as organization size and staff members.
  - Calculates total cost of deploying security solutions across licensing & subscriptions, and identifies areas of spending wasted license costs.
  - Calculates cost of additional benefits achieved by using Microsoft 365 products, including adoption costs.
  - Determines the additional benefit if a customer were to switch to using different security products that are provided by competitors.
  - Provides a filter for user with the highest value of selected Microsoft 365 products.
  - Also includes a detailed breakdown of all costs and benefits.
- Tool Organization**:
  - Print or Save the TCR Output: Use the "Print All" button in the header of the Results page. The "Print All" menu will automatically format your output and give you the option to "Save As..." or "Print All".
  - Find hidden information: Microsoft 365 has many notes. When you select one of them, you will see a description of the cell content, source information, and the date it was last modified.
  - Reset: Use the "Reset TCR" button in the top menu to reset inputs in the worksheet tabs, or all tabs in the Deep Dive Tool. This can be used to reset the default settings using the "Reset All" button in top menu of the Results tab.
- Cell Types**:
  - Input Cells with Defaults: Customer specific and should be changed if more accurate information is available.
  - Input Cells with Missing Defaults: Customer specific and needs to be changed when the specific option is selected.
  - Editable Output Cells: Calculations based on other inputs but that could be modified when better data are available.
  - Output Cells: Calculations based on other inputs and should not be modified.
- Version History**:

Rev.	Date	Note
v1.1	Apr-18	Added 2018 license, new benefits, and cost of security products integration, additional competitive prices changes in cost have not yet been costed, awaiting update.
v1.2	Jul-18	Tool updated to revisions, added value steps, cost take out.
v1.3	Oct-18	Additional costs, corrections to year 3 costs.
v1.4	Dec-19	Initial release.
- © 2019 Microsoft Corporation. Microsoft confidential - Internal use. The results generated by this tool are illustrative and only intended for your internal use. Prices are estimates and are not intended as actual price quotes. The results may not be accurate or appropriate for your needs and should not be relied upon as your sole reference. MICROSOFT NAME AND TRADEMARKS OR ANY TRADEMARKS OWNED BY MICROSOFT ABOUT THIS TOOL, INFORMATION OR MATERIALS PROVIDED WITH THE TOOL, OR RESULTS GENERATED BY THE TOOL.

# Workshops and Trainings (Sample list)

---

**Microsoft Security Workshop (3 hrs)**

---

**Cybersecurity Strategy workshop with your CISO's Team ( 8 to 12 hrs)**

---

**Microsoft Cybersecurity Reference Architecture (2 hours)**

---

**Cloud Adaption Framework Workshop ( 6 hrs to 12 hrs)**

---

**Chief Information Security Officer (CISO) Workshop ( 6 to 8 hrs)**

---

**Microsoft Security Best Practices ( 8 to 12 hrs)**

---

**Zero Trust Maturity Assessment and Training ( 6 hrs)**

---

**SOC Integration with Zero Trust Workshop (4 to 6 hrs)**

---

**Compliance Workshop ( 4 to 6 hrs)**

---

**Microsoft Cyber Defense Operation (CDOC) Tour (2 hrs)**

---

**Microsoft Azure Defender (Ninja Training)**

---

**Microsoft Azure Sentinel SIEM (Ninja Training)**

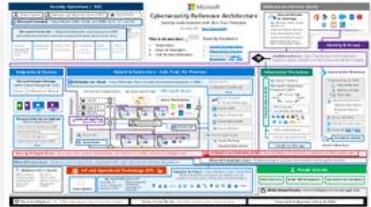
---

**Microsoft Defender for Endpoint (Ninja Training)**

# Microsoft Cybersecurity Reference Architectures (MCRA)

## Capabilities

What cybersecurity capabilities does Microsoft have?

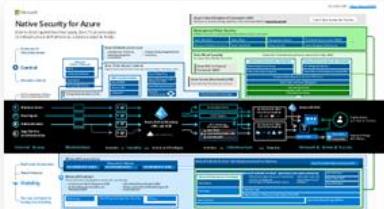


Build Slide



## Azure Native Controls

What native security is available?



## Attack Chain Coverage

How does this map to insider and external attacks?

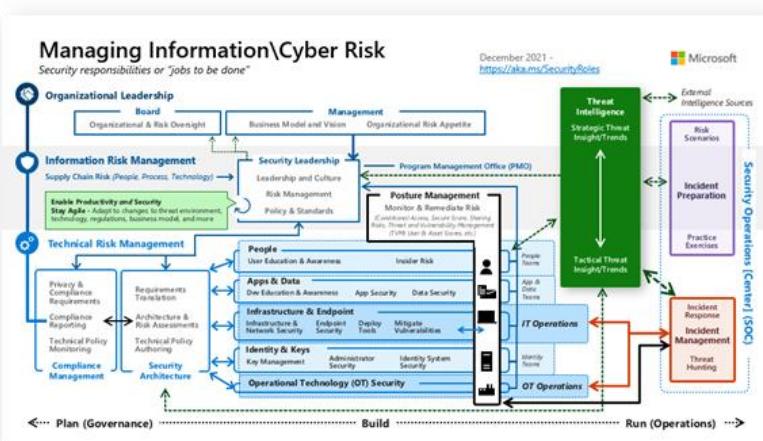


Build Slide



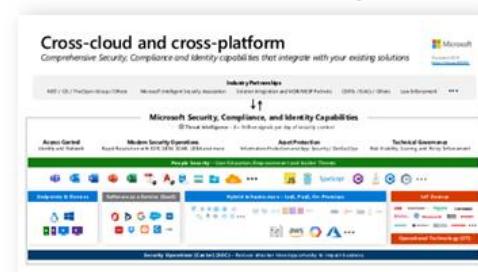
## People

How are roles & responsibilities evolving with cloud and zero trust?



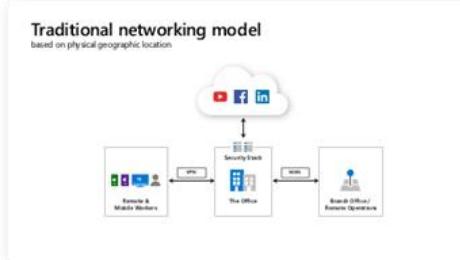
## Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?



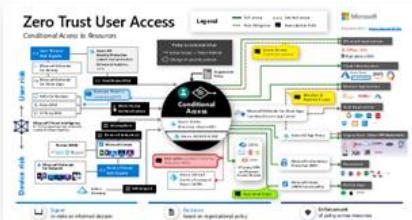
## Secure Access Service Edge (SASE)

What is it? How does it compare to Zero Trust?



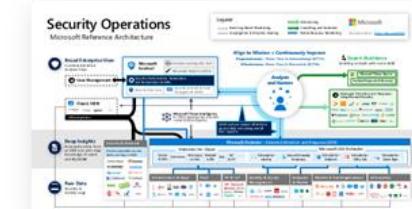
## Zero Trust User Access

How to validate trust of user/devices for all resources?



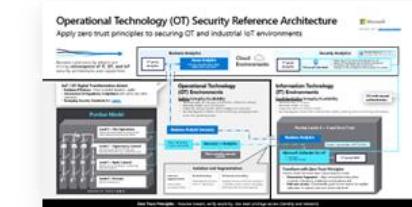
## Security Operations

How to enable rapid incident response?

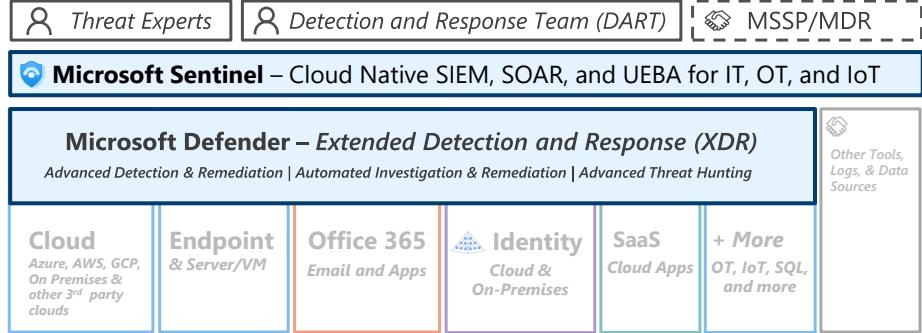


## Operational Technology

How to enable Zero Trust Security for OT?



## Security Operations / SOC



# Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

December 2021 – <https://aka.ms/MCRA>

This is interactive!

## Security Guidance

1. Present Slide
  2. Hover for Description
  3. Click for more information
1. [Security Documentation](#)
  2. [Microsoft Best Practices](#)
  3. Azure Security [Top 10 | Benchmarks | CAF | WAF](#)

## Software as a Service (SaaS)



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



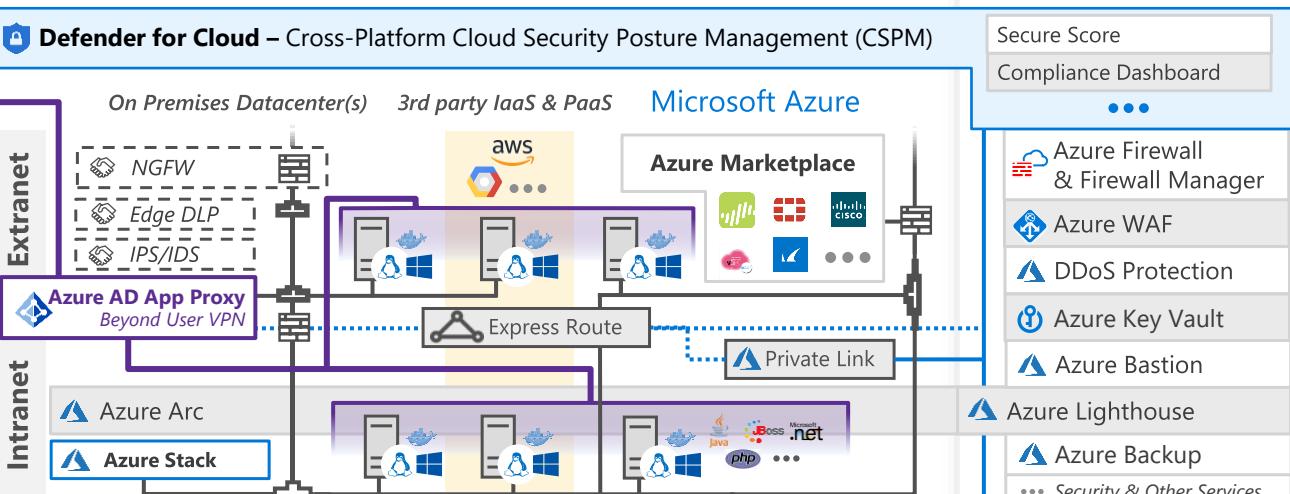
## Identity & Access

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

## Endpoints & Devices



## Hybrid Infrastructure – IaaS, PaaS, On-Premises



**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



## People Security



**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)**



## Find out how secure your organization really is

# Microsoft Security Workshop

### Workshop highlights

Identify real threats to your cloud environment by doing Threat Check

Work with you to understand your security goals and objectives

Deliver the end-to-end Microsoft security story

Showcase security scenarios with hands-on activities

Develop joint plans and next steps



### "Better security makes us a better business"

-Alain Quillet: Deputy CEO, Paule Ka

Do you know how many phishing attacks your organization has received? Whether your employees are using the right password protocol? Whether personal data is being exposed? In short, is your organization's cloud environment as secure as you think it is?

### Improve your security posture with a Microsoft Security Workshop

Organizations like yours are managing a growing volume of data and alerts, all while dealing with tight budgets and vulnerable legacy systems. In this environment, minimizing security risks is a massive challenge. Help achieve your broader security objectives—and identify current and real threats—by scheduling a Microsoft Security Workshop.

Designed for today's security stakeholders, the workshop will help you develop a strategic plan based on the recommendations of Microsoft cybersecurity experts, customized specifically for your organizational needs. You'll not only gain visibility into immediate threats across email, identity, and data; you'll get valuable clarity and support on how to upgrade your security posture for the long term.

### Why you should attend

Given the volume and complexity of identities, data, applications, devices, and infrastructure, it's essential to learn how secure your organization is right now, and how to mitigate and protect against threats moving forward. By attending this workshop, you can:

Identify current, ongoing risks to your cloud environment

Walk away with actionable next steps based on your specific needs and objectives

Document your security strategy for the benefit of key stakeholders

Better understand how to accelerate your security journey using the latest tools

## Azure Security Compass

### BASICS



#### TRANSFORMING TOOLS, SKILLS, & PRACTICES



#### STRATEGIES & THREATS EVOLVE



#### AZURE REGIONS & SERVICES



#### MICROSOFT SECURITY PRACTICES

### SECURITY GUIDANCE



#### COMPONENTS & MODELS

#### AZURE SECURITY CENTER (ASC)



#### GOVERNANCE, RISK, & COMPLIANCE



#### SECURITY OPERATIONS



#### IDENTITY



#### NETWORK CONTAINMENT



#### ADMINISTRATION



#### INFO PROTECTION & STORAGE

IDENTIFY

PROTECT

DETECT

RESPONSE

RECOVER

# NIST Cybersecurity Framework

	IDENTIFY	PROTECT	DETECT	RESPONSE	RECOVER				
DEVICES	SCCM InTune	Defender Antivirus	Azure Security Center	Defender for Endpoint	SCCM InTune	Backup Recovery	Azure		
APPLICATIONS	SCCM InTune	Azure Security Center	Advanced Compliance	Azure App Gateway	AAD P2	Defender for SQL	Defender for Endpoint	Backup Recovery	M365 E5
NETWORK	Azure Security Center	Azure Network Security groups	EOP	Azure Security Center	Defender For Office	Azure Security Center	Defender For Office	Azure	
DATA	AIP P1	AIP P2	AIP P1	AIP P2	Azure Pervue	AIP P2	Defender For Office P2	Defender For Office P2	
IDENTITY	AAD P1	AAD P2	AAD P1	AAD P2	AAD P2	Defender For Identity	Defender For Identity	Backup Recovery	

# Implementation prioritization (Example)

Solution	Effort	Impact	Details
Threat Protection	Low	High	Windows Defender, Office 365 Defender and Azure Defender
Identity as a Service	Medium	High	MFA, Conditional Access, Privileged Identity Management, Identity Protection
Security Insights into cloud and hybrid workloads	Low	High	Azure Security Center
Cloud Access and Security Broker	Low	High	Microsoft Cloud App Security
Mobile device and application management	Medium	Medium	Intune
Advanced Compliance	Medium	Medium	Customer Lockbox, Advanced eDiscovery and Advanced Data Governance
Information Protection	High	High	Azure Information Protection, Office Message Encryption

LE: Low Effort, max 3 months ME: Medium Effort, max 6 months HE: High Effort, max 12 months

LI: Low Impact, Nice to have MI: Medium Impact, Good to have HI: High Impact, must have

# Reduction of Attack Surface – Stage 1 (Example)

Global View of Risk	Use Cases
Identity	<ul style="list-style-type: none"><li>• Strengthen authentication through MFA for user logons</li><li>• Enable users to reset their passwords without contacting the Help Desk</li><li>• Prevent users from using weak passwords</li><li>• Detect potential vulnerabilities affecting KPMG identities, configure policies to respond to suspicious actions, and take appropriate action to resolve</li><li>• Manage, control, and monitor privilege access</li><li>• Enable administrators to elevate privileges only when needed to perform administrative tasks</li></ul>
Endpoint	<ul style="list-style-type: none"><li>• Deploy Windows 10 wherever possible and implement Windows Defender, Windows Defender ATP, Credential Guard, and other security capabilities to elevate end user protection</li></ul>
Data	<ul style="list-style-type: none"><li>• Discover sensitive information contained in Office and PDF documents that are stored on premise</li><li>• Empower users to encrypt emails that contain sensitive information</li><li>• Classify data as it's created</li><li>• Enable collaboration on protected documents</li><li>• Discover all cloud usage within KPMG</li></ul>
Server	<ul style="list-style-type: none"><li>• Gain insight into server assets (patching level, system configuration, file integration monitoring, etc.) that reside on-premise and in Azure</li></ul>

# Discussion

# Intelligent security

Microsoft 365

Identity and access management	Threat protection	Cloud security	Information protection & governance	Risk management	Compliance management
Azure AD Premium <ul style="list-style-type: none"><li>Azure AD Identity Governance</li></ul> Microsoft Endpoint Manager	<b>Microsoft 365 Defender</b> <ul style="list-style-type: none"><li>Microsoft Defender for Endpoint</li><li>Microsoft Defender for Office 365</li><li>Microsoft Defender for Identity</li><li>Microsoft Cloud App Security</li></ul> Threat and Vulnerability Management	<b>Microsoft Cloud App Security</b>	<b>Microsoft Information Protection</b> <b>Microsoft Information Governance</b> <b>Microsoft Data Loss Prevention</b> Records Management	<b>Insider Risk Management</b> <b>eDiscovery</b> Advanced Audit Communication Compliance Information Barriers Privileged Access Management	<b>Compliance Manager</b>

Azure

Azure AD B2C	<b>Azure Defender</b>	<b>Azure Defender</b>	Azure Purview
Azure AD Domain Services	<b>Azure Sentinel (SIEM)</b>	<b>Azure Security Center</b>	
Azure Key Vault	Azure AD Identity Protection Azure Defender for IoT Azure Sphere	Azure Firewall Azure DDoS Protection Azure Bastion Azure Web App Firewall Azure Front Door	