

# Partner customization guidance

This template can be customized for your brand by adding your logo and content where noted, and optionally replacing the colors and fonts.

(See example to right for how the original template colors can be customized)

Yellow highlights in this template indicate the areas where text or graphics should be customized for your brand.

**1** Replace the “Partner Logo” placeholder with your company logo where applicable.

Per Microsoft’s Partner Brand Guidelines, ensure your logo is 120% of the size of the Microsoft Security logo.

See more partner co-branding guidance [here](#).

**2** Replace all instances of “Partner Name” or “Partner Solution” with your own company/solution name and add any additional partner-specific content where identified. Be sure to remove the yellow highlighting and change the font color to match the surrounding text.

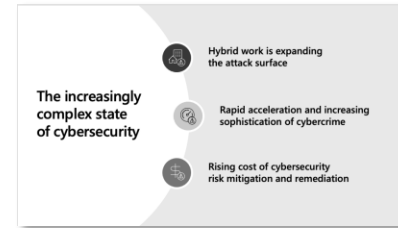
**3** Replace the template font with your brand font, matching weights. (Note that font type sizes vary and you may need to adjust your size to fit).

**4** Change the gray color blocks, overlays, icons, and text headlines to your own brand color(s). See example to right.

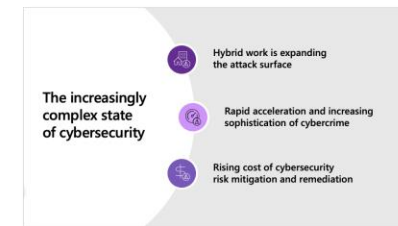
**5** Save your final customized presentation. Delete this instruction slide and use the **File** pulldown menu to select **Save As** to save your presentation with a new name.



Original template color scheme



Example of template that has been customized with brand colors, logo, and icons



Partner Logo

# Secure Multi-cloud Environments with **[Partner Name]** and Microsoft

# The increasingly complex state of cybersecurity



Hybrid work is expanding the attack surface



Rapid acceleration and increasing sophistication of cybercrime



Rising cost of cybersecurity risk mitigation and remediation

# Cloud security challenges

Security threats are compounded by the complexity of hybrid and multi-cloud environments

- » Lack of unified management and governance
- » Protecting workloads, no matter where they live
- » Misconfigurations/configuration drift
- » Maintaining consistent access controls
- » Silos, staffing constraints, training
- » Lack of interoperability
- » Lack of visibility/blind spots across environments
- » Developing and operating secure apps



# Securing multi-cloud

What's top of mind

Visibility into security and compliance



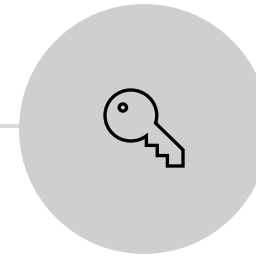
**52%** of organizations cite secure configuration of cloud resources as a top priority.<sup>1</sup>

Protect against increasing, sophisticated attacks



**\$4.24M** is the average cost of a breach, 2021.<sup>2</sup>

Manage access and permissions for users and applications



**1,295** different cloud services are used by enterprises, on average.<sup>3</sup>

Develop and operate secure apps in the cloud



**83%** of code vulnerabilities are caused by developer error.<sup>4</sup>

1. 451 Research

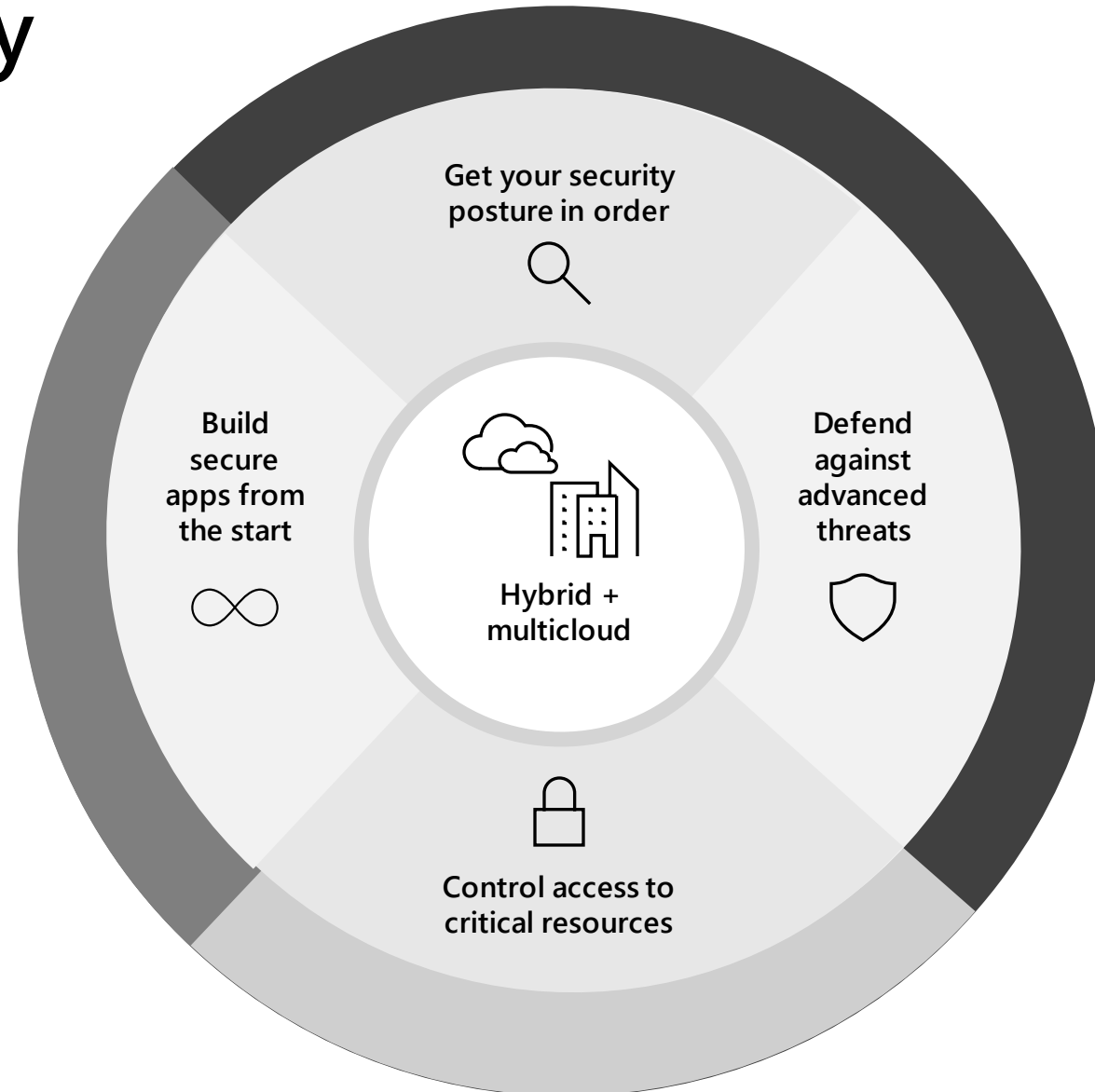
2. [Ponemon Institute, Cost of a Breach Report](#)

3. Netskope [Cloud Report](#).

4. <https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019>

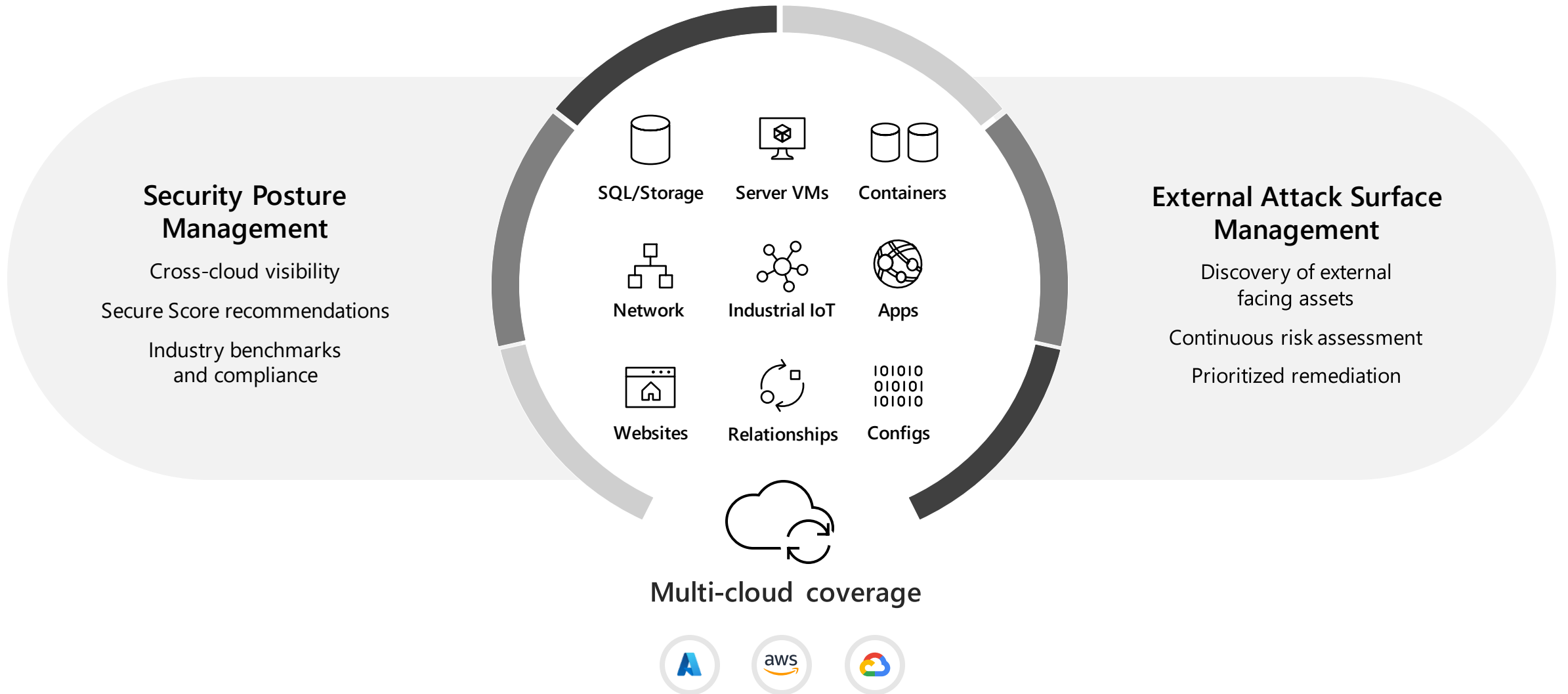
# Cloud security

Get integrated protection for your multi-cloud resources, apps, and data



# Strengthen your cloud security posture

Easily assess and improve the secure configuration of your critical multi-cloud resources





# Protect workloads against advanced threats

Cloud-native protection with Microsoft's leading threat protection technologies and shared intelligence

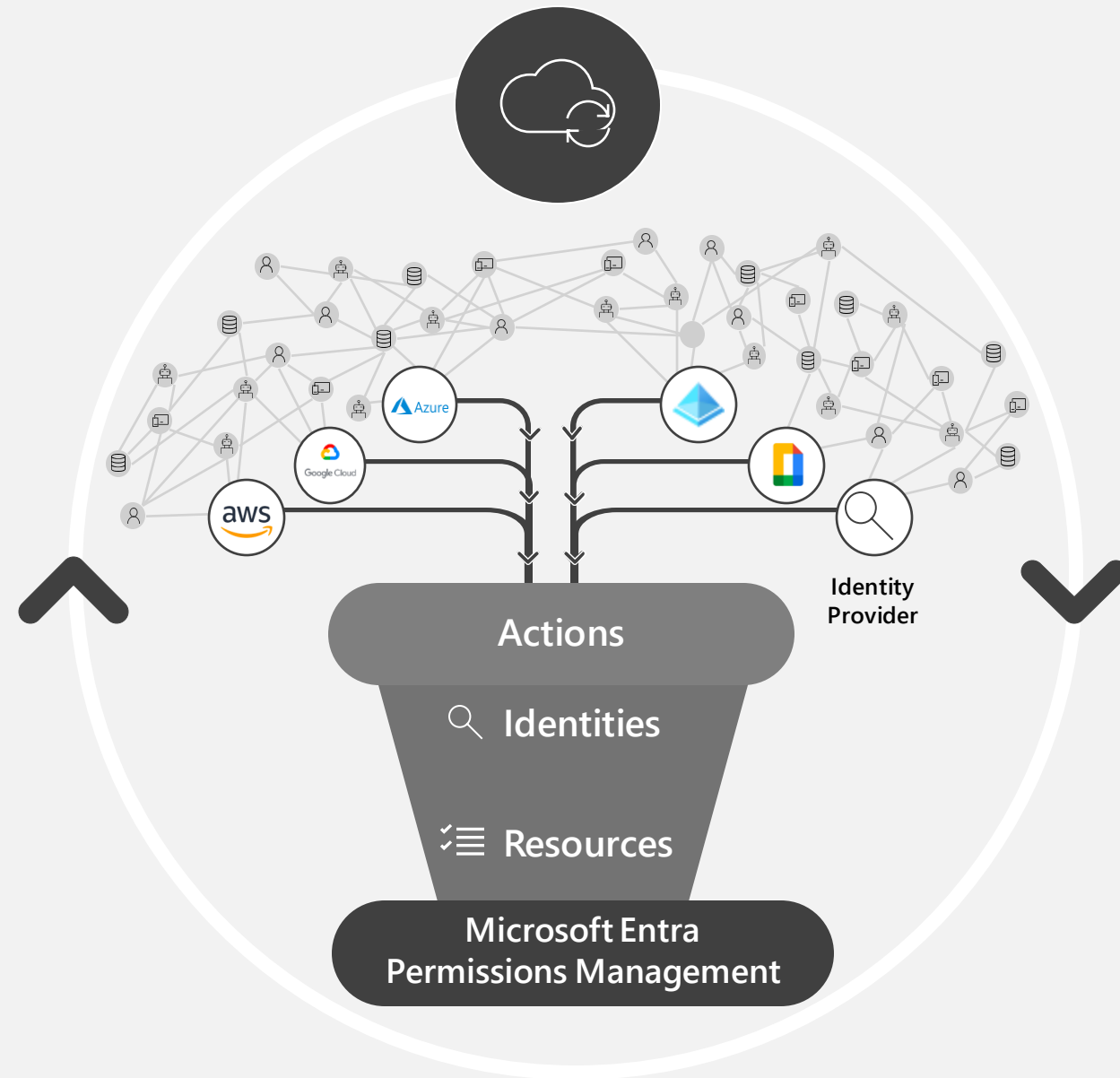




# Manage access & permissions to apps

Control access to critical resources and protect assets

- » Actions
- » Identities
- » Resources
- » Microsoft Entra Permissions Management

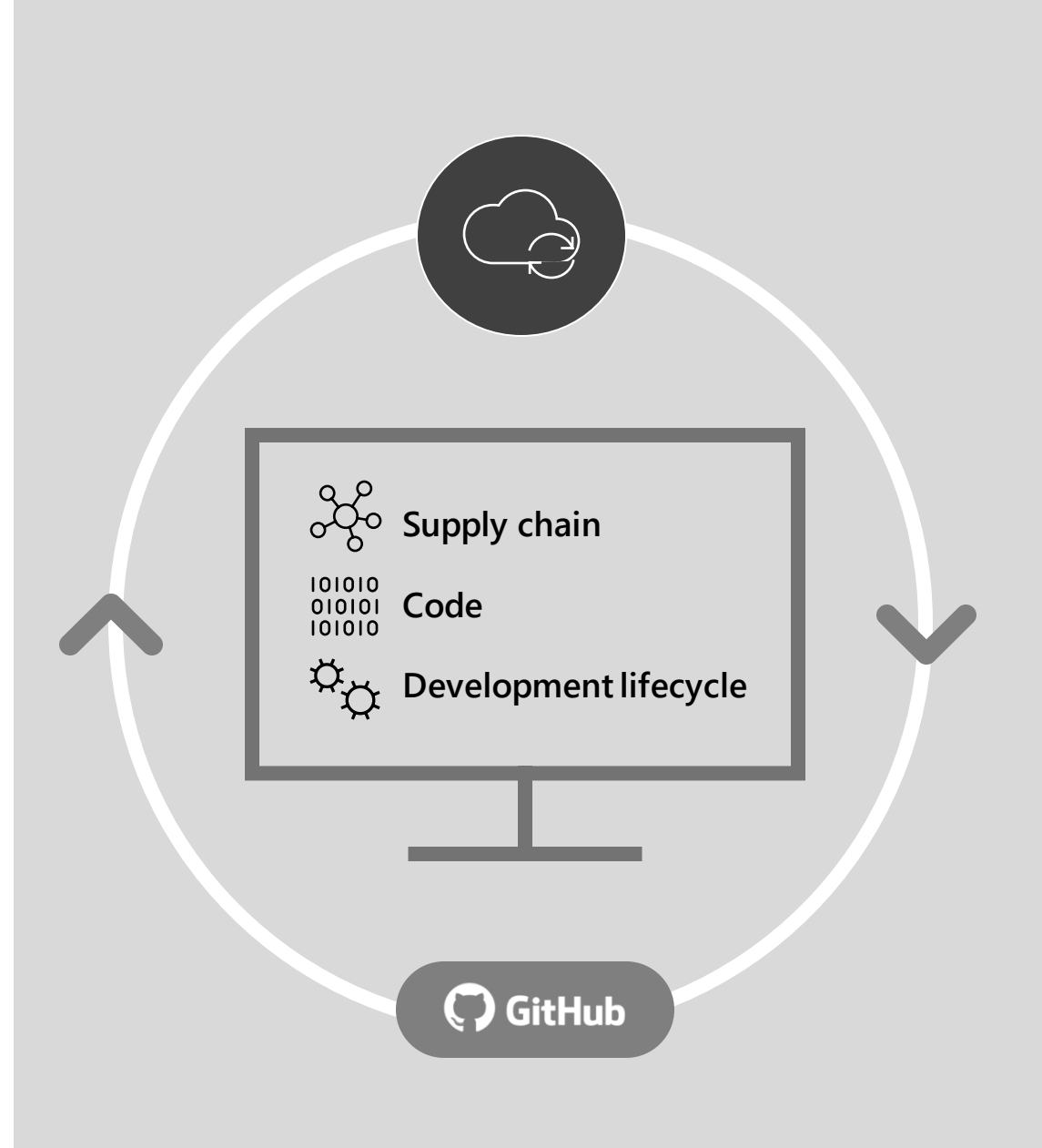


Cloud infrastructure entitlement management

# Build secure apps in the Cloud

Empower developers with the only community-driven, native application security testing solution within the developer flow

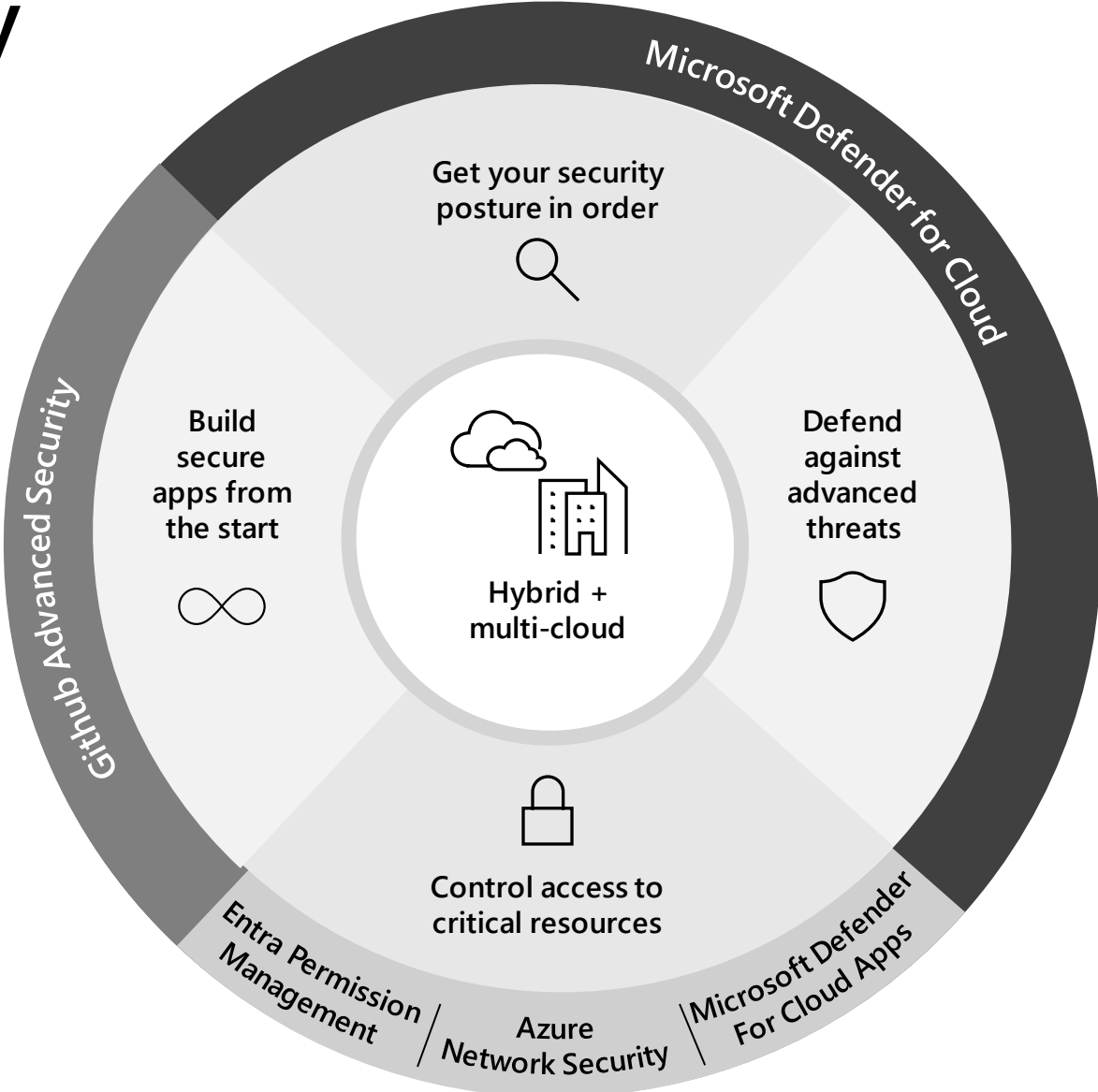
- » Develop securely, from idea to ship
- » Fix the vulnerabilities that matter the most for your organization in minutes
- » Trust your software with an end-to-end, automated security solution



Innovate with peace of mind

# Cloud security

Get integrated protection for your multi-cloud resources, apps, and data



“ It’s difficult to ensure that we have full insights from a security perspective when our platforms are so varied. We wanted protection and visibility everywhere. That’s why we use Defender for Cloud—it gives us single-pane-of-glass visibility across our hybrid and multi-cloud environment.”

Raoul van der Voort  
Global Service Owner, Cyber Defense Center  
Rabobank



**\$460K**

immediate cost savings

**\$3M**

estimated cost savings with Azure  
Arc + Defender for Cloud

**20 to 4**

vendor reduction with  
Microsoft solution



# Industry-leading security from Microsoft

Monitoring

**140+**<sup>3</sup>  
Threat groups

**40+**<sup>3</sup>

Nation state-groups

Serving billions of global customers,  
learning and predicting what's next

**43T**<sup>1</sup>

Analyzing  
Threat signals daily  
50% increase

**32B**<sup>1</sup>

Blocking  
email threats annually

**\$20B**<sup>1</sup>

in the next 5 years

Investing to improve and share  
knowledge, gain insights, and  
combat cybercrime



Keeping you  
secure, while  
saving you time  
and resources

**60%**

Up to **savings**, on  
average, over  
multi-vendor  
security solutions

**15K**<sup>4</sup>

partners in security  
ecosystem

**785K**<sup>2</sup>

customers rely on  
Microsoft for their  
multicloud,  
multiplatform  
infrastructure security

Trusted globally, protecting organizations'  
multi-Cloud and multi-platform infrastructures

Source:

1. [FY22 Q4 - Press Releases - Investor Relations - Microsoft](#)

2. [Microsoft FY22 Q4 Earnings Report](#)

3. [Microsoft Digital Defense Report - Microsoft Security](#)

4. [FY22 Q2 Earnings Call](#)

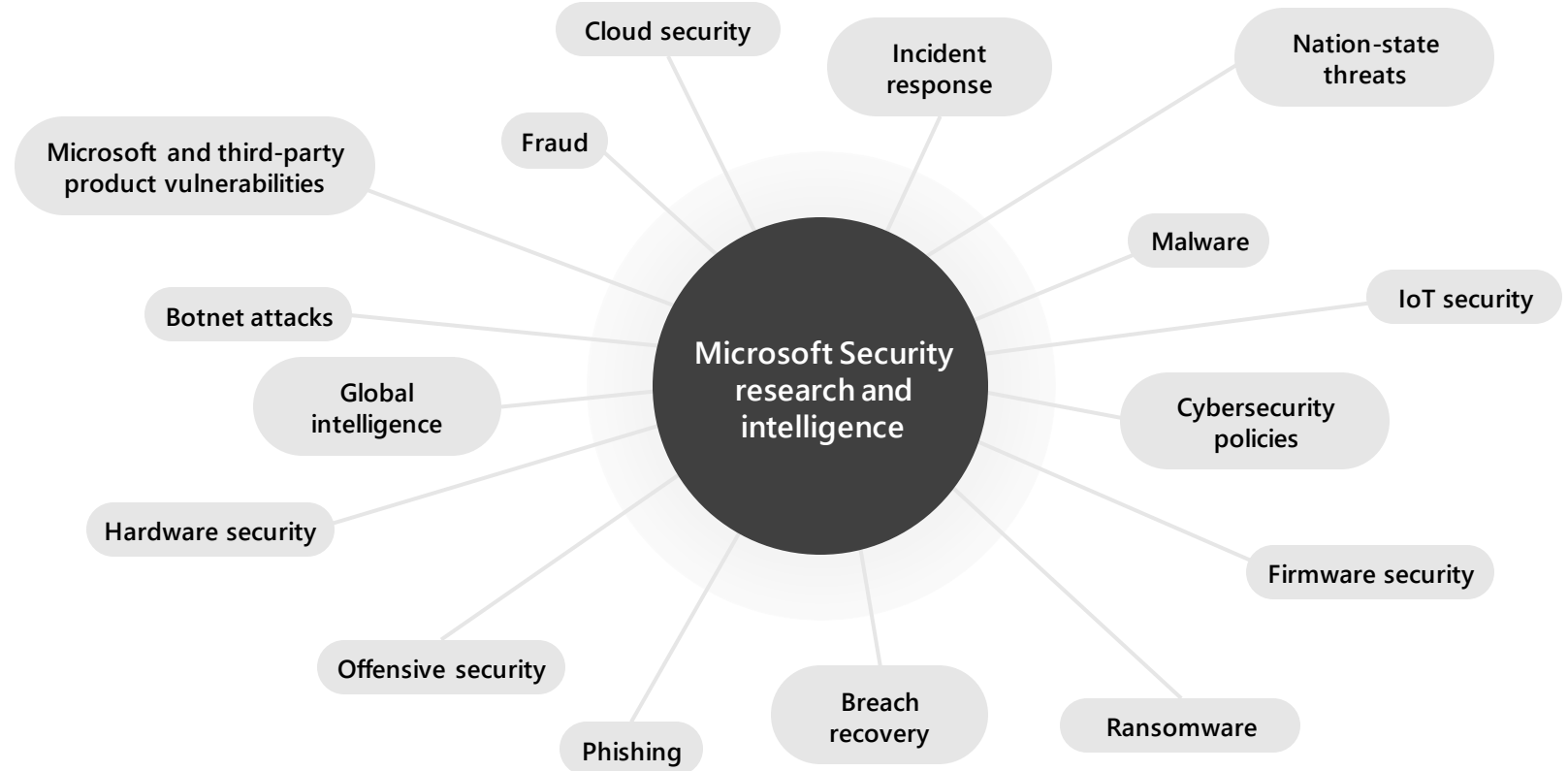
# Augment your security teams with Microsoft's world-class research and intelligence teams

8,500+<sup>1</sup>

engineers and researchers always working to mitigate and remediate the next threat

300+

members of Microsoft Intelligent Security Association (MISA)



Focused on all areas of the threat landscape.

# [Partner Service/Solution]

Let [Partner Name] help you with your modernization journey

Service/Solution benefits and value-add content to go here...

❖ Benefit 1 .....

❖ Benefit 2 .....

❖ Benefit 3 .....

**Proof Point/Success Stat**

**Proof Point/Success Stat**

**Proof Point/Success Stat**



# Headline with [Customer Name] and high-level statement on the achieved results

**Challenge:** Description of the challenges the customer was facing before help from <Partner Solution>...

**Solution:** Description of how <Partner Solution> helped to address the customer's challenges...

**Outcome:** Description of the outcome/benefits the customer achieved as a result of <Partner Solution>...



Customer logo  
goes here

Partner Logo

**[Partner Name]**

# Secure Multi-Cloud Environments Workshop



Given the volume and complexity of identities, data, apps, endpoints, and infrastructure, it's essential to learn how secure your organization is right now, and how to mitigate and protect against threats moving forward. With a Secure Multi-Cloud Environments Workshop, you'll get a customized threat and vulnerability analysis of your hybrid and multi-cloud environment and learn how to build a more robust cloud security system.



**Contact us today** to learn more  
and to schedule your workshop!

Partner Logo

Thank you

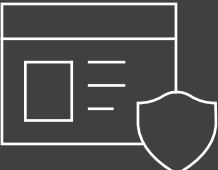
# Control access and secure your network infrastructure and applications

Protection from edge to cloud with cloud-native network security based on Zero Trust

## Azure network security



### Infrastructure Security



### Application Security



Segmentation controls

Intelligent threat protection

Traffic encryption

Private access



Defense-in-depth protection from edge to cloud

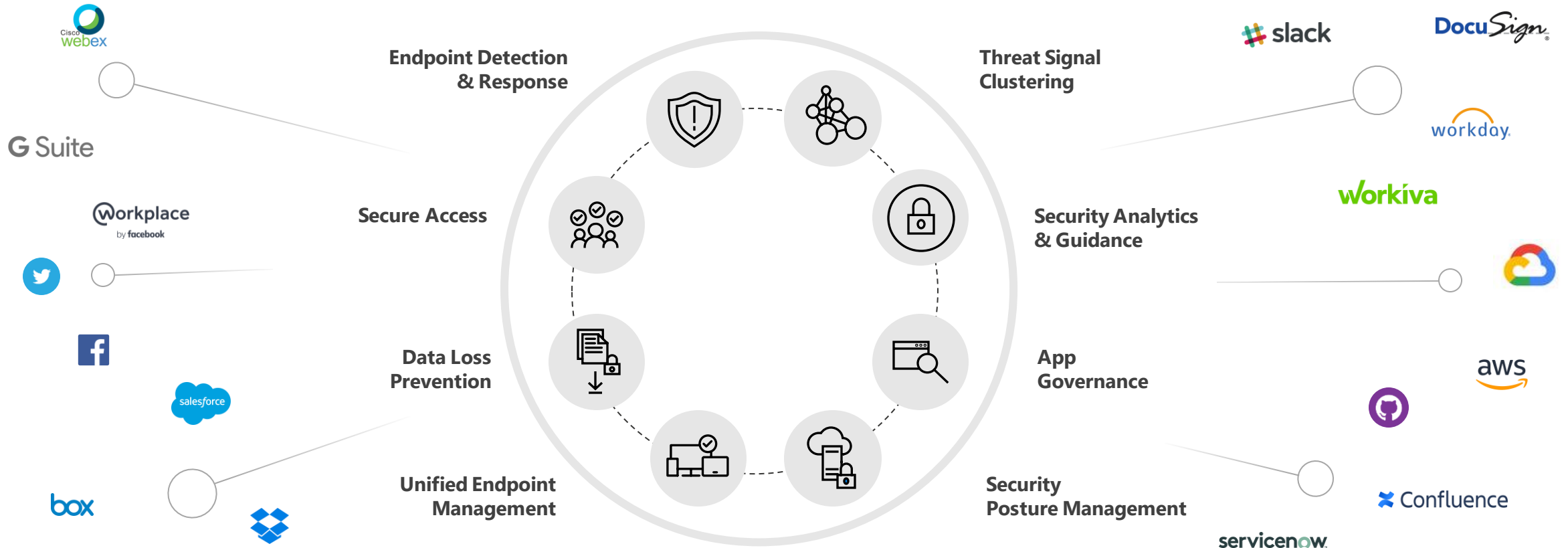
# Microsoft Defender for Cloud Apps

The go-to CASB for all your cloud enablement, monitoring and governance

Simple deployment

Natively integrated across the broader Microsoft product stack to deliver unique capabilities

Rooted in supporting any app



# Microsoft Defender for Cloud | Overview

Showing 54 subscriptions

Search Subscriptions What's new

**General**

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

**Cloud security**

- Secure score
- Regulatory compliance
- Workload protection
- Firewall manager

**Management**

- Environment settings
- Security solution
- Workflow automation

**54**  
Azure subscriptions

**4**  
AWS accounts

**18**  
GCP projects

**8928**  
Assessed resources

**215**  
Active recommendations

**7768**  
Security alerts

### Security posture

Recommendations status

**95** of 455 overdue recommendations

Secure score

**59%** SECURE SCORE

Azure	78%
AWS	42%
GCP	57%

[Explore your security posture >](#)

### Regulatory compliance

Azure security benchmark

**2** of 44 passed controls

Lowest compliance regulatory standards by passed controls

CMMC Level 3	0/55
ISO 27001	1/20
AWS CIS 1.2.0	3/43

[Improve your compliance >](#)

### Workload protections

Resource coverage

**95%** For full protection, [enable 8](#) resource plans

Alerts by severity

[Enhance your threat protection capabilities >](#)

### Firewall manager

**5** Firewalls | **3** Firewall policies | **4** Regions with firewalls

Network protection status by resource

Virtual hubs	0/0
Virtual networks	8/126

[Improve your network security >](#)

### Inventory

Unmonitored VMs

**54** To better protect your organization, we recommend [Install agents](#)

Total resources

**8928**

Unhealthy (7566)	Healthy (1156)	Not applicable (206)
------------------	----------------	----------------------

[Explore your resources >](#)

### Information protection Preview

Integrated with Purview

Resource scan coverage

**2%** For full coverage [scan](#) additional resources

Recommendations & Alerts by classified resources

[View classified resources in Insights >](#)

### Insights

#### Upgrade to New Containers plan

Cloud-native **Kubernetes security** capabilities including environment hardening, vulnerability assessment, and run-time threat protection. The **new plan** merges two existing Defender plans, in addition to new and improved features.

[Click here to upgrade >](#)

#### Most prevalent recommendations

- Audit diagnostic setting 619 Resources
- Storage account public access should... 161 Resources
- A vulnerability assessment solution... 107 Resources

#### Most attacked resources

- contoso5.cloudapp.net 63 Alerts
- Virtual machine 2 41 Alerts
- CentOS 28 Alerts

[View full alert list >](#)

#### Controls with the highest potential increase

- Remediate vulnerabilities +11% (6pt)
- Enable encryption at rest +7% (4pt)



# Microsoft Defender for Cloud | Security posture

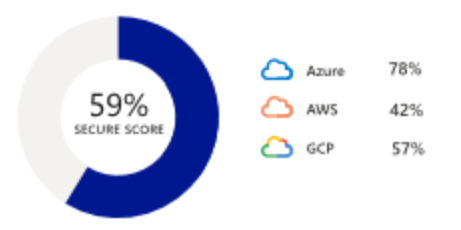
Showing 40 subscriptions

Secure score over time | Guides & Feedback

- General**
- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Community
- Cloud security**
- Security posture
- Regulatory compliance
- Workload protection
- Data governance (Purview/Mau)
- IoT
- Firewall manager
- DevOps
- CIEM
- API security
- ASM (Rome-RiskIQ)
- Management**
- Environment settings
- Security policy
- Security solution
- Workflow automation

## All environments

### Secure score



### Environment



### Governance



Environments: Azure AWS GCP

### See your score over time

Track the progress of your score with this workbook. View what's changed recently, scores for individual subscriptions, and other useful metrics.

[Go to workbook](#) | [Learn more](#)

Environment | Owner

Environment: All | Grace period: All

Name ↑↓	Secure score ↑↓	Unhealthy resources ↑↓	Recommendations ↑↓
<b>ASC Multi-Cloud Demo</b> Azure subscription	<b>35%</b>	153 of 454	<a href="#">View recommendations &gt;</a>
<b>Code generate Test</b> AWS account	<b>65%</b>	198 of 678	<a href="#">View recommendations &gt;</a>
<b>Contoso Infra3</b> Azure subscription	<b>65%</b>	98 of 154	<a href="#">View recommendations &gt;</a>
<b>Contoso Infra3</b> Azure subscription	<b>78%</b>	94 of 678	<a href="#">View recommendations &gt;</a>
<b>ASC Multi-Cloud Demo 213</b> Azure subscription	<b>53%</b>	165 of 198	<a href="#">View recommendations &gt;</a>
<b>Bing MM Measurement</b> Azure subscription	<b>53%</b>	65 of 254	<a href="#">View recommendations &gt;</a>



# Microsoft Defender for Cloud | Recommendations

Showing 40 subscriptions

Download CSV report Guides & Feedback

## General

- Overview
- Getting started
- Recommendations**
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

All recommendations Secure score recommendations

Use these recommendations to harden your resources. Each one has a description, steps to take and the affected resources. [Learn more >](#)  
 For the full details of a recommendation, select it from the list.



Search by subscription name Recommendation status: All Recommendation maturity: All Severity: All Resource type: All Response action: All Contains exemptions: All Environment: All Initiative: All [Reset filters](#)

Showing 1-15 of 140 items

Recommendation	Unhealthy resources	Resource health	Initiative	Actions
D diagnostic logs in Data Lake Analytics should be enabled	3 of 3 data lake analytics ac...	<div style="width: 100%; height: 10px; background-color: red;"></div>	ASB	
Container registries should use private link	8 of 8 container registries	<div style="width: 100%; height: 10px; background-color: red;"></div>	ASB, MyOrgDemoCustomPolicy	
Audit usage of custom RBAC rules	36 of 36 GCP compute engines	<div style="width: 100%; height: 10px; background-color: red;"></div>	HIPAA, ISO 27001 +2	
Key Vault keys should have an expiration date	1 of 1 key vault	<div style="width: 100%; height: 10px; background-color: red;"></div>	Azure CIS 1.1.0, Azure CIS 1.3.0	
Kubernetes Services Management API server should be configured with restricted access	15 of 15 managed clusters	<div style="width: 100%; height: 10px; background-color: red;"></div>	ASB	
Web apps should request an SSL certificate for all incoming requests	28 of 28 GCP GKE clusters	<div style="width: 100%; height: 10px; background-color: red;"></div>	ASB, Azure CIS 1.1.0 +2	
An activity log alert should exist for Create or Update Network Security Group Rule	2 of 2 azure resources	<div style="width: 100%; height: 10px; background-color: red;"></div>	Azure CIS 1.1.0, Azure CIS 1.3.0	
Diagnostic logs should be enabled in App Service	24 of 24 web applications	<div style="width: 100%; height: 10px; background-color: red;"></div>	ASB, Azure CIS 1.3.0 +1	
SSM agent should be installed on your AWS EC2 instances	3 of 3 AWS S3 service	<div style="width: 100%; height: 10px; background-color: red;"></div>		
AWS Security Hub should be enabled in every region in your AWS accounts	4 of 4 AWS Kubernetes	<div style="width: 100%; height: 10px; background-color: red;"></div>		
Storage account public access should be disallowed	173 of 173 storage accounts	<div style="width: 100%; height: 10px; background-color: red;"></div>	ASB, Azure CIS 1.1.0 +1	
Audit Windows machines that do not have a maximum password age of 70 days	42 of 42 azure resources	<div style="width: 100%; height: 10px; background-color: red;"></div>	ISO 27001, NIST 800-53 +1	
Audit Windows machines that allow re-use of the previous 24 passwords	21 of 21 azure resources	<div style="width: 100%; height: 10px; background-color: red;"></div>	ISO 27001, NIST 800-53 +1	

# Amazon S3 permissions granted to other AWS accounts in bucket policies should be restricted

Open query

Severity **High** Freshness interval 6 Hours

**Description**  
 Implementing least privilege access is fundamental to reducing security risk and the impact of errors or malicious intent. If an S3 bucket policy allows access from external accounts, it could result in data exfiltration by an insider threat or an attacker. The 'blacklistedactionpatterns' parameter allows for successful evaluation of the rule for S3 buckets. The parameter grants access to external accounts for action patterns that are not included in the 'blacklistedactionpatterns' list.

**Remediation steps**

**Affected resources**

Unhealthy resources (0) Healthy resources (22) Not applicable resources (0)

Search AWS resources

Name	↑↓ AWS Account	Connector name	Region	Resource type
testbucketdelete548	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
sentinel-bucket-for-logs-us-west-2	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
sentinel-bucket-for-logs-us-east-2	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
s3-flow-logs-us-east-2	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
s3-cloudwatch-us-west2	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
ninjas3awsconfig	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
lianabucketdemo	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
daily-billing-report-ms	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
contoso-hotel-sentinel-s3-bucket	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
contoso-hotel-partner-sentinel-s3-bucket	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
contoso-financialresults	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
config-bucket-424151343163	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
cloudsa3-permision-test-424151343163-co4bkn	424151343163	AWSNinjaConnector	global	AWS S3 Bucket

Trigger logic app

# Microsoft Defender for Cloud | Workload protections

Showing 54 subscriptions

Search Subscriptions What's new

- General
  - Overview
  - Getting started
  - Recommendations
  - Security alerts
  - Inventory
  - Workbooks
  - Community
  - Diagnose and solve problems
- Cloud security
  - Secure score
  - Regulatory compliance
  - Workload protection
  - Firewall manager
- Management
  - Environment settings
  - Security solution
  - Workflow automation

## Defender for Cloud coverage



**216/225**  
Servers  
[Upgrade](#)

**51/51**  
App service  
[Upgrade](#)

**21/30**  
Containers  
[Upgrade](#)

**40/40**  
Key vaults  
[Upgrade](#)

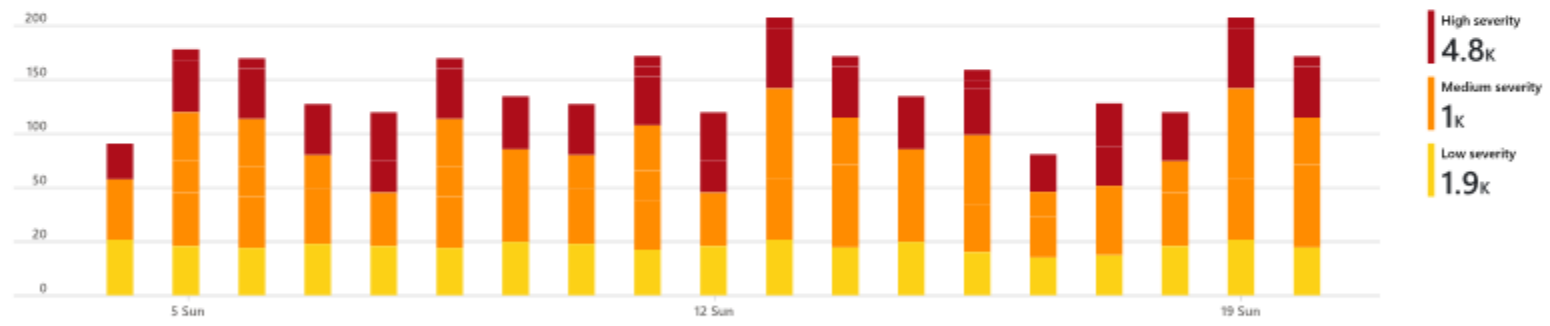
**27/27**  
Azure SQL database servers  
[Upgrade](#)

**195/209**  
Storage  
[Upgrade](#)

**12/12**  
Resource manager subscriptions  
[Upgrade](#)

**12/12**  
DNS subscriptions  
[Upgrade](#)

## Security alerts



## Advance protection

VM vulnerability assessment 127 Unprotected	Just-in-time VM Access 70 Unprotected	Adaptive application control 44 Unprotected	Container image scanning 6 Unprotected
SQL vulnerability assessment	File integrity monitoring	Network map	IoT security

## Insights

### Upgrade to New Containers plan

Cloud-native **Kubernetes security** capabilities including environment hardening, vulnerability assessment, and run-time threat protection. The **new plan** merges two existing Defender plans, in addition to new and improved features.

[Click here to upgrade >](#)

### Most prevalent recommendations

- [Audit diagnostic setting](#) 619 Resources
- [Storage account public access should...](#) 161 Resources
- [A vulnerability assessment solution...](#) 107 Resources

### Most attacked resources

- contoso5.cloudapp.net 63 Alerts
- Virtual machine 2 41 Alerts
- CentOS 28 Alerts

[View full alert list >](#)

### Controls with the highest potential increase

- Remediate vulnerabilities +11% (6pt)
- Enable encryption at rest +7% (4pt)
- Remediate security configurations +6% (4pt)

[View controls >](#)

# Microsoft Defender for Cloud | Security alerts

Showing subscription 'CyberSecSOC'

- General
  - Overview
  - Getting started
  - Recommendations
  - Security alerts**
  - Inventory
  - Workbooks
  - Community
  - Diagnose and solve problems
- Cloud Security
  - Secure Score
  - Regulatory compliance
  - Workload protections
  - Firewall Manager
- Management
  - Environment settings
  - Security solutions
  - Workflow automation

Refresh
Change status
Open query
Suppression rules
Security alerts map
Sample alerts
Alerts workbook
Download CSV report
Guides & Feedback



Subscription == All
Status == Active
Severity == Low, Medium, High
Add filter

Severity	Alert title	Affected resource	Activity start time (UTC-7)	MITRE ATT&CK® tactics	Status
High	Invalid SMB Message (DoublePulsar Backdoor Implant)	cybersecurityiothub	03/19/22, 10:00 PM		Active
High	Suspicion of NotPetya Malware - Illegal SMB Parameters Detected	cybersecurityiothub	03/19/22, 10:00 PM		Active
High	Suspicion of NotPetya Malware - Illegal SMB Transaction Detected	cybersecurityiothub	03/19/22, 10:00 PM	Lateral Movement	Active
High	Suspected brute-force attack attempt	ninjasqlattack	03/19/22, 09:00 PM	Pre-attack	Active
High	Suspicion of Malicious Activity (BlackEnergy)	cybersecurityiothub	03/18/22, 07:00 PM	Command and Control	Active
High	Unauthorized Internet Connectivity Detected	cybersecurityiothub	03/18/22, 07:00 PM	Initial Access	Active
High	Port Scan Detected	cybersecurityiothub	03/18/22, 07:00 PM	Discovery	Active
High	Excessive SMB login attempts	cybersecurityiothub	03/18/22, 07:00 PM		Active
High	No Traffic Detected on Sensor Interface	cybersecurityiothub	03/18/22, 06:00 PM		Active
High	Suspected brute-force attack attempt	ninjasql <span>Secret</span>	03/17/22, 09:00 PM	Pre-attack	Active
High	Suspected brute-force attack attempt	ninjasql <span>Secret</span>	03/15/22, 09:00 PM	Pre-attack	Active
High	Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)	aws-eks-cluster-eks-protected-demo-us-east-2	03/15/22, 07:19 AM		Active
High	Mimikatz credential theft tool	EC2AMAZ-HK672QP	03/15/22, 04:30 AM	Credential Access	Active
High	Mimikatz credential theft tool	EC2AMAZ-HK672QP	03/15/22, 04:30 AM	Credential Access	Active
High	Mimikatz credential theft tool	EC2AMAZ-HK672QP	03/15/22, 04:29 AM	Credential Access	Active
High	Mimikatz credential theft tool	EC2AMAZ-HK672QP	03/15/22, 04:29 AM	Credential Access	Active
High	Mimikatz credential theft tool	EC2AMAZ-HK672QP	03/15/22, 04:28 AM	Credential Access	Active
High	Mimikatz credential theft tool	EC2AMAZ-HK672QP	03/15/22, 04:28 AM	Credential Access	Active