Remove before presenting

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

Microsoft Security

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

Securing multi-cloud

What's top of mind

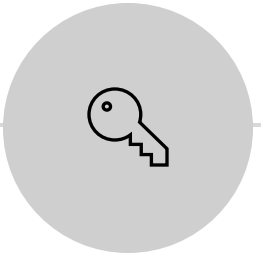
Visibility into security and compliance

52% of organizations cite secure configuration of cloud resources as a top priority.[1]

Protect against increasing, sophisticated attacks

$4.24M is the average cost of a breach, 2021.[2]

Manage access and permissions for users and applications



1,295 different cloud services are used by enterprises, on average.[3]

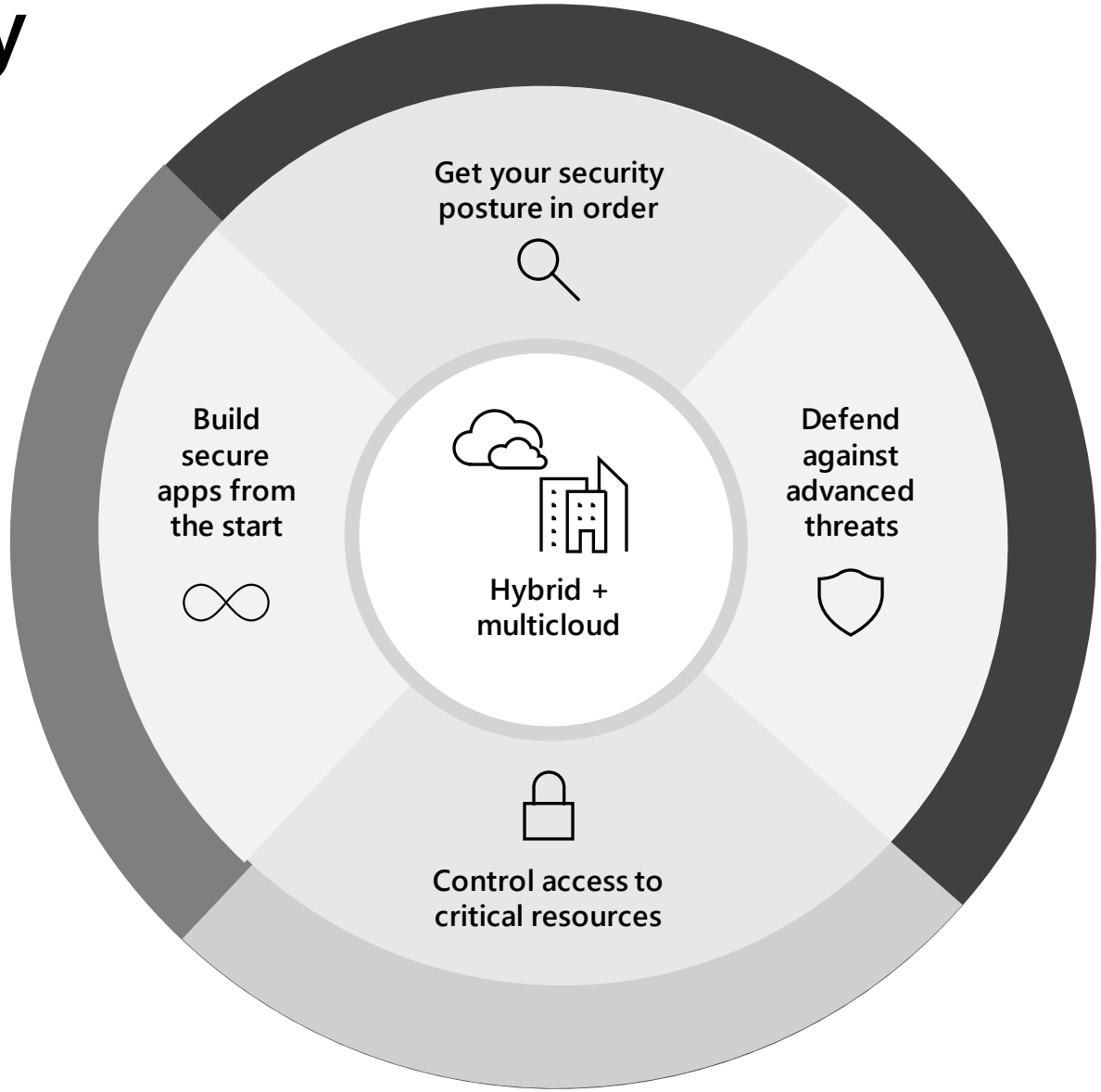
Develop and operate secure apps in the cloud

83% of code vulnerabilities are caused by developer error.[4]

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

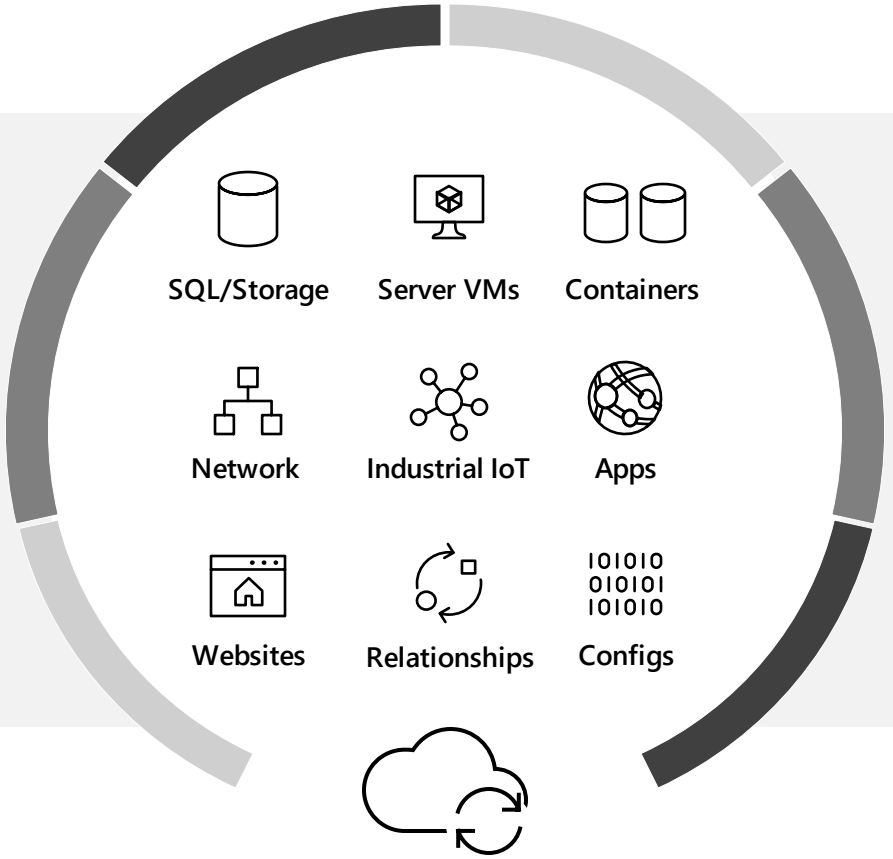
Easily assess and improve the secure configuration of your critical multi-cloud resources

Security Posture Management

Cross-cloud visibility

Secure Score recommendations

Industry benchmarks and compliance



External Attack Surface Management

Discovery of external facing assets

Continuous risk assessment

Prioritized remediation

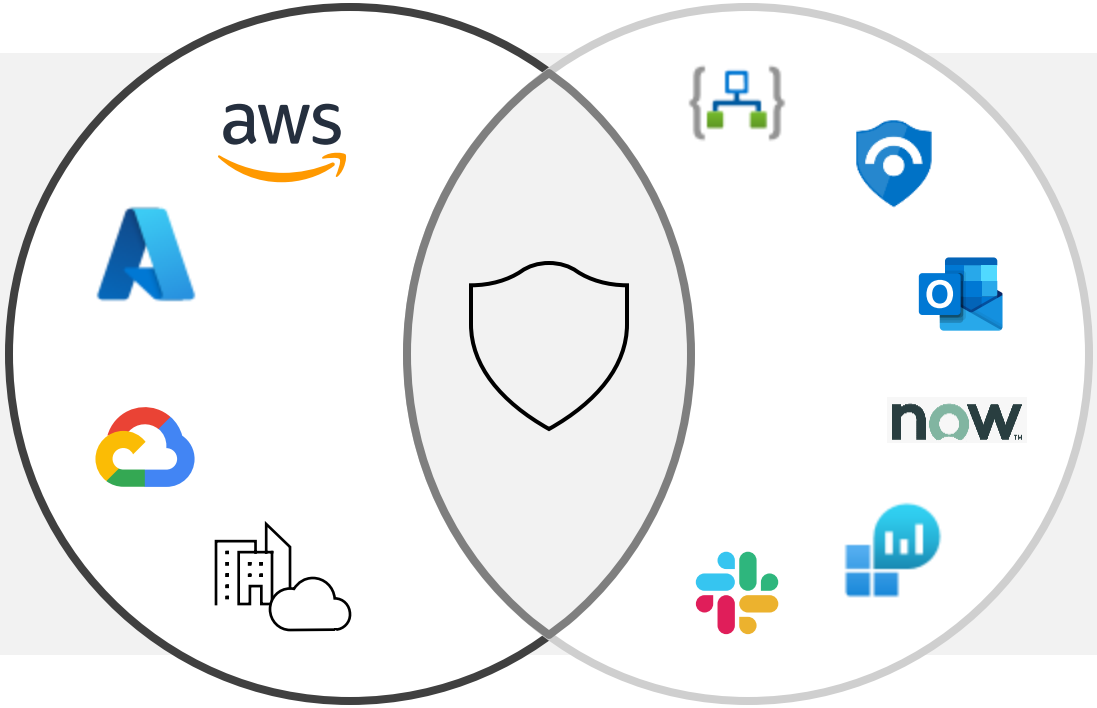
Protect workloads against advanced threats

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

Detect threats and protect your workloads

Assess and remediate vulnerabilities

Protect full stack of workloads



Respond and automate

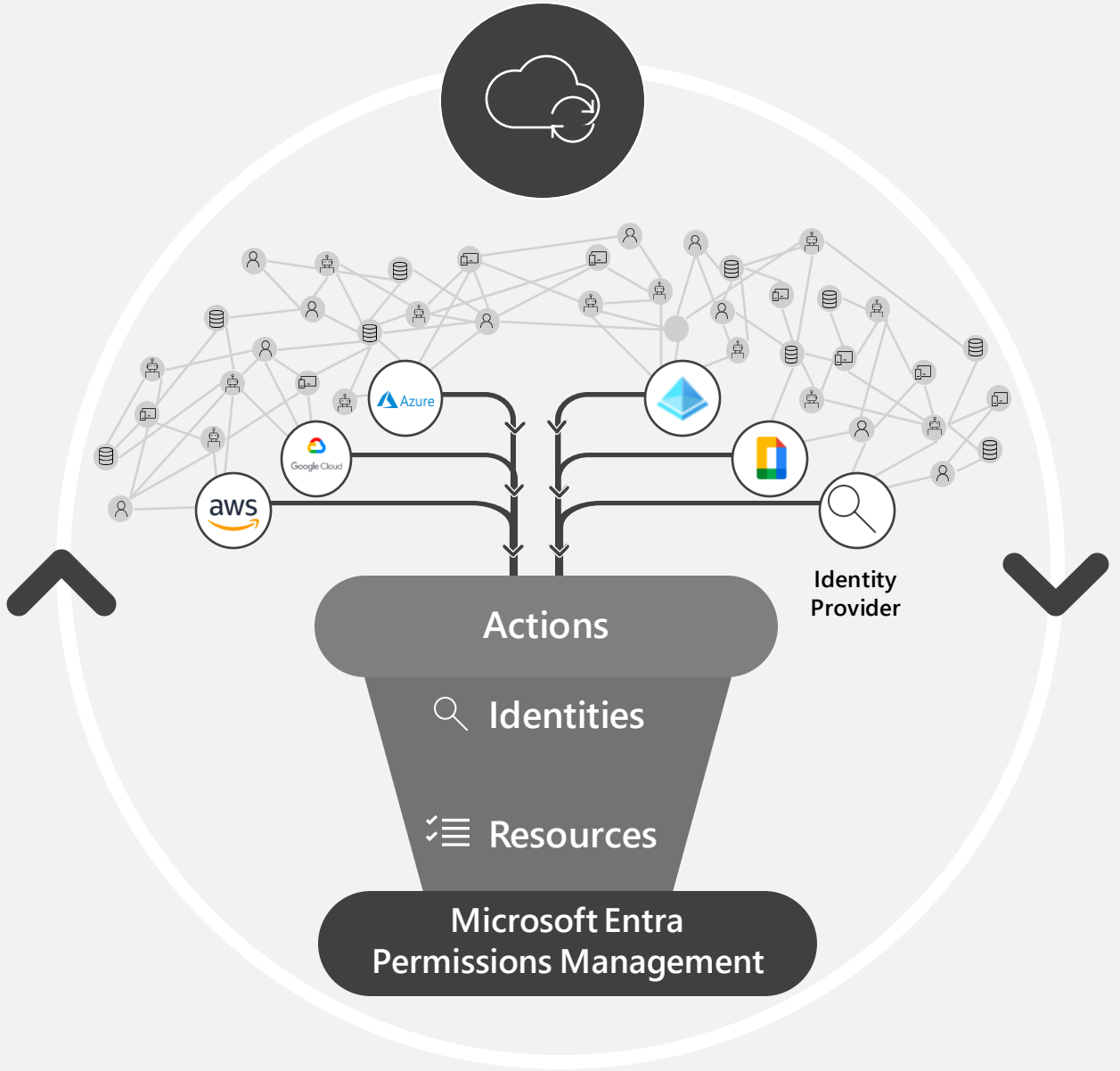
Get actionable, prioritized alerts

Automate with your choice of tools

Manage access & permissions to apps

Control access to critical resources and protect assets

- Actions
- Identities
- Resources
- Microsoft Entra Permissions Management

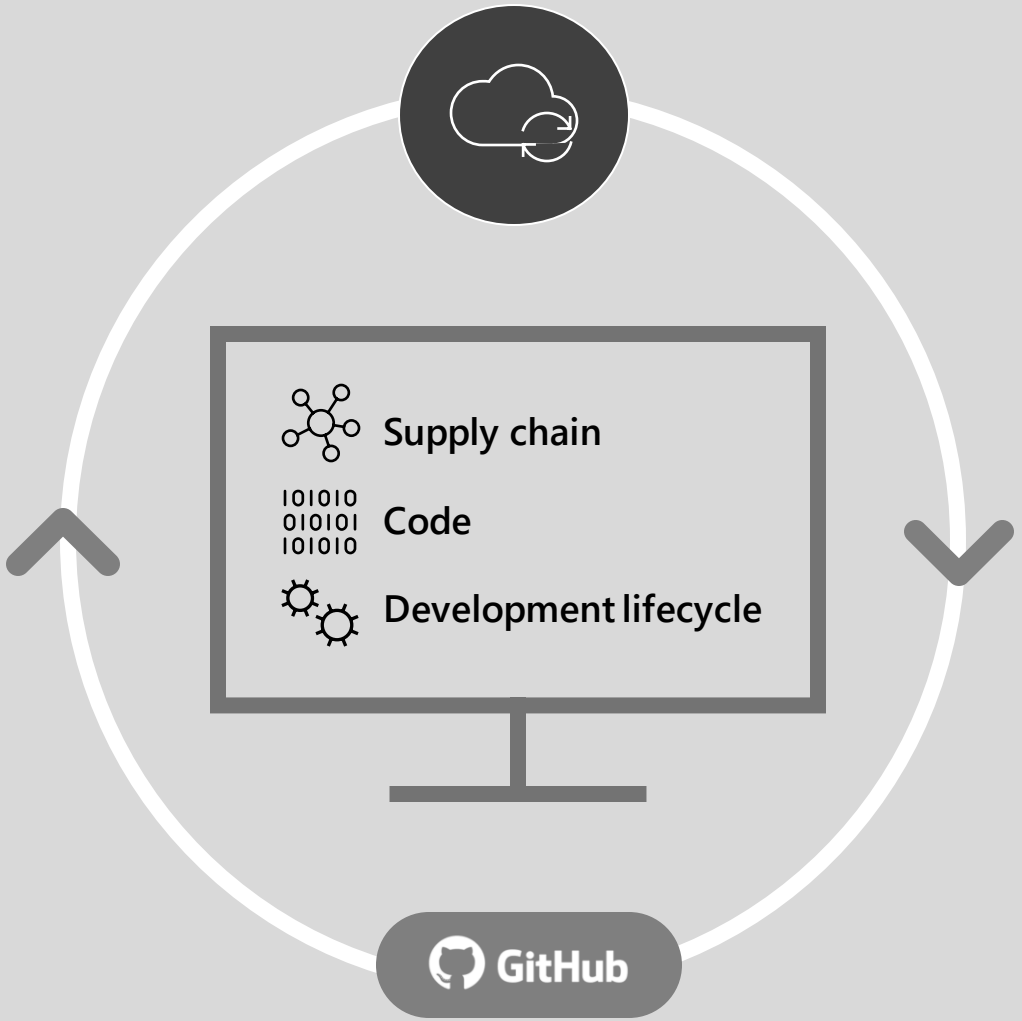


Cloud infrastructure entitlement management

Build secure apps in the Cloud

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

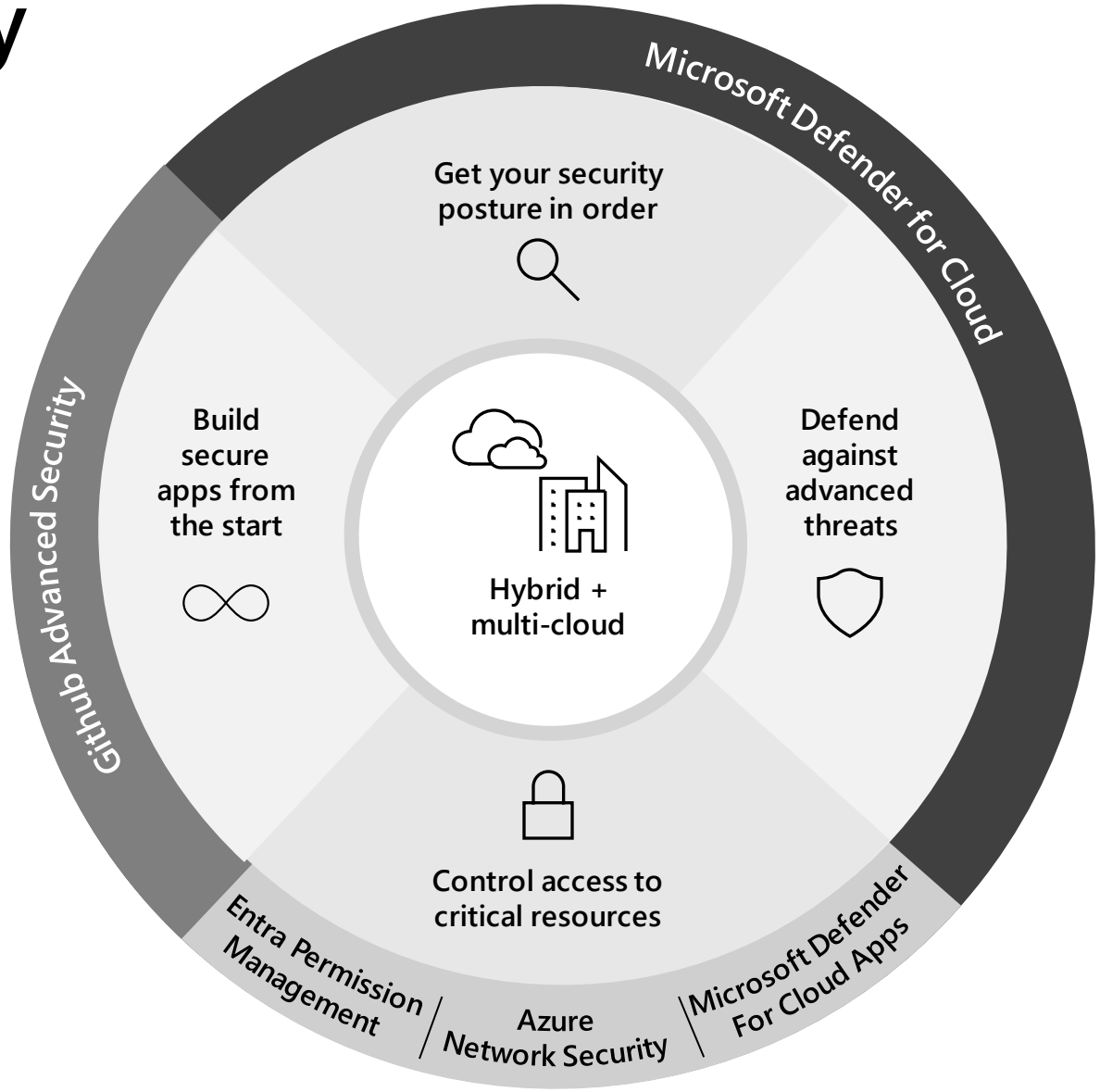
- **Develop securely, from idea to ship**
- **Fix the vulnerabilities that matter the most for your organization in minutes**
- **Trust your software with an end-to-end, automated security solution**



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

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+[3]

Threat groups

40+[3]

Nation state-groups

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

43T[1]

Analyzing

Threat signals daily

50% increase

32B[1]

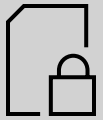
Blocking

email threats annually

$20B[1]

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[4]

partners in security ecosystem

785K[2]

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

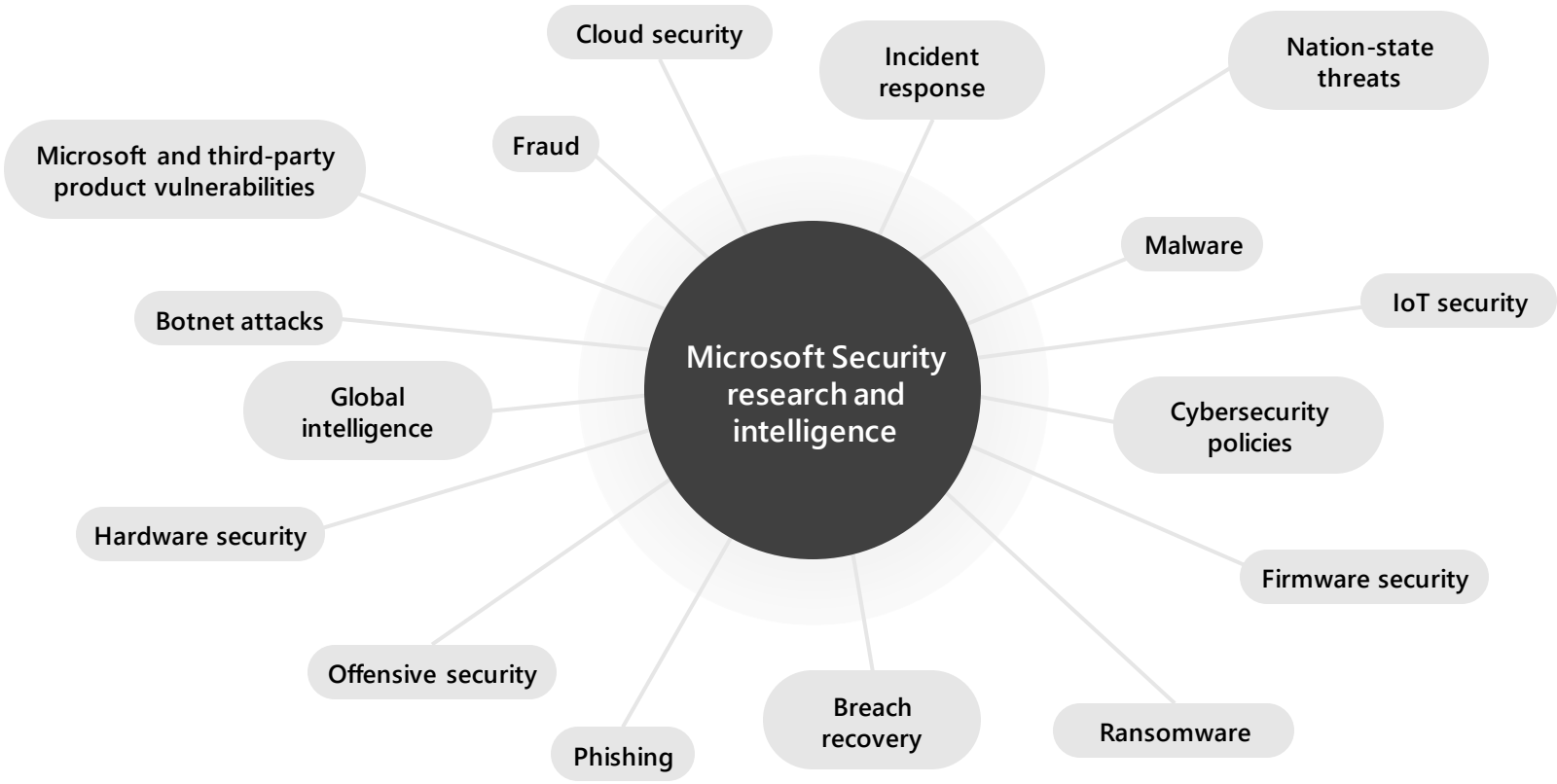
Augment your security teams with Microsoft's world-class research and intelligence teams

8,500+[1]

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.

Source:
1. Cyber Signals Blog

[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

Microsoft Security

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!

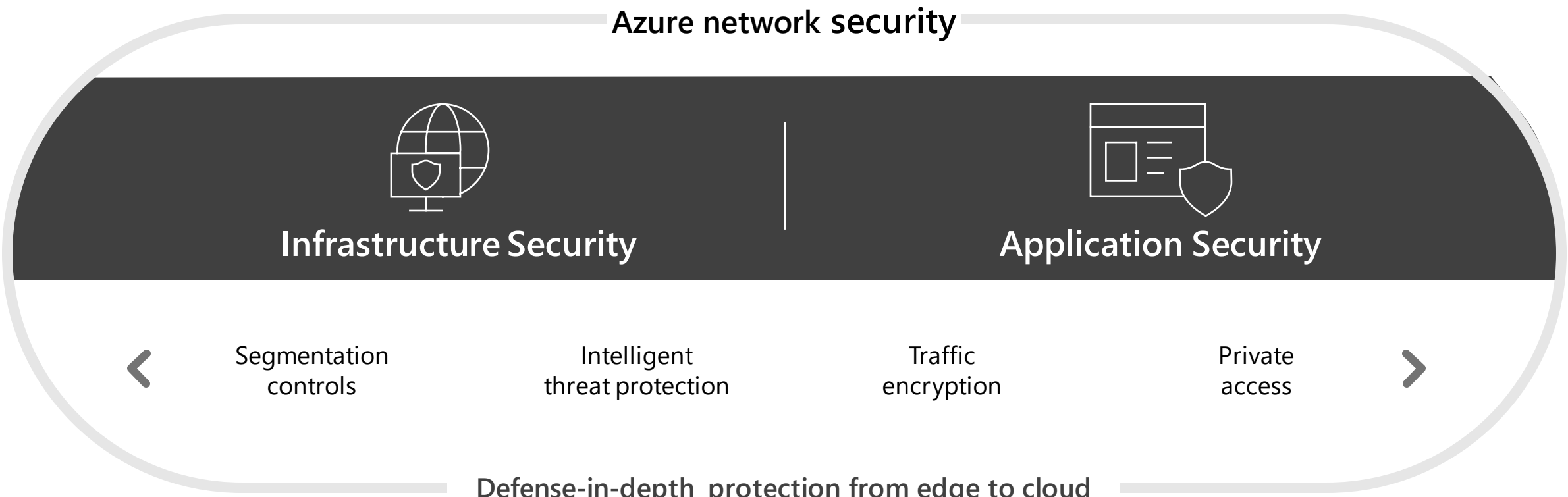
Partner Logo

Thank you

Microsoft Security

Control access and secure your network infrastructure and applications

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



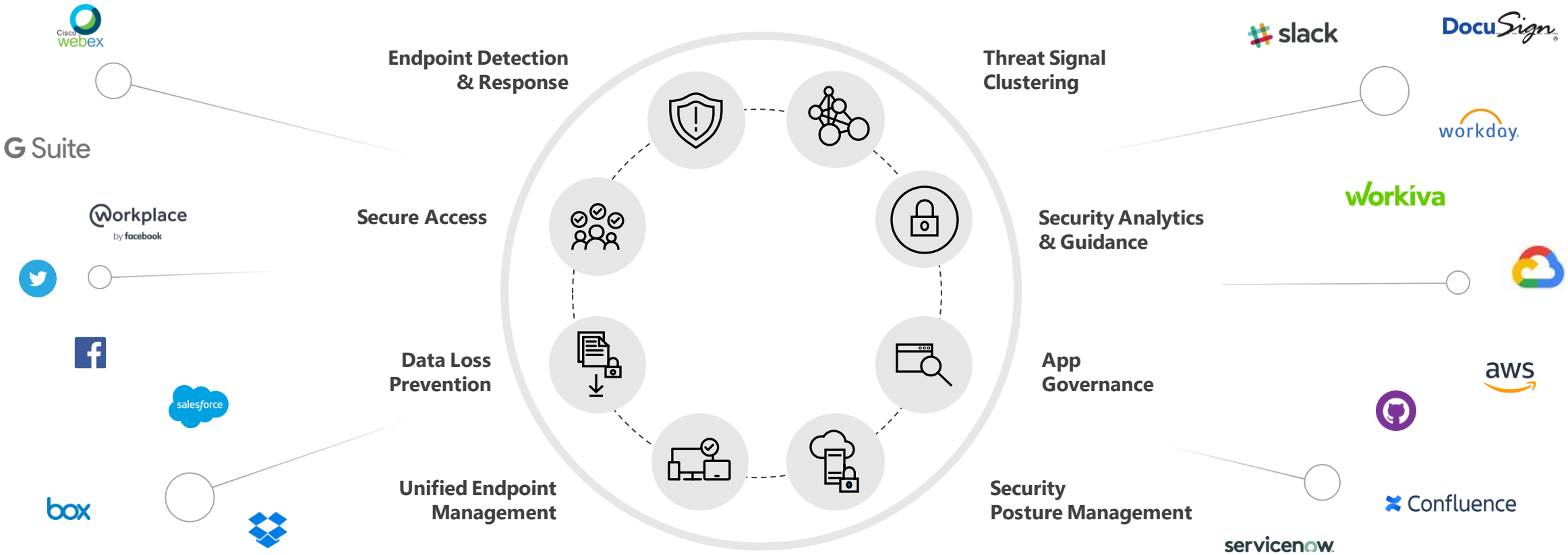
Microsoft Defender for Cloud Apps

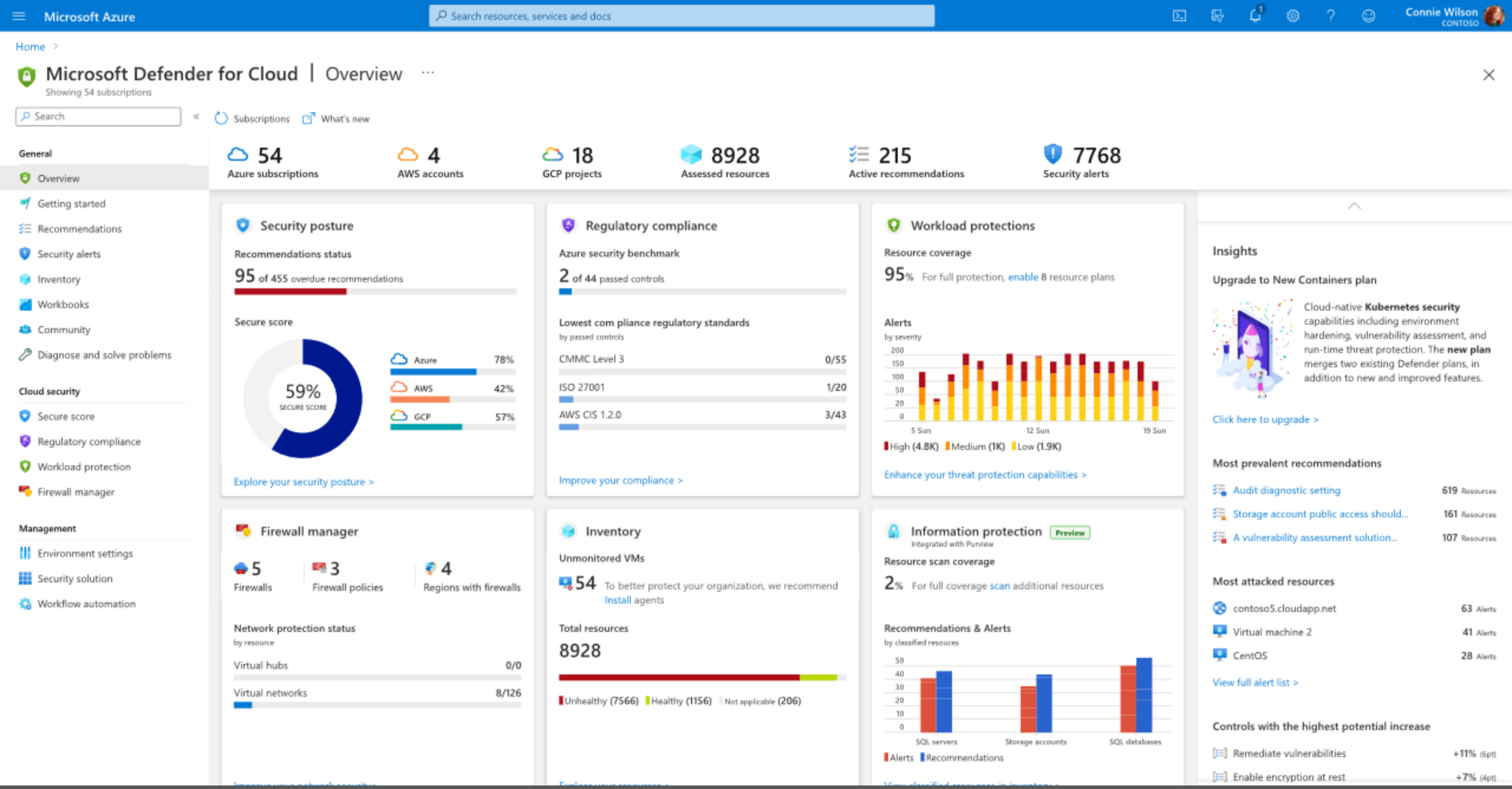
The go-to CASB for all your cloud enablement, monitoring and governance

Simple deployment

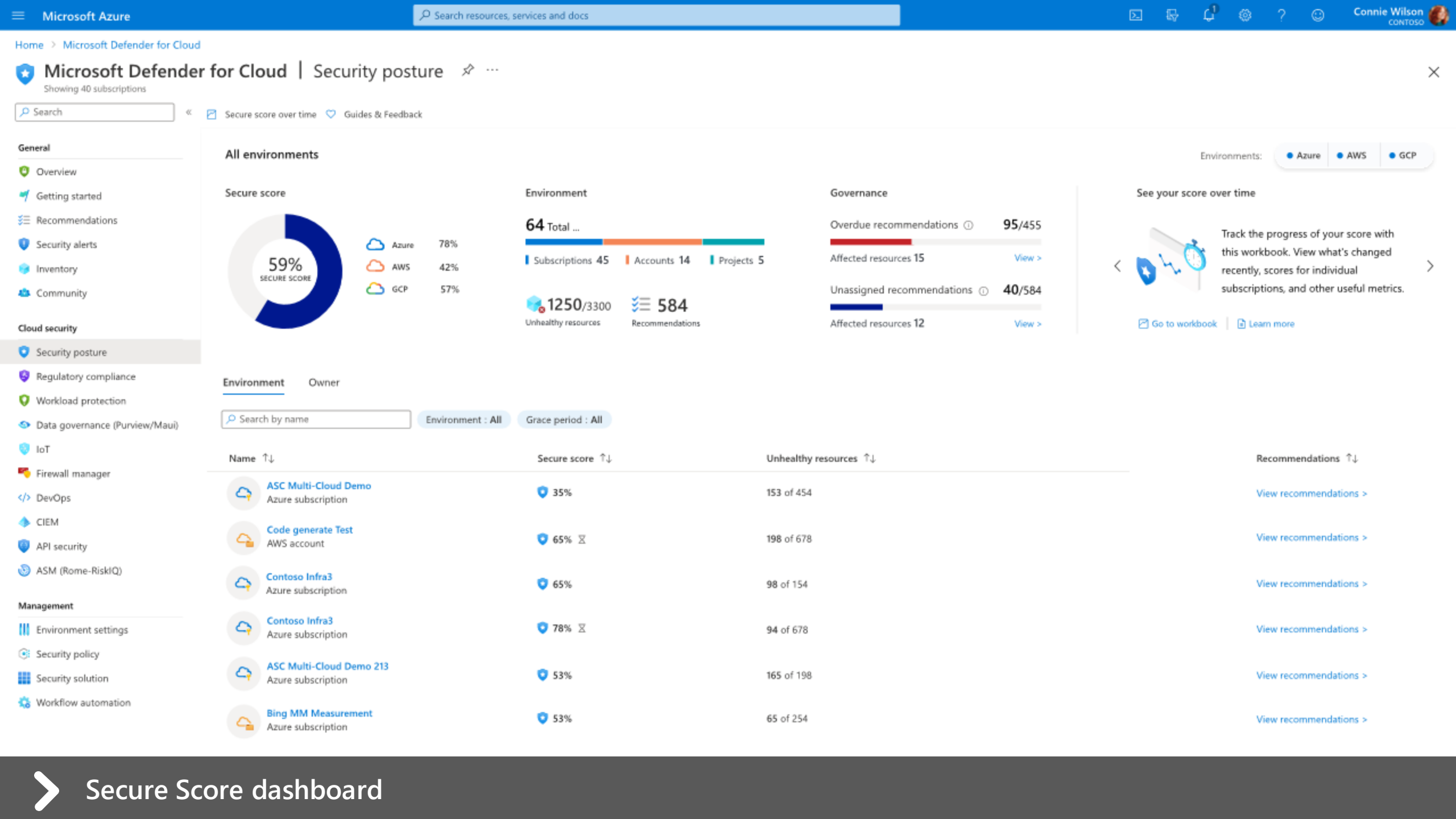
Natively integrated across the broader Microsoft product stack to deliver unique capabilities

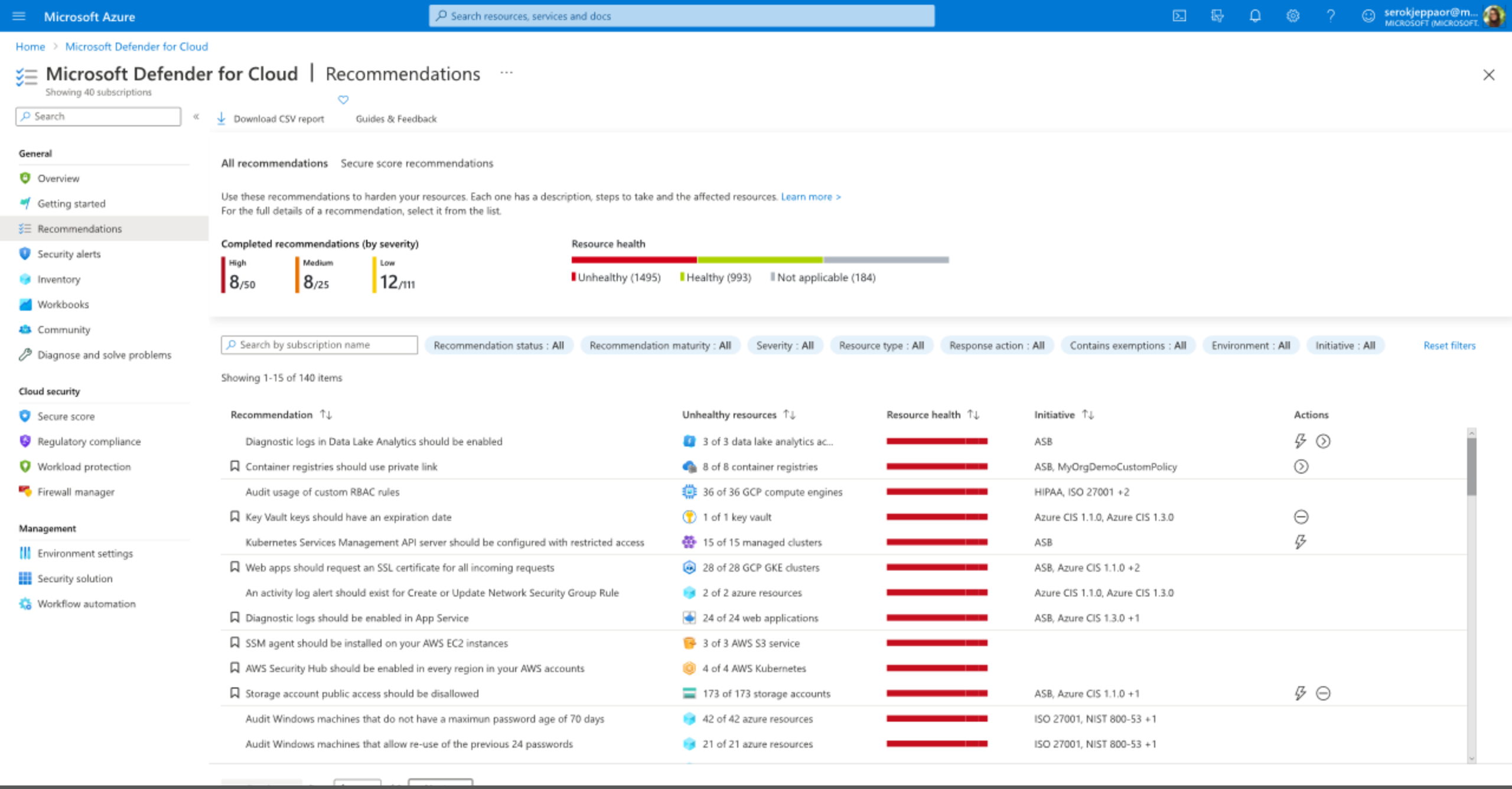
Rooted in supporting any app





Microsoft Defender for Cloud dashboard


Microsoft Azure
Search resources, services and docs
Connie Wilson
CONTOSO
Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Security posture
Showing 40 subscriptions
Search
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/Maui)
IoT
Firewall manager
DevOps
CIEM
API security
ASM (Rome-RiskIQ)
Management
Environment settings
Security policy
Security solution
Workflow automation
All environments
Environments:
Azure
AWS
GCP
Secure score
59%
SECURE SCORE
Azure 78%
AWS 42%
GCP 57%
Environment
64 Total ...
Subscriptions 45
Accounts 14
Projects 5
1250/3300
Unhealthy resources
584
Recommendations
Governance
Overdue recommendations
95/455
Affected resources 15
View >
Unassigned recommendations
40/584
Affected resources 12
View >
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
Search by name
Environment : All
Grace period : All
Name
Secure score
Unhealthy resources
Recommendations
ASC Multi-Cloud Demo
Azure subscription
35%
153 of 454
View recommendations >
Code generate Test
AWS account
65%
198 of 678
View recommendations >
Contoso Infra3
Azure subscription
65%
98 of 154
View recommendations >
Contoso Infra3
Azure subscription
78%
94 of 678
View recommendations >
ASC Multi-Cloud Demo 213
Azure subscription
53%
165 of 198
View recommendations >
Bing MM Measurement
Azure subscription
53%
65 of 254
View recommendations >
Secure Score dashboard



Multicloud recommendations

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

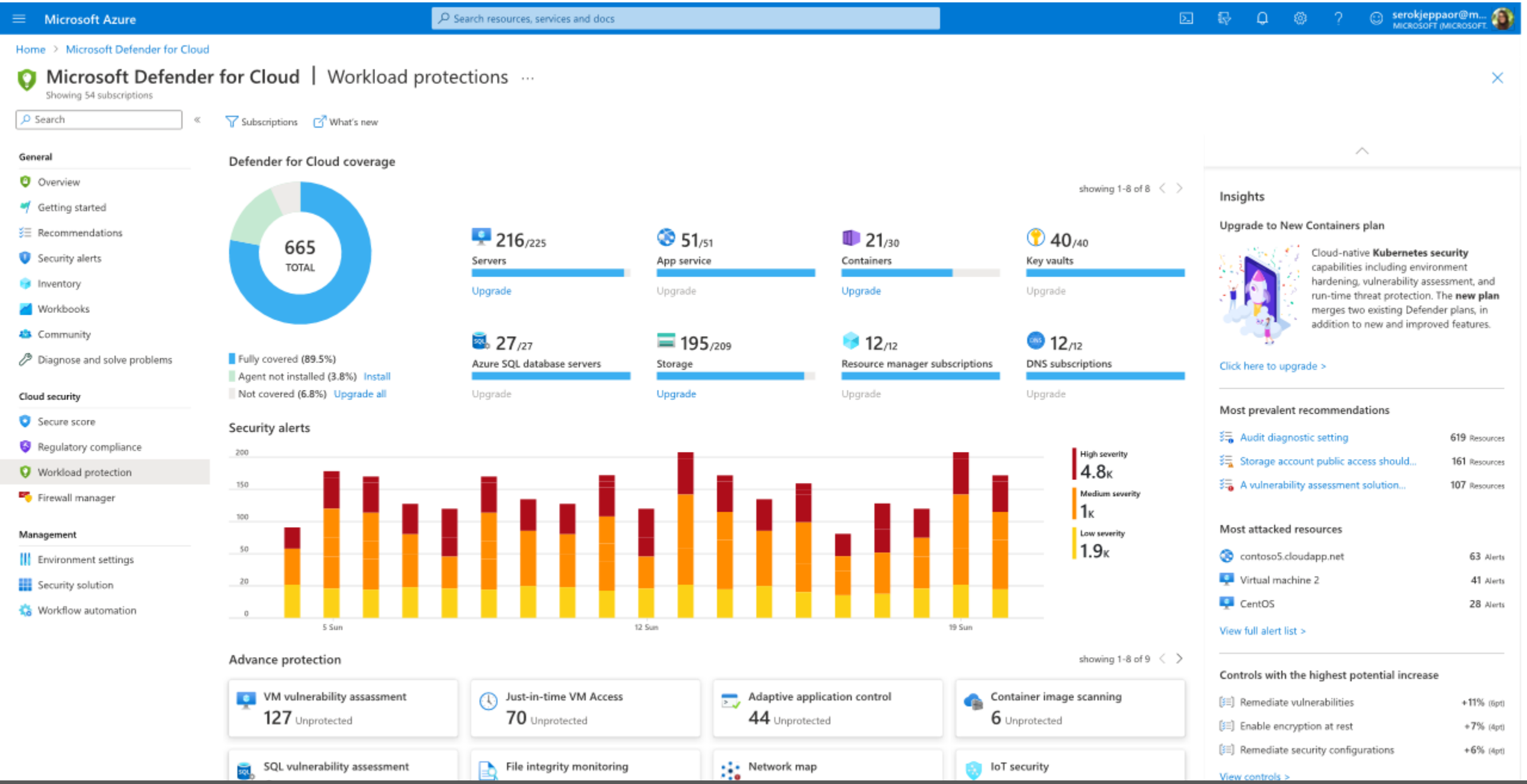
Unhealthy resources (0) | Healthy resources (22) | Not applicable resources (0)

Search AWS resources

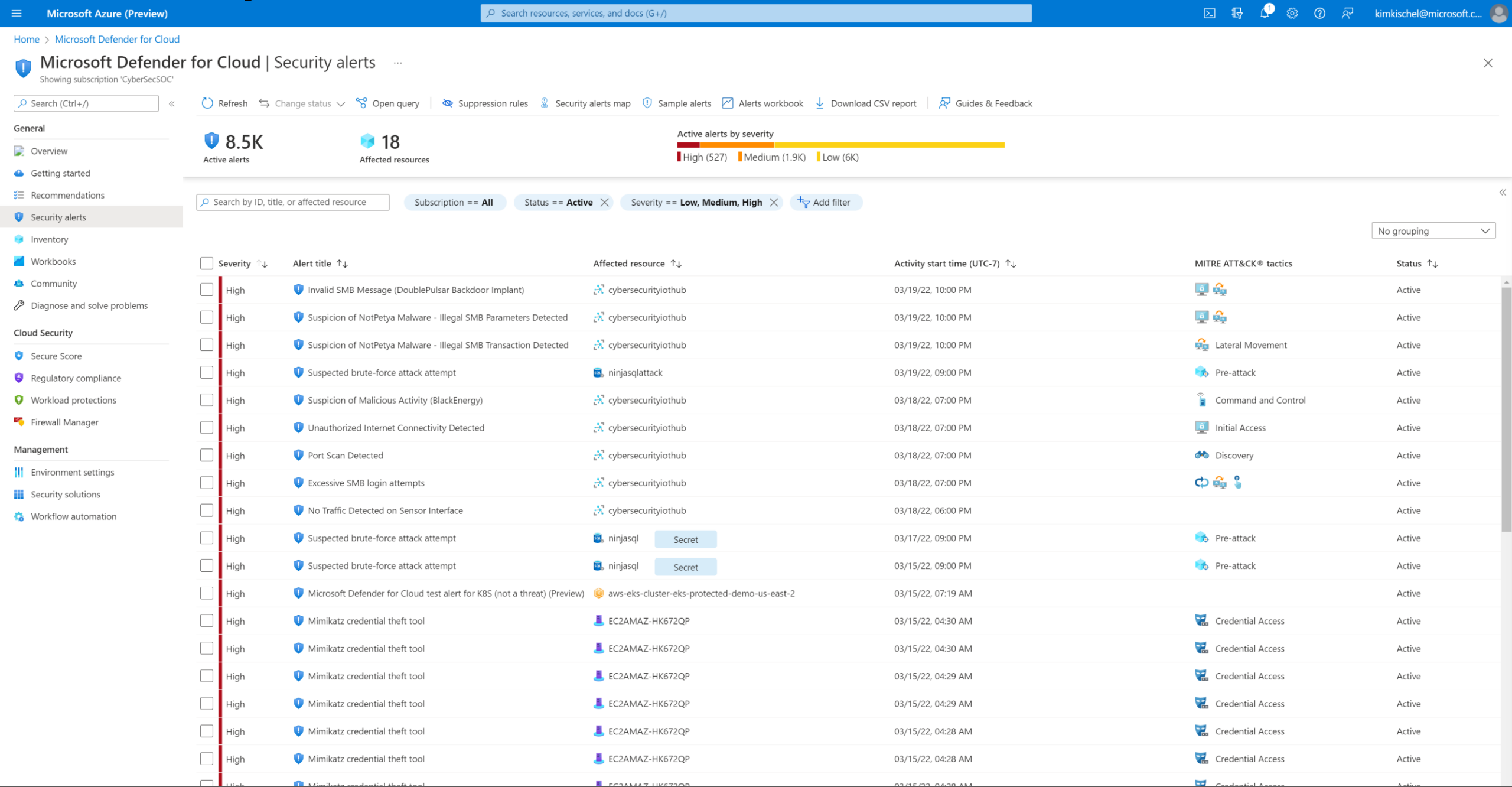
Name	AWS Account	Connector name	Region	Resource type
testbucketdelete548	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
sentinel-bucket-for-logs-us-west-2	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
sentinel-bucket-for-logs-us-east-2	424151343163	AWSNinjaConnector	global	AWS S3 Bucket
s3-fllow-logs-us-east-2	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-bocket	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
cloudsaga-permission-test-424151343163-so4bkp	424151343163	AWSNinjaConnector	global	AWS S3 Bucket

Trigger logic app

Recommendation details view



Workload protection overview



Security Alerts view