Microsoft Security

Microsoft Defender for Cloud

Protect your multicloud and hybrid environments

Alex Steele and Fernanda Vela
Microsoft Defender for Cloud Product Managers

Cloud security is more important than ever

Cloud migration involves ongoing on-prem (hybrid) and multicloud resources, expanding the attack surface

Increasing complexity of in the development and deployment of cloud applications

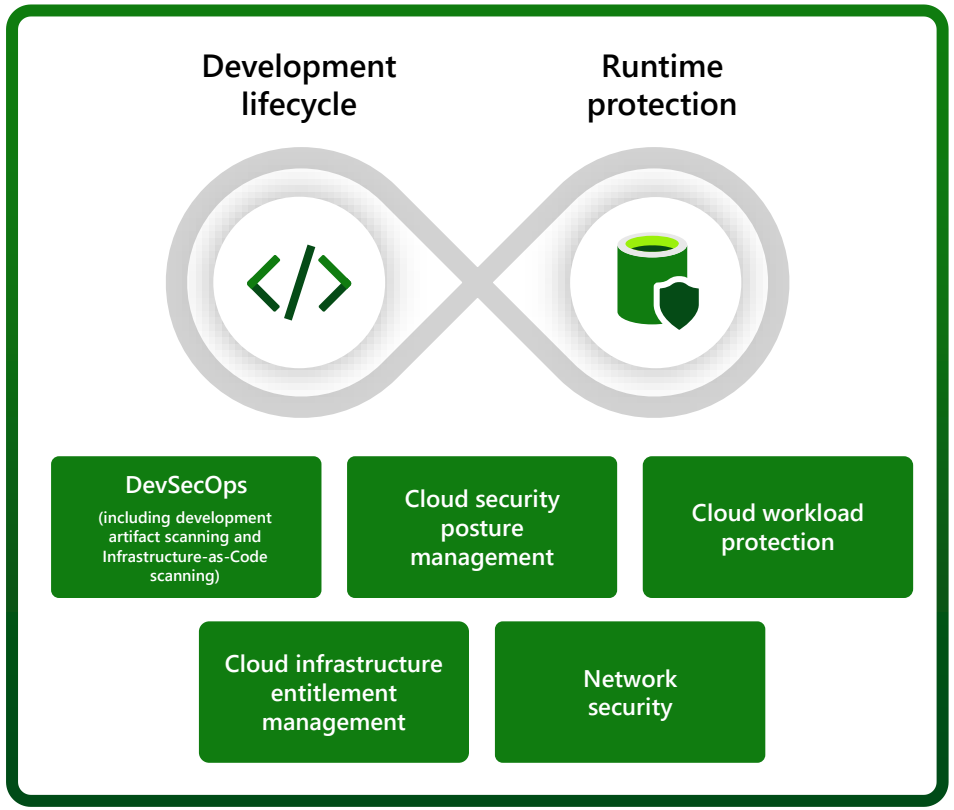
Complex and dynamic regulatory landscape

Microsoft's cloud-native application protection platform (CNAPP)

Get integrated protection for your multicloud resources, app, and data.
Named by Gartner as a representative CNAPP provider in its 2023 Market Guide[1].

Hybrid and multicloud

- Code
- Compute
- Identity
- Data
- Storage



Unified security and compliance capabilities to help prevent, detect, and respond to modern cloud security threats across the entire cloud app lifecycle

1 Gartner®, Market Guide for Cloud-Native Application Protection Platforms, March 14, 2023. Neil MacDonald, et al.

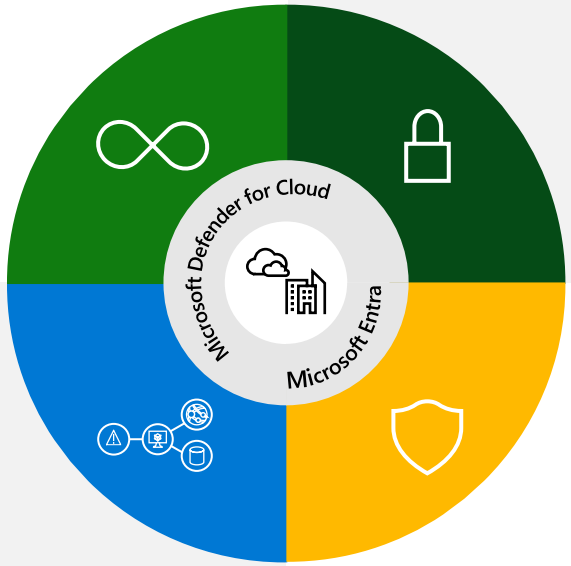
Microsoft's cloud-native application protection platform (CNAPP)

DevSecOps

Unify your DevOps security management across multi-pipelines

Cloud infrastructure entitlement management

Enforce principle of least privilege across multicloud with CIEM



Cloud security posture management

Visibility and contextual insights to identify and help remediate your most critical risk

Cloud workload protection

Help detect and respond to modern threats across your cloud workloads in runtime

Integrated to protect across your cloud infrastructure

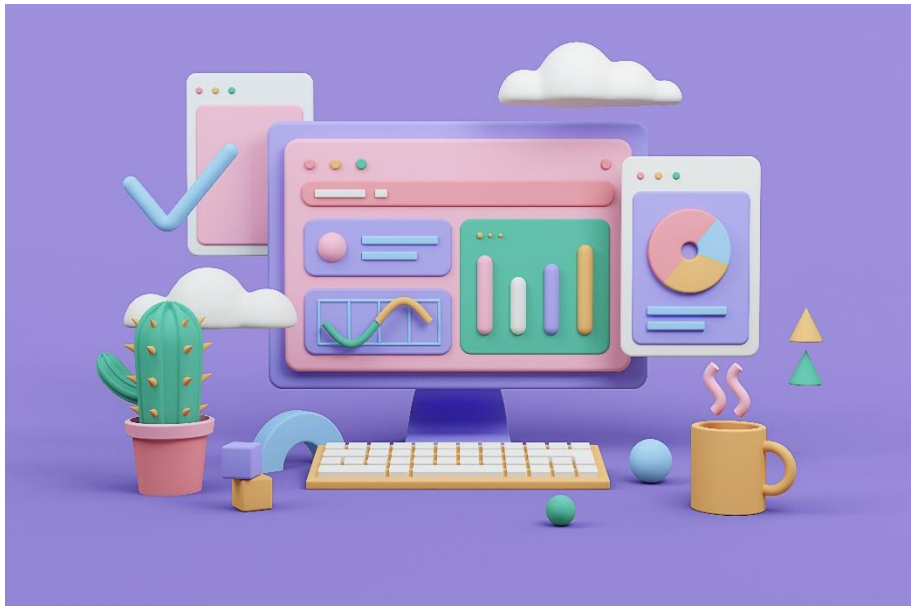
Microsoft Purview (Data Security)	Microsoft Defender External Attack Surface Management (EASM)	Azure Network Security	Microsoft Sentinel (SIEM)

Log Analytics Workspace

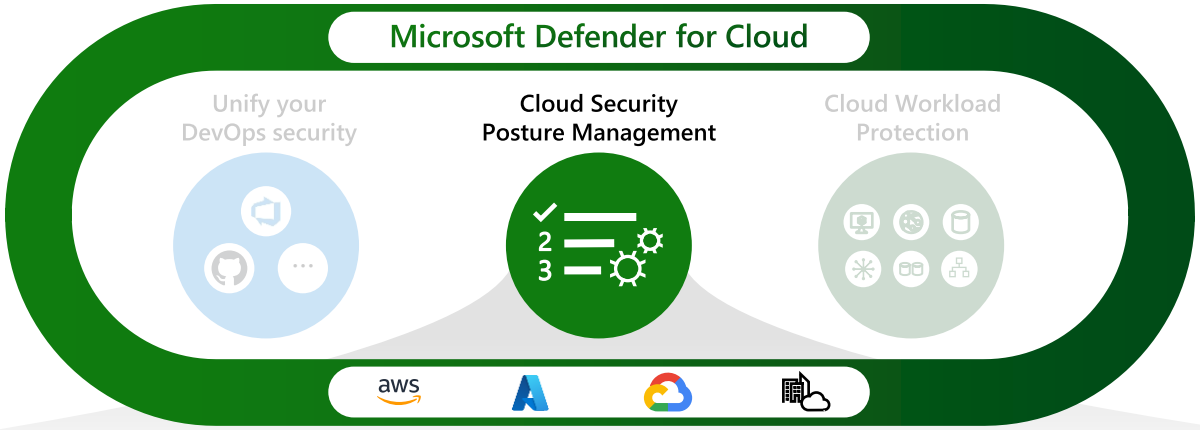
Defender for Cloud collects data from your Azure virtual machines (VMs), Virtual Machine Scale Sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.

The agent collects various security-related configuration details and event logs from connected machines, and then copies the data to your Log Analytics workspace for further analysis.

Examples: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.



Cloud security posture management



Foundational CSPM (free)

Asset inventory and secure score analysis
Frictionless onboarding | +450 built-in assessments | Custom capabilities | Policy management

Advanced remediation
Quick-fix remediation | Automated remediation using LogicApps | Enforcement policies

Data export and out-of-the-box reporting
Built in Azure Workbooks | At-scale data streaming and export | Integration with SIEM/SOAR solutions

Integrated workflows and automation
Out-of-the-box and custom automations triggered by security events

Defender CSPM

Agentless vulnerability scanning
Visibility on software and CVEs | Disc snapshots | Insecure secrets and keys

Integrated data and insights
Defender for DevOps | Defender External Attack Surface Management | Entra Permissions Management

Contextual cloud security and risk prioritization
Attack path analysis | Intelligent cloud security graph | Custom path queries on cloud security explorer | Risk-based prioritization

Regulatory compliance and industry benchmarks
Over 50 standards | Multicloud Microsoft security benchmark | Compliance dashboard and reporting | Integration with Microsoft Purview compliance manager

Governance management
Assign owners automatically | Drive accountability in the organization | Grace period | Reduce time to remediate

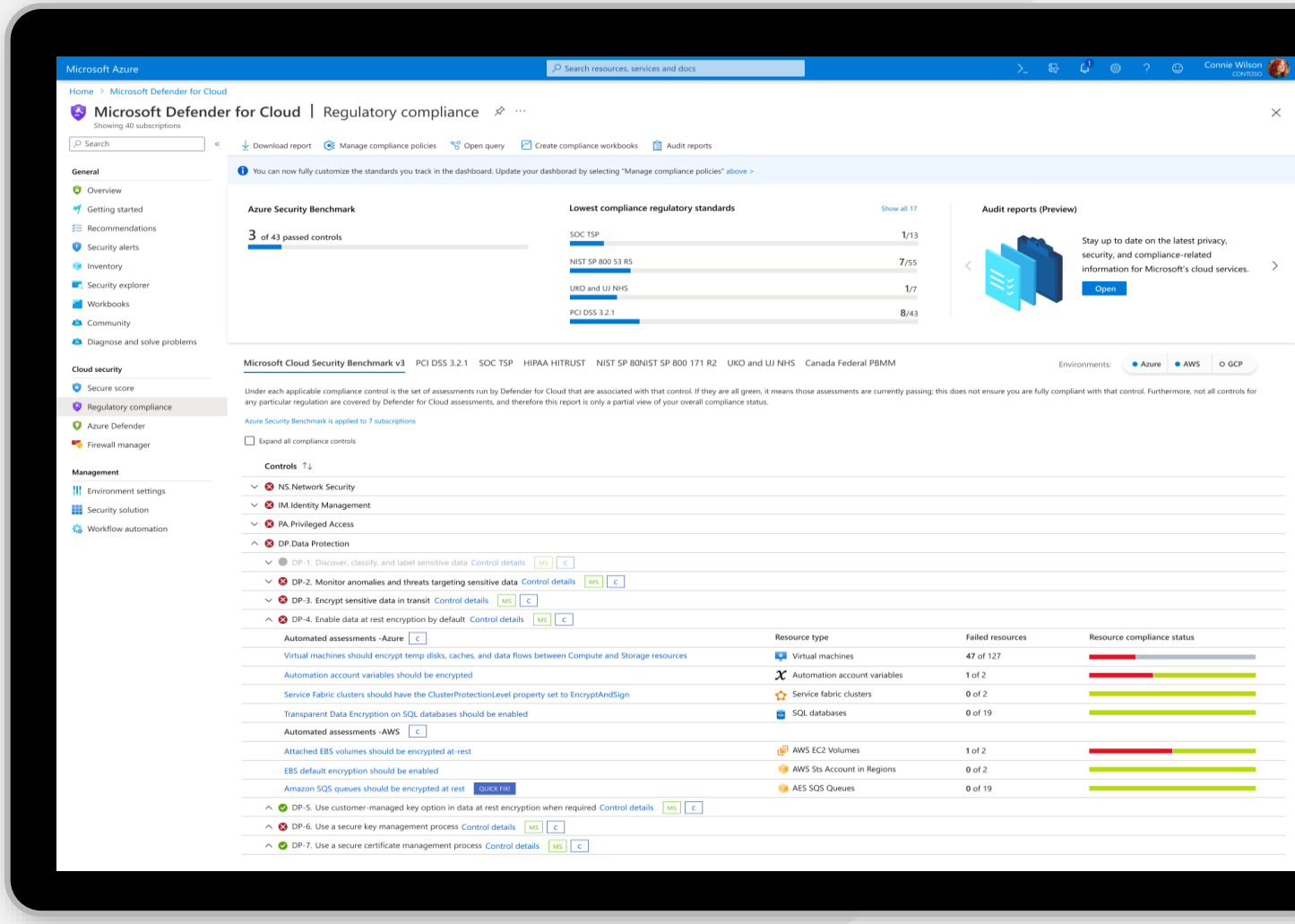
Data-aware security posture
Multicloud data estate discovery | Identify data flows and resources containing sensitive and shadow data | Uncover potential sensitive data exposure and data breaches

Multicloud security benchmark for compliance assessment and management

- Assess and manage your compliance status with a continuous assessment of your cloud resources across AWS, Azure, and GCP in a single, integrated dashboard
- Use industry standards, regulatory compliance frameworks, and vendor provided cloud-specific benchmarks to implement security and compliance best practices
- Create custom recommendations to meet unique organizational needs

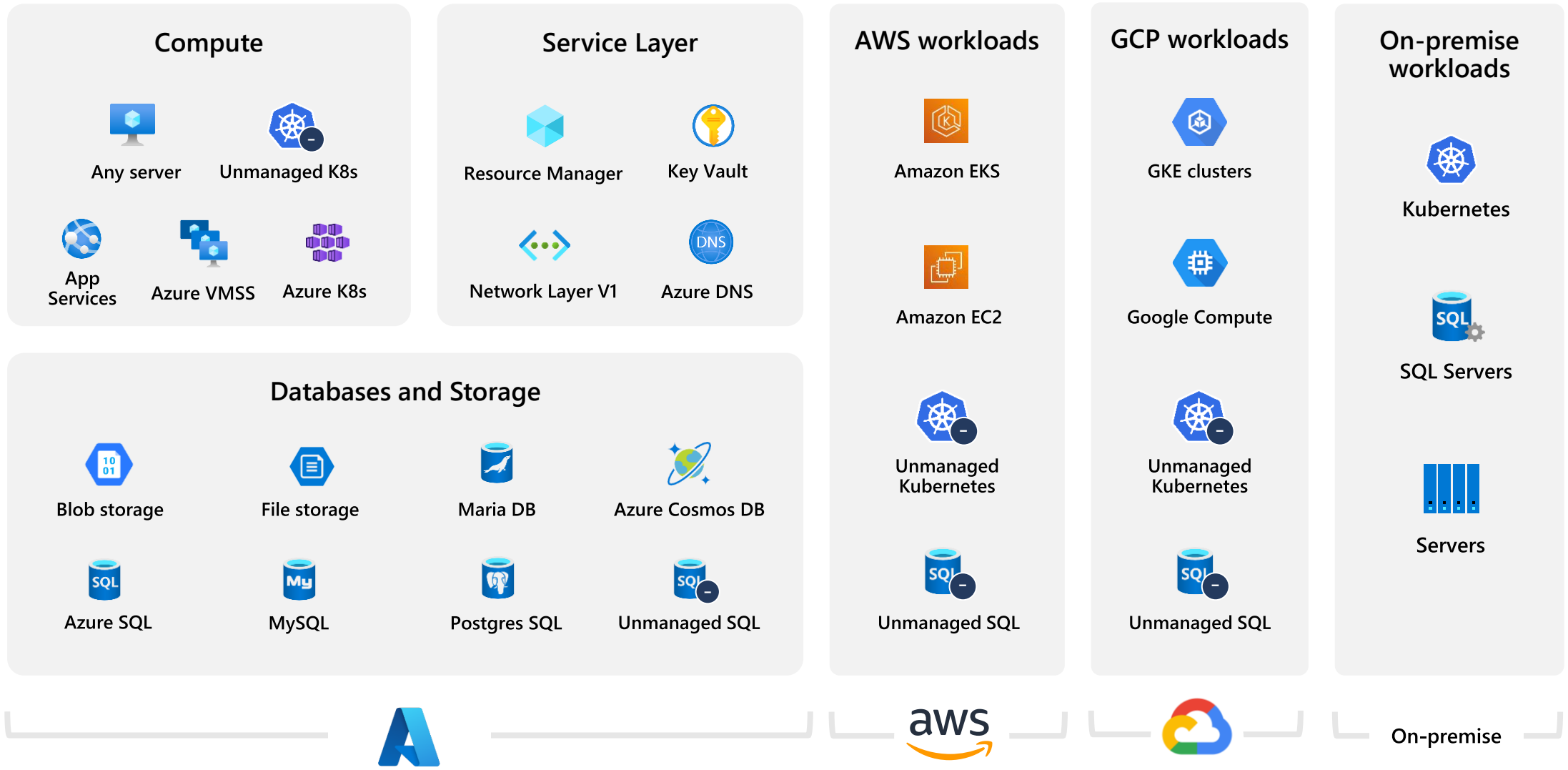
Support for:

- ✓ CIS
- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ Local/National compliance standards
- ✓ Azure Security Benchmark
- ✓ AWS Foundational Security best practices



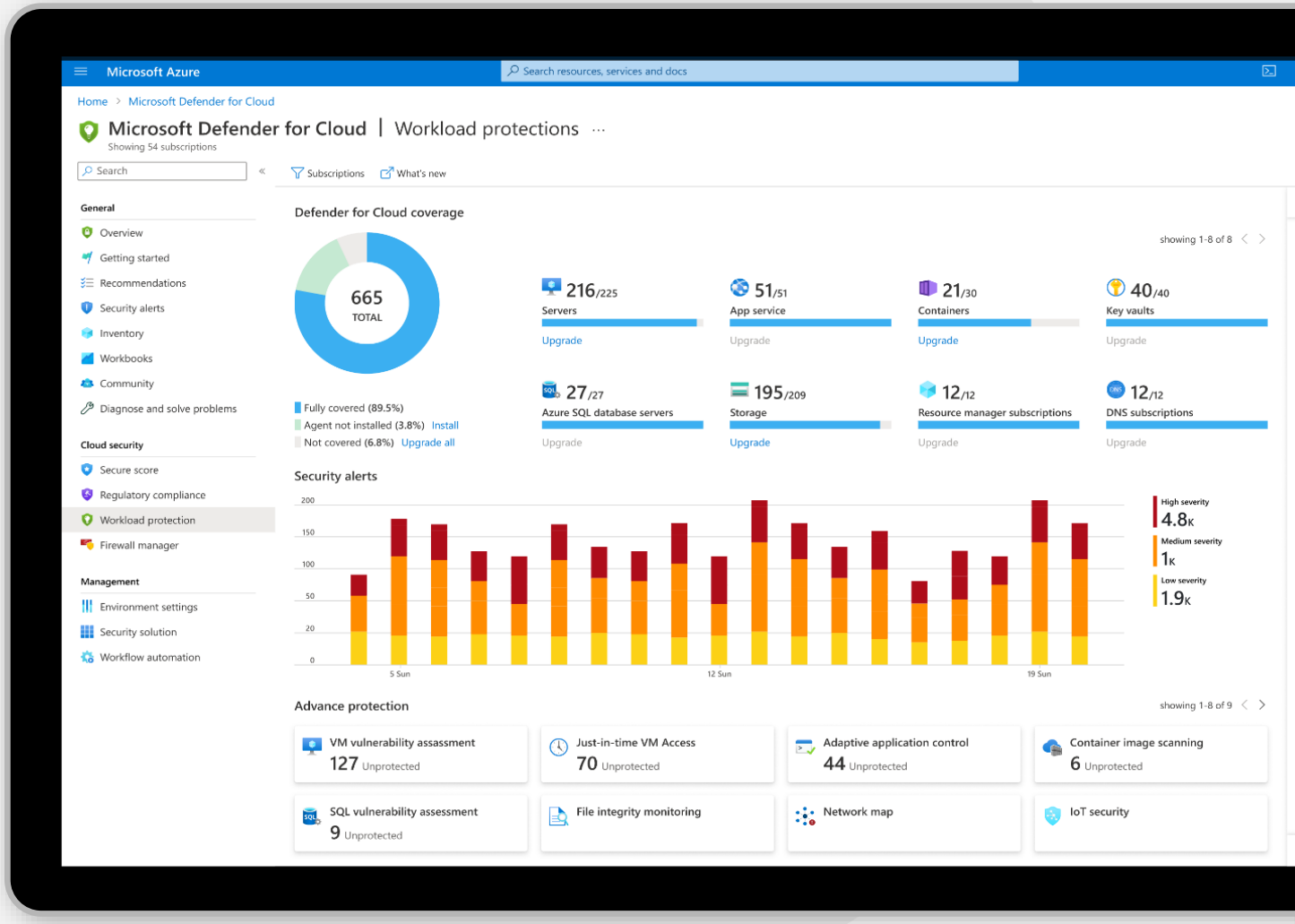
Detect threats and protect your workloads

Full-stack coverage with dedicated detections



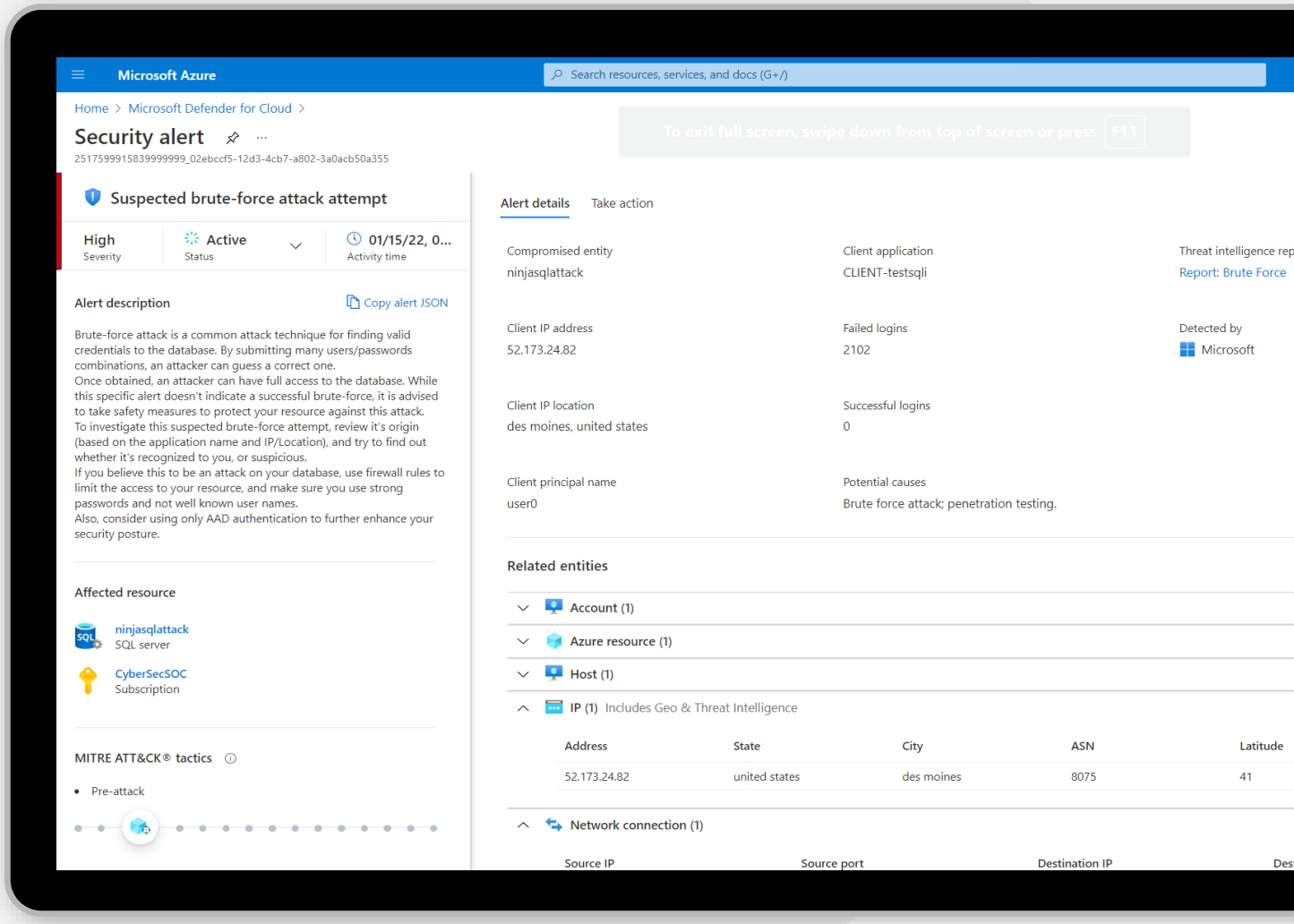
Protect your workloads in the cloud and on-premises

- Use detections that are built for the unique attack vectors of each resource type, built on the powerful insights of Microsoft Threat Intelligence
- Reduce your attack surface by continuously scanning workloads to identify and manage vulnerabilities
- Automatically protect new workloads as soon as they are deployed
- Integrate with your SIEM for easy management of incidents



Security alerts and incidents

- Use prioritized alerts when threats are detected on your resources
- Investigate effectively with smart alert correlation that combines different alerts and low fidelity signals into security incidents
- Manage incidents with a central view of attack campaigns and related alerts



Defender for Cloud security dashboard

Centralized posture view

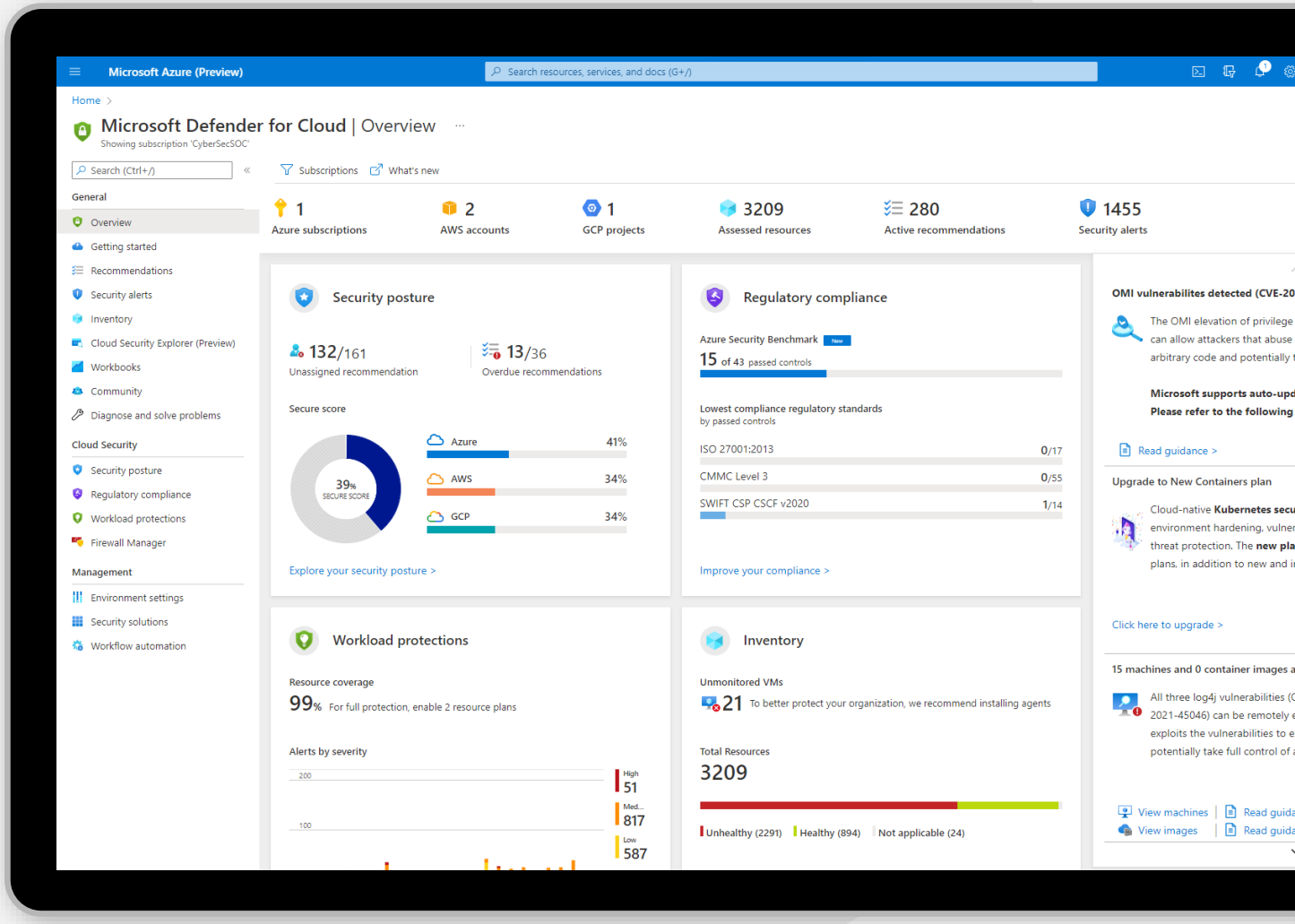
- Your security posture across Azure, AWS, and GCP in one place
- Asset inventory across your hybrid and multicloud environment

Focused views

- Easily access deep dive views for security posture, resource inventory, workload protection, and more

Top insights front and center

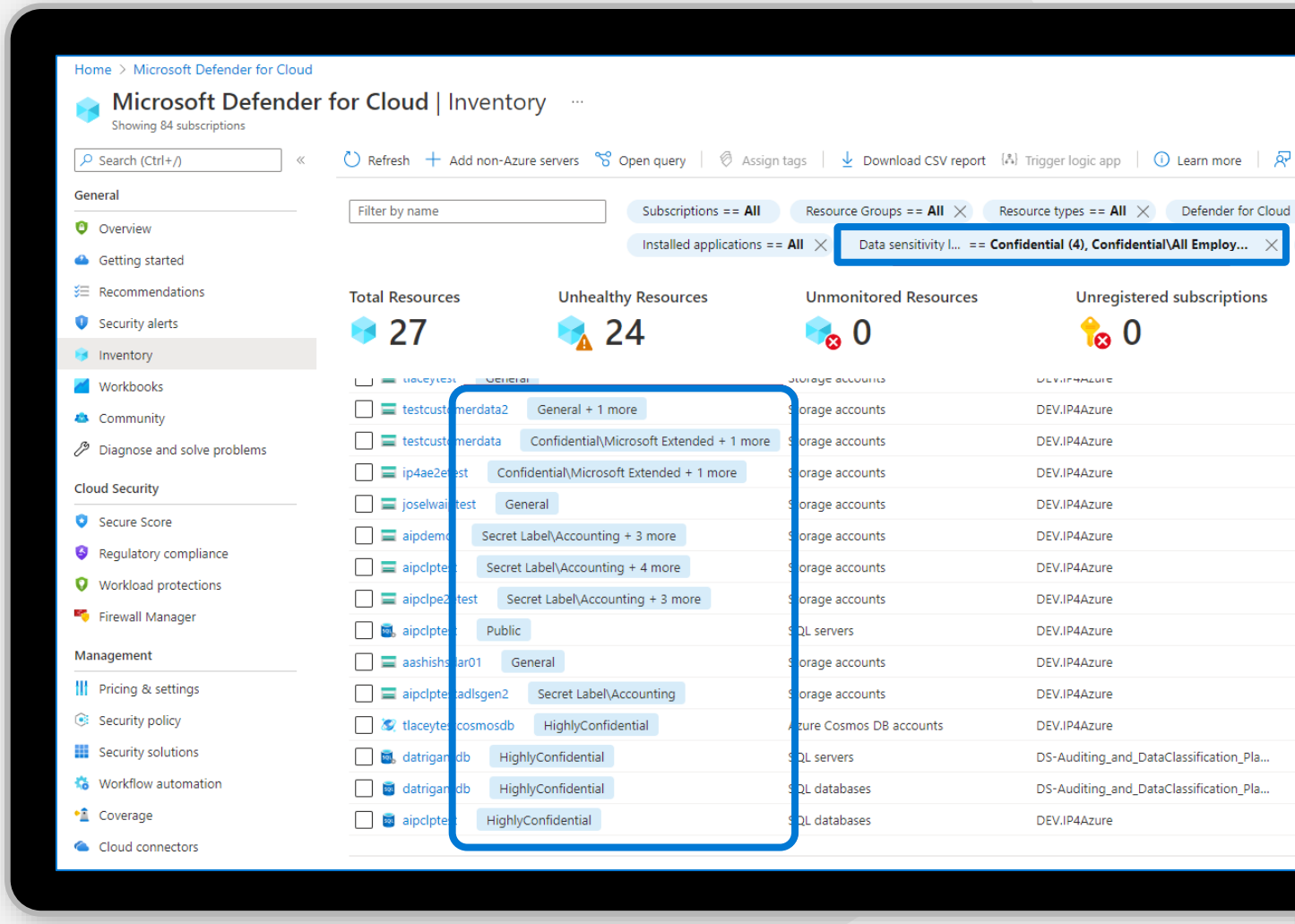
- Understand which recommendations to prioritize
- See your most attacked resources and take action



Identify sensitive data in cloud resources

Integrated with Microsoft Purview

- Extend visibility from cloud infrastructure resources into the data layer
- Leverage an entirely new way to prioritize security policies and the investigation of alerts
- Filter recommendations and resources by data sensitivity
- Easily view the number of assets that contain sensitive information across your environment



Classify and understand the security posture of your APIs

Unified inventory

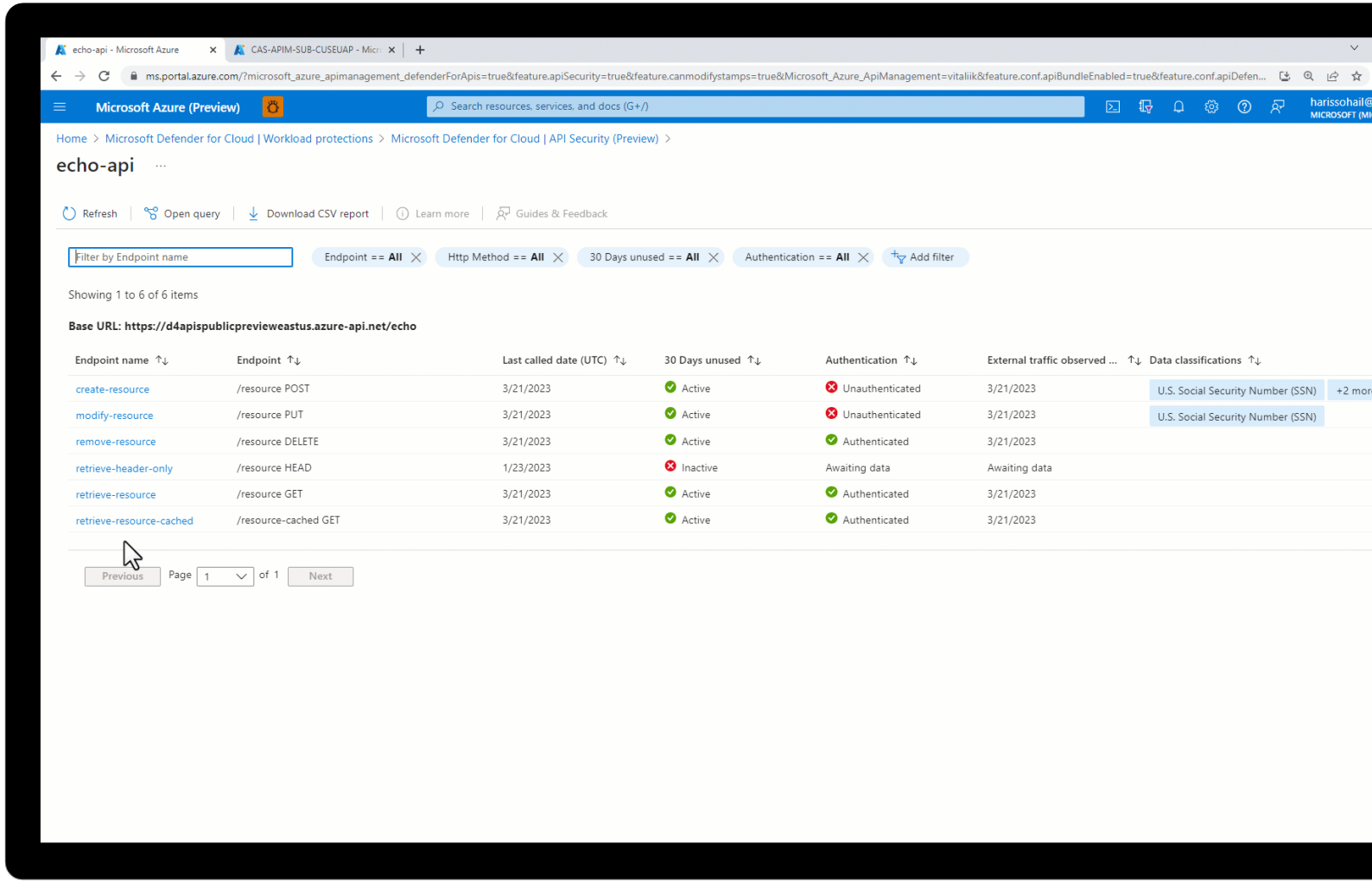
Bring centralized visibility to APIs published across all Azure API Management services

Security insights

Identify externally exposed, dormant, and unauthenticated APIs

Sensitive data classification

Classify APIs exposing, receiving, or responding with sensitive data



Microsoft Security

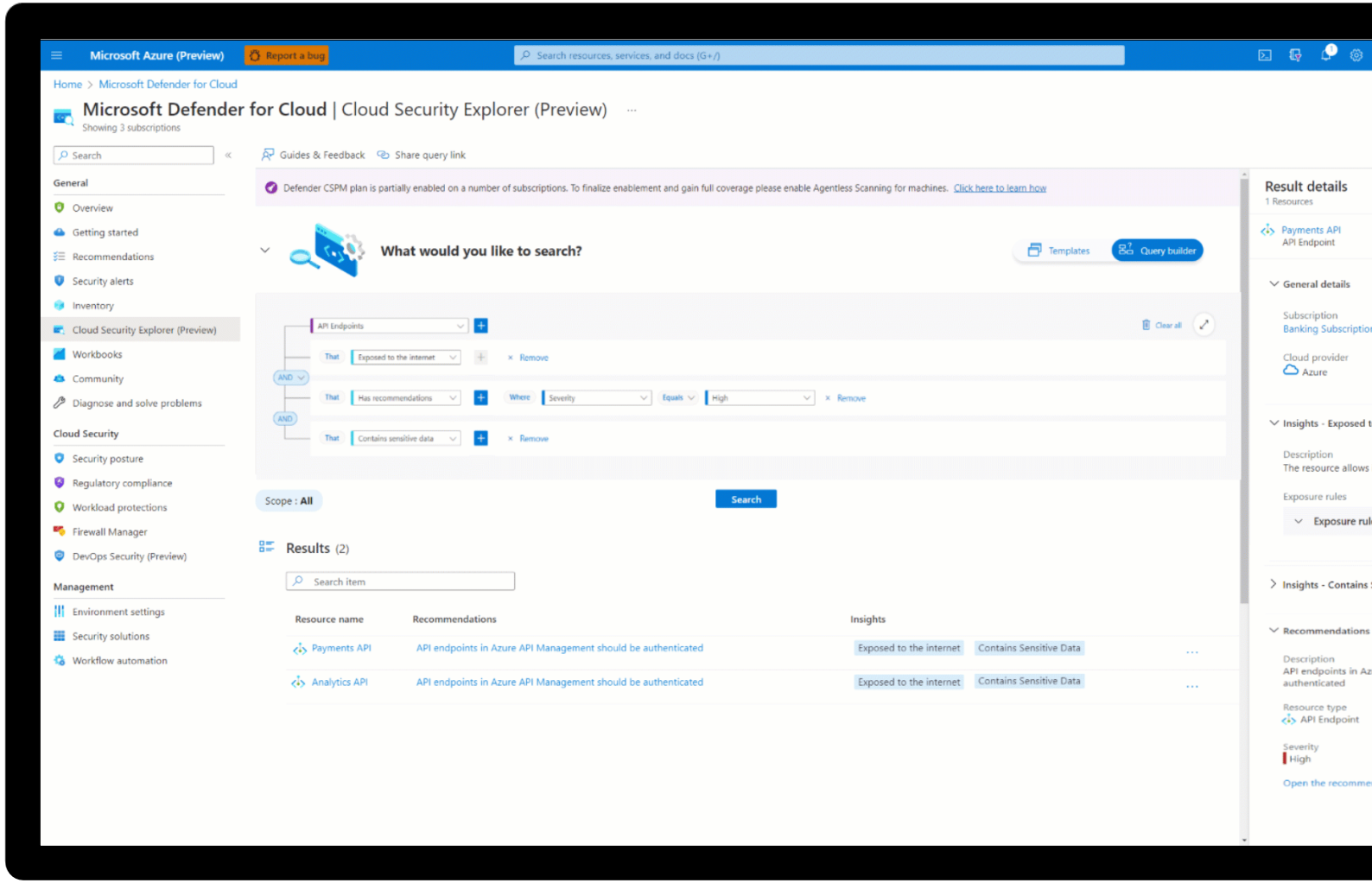
Harden API configurations and prioritize risk remediation

API hardening

Harden APIs against high-risk misconfigurations including broken authentication flows, Azure API Management gateway security controls and more - both in runtime and CI/CD

API risk prioritization

Prioritize and mitigate risks quickly with query support for identifying high risk attack paths



Microsoft Security

Monitor and protect APIs against attacks in runtime

OWASP API top 10 coverage

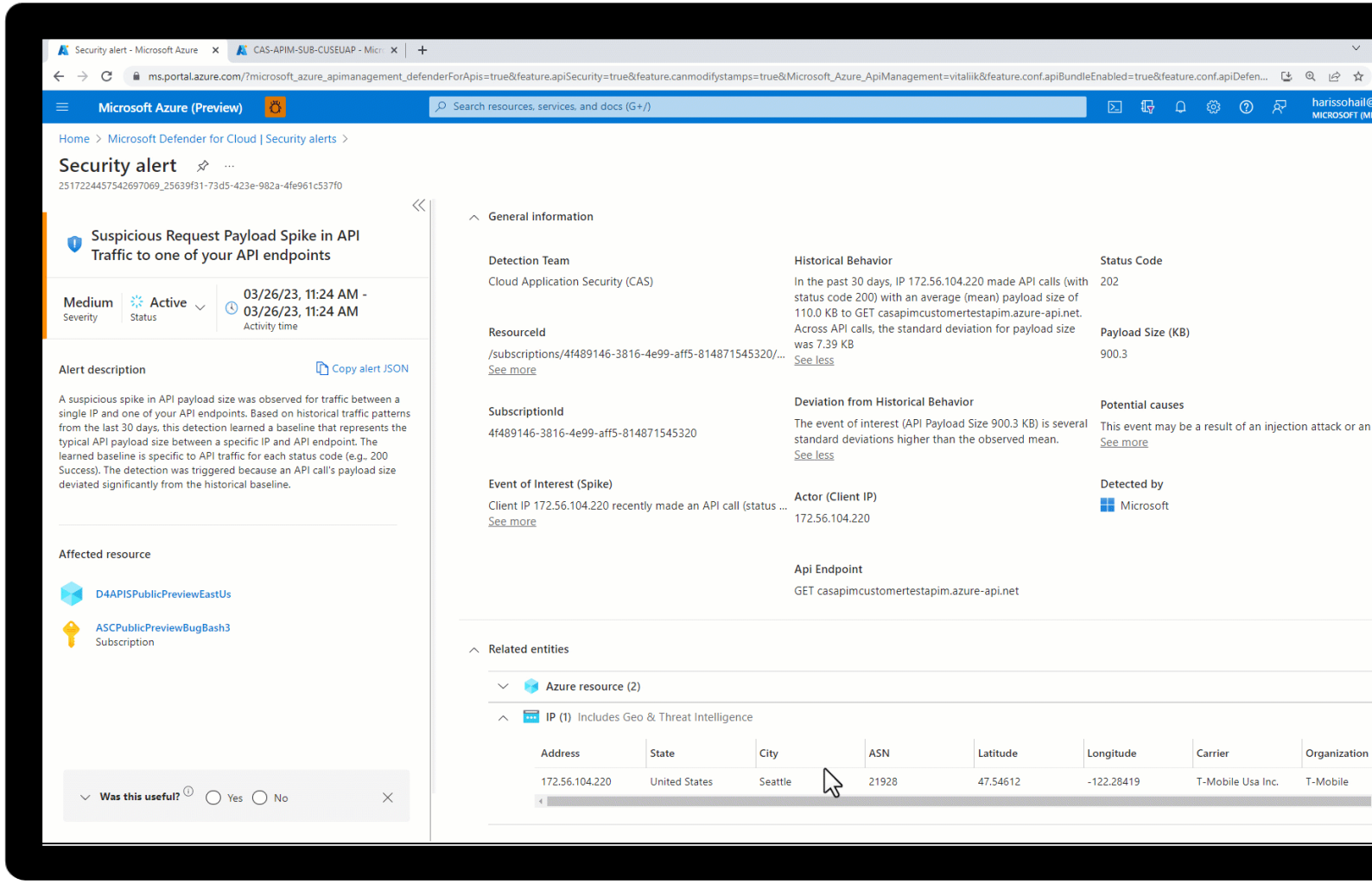
Detect against top OWASP API threats, data exfiltration, volumetric attacks, and more

Machine learning-based anomaly detections

Get a unified view of the active API threats and anomalous and suspicious API usage patterns from runtime traffic monitoring and threat intelligence feeds

Integrated with Microsoft Sentinel and other SIEMs

To enable SOC teams with faster and more efficient remediation efforts



Microsoft Security