

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



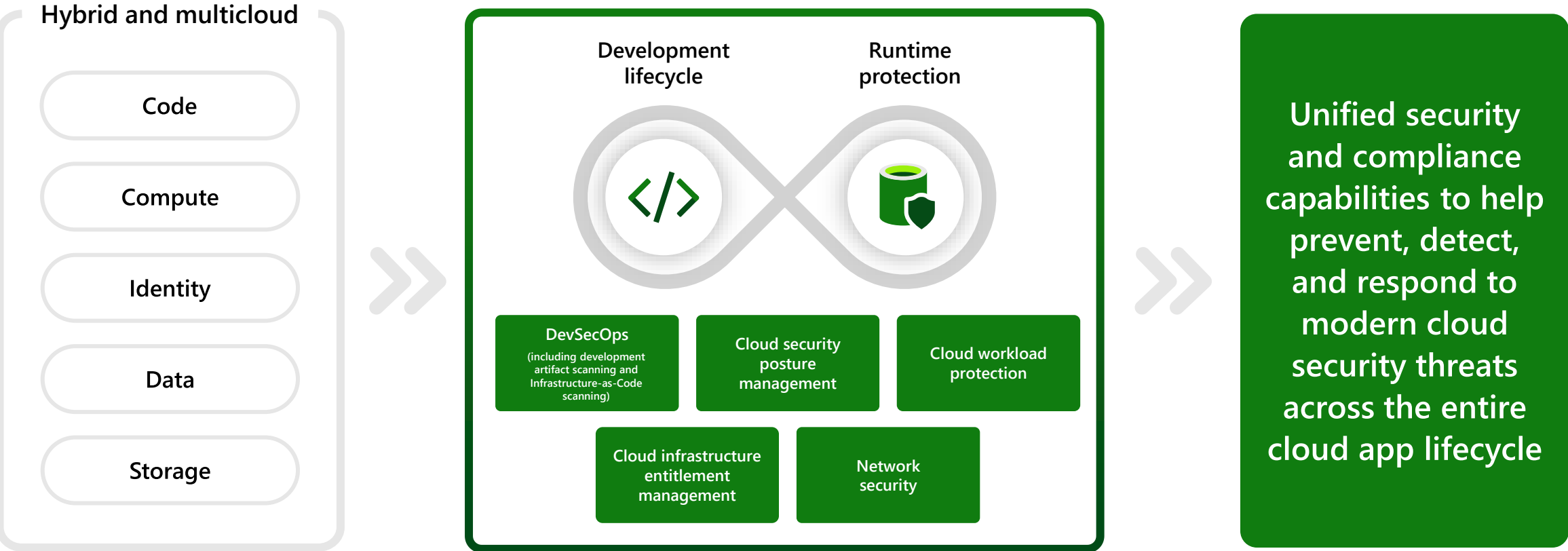
Increasing complexity of in the development and deployment of cloud applications



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 Guide¹.



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)

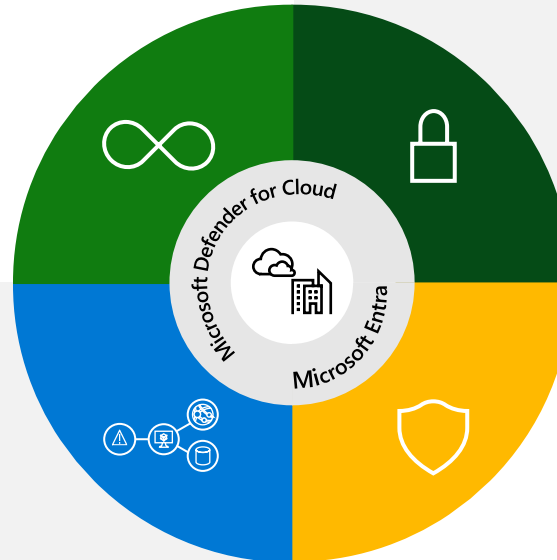


DevSecOps

Unify your DevOps security management across multi-pipelines

Cloud security posture management

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



Cloud infrastructure entitlement management

Enforce principle of least privilege across multicloud with CIEM

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

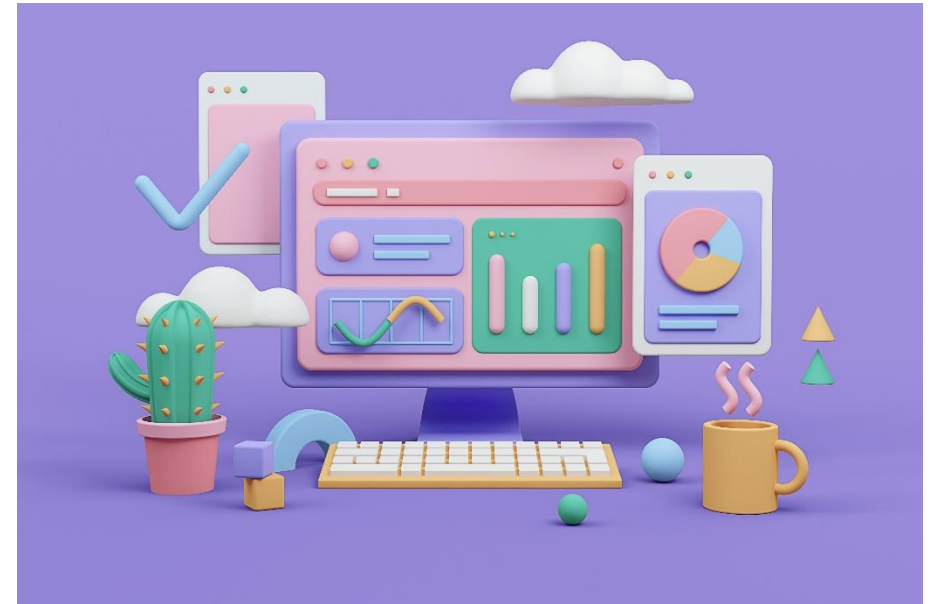
Microsoft Sentinel
(SIEM)

Log Analytics Workspace

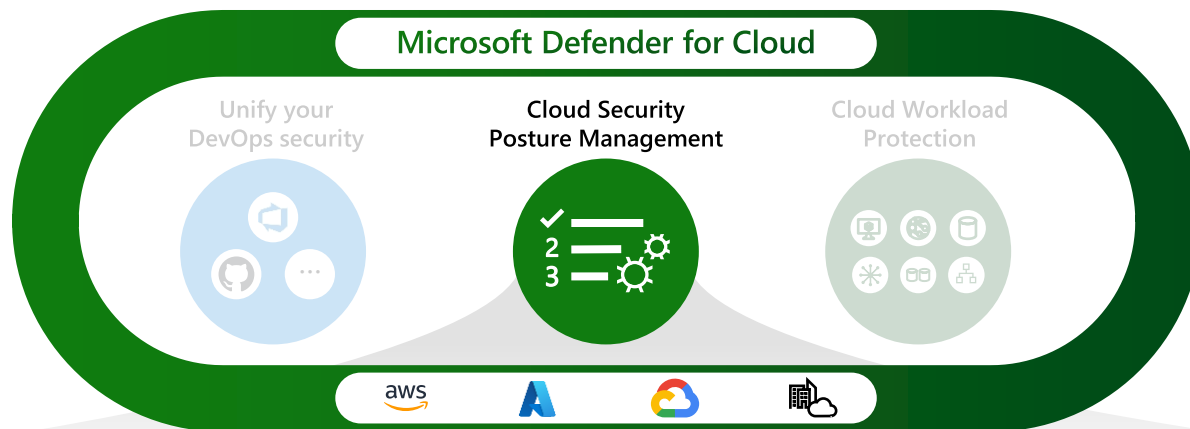
Defender for Cloud collects data from your Azure virtual machines (VMs), Virtual Machine Scale Sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.

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

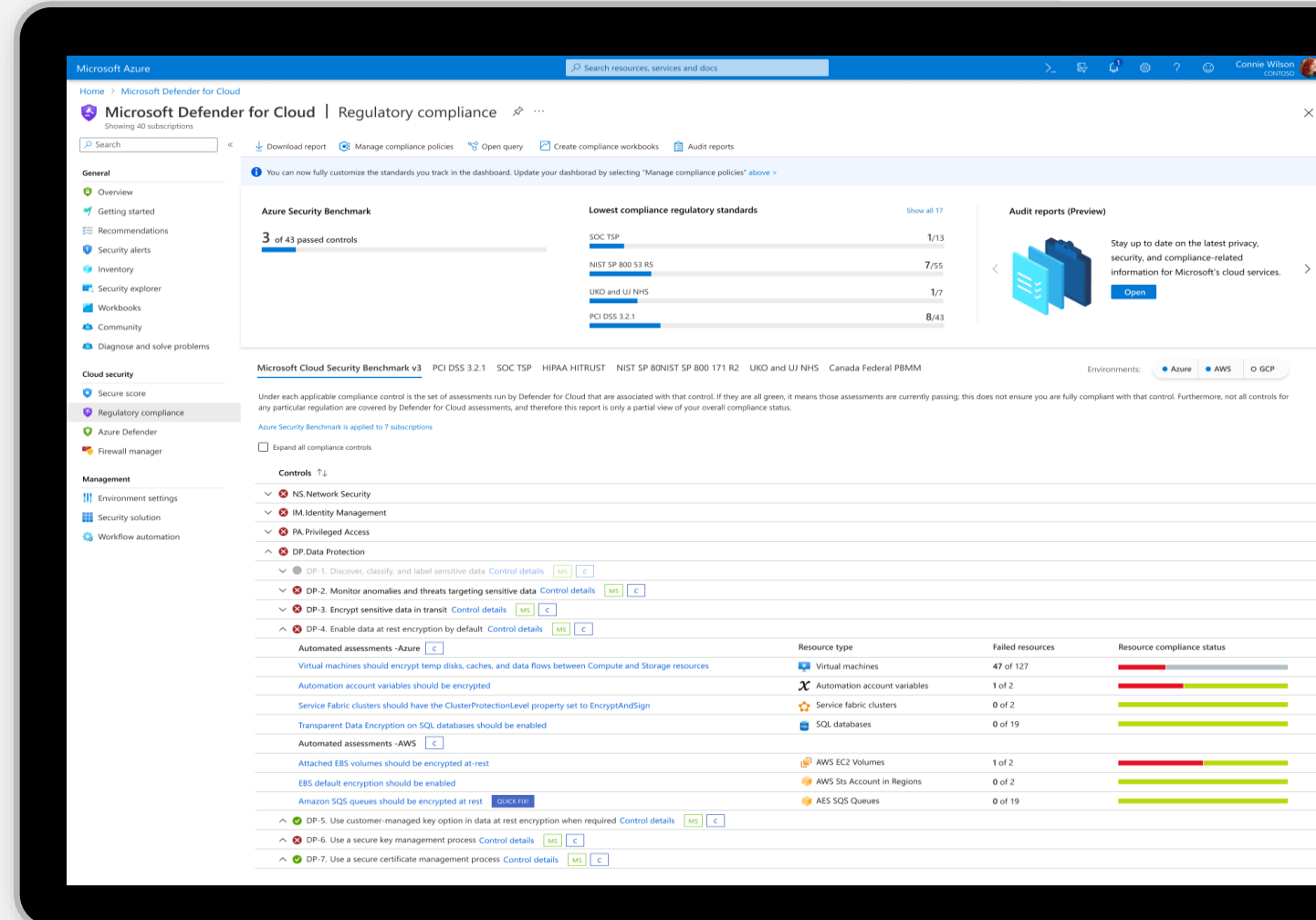
Multicloud data estate discovery | Identify data flows and resources containing sensitive and shadow data | Uncover potential sensitive data exposure and data breaches

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:

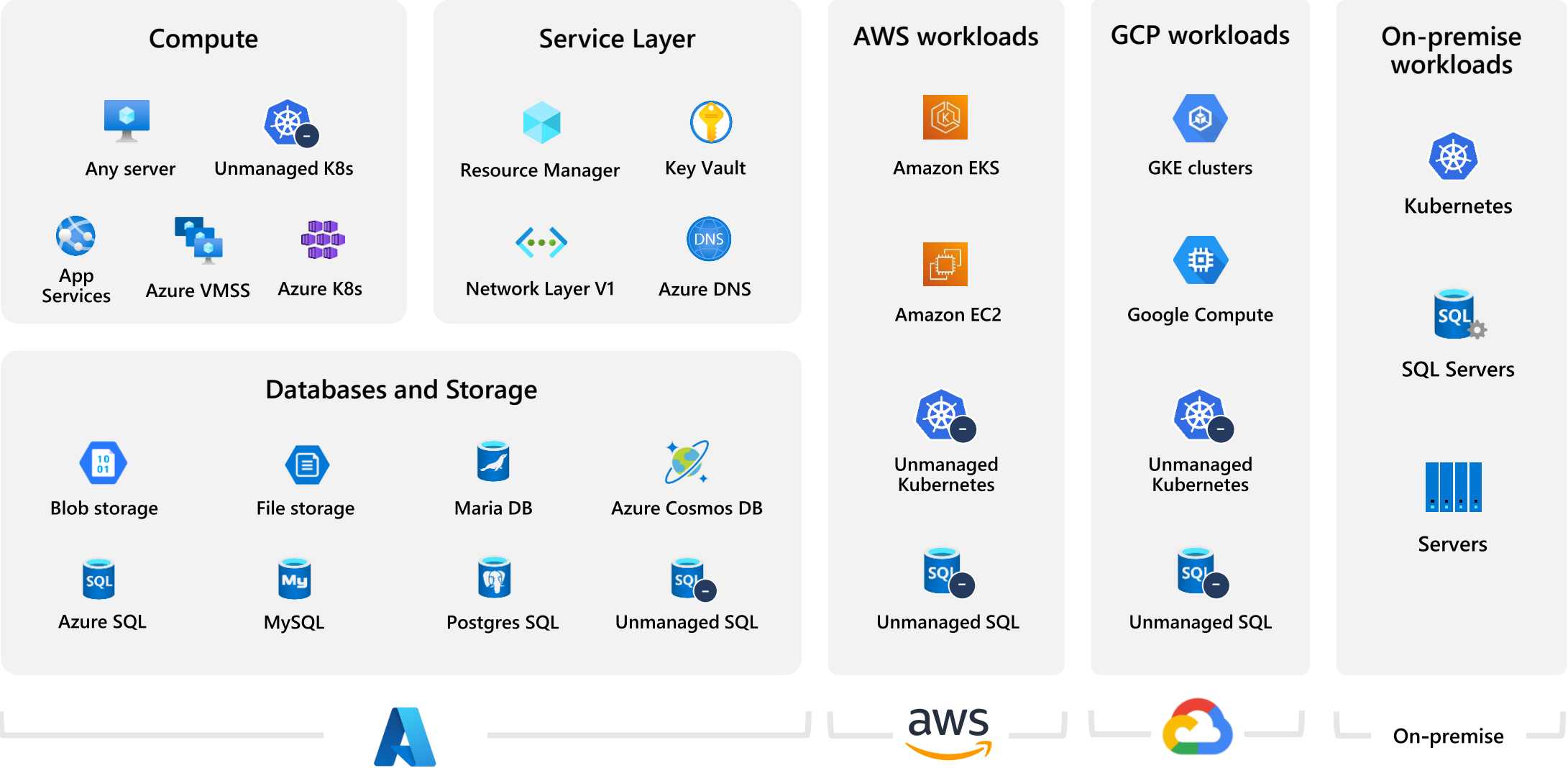
- ✓ CIS
- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ Local/National compliance standards
- ✓ Azure Security Benchmark
- ✓ AWS Foundational Security best practices



Detect threats
and protect
your workloads

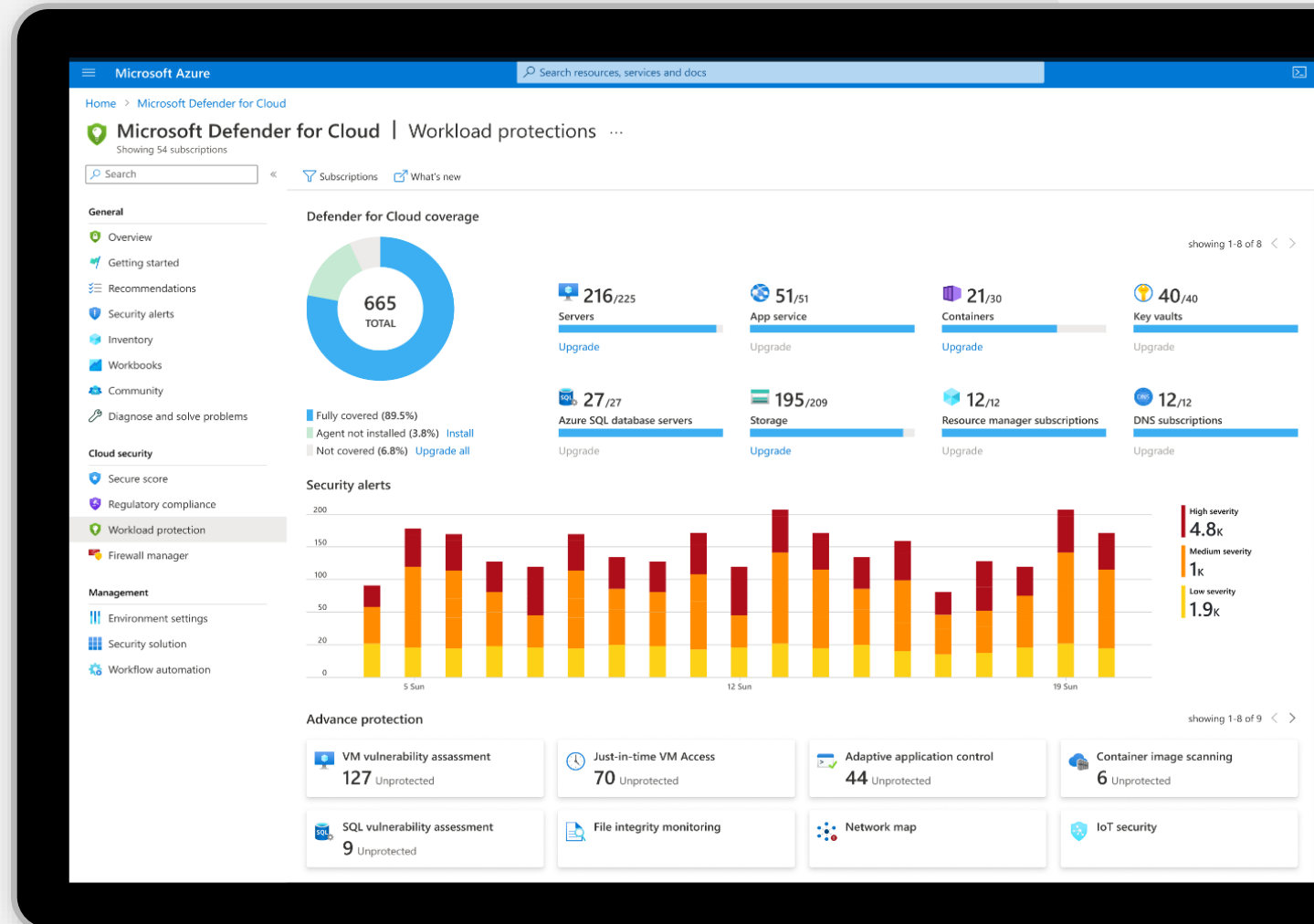


Full-stack coverage with dedicated detections



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

The screenshot displays the Microsoft Azure Security Center interface. At the top, the navigation bar shows 'Microsoft Azure' and a search bar. Below the navigation bar, the breadcrumb trail indicates 'Home > Microsoft Defender for Cloud >'. The main heading is 'Security alert' followed by an icon and a three-dot menu. Below this, the alert ID '2517599915839999999_02ebccf5-12d3-4cb7-a802-3a0acb50a355' is shown.

The alert is titled 'Suspected brute-force attack attempt' with a shield icon. It has a 'High' severity, 'Active' status, and an activity time of '01/15/22, 0...'. Below the alert header, the 'Alert description' section provides a detailed explanation of the brute-force attack technique and advises on investigation steps. A 'Copy alert JSON' link is available.

The 'Affected resource' section lists the following resources:

- ninjasqlattack (SQL server)
- CyberSecSOC (Subscription)

The 'MITRE ATT&CK' tactics section shows 'Pre-attack' as the active tactic.

The 'Alert details' section on the right provides a table of key information:

Compromised entity	Client application	Threat intelligence rep
ninjasqlattack	CLIENT-testsqli	Report: Brute Force
Client IP address	Failed logins	Detected by
52.173.24.82	2102	Microsoft
Client IP location	Successful logins	
des moines, united states	0	
Client principal name	Potential causes	
user0	Brute force attack; penetration testing.	

The 'Related entities' section lists the following entities:

- Account (1)
- Azure resource (1)
- Host (1)
- IP (1) Includes Geo & Threat Intelligence

The 'IP (1)' entity is expanded, showing a table of IP details:

Address	State	City	ASN	Latitude
52.173.24.82	united states	des moines	8075	41

The 'Network connection (1)' section is also expanded, showing a table of network connection details:

Source IP	Source port	Destination IP	Des
-----------	-------------	----------------	-----

Defender for Cloud security dashboard

» Centralized posture view

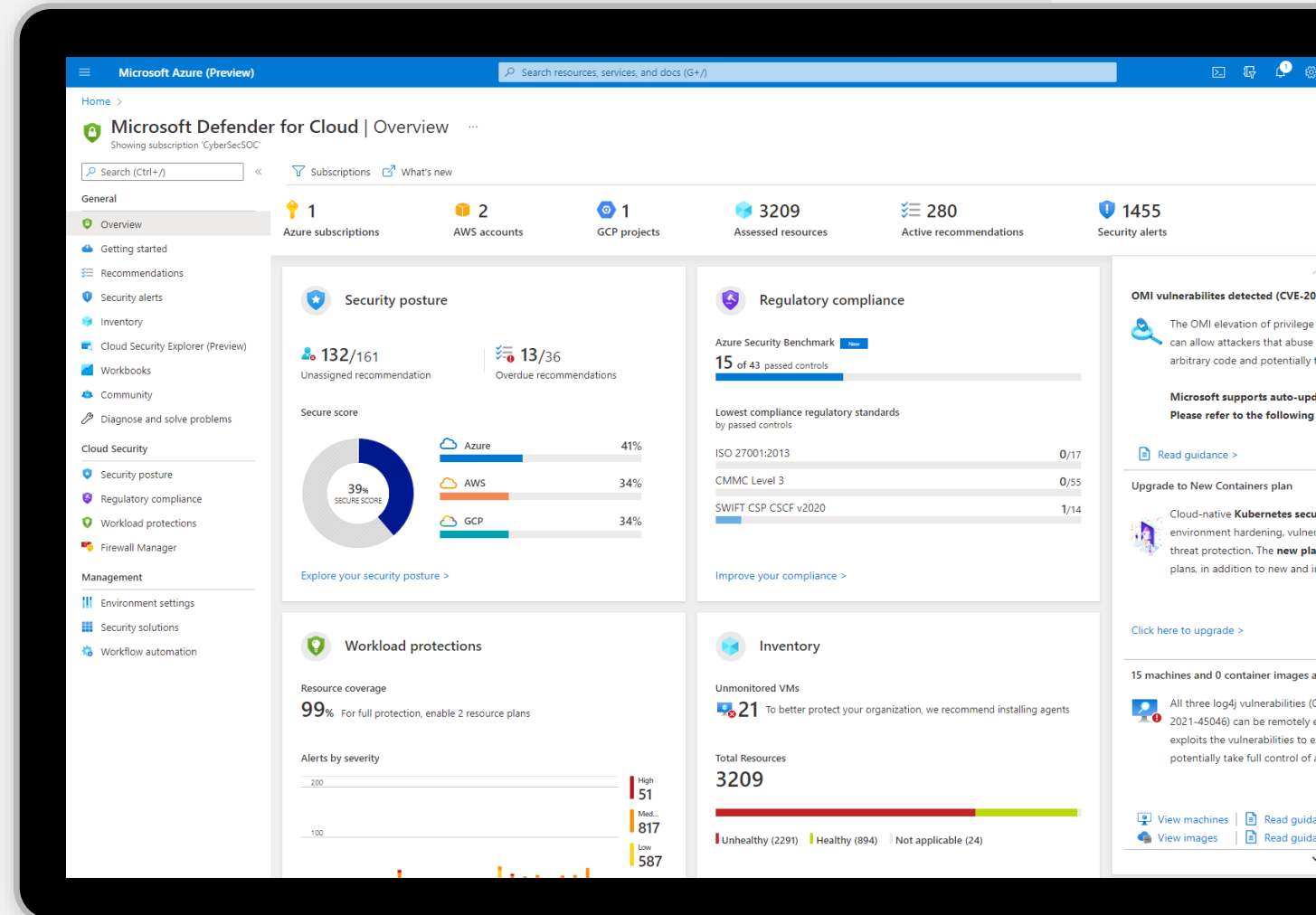
- Your security posture across Azure, AWS, and GCP in one place
- Asset inventory across your hybrid and multicloud environment

» Focused views

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

» Top insights front and center

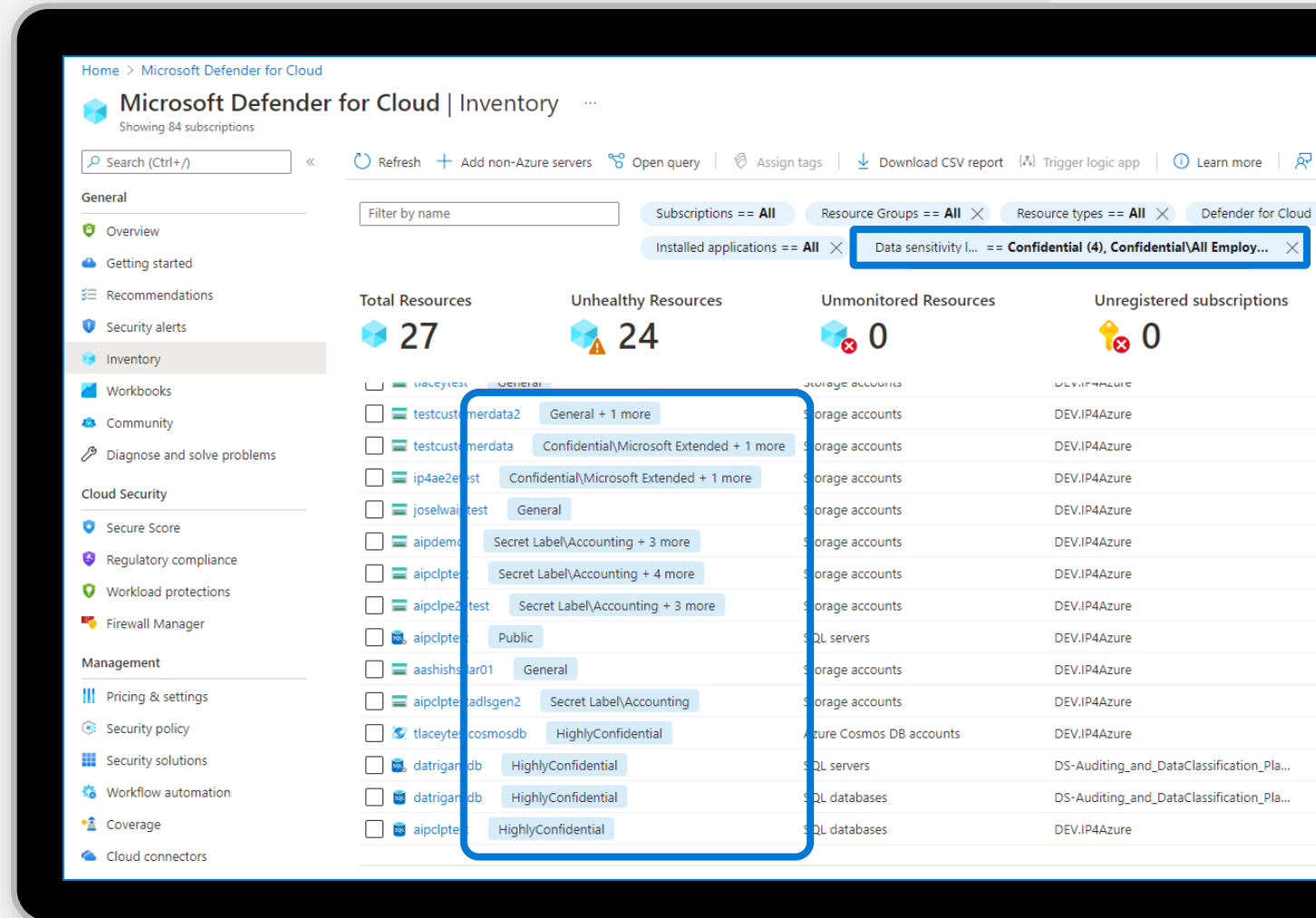
- Understand which recommendations to prioritize
- See your most attacked resources and take action



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 Azure (Preview)

Home > Microsoft Defender for Cloud | Workload protections > Microsoft Defender for Cloud | API Security (Preview)

echo-api

Refresh Open query Download CSV report Learn more Guides & Feedback

Filter by Endpoint name Endpoint == All Http Method == All 30 Days unused == All Authentication == All Add filter

Showing 1 to 6 of 6 items

Base URL: <https://d4apispublicprevieweastus.azure-api.net/echo>

Endpoint name ↑↓	Endpoint ↑↓	Last called date (UTC) ↑↓	30 Days unused ↑↓	Authentication ↑↓	External traffic observed ... ↑↓	Data classifications ↑↓
create-resource	/resource POST	3/21/2023	Active	Unauthenticated	3/21/2023	U.S. Social Security Number (SSN) +2 mor
modify-resource	/resource PUT	3/21/2023	Active	Unauthenticated	3/21/2023	U.S. Social Security Number (SSN)
remove-resource	/resource DELETE	3/21/2023	Active	Authenticated	3/21/2023	
retrieve-header-only	/resource HEAD	1/23/2023	Inactive	Awaiting data	Awaiting data	
retrieve-resource	/resource GET	3/21/2023	Active	Authenticated	3/21/2023	
retrieve-resource-cached	/resource-cached GET	3/21/2023	Active	Authenticated	3/21/2023	

Previous Page 1 of 1 Next

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

The screenshot displays the Microsoft Azure Cloud Security Explorer (Preview) interface. The left sidebar shows navigation options under 'General', 'Cloud Security', and 'Management'. The main area is titled 'Microsoft Defender for Cloud | Cloud Security Explorer (Preview)' and shows a search bar and a 'What would you like to search?' section. Below this, a query builder is visible with filters for 'API Endpoints', 'Exposed to the internet', 'Has recommendations', and 'Contains sensitive data'. The 'Results (2)' section shows a table with two rows of API endpoints and their associated recommendations and insights.

Resource name	Recommendations	Insights
Payments API	API endpoints in Azure API Management should be authenticated	Exposed to the internet, Contains Sensitive Data
Analytics API	API endpoints in Azure API Management should be authenticated	Exposed to the internet, Contains Sensitive Data

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

The screenshot displays the Microsoft Azure portal interface for a security alert. The alert is titled "Suspicious Request Payload Spike in API Traffic to one of your API endpoints" and is categorized as "Medium" severity and "Active" status. It occurred on 03/26/23 at 11:24 AM. The alert description states: "A suspicious spike in API payload size was observed for traffic between a single IP and one of your API endpoints. Based on historical traffic patterns from the last 30 days, this detection learned a baseline that represents the typical API payload size between a specific IP and API endpoint. The learned baseline is specific to API traffic for each status code (e.g., 200 Success). The detection was triggered because an API call's payload size deviated significantly from the historical baseline." The affected resource is identified as "D4APISPublicPreviewEastUs". The alert is linked to the "ASCPublicPreviewBugBash3" subscription. The right-hand pane provides detailed information about the alert, including the detection team (Cloud Application Security (CAS)), the resource ID, the subscription ID, the event of interest (a spike in payload size), the actor (Client IP 172.56.104.220), the API endpoint (GET casapimcustomertestapim.azure-api.net), and the status code (202). It also shows the historical behavior, deviation from historical behavior, and potential causes. The bottom section lists related entities, including the Azure resource and the IP address (172.56.104.220) with its associated location and organization (T-Mobile Usa Inc.).

Address	State	City	ASN	Latitude	Longitude	Carrier	Organization
172.56.104.220	United States	Seattle	21928	47.54612	-122.28419	T-Mobile Usa Inc.	T-Mobile