

Search the blog



News Cloud security Microsoft Defender

8 min read

New Microsoft Security innovations expand multicloud visibility and enhance multiplatform protection

By Vasu Jakkal, Corporate Vice President, Security, Compliance, Identity, and Management

August 9, 2023



Device management Endpoint security Security management [more](#) ▾

With more than 90 percent of organizations adopting a multicloud strategy¹ and cloud-based cyberattacks growing 48 percent year over year,² securing multicloud and hybrid environments is more important than ever. To successfully protect multicloud infrastructure—where customers are utilizing two or more cloud providers—as well as applications and data, today’s organizations need to both proactively reduce risk and quickly detect and respond to threats in real time.

Multicloud and multiplatform deployments increase the potential for security risks and data breaches. Today, many customers are working to secure a complex patchwork of technologies across different devices, applications, platforms, and clouds. Some are also dealing with separate security infrastructures for each cloud they’re operating in, which introduces incredible complexity, creates seams for attackers to exploit, and increases the likelihood of mistakes.

I am excited to share several innovations that **improve multicloud visibility and help customers proactively reduce risk and respond to threats in real time.** Read on to see how we continue to expand our end-to-end security solution to help organizations defend against threats across all endpoints and clouds.



Microsoft Defender for Cloud

Protect multicloud and hybrid environments with comprehensive security across the full lifecycle, from development to runtime.

[Learn more >](#)

Extend multicloud visibility to proactively prevent breaches

Today, we’re thrilled to announce **new advanced multicloud posture management capabilities for Google Cloud Platform (GCP) in Microsoft Defender for Cloud** to help customers proactively prevent [data breaches](#) across multicloud and hybrid environments.

Microsoft is recognized as a Representative Vendor in the 2023 Gartner Market Guide for Cloud Native Application Protection Platforms.³ **Microsoft Defender for Cloud** became the first cloud provider to offer multicloud workload protection for cloud infrastructure, applications, and data across the full lifecycle for all three public clouds.⁴ Since then, we’ve rapidly expanded our CNAPP capabilities to provide advanced posture management with [Microsoft Defender Cloud Security Posture Management](#) (Defender CSPM), DevSecOps security with integrations into GitHub Advanced Security, and continued investments in our [cloud workload protection \(CWP\)](#) solutions across servers, containers, APIs, storage, and databases.

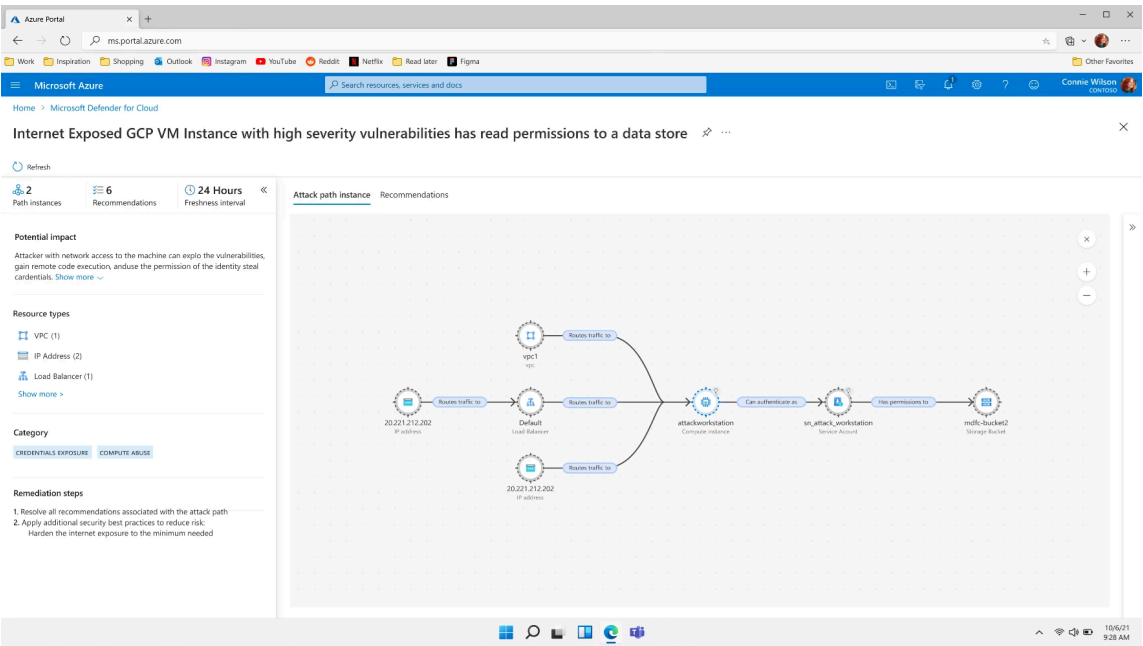


Figure 1. Attack path showing a GCP virtual machine exposed to the internet with permissions to a data store.

On August 15, 2023, **Defender CSPM will extend its advanced agentless scanning, data-aware security posture, cloud security graph, and attack path analysis capabilities to GCP**, providing a single contextual view of cloud risks

across Amazon Web Services (AWS), Azure, GCP, and hybrid environments. Defender CSPM provides advanced posture management capabilities and is recognized by KuppingerCole as an Overall Leader, Market Champion, Product Leader, and Innovation Leader in its 2023 CSPM Leadership Compass, noting “Organizations looking for a CSPM which provides multicloud capabilities including data-aware security posture should consider Microsoft Defender for Cloud.”⁵ Defender CSPM provides advanced posture management capabilities with full visibility across cloud and hybrid resources from agentless scanning, integrated contextual insights from code, identities, data, internet exposure, compliance, attack path analysis, and more, to prioritize your most critical risks. Customers will be able to leverage agentless scanning to gain full visibility of their GCP, AWS, Azure, and on-premises compute resources in the cloud security graph and attack path analysis to prioritize and mitigate risk against potential threats.

Within the new Defender CSPM capabilities for GCP, we’re also **extending our sensitive data discovery capabilities to GCP Cloud Storage**. With this advancement, customers will be able to discover all their GCP Cloud Storage buckets, identify more than 100 sensitive information types, and assess their data security posture through cloud security graph queries and attack path analysis. Now customers can identify potentially sensitive data exposure risks across Azure, AWS, and GCP storage resources and harden their multicloud data security posture.

We chose Microsoft Defender for Cloud as our CNAPP because of the robust, intelligent end-to-end cloud security it provides with proactive CSPM and in protecting our cloud workloads. We’ve already been impressed with the value of Microsoft’s cloud workload protection, so it was an easy choice to also use Defender CSPM. Its agentless scanning allows us to quickly gain insights about our VMs, storage accounts, and containers, and attack path analysis with its contextual insights helps us prioritize and remediate risks. Defender for Cloud is critical in further helping our security teams save time to focus on preventing security incidents and give us peace of mind by knowing we have security across the application lifecycle.

—Cloud Security Manager, Mercedes-Benz Group AG

Get multicloud policy monitoring as a free offering

Microsoft’s cloud security benchmark (MCSB) extends security control guidance and compliance checks to GCP, completing multicloud monitoring across Azure, AWS, and GCP as a free offering. MCSB provides a cloud-centric control framework mapped to major regulatory industry benchmarks (CIS, PCI, NIST, and more) and cloud-specific implementation tools turned on by default to maintain your cloud security compliance across clouds.⁶ Today, along with existing Azure and AWS guidance, organizations can now leverage the MCSB security guidance for GCP environments and access GCP checks (as a preview feature) in the context of MCSB controls in the regulatory compliance dashboard in Microsoft Defender for Cloud. In addition to the policy compliance checking available through MCSB, Microsoft customers also benefit from the free [expanded cloud logging support](#) we announced last month.

Prevent malware upload and distribution in near real time

Defender for Cloud is also advancing cloud data security at runtime. We’re excited to share the upcoming general availability of **Malware Scanning in Microsoft Defender for Storage**.⁷ Starting September 1, 2023, security teams can enable an additional layer of protection to detect and prevent storage accounts from acting as a point of malware entry and distribution.

Organizations rely on cloud storage to store and access data and files, which often contain sensitive and critical data. However, due to its critical and connected role in an organization’s cloud environment, cloud storage can be an effective attack vector for malicious actors to upload and distribute malware. Malware protection methods in the past have focused mostly on compute resources. Protection for storage in this old model would require complex networking workarounds that negatively impact overall performance.

We built Malware Scanning in Defender for Storage to cut through the networking complexities and optimize malware detection for Microsoft Azure Blob Storage in near real time when content is uploaded. Content is automatically scanned for metamorphic and polymorphic malware, with results automatically recorded on the blob metadata.

Read more about [Defender for Cloud’s new multicloud security capabilities](#).

Manage vulnerability risk across cloud deployments

As organizations adopt new technologies across cloud computing, Internet of Things (IoT) devices, and remote work, their attack surface is expanding, making vulnerability management increasingly challenging. Security teams must rethink how to secure a growing and diverse portfolio of devices outside of traditional organizational boundaries, adding complexity to the vulnerability management process. This process requires a combination of policy and scope definition that cannot be purchased off the shelf. Instead, it must be established and matured within an organization, based on its specific risk appetite and maturity level.

In recent years, Microsoft has established itself as a leading solution for vulnerability risk management (VRM) by leveraging its threat intelligence and security expertise. [Microsoft Defender Vulnerability Management](#) has become a leading solution for a vast range of customer organizations, providing them end-to-end capabilities across the VRM lifecycle. It is designed to help organizations identify, assess, prioritize, and remediate vulnerabilities in their IT environments, making it an ideal tool for managing an expanded attack surface and reducing overall risk posture, We are thrilled to announce **Defender Vulnerability Management is now offered as a standalone solution**, which means that customers can purchase it separately and take advantage of the full set of core and premium capabilities across their portfolio of managed and unmanaged devices. Microsoft 365 E5 and Defender for Endpoint Plan 2 customers have the core capabilities included and can continue to get the full vulnerability management solution with the Defender Vulnerability Add-on.

		Defender Vulnerability Management Standalone	Defender for Endpoint P2 or Defender for Servers P1	Defender for Endpoint P2 + Defender Vulnerability Management Add-On or Defender for Servers P2
Core capabilities	Device inventory	✓	✓	✓
	Vulnerability assessment	✓	✓	✓
	Configuration assessment	✓	✓	✓
	Risk based prioritization	✓	✓	✓
	Remediation tracking	✓	✓	✓
	Continuous monitoring	✓	✓	✓
	Software inventory	✓	✓	✓
	Software usages insights	✓	✓	✓
	Security baselines assessment	✓		✓
	Block vulnerable applications	✓		✓
Premium capabilities	Browser extensions assessment	✓		✓
	Digital certificate assessment	✓		✓
	Network share analysis	✓		✓
	Hardware and firmware assessment	✓		✓
	Authenticated scan for Windows	✓		✓

Figure 2. Core and premium capabilities of Microsoft Defender Vulnerability Management and how customers would acquire them.

Committed to protecting the entire organization’s estate, we are excited to announce **the general availability of vulnerability assessments for containers in Defender CSPM** and the preview of vulnerability assessments for containers in Microsoft Defender for Containers using Defender Vulnerability Management. With the rise of containerization and microservices, it’s more important than ever to

secure the software supply chain and ensure that container images are free from vulnerabilities. Defender Vulnerability Management's new container vulnerability assessment capabilities enable organizations to scan container images for vulnerabilities and prioritize remediation efforts, based on the severity of the vulnerabilities.

Read more about the new standalone offer and the [expanded capabilities of Defender Vulnerability Management](#).

Get additional protection and expanded endpoint coverage

You can't protect and manage what you can't see. This means that a [Zero Trust](#) model can't just be limited to the endpoints enrolled in Microsoft Intune—it must extend to devices integrated with Microsoft Security solutions. If you can't distribute compliance or security policies to all your devices, you can't implement a Zero Trust model.

Now you can expand coverage and provide additional protection from a single unified pane of glass with [Microsoft Intune](#), which can manage the security settings of any device with Microsoft Defender for Endpoint, including Windows, macOS, and Linux endpoints.⁸ These policies and settings allow security admins to remain in the Defender portal to manage Defender for Endpoint and the **Intune endpoint security policies for Defender security settings configurations**. Now security admins can deploy policies from Intune to manage the Defender security settings on devices onboarded to Defender for Endpoint, without enrolling those devices with Intune.

Secure Score integration with Microsoft Intune means that recommendations for device health and security settings for your organization's endpoints from Intune are now included in [Microsoft Secure Score](#). Secure Score is the measurement of an organization's security posture. This score is used to assess risk, drive configuration actions, plan improvements, and report to management. More points in Secure Score equates to more actions taken to improve an organization's security posture.

And finally, we recently announced a new solution that adds another layer of protection for Samsung Galaxy devices with **hardware-backed device attestation**.⁹ Device attestation is a crucial mechanism to verify device trust and health to help detect if a device has been compromised. Building on our strategic partnership with Samsung, this attestation helps to prevent malicious endpoints from accessing organization resources using valid client information taken from another device and limiting tampering with client requests. Samsung's hardware-backed cryptography and Intune app protection policies verify the client endpoint and secure the communication between Intune client and service. It enables a trusted, on-device hardware-backed health check, giving organizations that allow Samsung Galaxy mobile devices to access their corporate network the confidence that personally owned Galaxy devices have the same strong level of extra protection as company-owned devices.

Continuing to deliver for our customers

With our latest product and feature announcements, customers working to secure their multicloud and multiplatform deployments can have a clearer view of their environment, reduce risk, and gain improvements in the safety of their data and systems. At Microsoft, we are committed to providing our customers with the tools and resources they need to protect everything.

Join us at Black Hat 2023

Microsoft Security has a central presence at this year's [Black Hat USA](#), taking place August 5 to 10, 2023, at Mandalay Bay in Las Vegas, Nevada. If you haven't already made plans to attend, check out [our previous blog post](#) for information about our Black Hat sessions, product demos, meetings at our booth (number 1740), and a customer happy hour.

Learn more

To learn more about Microsoft Security solutions, visit our [website](#). Bookmark the [Security blog](#) to keep up with our expert coverage on security matters. Also, follow us on LinkedIn ([Microsoft Security](#)) and Twitter ([@MSFTSecurity](#)) for the latest news and updates on cybersecurity.

¹[2023 State of the Cloud Report](#), Flexera. 2023.

²[Cloud-based cyber attacks increased by 48 percent in 2022](#), Continuity Central. January 19, 2023.

³Gartner®, Market Guide for Cloud-Native Application Protection Platforms, Neil MacDonald, et al. March 14, 2023.

⁴[The next wave of multicloud security with Microsoft Defender for Cloud, a Cloud-Native Application Protection Platform \(CNAPP\)](#), Vlad Korsunsky. March 22, 2023.

⁵[Leadership Compass: Cloud Security Posture Management](#), KuppingerCole. July 27, 2023.

⁶[Announcing Microsoft cloud security benchmark \(Public Preview\)](#), Jim Cheng. October 13, 2022.

⁷[Malware Scanning for cloud storage GA pre-announcement | prevent malicious content distribution](#), Inbal Argov. July 26, 2023.

⁸[Manage security settings for Windows, macOS, and Linux natively in Defender for Endpoint](#), Dan Levy. July 11, 2023.

⁹[Hardware-backed device attestation powers mobile workers](#), Michael Wallent. July 27, 2023.

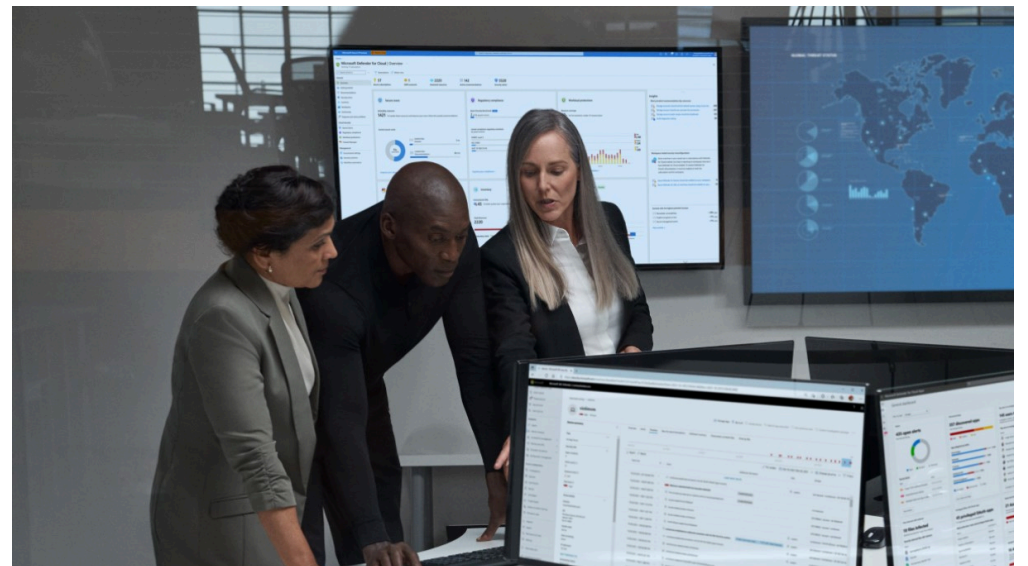
Related Posts



News [Cloud security](#) [Microsoft Purview](#) Jun 14, 2023 5 min read

[Expanding horizons—Microsoft Security's continued commitment to multicloud](#) >

Learn how to manage multicloud security risk with Microsoft's native multicloud protection for three of the industry's main cloud platforms.



Best practices [Cloud security](#) [Microsoft Defender](#) Mar 22, 2023 7 min read

[The next wave of multicloud security with Microsoft Defender for Cloud, a Cloud-Native Application Protection Platform \(CNAPP\)](#) >

Organizations are turning to cloud native application protection platforms (CNAPPs) to overcome the challenges of securing the entire cloud lifecycle. Here are the major advantages Microsoft Defender for Cloud offers as a CNAPP.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Protect it all
with Microsoft Security

Connect with us on social



What's new

- Surface Laptop Studio 2
- Surface Laptop Go 3
- Surface Pro 9
- Surface Laptop 5
- Microsoft Copilot
- Copilot in Windows
- Explore Microsoft products
- Windows 11 apps

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Certified Refurbished
- Microsoft Store Promise
- Flexible Payments

Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education
- How to buy for your school
- Educator training and development
- Deals for students and parents
- Azure for students

Business


- Microsoft Cloud
- Microsoft Security
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Copilot for Microsoft 365
- Small Business

Developer & IT

- Azure
- Developer Center
- Documentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Visual Studio

Company

- Careers
- About Microsoft
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility
- Sustainability

 English (United States)

 Your Privacy Choices Consumer Health Privacy

[Sitemap](#) [Contact Microsoft](#) [Privacy](#) [Terms of use](#) [Trademarks](#) [Safety & eco](#) [Recycling](#) [About our ads](#) © Microsoft 2024