

[News Data protection Microsoft Purview Audit](#)

3 min read

Expanding cloud logging to give customers deeper security visibility

By [Vasu Jakkal](#), Corporate Vice President, Security, Compliance, Identity, and Management

July 19, 2023



Microsoft Purview

In response to the increasing frequency and evolution of nation-state cyberthreats, Microsoft is taking additional steps to protect our customers and increase the secure-by-default baseline of our cloud platforms. These steps are the result of close coordination with commercial and government customers, and with the Cybersecurity and Infrastructure Security Agency (CISA) about the types of security log data Microsoft provides to cloud customers for insight and analysis.

Moving to the cloud gives organizations significant advantages in terms of performance, automatic software updates, and centralized security monitoring. Log data plays an important role in incident response because it provides granular, auditable insight into how different identities, applications, and devices access a customer's cloud services. These logs themselves do not prevent attacks, but they can be useful in digital forensics and incident response when examining how an intrusion might have occurred, such as when an attacker is impersonating an authorized user.

Today we are expanding Microsoft's cloud logging accessibility and flexibility even further. Over the coming months, we will include access to wider cloud security logs for our worldwide customers at no additional cost. As these changes take effect, customers can use [Microsoft Purview Audit](#) to centrally visualize more types of cloud log data generated across their enterprise.

Microsoft Purview Audit enables customers to centrally visualize cloud log data generated across their enterprise, thus helping them effectively respond to security events, forensic investigations, internal investigations and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded and retained in customers unified Purview Audit logs.

As our expanded logging defaults roll out, **Microsoft Purview Audit (Standard)** customers will receive deeper visibility into security data, including detailed logs of email access and more than 30 other types of log data previously only available at the Microsoft Purview Audit (Premium) subscription level. In addition to new logging events becoming available, Microsoft is also increasing the default retention period for Audit Standard customers from 90 days to 180 days.

Commercial and government customers with E5/G5 licenses already using **Microsoft Purview Audit (Premium)** will continue to receive access to all available audit logging events, including intelligent insights, which help determine the scope of potential compromise by using the Audit log search in the Microsoft Purview compliance portal and the Office 365 Management Activity API. Additional [Audit Premium](#) features include longer default retention periods and automation support for importing log data into other tools for analysis.

Today's news comes as a result of our close partnership with CISA, which has called for the industry to take action in order to

better protect itself from potential cyberattacks. It also reflects our commitment to engaging with customers, partners, and regulators to address the evolving security needs of the modern world.

Microsoft is deeply committed to building a safer world for all, and over the last years has continued to build solutions that are secure by design with built-in chip-to-cloud technology, our security development cycle, and [multifactor authentication default settings](#). Today is another milestone in that commitment and we are grateful to work in close coordination with CISA and our customers as we continue to invest in our built-in security and other protections.

"After working collaboratively for over a year, I am extremely pleased with Microsoft's decision to make necessary log types available to the broader cybersecurity community at no additional cost," said CISA Director Jen Easterly. "While we recognize this will take time to implement, this is truly a step in the right direction toward the adoption of Secure by Design principles by more companies. We will continue to work with all technology manufacturers, including Microsoft, to identify ways to further enhance visibility into their products for all customers."

Microsoft will begin rolling out these logging updates in September 2023 to all government and commercial customers. To access existing and new logs as they become available, visit the [Microsoft Purview compliance portal](#) and select Audit from the Solutions panel. Microsoft has historically provided security log data to customers, with options to maintain logs through Microsoft's storage services or with other security and storage vendors, depending on preferences. Different customers have varying preferences and needs for where they save their audit logs, how they are analyzed, and how long they are retained. We know customers have multiple issues to consider, including data storage capacity and which Microsoft or third-party log management tools they want to use, and our newly expanding, flexible logging options help customers decide what is best for their requirements.

Cybersecurity is a team sport relying on trust and transparency, which is why we are pleased to share today's cloud logging announcement as the result of thoughtful conversations between our security experts, customers, and influential authorities like CISA. We look forward to keeping the community posted on this [expanded logging rollout](#) and sharing additional news moving forward.

Learn more

Learn more about [Microsoft Purview Audit](#).

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.

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](#)

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](#)