Auditing in Microsoft 365

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Auditing in Microsoft Purview

- Microsoft Purview Audit (Standard)
- Microsoft Purview Audit (Premium)

Auditing in Microsoft Purview

Auditing in Microsoft Purview

Audit (Standard)

Included in all licenses

Audit (Premium)

Available for organizations with an Office 365 E5/A5/G5 or Microsoft 365 Enterprise E5/A5/G5 subscription

Core Auditing in Microsoft Purview: Audit Standard

Unified Audit Log

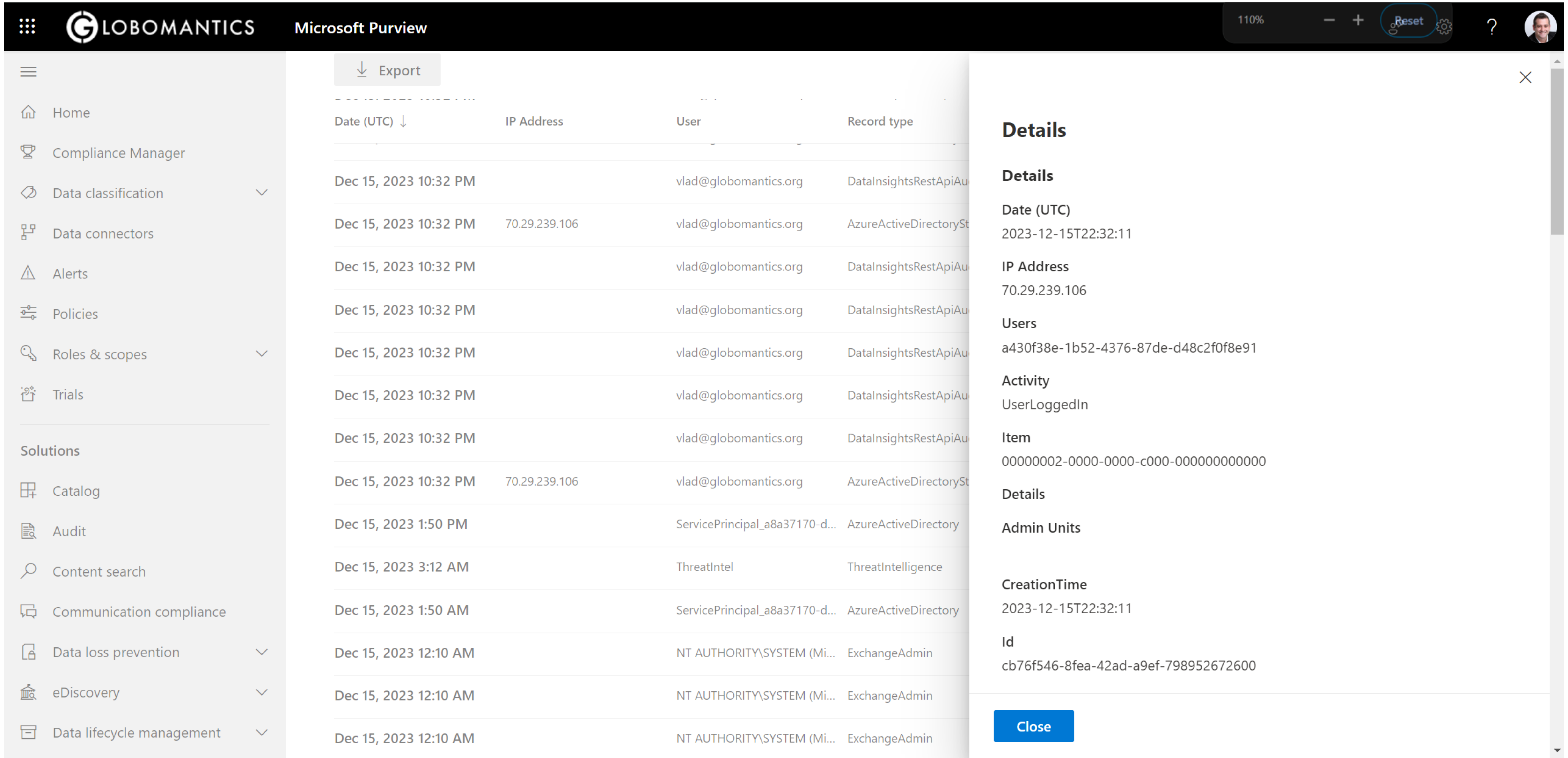
- Centralized Audit Log that contains most Microsoft 365 activities

Audit records retained for 180 days

APIs allow you to export audit logs into your own systems to keep longer

- You can also simply export to CSV

Audit Log Example



Date (UTC) ↓	IP Address	User	Record type
Dec 15, 2023 10:32 PM		vlad@globomantics.org	DataInsightsRestApiAu
Dec 15, 2023 10:32 PM	70.29.239.106	vlad@globomantics.org	AzureActiveDirectorySt
Dec 15, 2023 10:32 PM		vlad@globomantics.org	DataInsightsRestApiAu
Dec 15, 2023 10:32 PM		vlad@globomantics.org	DataInsightsRestApiAu
Dec 15, 2023 10:32 PM		vlad@globomantics.org	DataInsightsRestApiAu
Dec 15, 2023 10:32 PM		vlad@globomantics.org	DataInsightsRestApiAu
Dec 15, 2023 10:32 PM		vlad@globomantics.org	DataInsightsRestApiAu
Dec 15, 2023 10:32 PM	70.29.239.106	vlad@globomantics.org	AzureActiveDirectorySt
Dec 15, 2023 1:50 PM		ServicePrincipal_a8a37170-d...	AzureActiveDirectory
Dec 15, 2023 3:12 AM		ThreatIntel	ThreatIntelligence
Dec 15, 2023 1:50 AM		ServicePrincipal_a8a37170-d...	AzureActiveDirectory
Dec 15, 2023 12:10 AM		NT AUTHORITY\SYSTEM (Mi...	ExchangeAdmin
Dec 15, 2023 12:10 AM		NT AUTHORITY\SYSTEM (Mi...	ExchangeAdmin
Dec 15, 2023 12:10 AM		NT AUTHORITY\SYSTEM (Mi...	ExchangeAdmin

Details

Details

Date (UTC)
2023-12-15T22:32:11

IP Address
70.29.239.106

Users
a430f38e-1b52-4376-87de-d48c2f0f8e91

Activity
UserLoggedIn

Item
00000002-0000-0000-c000-000000000000

Details

Admin Units

CreationTime
2023-12-15T22:32:11

Id
cb76f546-8fea-42ad-a9ef-798952672600

Microsoft Purview Audit (Premium) Additional Features

Long-term retention of audit logs

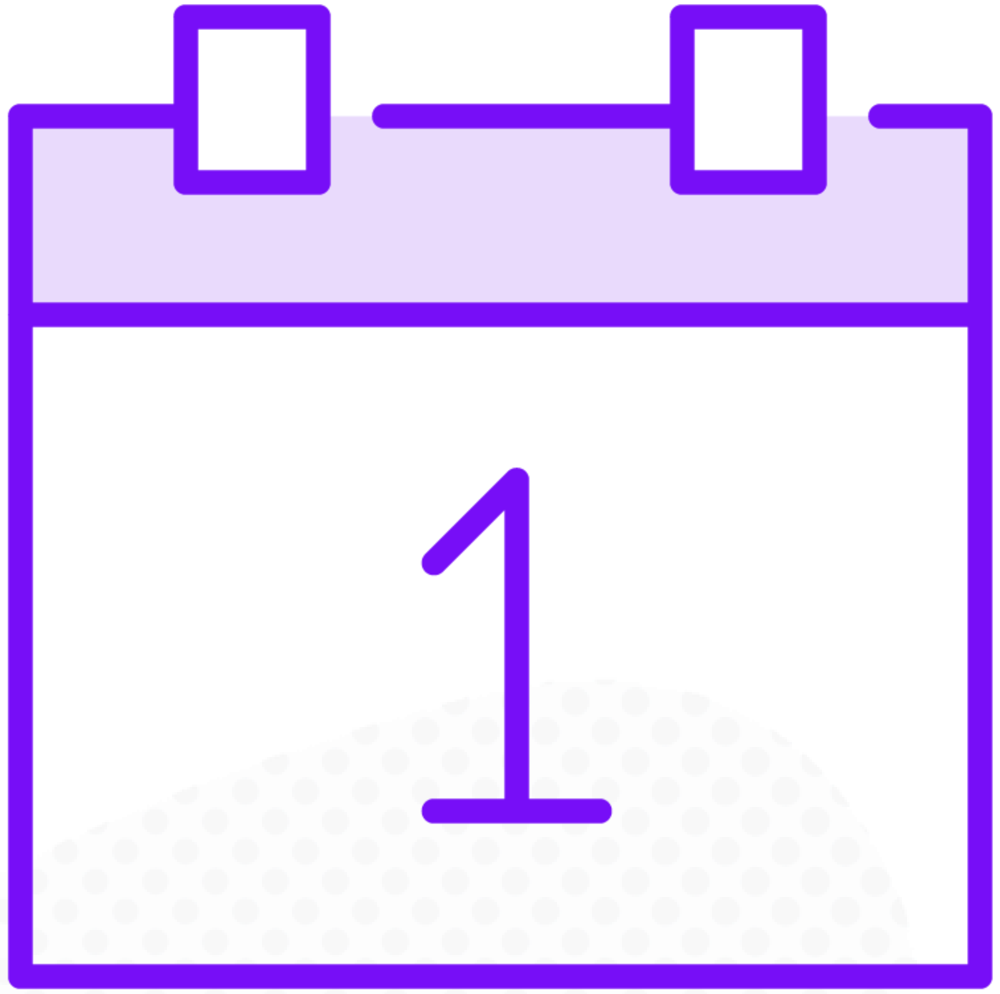
High-bandwidth access to the Office 365 Management Activity API

Long-term Retention of Audit Logs

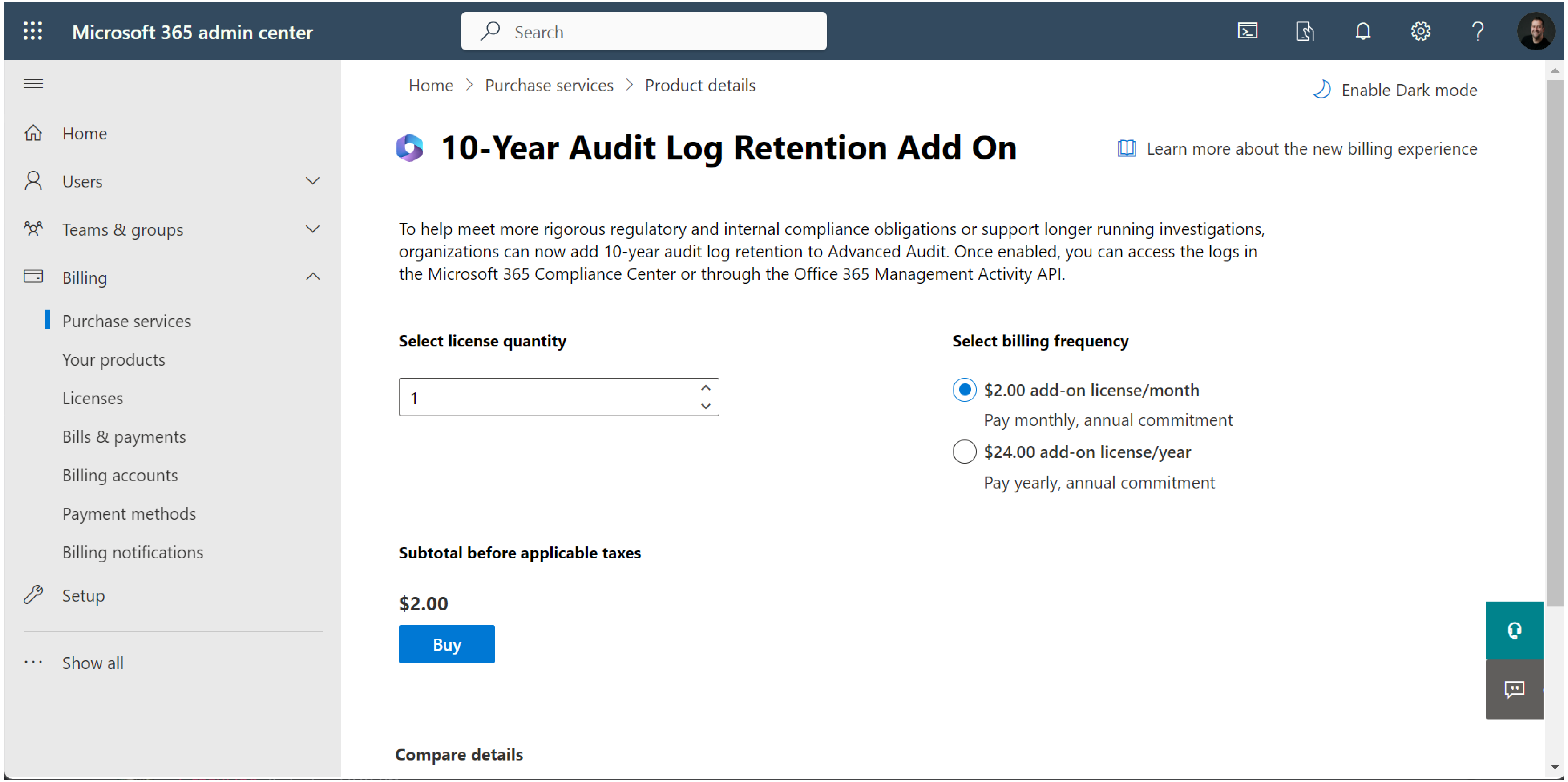
Audit Premium retains the following audit records for one year

- Exchange
- SharePoint
- Microsoft Entra

There is an available add-on license to increase retention for up to 10 years!



10-year Audit Log Retention Add On



10-Year Audit Log Retention Add On

To help meet more rigorous regulatory and internal compliance obligations or support longer running investigations, organizations can now add 10-year audit log retention to Advanced Audit. Once enabled, you can access the logs in the Microsoft 365 Compliance Center or through the Office 365 Management Activity API.

Select license quantity

1

Select billing frequency

● $2.00 add-on license/month
Pay monthly, annual commitment

○ $24.00 add-on license/year
Pay yearly, annual commitment

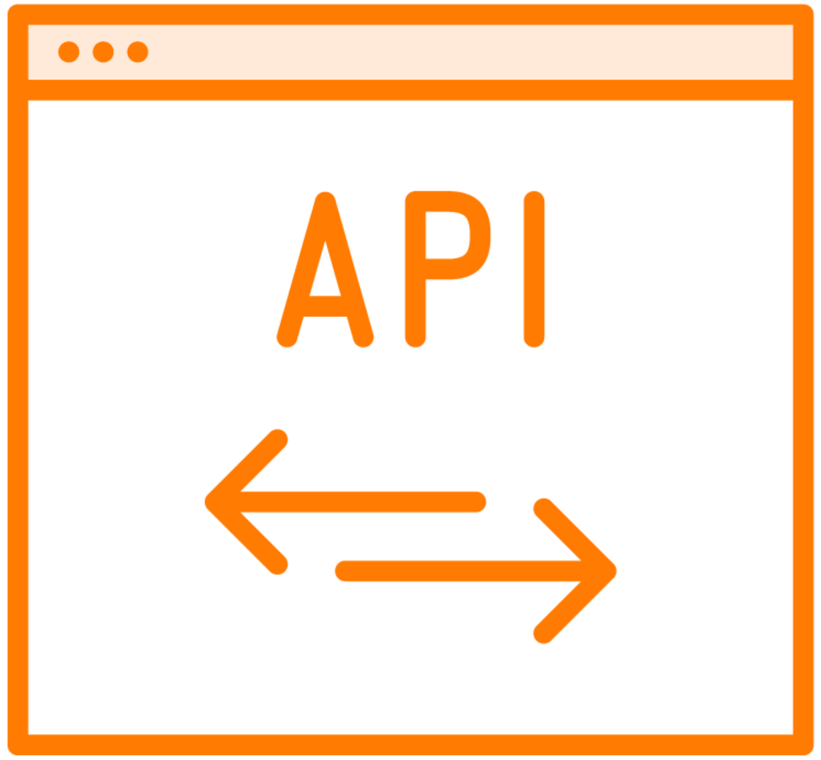
Subtotal before applicable taxes

$2.00

Buy

Compare details

High-bandwidth Access to the Office 365 Management Activity API



Allows organizations that use the API to access Audit Log data with a higher bandwidth limit

- Less throttling

Twice as much as non-premium organizations

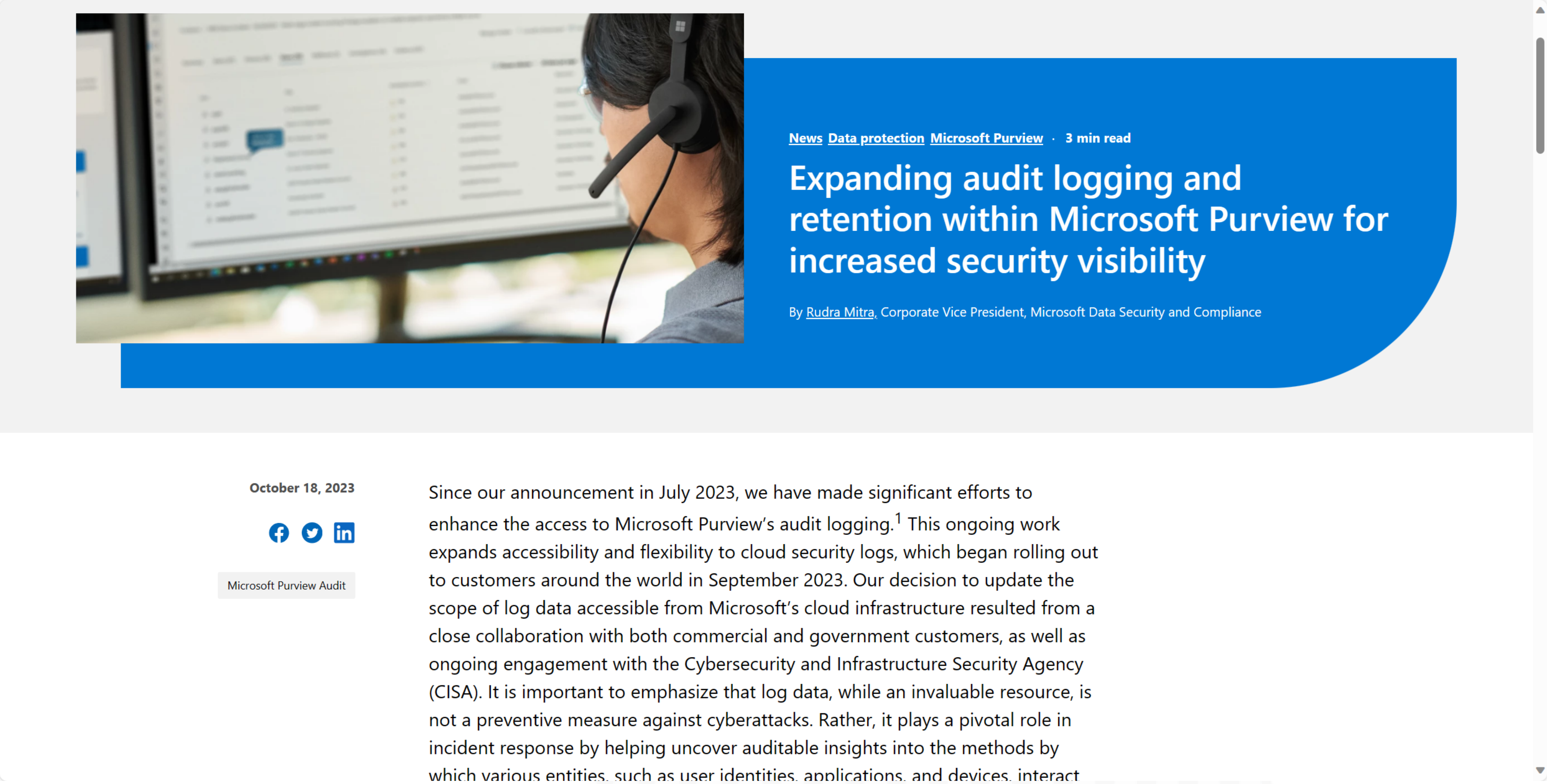
- At least 2,000 requests per minute
  - Limit dynamically increases depending on seat count and licenses

Microsoft made major changes to Purview audit licensing in October 2023

Before October 2023:

- Audit (Standard) retention was only 90 days
- Only Audit (Premium) offered some critical activities

Old documentation might still refer to the previous numbers



News Data protection Microsoft Purview · 3 min read

Expanding audit logging and retention within Microsoft Purview for increased security visibility

By Rudra Mitra, Corporate Vice President, Microsoft Data Security and Compliance

October 18, 2023

Microsoft Purview Audit

Since our announcement in July 2023, we have made significant efforts to enhance the access to Microsoft Purview's audit logging.[1] This ongoing work expands accessibility and flexibility to cloud security logs, which began rolling out to customers around the world in September 2023. Our decision to update the scope of log data accessible from Microsoft's cloud infrastructure resulted from a close collaboration with both commercial and government customers, as well as ongoing engagement with the Cybersecurity and Infrastructure Security Agency (CISA). It is important to emphasize that log data, while an invaluable resource, is not a preventive measure against cyberattacks. Rather, it plays a pivotal role in incident response by helping uncover auditable insights into the methods by which various entities, such as user identities, applications, and devices, interact

https://www.microsoft.com/en-us/security/blog/2023/10/18/expanding-audit-logging-and-retention-within-microsoft-purview-for-increased-security-visibility

Demo

Exploring the Audit Log

Module Conclusion

Auditing in Microsoft Purview

Microsoft Purview Audit (Standard)

- Most Microsoft 365 activities
- 180 days retention

Microsoft Purview Audit (Premium) has additional features

- Long-term retention of audit logs
  - 1 year
- High-bandwidth access to the Office 365 Management Activity API
  - At least double

Microsoft offers a 10-year Audit Log Retention Add On

Up Next:

Resource Governance in Azure