Lepide Data security. **Simplified.**

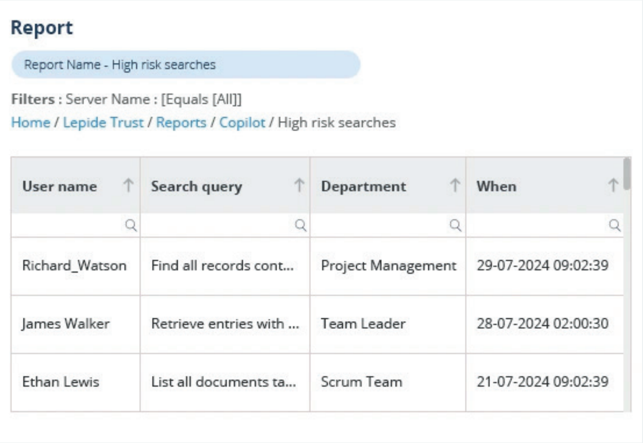
Microsoft 365 Copilot Security

Ensure that your sensitive data remains secure before, during and after the implementation of Microsoft 365 Copilot. Understand who has access, why they have access and what is happening to your data.

Minimize your threat surface to avoid the unintentional exposing of sensitive information and keep your Microsoft 365 Copilot data secure. Identify, classify and monitor all AI created data and detect and respond to any suspicious Copilot user behavior with the Lepide Copilot Security Solution.

Detect high risk Copilot searches.

Detect and respond to high-risk searches that your copilot users are making, including requests to access sensitive information. Lepide also learns what normal behavior for your Copilot users looks like and will generate automated threat responses in real time when anomalies are detected. Our AI-backed anomaly spotting removes false positives to ensure accurate threat detection.



Report

Report Name - High risk searches

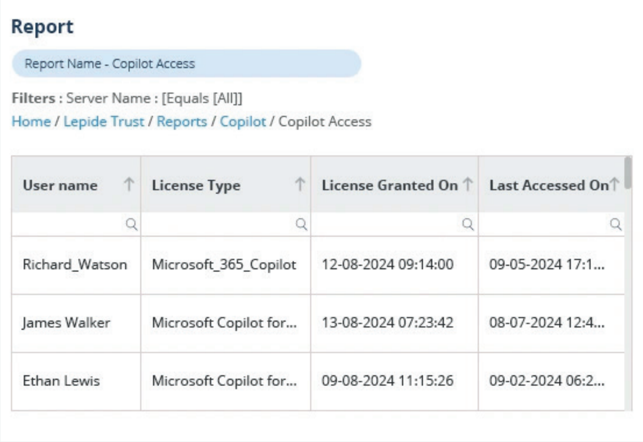
Filters : Server Name : [Equals [All]]

Home / Lepide Trust / Reports / Copilot / High risk searches

User name	Search query	Department	When
Richard_Watson	Find all records cont...	Project Management	29-07-2024 09:02:39
James Walker	Retrieve entries with ...	Team Leader	28-07-2024 02:00:30
Ethan Lewis	List all documents ta...	Scrum Team	21-07-2024 09:02:39

Monitor Copilot access.

Lepide enables you to see who has what levels of access within Copilot, including their license type, when the license was granted, and when it was last used. Use this information to make informed decisions on who needs what levels of access, so that you can limit the exposure of your sensitive data.



Report

Report Name - Copilot Access

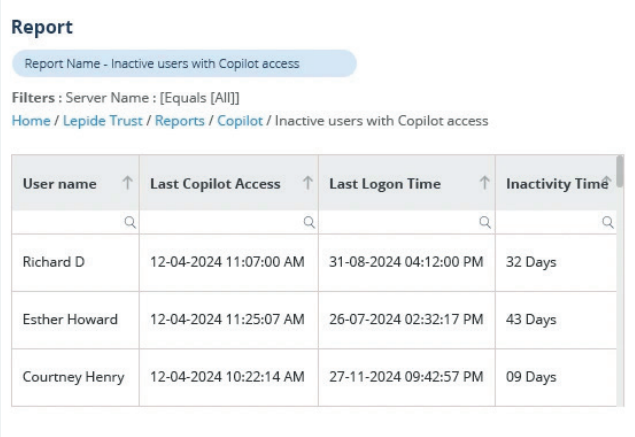
Filters : Server Name : [Equals [All]]

Home / Lepide Trust / Reports / Copilot / Copilot Access

User name	License Type	License Granted On	Last Accessed On
Richard_Watson	Microsoft_365_Copilot	12-08-2024 09:14:00	09-05-2024 17:1...
James Walker	Microsoft Copilot for...	13-08-2024 07:23:42	08-07-2024 12:4...
Ethan Lewis	Microsoft Copilot for...	09-08-2024 11:15:26	09-02-2024 06:2...

Identify inactive users with Copilot access.

Inactive users do not need access to Copilot. If an attacker were to gain access to an inactive user account, they would have a simple way to breach sensitive data. With Lepide, you can identify all users that have Copilot access that are also inactive so that you can reduce your threat surface area.



Report

Report Name - Inactive users with Copilot access

Filters : Server Name : [Equals [All]]

Home / Lepide Trust / Reports / Copilot / Inactive users with Copilot access

User name	Last Copilot Access	Last Logon Time	Inactivity Time
Richard D	12-04-2024 11:07:00 AM	31-08-2024 04:12:00 PM	32 Days
Esther Howard	12-04-2024 11:25:07 AM	26-07-2024 02:32:17 PM	43 Days
Courtney Henry	12-04-2024 10:22:14 AM	27-11-2024 09:42:57 PM	09 Days

Want to see it in action?

Request a demo