

Increasing my Identity Security with Microsoft Security Copilot

Jan Vidar Elven

Seniorarkitekt Evidi AS | MVP Security | @JanVidarElven

MVP
Dagen

Jan Vidar Elven

Evidi AS

```
{  
  "MVP": "Security",  
  "Awards": 8,  
  "Title": "Senior Architect",  
  "Organization": "Evidi",  
  "Blog": "http://gotoguy.blog",  
  "SoMe": "@JanVidarElven"  
}
```



Takk til vår sponsor i dag

The logo for Itera, featuring the word "ITERA" in a bold, white, sans-serif font. The letters are spaced out and centered within a solid black rectangular background.

I T E R A

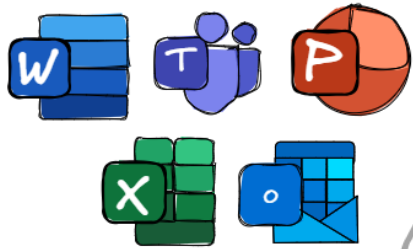
What do we know about Security Copilot?

How to present a talk about Security Copilot without having access to Security Copilot..?

..ok, thanks for coming to this talk ;)

Microsoft 365 Copilot System

Microsoft 365 Apps



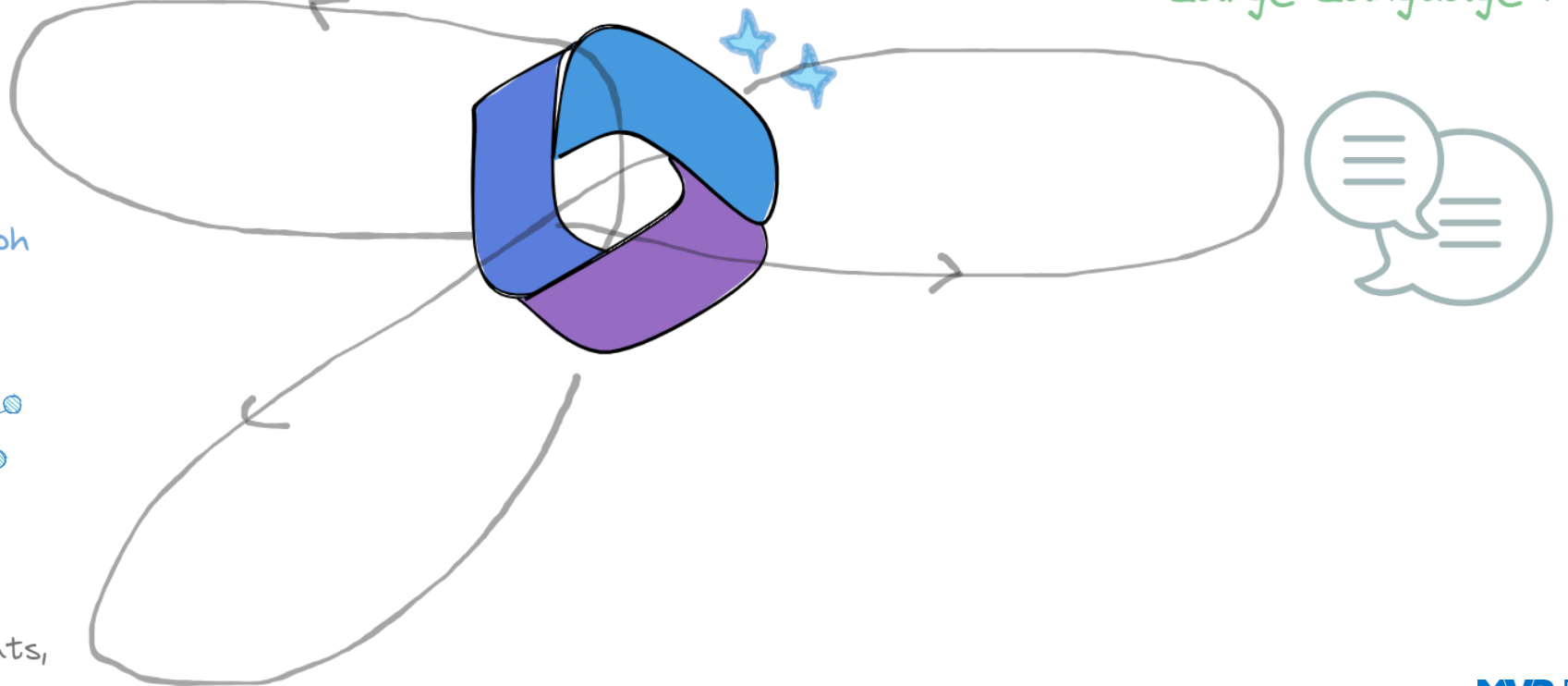
Microsoft 365 Copilot

Large Language Model

Microsoft Graph



-Your data-
emails, files, meetings, chats,
calendars, contacts



Microsoft 365 Apps

Microsoft 365 Copilot

Microsoft 365 Service Boundary

Large Language Model

Azure OpenAI instance is maintained by Microsoft. OpenAI has no access to the data or the model.

Azure OpenAI

RAI is performed on input prompt and output results

Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation models

Modified prompt

LLM response

Microsoft Graph

Semantic Index

Your context and content
emails, files, meetings, chats,
calendars, and contacts

Customer Microsoft 365 Tenant

Response + app commands

User prompt

Pre-processing

Grounding

Grounding

Post-processing

Data flow (🔒 = all requests are encrypted via HTTPS and wss://)

- 1 User prompts from Microsoft 365 Apps are sent to Copilot
- 2 Copilot accesses Graph and Semantic Index for pre-processing
- 3 Copilot sends modified prompt to Large Language Model
- 4 Copilot receives LLM response
- 5 Copilot accesses Graph and Semantic Index for post-processing
- 6 Copilot sends the response, and app command back to Microsoft 365 Apps

How the Microsoft Security Copilot System Works



Microsoft

Security Copilot System

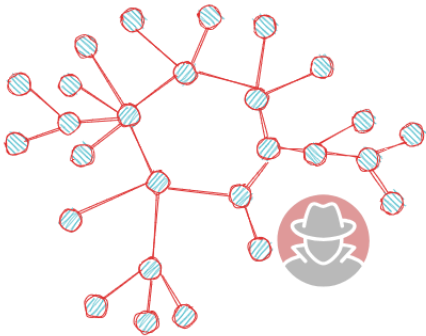
Microsoft Security Portfolio



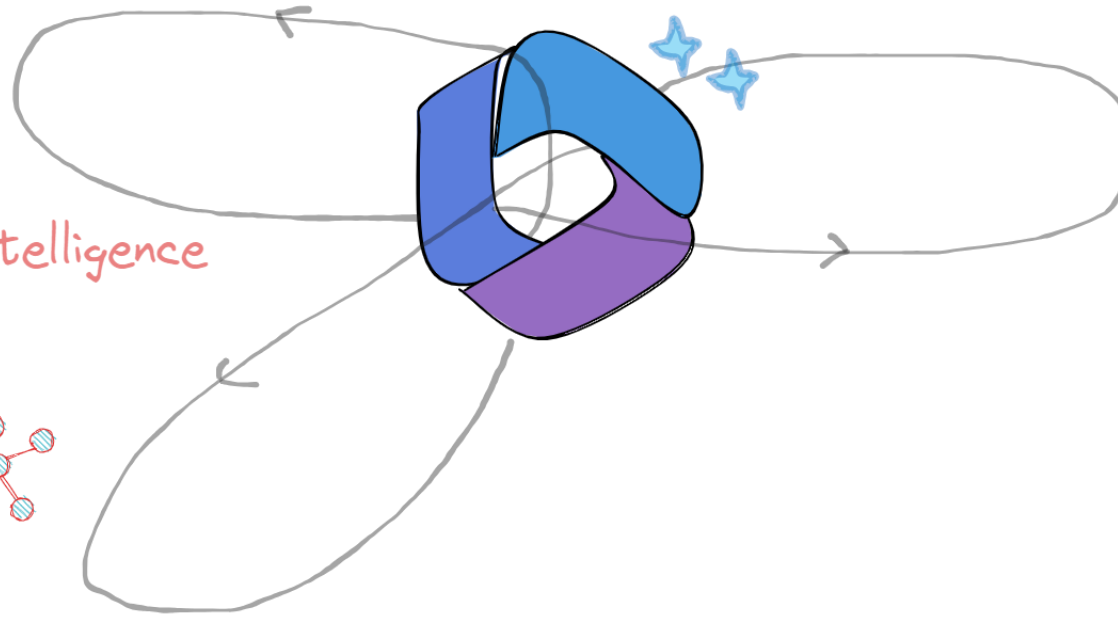
Microsoft Security Copilot

Large Language Model

Microsoft Threat Intelligence



-Your data-
endpoints, users, applications



Why Security Pilot?

- The odds are against today's Security Analysts
- Paradigm shift with AI
- Tools consolidation and Generative AI can transform security

💡 Tell me about my latest incidents.

💡 Are any of my machines affected?

💡 Summarize this incident in PowerPoint.

💡 Which alerts are being triggered the most?

💡 What is log4shell?

💡 How can I improve my security posture?



DEMO

Security Copilot (Video)



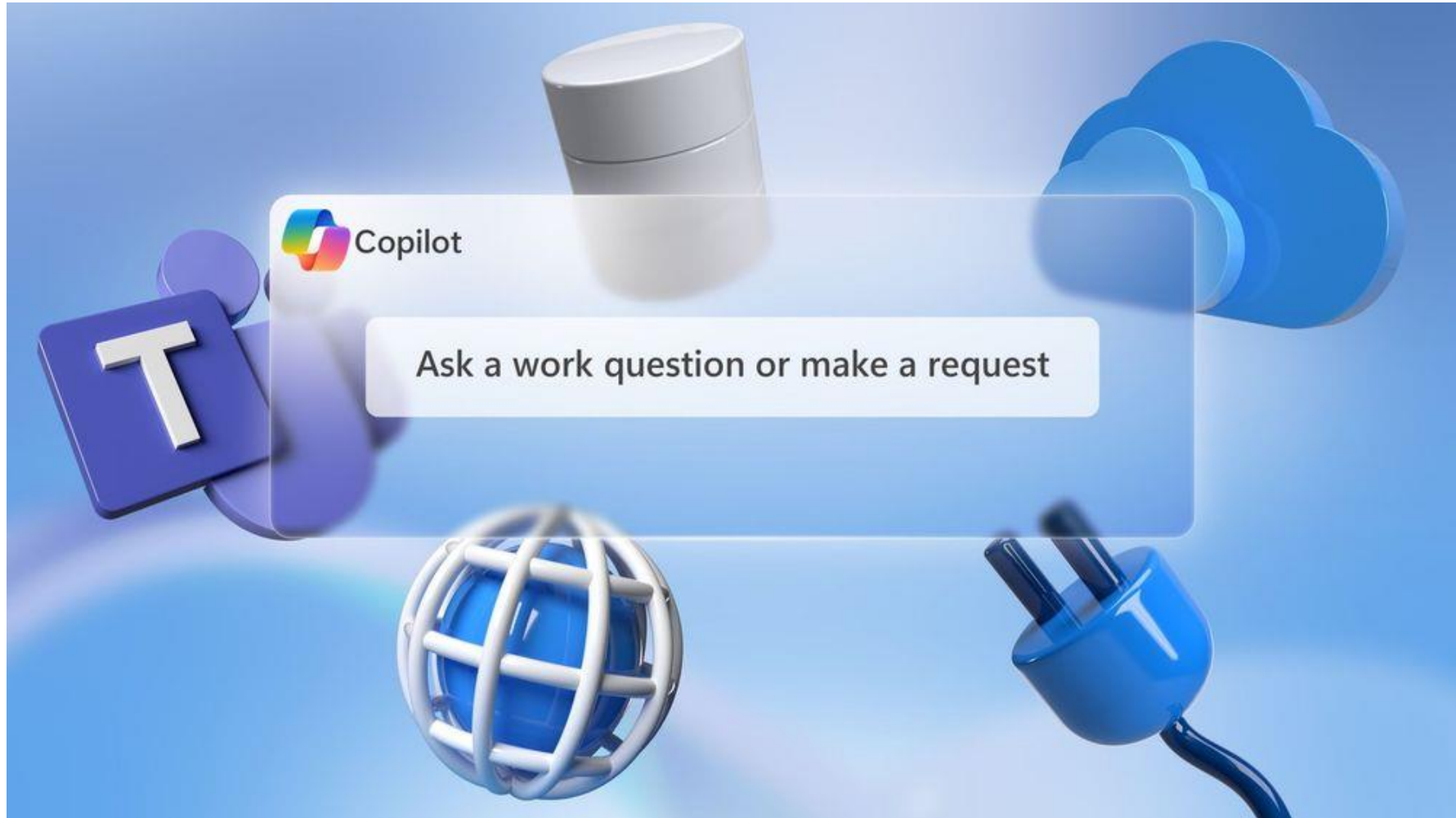
Microsoft Security Copilot

AI-powered security assistance for Microsoft 365, Azure, and Windows



Microsoft

Copilot and External Data



Azure OpenAI on your Data

- Works with GPT-35-Turbo and GPT-4 LLMs
- Access via OpenAI Studio or REST API
- Uses Azure Cognitive Search index
- Data formats and file types
 - .txt, .md, .html, Word & PowerPoint files, PDF
- Source blob storage or local files

Cognitive Services Preview Data Sources

Preview data sources by Cognitive Search

New data sources are issued as preview features. [Sign up](#) to get started.

Azure Cosmos DB for Apache Gremlin

by [Cognitive Search](#)

Connect to Azure Cosmos DB for Apache Gremlin to extract items from a container, serialized into JSON documents, and imported into a search index as search documents. Configure change tracking to refresh the search index with the latest changes in your database.

[More details](#)



Azure Cosmos DB for MongoDB

by [Cognitive Search](#)

Connect to Azure Cosmos DB for MongoDB to extract items from a container, serialized into JSON documents, and imported into a search index as search documents. Configure change tracking to refresh the search index with the latest changes in your database.

[More details](#)



SharePoint

by [Cognitive Search](#)

Connect to a SharePoint site and index documents from one or more document libraries, for accounts and search services in the same tenant. Text and normalized images will be extracted by default. Optionally, you can configure a skillset for more content transformation and enrichment, or configure change tracking to refresh a search index with new or changed content in SharePoint.

[More details](#)



Azure MySQL

by [Cognitive Search](#)

Connect to MySQL database on Azure to extract rows in a table, serialized into JSON documents, and imported into a search index as search documents. On subsequent runs, assuming High Water Mark change detection policy is configured, the indexer will take all changes, uploads, and delete and reflect those changes in your search index.

[More details](#)



Azure Files

by [Cognitive Search](#)

Connect to Azure Storage through Azure Files share to extract content serialized into JSON documents, and imported into a search index as search documents.

[More details](#)

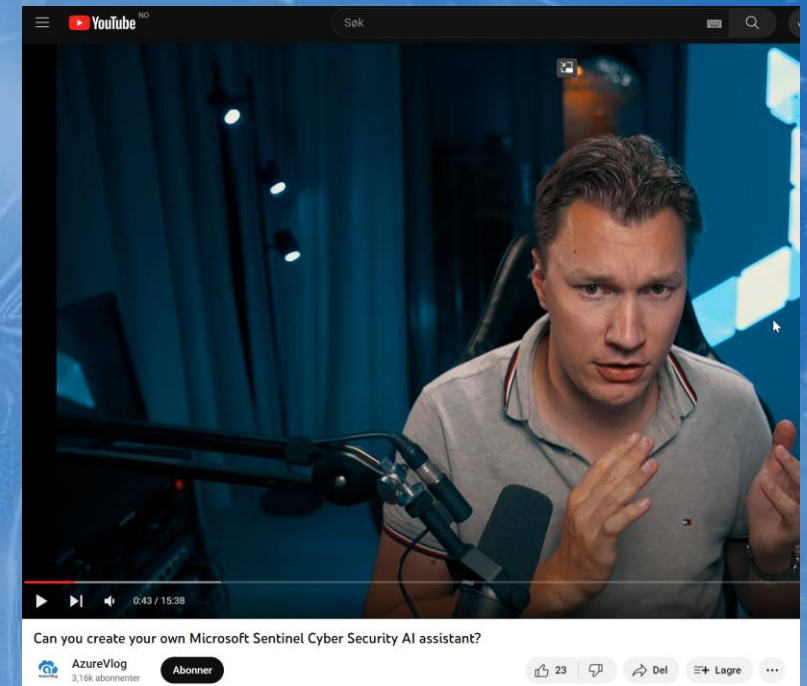




[https://youtu.be/L31mYYUt75o?
si=BcvUhSOsst89FE4B](https://youtu.be/L31mYYUt75o?si=BcvUhSOsst89FE4B)

DEMO

Security AI Assistant for Sentinel via Azure OpenAI



Possible Use Cases for OpenAI and Security

- Bring your own data to Azure OpenAI
 - Storage Account Blob
 - Cognitive Services Search (including Preview sources)
 - Partner
 - Document-level access control (Security filters)
- Data Sources for Security
 - Microsoft Security Products
 - Microsoft Graph

How to Prepare for Security Copilot?

- Implement Microsoft Security Products
 - Microsoft Defender for Endpoints
 - Microsoft Sentinel
 - Intune
- Microsoft Learn
- Microsoft Ignite November 15-16





Tusen takk!

MVP-Dagen