



# Safely Enabling AI Copilots with Varonis

Jack Eid

Regional Sales Manager

April 2025





Search



- Activity
- Chat
- Teams
- Calendar
- Calls
- Files
- ...
- Apps

### Feed

Unread only

**Meeting Recap** 10:00 am  
 Here's a recap of a missed meeting  
 Core accounts business review

**Sarah mentioned you in 5 channels** 3:45 pm  
 Hi all - I've attached the document that we discussed today.

**Marie mentioned you** 12:58 pm  
 Thanks Samantha, I'll fix that!  
 Chat with Marie

**Will posted** 11:39 am  
 I've attached the file we discussed...  
 Northwind Traders > Marketing

**Daichi mentioned Tailspin Toys** 8/20  
 Tailspin Toys team, our meeting is...  
 Tailspin Toys > Accounting

**Alvin posted an announcement** 3:45 am  
 We're going live with our latest pro...  
 Yammer Communities

**Sarah +2 reacted** 7:15 am  
 I prefer the blue one  
 Chat with Reta, Miguel, +3

**Voicemail from Marie** 8/23  
 (121)-489-1902

**Northwind Traders is** 8/22

### Marie Beaudouin Chat Files +



Marie Beaudouin 11:25 AM

Yes that would be wonderful.

I'll make a reservation for next week.

Sound good?



Yeah, we haven't gotten lunch together in awhile either!  
 We should go back to that ramne place. I've been craving it the last few days  
 ramen\*

11:28 AM

I would love that!



Marie Beaudouin 11:05 AM  
 Here is the latest spec doc we reviewed with the engineers this mo...

Oh btw Marie, I noticed in the document that there's a typo on the second page

Marie Beaudouin 11:35 AM

Thanks **Samantha**, I'll fix that!

Type a new message



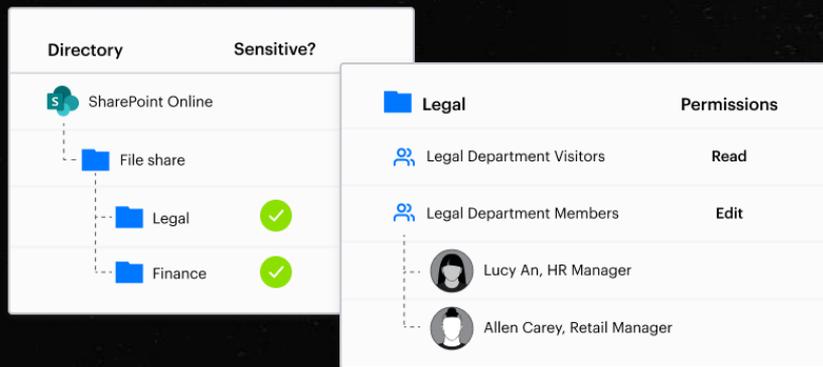




All [Microsoft] partners noted that **security** and **privacy** concerns continue to be the primary issue to [Copilot] adoption

- Karl Keirstead, UBS Research





## How do Copilot security controls work?

- + User inputs a prompt in an app like Word, Outlook, or PowerPoint
- + Microsoft gathers business content **based on the user's M365 permissions**
- + Modified prompt is sent to the LLM to create a response
- + Microsoft performs post-processing responsible AI checks



You

How do I prepare for Copilot for 365?



Copilot

To prepare for **Microsoft 365 Copilot**, follow these steps:

1. **Get Your Organization's Information Ready for Search:**

Ensure you have **Just Enough Access permissions** in place for each user.

2. **Put Microsoft 365 Copilot Prerequisites in Place:**

- Assign **Copilot licenses** to users and groups to provide them access<sup>2</sup>.
- Identify Microsoft 365 security features that control oversharing of data in Copilot<sup>2</sup>.

3. **Drive Adoption:**

- Create a **Copilot Center of Excellence** to promote awareness and adoption within your organization<sup>2</sup>.

Remember that Copilot users must have either a **Microsoft 365 E3 or E5 license** and an **Azure Active Directory account**. Once available to your organization, users should be on the **Current Channel or Monthly Enterprise Channel** for Microsoft 365 apps to have access to Copilot in desktop clients

**What can someone  
really do?**



# Copilot

For Microsoft 365

## What's new?

What's the latest from **person**, organized by emails, chats, and files?

## Get the gist

Give me a bullet list of key points from **file**

## Draft an FAQ

Create an FAQ based on **file**

## How to

How do I write a request for proposal?

## Generate ideas

List ideas for a fun remote team building event

## Help me write

Write an email to my team about our top priorities for next quarter from **file**

OK, what can I help with? Try one of the examples or enter your own prompt.

# Why does this happen?

# The graph is growing relentlessly

Annual data  
growth rate

23%

Microsoft 365  
pilot

Unique permissions  
to manage

40M

ChatGPT

Files open to  
every employee

17M

einstein

# Security Challenges in the Age of AI

- Employees have access to far too much data
- Sensitive data is often not labeled or mislabeled
- Insiders can quickly find and exfiltrate data
- Attackers can find secrets for privilege escalation and lateral movement
- Right-sizing access and enforcing least privilege is impossible to do manually
- Generative AI can create net new sensitive data extremely fast



These are the **same**  
**problems** we've had for  
years!



# Safely Enabling Copilot with Varonis



**Varonis' integration gives customers the added security and compliance controls necessary to quickly and confidently adopt Microsoft Copilot for M365.**

Anat Gil, Partners Lead, Microsoft



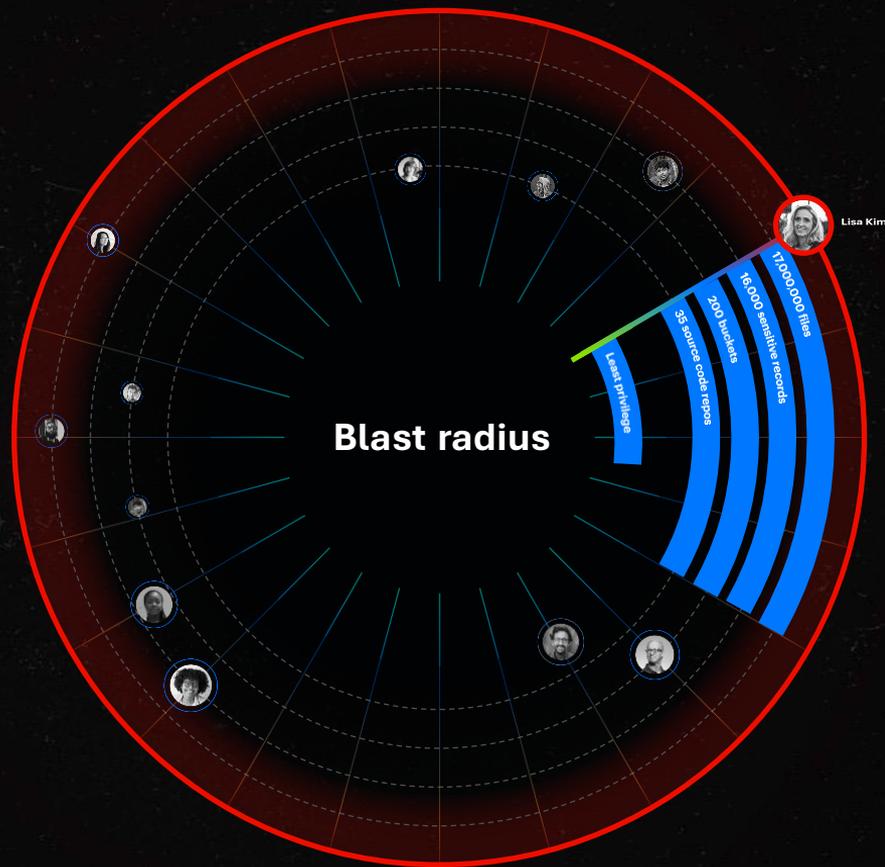
# Varonis delivers real outcomes.

 Real-time understanding of risk

 Continuously reduced blast radius

 Data-centric detection

 Simplified compliance, labeling

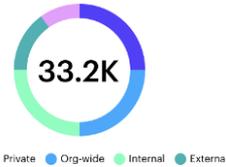


# Phase 1: Before Copilot

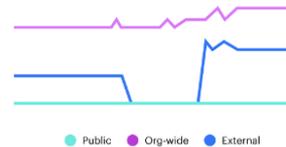
# 1. Deploy and Complete Initial Scans

- ✓ Data sensitivity
- ✓ Configuration and security posture
- ✓ Access controls and shared links
- ✓ Connected third-party apps
- ✓ Existing labels

Overall data security posture



Sensitive data by exposure



Open misconfigurations



## 2. Add/Fix Purview Sensitivity Labels

- + Automatically identify files that are missing or don't have accurate labels
- + Automatically identify and fix misapplied labels
- + Automatically identify and fix files with missing labels

File	Classification results	Classification labels
	PCI	
	GDPR, PII	 
	CCPA, PII	 

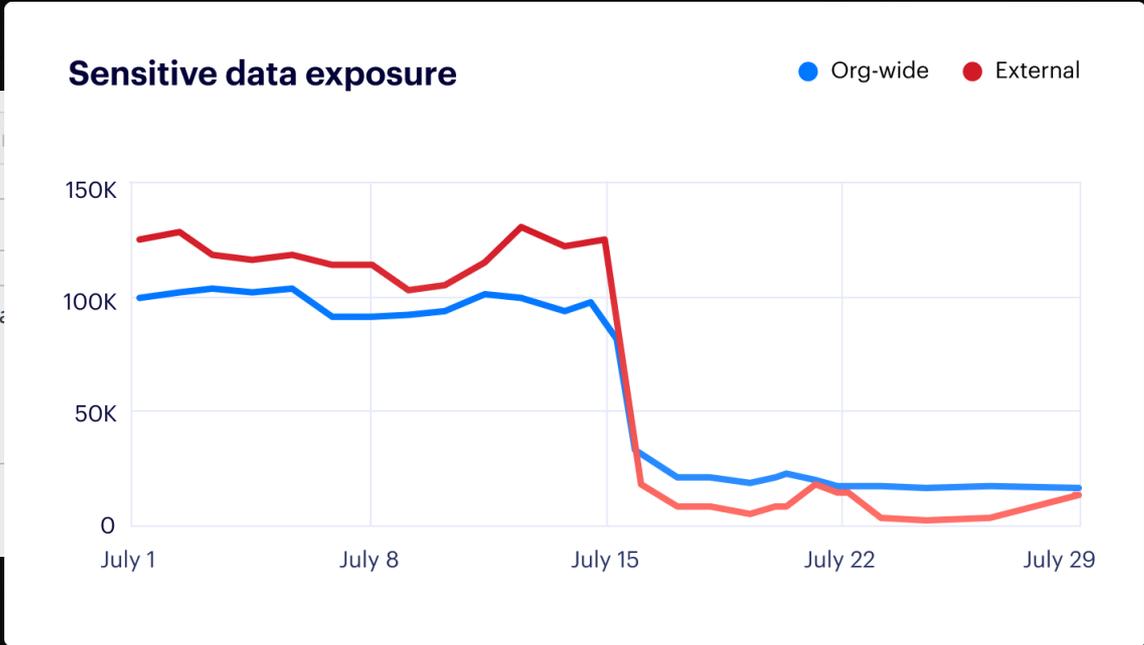
# 3. Remediate High Risk Exposure

Type: Remove collaboration link

Policy name: Remove "Anyone in the

Description: This policy removes collaboration links with the link" type.

State:  Enabled



# 4. Review Access to Critical Data

Resources

display sensitive files available to large numbers of users in 365 Cancel Saved searches

**379** Results

51 Unique resources | 51 Protected resources | 322 Direct sensitive resources | 17 Resources with anyone exposure | 56 Resources with org-wide exposure | 314 Resources with stale access

Attributes | Actions | Export Items per page 100

Resource

- Classification categories... (6)
- Classification labels (dir... (1)
- Classification rules (dir... (44)
- Exposure level (3)
- File servers (3)
- Mailbox type (1)
- Platforms (3)
- Protected (13.5%)
- Resource types (7)
- Sensitive (direct) (85.0%)
- Site types (3)
- Stale (69.7%)

Drag here to set row groups						
	Sensiti...	Path	Total Record Count (...)	Modify Date	Classification Results	
<input type="checkbox"/>	Yes	/sites/HR/Documents/Salary and Compensation/UK	522	11/01/2022 5:46 PM	UK Data Protection Act 1998 (204/2	
<input type="checkbox"/>	Yes	/sites/HR/Documents/Salary and Compensation/Cyprus	520	11/01/2022 5:46 PM	PCI Data Security Standards (PCI-D	
<input type="checkbox"/>	Yes	/sites/HR/Documents/Salary and Compensation/UK/UsersUK.csv	488	11/01/2022 5:47 PM	UK Data Protection Act 1998 (190/1	
<input type="checkbox"/>	Yes	/sites/HR/Documents/Salary and Compensation/Cyprus/UsersUK.csv	488	11/01/2022 5:47 PM	UK Data Protection Act 1998 (190/1	
<input type="checkbox"/>	Yes	/personal/elenacabrera_varonistest226_onmicrosoft_com/Documents/SEC R...	256	12/07/2022 2:29 PM	California SB-1386 (18/18),HIPAA P	
<input type="checkbox"/>	Yes	/sites/Legal/Documents/Corporate/Web stuff	246	11/01/2022 5:44 PM	PCI Data Security Standards (PCI-D	
<input type="checkbox"/>	Yes	/personal/margaretcoakley_varonistest226_onmicrosoft_com/Documents/A...	231	12/07/2022 2:51 PM	MA 201 CMR 17 (33/33),GLBA (G	
<input type="checkbox"/>	Yes	/sites/Finance/Documents/Controllers/Finance reports/Corporate/2006/Q1 ...	202	11/01/2022 5:43 PM	US Social Security Number (16	
<input type="checkbox"/>	Yes	/sites/Finance/Documents/Financial Reports/alice/Billing MTIL01	168	11/01/2022 5:43 PM	Document Passwords - 2.0 (18/18),I	

# 5. Enable Downstream DLP

- ✓ Encrypt sensitive data
- ✓ Prevent risky sharing
- ✓ Block attempted exfiltration
- ✓ Apply file-level controls
- ✓ Enforce residency and retention

The screenshot shows the 'Microsoft 365 compliance' interface, specifically the 'Data Loss Prevention > Create a policy' wizard. The current step is 'Choose locations to apply the policy'. A progress bar on the left indicates the following steps: 'Choose the information to protect' (completed), 'Name your policy' (completed), 'Locations to apply the policy' (current step), 'Policy settings', 'Test or turn on the policy', and 'Review your settings'. The main content area shows a table of locations to apply the policy to, with a note: 'We'll apply the policy to data that's stored in the locations you choose.' A warning message states: 'Protecting sensitive info on Windows devices is now in preview. Learn more about the capabilities'. The table has columns for Status, Location, Included, and Excluded. Each row has a toggle switch for 'Status' (all are 'On') and buttons for 'Included' and 'Excluded'.

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All <a href="#">Choose distribution group</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	SharePoint sites	All <a href="#">Choose site</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	OneDrive accounts	All <a href="#">Choose account</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All <a href="#">Choose account</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	Devices	All <a href="#">Choose user or group</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	Microsoft Cloud App Security	All <a href="#">Choose instance</a>	None <a href="#">Exclude</a>



Microsoft 365 Copilot

**Enable Copilot**



# Phase 2: After Copilot

## 6. Monitor Copilot activity

- + Collect and enrich Copilot audit sources
  - + Compliance audit log
  - + Content Search
  - + eDiscovery
  - + Communication compliance
- + Collect and analyze all Copilot interactions — prompts and responses

Platform	Event type	Object name	Is sensitive?	Prompt
	file accessed	schema_map.xml		Find admin passwords
	file accessed	10-K Report.docx		Find social security ...
	file deleted	bonuses.xlsx		Show bonuses given
	file created	Admin		Find admin passwords
	file accessed	commissions.pdf		Show commissions ...

## CoPilot Live

Prompts Today

4,242

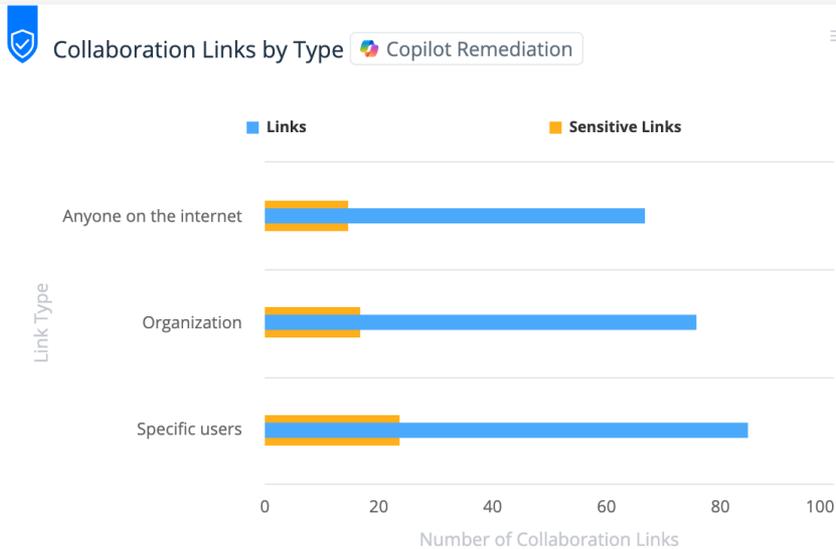
Sensitive File References Today

895

## Copilot

Data source = All

Compare over time



### Overexposed Sensitive File References



### Sensitive File References by Category

Categories All

Financial



File server = All | Generation time (UTC) = from Today | Response Contains finance | Add + | Run Search

1,080 Results

256 Unique resources | 256 Protected resources | 208 Resources with anyone exposure | 158 Resources with external exposure | 281 Resources with guest exposure | 338 Resources with org-wide exposure

Refine | Attributes | Actions | Export

Resource details

Exposure level (5)

File server - https://varonistest118...

File system owners (99)

Platform - SharePoint Online

Protected (23.7%)

Resource types (3)

Site types (3)

Stale resource (49.3%)

Unique (23.7%)

Drag here to set row groups					
	Event time	Event type	Platform	Account Name (ac)	
<input type="checkbox"/>	04/14/2024 10:59:20 AM	Interacted with Copilot	Microsoft Entra ID	Jo Smith	
<input type="checkbox"/>	04/14/2024 10:59:20 AM	File referenced by Copilot interaction	SharePoint Online	Jo Smith	
<input type="checkbox"/>	04/14/2024 10:59:20 AM	File referenced by Copilot interaction	SharePoint Online	Jo Smith	
<input type="checkbox"/>	04/08/2024 12:58:44 PM	Interacted with Copilot	Microsoft Entra ID	Jo Smith	
<input type="checkbox"/>	04/08/2024 12:58:44 PM	File referenced by Copilot interaction	SharePoint Online	Jo Smith	
<input type="checkbox"/>	04/08/2024 12:58:44 PM	Interacted with Copilot	SharePoint Online	Jo Smith	
<input type="checkbox"/>	04/08/2024 12:58:44 PM	File referenced by Copilot interaction	SharePoint Online	Jo Smith	

Copilot Conversation

Teams | User: Jo Smith | Created: March 29, 2020

Conversation | Files Reference

Which employees got raises or bonuses this year? 07/21/2020 4:55 PM

Chris Warner, a network engineer, received a 12% raise for leading a successful security overhaul, as documented in Tech Department Achievements 2024.

- Mia Wong, head of sales, was awarded a 7% raise for exceeding annual targets, noted in Annual Sales Report.

Tech Department Achievements 2024.docx | Annual Sales Report.docx

Who else received a raise? 07/21/2020 4:55 PM

In addition to Chris Warner and Mia Wong, here are more employees who received raises:

- Olivia Turner, a product designer, received a 9% raise for her innovative redesigns, as mentioned in Design Department Successes.
- Ethan Hunt, a financial analyst, was given an 8% raise for his accurate market forecasts, detailed in Finance Team Highlights.

Design Department Successes.pptx | Finance Team Highlights.docx

# 7. Alert on abnormal Copilot behavior

- + Detect inappropriate or risky interactions
- + Detect sharing of confidential information
- + Track files accessed and relevant labels
- + Apply labels as a response to alerts



3 alerts



Abnormal data access pattern  
via Copilot

## Insider threat indication

David Johnson

djohnson@company.com

inactive entity

orphaned user

no mfa

# 8. Automate Policies for Access Control

The screenshot displays a configuration window for automating access control policies. The resource is set to 'prod1.sharepoint.com'. The configuration includes several filters: 'Removal link' set to 'Yes', 'Link type' set to 'anyone on the internet' and 'org-wide', and 'Sensitive (incl. subfolders)' set to 'OneDrive' and 'SharePoint Online'. An 'Add filter' button is visible. The 'Actions' section shows a 'Remove permission' action. The 'Execute actions' dropdown is set to 'Continuously'. A line graph titled 'Org-wide sharing links' shows a sharp drop in activity starting in August.

Month	Activity Level
4/1	~50k
5/1	~50k
6/1	~75k
7/1	~75k
8/1	~0
9/1	~0

- ✓ Revoke excessive access
- ✓ Fix misconfigurations
- ✓ Fix labels
- ✓ Disable third-party apps
- ✓ Data lifecycle
- ✓ Data residency

# Operational Plan Summary

## Before Copilot:

- + Deploy Varonis
- + Complete Initial Scans
- + Add/Fix Data Labels
- + Remediate High-Risk Exposure
- + Review Access to Critical Data
- + Enable Downstream DLP with Purview

## After Copilot:

- + Ongoing Monitoring and Alerting
- + Automate Access Control Policies

# Copilot Readiness in 10 days

Varonis reduced a financial institution's Copilot exposure by 99.8% in 10 days.  
Zero impact on the business using 20 automation policies to lock down ~1 million files.

**992K**  
files

## Starting point

~1M files across the org's SharePoint, Teams, and OneDrive. Varonis quickly classified 120K sensitive files.

**57K**  
exposed files

## Identifying Copilot risk

Used Varonis to identify exposed PHI, PII, credentials at risk of being exposed via Copilot.

**99.8%**  
exposure reduction

## 10-Day Difference

Automatically eliminated ~2K sharing links and right-sized access to 57K files with Varonis policies.

**0**  
tickets complaints

## Zero customer impact

Proactively notified M365 admins of the remediation plan. The team heard zero complaints.



# Microsoft 365 Copilot Readiness Assessment

🚫 1.7K overexposed sensitive files

Platform	Classification	Exposure
	PHI PII	share externally
	PCI CCPA	share externally
	PII	share externally

**Classify and label data Copilot creates.**

**Reduce Copilot's blast radius.**

3 alerts

Cameron Hubbard accessed an anomalous number of account records

**Insider threat indication**

Cameron Hubbard  
chubbards@company.com

inactive entity orphanded user no mfa

**Monitor Copilot activity in real-time.**

Records with org-wide exposure

● All records ● Exposed

**Sensitive data by exposure**  
● Public ● Org-wide ● External

**Enable downstream DLP controls.**

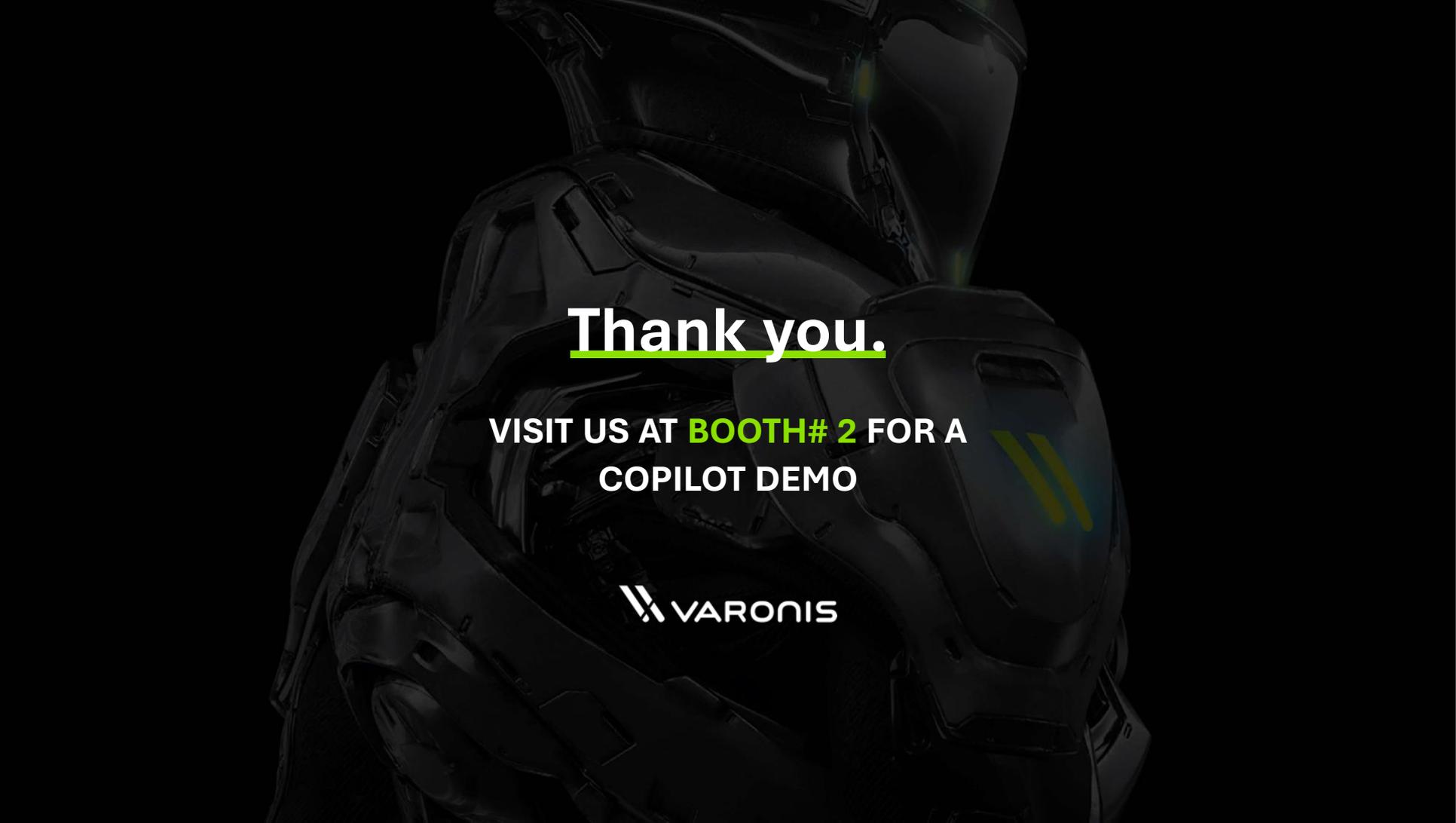
**SCAN TO ENTER**



**Ferrari Daytona SP3  
LEGO**



**SCAN ME**



Thank you.

VISIT US AT **BOOTH# 2** FOR A  
COPILOT DEMO

 VARONIS