

Is AI Putting Your Sensitive Data at Risk?

Challenge

Many organizations are rapidly deploying Microsoft Copilot, Copilot Studio, ChatGPT, Claude, Google Gemini, and other AI tools to drive operational efficiency.

But when AI connects to Microsoft 365, Google Workspace, and enterprise search platforms, overshared data makes your most sensitive information a single query away.

! **Most breaches trace back to over-permissioned access and misplaced trust**

! **Average cost of a data breach: \$4.88M, a 10-year high** — IBM, 2024

! **74% of breaches involve a human element** — Verizon DBIR, 2025

Enterprise CISOs now face a new reality: scale AI innovation without the data risk.

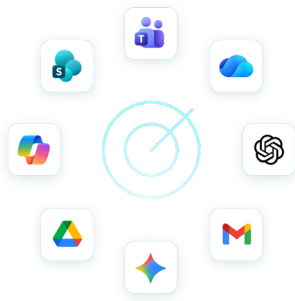
Solution

Opsin enables organizations to scale AI adoption without compromising on governance or data security.

Discover Sensitive Data Exposure Before AI Does

Opsin rapidly maps where AI systems access and interact with sensitive data across enterprise platforms. Using full-context AI interaction analysis, Opsin identifies day-one visibility into real AI exposure risk:

- Over-permissioned access to data and agents
- Sensitive data exposure across platforms



Prioritize What Matters Most

Not all exposure is equal. Opsin analyzes AI interactions across identity, data, prompts, and behavior to isolate the data exposures that create real business risk, helping your team prioritize what to fix first.

Surface root-cause issues with clear ownership, reducing burden on security and IT teams.

Issues

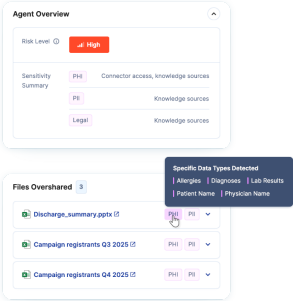
Severity	Platform	AI App / Agent	Root Cause	Data Category	First Detected
PI Issues Total					
Severity	Issue	Platform	Root Cause	Data Category	
High	Patient portal accessible to all internal users	Site	Site	PHI	
Medium	Oncology team files accessible to all inter...	Team	Team	PHI	1
Medium	Discharge_summary.pdf accessible to all...	File	File	PHI	
Medium	Claims Processor authentication disabled	Agent	Agent	PHI	
Medium	Claims Processor connected to sensitive...	Agent	Agent	PHI	

IT Administration vs Continuous Governance

AI risk evolves as usage scales. Opsin continuously monitors:

- Sensitive data appearing in AI prompts
- AI responses surfacing sensitive data
- Suspicious user behavior across environments

Enforce your organization's AI policies in real time and maintain alignment as AI adoption grows.



“As our Copilot usage grew, with active users performing tens of queries daily, we discovered the AI tool was surfacing sensitive documents that users shouldn't have had access to, highlighting long-standing governance challenges across Microsoft 365.”


Mike D'Arezzo
Executive Director of Security,
Wellstar Health

Trusted by
barrywehmler
BUILDING A BETTER WORLD

CASCADE

Culligan

encore
TECHNOLOGIES

UiPath

Wellstar

WTA

opsin

contact@opsinsecurity.com

opsinsecurity.com

 **With Opsin,** AI becomes a secure, compliant innovation layer, eliminating data exfiltration risk before it reaches your users.