INNOVATE *FEARLESSLY*

WHY ENTERPRISES NEED SECURITY ENGINEERED FOR AI INTERACTIONS

Aurascape®
Innovate Fearlessly.

APRIL 8, 2025

https://aurascape.ai

EXECUTIVE SUMMARY

Every application becomes an AI application. And every user becomes an AI user. Easy-to-use, powerful productivity tools incentivize users to feed AI applications more and more data. It's a potent positive feedback loop: more data, better results, faster work.

This new frontier brings brand-new opportunities, and risks.

To best understand these risks, the Aurascape team spoke with 100's of security and AI leaders to find out how they think about the role of security in the AI-powered future.

3 themes emerged from our conversations:

1. These leaders are under pressure to allow AI use for their workforce.
2. Most security teams lack the visibility they need to monitor AI use and risks.
3. Many organizations have adopted short-term security strategies for AI use, but are looking for more nuanced, long-term solutions so their teams can unleash the productivity benefits of AI.

Aurascape has listened closely to these leaders. In this whitepaper, we've outlined the problems and strategies they highlighted so their peers can learn how others think about these new security challenges. We then put forth a new approach to solve these problems.

Our goal is to allow these leaders, their teams, and their organizations to innovate fearlessly with AI.

Concern # 1

PRESSURE TO ADOPT AI

People report that using AI in their jobs helps them be more productive, creative, and enjoy work more. At the same time, nearly all organizations are incorporating AI in their internal processes in some way.

These benefits for users come with risks for businesses, such as sensitive data exposure, brand-new AI-driven threats, and uncertainty about staying compliant with regulations.

Don't get in the way of business

Those responsible for protecting their organization and its data — CISOs, CIOs, AI Governance teams — cannot afford to block total access to these powerful applications.

Business leaders are moving aggressively to adopt AI, and no security or AI governance team wants to stand in the way of these projects' ROI.

Most leaders report they understand this problem, but are unsure how to solve it.

> *I see a lot of potential value in AI, especially for our physicians to save time on repetitive tasks. I am just concerned by what I'm hearing in the news and from my peers, so I'm trying to hold back on allowing widespread use of these apps and move deliberately. I am starting to get significant pushback internally on this.*
>
> **CIO, Healthcare Organization**

What leaders say:

70%

reported all-or-nothing, block-or-allow AI use policies

100%

acknowledged this cannot be a long-term solution

Aurascape®
Innovate Fearlessly.

Concern # 2

LACK OF VISIBILITY

Effective protection must start with complete visibility. Most of the leaders we interviewed reported “not knowing what they don’t know” about AI use in their organization. Why is this the case?

“Unseen” doesn’t mean safe

Legacy security solutions (Firewalls, Proxies, CASB, SSE) struggle to inspect protocols utilized by popular new AI, generative AI and agentic AI tools.

These apps use different technologies, and often switch between communication protocols–MCP, WebSocket, Protobuf, for example–depending on intention.

Moreover, activity from embedded AI elements within SaaS apps and websites often slips through the cracks, going unseen by traditional security products.

The problem:

The inability to see into and understand all AI interactions means two things:

1. Security teams cannot know every AI-powered tool active in their environment
2. Leaders cannot monitor and measure all AI-related risks for data and threats

And with dozens or even hundreds of new AI apps being released every day, this lack of visibility will only continue to grow.

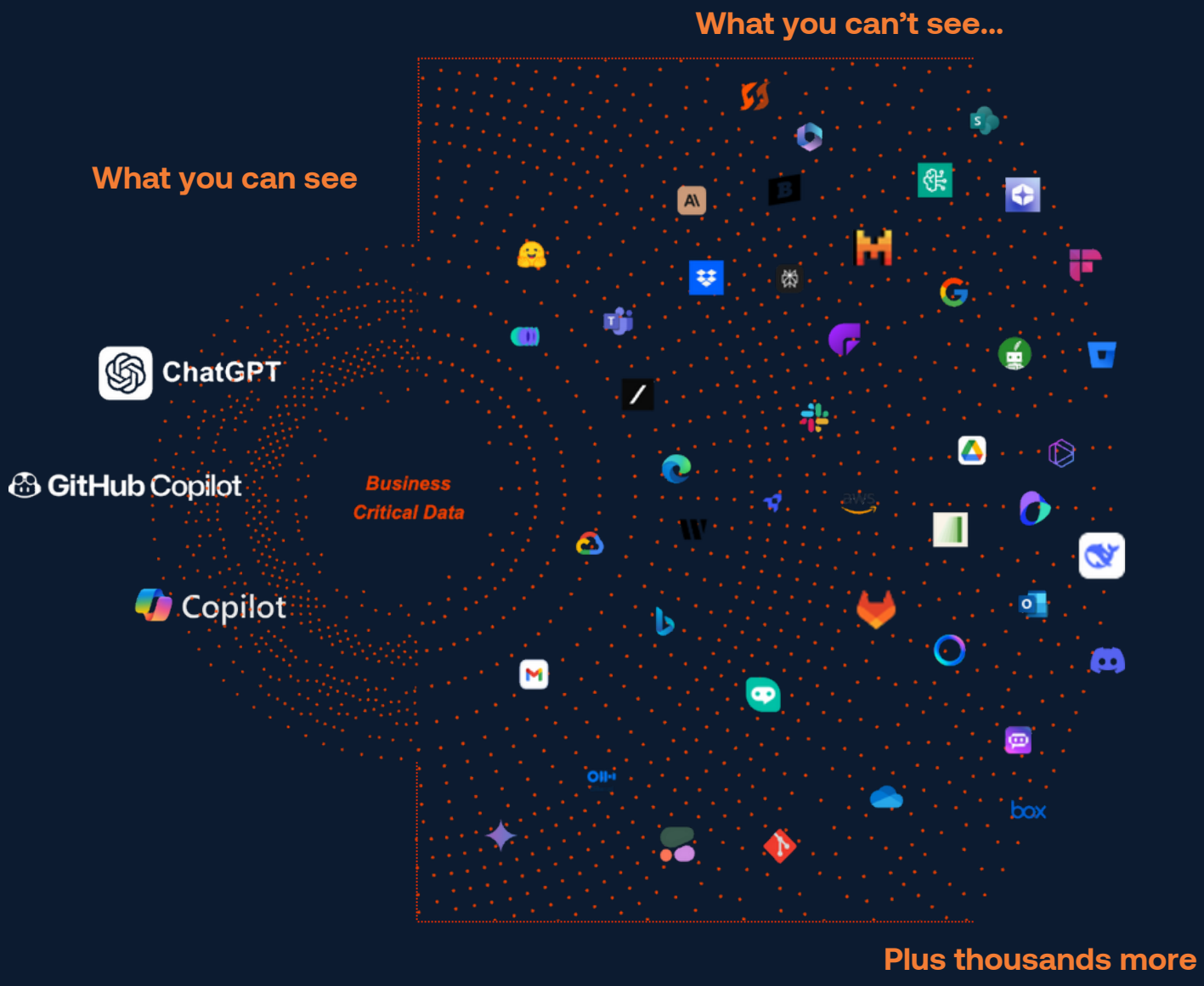
> *Source code is our most valuable intellectual property. We have a sanctioned AI coding assistant for our developers, but I’ve heard there are other tools in use. I don’t know for sure. If there are unknown AI apps with access to our code, that is a problem waiting to happen.”*
>
> **CISO, Financial Services Firm**

> *I realized that employees can still use this new app even though we "block" AI access. There are too many of them these days.”*
>
> **CIO, Technology Company**

Aurascape®
Innovate Fearlessly.

A Dangerous Duo

Pressure to adopt AI + Lack of visibility for AI



Our takeaway: leaders need better visibility into the growing levels of AI activity across their organizations.

Aurascape®
Innovate Fearlessly.

Concern # 3

LIMITED PROTECTION

We then spoke with these leaders about their AI security posture.
Most reported having policies in place. However, a few follow-up questions revealed that these policies are from from perfect:

- 40% of security leaders with AI security policies in place reported they rely on written (unenforced) acceptable AI use policies.
- On the other end of the spectrum, 40% told us they “block all AI access.”

Neither group seemed satisfied with the results so far.

What’s (not) working

Those who rely on written policies stated they could not monitor actual user adherence to their policies.
Those taking the all-or-nothing, block-it-all approach say they can only block a limited number of apps, and they suspect there’s more usage under the radar.
Not to mention, security operations teams are already overloaded. Trying to research and craft policies for the long-tail of new AI-powered apps would require even more work. Plus, AI copilots and plug-ins routinely index overshared files with sensitive data when given access to corporate file repositories.

Our takeaway was clear: security teams need the ability to apply accurate, granular policy to protect data and prevent threats, for all AI tools.

What leaders say:

80%

ranked uncertainty about sensitive data & IP leakage through GenAI and AI agents as their top AI security concern

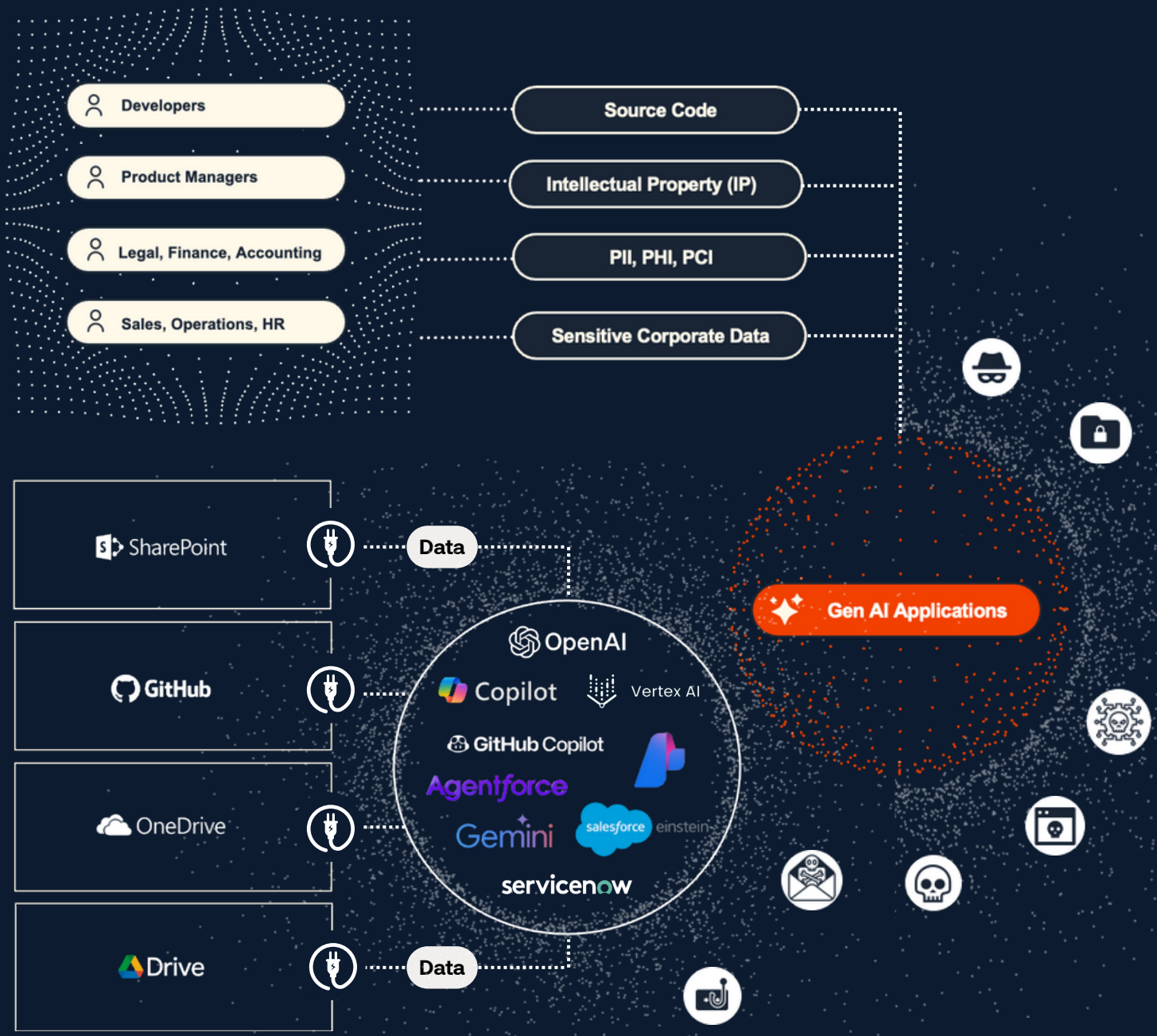
40%

mentioned they worry about at least one specific threat-based risk from the OWASP Top 10 for LLMs

Aurascape®
Innovate Fearlessly.

IT'S GETTING COMPLICATED.

GenAI apps and copilots present new threats + new channels for data exposure



Our takeaway: effective threat prevention and data security have never been more vital.

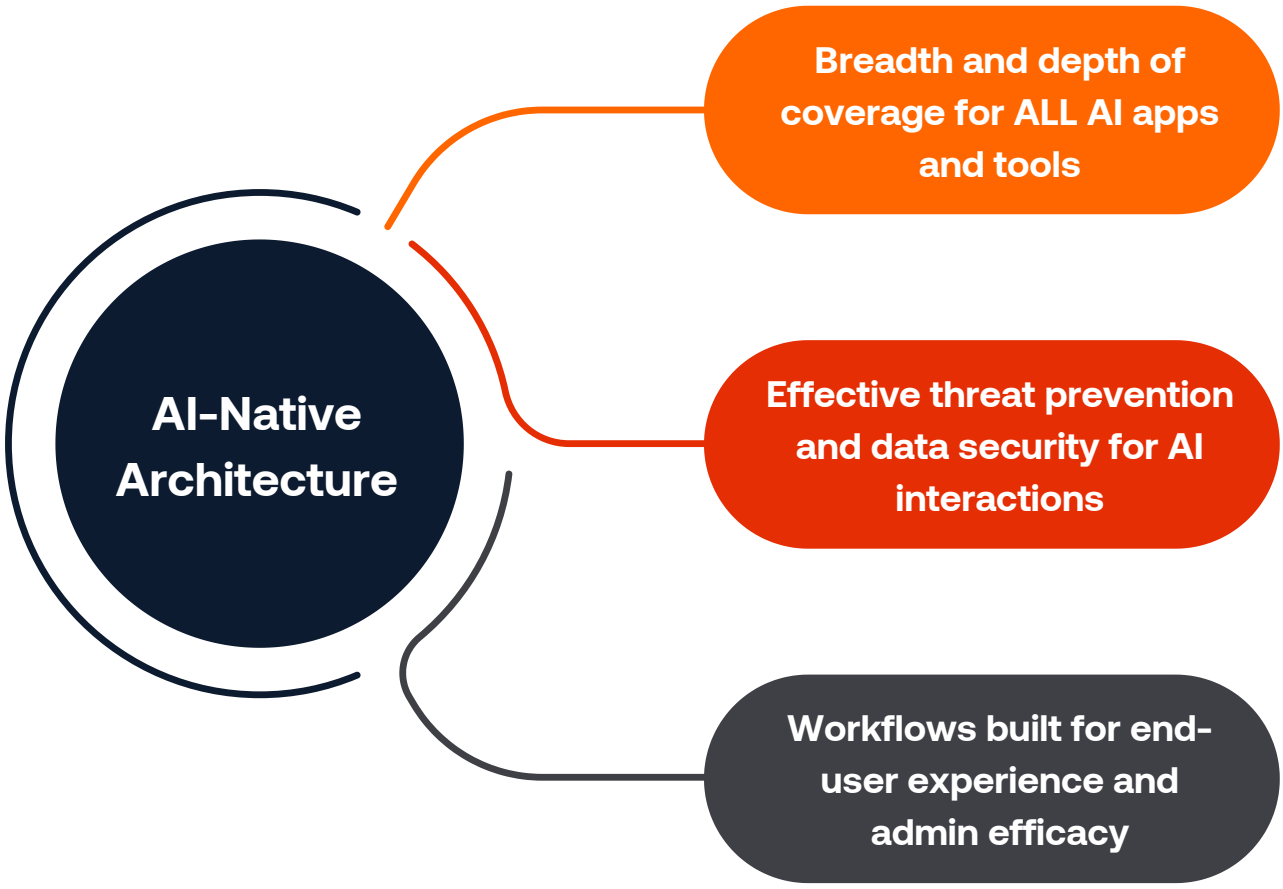
Aurascape®
Innovate Fearlessly.

A Platform Engineered for AI Interactions

Effective AI security must evolve at the pace of AI.

What's needed: human-like understanding of all content, in real-time.

This necessitates using AI to understand content for better data protection and threat prevention.



Aurascape
Innovate Fearlessly.

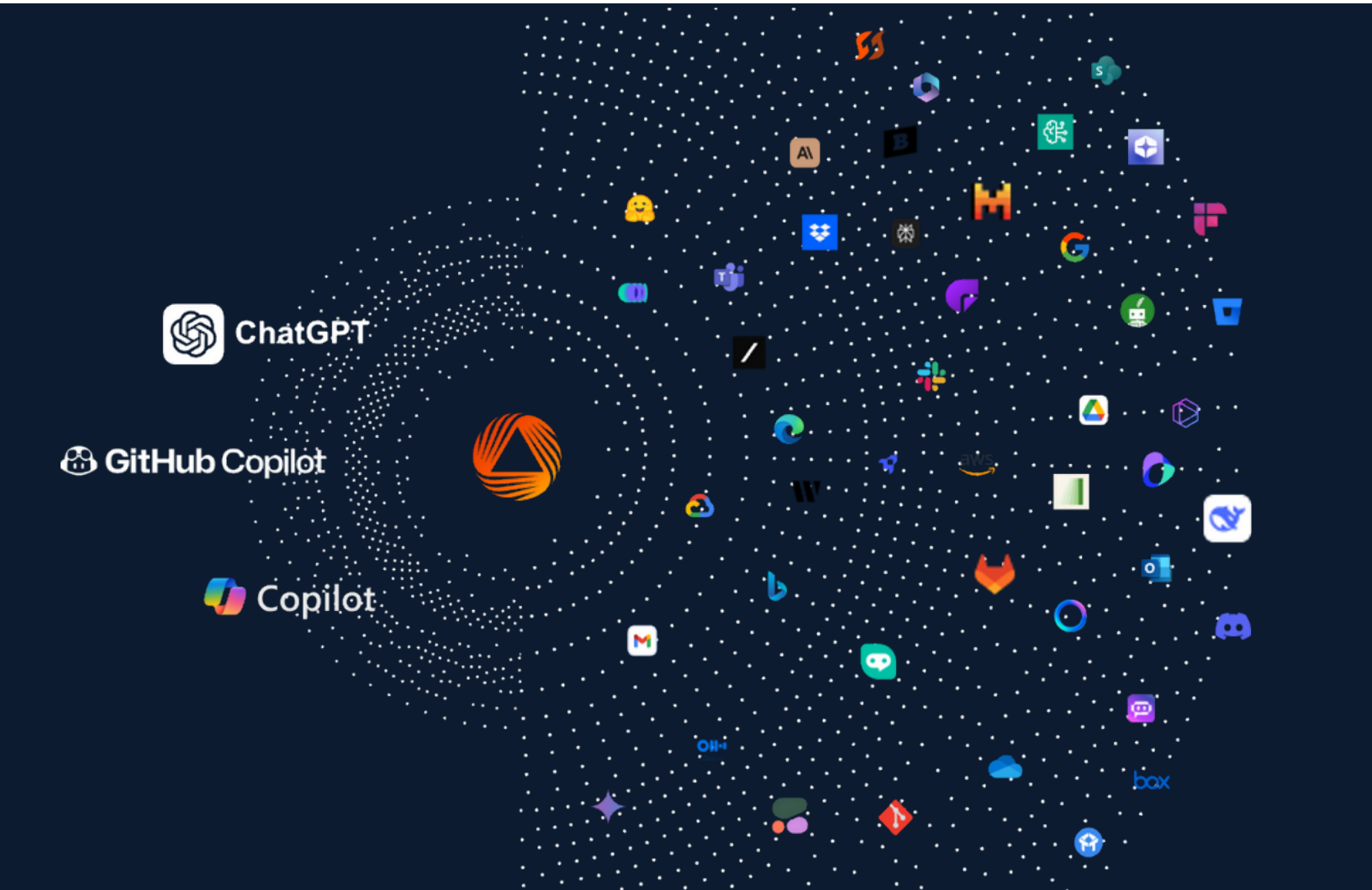
VISIBILITY

Cover ALL AI activity

Comprehensive visibility requires rapid detection and inventorying of brand-new AI apps, tools, and embedded AI components.

This means capturing the newest AI apps, pulling in all publicly available vulnerabilities, plus terms and conditions and other factors, and applying appropriate policy based on this automated risk analysis.
For zero-day AppID and observability, the entire process must be closed-loop.

This necessitates device-level and network-level visibility, requiring deployment capable of sitting inline, plus architecture capable of scaling for enterprise AI use.



PROTECTION

Pinpoint data security

What if data security didn't generate endless false positives, and didn't miss any real leakage? This solution would need to recognize truly sensitive data specific to that business.

This only becomes more relevant once users utilize AI applications.

For example, traditional DLP cannot tell the difference between a developer feeding an AI coding assistant non-sensitive code, or mission-critical source code. Or, feeding an AI chatbot a 9-digit SSN, versus a 9-digit parts number. It's time for better data security.

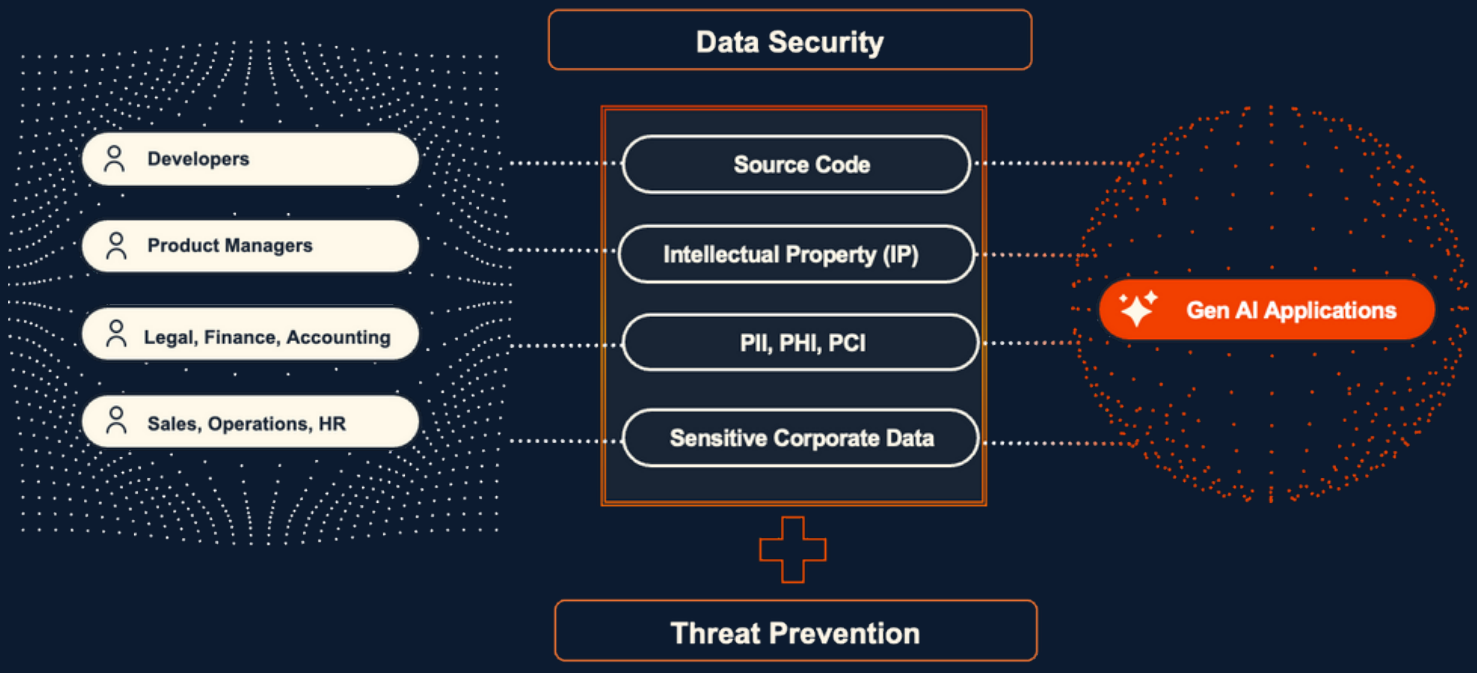
Effective threat prevention

With AI, adversaries now have unprecedented speed, sophistication, and computational power.

As users adopt thousands of AI tools, these platforms become a growing attack vector for lateral movement and exploitation.

New threats appear daily, from toxic AI-generated responses, phishing and malware, to sophisticated social engineering within AI.

To defend against these threats, a security platform must have the ability to fully inspect and protect AI interactions, whether that interaction is user-to-app, app-to-app, app-to-agent, or agent-to-agent.



Aurascape®
Innovate Fearlessly.

READINESS

Get (and stay) AI-Ready

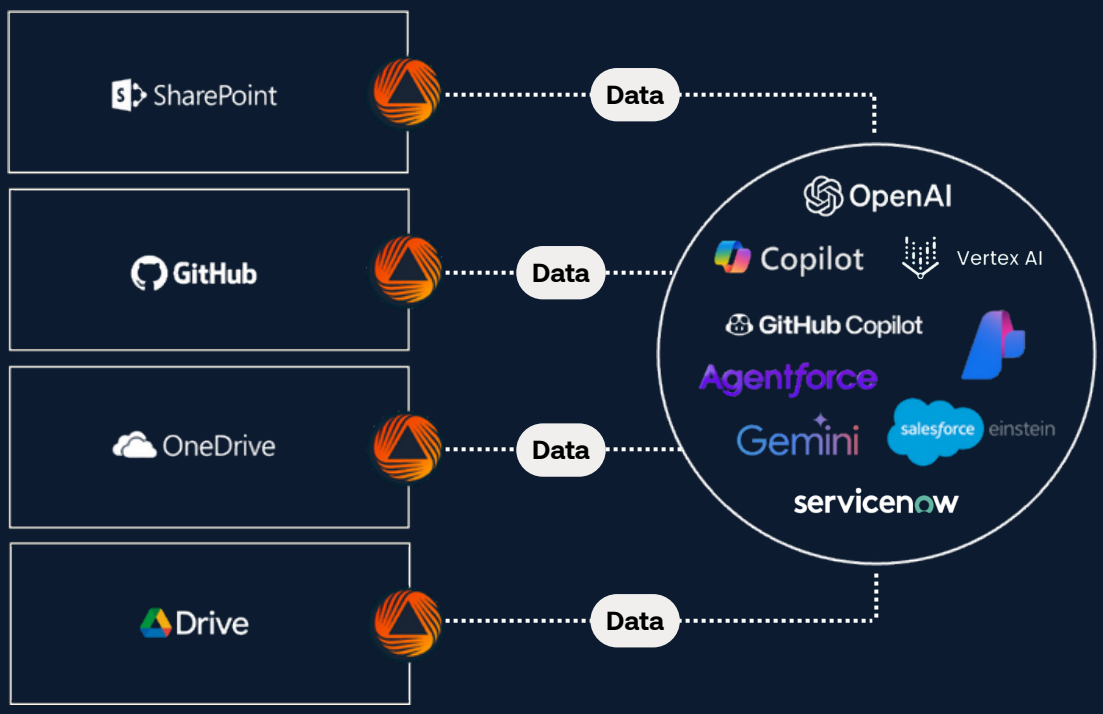
Security operations and IT teams already have too much on their plate. However, a whole new set of tools demands attention: AI apps.

We have discussed the challenges related to unsanctioned AI use (see “Visibility”), so we will now explore protections for sanctioned AI use.

These are sanctioned AI apps, which often operate as plug-ins for corporate repositories and act as Copilots.

The problem: AI Copilots and AI plug-ins easily index overshared sensitive data within corporate file repositories.

Teams must protect against this by auditing their AI Copilot readiness, then continuously monitoring the activity of these AI tools to ensure they only share the right data with the right people.



Aurascape®
Innovate Fearlessly.

What does it take?

After all we have learned, here is what we believe a security platform needs in order to enable organizations to innovate safely in the AI age.

Deployment: should sit inline and have an endpoint presence for network & device level visibility plus real-time protection.

Understands advanced communication protocols to cover ALL new AI tools, for complete visibility.

AI-powered data classification, plus data fingerprinting capabilities, to protect data with near-zero false positives.

Model-agnostic, multimodal engine drives AI-powered security with very low latency or gaps in file type coverage.

AI security workflows automate visibility and protection, from readiness to continuous security.

Simple to deploy, configure, and use
+ evolves with the pace of AI.

Aurascape®
Innovate Fearlessly.

AI is here to stay.

Make sure your security platform is, too.

Visit our website to book a demo and learn more about the Aurascape platform.

https://aurascape.ai