Aurascape®

SOLUTION BRIEF

# CLOSE THE AI SECURITY GAPS CREATED BY TRADITIONAL SECURITY

AI is everywhere—from copilots and GenAI tools to embedded features in the SaaS apps your teams use every day.
But traditional security stacks weren't designed to see or protect this kind of traffic.
Aurascape closes the visibility and protection gaps that traditional firewalls, proxies, and DLP tools simply weren't built to handle.

Aurascape works alongside your existing security solutions to help secure the spread of AI tools across your business.

Security and AI leaders report three consistent challenges which their current security tools cannot address:

- Business pressure to allow AI use, without introducing unmanaged risk
- Lack of visibility into how AI apps interact with users and data
- Inability to enforce and report on policy based on intent, context, and risk

https://aurascape.ai

## Aurascape AI Security

# KEY USE CASES

### Control Shadow AI

Automatically discover AI tools used across the organization—including unapproved apps, embedded AI within SaaS and websites, and agentic AI.

### Safeguard Sensitive Data

Gain real-time visibility into how users interact with AI apps, and apply precise policies based on app risk, user identity plus intent, and data sensitivity.

### Secure AI Copilots

Prevent copilots from learning and oversharing sensitive files. Scan repositories to find and label sensitive data, fix sharing permissions, and unlearn previously learned sensitive files.

### AI Compliance Readiness

Detect and prevent out-of-compliance AI access and usage. Apply access and usage policies aligned with internal controls and external regulations like GDPR, HIPAA, and PCI.

### Enforce AI Governance

Guide end-users to safe AI usage with automated and customizable coaching. Democratize investigation and streamline reporting with a conversational natural language agent.

### Guardrails for AI Coding Tools

Monitor AI-powered coding assistant tools to ensure developers don't expose proprietary source code or unknowingly import unsafe code.

### Safe Use of Embedded AI

Automatically discover AI tools used across the organization—including unapproved apps, embedded AI within SaaS and websites, and agentic AI.

### Secure Agentic AI

Agentic AI chains over MCP introduce invisible risk pathways. Aurascape provides real-time visibility and context-aware policy controls—so you can embrace agentic AI with confidence.

Aurascape®

# VISIBILITY AND CONTROLS THAT KEEP PACE WITH AI

AI now shows up in many forms: standalone GenAI apps, embedded features inside SaaS and websites, AI-infused workflows hidden in browser tools, plus increasingly interdependent AI agents and models connected through MCP, A2A and other emerging protocols.

Legacy security depends on manual research and slow signature creation. But by the time a policy is written, dozens of new tools are already in use.

**20-50 New GenAI Apps Daily**

**Traditional Firewall/SWG**

**Weeks to Create Signatures**

**Manual Research Process**



**Aurascape**

**Same Day New AI Support**

**Automated App Risk Scoring**

**10,000+ Apps with Embedded AI**

To address these converging and growing gaps, Aurascape continuously scans for known and unknown AI tools—across devices, networks, and browsers. It automatically:

- Detects new GenAI and embedded AI usage
- Generates security signatures without manual effort
- Creates a risk score for every new app, based on all available information

With thousands of AI apps already supported, Aurascape secures the long-tail of emerging AI tools.

The result: security that scales as fast as AI evolves.

Aurascape®

# SECURITY THAT UNDERSTANDS AI TRAFFIC

AI apps don't rely on just HTTP traffic. They increasingly communicate using complex, shifting protocols—WebSocket, Protobuf, QUIC, and more. Within these interactions, intent defines risk. A simple user prompt might be safe—until it triggers a file upload, repo query, or app-to-app action. Intentions fundamentally alter the context of an AI interaction, and without decoding them, security teams are flying blind.

**HTTP/HTTPS**

The universal transport that all vendors use to secure traffic through DLP and threat prevention.

**Custom Protocol**

Customized per AI application using Websocket, Protobuf, QUIC, etc.

**Custom Schema**

Each AI application has a unique schema.

**Complex AI Intentions**

The many possible actions and interaction types within AI applications.


**Hidden Intentions**

- Inline Suggestions
- Deep Research
- Take Action
- Chat w Extension
- Dictation
- Copilot Edits
- Attach Files
- Image Upload
- Connect to App
- ...and many more

## Protocol-Agnostic AI Traffic Inspection

Aurascape deeply understands AI-specific protocols and schemas used across GenAI, embedded AI, and agentic tools.
This fluency allows full visibility into entire AI conversations, rather than the one-sided, prompt-only visibility afforded by traditional security tools.

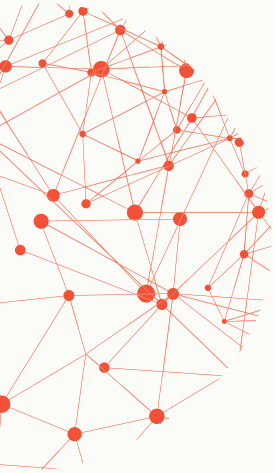
## Intention-Aware Security

Aurascape automatically decodes intentions for every AI app, unlocking the context needed to enforce granular, risk-based policies in real time.
This provides true context-aware protection—where intent matters as much as content.

Aurascape®

# EFFECTIVE DATA PROTECTION THAT CUTS THROUGH THE NOISE

## What's Missing



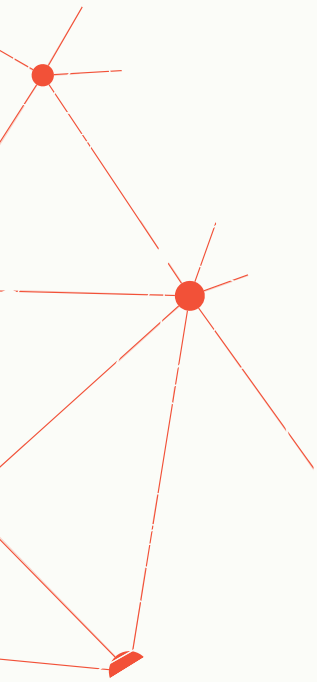
### Static Rules Can't Keep Up With Dynamic AI

Legacy DLP tools depend on regex and keyword patterns. These static rules miss the nuance and context in AI usage. For example, traditional DLP generates an alert when a user enters a string of 16 digits for a part number into an AI app, mistaking this for a credit card number.
Not understanding the context of an interaction leads to an unusable volume of false positive alerts for data security teams to sift through, making traditional data protection tools ineffective for AI interactions.

### Prompt-Level Visibility Isn't Enough

Even if a user input looks low-risk, the AI app might pull data from connected drives, code repos, or databases, depending on user intent.
Traditional tools only see prompts, not responses. And they cannot decode intentions.
Without this conversational context, data protection controls that work for other uses cannot work for AI usage.

## What's Needed



### Real-Time and Context-Aware Data Protection

Aurascape uses real-time AI models to inspect traffic at the conversational context level, not just the prompt.

- Understands the full interaction—from user input to AI output
- Categorizes data dynamically, with predefined categories for industry-specific regulatory frameworks

Context-aware enforcement means fewer false positives—and stronger protection against data loss or abuse.

### Sensitive Data Fingerprinting

Aurascape builds and applies fingerprints of high-value, business-specific data—like crown jewel code, design files, and sensitive information.

- Securely identifies and protects content unique to your org with BYOK encryption
- Prevents leakage that pattern-based DLP would miss
- Enhances accuracy and reduces false positives

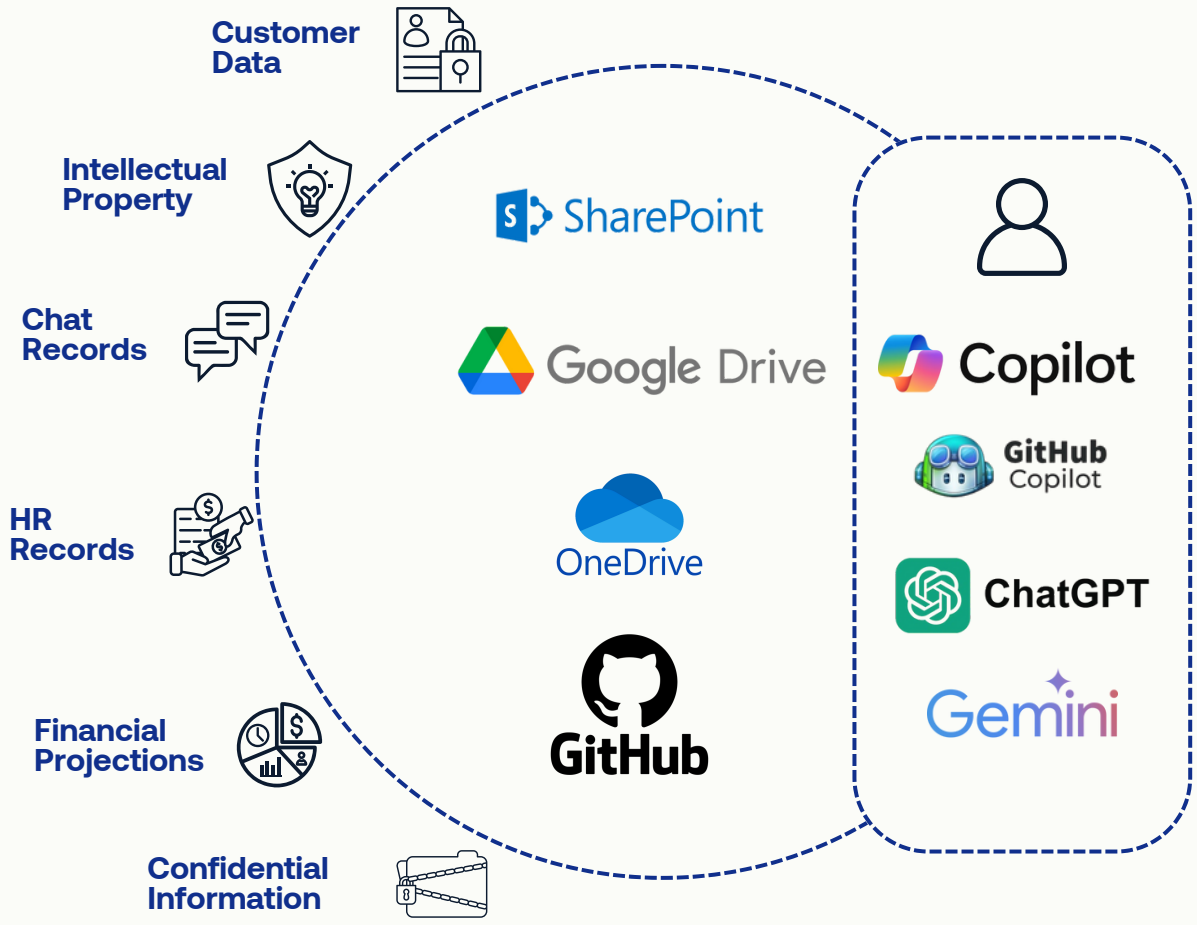
Together, these capabilities deliver precision protection for the way your users actually work with AI.

Aurascape®

# SECURE AI COPILOTS

When copilots connect to SaaS platforms like SharePoint, Teams, Google Drive, or GitHub, they gain broad access to organizational data.
If those repositories contain overshared, misclassified, or unlabeled content, copilots can index and surface it to the wrong users.

Built-in security tools offer basic protections—but they don't scan for oversharing, apply enterprise data labels, or unlearn what's already exposed.




**Aurascape secures your Copilot deployment from end to end by:**

- Discovering over-permissioned and unlabeled sensitive data in connected repositories
- Applying Microsoft Purview labels to enforce access controls
- Automatically remediating oversharing by adjusting sharing settings
- Instructing Copilots to unlearn previously indexed high-risk content
- Monitoring prompts and responses in real time to detect and block risky queries and replies

Aurascape adds a layer of security so Copilots can drive productivity—without driving risk.

Aurascape®

# KEEP USERS MOVING AND STREAMLINE OPERATIONS

## Beyond Block or Allow: What's Next

Some organizations try to manage AI risk by blocking all usage—but this approach rarely holds. Users find workarounds. Teams bring in tools under the radar. And business leaders push for adoption to stay competitive.

At the same time, security teams are left with no visibility, no control, and mounting pressure to allow AI—without sacrificing data protection or compliance.

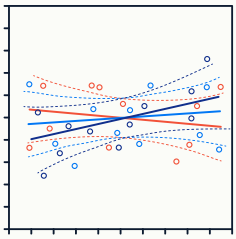
Blocking without context creates a false sense of security. What's needed is a smarter, more flexible approach.

---

## Dynamic & Scalable Governance

Aurascape enables safe AI use without slowing down your users or your security operations team:

- Real-time coaching at the moment of risky behavior—guiding users with context, not just blocking them
- Automated limited-time exceptions for sanctioned, short-term AI usage





## Democratized Investigation & Reporting

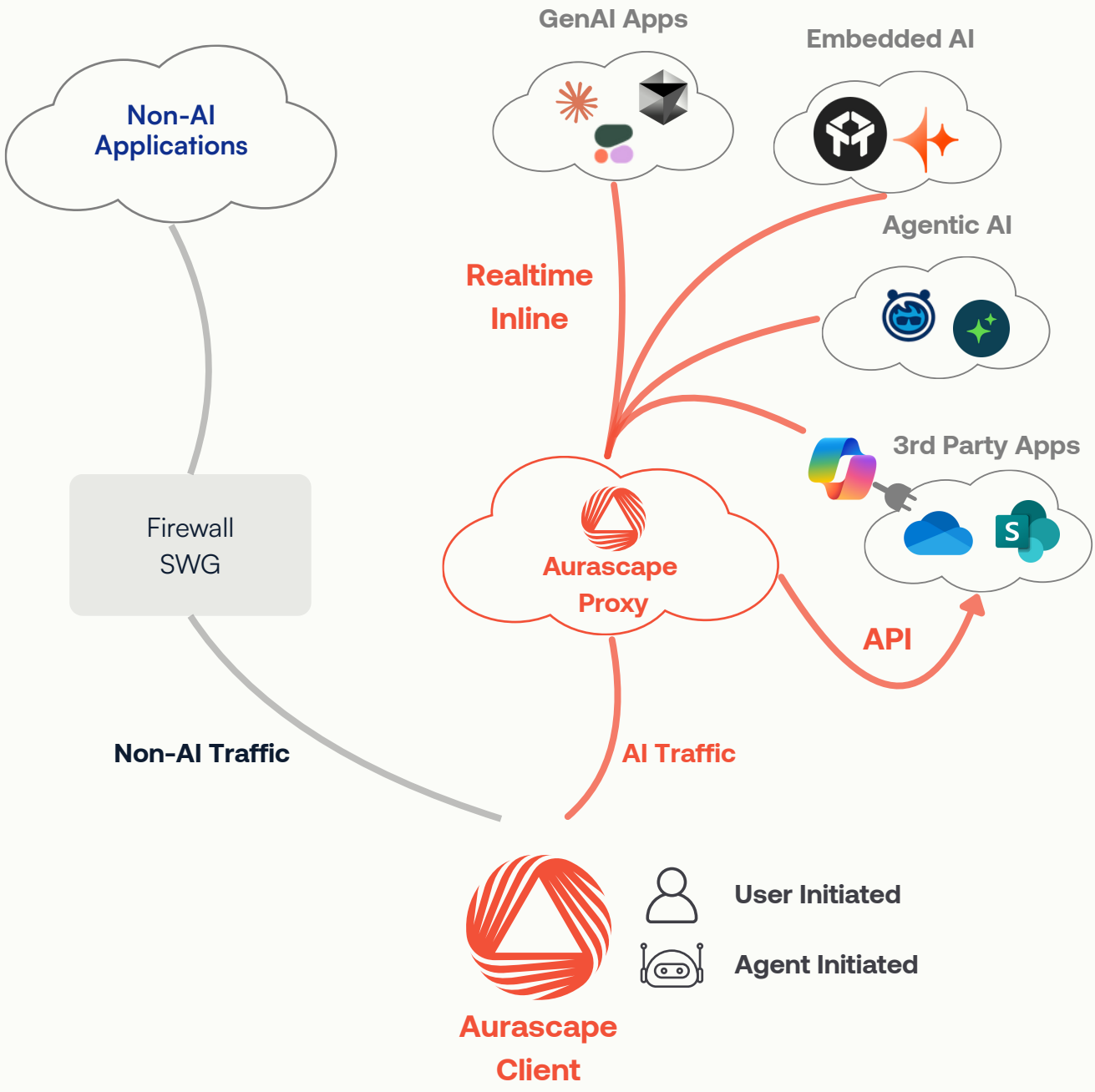
Auri, Aurascape's natural language agent, allows security teams, HR, legal, and compliance to ask plain-language questions like:

"Which users uploaded sensitive files to unauthorized AI tools last week?"
"Show me all prompt activity mentioning customer PII in the last 30 days."

With Auri, security investigation and reporting become faster, more accessible, and democratized across teams and roles.

Aurascape®

# AURASCAPE ARCHITECTURE OVERVIEW




SOC 2 TYPE 2 VERIFIED BY ASSURANCELAB

Aurascape sits between your enterprise endpoints and the AI tools they interact with.

AI traffic flows through the Aurascape proxy, where security enforcement and policy controls are applied before traffic reaches external AI tools or returns to the endpoint.

Aurascape®

# AI Upgrades the Way People Work.

## Aurascape Upgrades the Way You Secure AI.

Traditional security tools weren't built for real-time AI conversations, dynamic protocols, or user-driven intent.

Aurascape is.

It adds the missing layer:

- Visibility into all AI activity, without time delays to create signatures or coverage gaps due to protocol support
- Context-aware protection that understands data, user behavior, and risk
- Policy enforcement that works in real time, and guides users away from risky behavior without disrupting productivity
- Streamlined investigation and reporting for immediate insight into any aspect of your organization's AI security status

Aurascape doesn't replace your security stack—it extends it, so your business stays secure in the AI-powered future.

Get in touch today to discuss how Aurascape can fit into your existing security architecture.

**aurascape.ai/request-a-demo**

Aurascape®