JupiterOne

DATASHEET · AI ATTACK SURFACE MANAGEMENT

Ask your attack surface anything — and get an answer the graph can back up.

Discover every asset — including AI agents, models, and MCP servers — query the graph in plain English and act on what matters.

THE PROMISE

One AI-native platform for every cyber asset.

THE PROBLEM

Security teams know the drill. Asset inventory tells you what's out there — flat, in a spreadsheet. CSPM tells you which cloud configs are wrong. The vuln scanner lists 8,000 findings. The CMDB is eight months stale. And now your engineers are shipping AI agents, copilots, and MCP servers that none of those tools even know exist. When a CISO asks "which internet-facing workloads — or AI agents — are missing EDR and hold customer PII?", the answer takes five tools, three queries, and a week.

THE JUPITERONE APPROACH

JupiterOne AI ASM unifies every asset, identity, vulnerability, control, and AI agent into one live security graph — then layers JupiterOne AI on top. Traditional assets and the AI layer — models, agents, MCP servers, and the services they call — are discovered continuously and mapped to the identities, data, and systems they touch. Architects ask questions in plain English and get answers grounded in the graph. No stitched-together inventories. Just a queryable attack surface, 200+ integrations deep.

01

Discover every asset — including AI

Enumerate every asset, owner, and relationship across cloud, code, identity, SaaS, endpoints, on-prem — and every AI agent, model, copilot, and MCP server. Traditional and AI assets in one graph. No blind spots.

02

Analyze in plain English

Ask JupiterOne AI a natural-language question and traverse the graph for the answer. No J1QL syntax required, no ticket to the data team — but full J1QL power when you want it, with auditable reasoning behind every response.

03

Act on what matters

Drive remediation, exposure reduction, and compliance evidence from a single source of truth. Save queries as alerts, dashboards, and controls — codify "what should be true" once, detect every deviation.

200+ INTEGRATIONS

Across cloud, code, identity, endpoints, SaaS, security, and AI — including:

AWS · Azure · GCP · Okta · Entra · GitHub · GitLab · Jira · ServiceNow · Snowflake · CrowdStrike · Wiz · OpenAI · Anthropic · AWS Bedrock · Azure AI Foundry · MCP

JupiterOne

Stop stitching together Assets, CSPM, vuln management, CMDBs, and AI inventories. See it, query it, prove it.

AI-NATIVE ASSET VISIBILITY

- **Live security graph for every asset — including AI**
  Cloud, code, identity, endpoints, SaaS, vulnerabilities, controls, and the AI layer — models, agents, copilots, MCP servers — all mapped into a single graph that updates continuously from 200+ integrations.
- **Continuous AI agent and service discovery**
  Automatically inventory AI agents, models, MCP servers, and the services they call — across OpenAI, Anthropic, AWS Bedrock, Azure AI Foundry, Vertex AI, and custom stacks. Includes shadow agents provisioned outside IT awareness.
- **Graph-based relationship mapping, humans and agents alike**
  See how users, roles, resources, data, controls, and AI agents interact. Trace identities each agent runs under, the data it can reach, the systems it changes — attack-path questions spreadsheets can't represent.
- **Natural-language queries with JupiterOne AI**
  Ask "which production workloads or AI agents are exposed to the internet and have access to customer PII?" and get an answer in seconds — with the entities, the relationships, and the full J1QL behind it.

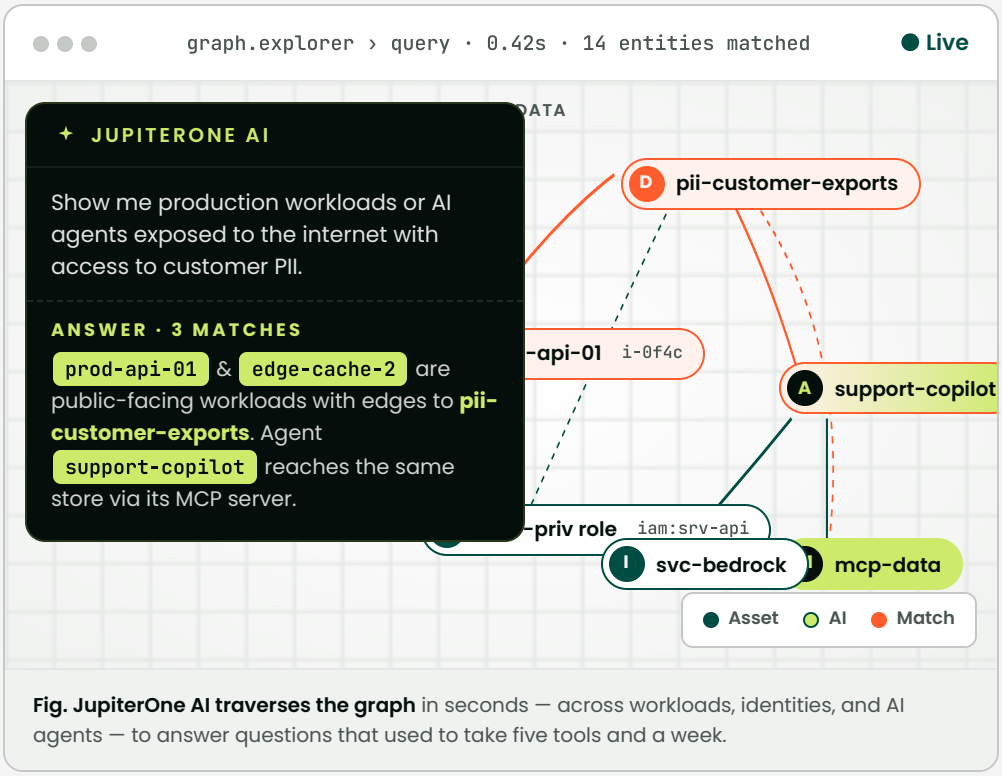

Fig. JupiterOne AI traverses the graph in seconds — across workloads, identities, and AI agents — to answer questions that used to take five tools and a week.

WHAT CUSTOMERS SAY

"JupiterOne isn't just our asset management tool. It's our security data platform. Any time there's new data in the platform, J1 is natively and automatically connecting it to everything else we care about. That's where the power is.

Head of Security Engineering
Identity & Access Management

90M+
Cyber assets under management across the JupiterOne graph

150%
More attack surface coverage than legacy spreadsheet tools

85%
Less manual investigation with JupiterOne AI

EXPOSURE REDUCTION THAT ACTUALLY SCALES

- **Blast-radius prioritization**
  JupiterOne AI ranks exposures by reachability, criticality, and control coverage — not CVSS score — so a four-person team can focus on the handful of findings that represent real risk.
- **Continuous controls evidence**
  Detect the moment an asset drifts out of compliance, down to the user and endpoint. Automate evidence collection and walk into every audit with the receipts.
- **Saved queries become alerts, dashboards, controls**
  Codify "what should be true" once. The platform detects every deviation, continuously, across every environment you run.
- **Open platform, J1QL + JupiterOne AI**
  200+ integrations included, open Collector for anything else. Architects keep full power; everyone else gets answers in plain English.

ABOUT JUPITERONE

JupiterOne is the AI Risk Management Platform that helps security teams in highly regulated industries understand and prioritize risk across complex, AI-driven environments. Built on a true graph-native data model, JupiterOne brings together assets, identities, security posture, and controls, showing the intuitive relationships that connect everything across the enterprise. Unlike list-based approaches, it enables querying of those relationships to understand how risk flows, the blast radius, and what to prioritize in seconds, at enterprise scale. With deep integrations and automated discovery across hundreds of tools, JupiterOne provides a continually updated view of asset relationships and context to cut through tool sprawl and prioritize fixes quickly.

jupiterone.com →