JupiterOne

DATASHEET

JupiterOne Unified Vulnerability Management

Your team can't remediate 8,000 findings. Stop trying.

Fix the vulnerabilities that matter — not the ones that score highest. Risk-based vulnerability management on a security graph that already knows your environment.

THE PAIN

Your scanner found **8,000 vulnerabilities** this week. Your four-person security team can action maybe fifty. If the first fifty are the wrong fifty, the sprint is wasted and the exposure is still there. CVSS doesn't know whether a critical CVE sits on an isolated dev instance or on the internet-facing service with privileged access to customer PII. Wiz covers your cloud. Your scanner covers infrastructure. Neither covers the attack paths that actually traverse code dependencies, SaaS, and identity.

THE FIX

JupiterOne UVM is risk-based vulnerability management built on a security graph. Every finding from every scanner lands in the same graph as your assets, identities, and controls — so prioritization reflects how your environment actually works. A single J1QL query returns every open CVE on an internet-facing asset with privileged IAM access to PII that lacks MFA, across cloud, code, SaaS, and endpoints. Your team works the handful of exposures that represent real breach risk — and your board gets an answer in business terms, not a CVE count.

01

Prioritize by attack path

Every vulnerability is contextualized by the asset's connections — not just its CVSS score. An exposure on an internet-facing workload with admin access to customer data ranks above the same CVE on an isolated dev box. Your team fixes what actually matters.

02

Cover the full attack surface

Cloud, code dependencies, SaaS, identity, and endpoints — all in one queryable graph. See the attack paths that start with an npm CVE, move through an over-privileged service account, and reach customer data. No single-domain scanner can show you this.

03

Report exposure in business terms

Translate technical findings into board-ready risk language. *"Three exposures represent a realistic path to customer PII, remediating by Friday"* — not *"847 criticals open."* Ready for SOC 2, PCI, investor diligence, and the next board meeting.

Integrates with the scanners and platforms you already run, including

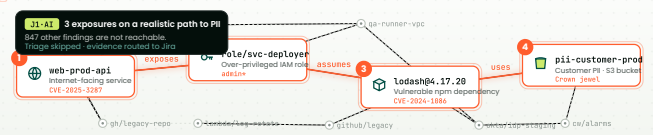
- Wiz
- Tenable
- Qualys
- Rapid7
- Snyk
- GitHub Advanced Security
- AWS Inspector
- CrowdStrike
- Lacework
- Orca
- Prisma Cloud

JupiterOne

Detection is solved. Prioritization isn't. JupiterOne gives lean teams the signal to act on.

8,000 → 3
FINDINGS THAT MATTER

FIG. ATTACK PATH · J1QL RESULT — FINDINGS 847 — ON-PATH 3



The 3 exposures that matter, out of 850. JupiterOne turns a scanner queue into a prioritized remediation plan — the path from an internet-facing service through an over-privileged role and a vulnerable npm dependency to a customer-PII S3 bucket.

On attack path · Asset · Unreachable

WHY NOW

Project Glasswing

Anthropic's Claude Mythos model autonomously **chains low- and medium-severity vulnerabilities into full system compromise** — including a Linux kernel chain that escalates from unprivileged user to root. "Patch the criticals" is dead. The findings CVSS tells your team to deprioritize are the exact ones AI-assisted attackers are stitching together.

> Prioritization without graph context isn't conservative — it's wrong.

Prioritization that reflects your real environment

- **Graph-based risk scoring**
  Every finding is ranked by asset relationships — internet exposure, identity reachability, data sensitivity, control coverage — not a generic CVSS number.
- **Attack path visualization**
  See the realistic path from an initial exposure to a crown-jewel asset, so conversations move from "fix criticals" to "fix these three things."
- **J1QL for the questions CVSS can't answer**
  One query returns every open CVE on an internet-facing asset with privileged access to PII that lacks MFA — across every cloud, SaaS tool, code repo, and identity system you run. Save it as an alert, a dashboard, or a control.

One graph for the whole attack surface

- **Scanner-agnostic ingestion**
  Keep Wiz, Tenable, Snyk, or whatever you run. JupiterOne sits on top and adds the asset relationship layer — no rip-and-replace.
- **Cross-domain coverage**
  Cloud, code dependencies, SaaS, identity, endpoints — all in one graph. Wiz sees cloud. We see the attack.
- **Inventory, unified**
  Every finding is automatically joined to its asset, owner, integration, and control — triage is not a multi-tool scavenger hunt.
- **Evidence & remediation routing**
  Tickets to Jira, ServiceNow, or Slack with full context. Evidence auto-collected for SOC 2, PCI, and investor diligence.

WHAT CUSTOMERS SAY

"We were drowning in findings from Wiz and Snyk. JupiterOne gave us the context to rank them by actual attack path — our four-person team went from triaging for days to shipping fixes in a sprint."

VP, Security
Growth-stage fintech

95%+
Reduction in findings needing human triage

2–3
Point tools typically replaced on deploy

1 query
To find every exposure on a real path to PII

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.

See your attack paths.

Connect Wiz, Tenable, or Snyk in 10 minutes. Run one J1QL query.

jupiterone.com →