

Exposure Management

Prioritize the exposures that actually put you at risk.

JupiterOne maps every exposure to the asset it lives on, what that asset connects to, and what's reachable from it so remediation targets real risk, not just finding volume.

WHAT EXPOSURE MANAGEMENT REQUIRES AND HOW JUPITERONE DELIVERS IT

Three capabilities every exposure management program needs to get right.



DISCOVERY

Discover every attack surface

Exposure management starts with discovering assets across internal, external, cloud, and end-user surfaces — endpoints, identity, containers, IoT/OT, cloud. JupiterOne pulls asset data continuously from 200+ sources into one graph — agentless, no manual reconciliation.



PRIORITIZATION

Prioritize by what's reachable

Discovery alone doesn't reduce risk — exposures need to be prioritized by accessibility, exploitability, and control context. JupiterOne scores every exposure by the relationships of the asset it sits on, not CVSS or EPSS alone.



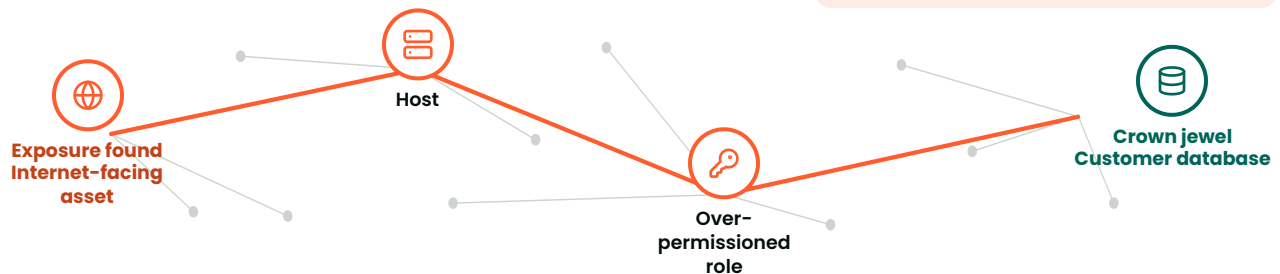
MOBILIZATION

Mobilize the fix

Prioritization only matters once it turns into action. JupiterOne turns a graph query into an assigned, tracked ticket through native ServiceNow and Jira integrations and policy-as-code.

SEE THE ATTACK PATH, NOT JUST THE FINDING

1 of 4,218 paths reaches this crown jewel



WHERE JUPITERONE EXTENDS FURTHER

 **Adversarial validation context.** Attack pathways trace across the same graph as asset, identity, and config data.

 **Control integration.** The graph that scores an exposure also feeds Continuous Controls Monitoring.

 **Lifecycle tracking.** Ownership, status, and SLAs live on the asset graph itself, not a parallel sheet.

“ Exposure tools generate findings, but findings without relationships are just a longer list. JupiterOne maps the connections — and it's the connections that reveal which exposures actually put you at risk.

HOW JUPITERONE COMPARES

Built on one graph, not stitched from three tools

Most exposure management approaches fall into three categories: dedicated CAASM platforms, traditional scanners and RBVM tools, and cloud security platforms scoped to one environment. JupiterOne's Exposure Management runs on the same asset graph as its CAASM and Continuous Controls Monitoring capabilities — so it isn't confined to any one of the three.

Capability	JupiterOne	Dedicated CAASM	Scanners & RBVM	Cloud security platforms
Assets stored as a relationship graph	Core architecture	Aggregated & deduplicated, limited native relationships	Vulnerability-centric, minimal asset context	Native for cloud, scoped to cloud only
Attack path / blast radius analysis	Native, across the full graph	Not native in most tools	Limited, engine-dependent	Native, scoped to cloud workloads
One query across cloud + identity + code + endpoints	Yes — JIQL	Aggregation, not unified cross-domain query	Scanner-source data only	Cloud scope only
Continuous Controls Monitoring on the same graph	Yes	Not offered	Not offered	Not offered
Natural-language (AI) queries across the graph	Yes — JupiterOne AI	Limited	Not offered	Limited
Policy-as-code	Yes	Not offered	Not offered	Not offered

1,000:1

typical funnel compression from raw vulnerability findings to prioritized, relationship-contextualized exposures

75%

reduction in remediation plan size when exposures are prioritized by asset relationship instead of CVSS alone

QUESTIONS WORTH ASKING ANY EXPOSURE MANAGEMENT VENDOR

- › Can it show the attack path from a specific exposure to your most sensitive data — using your actual asset relationships, not a generic model?
- › Does fixing an exposure update your compliance posture automatically, or does that live in a separate tool you reconcile by hand?
- › Can one query span cloud, identity, code, and endpoint assets together — or does each domain need its own tool and export?
- › Is prioritization tied to your environment's actual topology, or to a vendor-generic severity score?

Best fit: security teams running 100+ cloud accounts or hybrid environments who already have EDR, vulnerability scanners, or CSPM tools but no unified view; teams drowning in scanner findings who need to prioritize by real reachability; organizations that need to report exposure to a board or risk committee in business terms — blast radius, crown-jewel risk — not CVE counts.

See your exposures mapped, not just listed.

Talk to JupiterOne →