# Business case for JupiterOne

Gain the context and clarity to secure your organization





# Are your cybersecurity tools telling you everything you need to know?

Depending on where you sit in your company's InfoSec organization, you have specific demands from the tools you use. While the details will look different from team to team, the core questions are often the same.

What do I have?

What's most important?

Do my cyber assets have any problems and who can fix them?

Are things getting better over time?

Securing your organization can feel like a daunting task, made more difficult by lack of or unclear ownership, data growth, GRC requirements, new tools, siloed technology, and many other factors. In the end, however, every cybersecurity concern requires you to answer the same questions.

You can ask these questions using many of the tools available on the market today, but are the answers you're getting complete and accurate? Getting thorough answers that connect the dots across the assets in your complex digital environment is key to building the foundation for your security, IT, and DevOps program.





### What is greater cyber asset visibility worth to your company?

Answering these questions begins with visibility into your enterprise's cyber assets - that is, every single thing that lives in your digital environment, well beyond endpoints and IP-based devices. Without this foundational, all-encompassing visibility, it's simply impossible to rely on your security, IT, and DevOps workflows, let alone make decisions based on such workflows with complete confidence. This is especially important to consider as these teams are under increasing stress.

Cyber asset visibility therefore serves as the underlying building block of your entire security, IT, and DevOps program. It's the essential first step in finding and resolving vulnerabilities, protecting your cloud and on-premises assets, and meeting regulatory and compliance obligations.

It's also key to your bottom line. In the United States in 2022, the average cost of a data breach to organizations was \$9.44M and took an average of 277 days to identify and contain a breach. Organizations that responded more quickly, in under 200 days, saved over \$1M in detection and remediation.1

After achieving greater visibility using JupiterOne, you're ready to tackle the most pressing cybersecurity concerns facing your organization, which we'll cover over the next few pages.

2,011:1

Average number of assets per employee at large organizations (500+ employees)<sup>2</sup>

\$9.44M

Average cost for U.S. organizations to identify and contain a breach in 2022<sup>3</sup>

\$1M

Three-vear reduction in business risk from severe security breaches using JupiterOne⁴

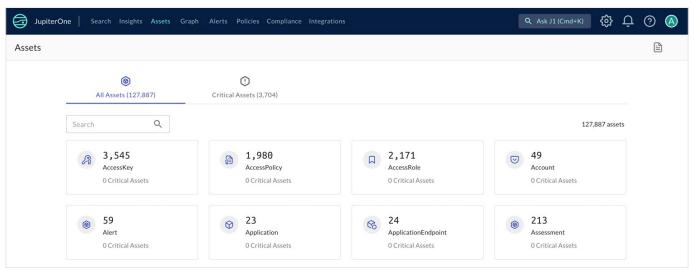
<sup>&</sup>lt;sup>1</sup> IBM, Cost of a data breach 2022, ibm.com/reports/data-breach

<sup>&</sup>lt;sup>2</sup> JupiterOne, The 2023 State of Cyber Assets Report, info.jupiterone.com/resources/scar-2023

<sup>&</sup>lt;sup>3</sup> IBM, Cost of a data breach 2022

<sup>&</sup>lt;sup>4</sup> Forrester Consulting, The Total Economic Impact of JupiterOne, A commissioned study conducted by Forrester Consulting on Behalf of JupiterOne, info.jupiterone.com/resources/totaleconomicimpact-study-forrester-jupiterone





Asset inventory in JupiterOne

### Concern over growing attack surface

Data proliferation and expanding technology offerings have created a 'target-rich' environment for bad actors to take advantage of. Security teams are, on average, responsible for securing and managing nearly 400K diverse and distributed cyber assets across nearly 100 asset categories.⁵

JupiterOne gives these teams a beacon of hope, allowing them to identify and decommission outdated, ungoverned, and misconfigured cyber assets. In the first year using JupiterOne alone, security teams can decrease the organization's attack surface by 150% while also proactively mitigating potential risk from cyber assets the organization likely didn't know existed previously.6

" I've never imagined this amount of visibility. This is amazing." MODUS John Crites, CIO

393,419

Average number of cyber assets and attributes security teams are responsible for<sup>7</sup>

Categories of cyber assets recognized by JupiterOne

Reduction in attack surface over the first year using JupiterOne8

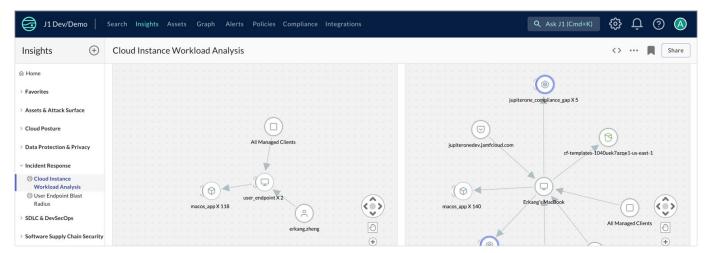
<sup>&</sup>lt;sup>5</sup> JupiterOne, The 2023 State of Cyber Assets Report

<sup>&</sup>lt;sup>6</sup> Forrester Consulting, The Total Economic Impact of JupiterOne, A commissioned study conducted by Forrester Consulting on Behalf of JupiterOne

<sup>&</sup>lt;sup>7</sup> JupiterOne, The 2023 State of Cyber Assets Report

<sup>8</sup> Forrester Consulting, The Total Economic Impact of JupiterOne, A commissioned study conducted by Forrester Consulting on Behalf of JupiterOne





Insights Dashboard for Incident Response

#### Security operations and incident response

Even the smallest gap in visibility across cyber assets in your digital environment can put your security team at a serious disadvantage when responding to an incident, addressing a vulnerability or misconfiguration, or conducting a root cause analysis. JupiterOne aggregates cyber asset data, alerts, and observations from different sources, and leverages a graph data model to correlate, deduplicate, prioritize, and alert on findings. By centralizing this workflow and giving you unprecedented visibility and context to augment your security investigations, your team can take precise response action and solve incidents faster.

Most organizations, 7 out of 10, admit they've experienced at least one cyber attack9, and it's likely there are others that either won't admit to being breached or don't know they've been compromised yet.

Your SecOps and incident response teams are responsible for conducting the very time consuming, often manual, task of investigating and responding to anomalous behavior. JupiterOne's powerful search, alerting, and custom-built incident response dashboards drastically reduce the time spent manually analyzing data sets and configuration settings to extract key insights.

## out of 10

Organizations that admit they've experienced at least one cyber attack<sup>10</sup>

85%

SecOps hours saved devoted to manual investigation and cyber asset identification<sup>11</sup>

Out of the 5,212 breaches studied, over 37% affected just three types of organizations: Finance (690), Professional (681), and Healthcare  $(571)^{12}$ 

We can map application users to entities and can, for example, ask if a terminated employee is seen as active in any applications. We are able to point to the root cause and escalate it, and that's quite good for risk reduction."

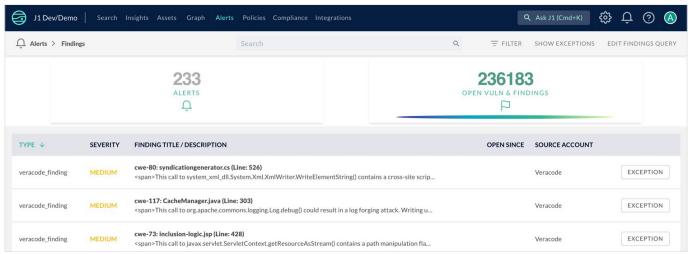
Director of Information Security, Anonymous Marketing Company

JupiterOne, The 2022 State of Cyber Assets Report, info.jupiterone.com/resources/scar-report-2022

<sup>&</sup>lt;sup>11</sup> Forrester Consulting, The Total Economic Impact of JupiterOne, A commissioned study conducted by Forrester Consulting on Behalf of JupiterOne

<sup>&</sup>lt;sup>12</sup> Verizon, 2022 Data Breach Investigations Report, verizon.com/business/resources/reports/dbir/





Open vulnerabilities and findings

#### Vulnerability management

Your security operations likely rely on numerous point solutions to detect and monitor for vulnerabilities and keep adversaries from exploiting weaknesses to gain access to your data and systems. JupiterOne aggregates vulnerabilities and findings from sources like vulnerability scanners, codescanners, cloud service providers, endpoint management tools, and more. Using a graph data model to facilitate contextual analysis, giving you a centralized view to manage vulnerabilities more effectively.

New software and hardware vulnerabilities, along with

misconfigurations, are discovered every day, leading to seemingly endless backlogs of threats for software engineering and security teams to address. Systems with outdated or vulnerable software add to the complexity inherent in taking the appropriate action to address these vulnerabilities.

With the centralized view provided by JupiterOne, it's possible to identify key assets, prioritize critical vulnerabilities, coordinate remediation actions via our workflow integration, and reduce cycles spent by system stakeholders remediating those vulnerabilities.

952,435

Actual vulnerabilities identified out of 151m total findings. While the overall percentage is low, just over half a percent, it shows that without clear visibility and assessment, your red, blue, or purple team will spend extensive time reviewing findings that don't require further action.13

120,561

Average backlog of findings security teams are responsible for.14

CIOs surveyed who believe their software supply chains are vulnerable. 15

a

JupiterOne has become critical for S3 bucket security because it provides a really good line of sight into assets to get ahead of vulnerability management."

Adam Youngberg Sr., Manager, Security Engineering

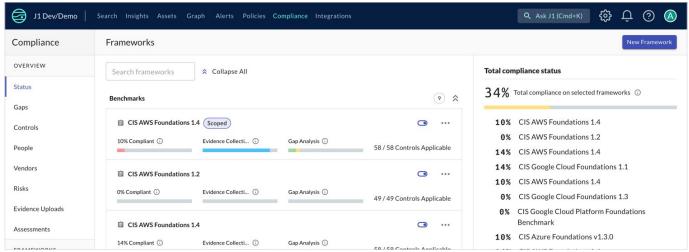


<sup>&</sup>lt;sup>13</sup> JupiterOne, The 2022 State of Cyber Assets Report

<sup>14</sup> Ibid.

<sup>15</sup> BetaNews, 82 percent of CIOs believe their software supply chains are vulnerable, betanews. com/2022/05/31/82-percent-of-cios-believe-theirsoftware-supply-chains-are-vulnerable/





Compliance management in JupiterOne

### Governance, risk, and compliance (GRC)

The first step in your GRC program must be a complete inventory of all the cyber assets in your environment. Any gaps in visibility or unaccounted assets can put your compliance status - and your enterprise - at risk. JupiterOne lets you gain full visibility and automated mapping of assets to compliance frameworks. With outof-the-box support for all the major frameworks, such as SOC 2, NIST, CIS, PCI, ISO, and HIPAA, and support for custom policies, JupiterOne helps you stay on top of your governance

and compliance needs ensuring you have accurate, timely answers backed by evidence to any questions your internal or external auditors may have.

Compliance is not just a reactive requirement. Using JupiterOne, organizations can start down the path to gaining new certifications that will open up expanded markets for their goods or services, directly affecting their potential bottom line with increased revenue sources.

Average cost of a breach for organizations that had high levels of compliance failures16

Increase in compliance operating costs for financial institutions compared to pre-COVID levels17

Annual cost saved using JupiterOne vs. a separate compliance solution.18

We're going through our SOC2 audits yesterday and today. Coalfire auditor loved the JupiterOne dynamic data asset inventory platform. So thank you for that."

Georgeo Pulikkathara, Former CISO

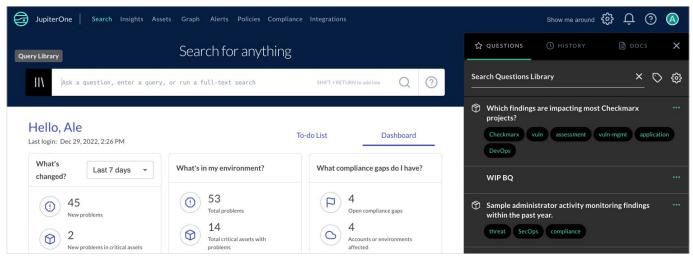


<sup>&</sup>lt;sup>16</sup> IBM, Cost of a data breach 2022

<sup>&</sup>lt;sup>17</sup> Deloitte, Regulatory productivity: Is there an answer to the rising cost of compliance?, deloitte.com/us/ en/pages/regulatory/articles/cost-of-complianceregulatory-productivity.html

<sup>18</sup> Forrester Consulting, The Total Economic Impact of JupiterOne, A commissioned study conducted by Forrester Consulting on Behalf of JupiterOne





Search and Questions Library

SOLUTION

### Why JupiterOne?

Simply put, JupiterOne collects more asset data than any other provider. We go beyond endpoints, IP addresses, users, and devices, and ingest data from CSPs, SaaS apps, code repos, IAM policies, security controls, vulnerability findings, and more. Feel confident knowing there is less risk from an unknown or undiscovered asset.

#### JupiterOne's differentiators:

- Agentless platform: Gain immediate cyber asset visibility across your organization
- Continuous compliance: Identify changes that may pose a risk to your organization and take immediate action to respond
- Depth and breadth of visibility: Drill deeper into your cloud, on-premises, and ephemeral assets while also immediately understanding the blast radius of any compromised asset in your environment.
- Graph data model: Go beyond individual assets with graphpowered visualizations and relationships, and get contextual analysis about any asset

- Mapper processor engine:
  - Proprietary data pipeline engine that builds the relationships between data points - the proverbial 'power under the hood' of JupiterOne
- 'Out of the box' content: Get immediate value thanks to several rule packs, 20+ compliance frameworks, 160+ individual alert rules, 20+ dashboards, and 700+ pre-built queries
- Queryability: Find what you're looking for with predefined search questions, our user-friendly query builder, or write your own powerful queries with the extensible and integrated J1QL query language

332%

Return on investment over three years using JupiterOne.19

u JupiterOne has been great so far. There have been numerous instances where we needed to get a datacentric answer to a big question and we had it in minutes where it would have taken us hours and a lot more work to get that answer without JupiterOne." Mike Sabbota, VP, Security & TIFIN Compliance

<sup>19</sup> Forrester Consulting, The Total Economic Impact of JupiterOne, A commissioned study conducted by Forrester Consulting on Behalf of JupiterOne



JupiterOne is a cloud-native cyber asset attack surface management platform that enables security teams to solve persistent asset visibility and vulnerability challenges. Combine cyber asset data from all of your security tools into a single, unified view, and strengthen the foundation of your security program with JupiterOne.

Know what you have. Focus on what matters.

Schedule a Demo →
JupiterOne.com

