JupiterOne watchTowr

Continuous Threat Exposure Management (CTEM) with JupiterOne & watchTowr

Discover the most critical and exploitable vulnerabilities, prioritize with asset context based on business impact and receive a recommended remediation plan to improve your security posture.

Benefits

Faster Remediation

Rapidly prioritize and fix vulnerabilities impacting your environment.

Quantified Risk

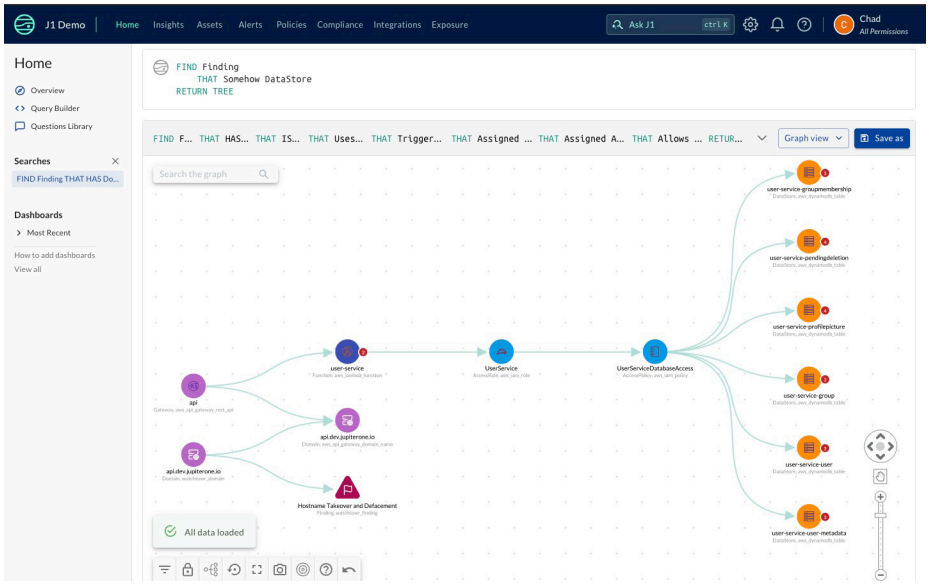
Improve your resilience against dynamic shifts in the threat landscape that impact both cyber and financial risks.

End Tedious Work

Reduce manual processes from your attack surface and asset management programs.

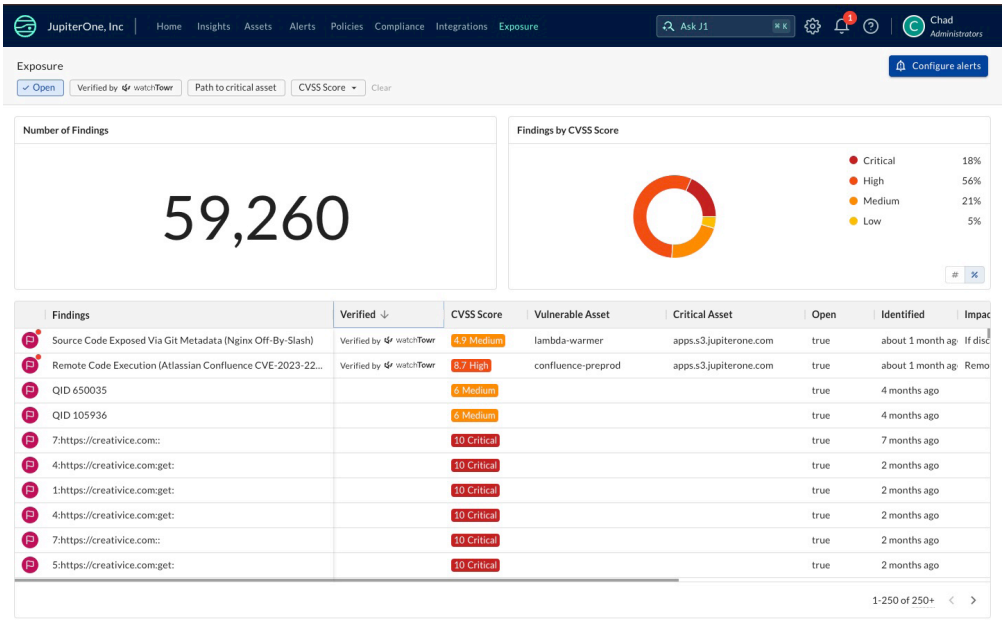
Attack Surface from All Angles

See everything that matters, inside and out.



In today's dynamic environment, factors like digital transformation, workforce shifts, and regulatory compliance are expanding organizational attack surfaces. This new threat landscape demands a shift from reactive security programs and tools, involving an endless list of vulnerabilities and threats, to a proactive security approach. A strategy focusing on prioritizing only exploitable vulnerabilities that adversaries can use to penetrate and compromise critical assets.

A CTEM solution should continuously identify, prioritize, monitor, validate, and remediate exposures across an organization's diverse environments, including public clouds, SaaS platforms, and mobile. This solution must provide visibility from both the external attacker's perspective and the internal view of assets, enriched with context that accounts for the business value of assets, ease of discoverability, exploitability, and attractiveness to potential attackers, ensuring effective management and security of the digital landscape.



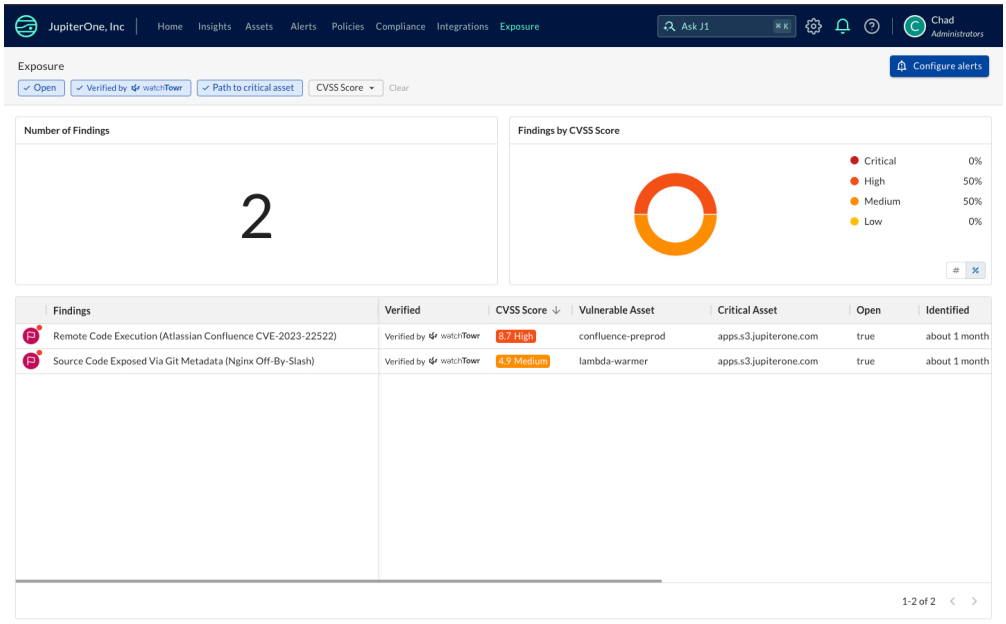
Total Visibility Across All Assets

Easily see and measure how exposed your organization is to potential security threats. JupiterOne and watchTowr provide real-time visibility of your attack surface and all your assets, including mobile apps, cloud resources, SaaS platforms, an IP and more.

Easily see which of your devices are at risk, how serious the risk is, and get fast updates on any recent security issues or changes in your system.

Verified Critical Assets

Understanding both your internal and external assets—everything that could be attacked—is crucial. However, it's not possible to fix every single vulnerability, so it's important to prioritize which issues to tackle first. JupiterOne and WatchTowr identify the most critical assets with exploitable vulnerabilities. Get detailed understanding of your assets that combine business and security risk, along with how critical assets are interconnected within your environment.



CONTINUOUS THREAT EXPOSURE MANAGEMENT

CTEM

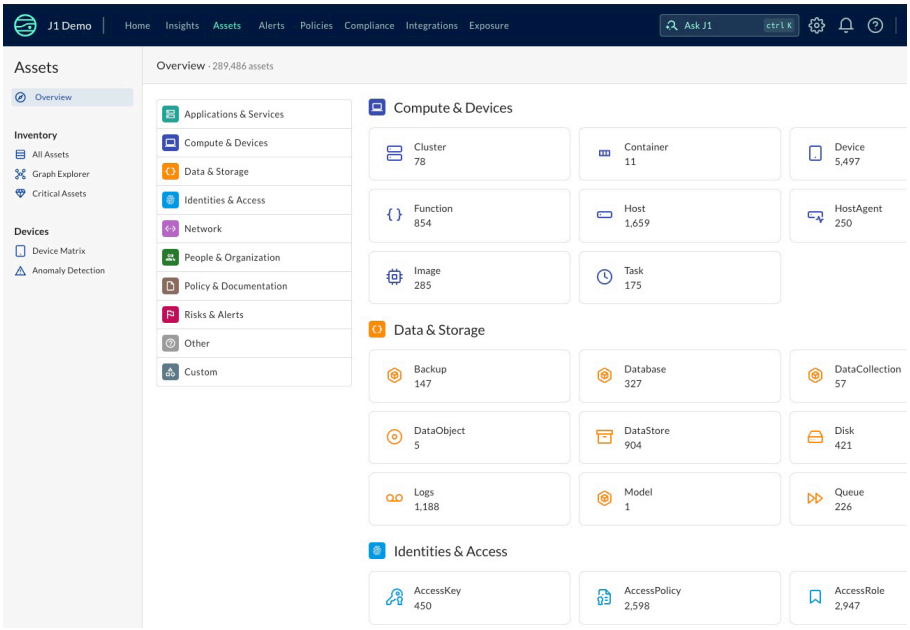
CTEM Use Cases with JupiterOne and watchTowr

Exposure Management Reporting: Communicate a single picture of risk across all departments

Comprehensive Risk Quantification: Broaden the range of data collected on exposures to include more types of risks

Security Testing to Reduce Prioritized Issues: Validation to prioritize list of vulnerabilities most likely to be exploited

Assessing Adversary Attack Impact: Map the most likely path an attacker would take to exploit a vulnerability and verify if existing controls mitigate the exposure



Visibility Across All Asset Classes

JupiterOne's extensive data model offers unparalleled insights into your digital infrastructure. By transforming your cyber asset inventory into an interactive visual map, we provide a comprehensive view of your threat landscape and relationship mapping across all of your asset types. This enables clear identification of vulnerabilities, prioritization of remediation efforts, and significant reduction of your internal attack surface, ensuring robust security posture management.

100 Asset Classes

5,000 Unique Asset Types

20,000 Unique Relationship Types

> "Initially, JupiterOne was just our asset management platform. But, there's so much more to it. Any time you have data in the platform, JupiterOne is constantly and automatically connecting it to other data. That's where the power comes in. We've been able to offload a lot of our work because of it."

Becki True
Manager, Security Engineering at Okta CIC

How It Works

1. Connect your infrastructure and security tooling to JupiterOne via API.
2. Immediately gain visibility into your entire cyber asset inventory.
3. Understand security and compliance posture and begin risk-based prioritization.
4. Take action on prioritized vulnerabilities, gaps, and misconfigurations.

Integrations

With over 200 integrations, you can identify, map, and analyze your entire digital infrastructure, including:

- Cloud service providers
- SaaS applications
- Code repos
- Identity providers
- Application vulnerability scanners
- Infrastructure vulnerability scanners
- Endpoint security agents
- User training
- And more

Dynamic Exposure Management

With JupiterOne and watchTowr cut through the noise: finding the exploitable vulnerabilities that attackers are most likely to exploit and prioritizing them with context based on impact to your business. We don't list every possible threat; we pinpoint the most critical exploitable vulnerabilities and paths an attacker could take, giving you a clear remediation plan. By focusing on what truly matters, you optimize your resources, address today's security challenges, and reduce your exposure to threats.

Attack Surface Assessment

Discover your external attack surface from an attacker's perspective, and identify internal assets along with their relationship to the external attack surface.

Continuously Assess

Continual real-time discovery of your external assets, known and unknown, for comprehensive attack surface visibility.

Identify Vulnerabilities

Find vulnerabilities across all external assets, classifying them with business context for clear and logical findings.

Validate Exploitability

Automatically identify exploitable vulnerabilities at scale with low false-positive rates and validated findings.

Effects Range *(Blast Radius)*

Gain insight into the impact of a threat actor's actions on your cloud infrastructure, SaaS platform, containers, repositories and more.

Asset Attack Paths

Visualize and analyze your environment to identify any potential attack paths, starting with the highest priority exploitable vulnerabilities to your critical assets.

Report & Alert

Report and alert if critical assets are exposed by a vulnerability, directly or indirectly.

Remediate

Take action on choke points and potential attack paths with recommended responses and automated workflows for vulnerability and IT analysts.

200+ INTEGRATIONS INCLUDING

aws · Google Cloud · Microsoft Azure · CISCO

okta · GitHub · ATLASSIAN

About JupiterOne

JupiterOne is the asset, attack surface and exposure management platform for security and IT, that empowers organizations to prioritize and remediate what matters most. Customers use the JupiterOne platform to perform cyber asset inventory, manage their attack surface, respond to incidents, hunt for the latest exploits and continuously monitor their exposure with complete visibility across assets and relationships.

About watchTowr

watchTowr is a global cybersecurity technology company, built by former adversaries. The watchTowr Platform, watchTowr's world-class External Attack Surface Management and Continuous Automated Red Teaming technology, is informed by years of experience compromising some of the world's most targeted organisations and utilised by Fortune 500, financial services and critical infrastructure providers globally every day.

See CTEM in action with JupiterOne & watchTowr

Schedule a personalized demo to experience how you can identify exploitable vulnerabilities, prioritize them based on business impact, and get a recommended remediation plan to minimize your exposure.

JupiterOne.com/get-a-demo

JupiterOne