JupiterOne

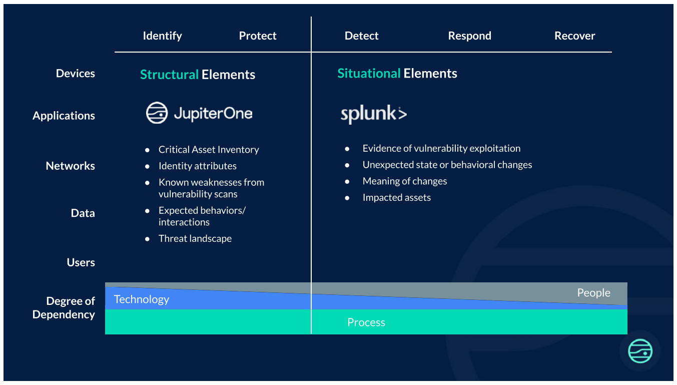
JupiterOne and Splunk

Complete structural and situational awareness across all of your cyber assets to optimize and automate SecOps

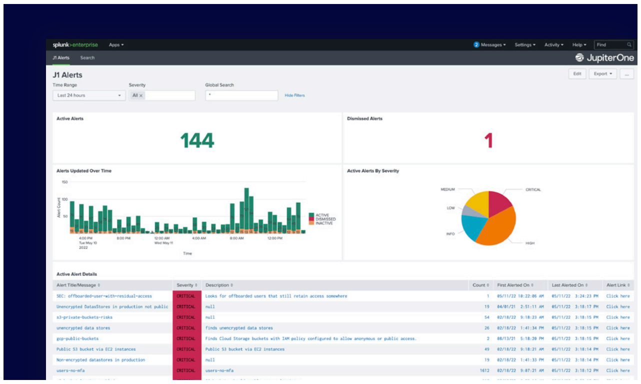
Introduction

Many successful SecOps teams rely on Splunk Security to turn data into doing, as their security operations platform. It allows them to ingest data from any source, providing accurate threat detection, investigation, and automated response, and delivering cyber resilience for their organization. As businesses continue on their cloud-first journey, their needs evolve and their infrastructures and assets increase in complexity. These teams are presented with new challenges from environments they can't get full visibility into, leaving their expanding attack surface open and more vulnerable.

JupiterOne brings new visibility into cloud asset data to your Splunk Security deployment, taking your security operations even further into the cloud. Through the integration, JupiterOne automates difficult security workflows like surfacing findings, classifying and monitoring all your cloud-native assets, users, ephemeral devices and more, and seamlessly adds this data into your Splunk Security deployment for analysis. This unique partnership provides you with a complete picture of your risk profile and the ability to identify and secure potential weak points, while also providing detailed contextual data on any cyber asset to detect, respond, and recover from incidents with greater precision and speed.



Together, Splunk and JupiterOne provide situational and structural awareness of all data, events, and assets, so you don't just know what is going on, but also where. You can identify incidents or critical assets, automate remediation to fast-track security operations, and reduce your overall attack surface.



J1 Alerts

Time Range: Last 24 hours
Severity: All
Global Search: *
Hide Filters

Active Alerts: 144

Dismissed Alerts: 1

Active Alert Details

Alert Title/Message	Severity	Description	Count	First Alerted On	Last Alerted On	Alert Link
SEC: offboarded-user-with-residual-access	CRITICAL	Looks for offboarded users that still retain access somewhere	1	05/11/22 10:22:06 AM	05/11/22 3:24:23 PM	Click here
Unencrypted DatasStores in production not public	CRITICAL	null	19	04/01/21 2:51:11 AM	05/11/22 3:18:17 PM	Click here
s3-private-buckets-risks	CRITICAL	null	54	02/18/22 9:18:23 AM	05/11/22 3:18:15 PM	Click here
unencrypted data stores	CRITICAL	finds unencrypted data stores	26	02/18/22 1:41:34 PM	05/11/22 3:18:15 PM	Click here
gcp-public-buckets	CRITICAL	Finds Cloud Storage buckets with IAM policy configured to allow anonymous or public access.	2	08/13/21 5:18:20 PM	05/11/22 3:18:15 PM	Click here
Public S3 bucket via EC2 instances	CRITICAL	Public S3 bucket via EC2 instances	49	02/18/22 9:18:21 AM	05/11/22 3:18:14 PM	Click here
Non-encrypted datastores in production	CRITICAL	null	19	02/18/22 1:41:33 PM	05/11/22 3:18:14 PM	Click here
users-no-mfa	CRITICAL	users-no-mfa	1612	02/18/22 9:07:21 AM	05/11/22 3:18:12 PM	Click here

Integration Benefits

- Full visibility across your cyber asset ecosystem and infrastructure for enhanced situational awareness and actionability
- Detailed context on all your cyber assets to augment event-driven data and automate incident response with reliable precision
- In-depth view and information on impacted assets to quickly determine an incident's blast radius impact and take swift action

Example Use Cases

Extend the reach of your security investigations into cloud-native technologies.
Take your Splunk Security deployment even further into your cloud environment with JupiterOne to protect cyber assets that were previously out of your view. Conduct thorough security investigations that take into account the entirety of your enterprise, including your ever-changing, ever-growing cloud environment and all the cloud-native technologies it supports.

Accelerate incident response with context-driven awareness across your cyber assets.
With both JupiterOne and Splunk, you have a powerful investigation capability to understand both the structural and situational details of any cyber asset. JupiterOne's App and Add-On for Splunk enable security teams to ask complex questions, assess the blast radius of an impacted asset, and connect it back to Splunk's rich event-driven data. This enables teams to respond to incidents and automate remediation with reliable accuracy and the complete context of knowing when, how, and what assets were impacted.

Discover and understand all of your cyber assets and infrastructure.
Extend Splunk Security's visibility into endpoints, IP addresses, users, and devices with JupiterOne to secure all your cyber assets including cloud security providers, SaaS apps, code repos, IAM policies, vulnerability findings, and more. From asset management to vulnerability to compliance, gain in-depth knowledge of your cyber asset and infrastructure so you can have a complete picture of potential risks, threats, or security gaps and address any issues faster.

Seamlessly correlate both situational and structural context.
Combining Splunk Security's situational awareness, which alerts you of security events in the enterprise, with JupiterOne's structural awareness, which lets you know exactly where those events have occured, your security investigations are seamlessly optimized with greater context. With the data all in one place, you can easily connect all the pertinent information back to all of your workflows and event-driven data within Splunk.

Protect your expanding attack surface without adding complexity.
Most systems grow more complex over time and that has accelerated with the increase of cloud-first environments and the point-solutions that are added to manage this complexity. As this complexity grows, so does your attack surface. JupiterOne and Splunk Security enable you to protect your operations as they scale by giving you a detailed view of your environment and anything that could be posing a risk to your attack surface. Limiting unnecessary complexity helps minimize the attack surface and protect your assets from malicious actors.

JupiterOne Apps and Add-Ons for Splunk

Today, you can access JupiterOne from readily available applications and add-ons to augment your current Splunk Security data and enhance your workflows.

	Capabilities
JupiterOne App	Provides a dashboard to view your JupiterOne alerts in Splunk for shared reporting across your team.
JupiterOne Add-on for Splunk	Imports and enriches JupiterOne alerts, allowing you to access this data in Splunk. It also provides workflow actions that allow you to link back to entities in JupiterOne or search your JupiterOne account for any field value in Splunk, regardless of entity type. It also supports a custom Command so that you can execute a J1QL query directly from Splunk. Used in combination with the JupiterOne add-on, this app provides a dashboard to view your JupiterOne alerts in Splunk.
Splunk SOAR Integration with JupiterOne	Enables current Splunk users to dynamically query JupiterOne as part of their end-to-end security and remediation workflows. Users can get an alert from Splunk which will automatically trigger a query to JupiterOne and start remediation via a third-party tool.

JupiterOne is a cloud-native cyber asset management platform that helps enterprises easily map, analyze, and secure complex cloud environments.

Gain full visibility into your assets and the relationships between them to uncover threats, close compliance gaps, and prioritize risk. Strengthen the foundation for your cloud security program with JupiterOne.

Get unprecedented visibility into your cloud security posture, and start scaling your security program with JupiterOne.

Scan to Schedule a Demo ⟶

JupiterOne.com

JupiterOne