JupiterOne

Top 3 Use Cases for JupiterOne and Splunk

3 Common Use Cases

This brief walks you through 3 common use cases for how JupiterOne and Splunk provide greater visibility to enable faster response times on a broader set of assets for your SOC.

Introduction

Your attack surface is growing exponentially. As your cloud expands, so does your threat landscape. To stay secure, you need to have both situational (event logs and activity) and structural (configurations and correlations) awareness across all of your data, events, and assets. **Situational and structural awareness enable security teams to not only know *what* is going on, but also *where*.**

JupiterOne brings new visibility into cloud asset data (and more) to your Splunk Security deployment, taking your security operations even further into the cloud and supplying structural configuration and correlation context for cyber assets. Through the integration, JupiterOne automates difficult security workflows like consolidating cloud alerts, providing context around incidents, and monitoring all your cloud-native assets, users, ephemeral devices and more. JupiterOne leverages SplunkBase applications to add this data into your Splunk Security deployment for analysis.

Protect Your Entire Attack Surface Without 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.

Our Playbook for you
1. Connect the foundational technologies: Splunk SOAR and JupiterOne.
2. Build a complete cyber asset inventory in minutes
3. Understand your cyber asset relationships for added context
4. Prioritize security actions across business-critical assets
5. Continuously monitor any security event or drift across your assets

How it works
1. Install the Jupiter Add-On and JupiterOne App in Splunk
2. Add your JupiterOne credentials to enable the integration
3. JupiterOne Alerts and details are automatically imported to Splunk
4. Combine data from Splunk and JupiterOne in the same search
5. Use direct links from Splunk to JupiterOne to quickly dig deeper
6. Take immediate action on threats, vulnerabilities, gaps, and misconfigurations

Top 3 Use Cases

This brief walks you through **3 common use cases** for how JupiterOne and Splunk provide greater visibility to enable faster response times on a broader set of assets for your SOC.

Extend the reach of your security investigations into cloud-native technologies.

Take your Splunk deployment even further into your cloud environment with JupiterOne to protect cyber assets that were previously out of your view. Ingest CSPM style alerts from JupiterOne to bring cloud monitoring to your SOC, in Splunk. Manage 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 rapidly, and even triage or automate remediations involving correlated assets 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.

JupiterOne discovered data is directly queryable from Splunk. 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.

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

© 2022 JupiterOne. All Rights Reserved.