Case Study

Robinhood

Robinhood Achieves Continuous Monitoring and Actionability Across Vulnerabilities and Assets with JupiterOne

JupiterOne

Meet Daniel Miessler, Head of Vulnerability at Robinhood

Daniel leads the company's asset and attack surface management program. His team is actively responsible for securing all cloud resources, physical devices, and SaaS applications that process sensitive financial and customer data across the online brokerage.

The company's vulnerability management group needs to ensure that they are discovering, triaging, fixing, and continuously monitoring for any critical vulnerabilities and misconfigurations associated with the organization's most critical assets.

CHALLENGES

Vulnerability management needs more than siloed scanners and databases

Daniel had been searching for a better solution to help his team level up its vulnerability management and asset management programs. Visibility into important security metrics are top of mind for the vulnerability management group, as it determines how quickly the team can discover new vulnerabilities in order to triage, fix, and close them out in an efficient and timely manner. The work they do to protect the organization is highly visible. For example, Daniel's team and their security metrics (e.g. mean time to discover, triage, and fix vulnerabilities, etc.) are shared across the organization, as they are a critical priority for Robinhood's security strategy and program.

"There's a huge problem in the industry of different products building their own databases of vulnerabilities. We have many vulnerability scanning products that show us threats and risks. But each is selling their own individual vulnerability databases with their own associations. The problem we face is that all of these databases don't agree with each other. Even when someone has an asset management database, there's a huge challenge in getting vulnerabilities into that database and connecting them to assets in a meaningful way," said Daniel.

The Robinhood team needed a better way to do vulnerability management in order to continue to keep their platform and users secure. The first order of business for Daniel was to shift the way his team viewed vulnerability management. By shifting the focus away from constant patching and toward continuous risk management, he could start focusing on why the assets themselves have vulnerabilities attached to them and begin filtering problems by risk level.

> "We believe Vulnerability Management is more about Asset Management, Attack Surface Management, and Risk Management than pure patching. Our team's goal is to understand our current security posture as close to real-time as possible, and to properly prioritize action for deviations from ideal state.
>
> **Daniel Miessler**
> *Head of Vulnerability at Robinhood*
>
> Robinhood

SOLUTIONS

Robinhood achieves collaborative vulnerability management and asset management *that actually works*

Prior to JupiterOne

Robinhood followed the typical approach to asset management — going through all their different database sources and tools, manually translating all the asset metadata, pulling the data into an Excel spreadsheet, and manually mapping assets and vulnerabilities.

"This is a very human-intensive process and it's not automated. It's not like real asset management," said Daniel.

Although the vulnerability management team had set up automated workflows for their scanning tools to bring awareness of their vulnerabilities, the ongoing challenge was that their vulnerabilities data and processes weren't correlated with their asset management solution. This kept the team in the dark about additional vulnerabilities, their connections, and how they could inadvertently exploit each other.

In their search for a better way to discover, automate, and manage vulnerabilities across their entire asset ecosystem, the vulnerability team evaluated several solutions. As a fintech company, Robinhood has stringent compliance requirements to meet. Daniel built a vulnerability management program that clearly defined everything for compliance requirements, and that could also continue to effectively protect sensitive customer and financial data.

With JupiterOne

Robinhood now ingests, aggregates, and normalizes all critical vulnerability and asset data through their homegrown tools and commercial security solutions. With a centralized repository of their entire vulnerability database and asset ecosystem, Daniel's team can now effectively achieve a risk-based approach to managing Robinhood's asset ecosystem.

The vulnerability team uses JupiterOne's Questions as a foundation for their program to create an echelon of risk scoring to continuously monitor and alert on both managed and non-managed assets that are critical to their business. If any managed critical asset with a vulnerability exceeds their set risk threshold, his team is alerted immediately, and a ticket is assigned to the appropriate team, where immediate action can be taken to fix the vulnerability.

"What we've built starts with asset management from JupiterOne at the center. It serves as a single system of record for all asset types across the company — EC2 databases, IP addresses, applications, code, repositories, DNS, endpoints … everything," said Daniel. "We went with JupiterOne for this because it is based on a graph database, and has lots of features around asking questions. Once you ask the questions you can do really powerful stuff with the results."

> "What I liked about JupiterOne is that the platform understood this automatically. With JupiterOne, data is automatically associated and normalized with the authoritative set of assets and it's a natural part of the process. And that was the primary feature I was searching for.
>
> **Daniel Miessler**
> *Head of Vulnerability at Robinhood*
>
> Robinhood

RESULTS

A better questions-based approach to security, continuous monitoring, and reporting with JupiterOne

For years, Daniel has been a known advocate for asset management in the security industry. Prior to joining Robinhood, he championed the idea of a questions-based approach. He calls these "attack surface questions."

"My approach for vulnerability and asset management is fairly straightforward — regardless of the tech I use, these are the questions I care about and I want to know the answers at this cadence," said Daniel.

"When I was shown JupiterOne, that's exactly what I got. JupiterOne's Questions is the centerpiece to everything that we do and always gives us actionability. JupiterOne's Search feature allows me to query any asset across any dataset and I can save it as a question and an alert. It turns out, JupiterOne was exactly the model I had advocated for and was the product that should've always existed."

With JupiterOne, Daniel's team can turn highly specific questions into full queries that continuously run and automatically trigger an action when a match is found, such as sending a notification via Slack or email, creating a Jira ticket, or running other custom actions. This, in addition to having a centralized location for all querying — eliminating the need to query individual tools — tremendously accelerates Robinhood's vulnerability management workflows.

Among the benefits of using JupiterOne, the ability to optimize and scale resources has been key for Robinhood. "A JupiterOne query takes a few seconds and if we did it the manual way, it would take several minutes to get the answers to the same question." Before JupiterOne, Daniel estimates that it would have taken his team 20 times longer to achieve what they can accomplish in the JupiterOne platform with a single query.

His team also leverages JupiterOne data and metrics as part of their primary security reporting process when sharing results and metrics up to the company's executives, board members, and all employees at Robinhood. When Robinhood's SLA success rate suffered from inefficient discovery, assessment, triage, and remediation, JupiterOne's continuous search for vulnerabilities and acceleration of these activities took their team from spending up to two days on discovery alone to close to five minutes in total. Not only did their ability to meet SLAs improve for each part of the process, JupiterOne's up-to-date metrics dashboards made it easy to compare success rate across teams and provided critical, contextual knowledge that illuminated hidden information behind each SLA's performance.

The majority of the Robinhood's security team is now using JupiterOne. The vulnerability management team continues to ingest new integrations and data into the JupiterOne platform to support their growing attack surface and evolving needs. Even colleagues in engineering and across other parts of the company are now using JupiterOne's Search feature to discover and monitor assets related to their own teams.

"The great thing is that they're all self-serving on the JupiterOne platform," added Daniel.

> "
>
> Daniel estimates that it would have taken his team 20 times longer to achieve what they can accomplish in the JupiterOne platform with a single query.
>
> **Daniel Miessler**
> *Head of Vulnerability at Robinhood*
>
> Robinhood

SUMMARY

- Vulnerabilities and assets are ingested, aggregated, and normalized in a single platform
- Complete visibility and centralized repository of vulnerabilities and assets
- Vulnerability management team can achieve more with fewer resources
- Improved internet-facing security and risk posture
- Company-wide self-servicing for asset discovery and management

20x

Reduced time spent on correlating vulnerabilities to a single asset by 20x

Robinhood

About Robinhood

Robinhood is a commission-free stock trading and investing platform. Robinhood believes the financial system should be built to work for everyone. The company creates products that let their customers invest at their own pace and on their own terms.

Major integrations include:

aws

Jira Software

GitHub

okta

hackerone

snyk

vmware

Google

slack

orca security

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.

Scan to Schedule a Demo →

JupiterOne.com