CUSTOMER STORY

# Square

Square Financial Services Achieves 100% Visibility Across All Cloud Resources

### Products

InsightCloudSec

### Industry

Finance

### Size

Enterprise (Large)

# Overview

## The Company

Square Financial Services (Square), a wholly-owned subsidiary of Block, offers a complete suite of business tools and equitable loans that give every eligible business with a dream access to funding. Square partners with businesses of all sizes — from large, enterprise-scale businesses with complex commerce operations to sellers just starting out, as well as merchants who began selling with Square and have grown larger over time. Square supports sellers from Australia to Ireland, Canada to Japan, and across all 50 United States.

## The Challenge

- The security team lacked complete visibility into their multi-cloud environment and the resources running at any given time.
- Complete visibility was vital for consistent misconfiguration management.
- They needed a way to maintain tight security without stifling innovation.
- Security feature requests were being backlogged because they didn't have the bandwidth to address them.

# The Solution

- With InsightCloudSec, they gained 100% visibility across all cloud environments within a single pane of glass.
- This visibility enables them to uncover potential vulnerabilities in settings, code, or metadata that they can mitigate with the appropriate cloud developer or architect.
- The Rapid7 support team works on feature requests asynchronously so Square no longer has a growing backlog.

## Cloud Growth at Block Means Securing Innovation

The Block cloud security team is a foundational unit that supports any line of business at Block that uses a cloud platform, including Square. They are responsible for preventative controls, reactive controls, and secure by default options for developers and programmers. They also create security-approved modules that fit many different use cases, train teams on industry security standards, and ensure the secure use of all cloud platforms.

In 2019, business at Square was booming, and they focused on scaling their AWS and GCP cloud footprints to accommodate this growth. As they did so, the Block security team started to face some new challenges around security scalability.

## Lack of Asset Visibility

The major challenge the cloud security team encountered was one of quantity: Because the cloud offers the flexibility to scale resources up and down as needed, developers and engineers at Square would regularly spin up new instances and decommission others without the security team's awareness.

With so many environments — and separate AWS and GCP consoles to view the resources of each cloud provider — security didn't have consistent visibility into what was running at any given time, making it difficult to deliver comprehensive reporting on potential security risks.

> **It’s hard to know what resources are misconfigured if you don’t know what resources you have. Asset management is probably one of the toughest things in the cloud to do because it is so easy to create resources. You want that flexibility for users of the cloud to be able to spin things up and down whenever they need it. You don’t want to be in the way of that.**

Jason, Staff Security Engineer, Block

## Need for Innovation

The security team didn’t want their protocols to stifle innovation — but they also couldn’t accept less than secure configurations. Cloud platforms offer a host of new ways to solve problems and create efficiencies. Software programmers, engineers, and architects can be as detailed or holistic as they want with innumerable pathways, structures, and patterns to leverage. Square wanted their developers to experiment with new approaches to old problems and take advantage of whichever cloud platform was the right tool for the job. But they needed a way to secure their environments without getting in the way of this innovation.

## New Approaches to Security

The security team was also on a path of continuous growth and improvement. They regularly received security feature requests from various departments and discovered new, more valuable ways to approach security — but they didn’t have the bandwidth to tackle them. These requests would typically get tabled or placed in the backlog in hopes of getting to them in the future. Eventually, this pattern prevented a more modern, technologically advanced approach to security.

## InsightCloudSec Delivers Visibility and Innovation

When Square started searching for a cloud security solution, they looked for a true partner. They wanted a stellar product, but also the expertise and strategic guidance to build security features the organization needed.

Finding a product that could track resources in both AWS and GCP and aggregate that data in a central location was non-negotiable. They needed to be able to see what resources were running, who was running them, how they were configured, and whether changes needed to be made to maintain security.

Rapid7's InsightCloudSec product — along with with Rapid7's support team — checked all the boxes. InsightCloudSec provided comprehensive security across Square's AWS and GCP cloud environments, misconfiguration monitoring and alerting, and an extended team that could offer feature support as-needed.

> **We are multi-cloud, so having one provider that can see all of the different clouds and aggregate that data in a centralized location is invaluable.**
>
> Jason, Staff Security Engineer, Block

## Tracking Cloud Resources

InsightCloudSec's greatest value is in its unique ability to keep track of when resources are created and how many resources are in use across many different projects — and deliver that information across all cloud providers in one unified view.

This asset management capability offers a consolidated and normalized view of individual resources and their metadata. Square's security team can now zoom in to dig through settings and code, and then zoom back out to get a broader view of all assets organization-wide. The team can answer questions like:

- Which accounts have the most resources?
- Which accounts have a specific type of resource?"
- What databases are in use?
- What does the storage structure look like?
- What do the firewall rules look like?

This ability to see everything happening in the cloud, how it is built, and what security rules and configurations have been applied is invaluable to security professionals who aren't in the cloud building and developing every day.

> **One of the key strengths of InsightCloudSec and Rapid7 in general is that they do asset management really well. There are lots of dashboards that are incredibly easy to manage and give really nice granular views of individual resources and their metadata.**

Jason, Staff Security Engineer, Block

## Identifying Misconfigurations

Now that the security team has all cloud environments available to them from a single pane of glass, they can dig deeper to uncover misconfigurations and potential vulnerabilities that might be hiding in the settings, code, or metadata of a particular workload.

A single, buried misconfiguration can make the difference between a secure environment and an environment that provides an attack pathway, so it is incredibly valuable for the team to have full visibility into each workload to ensure no stones are left unturned. Once they discover an issue, InsightCloudSec's integrations with Slack, ServiceNow, and Jira enable them to shoot a quick message to a developer, architect, or engineer to fix the problem and keep security airtight.

## Building New Security Features

Rapid7's support team offers additional value by taking on the work of building out feature requests. Instead of dedicating valuable employee time to address these, Square can offload them to Rapid7 to be completed asynchronously with other projects. With a quick Slack message to the support team, Square gets an extra set of skilled hands to:

- brainstorm new approaches
- evaluate and prioritize requests
- build those requests into usable features

## Square Achieves 100% Cloud Visibility with InsightCloudSec

With this newfound capability, there are no more guessing games about who is using what, where, and how they've built it. Everything is available to the cloud security team at a glance from an easy-to-access dashboard. The security and development teams work in tandem to keep the cloud flexible and safe.

They now also leverage custom insight packs from InsightCloudSec that deliver weekly reports on security posture over time. With this intelligence, Square's cloud security team can look back over months and even years to see how their security posture has matured.

Finally, feature requests are now actively built in conjunction with Rapid7 rather than getting queued in the Square team's own lengthy backlog. With a quick Slack message from the Square security team, an idea turns into a feature request and the Rapid7 support team is on top of it.

## Looking Ahead

Regarding the future partnership between Square and Rapid7, Square's staff security engineer, Jason, has this to say: "Well, I hope it [the partnership] continues. We've had a lot of success in the last year and...you all are super receptive to feature requests to improve your own products and tailor them to our needs."

Square's financial services security lead added, "I think the customer support has also been really attractive for us. It's been a really great partnership."

> **Once configured, InsightCloudSec provided me 100% visibility into the Square Financial Services cloud accounts. Before InsightCloudSec, I had to ask the engineering team, cloudsec, or cloud foundations about what cloud services were in use.**
>
> Thomas, Financial Services Security Lead, Square Financial Services

## About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

**PRODUCTS**

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

**CONTACT US**

rapid7.com/contact

To learn more or start a free trial, visit: **https://www.rapid7.com/try/insight/**