CUSTOMER SUCCESS STORY

BigID Uses Reco To Integrate SaaS Security With The SOC

BigID is a leader in data security, privacy, compliance, and governance: enabling organizations to proactively discover, manage, protect, and get more value from their data in a single platform for data visibility and control. Customers use BigID to reduce their data risk, automate security and privacy controls, achieve compliance, and understand their data across their entire data landscape.

Before Reco

BigID is a modern, remote-first technology company. Being heavily reliant on SaaS apps, such as Google Workspace, MongoDB, and Salesforce, the Cloud Security team realized that the very large SaaS landscape was a critical attack surface that needed more attention and capabilities. They didn't have visibility into what was going on across their SaaS landscape or a cohesive way to monitor and protect it.

Tedious, Manual Processes

BigID was sending logs from its most critical SaaS applications into its SIEM. But with all the diversity and nuance of SaaS applications, this required a lot of manual work to get the data flowing to the SIEM. Some apps don't have a native way to connect to the SIEM, relying on time-consuming engineering cycles to build APIs and custom workflows as a workaround. Meanwhile, other apps require expensive upgrades to even produce logs. Visibility was severely limited by which apps would produce logs and which ones were deemed important enough to invest the time to build the connections.

Limited Threat Detections

BigID was working to build a threat detection library. But with all the information coming out of SaaS apps, it was a time-consuming process. Parsing out thousands, if not millions of events, analyzing the data, and then creating threat detection frameworks demanded a lot of effort and yielded slow progress. It took several days to create one threat detection. What's more, not having the threat detections meant there was a risk that something malicious could slip through the cracks.

Configuration Management

With the diversity of SaaS, there is an incredible amount of nuance in how each one is configured. There's no single person who is a master at configuring them all. Plus, SaaS landscapes are fragmented. Managing configurations means toggling through multiple dashboards, each with unique controls. Not to mention, SaaS apps are constantly changing and being updated. Could a new setting or feature, like GenAI, introduce security risks?

The old way of managing SaaS security was just not scalable. As BigID's SaaS landscape rapidly grew, they needed a solution to help them unify SaaS security controls and integrate remediation workflows with Security Operations.

The Solution

BigID deployed Reco and immediately saw value. They were able to understand their posture for core apps like Google Workspace, Salesforce, and MongoDB and also gain insight into their second line of business critical applications, like Okta, Jira, and Confluence – all from one platform.

The biggest "Aha" was the scale of the SaaS landscape and how the misconfigurations can accumulate over time. BigID realized they had some gaps in change management processes, like offboarding users and deactivating inactive Admin accounts. Reco was the catalyst that caused them to look into where the gaps were and implement processes that could reduce potential exposure points.

One-Click Remediation Insights

Reco identified the most critical areas that needed BigIDs attention first. Using the ‘How to Fix’ feature, the Security team was able to get one-click insights into how to clean up risks. Then, they could triage the issue through the Reco platform, sending detailed remediation instructions to each app owner.

BigID + Reco for Holistic Data Security Across SaaS

The BigID platform helps with discovering and classifying sensitive data across the entire stack, including SaaS. It helps identify the “crown jewels” so that the Security team can understand which apps are the most critical. When the Security team deployed Reco, it told a powerful story with BigID.

> “ When we use BigID and Reco together, we get the full picture of where sensitive data is flowing, how it’s being shared, and what actions people are taking. We also see the relationships between apps, i.e. how Salesforce is sharing data with Jira, and what type of data is being shared. Then, we know what changes need to be made to keep our most critical assets protected.,says Kyle Kurdziolek, VP of Security at BigID.

A Dynamic Solution for a Dynamic Landscape

But it wasn’t about a point-in-time snapshot of their SaaS security posture. BigID deployed Reco to keep tabs on how SaaS changes over time.

> “ It’s about what our Salesforce instance has become – versus what it was in the former. What new settings or features have been introduced that may impact security? Have new users been added and what do their permissions look like? Which accounts are inactive and still connected? And what actions have been taken that may be suspicious that warrant an investigation? Reco allows us to monitor our SaaS apps continuously, as the environment changes and grows, says Kurdziolek.

The Results

Today, BigID has the intelligence it needs to reduce its SaaS security risk, while also keeping a watchful eye on real-time threats that demand immediate action.

Eliminated Months of Work Building Threat Detections

Instead of spending days combing through logs and manually building threat detections one-by-one for each app – a process that took months – Reco comes out-the-box with threat detections built in. This not only saves valuable time, but also ensures nothing slips through the cracks.

> “ When it comes to threat detections for SaaS, Reco has done the heavy lifting for you. It’s been an enabler for us to expedite our threat detection library and has allowed us to extend our automation capabilities so we can remediate those threats fast. I wouldn't recommend any other tool to accelerate the SaaS threat detection development program, says Kurdziolek.

Enhanced Security Operations with Automation

Using Reco Identity Threat Detection and Response (ITDR), Reco empowers BigID to rapidly assess, triage, remediate, and recover the whole security event through automation with just one click. Threat detections are triggered by Reco alerts, which push to the SIEM through the capabilities of Torq, a SOC automation tool.

> “ That’s how impactful Reco can be for an organization. Using the threat detections and the identity context Reco provides, you can feed that information into the automation of Security Operations and trigger a remediation workflow. This saves time for your engineers and frees them to focus on the work that matters most to them,says Kurdziolek.

Elevated Insider Risk Program

With the identity context provided by Reco, BigID is able to monitor for insider threats. They can see if someone is sending files to a personal email address, which is something that native Google Workspace monitoring couldn’t reveal. Then, they can use the BigID platform to understand if that file contains sensitive information.

With this holistic context, Security engineers can quickly identify insider threats and remediate within the SOAR.

> “ Reco and the BigID platform together have really enhanced our insider risk capabilities. Reco will flag suspicious insider activities, and then the BigID platform will provide insight on what type of data was accessed or shared. You get the full context of the activity, and can push that to your SOC through automation so they can respond appropriately, says Kurdziolek.

Consolidated Configuration Management

Reco simplifies configuration management across the diverse array of SaaS apps in BigIDs ecosystem. No need to be an expert on each one. Reco identifies misconfigurations, ranks them in terms of priority, and provides intelligence on how to clean up each one. From there, Security can notify each app owner and provide them with detailed instructions on how to configure the app correctly.

> “ We’re happy to be a Reco customer, and we’re always looking for ways to extend upon the platform to enhance our capabilities. Not only for our security operations, but also our compliance, configuration management, and insider threat program. Reco is very pivotal for BigID across all those domains, says Kurdziolek.

About Reco

Reco is the leader in Dynamic SaaS Security — the only approach that eliminates the SaaS Security Gap (the growing gap between what you can protect and what’s outpacing your security). This gap is driven by SaaS Sprawl — the proliferation of apps, AI, and identities; the challenge of keeping their configurations secure amidst constant updates, and the challenge of finding threats hidden within an ever-growing number of events. Dynamic SaaS Security by Reco keeps pace with this sprawl, no matter how fast it evolves, by covering the entire SaaS lifecycle — cradle to grave. It tracks all apps, SaaS-to-SaaS connections, Shadow SaaS, AI Agents, and Shadow AI tools, including their users and data, and adds support for new apps in days, not quarters. Reco maintains airtight posture and compliance — even as apps and AI Agents are added or updated. And it also ensures accounts remain secure, access privileges are minimized, and alerts are provided for critical threats. Learn more at reco.ai.