Wellstar Health Uses Reco To Manage Shadow IT And Gain Visibility Into SaaS Risks

Wellstar Health System is the largest non-profit t integrated healthcare system in Georgia, with 12 hospitals, 400 ambulatory centers, and 40,000 employees. Wellstar is nationally recognized for its inclusive culture, exceptional doctors and team members, and personal, high-quality care.

The Benefits of Reco

Every day, Wellstar Health relies on SaaS applications to support care operations, communicate with patients, and transact with Payers. In many ways, Wellstar is just as much a technology company as it is a healthcare company. But being so large and so technology-forward created one, big problem for the Security team: shadow IT.

Shadow Apps

Wellstar's SaaS footprint was growing. With the self-service nature of SaaS, doctors, clinicians and business workers were rapidly adopting new SaaS applications to improve efficiency and support evolving needs. The Wellstar Security team knew that unauthorized SaaS usage was a problem, but they had no idea how big the problem was because they had no visibility into the SaaS ecosystem.

Lack of Visibility and Control

Without visibility into the SaaS ecosystem, the Wellstar Security team was unable to effectively manage the risks introduced by SaaS apps. They knew they used Microsoft 365, ServiceNow, and other business critical applications, but they didn't know how these applications were configured, who was using them, and how. Are people putting PHI in applications that are not HIPAA compliant? How are these applications sharing data with other apps? Too many questions remained unanswered.

Compliance Management

Being a healthcare provider and payment processor, Wellstar must comply with HIPAA and PCI. Since Wellstar provides Medicare and Medicaid, it also has some environments that are subject to NIST 800-53 and FISMA. Without visibility into the SaaS ecosystem, Wellstar's SaaS security program was non-existent.

First Step: Discovery

The Wellstar team knew team members utilized a lot of SaaS applications, but nothing could prepare them for what Reco would uncover once deployed. In a matter of minutes, Reco discovered over 1,100 shadow SaaS applications connected to its environment.

Other key findings included:

- 1185 shadow applications, 200 are unused
- 271 files exposed publicly and 8,200 files exposed to third parties
- 3523 users without MFA enabled and 1 admin
- Over 11,000 stale accounts

Next Step: Mitigation and Remediation

Seeing so many shadow applications felt overwhelming at first, but Reco Customer Success helped Wellstar create a plan to prioritize the most impactful remediation tasks.

Shadow Apps

Reco provides a vendor risk score for every application based on how risky the application is reputationally. It also shows how many people are using each application. Using this information, Reco Customer Success helped Wellstar sort by apps with the highest risk score and the highest number of users to prioritize first.

> ***"The Customer Success team has been very supportive in helping us with process management and helping us get the most value out of the tool. That was an added benefit I did not expect out of the Reco platform."***
> Mike D'Arezzo, Executive Director of Security and GRC, Wellstar Health System

Remediation

Reco helped Wellstar implement policies that improved their security posture and reduced the attack surface.

Remediation activities included:

- Built a workflow to review guest accounts in order to reduce stale accounts
- Unapproved 73 risky apps
- Migrated users to safer apps and consolidated licensing
- Improved posture from 39% to 62%

A Continuously Adaptable, Scalable Solution

As Wellstar's SaaS consumption grows, Reco is able to respond quickly to requests for new integrations to support Wellstar's evolving needs. If Wellstar needs coverage for a new app, they can count on Reco to offer support for that application in weeks, not months or years.

Result

The journey with Reco took Wellstar from a place of "I have zero visibility into my SaaS ecosystem" to having total visibility into SaaS deployments and granular control over how it's configured and how it's being used.

Visibility and Control

Now, Wellstar has the intelligence they need to reduce shadow IT, minimize risks, and investigate risky behavior within SaaS applications. If someone logs in from a suspicious location they can investigate. Was this doctor traveling or is this potentially a malicious threat? If someone is using a new app they can go straight to that person and ask about it.

> ***It's visibility. 1000 percent. I bought Reco and still pay for Reco because of visibility. So instead of, 'Hey, are you using this?' It's 'I know you're using this, and let's talk about how you're using this so we can make sure you're using it safely,"*** says D'Arezzo.

Targeted Interventions

The Wellstar team uses Reco to identify unauthorized applications and understand who's using them at the organization. From there, they can implement targeted interventions that remediate security issues and compliance violations. For example, they noticed a particular Doctor was using an unauthorized application. They went to speak with this doctor and found out he was putting PHI in that application. Since they didn't have a business associates agreement (BAA) with that vendor, that was a compliance violation. Next, they could make the decision to either get a BAA in place with that vendor or migrate that doctor to a safer, business approved application that served the same purpose.

> ***It's having the intelligence to say, Here's a tool that's rated A that's got 1000 users on it. Here's one that's rated F that has 200 users on it. They're comparable tools, so let's get these 200 users onto the safer tool with 1000 users. That way, we remove the risk of those 200 users using that site while still empowering employees with the tools they need to do their job safely,"*** says D'Arezzo.

Freed Up Costs

Reco helped Wellstar discover redundant accounts that were eating up extra costs so they could save money. For example, Wellstar discovered the organization had nine different accounts with SmartSheet. By removing the extra eight accounts and migrating users into one account, the discounts from the tiered pricing package allowed Wellstar to save $200K yearly on Smartsheet licenses.

> ***"Reco has not only helped us protect our business, but it has also produced measurable financial ROI by discovering redundant accounts and allowing us to consolidate licensing on SaaS tools."***

Continuous SaaS Compliance Program

Wellstar went from having virtually no SaaS compliance program to having a continuous SaaS compliance program. Using Reco, they can identify the application owner for a particular app and then provide this person with prescriptive guidance on how to clean up the app's compliance posture. They can monitor it over the year and sync up with app owners when audits are approaching to clean up any issues.

Stay Ahead of Evolving Technology

Reco not only helps Wellstar manage their current technology but also helps them understand where the market is going. What do folks want out of the next iteration of the transformation of healthcare? What types of applications are going to be useful in the future? Wellstar uses Reco to identify trends, for example: 500 doctors signed up for the same GenAI app. Equipped with this information, they can start looking into this technology to understand what direction it's going and the best way to secure it.

> ***"My journey with Reco has looked like this: I went from, 'I don't know my SaaS landscape' to 'I know my SaaS landscape but I don't know who's using it.' From 'I know who's using it but I'm not managing it,' to 'I'm managing it but I don't know if I'm managing it effectively', and finally to 'With Reco I've got everything I need to know, and I'm managing it effectively'. My processes are in place. I can accept any incoming requests for new SaaS applications and manage the risks around them."***

About Reco

Reco is a full lifecycle SaaS security solution. It empowers organizations with full visibility into every app, identity, and their actions to seamlessly prioritize and control risks in the SaaS ecosystem. Their AI based graph technology connects in minutes and provides immediate value to security teams to continuously discover all SaaS applications including sanctioned and unsanctioned apps, shadow apps, associated identities from both humans and machines, their permission level, and actions. Reco uses advanced analytics around persona, actions, interactions and relationships to other users, and then alerts on exposure from misconfigurations, over permission users, compromised accounts, and risky user behavior. This comprehensive picture is generated continuously using the Reco Identities Interaction Graph and empowers security teams to take swift action to effectively prioritize their most critical points of risk. Reco uses a low code/no code approach to add a new SaaS integration in 3-5 days.

You can learn more or book a demo at www.reco.ai