reco | CSK Cole Scott & Kissane

CUSTOMER SUCCESS STORY

CSK Secures Its SaaS And Enabled Responsible AI Usage, With Reco

About CSK

Cole, Scott & Kissane, P.A. (CSK) is the largest law firm in the state of Florida. As a full-service law firm, CSK provides clients with experienced counsel and services in numerous areas of the law. In order to better serve clients, CSK is committed to adopting and utilizing the best technology available.

Before Reco

Being a forward-thinking law firm, CSK embraces technology innovation, automation, and AI because it believes this enables the business to provide the best services to clients. When it comes to SaaS adoption, the Microsoft365 suite is core to its infrastructure, with other apps like Salesforce, ServiceNow, and DropBox being crucial to the business.

CSK eagerly encourages the use of technology to solve problems, while always keeping data privacy top of mind. The CIO, Jason Thomas, lives by the philosophy that “the answer is never ‘no’ – the answer is always, ‘let’s figure out how to support technology needs’.”

However, in the last few years the CSK Security team found themselves dealing with a new challenge driven by the rapid surge of a new technology trend: GenAI.

Shadow AI

First ChatGPT came out. Then Claude, then Microsoft Copilot, then Gemini, and then DeepSeek. Today, nearly every app offers native AI capabilities. The CSK team knew that restricting the use of AI wasn’t the answer.

They needed to be able to support the use of AI by providing policies, monitoring, and sanctioned platforms. However, CSK had no visibility into what was being used, who was using what, and how.

Regulatory Risk

It's easy to spin up a SaaS instance and start putting data in it. In today's SaaS-driven world, IT teams don't have control over this. What's more, CSK deals with personally identifiable information (PII) and protected health information (PHI), such as insurance information and claims. CSK is bound to HIPAA rules due to the sensitive nature of this data. Without visibility into the SaaS ecosystem, CSK was at risk of confidential data getting ingested and leaked via AI tools.

Complexity of Existing Solutions

CSK had tried two different solutions to deal with its sprawling SaaS and AI environment. But both solutions were overly complex, requiring extensive technical knowledge and continuous maintenance, including deploying and managing internal virtual machines. CSK desired a solution that was easier to deploy, integrate, and maintain.

First Step: Discovery

CSK signed up with Reco and was amazed at how fast and easy it was to get up and running. Reco integrated in minutes and within hours provided visibility into the entire SaaS environment, surfacing risks that had lay hidden as well as shadow apps and shadow AIs that were connected.

Some initial findings included:

- **780** totally applications discovered - **307** of which were shadow apps
- **38** apps using AI - **15** of which were shadow AI
- **451K** files shared publicly in Sharepoint - **50%** of which hadn't been touched in 90 days
- Discovered malicious agent, BAV2ROPC

Next Step: Mitigation and Remediation

CSK was floored by Reco's ability to make remediation simple.

> Reco does a great job of saying: here's the issue, here's why it matters, and here's what you can do about it. In plain English, no expertise or guesswork is required," says Jason Thomas, CIO at CSK.

Some initial remediation activities included:

- Enhanced password protections policies
- Enhanced conditional access for generative AI
- Enhanced security settings for guest accounts in Microsoft: MFA enforced and guests aren't allowed to access Copilot
- Enhanced MDM - don't allow users to connect to Microsoft from jailbroken or rooted devices
- Removed Salesforce external admin accounts

> Reco does a great job of saying: here's the issue, here's why it matters, and here's what you can do about it. In plain English, no expertise or guesswork is required," says Jason Thomas, CIO at CSK.

These are complex environments. There are so many different settings and configurations that you don't even think about that could have an impact on data leaking," says Thomas. "Reco presents the misconfigurations and the recommended configurations and enables you to improve your posture right away. It's extremely user-friendly.

The Results

With Reco, the CSK Security team can enable the safe use of technology in the business. They can maintain a watchful eye on their SaaS environment, protecting client privacy, reducing data exposure risk, and continuously discovering and managing shadow SaaS and shadow AI.

Enabling Safe AI Innovation

CSK doesn't ban anything. Instead, they uphold policies. If someone is using DeepSeek or another risky AI tool, Reco will notify the Security team right away. Then, they can go straight to that technology user, educate them about the risks, and offer them a safer tool to meet their needs.

> We never want to punish people for what they're doing. We want to redirect them to do their jobs the right way, the sanctioned way,

Visibility and Data Governance

Reco provides CSK with visibility into their SaaS ecosystem, including shadow IT and AI tool usage. It shows them what people are using and what they are trying to do. This visibility enables the Security team to identify potentially risky behaviors, investigate further, and implement targeted solutions.

For example, they can see in Reco if someone is uploading documents into unsanctioned AI tools. Then, they can use their Zscaler data security tool to understand what type of data this document contains, i.e. is it PII or something benign? The combination of these two tools allows CSK to gain a full view into how and where sensitive data is flowing by way of SaaS so they can proactively address issues through education.

> There's always a new AI app coming out every day, and tomorrow there will be another one. We're not trying to block everything. We just need to understand what people are using and how, and Reco allows us to do that," says Thomas.

Enhanced Security Posture

The CSK SaaS security posture has gone up from 45% to 75% in the last six months by making simple changes. Reco's recommendations have helped CSK identify and remediate security gaps they hadn't even considered.

> We think we have Teams configured in a pretty secure way, and then Reco recommends a bunch of things we didn't think of that could have an impact on data leaking," explains Thomas.

Saved Time

Compared with the previous two tools that CSK had used, Reco saves time and effort. The other tools took several days to get integrated, plus they required complex deployment processes. Integration with Reco takes minutes, and it starts providing alerts in a few hours.

Operational Efficiency and ROI

By simplifying security management and reducing the technical burden on analysts, Reco delivered immediate operational value.

> “Reco is the most user-friendly, simplest solution you can implement, and you get your ROI in terms of operations right away," Thomas says.

The platform also helped CSK optimize their application portfolio, reducing redundant tools and associated costs. For example, when they discover someone is using Asana, they can go to that person and say, 'Did you know we already have Smartsheet?'

CSK has further enhanced Reco's value by integrating it with their SIEM for instantaneous alerting and automated remediation. When something gets picked up, they can remediate it right away within existing workflows.

Looking toward the future, the CSK Security team is now building SOC automation playbooks to further streamline their security operations. As the law firm continues to embrace innovation, Reco provides the security foundation they need to move forward confidently.

> “We are a very creative organization in terms of finding technology, AI, and automated solutions to solve problems," concludes Thomas. "With Reco, we can maintain a handle on our attack surface while enabling technology advancement.