Streamlining Data Protection: How Reco Transformed Cresta's Approach to Safeguarding Customer Data

7 Minutes
Time to Onboarding

2 Days
Full Risk Assessment

50%
Teams Time Saved

Cresta makes every customer interaction excellent. Cresta turns real-time intelligence into real-time action to make the contact center smarter – and every agent and manager more productive. Powering customer experiences for companies like CarMax, Blue Nile, Earthlink, Intuit, and Porsche, Cresta is real-time generative AI for the real world. To learn more about Cresta, visit www.cresta.com.

One of the critical challenges faced by Cresta was the protection of customer data, given the sensitive nature of their business operations. Traditional Data Loss Prevention (DLP) solutions proved inadequate in meeting their requirements for safeguarding their SaaS data, resulting in headaches, disruptions, and falling short of auditor expectations. To address this issue, Cresta.ai turned to Reco, a cutting-edge SaaS security platform.

According to Robert Kugler, Head of Security and Compliance at Cresta,

> **Reco provided us with a seamless onboarding experience. Within minutes of connecting Reco to our systems, Cresta gained visibility into our sensitive SaaS data, identified its exposure, and experienced tangible value. Unlike our previous DLP tool, which took months to deploy and introduced operational burdens, Reco seamlessly integrated without creating any additional problems and had no impact on system performance.**

Protecting customer data remains a top priority for Cresta. Reco understood the specific challenges faced by Cresta and the limitations of traditional DLP solutions. Reco recognized the need for a solution that not only identified potential data exposure but also provided actionable insights and automated workflows to continuously reduce risk.

Reco's innovative approach enabled Cresta to identify and monitor customer data stored across various SaaS platforms, effectively highlighting potential vulnerabilities and exposures. This discovery process proved instrumental in strengthening Cresta's data protection efforts.

Driving Efficiency with Contextual Alerts

A key benefit offered by Reco to Cresta was the ability to provide context-rich alerts. This feature set Reco apart from other solutions in the market. Instead of inundating Cresta's security team with generic alerts, Reco delivered alerts that were easily understandable, reducing the time it took to detect, investigate and respond from 2 days on average, to 4.68 minutes.

> **Reco's alerts came with comprehensive context, eliminating the need for manual investigation and triage. Their contextual accuracy gave us the confidence to implement automation workflows and take swift action in response to alerts, reducing the burden on our security team and streamlining the process.**

Reco's policy management capabilities empowered Cresta with valuable control over suspicious behavior and access to sensitive information. The platform and the confidence gained from streamlining risk reduction enabled Cresta to increase coverage to other SaaS tools and define policies to identify risky behavior, overprivileged users, and other suspicious activities. Additionally, Reco provided insightful observations on user behavior. Cresta utilized Reco's features to monitor and analyze employee actions, ensuring compliance and effectively mitigating potential risks.

> **Alongside context, Reco's ability to understand identity behavior regarding sensitive data sets it apart from other SaaS security products. The added value of going beyond tool posture allowed us to be proactive in detecting and responding to sensitive data exposure and leakage.**

By implementing Reco, Cresta successfully overcame the limitations of traditional DLP solutions, significantly enhancing their data protection capabilities within the SaaS environment. Reco's seamless onboarding process, contextual alerts, automated workflows, and policy management functionalities delivered immediate value to Cresta, saving significant operational time.

"Reco's metadata-driven approach, combined with its comprehensive ability to map data, apps, and identities into an inventory of items and events, perfectly aligned with Cresta's needs. Reco empowered Cresta's security team to proactively protect customer data, mitigate risks, and ensure a secure environment for both customers and employees." Through Reco's partnership, Cresta can confidently continue its mission of revolutionizing customer service, knowing that their customers' sensitive data is safeguarded by a highly efficient and intelligent solution.

About Reco

Reco is the leader in Dynamic SaaS Security — the only approach that eliminates the SaaS Security Gap 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. 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. This comprehensive picture is generated continuously using the Reco Knowledge 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.

Learn more or book a demo