Banco BS2 Utilizes Reco for SaaS Security Visibility During M&As

Banco BS2 is a leading financial services provider that delivers API-driven banking solutions to other companies. With a massive transaction database and AI-powered fraud prevention systems, Banco BS2 has evolved from serving end customers directly to exclusively partnering with businesses in the B2B financial services market over the past five years.

Before Reco

As Banco BS2 rapidly expanded their B2B financial services model, their SaaS ecosystem grew exponentially. The company's transformation success created an unexpected challenge for the security team: complete lack of visibility into their sprawling SaaS environment.

Daily Security Surprises

Banco BS2's SaaS footprint was exploding. With employees across different business units rapidly adopting new applications to support evolving workflows, the security team faced a constant stream of surprises. Every day brought discovery of new applications, new integrations, and new risks they hadn't anticipated. The security team knew unauthorized SaaS usage was happening, but they had no idea of the scope because they lacked visibility into their SaaS ecosystem.

Shadow IT and Risky User Behavior

Without comprehensive SaaS discovery capabilities, Banco BS2 was unable to effectively manage the risks introduced by shadow applications. They discovered employees were using corporate email addresses to register for personal services like streaming apps, behavior that, while not directly risky, highlighted concerning patterns that needed awareness and training.

Acquisition Integration Challenges

During company acquisitions, Banco BS2 struggled to quickly gain visibility into new domains and their associated SaaS applications. The previous security approach made it difficult to seamlessly expand security processes to cover acquired companies and identify applications that weren't properly mapped by previous IT teams.

Step 1

Discovery

When Banco BS2 first implemented Reco's Dynamic SaaS Security platform, the initial visibility was overwhelming but transformative. Douglas Ferreira, CISO and Superintendent of Fraud Prevention, described it as "opening the skies and removing the clouds to see what was really happening in our company."

Key Findings Included:

- Shadow applications across multiple business units using corporate credentials
- Unauthorized AI tools and SaaS applications flying under IT radar
- Risky user behaviors like using corporate emails for personal service registrations
- Unmanaged integrations between SaaS applications creating security gaps
- Stale accounts and permissions from previous system migrations

Step 2

Mitigation and Remediation

Seeing the full scope of shadow IT felt overwhelming initially, but Reco's approach provided a clear path forward through systematic risk prioritization and remediation

A Systematic Approach

Reco's platform helped Banco BS2 prioritize remediation efforts by providing:

- Risk-based scoring for applications and user behaviors
- Business context for each discovered application and integration
- Clear remediation guidance with step-by-step actions
- Automated policy enforcement for consistent security controls

> It was like opening the skies and removing the clouds to see what was really happening in our company. It's better to know the risks and vulnerabilities before bad actors discover them.
>
> **Douglas Ferreira**
>
> CISO and Superintendent of Fraud Prevention
> Banco BS2

Remediation Activities Included:

- Built custom detection rules using payload analysis to correlate SaaS data with SIEM systems
- Implemented OAuth governance to control third-party application access
- Created targeted training programs to address risky user behaviors
- Established continuous monitoring for new application discoveries
- Developed acquisition playbooks for rapid security integration

Seamless Acquisition Integration

The real test came during Banco BS2's most recent acquisition. By simply adding the new company's domains to Reco, they immediately gained complete visibility into all SaaS applications, including ones the previous IT team hadn't mapped. This allowed seamless expansion of security processes to cover the acquired company with instant visibility and targeted action plans.

Result

The implementation transformed Banco BS2 from a reactive security posture constantly fighting fires to a proactive approach that anticipates and prevents security issues before they impact operations.

Complete Visibility and Control

Now, Banco BS2 has comprehensive intelligence needed to reduce shadow IT, minimize risks, and investigate suspicious behavior within SaaS applications. The security team can proactively identify new applications, understand user behavior patterns, and implement targeted interventions before risks escalate.

Advanced Technical Capabilities

The platform enabled Banco BS2 to create sophisticated detection rules using payload exploration and API analysis. By analyzing specific fields within SaaS application payloads, they can build custom use cases and correlate that data with information from other systems feeding into their SIEM, providing the same level of control over SaaS applications that they maintain for internal systems.

> The same level of control that we usually implement inside our internal systems, now we are having the possibility to create similar rules inside the SaaS applications that our users are using.
>
> **Douglas Ferreira**
>
> CISO and Superintendent of Fraud Prevention
> Banco BS2

Proactive Risk Management

Instead of discovering problems after they occur, Banco BS2 can now:

- **Anticipate security issues** before they impact operations
- **Create targeted action plans** for identified risks
- **Move from reactive to proactive** security posture
- **Enable business innovation** while ensuring responsible security practices

Continuous Adaptation for Business Growth

As Banco BS2's SaaS consumption continues to grow, Reco adapts quickly to support their evolving needs. When they need coverage for new applications, they can count on support in days, not quarters, enabling their security to scale with business velocity.

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