VARONIS

How a Real Estate Company Secures Salesforce with Varonis

> If you use Salesforce and you give a damn about security, you need to at least try Varonis. Without it, it's impossible to see all of that data from a holistic perspective in one pane of glass.

About this case study:

Our customer is a top real estate organization in the U.S. We have anonymized the company name at their request.

HIGHLIGHTS

Challenges

- Gaining data visibility for multiple Salesforce instances
- Limiting access in a complex Salesforce environment
- Preventing data exfiltration and insider threats

Solution

Varonis Data Security Platform:

- Finds and classifies sensitive data across cloud apps like Box and Salesforce
- Provides visibility and control over your critical data and IT infrastructure
- Monitors and alerts on abnormal behavior on critical systems
- Detects and helps prevent DNS exfiltration attempts

Results

- Ability to monitor and detect threats across cloud apps
- Decreased overexposure across Salesforce instances
- Peace of mind as their use of Salesforce evolves

CHALLENGES

Locking down permissions in Salesforce

One of North America's top real estate organizations (anonymous by request) adopted Varonis to protect sensitive data in their most relied-upon SaaS apps.

They knew sensitive data was potentially at risk in Box, but they didn't realize just how vulnerable other areas had become. Rampant permissions creep had left critical systems like Salesforce overexposed.

Senior Cybersecurity Engineer Tony Hamil explains:

> **"We did a Proof of Concept because we wanted visibility into Box. We applied it to Salesforce too because, I figured, why not?"**
>
> **"That's when we learned that gaining visibility into Salesforce was far more necessary than we had realized because of how little we knew about our Salesforce instances."**

Like many businesses, the real estate company had become reliant on Salesforce to connect its commerce channels, streamline marketing, and empower sales teams.

But if you're not preventing excessive access and properly offboarding users, your Salesforce blast radius — the damage attackers can do once they land on a network — increases exponentially.

That's what happened to this company: they had over 150 users with 64 unique permission sets spread across eight instances.

55% of user profiles were able to communicate with all other Salesforce APIs, export data, and perform other privileged actions. And the cybersecurity team had no idea.

According to Tony;

> **"We had eight instances of Salesforce—and it was a gaping black hole. I'd heard horror stories about Salesforce permissions and how literally hundreds can be applied in a manner of different ways, but I didn't realize how complicated our permission sets had grown."**

A free Cloud Data Risk Assessment revealed a large number of admin users making frequent changes, including permission changes. It also shed light on what data the company had and who was using it.

> **"I had no idea so many people had so much access. We didn't have a lot of sensitive data in Salesforce, but we needed to get our permissions locked down."**

"Gaining visibility into Salesforce was far more necessary than we had realized because of how little we knew about our Salesforce instances."

SOLUTION

Holistic cross-cloud activities in one pane of glass

Varonis enables the real estate organization to easily manage permissions, monitor for suspicious activity, and secure mission-critical data across different SaaS apps, including Salesforce.

Varonis scans every record and attachment across Salesforce instances to discover, classify, and flag sensitive data. Varonis also provides a complete view of effective access for every Salesforce user.

According to Tony:

> **"I don't think Salesforce inherently has a way of managing all of your instances together. There's no way to gain the 30,000-foot view you need to see where users have too much access and manage all of your permissions."**
>
> **"So we got Varonis for everything, and that helped a lot. Just in terms of holistic permission visibility, it was massive."**

With visibility and control of cross-cloud activities, Tony can:

+ Map and normalize permissions across SaaS apps, including Box and every Salesforce instance.
+ Visualize access permissions by user or cloud app and then safely offboard users to minimize the potential blast radius of an attack.
+ Automatically detect and alert on threats, including unusual access activity and escalating privileges.

Tony and his team finally have complete visibility into **who** is sharing data, **what** they are sharing, **where** data is exposed, and **how** users are sharing data. With Varonis, they're able to answer critical questions about their Salesforce data.

> **"We can easily run reports and see who has super admin rights or admin rights and where they overlap. The cross-cloud visibility is where Varonis comes in extremely handy because trying to do that manually is nearly impossible. It would be a crazy, massive spider web and you would definitely miss something."**

RESULTS

Minimized Salesforce blast radius

The practical benefits of Varonis are already speaking for themselves.

Tony uses these solutions to visualize where users have too much access to Accounts, Contacts, Leads, and Opportunities in Salesforce. This protects his company's critical data from overexposure and potential misuse by internal employees and vendors, as well as from malicious outsider attacks and compromised credentials.

According to Tony:

> **"From a cybersecurity perspective, it is nice to know that we're covered as our use of Salesforce continues to grow and evolve. I'm very confident in that."**

With better visibility and high-fidelity alerts that integrate seamlessly with existing security solutions, the organization has been able to decrease containment and response times.

The company's Salesforce blast radius is also dramatically smaller now that the security team can properly offboard users and proactively prevent excessive access.

> **"If you use Salesforce and you give a damn about security, you need to at least try Varonis. Without it, it's impossible to see all of that data from a holistic perspective in one pane of glass."**

As the company prepares to stand up another Salesforce instance in their environment — an HR instance that will house more sensitive data — Varonis provides peace of mind that their data is protected.

> **"If you have a Salesforce environment, buy Varonis or at least do the POC. Especially if you have multiple instances, it's a no-brainer."**

“From a cybersecurity perspective, it is nice to know that we’re covered as our use of Salesforce continues to grow and evolve.”

Your Data. Our Mission.

Secure your sensitive data in Salesforce and other cloud apps and services.

Request a demo