VARONIS

# How a Healthcare Org Enhances its Salesforce Security Posture With Varonis

> Varonis is definitely helping us improve our security posture in Salesforce. It's great. You can just remediate any posture management issues right in the tool itself.

# HIGHLIGHTS

## Challenges

- Classifying sensitive data, including PII and PHI in Salesforce
- Securing sensitive data, access, configurations and third-party apps
- Visibility into Salesforce environments

## Solution

**Varonis for Salesforce:**

- Provides continous and automatic visibility into who sees what in Salesforce
- Easily integrates with Salesforce Shield Event Monitoring and Setup Audit Trail
- Discovers third-party apps
- Identifies at-risk sensitive data in hard-to-find places
- Alerts you to abnormal or atypical user behavior or unwanted changes

## Results

- Visibility across their Salesforce environments (production, UAT, sandbox)
- Maximized investment in Salesforce Shield
- Reduced entitlements with "view all data" by 87%
- Reduced users without MFA by 96%

# CHALLENGES

## Safeguarding Private Healthcare Data in Salesforce

A leading organization in the healthcare industry was transitioning client data to Salesforce. At the top of their priority list: protecting PHI and PII.

Salesforce has its own roles, permissions sets, and org-wide configs, making it difficult to gain visibility into how users work with information and what they do with it. As third-party apps are added by both IT and users (shadow IT), APIs can provide dangerous on-ramps to sensitive data.

Salesforce Shield provides extensive logs, but actioning that intel requires work. The company's security team tried to integrate other tools into Shield.

Still, they weren't able to determine if their data — including sensitive personal information, contracts, and payment methods — across their sandbox, UAT, and production environments was secure.

Ask any security pro, and they'll tell you it's impossible to manually identify all sensitive data within records and objects, check permissions for every user, and remediate all risky links putting sensitive data at risk.

According to a security engineer at the organization:

> **"I needed a tool I could pick up on relatively quickly. I also needed a tool that would help me prioritize the biggest risk data in our environments."**

# SOLUTION

## Gaining visibility and reducing risk with Varonis for Salesforce

To tackle these challenges head-on, the organization turned to Varonis. According to the security engineer:

> **"We've been a Varonis customer for a long time, mostly using it for data security. Since we are a healthcare company, securing PHI and PII is our biggest priority. We wanted to use Varonis as we moved more data to Salesforce. Our data is the most important thing to us."**

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.

With Varonis, the organization could remediate sharing links and right-size permissions. Most importantly, they would be notified of unusual activities that could put their data at risk — all while working toward a least privilege model.

## Seamless integration with Salesforce

Integrating Varonis with Salesforce and Salesforce Shield was fast and easy, according to the customer:

> **"The integration was relatively quick. We didn't have to massage or change the data in any way. We let Varonis baseline and read the data for about a week. Varonis highlighted the key issues we needed to pinpoint in the environment.**
>
> **The proof of the value of Varonis was immediate. As soon as we saw what was outstanding, we worked on it right away."**

Varonis then enabled the company's security team and Salesforce Admins to systematically identify and remediate exposure risks.

## Remediating public access in record time

Like many SaaS applications, Salesforce makes it easy for users to create sharing links that can expose information. For companies in the healthcare space, these links — especially public links that can expose information to anyone — are a critical risk. The customer explains:

> **"A top concern was public links that could overexpose client PHI or PII to people outside the company. Our highest priority security-wise was to lock off all public-facing external links so there's nothing externally-facing somebody from outside of the company could access, including PHI or PII."**

With Varonis, the security engineer could safeguard data in the company's Salesforce environments in record time. Using Varonis, eliminating security gaps and remediating data at risk was a breeze.

> **"We locked down anything that was externally facing and had sensitive data right away. We also have a dashboard view that shows any link that's externally-facing, whether it has sensitive data or not."**

**"With Varonis, we can actually see where data is and classify it. Varonis will show if you have a public link with PHI, so you know it's more urgent."**

## Right-sizing permissions and enforcing MFA

Next, the organization pivoted toward access reviews. They used Varonis to understand who had what permission levels to begin right-sizing that access.

Varonis also enabled the company to easily enforce MFA — a best practice that sounds simple in theory but can be challenging to enforce. The customer explains:

> **"After we locked down PHI and PII, the next step for us was to enforce an MFA policy. It's one of the most beneficial protective measures security-wise. We enforce MFA to make sure everybody's going through SSO."**

## Alerting to unusual behavior

Varonis ingests Salesforce Shield events and enriches them with unique metadata to supercharge threat detection and investigation. Security teams don't waste hours parsing logs, running Apex codes, or getting bogged down chasing false positives.

The combination of Varonis and Salesforce Shield helps keep data safe from insider threats and cyberattacks. With Varonis, the security engineer and the team are notified of any suspicious activities and configuration changes for further investigation. If a user is promoted to super admin or assets are deleted, the team can take immediate action.

According to the security engineer:

> **"Companies get breached. You need to lock that data down. Being able to view all of our data with Varonis has been very helpful."**

# RESULTS

## Achieving a robust Salesforce security posture with Varonis

Varonis helps businesses understand their Salesforce data security posture in real time, ensure only the right people have access to crown-jewel data, automatically remediate misconfigurations, and detect suspicious activity.

Integrating Varonis into Salesforce enabled the healthcare organization to gain visibility into data risks and make their way to a least-privilege model.

> **"Varonis is definitely helping us improve our security posture. At this point, I only see the posture management things that are medium risk. There's almost nothing left I need to work on posture-wise."**

When Varonis identifies a problem, the security engineer appreciates how easy it is to take action.

> **"It's great. You can just remediate any posture management issues right in the Varonis solution."**

## Eliminating risk with tangible results

Varonis for Salesforce yielded tangible results for the healthcare org, significantly enhancing its data security posture and reducing its exposure risk. When these steps were complete, the team focused on boosting its overall Salesforce security posture.

Within weeks, Varonis reduced the company's Salesforce entitlements with "view all data" permissions by 87%. Varonis also reduced users without MFA enabled by 96%.

According to the security engineer, the difference between the other tools they were using and Varonis was night and day:

> **"Using Varonis is painless. It gives us all the reporting that the technical teams need to go and remediate. Everything is right there on the dashboard. "**

## Reducing the Salesforce blast radius

And because security is never one-and-done, Varonis ensures the healthcare organization can keep that risk down and close security gaps over time. Varonis helps the customer see and reduce their blast radius — all the potential information that could be exposed during a security event.

> **"Varonis has helped us reduce our blast radius. We've locked down our environment since we got it, and we're seeing a lot of value."**

According to the security engineer, the collaboration between Varonis and Salesforce has set a new standard for data security, providing peace of mind for the company and its clients.

> **"When I talk to my CSO or someone in upper management, I'm confident in the information that I'm providing them. It puts my mind at ease, and I can also convey that confidence because of how well we're integrating with Varonis and the visibility it has."**

It's one thing to have a great solution, but another to know you have a partner behind you every step of the way. According to the customer:

> **"It's just been a pleasure working with the Varonis team. They have great communication skills. They're ready to help at any moment. They're a client-facing team that's very energized and willing to work with you."**

# Improve your Salesforce security posture.

Varonis eliminates risky misconfigurations, finds and remediates exposed sensitive data, and detects anomalous behavior in Salesforce.

Request a demo