VARONIS

Salesforce for Security Pros

Risk assessment and action plan

Introduction

Salesforce is a powerful CRM tool used by organizations around the world, but the massive amount of critical data it houses, the sophisticated and complex permission models, and the dozens of security settings can be a headache for security and compliance teams. Often, those teams have little visibility into whether sensitive and regulated data is present in Salesforce, protected, and used correctly. And in many cases, Salesforce teams are more focused on availability and delivering new features than implementing tighter controls.

Several security, administrative, and reporting functions are manual and complex for Salesforce administrators as well; admins spend valuable time verifying and attesting to the security of the system and access levels of their users.

Varonis' complimentary Data Risk Assessment reveals issues and configurations that unnecessarily open organizations to risk, such as:

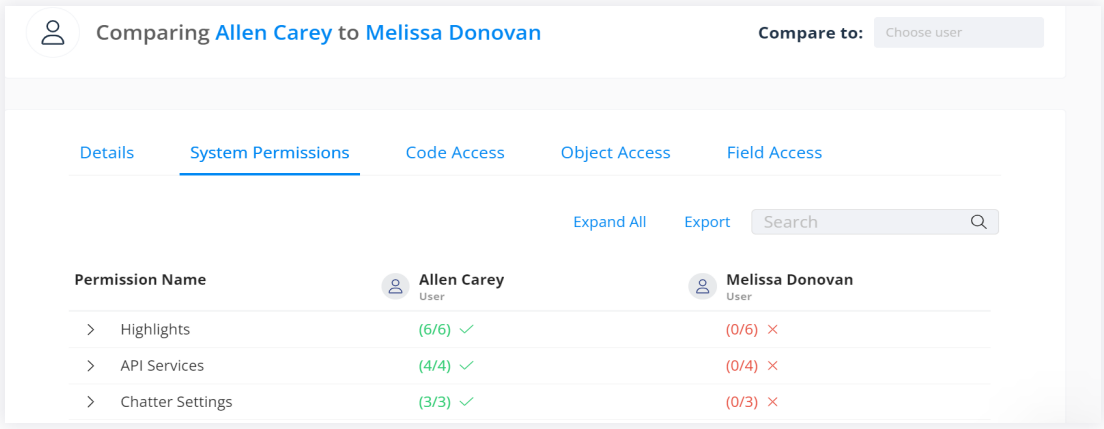


Figure 1. Many users essentially have admin-level privileges they don't need.

- Guest access to information meant for internal users
- External users with excessive privileges to access and export data
- A high proportion of administrative or admin-like credentials
- Stale and risky third-party applications installed
- Unprotected instances of Salesforce with copies of production data (e.g., dev and UAT)
- Unexpected concentrations of sensitive data, some of which are at risk due to excessive sharing settings or rule

Varonis can quickly lock down and monitor these settings and configurations. Similarly, Varonis can alert if sensitive data is placed in areas that are high risk. Regardless of remediation, Varonis will baseline normal behavior for every user on all Salesforce data and alert you should activity indicate the likely presence of an internal or external threat.

These outcomes can be achieved with almost no effort on the part of the security or Salesforce teams — Varonis will take Salesforce administrators directly to the offending setting or entitlement, and configuration and behavioral alerts are fully automated.

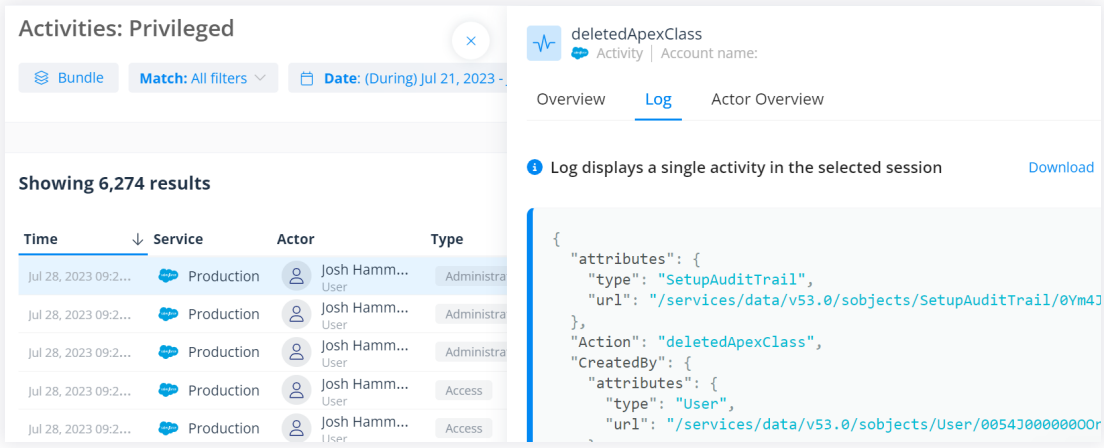


Figure 2. Monitor and detect unwanted changes and suspicious data access.

With the Varonis SaaS Data Security Platform, compliance teams can attest to the security posture controls in place on regulated Salesforce data. Security teams will gain visibility over the preventive and detective controls in Salesforce to help ensure sensitive data is secure, and alert on potential data abuse or unwanted changes.

Administrators will benefit from reduced reporting workloads, easy Profile and Permission Set comparison functionality, and increased visibility into configuration and identity concerns. They'll also be in far better shape to address Salesforce's upcoming permissions model changes that will deprecate the use of user profiles for system and object permissions.

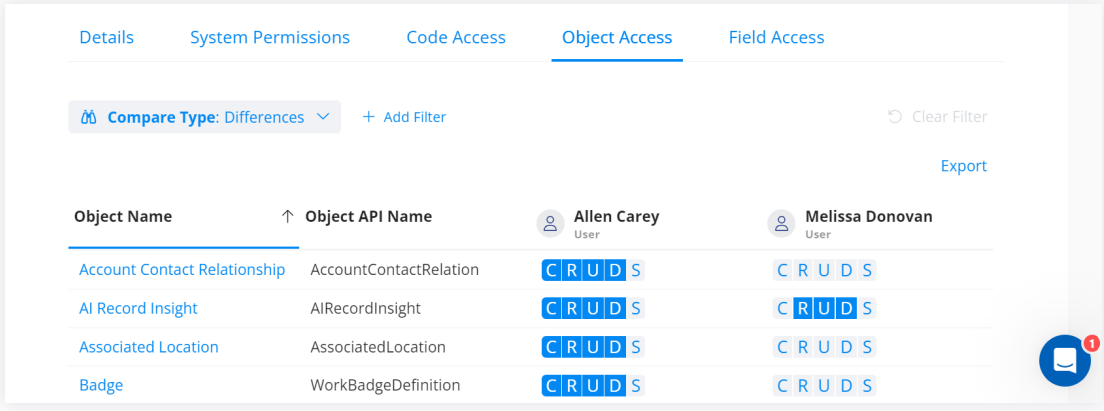
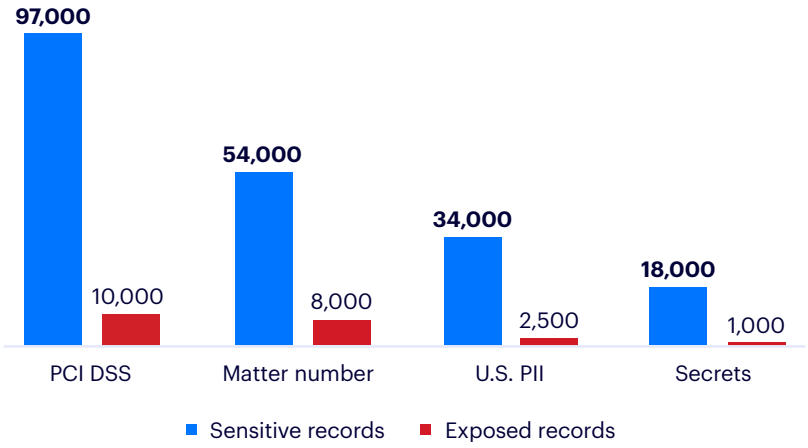


Figure 3. Compare effective Permissions, Profiles, and Permission Sets

Varonis Salesforce risk assessment process

Varonis connects to each Salesforce instance within minutes. Once configured, Varonis interrogates configurations, identities, third-party applications, and permissions, collects access activity with or without Salesforce Shield event-monitoring. The security platform then begins to classify data and generate behavioral baselines. Depending on the scope, initial data collection usually finishes within days, and most assessments conclude with a review three weeks after the initial configuration.

Salesforce data exposure



1.5K Sensitive records exposed externally

20K Sensitive records exposed org-wide

Salesforce risk assessment

Export reports
Allows users to export data directly out of Salesforce. If necessary, should be applied to Permission Sets.

View and modify all data
Users with this permission can view and modify all data inside the organization.

API enabled
Allows users to communicate with all Salesforce APIs, exfiltrate data, or perform other actions.

89 Entitlements with “view all data” enabled

59 Entitlements with “export risk report” enabled

29 Permission Sets with “API enabled” access

73 Profiles with “modify all data” enabled

VARONIS

Sample report and response plan

Inventory

- 1,300 Salesforce identities
- 2.6M resources (fields, records, objects)
- 220K sensitive records across fields and attachments, including PII, PHI, and clear-text credentials

Top risks

- Risky configurations
  - Admins can log in as any user
  - "View all data" and "export report" permission granted to external user
  - "Export reports" permission granted to three-fourths of all Salesforce users
  - Excessive access to sensitive data, including PHI
- 12 stale applications installed by users with admin-like access
- Access to data in Salesforce was unmonitored

Immediate action plan

- Monitor all user access with a Varonis audit trail.
- Monitor and/or revoke external user access (view all data, export, etc.).
- Review list of administrators and users that have "export/modify all" data permissions.
- Leave Varonis monitoring in place.
- Review and revoke unneeded third-party applications.
- Connect Varonis Proactive Incident Response with security operations.

Sample report and response plan (continued)

Ongoing action plan (120 days)

- Schedule quarterly calls with Varonis alerting, classification, and remediation ops.
- Review severity one threat models.
- Refine and extend classification rules.
- Triage overly accessible sensitive data.
- Work with the Salesforce admin team to automate the transition away from Profiles and redundant entitlements.
- Recertify permissions like “modify all data,” “manage Profile and Permissions Set,” and “admin.”

Key success metrics

- Configuration risks addressed: four Salesforce configs optimized
- Adherence to policy: one unscheduled change
- Access remediation: eight fewer users with administrative privileges (50% reduction); 15 redundant profiles removed
- Exposure detection: 100 exposed sensitive records (75% reduction)
- Usage exceptions: two incidents

Conclusion

As Salesforce continues to grow as a collaborative hub for key business data, keeping the CRM tool compliant and secure is crucial for organizations. As more functionality is integrated and more features are added, customers will inherit more responsibility for keeping configurations, access controls, and workflows secure. A Varonis Data Risk Assessment provides immediate visibility into your Salesforce security posture with respect to how data is stored, shared, and secured.
The complimentary report also gives you insight on how to achieve quick wins in risk reduction and how to take advantage of high-fidelity detective controls, ensuring correct use and processes.

Ready to experience the Varonis difference?

Reduce your risk without taking any. Contact our team to learn what will be covered in your **free** Data Risk Assessment.

Contact us

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data: sensitive files and emails; confidential customer, patient, and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects cyber threats from both internal and external actors by analyzing data, account activity, and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation.

Varonis products address additional important use cases including data protection, data governance, Zero Trust, compliance, data privacy, classification, and threat detection and response. Varonis started operations in 2005 and has customers spanning leading firms in the financial services, public, health-care, industrial, insurance, technology, consumer and retail, energy and utilities, construction and engineering, and education sectors.