Staying Ahead of Recent Salesforce Social Engineering Attacks

Background

Recent high-profile incidents, including the ShinyHunters-led theft of sensitive data from Salesforce environments at major organizations [1, 2] , highlight a growing and sophisticated threat: social engineering combined with misuse of connected applications. In these attacks, a threat actor convinces a targeted user to access Salesforce's Connect setup page and enter a "connection code," thereby linking the attacker-controlled Data Loader to the victim's Salesforce environment. Once connected, this access can enable large-scale exfiltration of sensitive data without triggering traditional perimeter-based alerts. While Salesforce recommends [3] measures such as enforcing trusted IP ranges, enabling MFA, restricting connected apps, and leveraging Salesforce Shield, these threats underscore that misconfiguration, excessive permissions, and lack of continuous monitoring remain significant risk factors. This is where Reco's Dynamic SaaS Security capabilities provide added layers of protection, detecting posture drift, monitoring connected apps and risky API usage, and identifying anomalies before they escalate into breaches.

1 Enforcing Trusted IP Ranges for Logins

Salesforce Control

- Restrict login attempts to trusted IP ranges.

Reco Control

- Salesforce - IP Range Enforcement Enabled for Every Request (Posture)

How Reco Helps

- Detects when IP range enforcement is missing or weakened. Ensures every request is validated against trusted ranges to block unauthorized network access.

2 Principle of Least Privilege for App Permissions (PoLP)

Salesforce Controls

- Multiple checks ensuring minimal permissions are granted to users and integrations.

Reco Controls

Risk Area	Reco Posture Check	Description
Excessive app scopes	Salesforce - OAuth Connected Apps Use Least Privilege Scopes	Flags apps requesting more access than needed.
MFA bypass	Salesforce - No Users With Bypass MFA Permission	Identifies users who can log in without MFA.
PII exposure	Salesforce - More than 15 users have permission to view (PII) data	Tracks exposure of personal data to too many users.
Bulk deletions	Salesforce - Max 15 Users With Bulk API Hard Delete Permission	Limits destructive mass operations.
Account deletions	Salesforce - More than 5 users have permission to delete accounts	Controls customer data loss risk.
Data export	Salesforce - Max 15 Users with Weekly Data Export Permission	Reduces chances of full data dumps.
Manage dataspace	Salesforce - Max 15 Users with Manage Dataspace Scope Permission	Restricts changes to data segmentation.
Data Cloud profile	Salesforce - Max 15 Users with Data Cloud Profile Explorer Permission	Limits data browsing by non-essential users.
Modify all data	Salesforce - Maximum 10 Users Have Modify All Data Permission	Prevents overuse of highest privilege.
API access	Salesforce - Users With API Access Permissions	Restricts external API integrations to approved accounts.

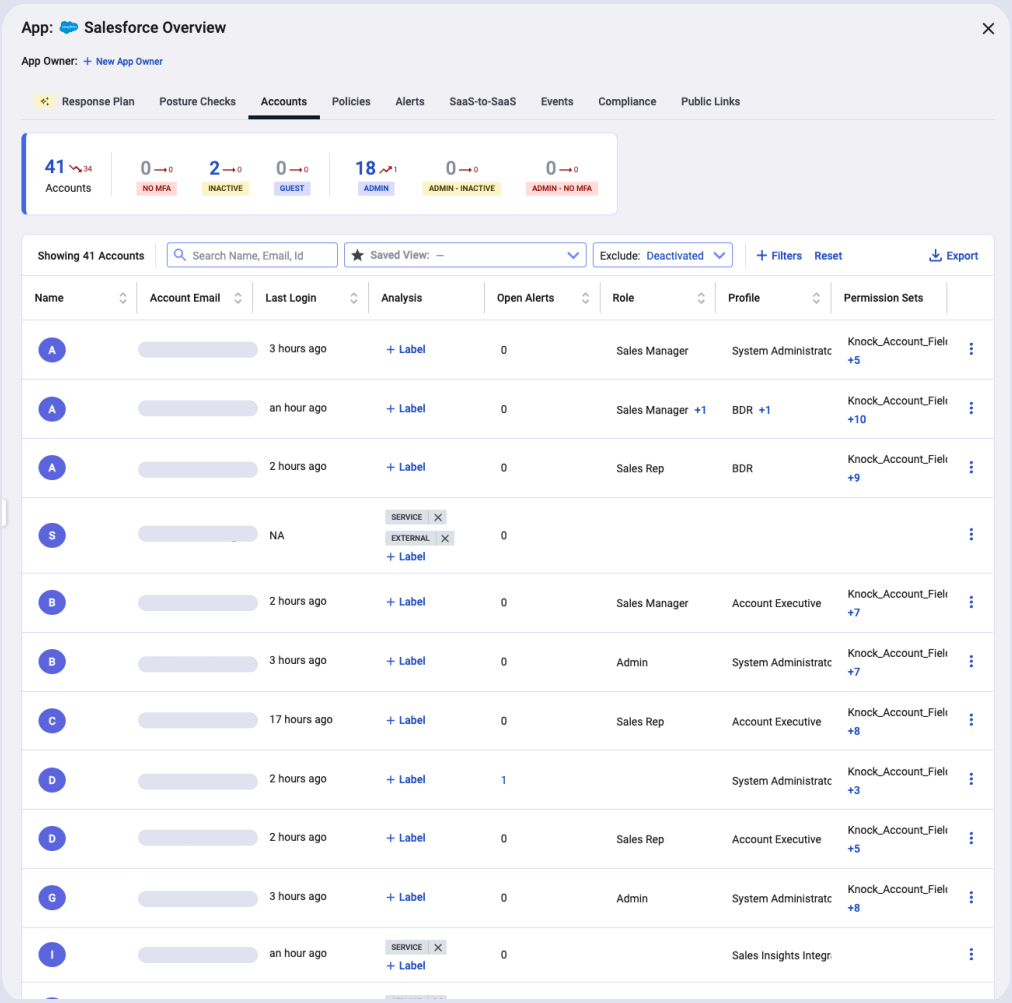
3 Enabling Multi-Factor Authentication (MFA)

Salesforce Controls

- Enforce MFA for all accounts.

Reco Controls

- Posture Check - Salesforce - Users without MFA - Flags non-compliant users for remediation.
- Identities Dashboard - Identities without MFA in Salesforce dashboard - Visualizes accounts lacking MFA.



4 Restricting Use of Connected Apps and Managing Access Policies

Salesforce Controls

- Ensure connected apps are secure and API access is restricted.

Reco Controls

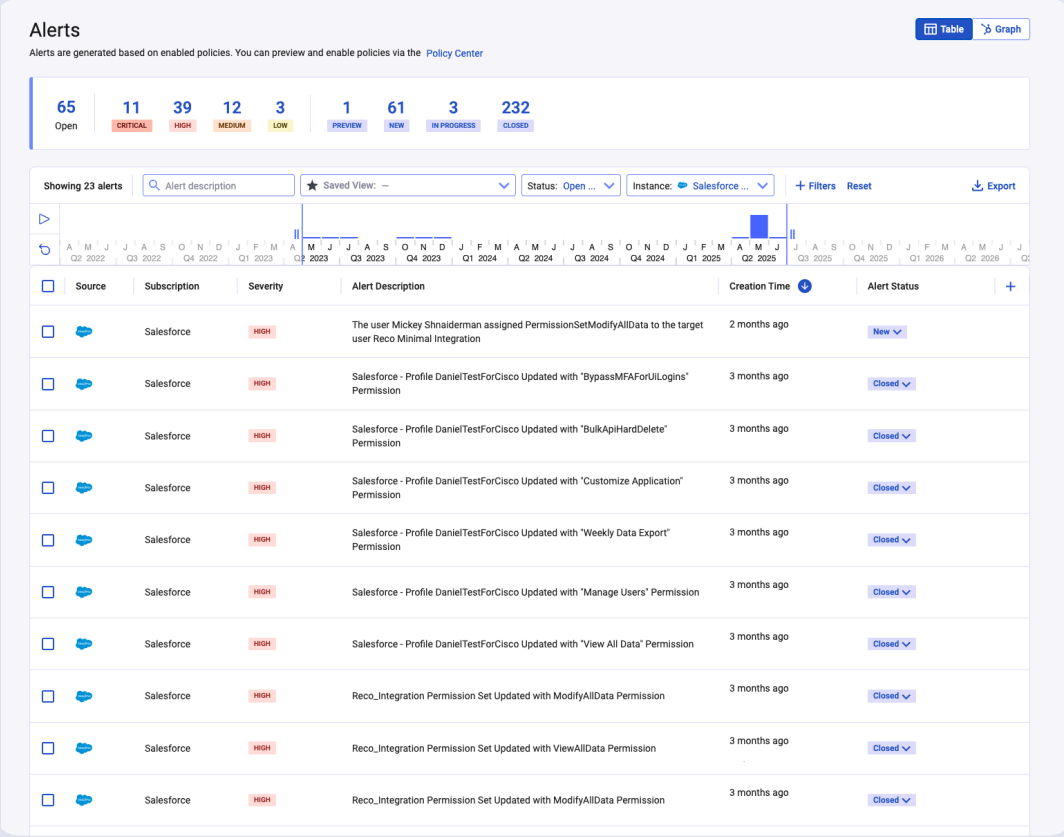
- Posture Check - Salesforce - Connected Applications Securely Configured - Detects insecure settings in connected apps.
- Posture Check - Salesforce - API Access Restricted to Admin-Approved Connected Apps - Ensures only vetted apps connect.
- Posture Check - Salesforce - Connected Apps Use API-Only Integration Users - Prevents apps from using full human accounts.
- **SaaS-to-SaaS applications dashboard** - Lists and risk-ranks all connected third-party apps.

5 Using Salesforce Shield for Threat Detection and Event Monitoring

Salesforce Controls

- Monitor events, enforce policies, and detect suspicious activity.

Reco Controls



Former Employee & Risky Account Monitoring

- Reco - Former Employees with Active Access to Salesforce (Advanced Analytics Policy) - Detects active accounts of terminated users.
- Salesforce - Former Org User Successfully Logged In (Policy) - Real-time alert on logins from former employees.
- Salesforce - Inactive User Successfully Logged In / Salesforce - Inactive External User Successfully Logged In - Flags dormant accounts suddenly used.

Anomalous & Malicious Activity Detection

- Salesforce - API Anomaly Event - Spots abnormal API usage patterns.
- Salesforce - Mass File Activity in Salesforce - Detects bulk file operations.
- Salesforce - Excessive Report Export Activity - Alerts on unusual data report downloads.

- Salesforce - Risky / Leaving Employee Excessive Download - Targets insider data theft scenarios.
- Salesforce - Potentially Customer Emails Exported by Leaving/Risky User - High-risk communication data leakage.

Privilege Escalation & Misconfiguration Changes

Detects assignment or update of high-privilege permissions:

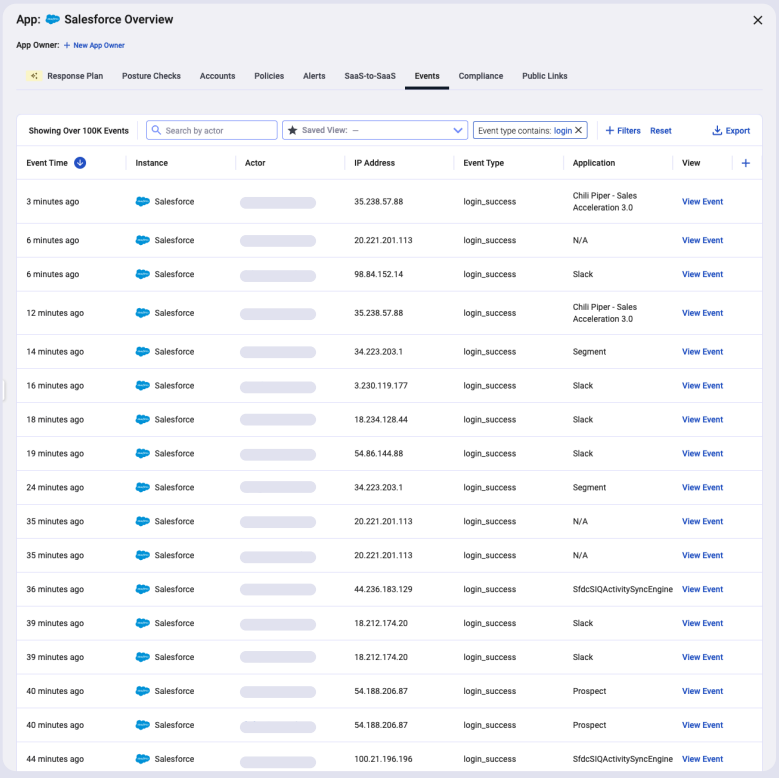
- ModifyAllData
- ViewAllData
- CustomizeApplication
- ManageUsers
- BulkApiHardDelete
- DataExport
- BypassMFAForUiLogins
- AuthorApex
- Read Logs/Events

Example policies

Salesforce - Permission Set Updated with "ModifyAllData" Permission, Salesforce - Profile Updated with "CustomizeApplication" Permission.

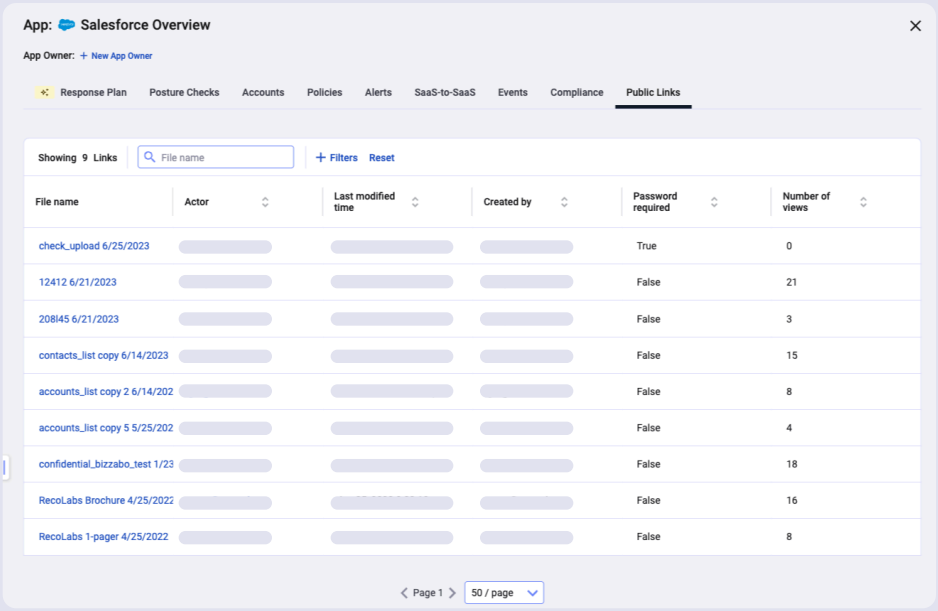
Session & Login Risks

- Salesforce - Session Hijacking Event - Identifies potential account takeover.
- Salesforce - Multiple Failed Logins by Same User - Brute force detection.
- Salesforce - Successful 3rd Party App Login to Salesforce with Stale User Credentials - Detects outdated credential usage.
- Salesforce - Successful 3rd Party App Login to Salesforce with Stale Admin Credentials - Admin credential risk detection.
- Salesforce - Attempted 3rd Party App Login to Salesforce with Inactive User Credentials - Flags blocked, but suspicious, access attempts.
- Salesforce - User Successfully Logged In without SSO - Detects MFA/SSO bypass.
- **Salesforce - Events Dashboard**



Data Exposure Prevention

- Salesforce - File Shared Publicly Without Password
- Salesforce - File Shared Publicly Without Expiry Date
- Both prevent uncontrolled external data exposure.
- Salesforce - Public Links dashboard



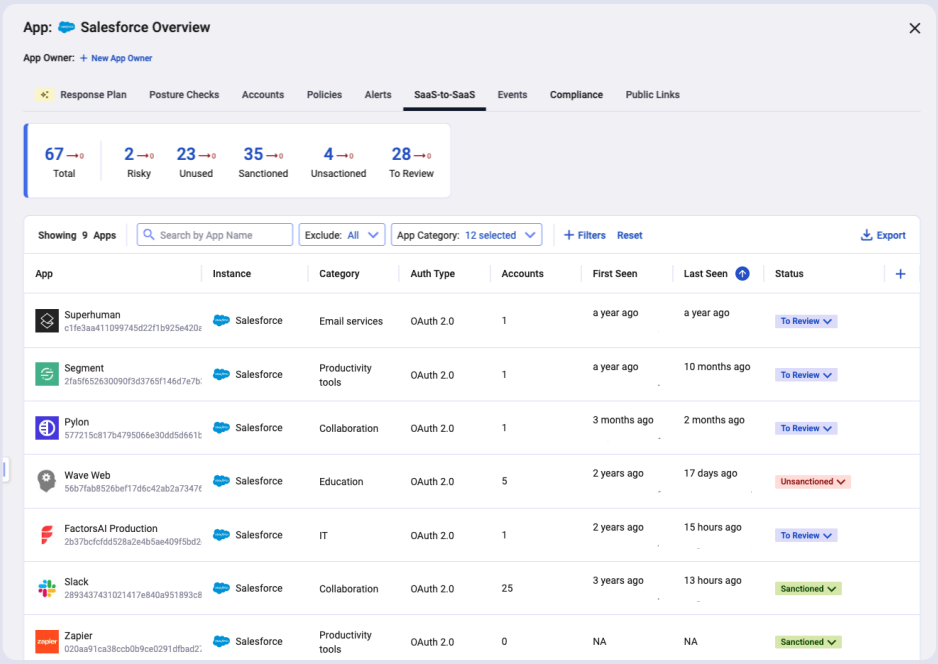
6 SaaS-to-SaaS Risk Visibility

Salesforce Controls

Monitor and secure third-party integrations.

Reco Controls

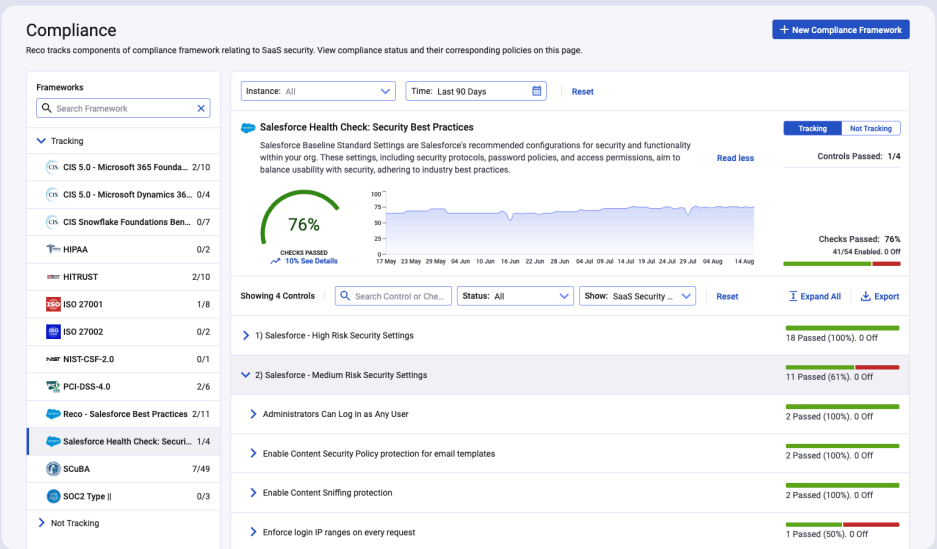
- SaaS-to-SaaS risky permissions dashboard - Shows integrations requesting excessive scopes.
- SaaS-to-SaaS applications dashboard - Comprehensive inventory of all integrated apps, including those bypassing security review.



7 Compliance

Reco Controls

- Salesforce Health Check: Security Best Practices [4]
- Reco - Salesforce Best Practices [5]



Summary & Next Actions

The Salesforce data theft campaign is a stark reminder that attackers increasingly exploit identity trust, connected app permissions, and misconfigurations, not just network vulnerabilities. With Reco, organizations can go beyond Salesforce's native controls to ensure:

- Continuous verification that security posture aligns with best practices (e.g., MFA enforcement, least-privilege permissions, IP range restrictions)
- Real-time detection of risky connected app activity, anomalous API calls, and privilege escalations
- Immediate alerting and remediation for suspicious logins, excessive data exports, or configuration changes
- Comprehensive visibility into SaaS-to-SaaS integrations and the identities involved

We recommend reviewing your current Salesforce posture in Reco, enabling all relevant detection policies, and scheduling ongoing posture drift reviews. Our team is here to help you make the most of Reco's capabilities, from ensuring the right controls are in place to providing guidance on maximizing detection and protection against connected app abuse scenarios.

Schedule a Demo