veza | Security you can see

Veza for Salesforce **Solution Brief**

Veza for Salesforce

Maintain least privilege and achieve continuous compliance for PII data

Salesforce has grown from a sales and marketing tool to a mission-critical application that stores enterprises' most sensitive business and customer data, including PII, customer lists, and financial data. Managing enterprise access and monitoring privileged user permissions on sensitive data becomes increasingly challenging as organizations customize their Salesforce environment to suit the needs of their business. Access control in Salesforce gets increasingly complicated due to the sprawling nature of relationships across users, groups, roles, profiles, permissions sets, and record-level sharing. Left unchecked, this complexity increases the risk of excess permissions, leading to insider threats and data loss when accounts are phished or otherwise compromised. To minimize this risk, organizations require visibility to, and governance of, access in Salesforce.

Veza secures access to customer data in Salesforce

Visualize

Enable identity, security, and IT compliance/risk teams to understand the full scope of access permissions for all users and roles in Salesforce.

Remediate

Secure sensitive data and demonstrate regulatory compliance with automated workflows for user access reviews and entitlement certifications. Reject access requests and manage temporary permissions all in one control plane.

Control

Enforce least privilege by monitoring for excess permissions that enable users to access sensitive account and customer data and do not comply with organizational security standards.

Challenges

- Identifying users with elevated permissions and understanding the extent of their access
- Managing access for contractors and temporary employees
- Verifying that offboarding procedures are working as intended across IdP (identity providers) accounts and users created locally in Salesforce
- Monitoring access to personally identifiable information (PII) and demonstrating compliance with policies specific to securing customer data for PCI DSS, GDPR, CCPA, etc.
- “Security theater” - rubber stamping of entitlement certifications

Benefits

- ★ **Reduce the risk of insider threats**
- ★ **Save time and reduce effort for governance teams with 90% faster access reviews and certifications**
- ★ **Pass audits by correcting excessive permissions**

© 2023 Veza, Inc. All Rights Reserved

RBAC Entities Supported

- Organizations
- Accounts
- Users
- Roles
- Groups
- Account Shares
- Profiles
- Permission Sets

> *Veza is looking forward for us. It allows us to understand who, what, where, when, and why. If you can do that, you have the ability to secure any environment. And when you're talking about a global organization, that's what you need.*

David Tyburski
VP of Information Security and CISO

Who uses Veza for Salesforce

IAM teams

- ✓ Monitor that offboarding works as intended by checking for orphaned local accounts in Salesforce
- ✓ View all accounts from Okta, Azure AD and other SAML providers that have not enrolled in MFA
- ✓ Manage local access in Salesforce by visualizing which privileged users can bypass IT policies and/or share their account
- ✓ Identify privileged access violations like tracking the number of admins or users assigned to a senior executive role

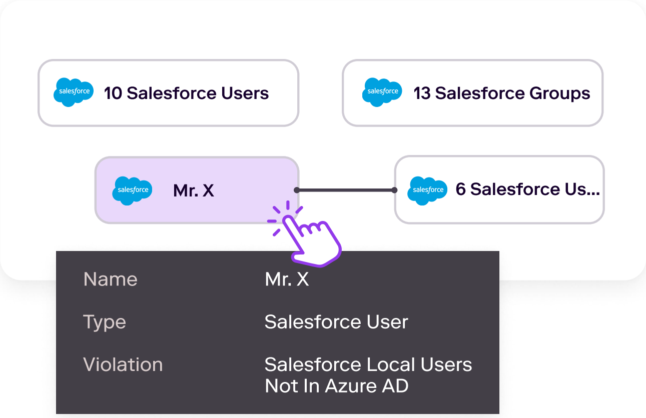
Security Operations (SecOps) Teams

- ✓ Pinpoint unused permissions to remove without business process or user experience impact
- ✓ Perform RCA by analyzing historical access and "blast radius "trends for any compromised account involved in a breach

IT Compliance (GRC) and Audit Teams

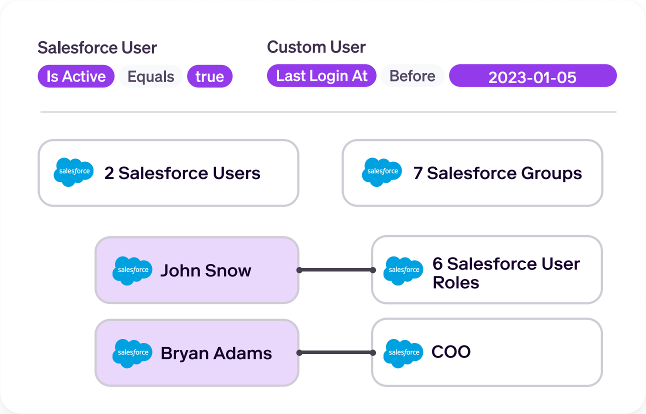
- ✓ Conduct automated access reviews to meet compliance requirements (PCI DSS, GDPR, SOC, ISO 27001, etc.)
- ✓ Demonstrate that PII data in Salesforce is limited to appropriate geographies
- ✓ Empower managers to decide access with rich context of true effective permissions

"Show me Salesforce local users not in my IdP"



Name	Mr. X
Type	Salesforce User
Violation	Salesforce Local Users Not In Azure AD

"Show me Salesforce users inactive for 90 days"


Salesforce User: Is Active Equals true

Custom User: Last Login At Before 2023-01-05