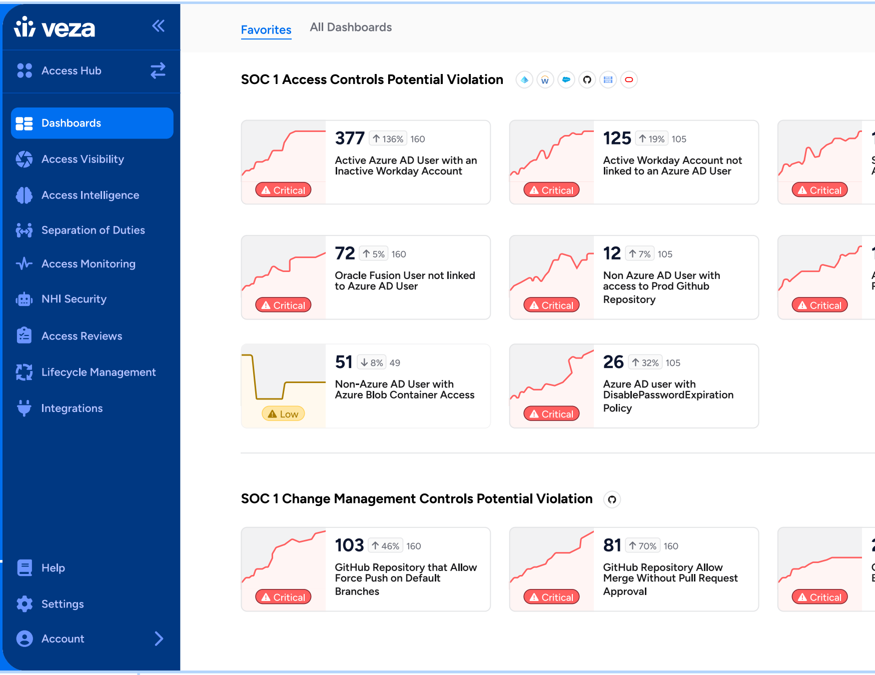
veza

Solution Brief

Identity Security Posture Management (ISPM)

Detect privileged users, dormant permissions, policy violations, and misconfigurations with Veza's 2,000+ pre-built queries. Veza shows you where to focus for maximum impact and automates remediation to resolve issues efficiently at scale.



veza

Access Hub

Dashboards

Access Visibility

Access Intelligence

Separation of Duties

Access Monitoring

NHI Security

Access Reviews

Lifecycle Management

Integrations

Help

Settings

Account

Favorites | All Dashboards

SOC 1 Access Controls Potential Violation

377 ↑ 136% 160 — Active Azure AD User with an Inactive Workday Account — Critical

125 ↑ 19% 105 — Active Workday Account not linked to an Azure AD User — Critical

72 ↑ 5% 160 — Oracle Fusion User not linked to Azure AD User — Critical

12 ↑ 7% 105 — Non Azure AD User with access to Prod Github Repository — Critical

51 ↓ 8% 49 — Non-Azure AD User with Azure Blob Container Access — Low

26 ↑ 32% 105 — Azure AD user with DisablePasswordExpiration Policy — Critical

SOC 1 Change Management Controls Potential Violation

103 ↑ 46% 160 — GitHub Repository that Allow Force Push on Default Branches — Critical

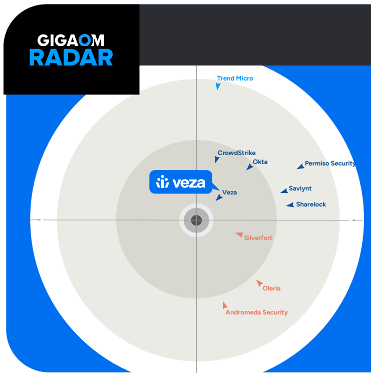
81 ↑ 70% 160 — GitHub Repository Allow Merge Without Pull Request Approval — Critical

Why ISPM? Why Now?

ISPM—Identity Security Posture Management—helps organizations continuously understand, score, and reduce identity risk, rather than react to it after an incident.

The identity perimeter has overtaken the network perimeter as the primary security boundary. Yet most organizations still rely on fragmented IAM tools that were never built for real-time visibility or non-human identity sprawl.

"For CXOs, ISPM represents a strategic investment in proactive security to reduce risk, provide measurable results, and support zero trust and regulatory initiatives."



veza

Veza is named a Leader in GigaOM Radar Report for ISPM

Get the Report

What Is ISPM?

- Unifies visibility across all identities and entitlements
- Scores identity risk posture continuously in real time
- Automates policy enforcement to remove unnecessary access
- Supports human and non-human identities across the enterprise

© 2025 Veza, Inc. All Rights Reserved | veza.com

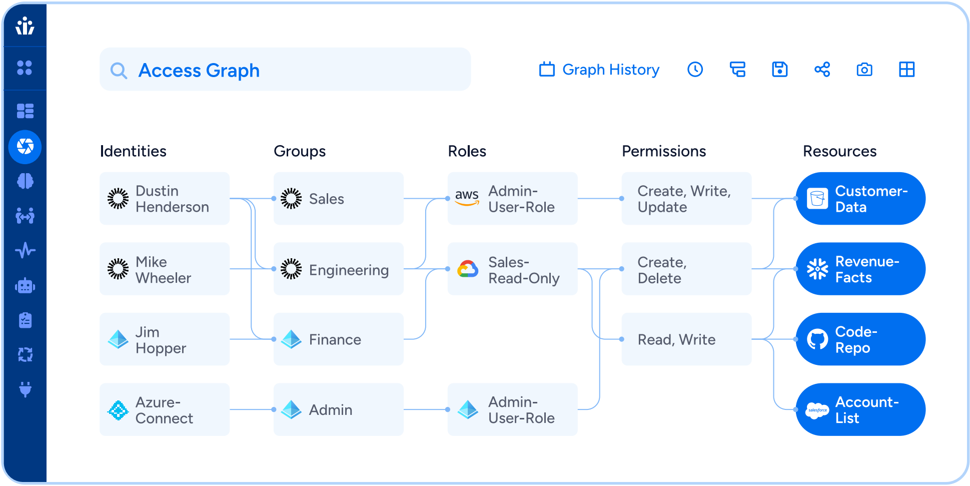
How Veza Helps You Adopt ISPM

Veza enables security, identity, and compliance teams to implement the ISPM framework without re-architecting their stack. Our platform connects to your existing identity systems and continuously delivers visibility, context, and control.

Establish Unified Identity Visibility

ISPM Requirement:
Aggregate identity and access data across all systems.

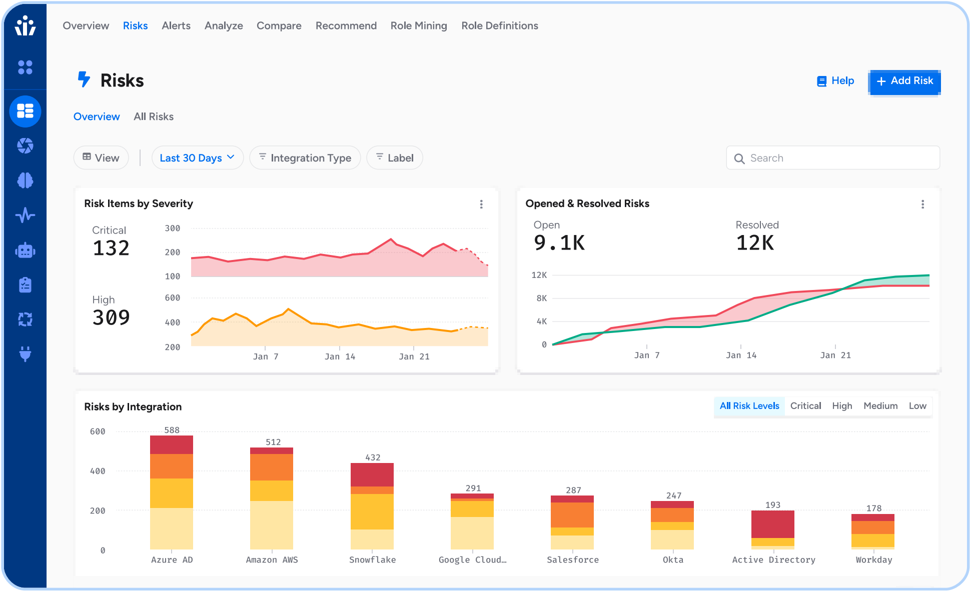
Veza's Access Graph provides real-time visibility into every identity and what it can access across Active Directory, Okta, AWS IAM, GitHub, service accounts, and more. It connects the dots between user roles, permissions, and actual entitlements.



Continuously Score Identity Risk

ISPM Requirement:
Measure the security posture of identities, not just their existence.

Our risk engine continuously monitors changes in access and evaluates posture in real time. You'll immediately spot dormant accounts, toxic permission combinations, or deviations from policy.

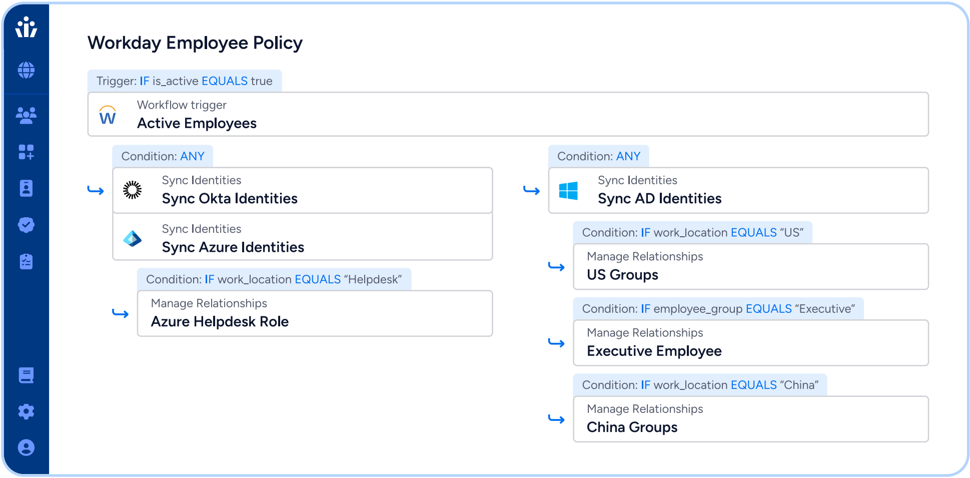


© 2025 Veza, Inc. All Rights Reserved |

Automate Enforcement and Remediation

ISPM Requirement: Use policy-based controls to reduce over-permissioning.

Veza's Lifecycle Management lets you automate identity reviews and enforce least privilege across both users and systems. It integrates with your IAM stack to close gaps faster, with full audit traceability.



Workday Employee Policy

Trigger: IF is_active EQUALS true

Workflow trigger
Active Employees

Condition: ANY

Sync Identities
Sync Okta Identities

Sync Identities
Sync Azure Identities

Condition: IF work_location EQUALS "Helpdesk"

Manage Relationships
Azure Helpdesk Role

Condition: ANY

Sync Identities
Sync AD Identities

Condition: IF work_location EQUALS "US"

Manage Relationships
US Groups

Condition: IF employee_group EQUALS "Executive"

Manage Relationships
Executive Employee

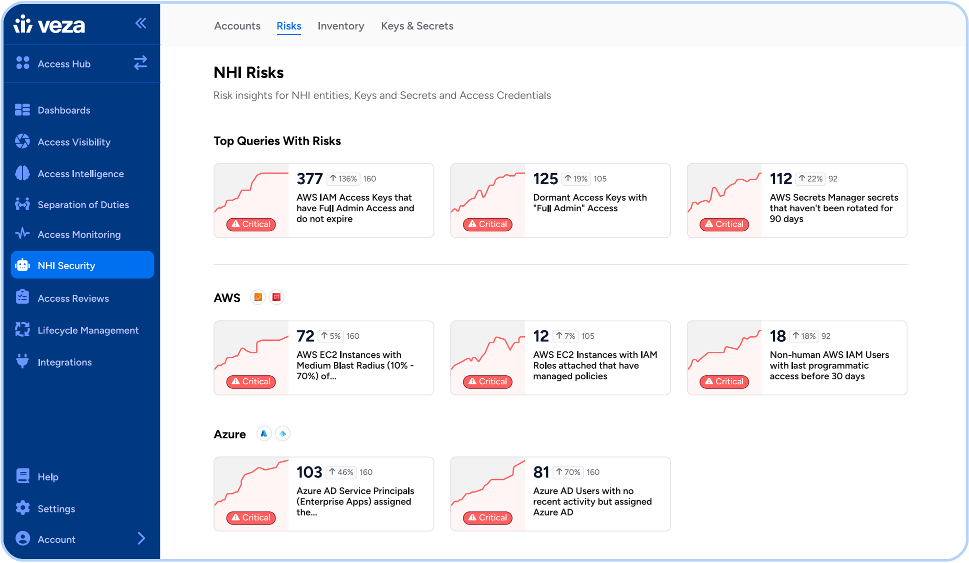
Condition: IF work_location EQUALS "China"

Manage Relationships
China Groups

Secure Non-Human and AI Identities

ISPM Requirement: Include service accounts, bots, and machine identities in your posture strategy.

Our platform identifies and governs non-human identities—API keys, AI agents, and service accounts. It ties them back to real entitlements, detects unused or risky access, and supports AI governance.



NHI Risks

Risk insights for NHI entities, Keys and Secrets and Access Credentials

Top Queries With Risks

377 ↑ 136% 160 AWS IAM Access Keys that have Full Admin Access and do not expire — Critical

125 ↑ 19% 105 Dormant Access Keys with "Full Admin" Access — Critical

112 ↑ 22% 92 AWS Secrets Manager secrets that haven't been rotated for 90 days — Critical

AWS

72 ↑ 5% 160 AWS EC2 Instances with Medium Blast Radius (10% - 70%) of... — Critical

12 ↑ 7% 105 AWS EC2 Instances with IAM Roles attached that have managed policies — Critical

18 ↑ 18% 92 Non-human AWS IAM Users with last programmatic access before 30 days — Critical

Azure

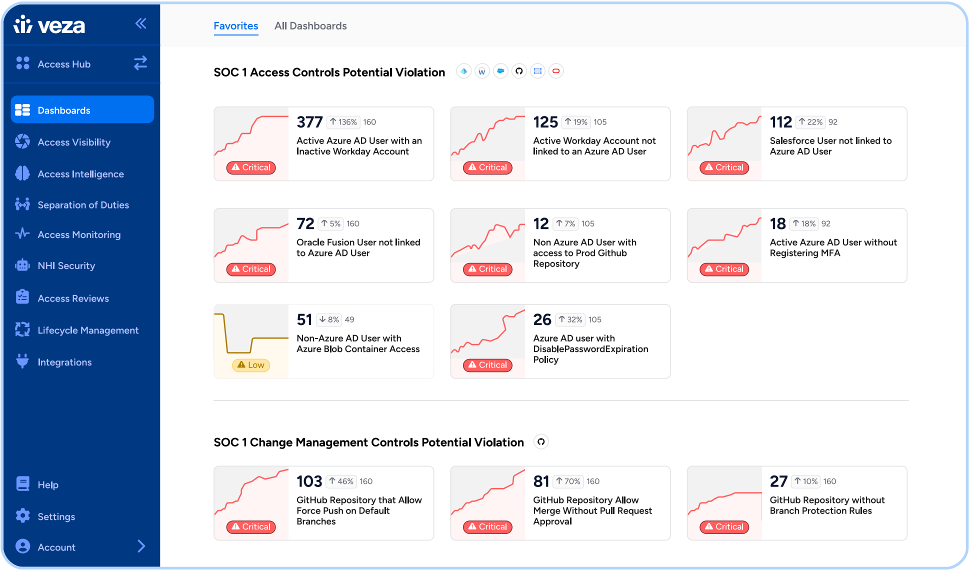
103 ↑ 46% 160 Azure AD Service Principals (Enterprise Apps) assigned the... — Critical

81 ↑ 70% 160 Azure AD Users with no recent activity but assigned Azure AD — Critical

Align with Audit and Governance Objectives

ISPM Requirement: Provide evidence of access control for internal and external audits.

Veza gives you point-in-time and real-time access snapshots. From SOX to HIPAA, ISO 27001, or internal GRC programs, Veza ensures you're audit-ready at all times.



SOC 1 Access Controls Potential Violation

377 ↑ 136% 160 Active Azure AD User with an Inactive Workday Account — Critical

125 ↑ 19% 105 Active Workday Account not linked to an Azure AD User — Critical

112 ↑ 22% 92 Salesforce User not linked to Azure AD User — Critical

72 ↑ 5% 160 Oracle Fusion User not linked to Azure AD User — Critical

12 ↑ 7% 105 Non Azure AD User with access to Prod Github Repository — Critical

18 ↑ 18% 92 Active Azure AD User without Registering MFA — Critical

51 ↓ 8% 49 Non-Azure AD User with Azure Blob Container Access — Low

26 ↑ 32% 105 Azure AD user with DisablePasswordExpiration Policy — Critical

SOC 1 Change Management Controls Potential Violation

103 ↑ 46% 160 GitHub Repository that Allow Force Push on Default Branches — Critical

81 ↑ 70% 160 GitHub Repository Allow Merge Without Pull Request Approval — Critical

27 ↑ 10% 160 GitHub Repository without Branch Protection Rules — Critical

Customer Results

Teams that adopt ISPM with Veza see measurable improvements in weeks:

☑ Cut access review time by 90%

☑ Surface overprivileged accounts across all systems

☑ Close identity gaps ahead of audits

☑ Reduce machine identity risk

☑ Accelerate Zero Trust and AI governance initiatives

veza® + sallie mae®

Sallie Mae used the power of Veza's Access Graph to achieve a 96% reduction in dormant non-human identities, and streamline regulatory compliance as they transition to a fully cloud-based organization.

Watch the video

About Veza

Veza is the identity security company. Identity and security teams use Veza to secure identity access across SaaS apps, on-prem apps, data systems, and cloud infrastructure. Veza solves the blind spots of traditional identity tools with its unique ability to ingest and organize permissions metadata in the Veza Access Graph. Global enterprises like Wynn Resorts, and Expedia trust Veza to visualize access permissions, monitor permissions activity, automate access reviews, and remediate privilege violations. Founded in 2020, Veza is headquartered in Los Gatos, California, and is funded by Accel, Bain Capital, Ballistic Ventures, GV, Norwest Venture Partners, and True Ventures. Visit us at veza.com and follow us on LinkedIn, Twitter, and YouTube.

© 2025 Veza, Inc. All Rights Reserved | veza.com