veza + servicenow

Product Solution Brief

Harness the power of ServiceNow across Veza's product ecosystem to proactively mitigate security risks while unlocking measurable business value.

Key Benefits

Complete Access Visibility

Gain comprehensive access insight into human and non-human access in ServiceNow and automatically enforce least-privilege access across your most critical applications.

Accelerated Time-to-Value

Plug directly into existing ServiceNow workflows for frictionless identity management and risk remediation without requiring new processes.

Unlock Value of ServiceNow Data

Activate the full value of your CMDB by using ServiceNow data to fuel intelligent and automated access management at scale.

 | veza.com

Core Capabilities

Who Has Access to What

Gain complete visibility into user, non-human identity, and AI agent access to ServiceNow data, roles, and ACLs—including risk factors such as no MFA, inactive accounts, or excessive entitlements.

Outcome: Improves security posture by revealing hidden access risks across human and non-human identities.

Insert Data into ServiceNow

Insert user identities, entitlement records, and access history directly into ServiceNow tables from Veza lifecycle and policy workflows.

Outcome: Establishes ServiceNow as a system of record for access and entitlement changes, supporting audit and compliance.

Automated Ticket Creation

Automatically create ServiceNow tickets for risk remediation, access changes, or violations identified across any Veza-connected system.

Outcome: Drives consistent, trackable remediation workflows across security and IT operations.

Integrated with ServiceNow Workflows

Power ServiceNow workflows with Veza access management capabilities to support employee access provisioning and deprovisioning, access requests, and risk remediation automation.

Outcome: Enables flexible and automated workflows that already exist minimizing disruption of business

ServiceNow Writeback to Veza

Sync ServiceNow CMDB data and ticket status change back to Veza to automate access requests approver look up and access revocation confirmation.

Outcome: Leverages the existing data within ServiceNow with near real-time updates between ServiceNow and Veza to strengthen access controls.

Veza *for* ServiceNow Use Cases

Account Security Monitoring and Alerts

Monitor account security risks and generate alerts using out-of-the-box ServiceNow security dashboards—for example, detecting accounts without MFA, inactive users, or elevated ServiceNow roles not aligned with IdP groups.

Elevated Access Validation

Review elevated access to ServiceNow to ensure access to updating critical business workflows is valid.

Identity & Entitlement Record Management

Populate user identities, roles, and application entitlements into ServiceNow to maintain historical records and support audit and compliance requirements.

Non-Human and AI Access Visibility

Reveal how non-human identities and AI agents interact with ServiceNow, including their access to sensitive data, roles, & workflow configurations.

Visualize user permissions to ServiceNow tables, and keep sensitive data secure by maintaining least privilege.

Veza + ServiceNow Use Cases

Access Violations Remediation

Get alerted on access violations and trigger remediation across all Veza-connected applications through ServiceNow - such as creating tickets to remove users who no longer need elevated access.

Risky NHI and AI Agent Monitoring

Monitor and alert on risky NHI and AI agents, such as AWS Bedrock agents granted permissions to accounts payable and bank reconciliation data, which may introduce segregation-of-duties risks.

Joiner, Leaver, and Mover Management

Be notified of joiner, leaver, and mover events across the organization, helping streamline JML workflows and maintain audit-ready records

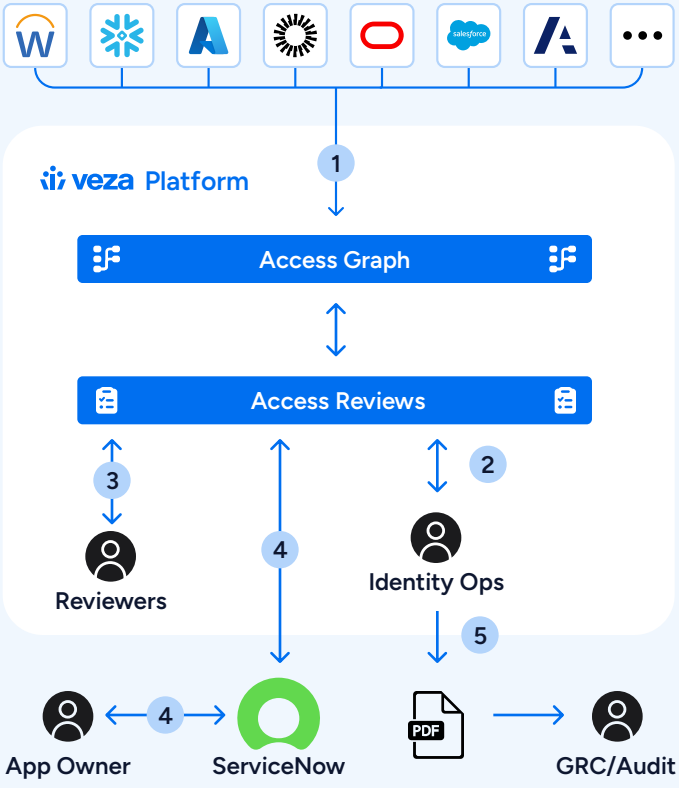
Automated Routing of Entitlement Requests

For entitlement requests, retrieve approver information from ServiceNow CMDB and automatically routing the requests to the appropriate approvers.

End-to-end UAR Rejection Validation

Upon rejection of a user's access in a UAR, automatically generated a ticket and routed to the application owner to revoke the access. Once the access is removed and the ticket is closed, the update writes back to Veza to mark the user as removed in the review.

Access Review Example



1. Veza continuously ingests user access metadata from IdP (Okta, Azure AD) and in-scope apps (Snowflake, SFDC, Workday, Anaplan, Oracle, Concur, SwiftConnect, Coupa etc.) into the Access Graph.
2. Identity Ops uses Veza to scope and launch quarterly UARs
3. Reviewers (i.e. user managers or app owners) are sent a notification with UAR link to allow them to review and approve/reject user access
4. **a.** Any rejections create ServiceNow tickets automatically. Tickets are routed to app team for access revocation.

   b. App team closes ticket when access is rejected. ServiceNow marks rejected access as fixed in UAR in Veza. ServiceNow ticket numbers are appended to UAR as evidence.
5. After all rejections are marked as fixed, Identity Ops generates the UAR report and sends it to GRC as well as Internal and External Audit