veza®

Solution Brief

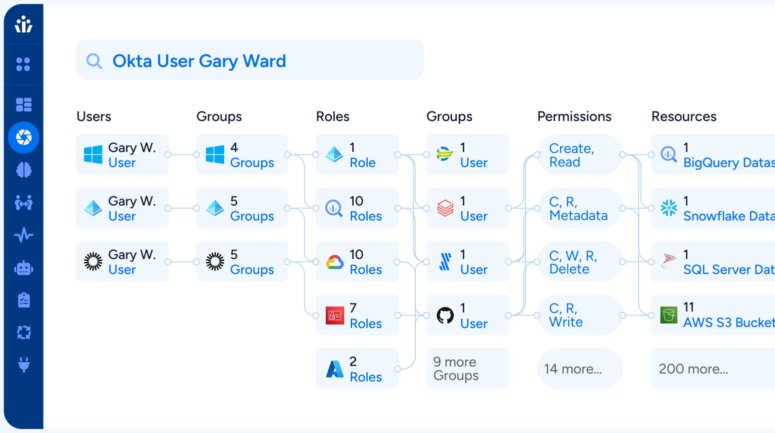
Veza for CrowdStrike

Know the Identity Risk. Kill the Access.

CrowdStrike's 2025 Global Threat Report makes it clear:

Identity is the #1 attack vector.

Defenders need to turn endpoint telemetry into actionable identity intelligence to stop breaches before they start. The Veza + CrowdStrike integration delivers end-to-end identity and access visibility, linking user context, device posture, and entitlements to sensitive data. This is more than risk scoring. It's a complete approach to identity threat detection, containment, and governance.



Okta User Gary Ward

Core Capabilities

The integration between Veza and CrowdStrike Falcon Identity Protection delivers more than just visibility - it enables real-time, risk-informed action. Here's what it empowers your team to do:

End-to-End Visibility Across Identity and Endpoint

- ☑ Combine CrowdStrike telemetry with Veza's Access Graph for unified identity visibility.
- ☑ See who has access to what, including device risk, identity status, and sensitive data (e.g., S3 buckets).

Example:
User A is in Okta, has admin access on a Falcon-managed laptop, and write access to regulated S3 data

Accelerated Threat Response

- ☑ Combine CrowdStrike telemetry with Veza's Access Graph for unified identity visibility.
- ☑ See who has access to what, including device risk, identity status, and sensitive data (e.g., S3 buckets).

Be able to answer:
What can this identity actually do right now?

Risk-Aware Remediation and Access Management with Veza Actions

- ☑ Detect toxic combinations, dormant access, and privilege escalation paths across users and service accounts.
- ☑ Tag high-risk identities using CrowdStrike endpoint risk signals and Veza access patterns.
- ☑ Auto-trigger privilege scans, access reviews, restrictions, or revocations in response to Falcon Identity Protection alerts.
- ☑ Enforce least privilege; disable, restrict, or escalate access with Veza Actions, no manual work required.
- ☑ Seamlessly route decisions to approvers or downstream systems — no code, no delay.

Key Use Cases

Use Case	Outcome
Identity Threat Containment	Restrict or escalate access when Falcon detects credential misuse
Blast Radius Mapping	Visualize risky entitlements across cloud, SaaS, and on-prem
Just-in-Time Reviews	Launch targeted reviews for high-risk users—skip the noise
Privilege Path Reduction	Detect and eliminate excessive permissions based on real risk

Customer Benefits

Faster Response

Triage identity threats based on real access, not just who triggered the alert

Better Decisions

Overlay Falcon risk scores with Veza access intel to guide investigations

Reduced Risk

Shrink the blast radius by removing dormant or excessive permissions

Increased Efficiency

Automate clean-up workflows and accelerate access certification cycles

Veza in Action—Powered by CrowdStrike

Highlight High-Risk Identities

Spot users with sensitive access on unmanaged or vulnerable devices

Trigger Conditional Access Actions

Auto-restrict or enforce MFA based on risk signals

Secure Joiner/Mover/Leaver Events

Flag and act on risky access during lifecycle transitions

Enforce Least Privilege at Scale

Right-size access from endpoints to data systems

Accelerate Audits

Instantly answer:
“What could this risky identity actually do?”

Explore the integration ↗

A one-stop hub for how Veza and CrowdStrike work together to protect identity and data.

See it in action ↗

Learn how Veza Actions streamlines detection-to-remediation workflows.

Set it up ↗

Step-by-step documentation for implementation teams and SecOps engineers.

| veza.com