Whitepaper

Veza Security

A Detailed Look at the Security Platform Cloud-First Organizations Need Now

About Veza

Veza is the identity-first security platform that provides security, engineering, and compliance teams with unprecedented visibility into identity and access to enterprise applications and data assets. As a cloud-native platform, Veza delivers highly scalable and highly available services, with security built in as a first principle. All of our designs and practices have been certified as SOC 2 Type II and ISO 27001 compliant.

This whitepaper details the Veza security platform across the following areas:

- Platform Overview
- Infrastructure Security
- Platform Encryption
- Access Control
- Audit and Compliance
- High Availability and Resiliency
- Secure Development Practices
- Enterprise Security Requirements
- Privacy First

Platform Overview

The Veza platform has two main components: the **Veza Control Plane** and the **Veza Insights Plane**. Here's a brief overview about both.

The **Veza Control Plane** is managed and operated by the Veza cloud engineering team in Amazon Web Services (AWS), where dedicated infrastructure is established for each customer with its own sub-domain-based namespace (for example, acme.Vezaprod.ai). A dedicated namespace is provisioned in Amazon's EKS service for each customer, and the network boundary is established by Kubernetes.

The **Veza Insights Plane** is a security-hardened Docker image that can optionally be installed within a customer environment, to connect to data stores in situations where customers don't want to expose the Veza Control plane directly. When deployed, the Veza Insights Plane connects to data sources within the customer environment, captures the associated identities and metadata, and communicates with Veza's control plane in AWS using a secure connection to Application Load Balancers within the dedicated customer environment.

Access Control

Strict access controls are applied across all Veza production and development environments, to maintain the integrity and confidentiality of all data. These access rules include:

- Veza maintains least privilege policies and permission. Access to production and staging environments is limited to specifically authorized Veza personnel only.
- Multi-Factor authentication (MFA) is required to access all production environments
- Dedicated VPN endpoint per cluster with granular access to each customer namespace
- Access to Veza's business apps (email systems, file-sharing systems, code repositories, and messaging systems) requires both SSO (Single sign-on) and Multi-Factor Authentication
- Production access is reviewed regularly every quarter
- The Veza platform monitors and verifies access granted to critical systems
- Veza uses our own product to monitor access control within our production environment, demonstrating our commitment by 'drinking our own champagne'.

Audit and Compliance

To maintain the strongest possible security posture, we employ select third-party tools and services to help us identify and address enterprise risk. Other audit and compliance details include:

- Veza continuously maintains SOC 2 Type 2 and ISO 27001 certifications
- Every container image used in production is scanned with the built-in Amazon Container Registry (ECR) scanning service
- Veza employs a third-party penetration testing service to assess the product annually (at minimum)
- All discovered issues that are labeled Critical or High are fixed upon discovery, not left to the next scheduled release
- Medium and Low findings are addressed in a patch release or during the regular release cycle

High Availability and Resiliency

The Veza platform employs several cloud-native and internally-developed methods for ensuring continuous service reliability and fault tolerance. These strategies include:

- High availability is designed into the Veza Control Plane for graph database, relational database, and messaging systems
- Persistent states are backed up on a periodic basis, as well as prior to system updates
- EKS nodes are distributed across different Availability Zones within AWS. EKS is backed by auto-scaling groups to achieve elasticity based on usage.
- Customer environments are continuously monitored for health using AWS CloudWatch, Grafana Cloud, and Honeycomb

Secure Product Development Practices

The Veza team adheres to industry standards and follows all best practices for secure software development. Some examples include:

- All code going into the Veza production environment is peer-reviewed
- Code versioning and branching practices follow OWASP standards
- Separation of duties is maintained between staff who develop code and staff who promote code to production

- Strong guidelines regarding error handling, availability, and security are followed during the system design phase
- Design reviews are conducted with engineering and product leadership as part of the product development and release cycles
- Automatic continuous scanning of code dependencies is performed with regular dependency upgrades
- For any new enhancements to the platform, our quality assurance engineering function maintains a strong focus on automated unit testing, integration testing, and approved test plans

Enterprise Security Requirements

Enterprise Security Requirements in the Veza platform are meticulously designed to safeguard against advanced threats and vulnerabilities, ensuring robust protection for critical enterprise data and applications.

- To prevent Denial of Service for all integrations Veza implements Rate Limiting. Veza also monitors and allocates resources properly to handle possible spikes.
- Veza has strict permissions that ensure only read permissions are granted to necessary information from each integration - restricted to required access only. All Veza permissions and roles can be regularly audited.
- Veza supports four static roles in the platform (Administrator, Operator, Access Reviewer and Viewer) to achieve needed granularity for access and permissions. Veza also supports Teams to limit access to only specific integrations and resources
- The Veza platform supports different authentication methods. For interactive users - Local User accounts and SAML SSO. For Non-Interactive Access: API Keys and OAuth2 Tokens

Privacy by Design

At Veza, we prioritize privacy at every stage of our product development lifecycle. Embracing a "Privacy by Design" mentality, we ensure that our products not only meet but exceed industry standards for data privacy and user confidentiality. Key aspects of our privacy-first approach include:

- Privacy First: From the initial stages of product design, privacy is a core consideration. We implement data minimization strategies, ensuring that only necessary data is collected, and default settings are configured to maximize user privacy.
- Our development practices align with international privacy regulations such as GDPR, CCPA, and others. We stay abreast of the evolving regulatory landscape to ensure continuous compliance.
- We maintain transparent data policies and ensure that user consent is sought wherever necessary. Users are provided with clear information about how their data is used and are given control over their personal information.
- Incident Response and Data Breach Protocols: In the unlikely event of a data breach, we have robust incident response protocols in place to minimize impact and communicate transparently with all stakeholders.

Conclusion

Veza's security platform offers unparalleled visibility and control, ensuring robust data security and standards compliance. This whitepaper underscores Veza's commitment to delivering a cutting-edge security solution, essential for modern enterprise environments.

– Veza Team