veza

Veza Security

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

Veza is a data security platform that provides security, engineering, and compliance teams with unprecedented visibility into identity and access to enterprise application 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 our designs and practices have been certified as SOC 2 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

Platform Overview

The Veza platform has two main components: the **Veza Control Plane** and the **Veza Insights Plane**. Here's a little detail about each.

The Veza Control Plane is managed and operated by the Veza cloud engineering team in Amazon AWS, where dedicated infrastructure is established for every 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.

Infrastructure Security

Veza uses a number of native AWS security controls to provide a layer of infrastructure protection for every customer environment. Key controls include:

- A dedicated Kubernetes namespace for each customer
- Application Load Balancer with Web Application Firewall (WAF) for all inbound traffic
- Enablement of AWS Shield, for protection against DDoS attacks
- A private subnet where Veza software (including control, management, and analytics) is only open to incoming traffic through environment-specific Web Application Firewall and Load Balancing
- A VPN endpoint and a bastion host for upgrades and maintenance that's only accessible (via MFA) by authorized Veza personnel

Platform Encryption

Data is encrypted by default across the Veza platform, both at rest and in transit. Encryption details include:

- Communication between the Veza Control Plane and the Veza Insights Plane is always encrypted over SSL using TLS 1.2 and AES-256 bit encryption
- Every Veza Insights Plane instance has a unique key pair. A public key is used to encrypt all credentials uploaded by the customer in the Veza platform, ensuring that only the customer's Veza Insights Plane can decrypt the credentials for that customer environment
- Disk encryption is enabled by default on all EKS compute instances, all databases, and all messaging subsystems

Access Control

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

- Access to production and staging environments are limited to authorized Veza personnel only.
- Multi-Factor authentication 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) require Multi-Factor Authentication
- The Veza platform monitors and verifies access granted to critical systems

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 a SOC 2 certification
- 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
- 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 push 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
- 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

To learn more about how Veza fits into your data security initiatives, visit us at www.veza.com/platform.

● sign up for a free trial

About Veza

Veza is the data security platform powered by authorization. Our platform is purpose-built for multi-cloud environments to help you use and share your data more safely. Veza makes it easy to dynamically visualize, understand and control who can and should take what action on what data. We organize authorization metadata across identity providers, data systems, cloud service providers, and applications — all to address the toughest data security challenges of the modern era. Founded in 2020, the company is remote-first and funded by top-tier venture capital firms including Accel Partners, Google Ventures, Norwest Venture Partners, and True Ventures. To learn more, please visit us at veza.com.