NOZOMI NETWORKS

WHITE PAPER

Protecting Customer Data: Vantage SaaS Multi-tenancy

1. Introduction

This white paper provides an overview of the Vantage data security architecture, emphasizing the importance of data protection for customers.

Nozomi Networks understands that addressing concerns and common challenges associated with Vantage as a multi-tenant SaaS solution is important. We believe that making the key security protections and architecture components transparent to its customers is key to establishing trust.

2. Secure by Design

Nozomi Networks Vantage is a multi-tenant, scalable SaaS platform, developed and operated in the cloud. It is architected to be cloud-native to take full advantage of the flexibility, scalability and operational advantages of cloud resources, while providing state-of-the art security at all levels. Vantage delivers centralized visibility and advanced threat detection across distributed industrial environments. The architecture is designed to meet the needs of enterprise customers and service providers by ensuring robust data isolation, seamless scalability, and strong alignment with regulatory compliance requirements. The platform supports granular access control and tenant-specific configurations, enabling secure and flexible deployments across diverse operational landscapes.

Vantage is engineered with strict controls around data residency, auditability, and customer-specific policy enforcement, supporting compliance with industry standards. Its architecture enables precise enforcement of security and privacy mandates while maintaining operational agility. By combining secure design principles with a scalable delivery model, Vantage empowers organizations to confidently meet their security, SLA, and architectural objectives—making it an ideal solution for complex and highly regulated environments.

At Nozomi Networks we believe that could-native security is a key criteria and has been the continuous point of attention while conceiving and enhancing the platform.

3. Technology

Secure Infrastructure

The infrastructure of Vantage has been designed with several layers of protection. Anti-DDOS, web application firewalls, load balancers, firewalls, gateways, service meshes and IDS act at the network level to separate the external public internet and the inner components of the system. Compute nodes run on hardened configurations, all data stores are encrypted, all communications are encrypted, and controls are put in place to log activity in the system and notify our SIEM.

Dataflow, Data Segregation and Encryption

Vantage is available in isolated regions, where a cluster is created and operated to be independent from the others. Each region is created in a Tier 1 public cloud service provider instance – AWS.

Customers access the system from the outermost component, the CDN – which also acts as WAF and Anti-DDOS. Through other internal networks/VPCs the traffic reaches the core of the system – the Kubernetes cluster, where requests are processed. The compute side of the cluster is shared among customers: it has been designed to be stateless and not hold any data.

Data Architecture

The data tiers are separated per customer: each customer has its own scalable data tier, to guarantee a logical and "physical" separation of data. There is also a shared data tier that is used by the system to orchestrate requests. A db-private data tier in the shared storage is used by Nozomi for internal test accounts and is not used by commercial Customers.

Encryption in Vantage is implemented at various layers and occurs multiple times. Access to the Vantage web interface is restricted to HTTPS connections only, utilizing TLS 1.2 or TLS 1.3, with strong encryption algorithms.

All internal network traffic between the different environment components is secured using TLS 1.3. Each customer has a dedicated encrypted database. A unique key, stored in a Key Management System (KMS), is used for this encryption and is rotated once a year.

The application functions within a completely encrypted environment, implementing encryption for data stored on disk, during network transfers, and in host memory. Furthermore, we use an envelope encryption strategy for sensitive data at the application level, creating a unique random session key for each encryption request.

Vantage is available in multiple regulatory data regions, with each region operating independently and without sharing data with one another.

Unique Customer and Organization ID

In the entire system, each customer has its own Customer ID. Each customer can create one or more isolated data containers called Organizations, each with a dedicated and globally unique Organization ID. Users live inside the Customer-private data tier and have a local user ID there.

When a user logs into the system, it is recognized by a session token that is bonded with its customer and organization ID. Based on this information, the compute nodes are able to process the request in isolation and connect to the right data tier – which is the core of each customer's state and the sole point where customer data is stored.

Access to Customer-private Data Tier

The Customer-private data tier can only be accessed by the compute nodes, and from specific containers (pods) of the Kubernetes cluster. From the outside, the data tier is protected by SAML

2.0 Single Sign On (which is secured on the customer side with multi-factor authentication) so that only users with a valid customer-branded domain account can access the system and thus the data contained in the private data tier.

Client-side Security

Like any modern web application, there is a component of the system which runs on each customer's web clients, in this case a React Single Page Application (SPA). This component is developed following the same Secure Software Development Lifecycle described below and thus scanned with static code analysis tools, penetration tested, etc.

The SPA connects to the Vantage cluster with TLS, negotiated at the possible highest secure level allowed by the web client.

4. Secure Processes

Access Control

In addition to the application-specific controls, access to customer data is further restricted by strong access controls to the control plane of the operational system. Only few internal staff members are authorized to have privileged access to the administrative support functions. This layer does not provide direct access to any data elements, which remain in encrypted state.

All activities are auditable, monitored, and subject to regular compliance checks.

Change Management

All changes to the system are managed exclusively in software and are subject to the same rigorous and secure development and release process.

Secure Software Development

The adopted Secure Software Development Lifecycle is rigorous about secure scanning of the code (static analysis) to prevent security flaws. Container images are scanned for vulnerabilities before being pushed to production. The Kubernetes cluster behind the scenes is also secured and checked against state-of-the art policies to guarantee maximum protection.

Data Deletion

Vantage utilizes the data destruction process of the cloud provider. Data is deleted after the application-specific retention policy is executed, using the most secure deletion and block reclamation method.

5. Assurance

To reinforce trust and transparency in the development and operation of Vantage, Nozomi Networks maintains a rigorous security assurance program aligned with globally recognized standards. The organization is ISO/IEC 27001 certified, demonstrating a systematic and risk-based approach to managing information security across its infrastructure, development lifecycle, and operational processes. This certification reflects a commitment to continuous improvement and adherence to best practices in safeguarding data and systems.

Validation

To validate the strength of the system and supporting infrastructure, third-party penetration tests are performed periodically, daily vulnerability scans with automated tools are conducted, along with internal penetration testing to provide continuous assurances of the security of the system and improve when necessary.

In addition, Nozomi Networks undergoes an independent SOC 2 Type 2 audit, evaluated under the Trust Services Criteria for security, confidentiality, and availability. This attestation provides assurance that Vantage is designed and operated with robust controls to protect customer data, ensure service continuity, and maintain strict confidentiality. These certifications validate the strength of Nozomi's internal controls and provide customers with confidence in the platform's ability to meet demanding compliance and risk management requirements.

6. Conclusion

Vantage's data protection methods are meticulously designed to offer robust security and peace of mind for customers. By leveraging a multi-layered secure infrastructure, a rigorous secure software development lifecycle, comprehensive data separation techniques, advanced encryption strategies, and client-side security measures, Vantage ensures that data is protected at every stage. With Vantage, users can trust that their data is safeguarded against potential threats, allowing them to focus on their core business activities with confidence.

For further inquiries regarding this white paper on Nozomi Networks' data protection practices, please contact the compliance team at **compliance@nozominetworks.com**

NOZOMI NETWORKS

Cybersecurity for OT, IoT and Critical Infrastructure

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.