WHITE PAPER

Security Measures for Nozomi Networks Vantage

1. Executive Summary

This white paper outlines the security framework, architecture, controls, and operational procedures designed to protect Nozomi Networks Vantage, a cloud-native platform hosted on Amazon Web Services (AWS). It is intended for clients, security reviewers, auditors, and partners who seek transparency into our security measures.

We utilize industry standards such as SOC 2 Type II and ISO/IEC 27001:2022 to ensure the confidentiality, integrity, availability, and privacy of customer information. These measures are crucial for safeguarding operational technology (OT) and IoT data.

2. Introduction

Nozomi Networks is dedicated to ensuring customer trust through a comprehensive governance, risk, and compliance program. We have adopted security standards and integrated them into our business operations as a fundamental component. Our administrative, technical, logical, and physical controls, along with third-party security audits and certifications, apply to all Nozomi Networks products, SaaS, and IT services. Security is prioritized at the highest levels of the company, with the executive management team regularly reviewing issues and coordinating company-wide security initiatives.

These measures are crucial for maintaining the integrity and trust of our services.

3. Governance & Risk Management

Our governance and risk management practices are overseen by the Governance, Risk, and Compliance department (GRC). Key activities include managing and improving the Information Security Management System (ISMS) based on ISO/IEC 27001:2022, assessing product service operations and obtaining SOC2/SOC3 attestation reports, and managing the information security policy framework to support all applicable requirements that include, but are not limited to:

- Policies are reviewed and approved annually.
- We conduct continuous risk assessments and mitigations, perform quarterly risk reviews and management reviews, and carry out regular internal and external audits.
- We have a robust third-party risk management process.

These measures are crucial for maintaining the integrity and trust of our services.

4. Access Control & Identity Management

Access management functions are consistently implemented to ensure robust security.

We enforce role-based access control (RBAC) and least privilege principles through identity federation and defined user roles for administrative access. Single Sign-On (SSO) and Multi-Factor Authentication (MFA) are mandatory for all users. Just-in-time provisioning and automated deprovisioning are integrated with AWS IAM (Vantage) and similar tools across all business applications. All system access accounts are authorized, periodically reviewed, and promptly removed as needed.

5. Encryption

Access to sensitive client data is restricted and remains under the clients' exclusive control. All data at rest is encrypted using AES-256, while data in transit is protected using TLS 1.2+.

6. Application Security

Vantage development is grounded in security-by-design principles. Our development process adheres to the Secure Software Development Lifecycle (SSDLC) and includes a formal release process with peer review and approval, threat modeling, and risk analysis.

We use hardened containers, dependencies, and software components.

Continuous static and dynamic application security testing (SAST/DAST) is performed. Our code testing methodology employs multiple mitigation strategies, tailored to specific code components, and includes OWASP, MITRE, and NIST CSF standards.

We conduct annual independent penetration tests, with findings prioritized, remediated, and documented. Additionally, dependencies and third-party components are monitored for vulnerabilities using automated scanning tools.

7. Infrastructure Security

Vantage is hosted on a secure, scalable multi-tenant architecture with AWS, utilizing the AWS Shared Responsibility Model. We use various AWS services, including CDN, WAF, Route 53, VPC, S3, RDS, IAM, CloudTrail, and KMS. Change management of the Vantage infrastructure, databases, and all administrative control functions are performed in code utilizing the secure code release process. Continuous vulnerability scanning is integrated into the CI/CD pipeline. These measures are crucial for maintaining the security and integrity of our infrastructure.

8. Personnel Security

The management of Nozomi personnel includes several key measures to ensure robust security.

We conduct comprehensive background checks prior to system access.

All employees must accept policies and complete security training during onboarding and annual refresh sessions. We also perform phishing simulations and incident response drills. Specialized training is provided based on role-based access to sensitive information.

9. Audit Logging & Monitoring

Monitoring and logging are applied to all critical services to ensure robust security. All access to and use of Vantage resources is logged in immutable, timestamped logs. These logs are stored securely and monitored for anomalies via integrated SIEM systems. Alerting is configured for suspicious behavior or failed access attempts.

10. Third-Party Risk & Supply Chain Security

Nozomi has implemented a comprehensive third-party risk program to ensure robust security. Third-party services and products are assessed for security risks and tracked in a vendor risk register. Each supplier undergoes periodic reviews for changes to security, continuity, and legal/regulatory requirements, based on their criticality to the business.

Vendor contracts include data processing clauses and data handling provisions. Data governance functions ensure the return or destruction of data at the end of agreements.

11. Resilience & Continuity

Ensuring continuous availability of Vantage services for monitoring critical infrastructure is of utmost importance. Vantage SaaS is continuously monitored for high availability and resiliency.

Application operations span across multiple AWS availability zones within the same regulatory regions, physically separated from one another.

Disaster recovery procedures are tested bi-annually. The Vantage architecture leverages resilient cloud-native database technology to achieve rapid scaling, clustering, replication, and automation.

Vantage operations team employs specialized methods to monitor server performance, data, and traffic load capacity within each availability zone and processing center.

12. Incident Response

Nozomi Networks maintains a documented incident response plan aligned with ISO 27001:2022 controls, which is tested periodically. All operational systems are monitored 24/7 by a dedicated security team. The team uses advanced and internal threat intelligence feeds for analysis and prevention of serious incidents.

Security incident notifications are processed according to regulatory breach notification timelines and contractual SLAs.

13. Assurance

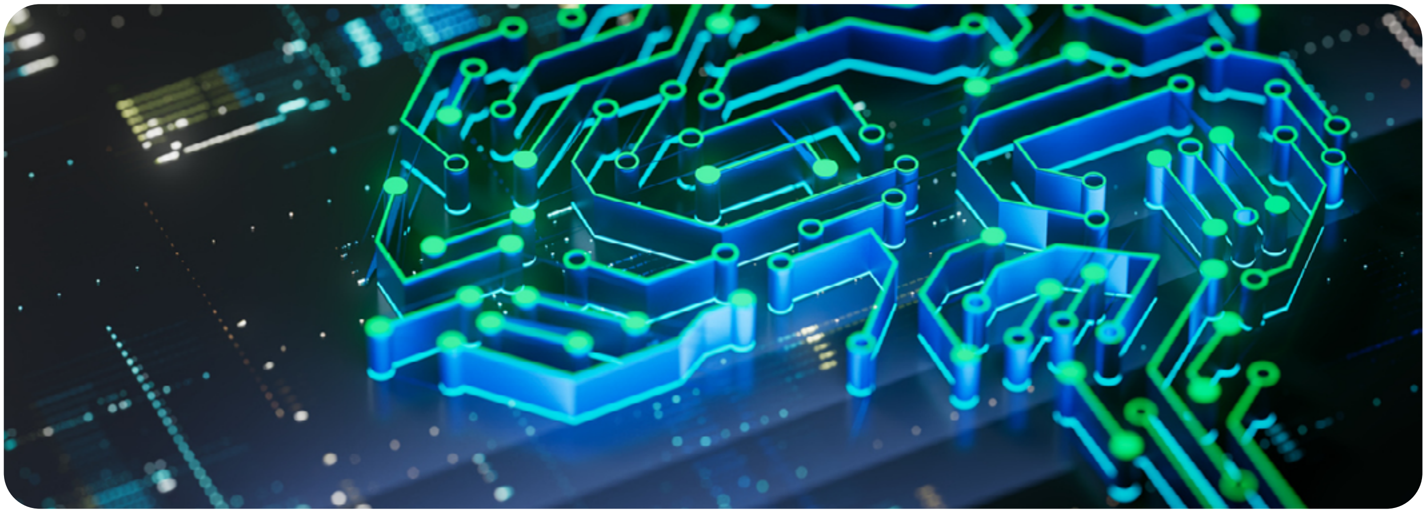
Nozomi Networks maintains SOC 2 Type II compliance, with SOC 3 reports available in the Trust Center. Vantage development and operations are part of an ISO/IEC 27001:2022 and ISO 9001:2015 certified ISMS and QMS respectively.

14. Conclusion

Security is our business and a foundational element of our service delivery. Our alignment with SOC 2 and ISO/IEC 27001:2022 ensures a robust and continuously improving security framework.

We invite customers and partners to review this paper and engage with us for further assurance details. These measures are crucial for maintaining the integrity and trust of our services.

For further inquiries regarding this white paper, please contact the compliance team at **compliance@nozominetworks.com**



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.