NOZOMI NETWORKS


WHITE PAPER

# Use and Development of AI and ML Technology in Nozomi Products

# 1. Overview

Nozomi Networks integrates advanced Artificial Intelligence (AI) and Machine Learning (ML) technologies across its cybersecurity product suite, including Vantage IQ and Asset Intelligence. These technologies are designed to enhance threat detection, asset classification, anomaly detection, and provide intelligent recommendations, while maintaining strict compliance with data privacy and regulatory standards.

Data used for AI processing is limited to technical and operational telemetry and does not include customer-provided content or any information intentionally identifying individuals. Nozomi Networks takes all reasonable measures to minimize and, where possible, eliminate personal data in AI-related processing. The primary outcomes of AI/ML feature development are to enhance the efficiency and resiliency of human decision-based operations.

This document is reviewed periodically and kept up to date, as the rapidly changing technological landscape demands increased attention to AI/ML governance.

# 2. AI/ML Capabilities and Use Cases

All AI/ML functionality in Nozomi Networks' products is analytical in nature. No feature makes or executes autonomous operational, security, or access-control decisions. All insights, recommendations, and classifications require human validation before action.

## 2.1 Core Technologies

- **Natural Language Processing (NLP):**
  Used in Vantage IQ for chatbot and assistant features, enabling users to interact with the platform using natural language queries.
- **Predictive Analytics / Forecasting:**
  Employed for anomaly detection and predictive analysis, supporting proactive threat identification and system health monitoring.
- **Generative AI:**
  Vantage IQ leverages generative AI for text generation and intelligent recommendations.
- **Custom Trained Models:**
  Asset Intelligence uses proprietary, custom-trained models to classify assets based on behavioral patterns.
- **Clustering (Unsupervised Learning):**
  Clustering and linear inference models are used for grouping similar assets, identifying recurring or anomalous network sessions, and supporting incident triage. Clustering is analytical, not autonomous, and always requires validation before the results become humanly actionable.
- **Bayesian Networks:**
  Applied for asset identification, combining multiple protocol hints to infer device attributes.
- **Knowledge Representation and Ontology Engineering:**
  Used for reasoning and generalizing behaviors within the product.

## 2.2 Primary Use Cases

- **Anomaly Detection:**
  Detects unusual patterns in network and asset behavior using supervised and unsupervised ML models.
- **Asset Classification:**
  Classifies assets based on observed behaviors and protocol evidence, using both ML and AI techniques.

- **Incident Triage and Decision Support:** Provides data-driven groupings and recommendations to support human analysts in incident investigation and response. Nozomi's clustering and ML models operate only in a decision-support capacity and cannot autonomously change configurations, initiate responses, or enforce security actions.
- **Reporting and Remediation Guidance:** AI-driven insights are used for configuration, reporting, and security recommendations.

# 3. Architecture and Data Handling

## 3.1 Processing Modes

- **Standard (External AI Infrastructure):** Vantage IQ can use external LLM services for advanced AI features. All data sent externally is transient, never stored, and not used for model training or fine-tuning. Data processing locations are restricted to regulatory regions with strong privacy protections. All external data exchanges are encrypted in transit and occur within authenticated, time-bound sessions. Nozomi Networks enforces zero-retention and data isolation agreements with third-party AI providers.
- **Local Processing Options:** Customers can disable external processing. All data processing takes place in the same data center as the customer instance in this mode, supporting strict data residency and compliance requirements.

## 3.2 Data Privacy and Security

- **Zero Data Retention:** Nozomi Networks applies a "zero customer data reuse" policy. Data processed by AI/ML features is transient and not retained beyond session completion, except for minimal technical logs maintained for service integrity, troubleshooting, or security auditing in accordance with the customer's Agreement and Nozomi Networks' Privacy Policy.
- **Model Training:** All AI models are pre-trained on internal or third-party data that has been validated and sanitized. Customer data is never used for training or fine-tuning.
- **Access Controls:** Role-Based Access Control (RBAC) and SAML integration ensure only authorized users can access AI-powered features.
- **No Data Sharing Across Customers:** Data processed by AI/ML features is never shared between customers. Customer data is contained within their Vantage instance.
- **API Access Restrictions:** AI-powered services can only be accessed through authenticated Vantage sessions; direct API access is not permitted.

# 4. Security, Ethical Safeguards, and Compliance

## 4.1 Security

- The development process includes guardrails aligned with best practices for AI feature development, specifically addressing the security concerns of Vantage customers. It includes:
- **Two-Layer Safety Checks**
  All prompts undergo rule-based screening (pattern matching, word analysis) and validation by an AI safety agent. System prompts to restrict model outputs to cybersecurity contexts.
- **Enforcement of security boundaries**
- **Secure API connections using TLS1.2+**
- **Pre-authenticated sessions in the Vantage environment**
- **Inheritance of LLM provider security**
  External providers are carefully vetted for strict security measures and compliance with emerging regulations. Notable features applied to the environment are:
  - Zero-data retention policy
  - Use of pre-trained and non-fine-tune model

Third-party AI providers used within Vantage are bound by contractual data protection terms equivalent to Nozomi Networks' own obligations, ensuring confidentiality, zero-training use, and compliance with applicable privacy and AI regulations.

- **Software Composition Analysis (SCA):**
  All AI/ML components are regularly scanned for vulnerabilities, and critical issues are promptly resolved.

## 4.2 Regulatory Compliance

- Vantage IQ's clustering and other machine learning features are designed to comply with the EU AI Act by operating strictly as limited- or minimal-risk AI systems. These features never take autonomous actions and always require human oversight, ensuring accountability and control. We maintain comprehensive documentation, transparency, and auditability across all AI functionalities, which supports adherence to regulatory standards and facilitates independent verification when needed. This approach reflects our commitment to responsible AI practices and alignment with current compliance frameworks.
- Beyond meeting today's requirements, we actively monitor emerging regulations and evolving standards across jurisdictions to anticipate changes before they take effect. Our governance process includes frequent reassessment of AI features to confirm they remain compliant with applicable laws and contractual obligations. By continuously reviewing risk classifications, updating documentation, and refining oversight mechanisms, we ensure Vantage IQ not only meets existing requirements, but is prepared for future regulatory developments. This proactive stance minimizes compliance risk and reinforces trust in our AI solutions.

# 5. Testing, Validation, and Documentation

- **Model Validation:**
  Models are tested using standard metrics (accuracy, Kappa value, etc.) and continuously validated in the field. Data is split into training and test sets to ensure generalization and avoid overfitting. Validation includes assessments of accuracy, bias, explainability, and reliability to ensure responsible operation in diverse customer environments.
- **Human-in-the-Loop:**
  All AI/ML outputs are subject to human validation before any operational action is taken. Nozomi's systems are designed as decision support tools, not autonomous agents.
- **Documentation and Auditability:**
  Technical documentation is maintained for all models, including purpose, scope, data sources, and operational use. Audit logs are kept for investigations and alerts.

# 6. Development Governance

**Key Elements of the Governance Process**

- **Integrated SSDLC:**
  Nozomi Networks integrates AI/ML development into its secure software development lifecycle (SSDLC). Each AI feature undergoes documented risk assessment, compliance review, and oversight before release. Nozomi Networks' governance framework ensures traceability, explainability, and continuous alignment with applicable AI regulations.
- **Continuous Oversight:**
  Our internal oversight process ensures that all engineering decisions are traceable, explainable, and aligned with Nozomi's governance standards. Rapid AI technology changes require the governance functions to remain in alignment. The oversight functions include ad-hoc and periodic reassessments and updated documentation.

# 7. AI/ML Features in Nozomi Products (summary)

| Capability | In Use? | Module/Feature | Products/Platform |
|---|---|---|---|
| **Natural Language Processing (NLP)** | Yes | Vantage IQ | Vantage IQ Assistant |
| **Predictive Analytics/Forecasting** | Yes | Predictive Analysis | Vantage, N2OS |
| **Generative AI** | Yes | Vantage IQ | Vantage IQ Assistant |
| **Custom Trained Models** | Yes | Asset Intelligence | N2OS, Vantage |
| **Clustering (Unsupervised Learning)** | Yes | Vantage IQ | Vantage IQ, Asset Intelligence |
| **Bayesian Networks** | Yes | Asset Identification | N2OS, Vantage |
| **Knowledge Representation** | Yes | Multiple | N2OS, Vantage |
| **Data Retention** | No | All | All Products |
| **Third-Party LLMs** | Yes | Vantage IQ Chatbot | Vantage IQ Assistant |

# 8. Summary

Nozomi Networks employs a robust, multi-layered approach to AI and ML, combining advanced analytics, strict privacy controls, ethical and regulatory compliance. The technologies are designed to support, not replace, human analysts—delivering actionable insights while ensuring transparency, security, and ethical operation.

Nozomi Networks enforces a structured and transparent governance process for the development and integration of AI/ML features, ensuring responsible innovation and regulatory compliance.

Nozomi Networks' AI/ML technologies are designed to enhance cybersecurity operations without compromising customer confidentiality or control. AI/ML features operate within the boundaries defined in customer agreements and are subject to continuous oversight, documentation, and compliance review. Nozomi Networks' commitment to ethical, transparent, and secure AI use ensures that automation always serves to empower, not replace, human expertise.

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.