NOZOMI NETWORKS

PRODUCT OVERVIEW

Vantage IQ

An AI-based Engine for Advanced Cybersecurity Analytics

Addressing modern cybersecurity threats has become a challenge in analytics. Security systems and teams have to analyze a large amount of data from potentially tens of thousands of sensors and devices, correlated over a period of time, to determine if an anomaly or alert is really a threat, the root cause and how to remediate it quickly.

Nozomi Networks raises the bar on security analytics and automation with the industry's first AI rules-based analysis and query engine, Vantage IQ.

Available as an optional add-on to the Nozomi Networks Vantage platform, Vantage IQ replicates learned experiences of seasoned security analysts and automates tedious tasks of reviewing, correlating, and prioritizing the enormous amount of collected network, asset and alert data to provide meaningful insights into real threats and how they should be addressed. Teams using Vantage IQ are more efficient by spending less time tuning the platform and more time focusing on priority issues.

Vantage IQ is the industry's first state-of-the-art AI and machine learning (AI/ML) engine that can emulate the acquired knowledge of experienced security admins over extremely large cloud-scale networks at a fraction of the cost. Like modern AI systems in other domains of expertise, Vantage IQ includes inherent knowledge of automated control systems and devices as it continues to learn expected behaviors over time. Vantage IQ allows any organization to close security gaps in mission critical operational infrastructure with more vigilance, focus and automation.

Highlights

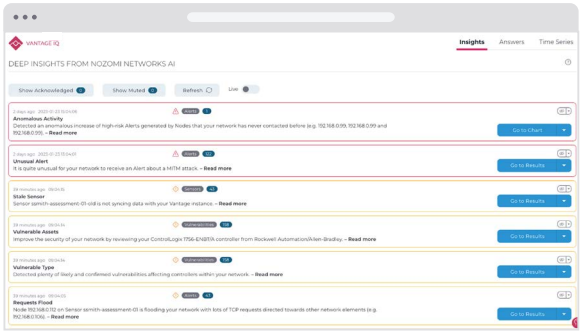
- **New AI/ML-based security engine and analytics** extends Vantage capabilities for deeper insights and more automation.
- **Stronger correlation** for more focus on fewer, prioritized actionable alerts.
- **Powerful new query and answer system** allows customizable research to improve security posture, anticipate issues and reduce risk.
- **Automated analytics** reduces the need for more administrative overhead, closes the security skills gap and learns long-term behavior cycles.
- **More natural problem descriptions and remediation recommendations** can be understood by less skilled security admins to accelerate response and reduce downtime.
- **No additional configuration required**. Vantage IQ can begin analyzing existing data and providing insights immediately with standard queries. Customized query analytics can be built easily.

Automated Intelligence with Vantage IQ

Key Features

Insights Dashboard

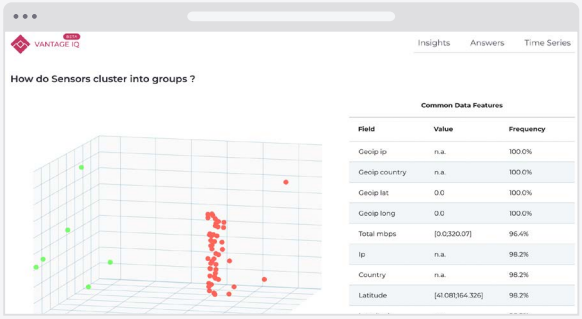
Vantage IQ Insights Dashboard highlights correlated alerts and root-cause analysis. Activity patterns in network data are identified via deep neural networks. Data is correlated across Vantage to streamline forensic analysis, tuning and security enhancements. Deeper insights from aggregated security data and network traffic reduce alerts to help prioritize remediation efforts and close security gaps.



AI-based Query and Analysis System

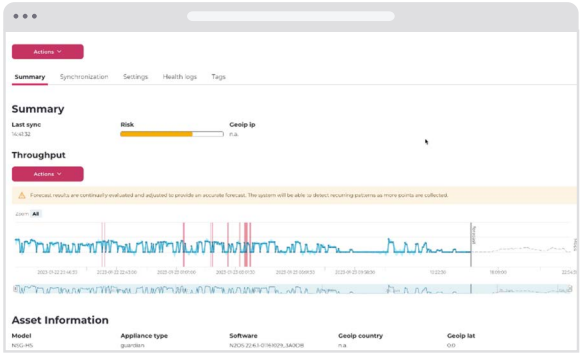
Powerful customizable queries are used to answer common questions and provide users with a better understanding of their environment. Semi-supervised preparation of ad-hoc queries can guide users to better identify anomalies. Sample questions:

- *What are the relevant characteristics of high-risk vulnerabilities?*
- *How are vulnerabilities clustered into groups?*
- *How do asset attributes correlate with each other?*
- *How do alert sources correlate with risk?*



Time Series

Time Series utilizes advanced machine learning techniques to predict and alert on abnormal bandwidth from any sensor's baseline network activity. Was the change expected or outside of a normal range of deviation for that period? Forecasting is done via deep neural networks. Online signal analysis can find existing trends and predict forecast reliability.



Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com