NOZOMI NETWORKS

Solution Brief

Real-time Cybersecurity and Visibility for Industrial Control Networks

Industrial organizations around the world are increasing the interconnectedness and digitization of their systems to gain efficiencies and competitive advantage. Unfortunately, this also increases their exposure to cyber risks – in an era of escalating cyberattacks.

To improve cyber resiliency, it's essential to have real-time visibility into OT environments and assets, as well as to cyber threats, risks and process anomalies. The Nozomi Networks solution delivers just that, in a way that is completely safe and non-intrusive for industrial control networks.

Customers in sectors such as critical infrastructure, energy, manufacturing, mining, transportation and utilities have improved reliability, cybersecurity and operational efficiency thanks to Nozomi Networks installations.

Let our passive solution, powered by artificial intelligence, automate the hard work of inventorying, visualizing and monitoring your industrial control system (ICS). You benefit from the real-time visibility and threat detection needed to ensure high cyber resiliency and reliability.

Superior Operational Visibility

- Automated, accurate asset inventory
- Intuitive network visualization
- Real-time network monitoring

The Best ICS Threat Detection

- Behavior-based anomaly detection
- Rules and signature-based detection
- Advanced correlation for detailed insights and rapid remediation

The Most Distributed Global Installations

- Multinational deployments with hundreds of facilities and thousands of devices
- Centralized OT visibility and cybersecurity
- Flexible ICS data consolidation
- Fast deployments with immediate ROI
- Easy integration with IT and ICS infrastructure
- Common platform to drive IT/OT convergence

enel

"Enel Power Plants are a strategic asset we are committed to protect. Malfunctions or damage to this infrastructure would be a threat to our national security. With SCADAguardian we can detect and collect operational and cybersecurity issues in real-time, and take corrective actions before threats can strike."

GIAN LUIGI PUGNI
Head of Cybersecurity Design, Enel

Real-time Cybersecurity and Visibility for Industrial Control Networks

Rapidly Detect Cyber Threats/Risks and Process Anomalies

Stop threats in their tracks or remediate using comprehensive, hybrid ICS threat detection.

- Behavior-based anomaly detection of cyber threats and process risks
- Rules and signature-based threat detection
- Correlated detection results for detailed insights, operational context and rapid remediation

Quickly Monitor ICS Networks and Processes with Real-time Insights

Avoid disruptions, expensive repairs and loss of revenue thanks to automated learning and insightful views.

- Intuitive network visualization
- Real-time network and process monitoring
- Quick identification of critical states and threats
- Customizable dashboards, queries and alerts

Automatically Track Industrial Assets and Know Their Cybersecurity Risks

Save time, know your current ICS inventory, and improve cyber resiliency.

- Accurate asset discovery
- Automated identification of devices with vulnerabilities, including severity levels
- Easy ways to visualize, find, and drill down on asset and vulnerability information

Significantly Reduce Troubleshooting and Forensic Efforts

Quickly assess risks and mitigate cybersecurity and process incidents with time-saving tools.

- Dynamic learning that reduces false alerts
- Smart grouping of alerts into root incidents
- Automatic packet capture
- TimeMachine™ system snapshots
- Real-time dashboards and ad hoc queries

Centrally or Remotely Secure Large, Distributed Industrial Networks

Reduce enterprise risk with consolidated OT visibility across hundreds of industrial facilities.

- The Nozomi Networks Central Management Console (CMC) centrally monitors huge multinational operations
- Deployment options support flexible, hierarchical aggregations of ICS data
- Multitenancy for shared or MSSP (Managed Security Service Provider) deployments

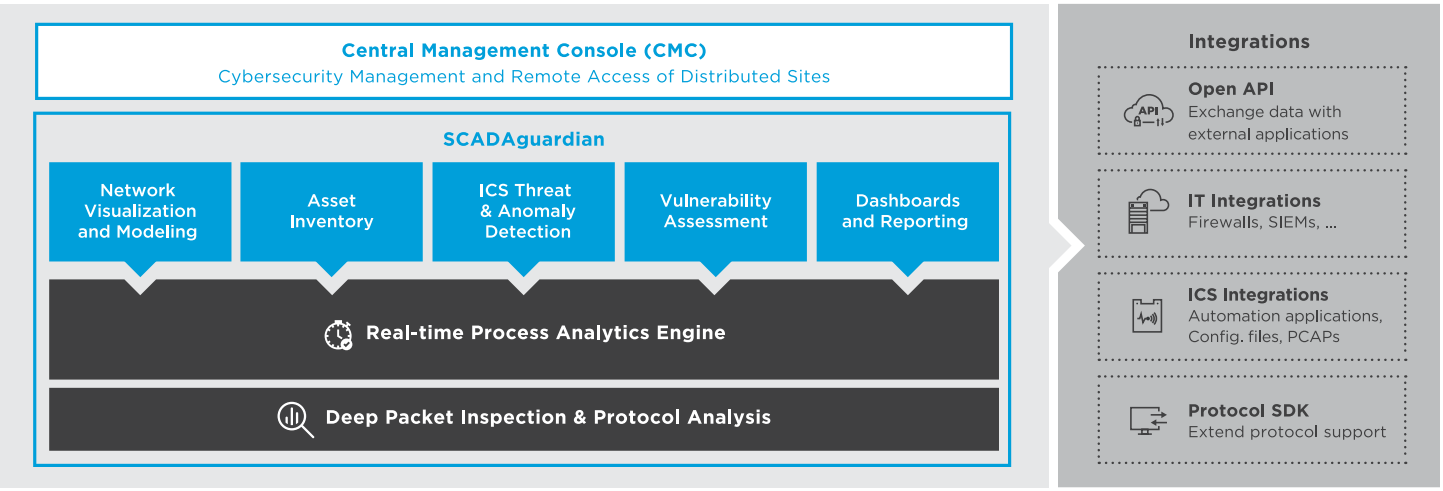
Scalability for Massive Multinational Deployments

Depend on a product fully optimized for enterprise-class performance and scale.

- Highly scalable and flexible architecture including multitenant and high availability (HA) options
- Fast, optimized performance
- Easy integration with IT/OT environments
- Quick deployments, automated results

Centralized and Remote Cybersecurity Management

THE NOZOMI NETWORKS SOLUTION ARCHITECTURE



Deep Packet Inspection and Protocol Analysis

- Evaluates dozens of ICS and IT protocol communications, with support for additional protocols available via an SDK
- Examines packets in all 7 levels of the OSI model
- Analyzes communications thoroughly for conformance with official protocol syntax and the real-world customizations used by specific industry sectors

Real-time Process Analytics Engine

- Learns dynamically, modeling stable network segments first and automatically switching to protection mode
- Compares current communications, devices and process variables to baseline profiles using a high performing, real-time algorithm
- Correlates alerts into root incidents
- Notifies staff of issues in real-time via dashboards, reports and alerts

SCADAguardian for Real-time Cybersecurity and Operational Visibility

- Installs in OT networks passively, with no downtime
- Deploys via a broad range of physical and virtual appliances, suitable for a wide range of sites
- Improves situational awareness with superior asset discovery and real-time network monitoring
- Delivers best-in-class ICS threat detection with a hybrid approach that combines behavior-based anomaly detection with rules-based techniques
- Reduces troubleshooting and mitigation efforts with time-saving incident and forensic tools

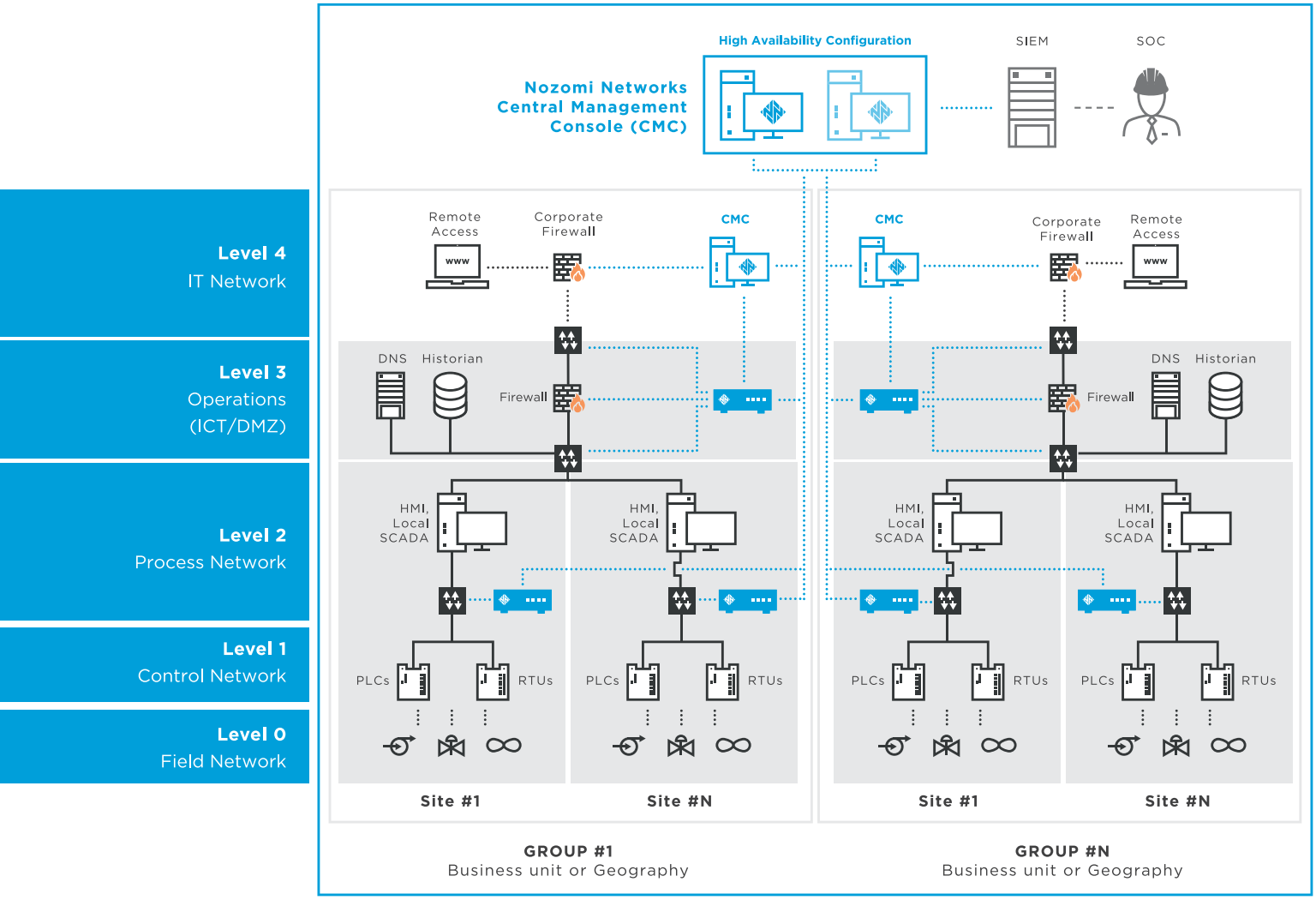
Easy IT/OT Integration

- Integrates seamlessly with IT/OT infrastructure such as asset management systems, firewalls, identity management systems, ticketing systems, SIEMs and more *(see website for current list)*
- Exchanges data with other IT/ICS applications through an open API
- Includes built-in support for dozens of IT/OT protocols, extends to others via a protocol software development kit (Protocol SDK)

Central Management Console for Consolidated Cybersecurity Monitoring

- Scales to monitoring OT risk for hundreds of facilities
- Consolidates ICS data flexibly, using hierarchical aggregations
- Deploys, optionally, as a multitenant or HA application

Sample Deployment Architecture



Nozomi Networks Products

SCADAguardian is a physical or virtual, passive appliance that provides real-time cybersecurity and operational visibility for industrial control networks.

The **Central Management Console (CMC)** aggregates data from up to hundreds of facilities, providing high availability centralized and remote cybersecurity management.

Together they deliver comprehensive OT visibility, cyber resilience and reliability.

About Nozomi Networks

Nozomi Networks is the leader of industrial cybersecurity, delivering the best solution for real-time visibility to manage cyber risk and improve resilience for industrial operations. With one solution, customers gain advanced cybersecurity, improved operational reliability and easy IT/OT integration. Innovating the use of artificial intelligence, the company helps the largest industrial facilities around the world See and Secure™ their critical industrial control networks. Today Nozomi Networks supports over a quarter of a million devices in sectors such as critical infrastructure, energy, manufacturing, mining, transportation and utilities, making it possible to tackle escalating cyber risks to operational networks (OT).

NOZOMI NETWORKS

www.nozominetworks.com

@nozominetworks

SB-8.5x11-005