NOZOMI NETWORKS

Solution Brief

Real-time Cybersecurity and Visibility for Industrial Control Networks

Many industrial organizations around the world are increasing the interconnectedness and digitization of their systems to gain efficiencies and competitive advantage. Doing so increases cyber risks, amid increasingly severe and frequent cyberattacks.

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

Major customers have improved reliability, safety, cybersecurity and operational efficiency thanks to their Nozomi Networks installation.

Let our passive solution, powered by machine learning and artificial intelligence, automate the hard work of knowing and monitoring your Industrial Control System (ICS). You benefit from the real-time visibility and threat detection you need to ensure high cyber resiliency and reliability.

Industrial Cybersecurity

- Best-in-class threat, risk and anomaly detection using a hybrid approach
- Automated vulnerability assessment

Operational ICS Visibility

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

Proven Large-Scale Deployments

- Readily scales to thousands of industrial sites
- Centralized ICS cybersecurity management
- Easy integration with IT/OT environments
- Major installations at critical infrastructure, process control, and manufacturing organizations

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 that combines:

- Behavior-based cyber threat and process anomaly detection
- Rules and signature-based threat detection
- Fast analysis powered by artificial intelligence

Quickly Monitor ICS Networks and Processes with Real-time Insight

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

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

Automatically Track Industrial Assets and Know Their Cybersecurity Risks

Save time, know your current ICS, and improve cyber resiliency with:

- Auto-discovery and mapping of all industrial assets
- 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 superior monitoring and forensic tools:

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

Centrally or Remotely Secure Large, Distributed Industrial Networks

Reduce enterprise risk with consolidated cybersecurity visibility across many industrial sites:

- The Nozomi Networks Central Management Console (CMC) scales to monitor thousands of sites
- Deployment options support flexible, hierarchical aggregations of ICS data
- Multitenancy for shared or MSSP (Managed Security Service Provider) deployments

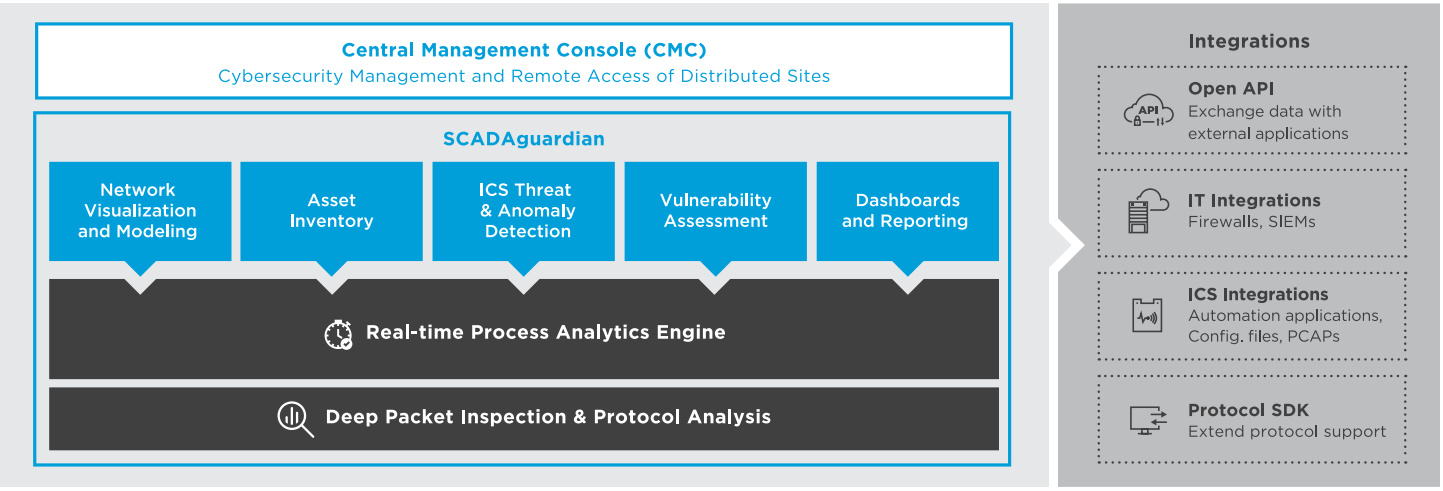
Confidently Deploy at Enterprise Scale Thanks to Proven Performance

Proven with large-scale deployments at critical infrastructure, process control and manufacturing organizations:

- Highly scalable and flexible deployment options
- Maximum control of who sees what data
- Fast, optimized performance
- Easy integration with IT/OT environments

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 a SDK
- Examines packets in all 7 levels of the OSI model
- Analyzes communications thoroughly for conformance with official protocol syntax and for 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
- Detects ICS threats and process anomalies using a comprehensive hybrid approach
- Reduces troubleshooting and mitigation efforts thanks to superior incident and forensic tools

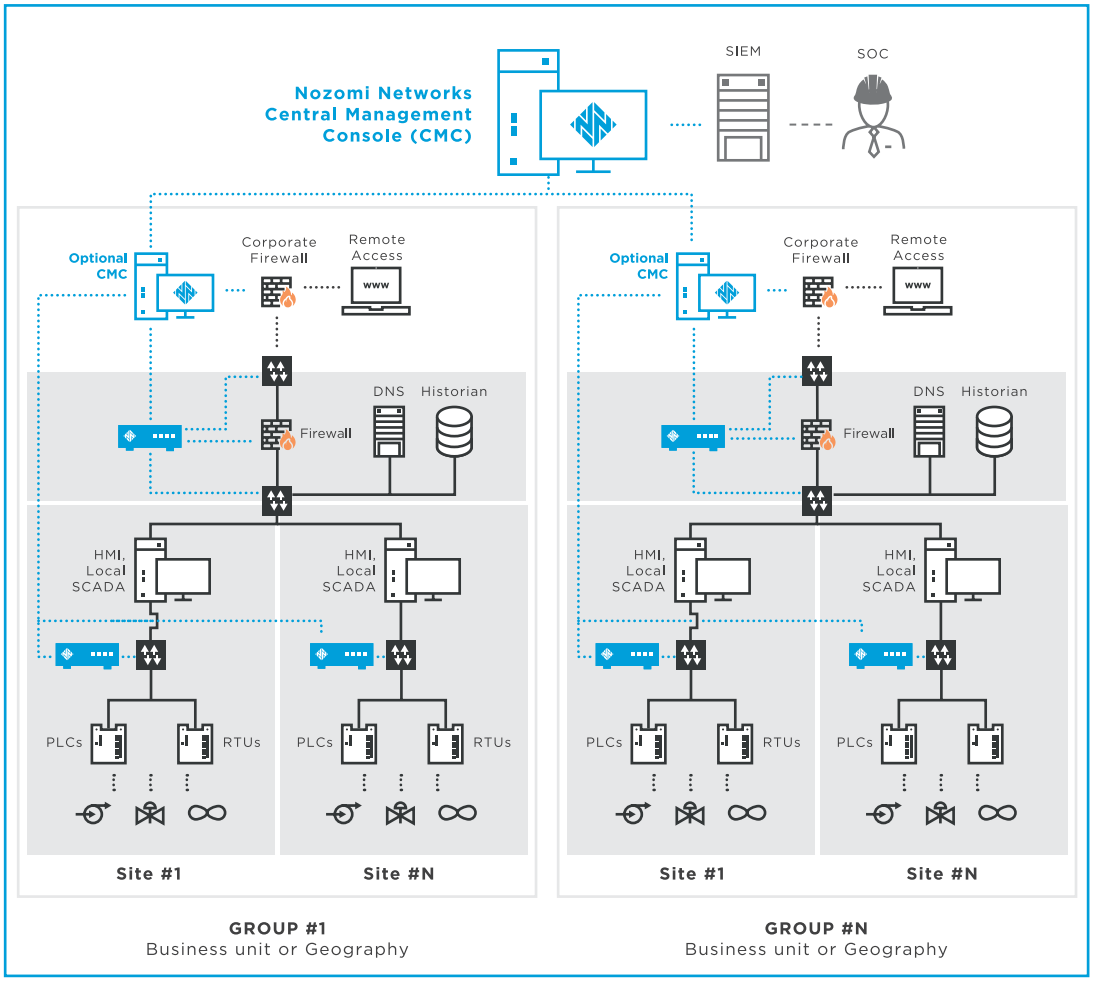
Central Management Console for Consolidated Cybersecurity Monitoring

- Scales to monitoring thousands of sites
- Consolidates ICS data flexibly using hierarchical aggregations
- Deploys, optionally, as a multitenant application

Easy IT/OT Integration

- Integrates seamlessly with IT/OT environments thanks to built-in integrations and easy-to-use API
- Includes SDK for extending protocol support

Sample Deployment Architecture



Nozomi Networks Products

SCADAguardian is a physical or virtual appliance that provides real-time cybersecurity and operational visibility of industrial control networks. The **Central Management Console (CMC)** aggregates data from multiple sites, providing centralized and remote cybersecurity management.

Together they deliver comprehensive ICS cyber resilience and reliability.

About Nozomi Networks

Nozomi Networks is revolutionizing Industrial Control System (ICS) cybersecurity with the most comprehensive platform to deliver real-time cybersecurity and operational visibility. Since 2013 the company has innovated the use of machine learning and artificial intelligence to secure critical infrastructure operations. Amid escalating threats targeting ICS, Nozomi Networks delivers one solution with real-time ICS monitoring, hybrid threat detection, process anomaly detection, industrial network visualization, asset inventory, and vulnerability assessment. Deployed in the world's largest industrial installations, customers benefit from advanced cybersecurity, improved operational reliability and enhanced IT/OT integration. Nozomi Networks is headquartered in San Francisco, California. Visit *www.nozominetworks.com*

NOZOMI NETWORKS

www.nozominetworks.com

@nozominetworks

© 2017 Nozomi Networks, Inc.
All Rights Reserved.

SB-8.5x11-004