NOZOMI NETWORKS

Data Sheet

Central Management Console

Consolidated OT Cybersecurity and Visibility Across Distributed Industrial Sites

- Centrally or Remotely Secure Large, Distributed Industrial Networks
- Automatically Track Industrial Assets and Cybersecurity Threats/Risks
- Significantly Reduce Troubleshooting and Forensic Efforts
- Readily Implement a Tailored Solution Using a Flexible Architecture
- Confidently Deploy at Enterprise Scale Thanks to Proven Performance
- Efficiently Track, Manage and Update SCADAguardian Appliances

Manage cybersecurity for distributed industrial installations with the Central Management Console (CMC). It provides consolidated and remote access to ICS data from field deployed SCADAguardian appliances.

Additionally, the CMC's multitenant capability allows enterprise customers with multiple business units, and Managed Security Service Providers (MSSPs), to monitor numerous sites using just one instance of the application.

The CMC uniquely provides:

- Centralized, scalable cybersecurity monitoring for thousands of industrial sites
- Consolidated best-in-class ICS threat and anomaly detection
- Remote access to ICS cybersecurity and process data
- Superior incident capture and forensic tools
- Easy integration and sharing of ICS and cybersecurity information with IT/OT environments

Find out how major customers have centralized ICS cybersecurity monitoring using the CMC, improving reliability, safety, cyber resiliency and operational efficiency.

Contact us today at nozominetworks.com/contact

Centralized Visibility and Threat Detection

- Actionable dashboards show key ICS cybersecurity and operational metrics
- Ad hoc query tool immediately provides answers regarding any aspect of network or process status

Scalable, Flexible Architecture

- Readily scales to thousands of industrial sites with optimal performance
- Flexible ICS data consolidation using hierarchical aggregations
- Includes multitenant configuration option

Enterprise-Class Solution

- Granular, role-based access control
- Built-in integration with SIEMs, firewalls and user authentication systems
- Easy integration with IT/OT environments via Open API and Protocol SDK
- Major installations at critical infrastructure, process control and manufacturing organizations

Value Delivered to Multinational Operators

Actionable Dashboards and Summaries

- Provides broad ICS network visibility within a single tool via 'at-a-glance' summaries
- Consolidates best-in-class ICS threat and anomaly detection results from distributed sites
- Enables real-time queries of any aspect of network or process status
- Identifies nodes most at risk with clear visual markers, including related alerts
- Eliminates the requirement for onsite data collection, saving time

Superior Incident and Forensic Tools

- Reduces troubleshooting and forensic efforts thanks to:
  - Smart grouping of alerts into root incidents
  - TimeMachine™ system snapshots
  - Real-time ad hoc query tool

Segregation of Duties

- Supports security best practices through the creation of user groups with granular permissions and restrictions
- Limits functionality permissions and visibility of network segments according to user roles

Timesaving Monitoring and Reporting

- Saves time through consolidation of compliance performance monitoring and reporting

Secure, Bandwidth Optimized Communication

- Encrypts communication between the CMC and SCADAguardian
- Optimizes data transfer bandwidth

Proven Value

Enel is a multinational energy company and one of the world's leading integrated electricity and gas operators. It operates in more than 30 countries across 4 continents and serves more than 61 million end users around the world.

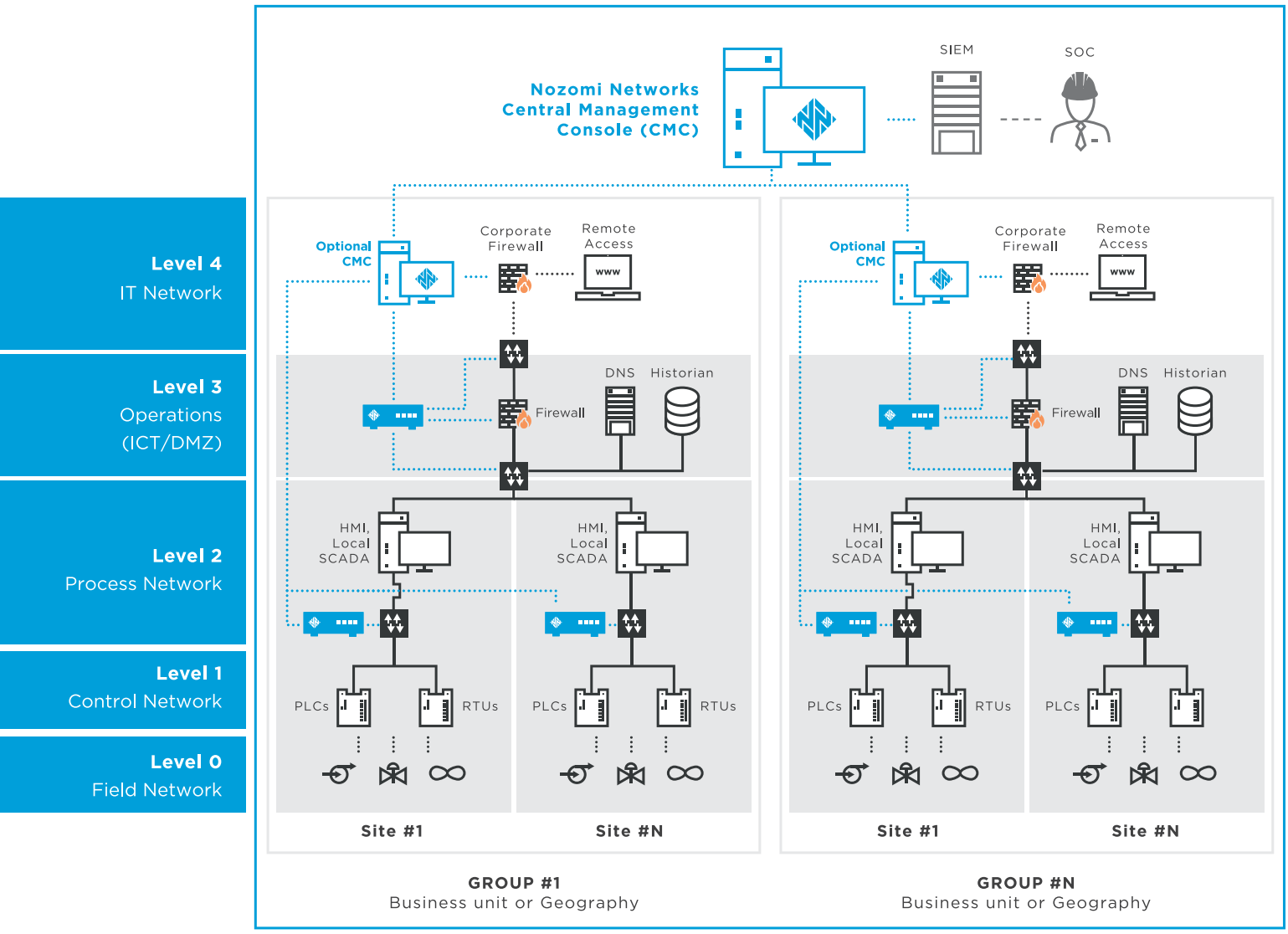
"With Nozomi Networks SCADAguardian we can now detect and collect operational and cybersecurity issues in real-time, and take corrective actions before the threat can strike."

Head of Cybersecurity Design
Enel

"Nozomi Networks SCADAguardian is now a fundamental element of our network infrastructure and an essential tool for our daily activities."

Head of Power Generation Remote Control System
Enel

Sample Deployment Architecture



Enterprise-Class Solution with Easy IT/OT Integration

- Monitor hundreds of SCADAguardian appliances
- Deploy CMCs in custom aggregations or across multiple tenants to meet your needs
- Install the CMC virtual appliance on any operating system or hardware
- Depend on a product fully optimized for enterprise performance and stability
- Manage SCADAguardian software with upgrade and rollback version control functionality
- Share ICS data via built-in integrations with SIEMs (HPE ArcSight, IBM QRadar, Splunk, etc.), firewalls (Check Point, Fortinet, Palo Alto Networks, etc.) and user authentication systems (Active Directory, LDAP, etc.)
- Exchange data with other IT/ICS applications using the Open API

Virtual Appliance is Easy to Deploy and Scalable

CENTRAL MANAGEMENT CONSOLE	
Summary	Consolidated and remote ICS cybersecurity and visibility for distributed industrial sites.
Installation Specs	AWS EC2, Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+
Max Managed Appliances	Unlimited (*)
Storage	100+ Gb
Updates	Optionally connect to the Nozomi Networks customer portal for vulnerability, rules and SCADAguardian updates. Easily propagate changes to all appliances in the field.

(*) Based on infrastructure. Visit **nozominetworks.com** for the latest technical specifications.

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

DS-CMC-8.5x11-004