NOZOMI NETWORKS

Data Sheet

# SCADAguardian™

## Real-time Cybersecurity and Visibility for Industrial Control Networks

- Automatically Track Industrial Assets and Know Their Cybersecurity Risks
- Quickly Monitor ICS Networks and Processes with Real-time Insights
- Readily Implement a Tailored Solution Using Multiple Appliance Models
- Rapidly Detect Cyber Threats/Risks and Process Anomalies
- Significantly Reduce Troubleshooting and Forensic Efforts
- Easily Integrate and Share ICS Information with IT/OT Environments

Protect your control networks from cyberattacks and operational disruptions with SCADAguardian. It provides unprecedented operational visibility and rapid detection of cyber threats and process risks – and does it in a completely passive way.

SCADAguardian automatically discovers your entire industrial network, including assets, connections, protocols and topology. It monitors network communications and behavior for risks that threaten reliability and cybersecurity, and provides the information you need to respond quickly.

**SCADAguardian uniquely provides:**

- Superior asset identification, network visualization and real-time monitoring
- Best-in-class ICS threat detection using a hybrid approach
- Enterprise-class scalability when deployed with the related Central Management Console
- Easy integration and sharing of ICS and cybersecurity information with IT/OT infrastructure

Find out how customers improve the reliability, cybersecurity and operational efficiency of their facilities with SCADAguardian.

**Contact us today at nozominetworks.com/contact**

### 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
- Monitors and reduces OT risks in sectors such as critical infrastructure, energy, manufacturing, mining, transportation and utilities

### Time-Saving Forensic Tools

- Dynamic learning that reduces false alerts
- Automatic packet capture
- TimeMachine™ system snapshots
- Real-time ad hoc query tool

## Five Modules Deliver ICS Cybersecurity and Operational Visibility

### Real-time Network Visualization

- Improve system awareness with a visualization interface that shows assets, links, protocols and topologies

### Superior Asset Inventory

- Auto-discovery of assets provides detailed, accurate information that is always up-to-date
- Asset views make it easy to visualize, find and drill down on asset information

### Automated Vulnerability Assessment

- Automated identification of device vulnerabilities saves time and improves cyber resiliency

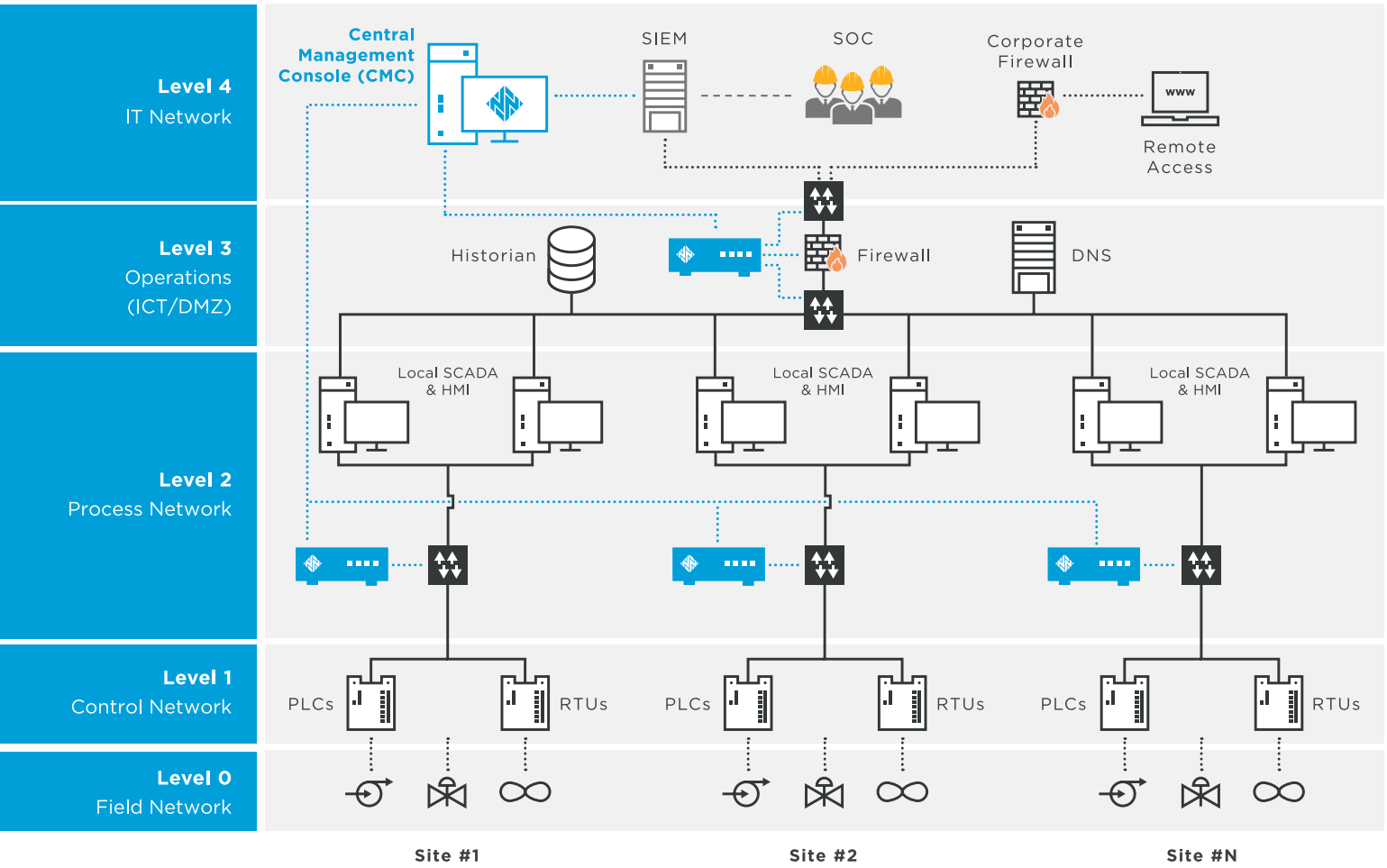
### Informative Dashboards and Queries

- Custom dashboards, detailed reports and ad hoc querying provide real-time visibility that improves both cybersecurity and operational efficiency

### The Best ICS Threat Detection

- Hybrid threat detection combines behavior-based anomaly detection with rules-based threat detection (YaraRules, SNORT-like Packet Rules and Assertions) to identify cybersecurity and process risks and threats
- All detection results are correlated and combined with operational context for detailed insight and rapid remediation
- Detect intrusions: scanning and MITM attacks, complex or zero-day attacks, known malware files or packets, DDoS attacks and more
- Detect unauthorized behavior: remote access, configuration changes, downloads, controller logic changes, edits to PLC projects and more
- Detect states of concern: misconfigurations, weak passwords, missing updates, open ports, communication failures, malfunctions and more

## Sample Deployment Architecture



## Immediate Value Delivered to Multinational Organizations

### Automated ICS Modeling

- Installs passively by connecting to network devices via SPAN or mirror ports
- Learns and models large heterogeneous ICS
- Identifies assets with a high degree of detail and accuracy, and triggers change alerts

### Dynamic Learning

- Switches from learning to protection mode automatically, providing quick risk detection

### Superior Operational Visibility

- Provides real-time network visualization, including interactive topology filtering
- Monitors assets, communications and processes
- Presents actionable information in dashboards
- Allows real-time querying of any aspect of network or ICS performance, reducing spreadsheet work

### Easy Integration with IT/OT Environments

- Includes built-in integration with IT/OT infrastructure: 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 SDK
- Exports data for analysis and presentation in other applications
- Adapts for each installation with customizable components

### Fast ROI

- Deploys quickly, without network changes
- Delivers immediate value at large, distributed installations, monitoring thousands of devices

## Multiple SCADAguardian™ Appliance Formats to Meet Your Needs

| PHYSICAL APPLIANCES | | | | | | |
|---|---|---|---|---|---|---|
| | N Series | | NSG-L Series | | NSG-R Series | R Series |
| |  1000 |  750 |  250 |  100 |  150 NEW |  50 |
| **Description** | *A powerful appliance for very large, demanding scenarios* | *A rack-mounted appliance for large scenarios* | *A rack-mounted appliance for medium scenarios* | *A rack-mounted appliance for small scenarios* | *A rugged rack-mounted appliance for medium scenarios* | *A rugged DIN-rail mounted appliance for small scenarios* |
| **Form Factor** | 1 Rack Unit | 1 Rack Unit | 1 Rack Unit | 1 Rack Unit | 2 Rack Units | DIN Mountable |
| **Monitoring Ports** | 8 | 4 | 5 | 5 | 7 | 4 |
| **Expansion slots** | n.a. | n.a. | 1 | 1 | 2 | n.a. |
| **Max Protected Nodes** | 5,000 | 1,000 | 500 | 200 | 450 | 200 |
| **Max Throughput** | 1 Gbps | 500 Mbps | 200 Mbps | 100 Mbps | 200 Mbps | 50 Mbps |
| **Storage** | 240 Gb | 180 Gb | 64 Gb | 64 Gb | 64 Gb | 64 Gb |
| **HxWxL (mm/in)** | 43 x 426 x 356<br>1.7 x 16.8 x 14 | 43 x 426 x 356<br>1.7 x 16.8 x 14 | 44 x 438 x 300<br>1.7 x 17.2 x 11.8 | 44 x 438 x 300<br>1.7 x 17.2 x 11.8 | 88 x 440 x 301.2<br>3.46 x 17.3 x 118.58 | 80 x 130 x 146<br>3.15 x 5.11 x 5.74 |
| **Weight** | 10 Kg | 10 Kg | 8 Kg | 8 Kg | 6 Kg | 3 Kg |
| **Max Power Consumption** | 260W | 260W | 250W | 250W | 60W | 60W |
| **Power Supply Type** | 110-240V AC | 110-240V AC | 110-240V AC | 110-240V AC | Dual Power Mode:<br>1) 36-48V DC<br>2) 90-264V AC / 100-300V DC | 12-36V DC |
| **Temperature Ranges** | 0 / +45º C | 0 / +45º C | 0 / +40º C | 0 / +40º C | -40 / +70º C | -40 / +70º C |
| **Compliance** | RoHS | RoHS | RoHS | RoHS | RoHS, IEC 61850-3, IEEE 1613 | RoHS |

## VIRTUAL APPLIANCES

| |  V1000 |  V750 |  V250 |  V100 |  V50 |
|---|---|---|---|---|---|
| **Description** | *A powerful appliance for very large, demanding scenarios* | *A virtual appliance for large scenarios* | *A virtual appliance for medium scenarios* | *A virtual appliance for small scenarios* | *A virtual appliance for very small scenarios* |
| **Installation Specs** | Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+ | | | | |
| **Monitoring Ports** | Unlimited (*) | 4 | 4 | 4 | 4 |
| **Max Throughput** | 300 Mbps | 300 Mbps | 300 Mbps | 300 Mbps | 300 Mbps |
| **Max Protected Nodes** | 5,000 | 1,000 | 500 | 200 | 200 |
| **Storage** | 100+ Gb | 100+ Gb | 100+ Gb | 100+ Gb | 100+ Gb |

(*) Limitation on the Number of ports can be present due to the version of the Virtual Infrastructure Firmware

## Broad Support for Industrial Control Systems and ICS / IT Protocols

| | |
|---|---|
| **ICS Vendors** | ABB, Allen-Bradley/Rockwell, Bristol Babcock, Beckhoff, Emerson, General Electric, Honeywell, IBM, Mitsubishi, Motorola, Rockwell Automation, Schneider Electric, Siemens, Yokogawa |
| **ICS Protocols** | ABB PGP2PGP, Aspentech Cim/IO, BACNet, Beckhoff ADS, BSAP IP, CC-LINK IE, CEI 79-5/2-3, COTP, DNP3, Emerson DeltaV, Enron Modbus, EtherCAT, EtherNet/IP - CIP, Foundation Fieldbus, Foxboro IA, Generic MMS, GE EGD, GE iFix2iFix, GE SRTP, GOOSE, Honeywell Experion protocols, Kongsberg Net/IO, IEC 60870-5-7 (IEC 62351-3 + IEC 62351-5), IEC 60870-5-104, IEC-61850 (MMS, GOOSE, SV), IEC DLMS/COSEM, ICCP, Modbus/RTU, Modbus/TCP, Modbus/TCP - Schneider Unity extensions, MQTT, OPC, PCCC, PI-Connect, Profinet/DCP, Profinet/I-O CM, Profinet/RT, ROC, Sercos III, Siemens S7, S7 Plus, Telvent OASyS DNA, Triconex TSAA, Vnet/IP |
| **IT Protocols** | ARP, Bittorrent, BROWSER, CDP, DCE-RPC, DHCP, DNS, DRDA (IBM DB2), Dropbox, eDonkey (eMule), FTP, FTPS, GVCP, HTTP, HTTPS, ICMP/PING, IGMP, IKE, Indigo Vision, IMAP, IMAPS, ISO-TSAP/COTP, Kerberos, KMS, LDAP, LDAPS, LLDP, LLMNR, MDNS, Mitsubishi Melsoft, Mitsubishi SLMP, NTP, MS SQL Server, MySQL, NetBIOS, NTP, OSPF, POP3, PTPv2, RDP, STP, RTCP, RTP, SSH, SNMP, SMB, SMTP, SSDP, STP, Symantec Endpoint Manager, Syslog, TeamViewer, Telnet, TNS, VNC |

Support for additional systems and protocols is constantly being expanded. Visit **nozominetworks.com/techspecs** for the latest technical specifications.
Further protocols can be quickly added using the Protocol SDK.

## 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



DS-SG-8.5x11-006