NOZOMI NETWORKS

Data Sheet

SCADAguardian™

Real-time Cybersecurity and Visibility for Industrial Control Networks

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

Protect your control networks from cyberattacks and operational disruptions with SCADAguardian. It rapidly detects cyber threats and process anomalies, providing unprecedented operational visibility.

SCADAguardian automatically discovers the industrial network including its components, connections and topology. It develops security and process profiles and monitors the system in real-time for any changes.

SCADAguardian uniquely provides:

- Comprehensive, hybrid ICS threat detection that combines behavior-based, rules, signatures and artificial intelligence analysis
- Superior incident capture and forensic tools
- Easy integration and sharing of ICS and cybersecurity information with IT/OT environments
- Enterprise-class scalability when deployed with the related Central Management Console

Find out how major customers have improved reliability, safety, cybersecurity and operational efficiency with SCADAguardian.

Contact us today at nozominetworks.com/contact

Hybrid ICS Threat Detection

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

Operational ICS Visibility

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

Superior Incident and Forensic Tools

- Dynamic learning minimizes false alerts
- Smart grouping of alerts into incidents
- Automatic packet capture
- TimeMachine™ system snapshots
- Real-time ad hoc query tool

Industries

- Major installations at critical infrastructure, process control and manufacturing organizations

Five Modules Deliver ICS Cybersecurity and Operational Visibility

Network Visualization and Modeling

- Improve system and process awareness with a visualization interface that shows all assets and links

Asset Inventory

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

Vulnerability Assessment

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

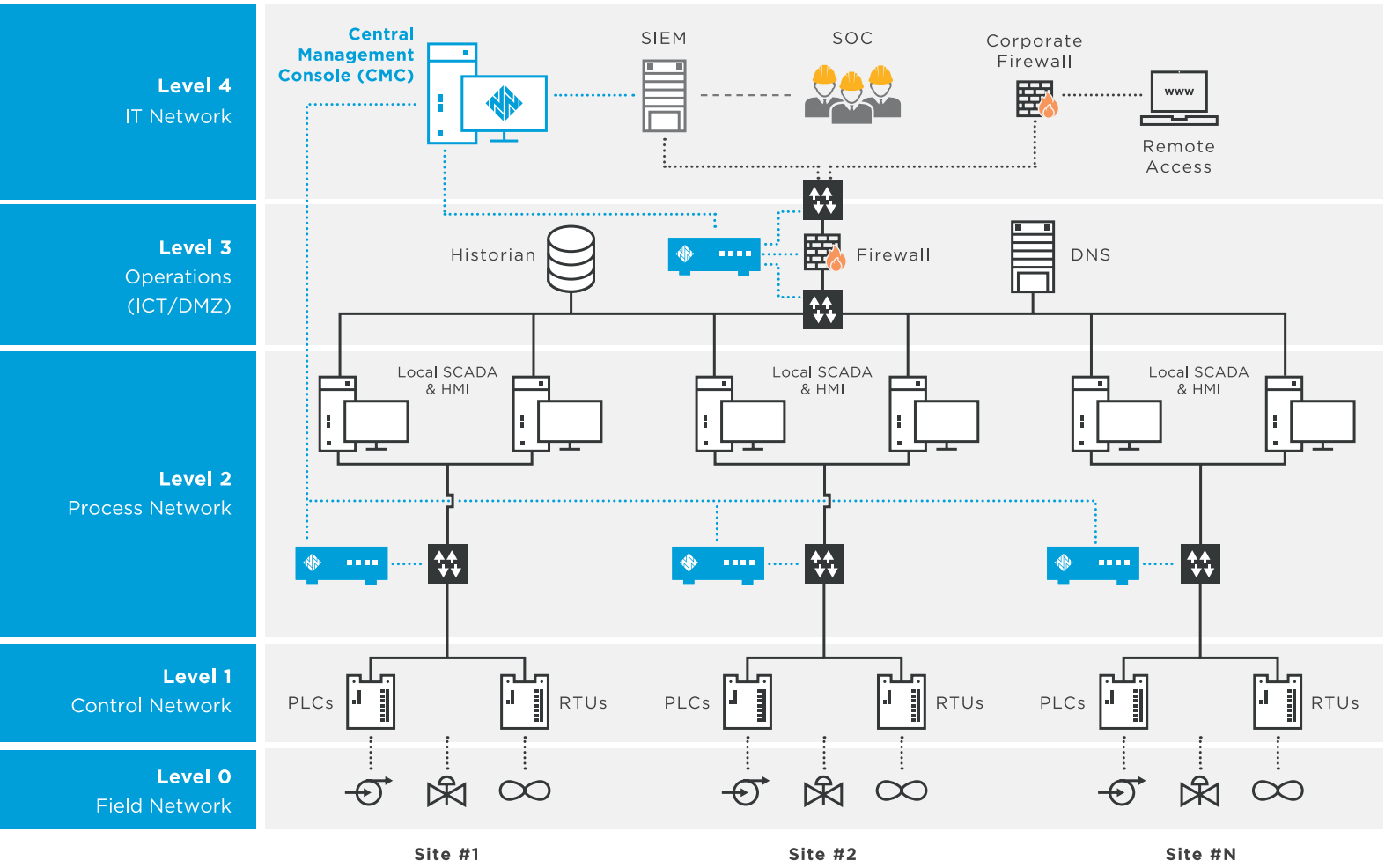
Dashboards and Reporting

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

ICS Threat and Anomaly Detection

- Rapidly detect cybersecurity threats, risks and process anomalies
- Hybrid threat detection combines best-in-class behavior-based anomaly detection with rules-based threat detection (YaraRules, Packet Rules and Assertions) and artificial intelligence analysis
- Detect intrusions: Scanning and MITM attacks · Complex or zero-day attacks · Known malware files or packets and more
- Detect unauthorized behavior: Remote access · Configurations · 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



Value Delivered to Multinational Operators

Automated ICS Modeling

- Installs passively and non-intrusively by connecting to network devices via SPAN or mirror ports
- Learns and models large heterogeneous ICS
- Identifies all assets and triggers alerts on changes

Dynamic Learning

- Switches from learning to protection mode automatically, starting anomaly detection quickly

Operational Visibility

- Provides real-time network visualization, including topology
- 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:
  - SIEMs: HPE ArcSight, IBM QRadar, Splunk, etc.
  - Firewalls: Check Point, Fortinet, Palo Alto Networks, etc.
  - User Authentication: Active Directory, LDAP, etc.
- Exchanges data with other IT/ICS applications via an Open API
- Includes built-in support for dozens of protocols, extends to others via the Protocol SDK
- Exports data for analysis and presentation in other applications
- Adapts for each installation with many customizable components

Fast ROI

- Deploys quickly, with no network changes
- Delivers value at numerous customer sites, with centralized monitoring of tens of thousands of industrial 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 1.7 x 16.8 x 14	43 x 426 x 356 1.7 x 16.8 x 14	44 x 438 x 300 1.7 x 17.2 x 11.8	44 x 438 x 300 1.7 x 17.2 x 11.8	88 x 440 x 301.2 3.46 x 17.3 x 118.58	80 x 130 x 146 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: 1) 36-48V DC 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	400	150	50
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	Aspentech Cim/IO, BACNet, Beckhoff ADS, BSAP IP, CEI 79-5/2-3, COTP, DNP3, Emerson DeltaV, Enron Modbus, EtherCAT, EtherNet/IP - CIP, Foundation Fieldbus, Foxboro IA, Generic MMS, GOOSE, Honeywell, 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, MQTT, OPC, PI-Connect, Profinet/DCP, Profinet/I-O CM, Profinet/RT, Sercos III, Siemens S7, Vnet/IP
IT Protocols	ARP, BROWSER, Bittorrent, CDP, DCE-RPC, DHCP, DNS, DRDA (IBM DB2), Dropbox, eDonkey (eMule), FTP, FTPS, GVCP, HTTP, HTTPS, ICMP/PING, IGMP, IKE, IMAP, IMAPS, ISO-TSAP/COTP, Kerberos, KMS, LDAP, LDAPS, LLDP, LLMNR, MDNS, MS SQL Server, MySQL, NetBIOS, NTP, OSPF, POP3, PTPv2, RDP, STP, SSDP, RTCP, RTP, SSH, SNMP, SMB, SMTP, STP, Syslog, Telnet, VNC

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

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-SG-8.5x11-005