NOZOMI NETWORKS

Data Sheet
SCADAguardian™

Real-time Cybersecurity and Visibility for Industrial Control Networks

Protect your control network from cyberattacks and operational disruptions with SCADAguardian. It rapidly detects cyberattacks and process anomalies, providing unprecedented operational visibility. SCADAguardian's up-to-the-minute insights help you improve cyber resiliency, reliability and safety.

Automated Real-time Modeling of Your ICS, Process and Assets

- Installs non-intrusively with no downtime or network disruption
- Connects to network devices via SPAN or mirror ports
- Learns and models large, heterogeneous ICS automatically, creating baseline security and process profiles
- Identifies and knows every system asset from every vendor
- Provides detailed information on each asset and its communications
- Presents assets in dedicated views that are easy to sort and search
- Triggers alerts when assets change, such as configuration, firewall or device modifications

Operational Visibility that Protects Reliability and Saves Time

- Provides real-time network visualization, including topology
- Monitors assets, communications, and underlying industrial processes
- Presents actionable information in customizable dashboards including consolidating alerts into context-aware incidents
- Allows real-time querying of any aspect of network or ICS performance, significantly reducing spreadsheet work and plant floor data collection
- Provides advance notice of failing equipment
- Reduces troubleshooting and remediation efforts. Assists forensics investigations thanks to ICS incident replay and archiving

Rapid Identification of Cybersecurity and Process Anomalies

Detects Intrusions

Scanning and MITM attacks • Complex or zero day attacks

Detects Unauthorized Behavior

Remote access • Configurations • Downloads • Controller logic changes • Edits to PLC projects • Connections to Internet or enterprise network • PLC authentication and more

Detects Vulnerabilities

Automated identification of assets with vulnerabilities • Dedicated, searchable view of all vulnerabilities with severities

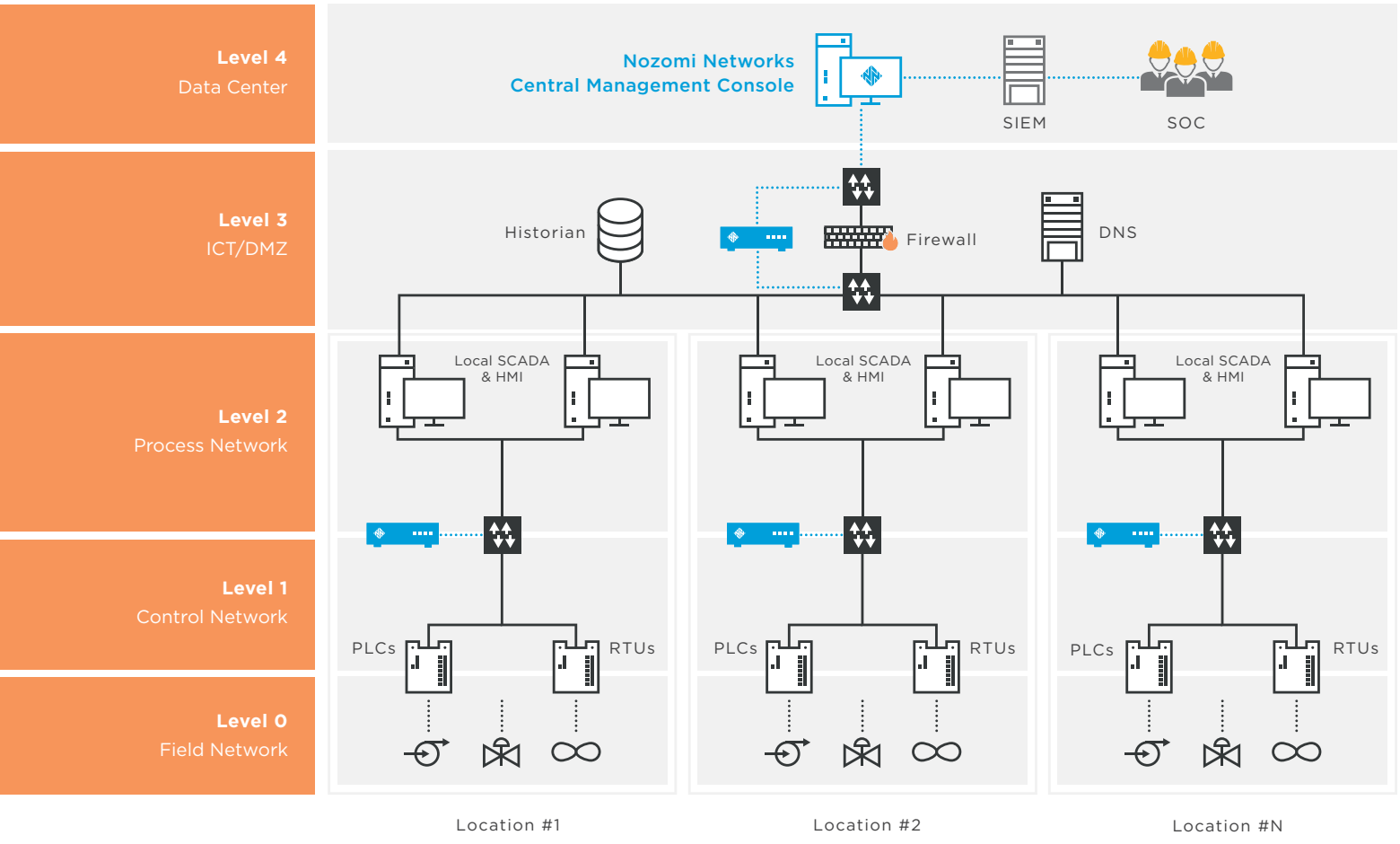
Detects Incidents or States of Concern

Misconfigurations • Weak passwords or configurations • Missing patches • Known vulnerabilities • Open ports • New or non-responsive assets • Cross level or zone communication • Device generated traffic storms • Malfunctions Insecure Internet communication • Unencrypted communication • Communication failures

Learns Automatically

Manual input not required to switch product from learning to protection mode • Anomaly detection and cybersecurity monitoring begin as quickly as possible

Sample Architecture



Value Delivered to Multisite, Multinational Operators

Meets Enterprise Requirements

- Scales to hundreds of sites, with aggregated information accessible using the SCADAguardian Central Management Console
- Provides advance, upgrade and rollback version control functionality
- Includes role-based access control for users and managed service providers
- Delivers optimal performance with fast responses to complex queries and rapid handling of continuous compliance checks

Integrates with Security Infrastructure

- SIEMs: HP ArcSight, Splunk, IBM QRadar
- User Authentication: Active Directory, LDAP
- Firewalls: Fortinet, Check Point

Delivers Fast ROI

- Deployed today at dozens of customer sites, monitoring tens of thousands of industrial devices spanning the oil & gas, electric utilities, manufacturing and transportation sectors

Multiple SCADAguardian™ Appliance Formats to Meet Your Needs

N1000

N750

R50

P500

PHYSICAL APPLIANCES	N1000	N750	R50	P500
Description	*This powerful appliance covers the most challenging scenarios.*	*This appliance covers small to medium scenarios.*	*This appliance covers very small scenarios.*	*A portable probe for temporary analysis of network trunks.*
Form Factor	1 Rack Unit	1 Rack Unit	DIN mountable	Portable Form Factor
Monitoring Ports	8	4	4	5
Max Throughput	1 Gbps	500 Mbps	50 Mbps	200 Mbps
Max Protected Nodes	10,000	1,000	200	250 (*)
Storage	240 Gb	180 Gb	64 Gb	180 Gb
H x W x L (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	80 x 130 x 146 3.15 x 5.11 x 5.74	93 x 202 x 200 3.66 x 7.95 x 7.87
Weight	10 Kg	10 Kg	3 Kg	5 Kg
Max Power Consumption	260W	260W	60W	100W
Power Supply Type	110-240V AC	110-240V AC	12-36V DC	110-240V AC
Temperature Ranges	0 / +45º C	0 / +45º C	-40 / +70º C	0 / +50º C
RoHS Conformity	Yes	Yes	Yes	Yes

(*) Plus other limitations

VIRTUAL APPLIANCES

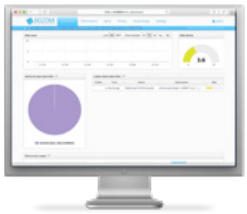
	V1000	V750	V250	V50
Description	*This appliance covers most challenging scenarios.*	*This appliance covers medium scenarios.*	*This appliance covers small to medium scenarios.*	*This appliance covers small scenarios.*
Installation Specs	VMware ESX 5.x+, Hyper-V 2012+, KVM, XEN			
Monitoring Ports	Unlimited (**)	4	4	4
Max Throughput	300 Mbps	300 Mbps	300 Mbps	300 Mbps
Max Protected Nodes	10,000	1,000	300	50
Storage	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

CENTRAL MANAGEMENT CONSOLE

Description	*CMC- The Virtual Appliance permits centralized control in a distributed installation.*
Installation Specs	VMware ESX 5.x+, Hyper-V 2012+, KVM 1.2+, XEN 4.4+XEN
Max Managed Appliances	Unlimited (***)
Storage	100+ Gb

(***) Based on the infrastructure



Broad Support for Industrial Control Systems and ICS / IT Protocols

ICS Vendors¯	Industrial Protocols¯°	IT Protocols¯
ABB, Allen-Bradley/Rockwell, Beckhoff, Emerson, General Electrics, Honeywell, Mitsubishi, Motorola, Rockwell Automation, Schneider Electric, Siemens, Yokogawa	Aspentech Cim/IO, Beckhoff ADS, CEI 79-5/2-3, DNP3, EtherNet/IP - CIP, Foundation Fieldbus, Honeywell, ICCP, IEC-60870-5-104, IEC-61850 (MMS, GOOSE, SMV), Modbus/TCP, MMS, OPC, PI-Connect, Profinet, Siemens S7	BitTorrent, DCE-RCP, DHCP, DNS, Dropbox, eDonkey (eMule), FTP, FTPS, HTTP, HTTPS, IMAP, IMAPS, ISO-TSAP/COTP, Kerberos, KMS, LDAP, LDAPS, MS SQL Server, MySQL, NetBIOS, NTP, POP3, RemoteDesktop, SSH, SMB, SMTP, SNMP (full parsing of MIBS), STP, Syslog, Telnet, VNC

¯ Support for additional systems and protocols is constantly being expanded. Check with your Nozomi Networks' representative or partner for the latest list.
° Support for other industrial protocols can be quickly added.

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 meet the unique challenges of critical infrastructure operations. Nozomi Networks delivers both cybersecurity and process anomaly detection along with industrial network visualization and monitoring, asset inventory, and vulnerability assessment. Deployed in the world's largest industrial installations, customers benefit from enhanced cybersecurity and improved operational reliability with one end-to-end solution. Nozomi Networks is headquartered in San Francisco, California. *www.nozominetworks.com*

NOZOMI NETWORKS

www.nozominetworks.com
@nozominetworks

DS-SG-8.5x11-002