NOZOMI NETWORKS

Solution Brief

Real-time ICS Cybersecurity and Visibility for MSSPs & MDRs

- Confidently Use a Solution Designed Specifically for OT
- Quickly Monitor ICS Networks and Processes with Real-time Insights
- Readily Implement Custom Solutions with Flexible Architecture
- Rapidly Detect & Hunt Cyber Threats Using a Best-in-Class Solution
- Efficiently Act on ICS Cybersecurity Threats and Risks
- Easily Provide Exceptional Forensics and Troubleshooting Services

As the cybersecurity risk to critical infrastructure and manufacturing organizations increases, it's more important than ever for enterprises to actively monitor and secure OT networks.

To answer this need, Managed Security Service Providers (MSSPs) and Managed Detection and Response (MDR) vendors are expanding their managed IT services to encompass industrial networks. This is not merely a matter of extending existing tools and practices to industrial control systems (ICS), however.

Effectively serving this market requires products that address the unique challenges of managing 24/7/365 operational systems where availability is often a bigger concern than confidentiality or integrity.

Furthermore, ICS often include legacy systems and the use of insecure industrial protocols – neither of which can be monitored or managed using IT solutions.

Nozomi Networks is the multitenant ICS cybersecurity and visibility vendor of choice because we thoroughly understand industrial networks and processes. Our technology is completely safe for ICS and delivers superior visibility, real-time network monitoring and threat detection.

Contact us today at: nozominetworks.com/contact

Superior Visibility & Forensic Tools

- Automated, accurate asset inventory
- Intuitive network visualization
- Real-time monitoring of threats, assets and communications
- Customizable dashboards and alerts
- Real-time ad hoc query tool
- Time Machine™ system snapshots
- Automatic packet capture

The Best ICS Threat Detection

- Behavior-based anomaly detection
- Rules and signature-based detection
- Advanced correlation for detailed insights and rapid remediation
- Multiple tools for threat hunting

Flexible, Scalable Architecture

- Multitenant application designed for powering service offerings with shared infrastructure
- High availability (HA) solution
- Flexible deployment options
- Easy-to-use open API

Why Select Nozomi Networks to Power Your Managed OT Security Services

Flexible, Scalable Architecture

Reduce cyber security risk for your clients using the Nozomi Networks solution:

- Consolidate cybersecurity visibility across hundreds of industrial facilities
- Deploy to fit each client's business with multiple appliance formats and flexible aggregations of ICS data
- Deliver optimal performance with a full stack technology solution

Easy Integration with IT/OT Environments

- Leverage built-in integrations with asset management systems, firewalls, SIEMs and more
- Integrate and exchange data with other applications via an open API
- Support dozens of IT and ICS protocols and extend to others via a Protocol SDK
- Export data for analysis and presentation in other applications
- Adapt for each client with customizable components

The Best ICS Threat Detection

Nozomi Networks hybrid threat detection combines:

- Behavior-based anomaly detection
- Rules and signature-based threat detection
- Advanced correlation of threats for rapid mitigation

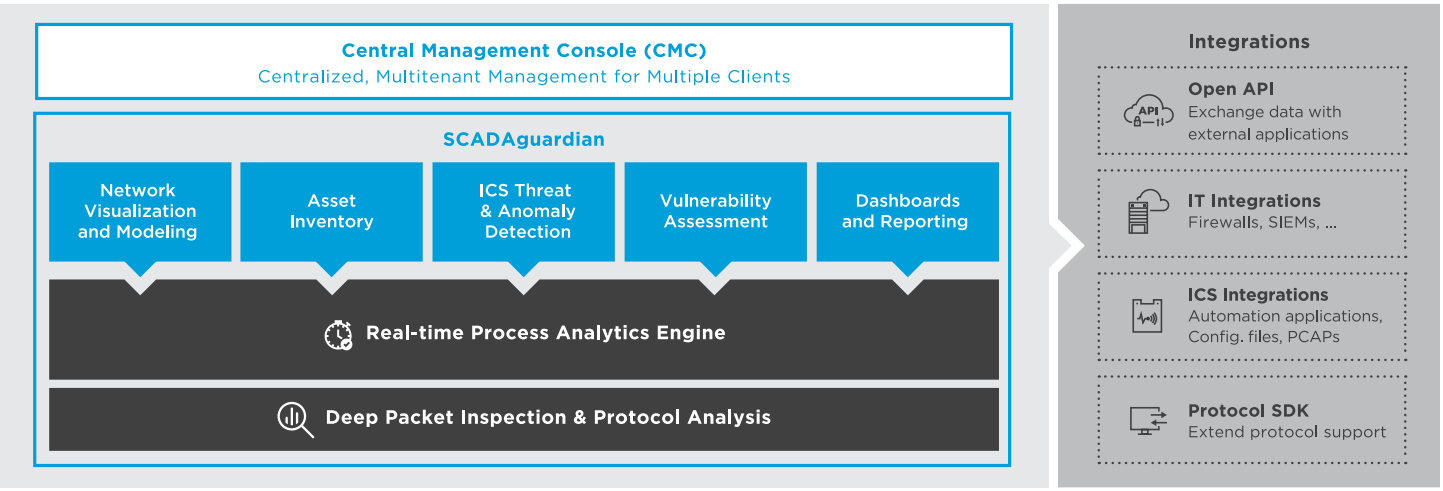
Examples of threats and risks identified include:

- Intrusions: scanning and MITM attacks, zero-day attacks, advanced persistent threats, known malware files / packets, DDos attacks and more
- Unauthorized behavior: remote access, configuration changes, field device manipulation, downloads and more
- States of concern: critical states involving multiple variables, weak passwords, missing updates, open ports, device vulnerabilities and more

Time-Saving Forensic Tools

- Custom assertions (rules) check any aspect of network or process status
- Automatic packet captures speed analysis
- TimeMachine™ system snapshots compare the entire industrial network at multiple points in time

The Nozomi Networks Solution Architecture



Deep Packet Inspection & Protocol Analysis - Evaluates insecure ICS communications at all 7 layers of OSI model
Real-time Process Analytics Engine - Analyzes process control variables for indications of advanced malware activity and critical states that could impact reliability
SCADAguardian - Deploys as a secure appliance in clients' industrial networks and passively analyzes traffic
Central Management Console (CMC) - Provides MSSP / MDR SOCs with ICS visibility and actionable threat intelligence
Integrations - Enables easy integration with IT/OT infrastructure

Why Your Clients Want the Nozomi Networks Solution

Passive, Easy-to-Deploy Solution

- Installs passively by connecting to network devices via SPAN or mirror ports
- Deploys easily without network changes
- Fits client installations thanks to a wide range of SCADAguardian appliances

Rapid, Real-time Monitoring of Threats and Risks

- Uses artificial intelligence to automatically learn and model clients' large, heterogeneous ICS
- Monitors threats, ICS protocol communications, assets and processes in real-time
- Switches from learning to protection mode automatically (Dynamic Learning), enabling MSSPs and MDRs to quickly provide protective services

Enterprise-Class Deployments

- 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
- Fast, flexible deployments with immediate ROI

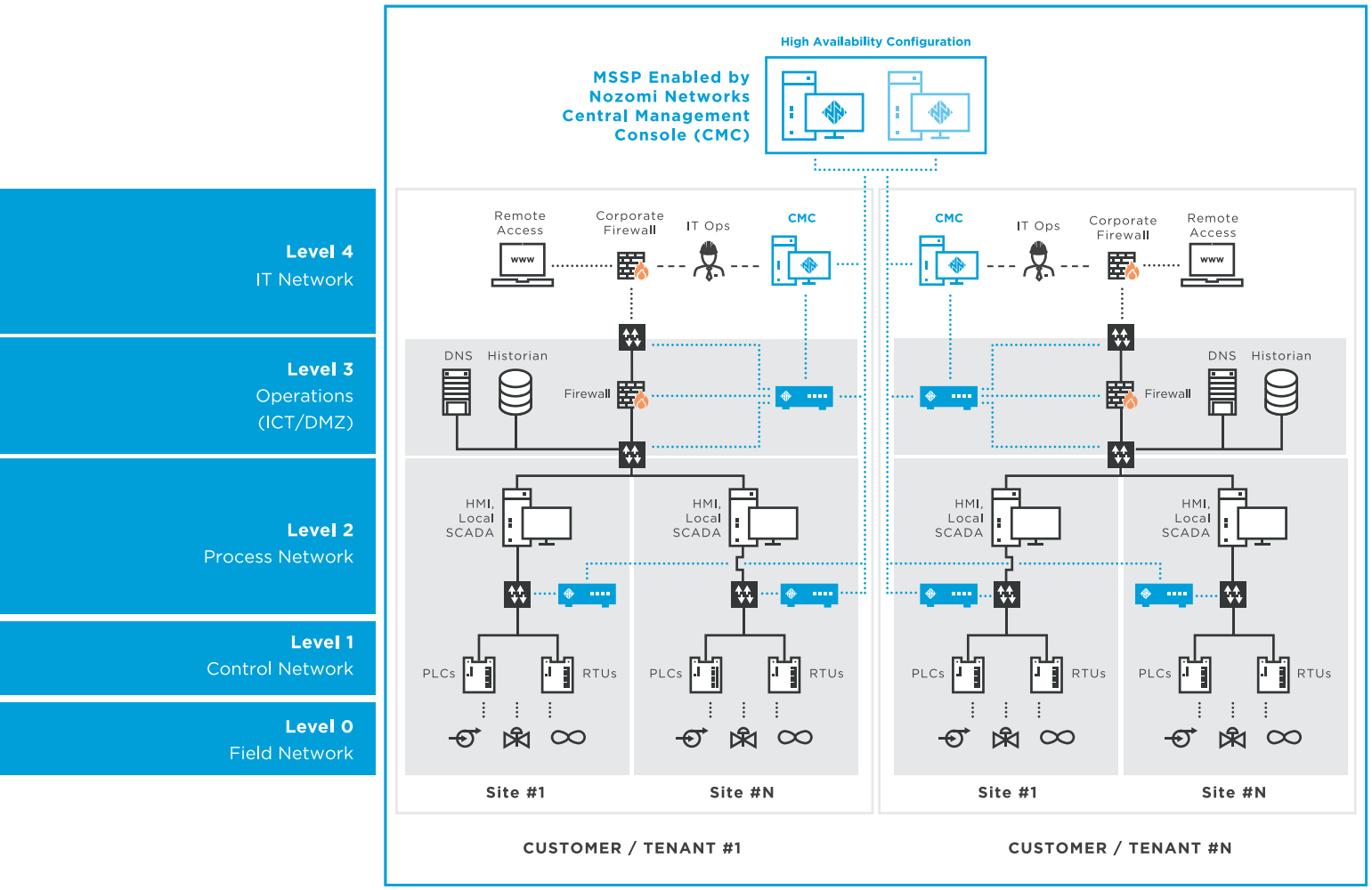
Reliability and Availability

- Addresses ICS operators' key concern – reduced reliability due to cyber incidents
- Identifies cyber risks and process anomalies that could reduce availability, such as malfunctioning equipment

Trusted Partner That Addresses ICS Risk

- Solves the ICS cybersecurity challenge by enabling trusted MSSP or MDR providers to deliver both IT and ICS security services

Sample Deployment Architecture



The Virtual, Multitenant CMC is Easy to Deploy and Scalable

Summary	Multitenant ICS visibility and actionable threat intelligence for MSSPs and MDRs.		
Installation Specs	Amazon AWS AMI, 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.		

Multiple SCADAguardian™ Appliance Formats For Every Type of Deployment

PHYSICAL APPLIANCES

	 N1000	 N750	 NSG-L 250	 NSG-L 100	 NSG-R 150 NEW	 R50
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*
Monitoring Ports	8	4	5	5	7	4
Max Protected Nodes	5,000	1,000	500	200	450	200

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*
Monitoring Ports	Unlimited (*)	4	4	4	4
Max Protected Nodes	5,000	1,000	500	200	200

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

Nozomi Networks Products

The Central Management Console (CMC) provides MSSP / MDR SOCs with centralized and remote OT cybersecurity and monitoring. It is a secure, multitenant, HA application that aggregates data from hundreds of industrial facilities.

SCADAguardian provides real-time cybersecurity and operational visibility for industrial control networks. It is passively deployed in your clients' industrial networks and can be accessed locally, or remotely through the CMC.

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

MSSP-SB-8.5x11-004