NOZOMI NETWORKS

Solution Brief

Real-time ICS Cybersecurity and Visibility for MSSPs & MDRs

- Confidently Use a Solution Designed for OT
- Rapidly Detect & Hunt Cyber Threats Using Best-in-Class Solution
- Quickly Monitor ICS Networks and Processes with Real-time Insight
- Efficiently Act on ICS Cybersecurity Threats and Risks
- Readily Implement Custom Solutions with Flexible Architecture
- Provide Superior Troubleshooting and Forensic 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 help meet this need, Managed Security Service Providers (MSSPs) and Managed Detection and Response (MDRs) vendors are expanding their managed IT services to encompass industrial networks. Doing so is not merely a matter of extending existing tools and practices to Industrial Control Systems (ICS), however.

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

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

Nozomi Networks is the ideal provider of a multitenant ICS cybersecurity and visibility solution because we thoroughly understand industrial networks and processes. Our technology is completely passive, making it the safest and most effective solution for sensitive control networks.

Contact us today to find why global industrial MSSPs / MDRs select our solution: nozominetworks.com/contact

Flexible, Scalable Architecture

- Multitenant application designed for powering service offerings with shared infrastructure
- Flexible deployment options
- Easy-to-use Open API
- Wide range of appliances

Advanced ICS Threat Detection

- Best-in-class ICS threat detection
- Rules and signature-based threat detection
- Behavior-based anomaly detection
- Multiple tools for threat hunting
- Fast and accurate analysis powered by artificial intelligence

Actionable Threat & Process Intelligence

- Intuitive network visualization
- Real-time monitoring of threats, assets and communications
- Customizable dashboards and alerts
- Automatic packet capture
- Smart grouping of alerts into incidents
- Real-time ad hoc query tool

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 thousands of industrial sites
- Deploy to fit each client's business with multiple appliance formats and flexible aggregations of ICS data
- Deliver optimal performance thanks to full stack technology ownership

Easy Integration with IT/OT Environments

- Leverage built-in integrations with SIEMS, firewalls and user authentication systems
- 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 many customizable components

Advanced ICS Threat Detection

Nozomi Networks advanced threat detection combines:

- Best-in-class behavior-based anomaly detection
- Rules and signature-based threat detection
- Artificial intelligence analysis

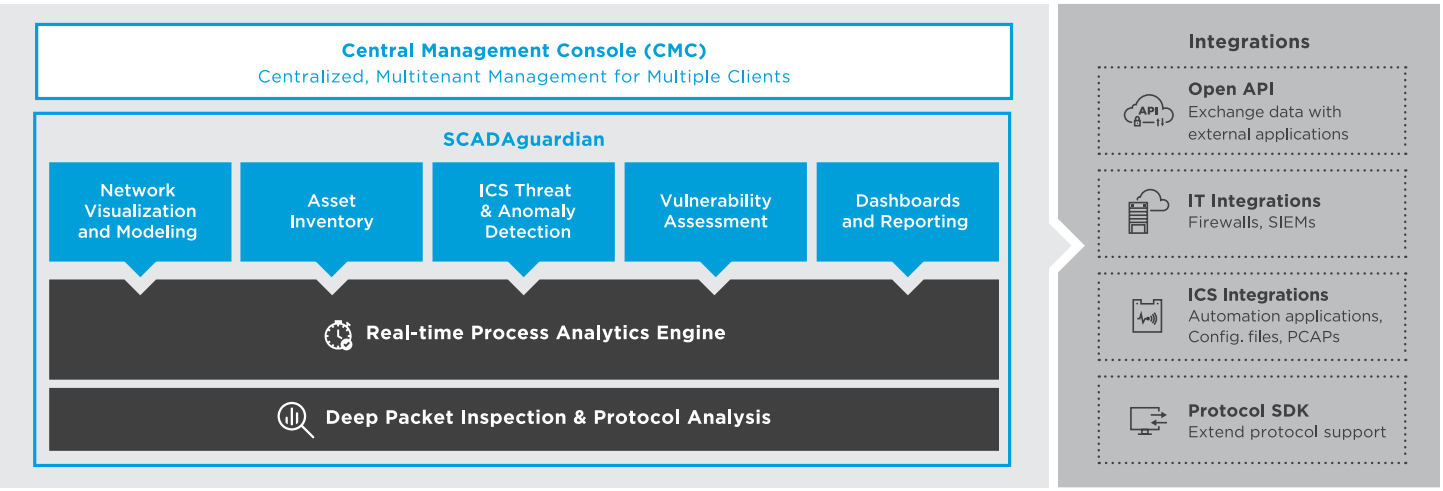
Examples of threats and risks identified include:

- Intrusions: Scanning and MITM attacks · Complex or zero-day attacks · Advanced persistent threats · Known malware files / packets and more
- Unauthorized behavior: Remote access · Configuration changes · Downloads and more
- States of Concern: Critical states involving multiple variables · Weak passwords · Missing updates · Open ports · Device vulnerabilities and more

Advanced ICS Threat Detection

- Custom Assertions (rules) check any aspect of network or process status
- Related alerts are grouped into root incidents
- Automatic packet captures speed analysis
- TimeMachine™ system snapshots compare the entire ICS network at two 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 security 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 with no network changes
- Fits client installations thanks to a wide range of SCADAguardian appliances

Rapid, Real-time Monitoring of Threats and Risks

- Uses machine learning and 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 start providing protective services

Proven, Large-Scale Deployments

- Enhances cyber resilience today at major critical infrastructure, process control and manufacturing organizations
- Scales to hundreds of client sites

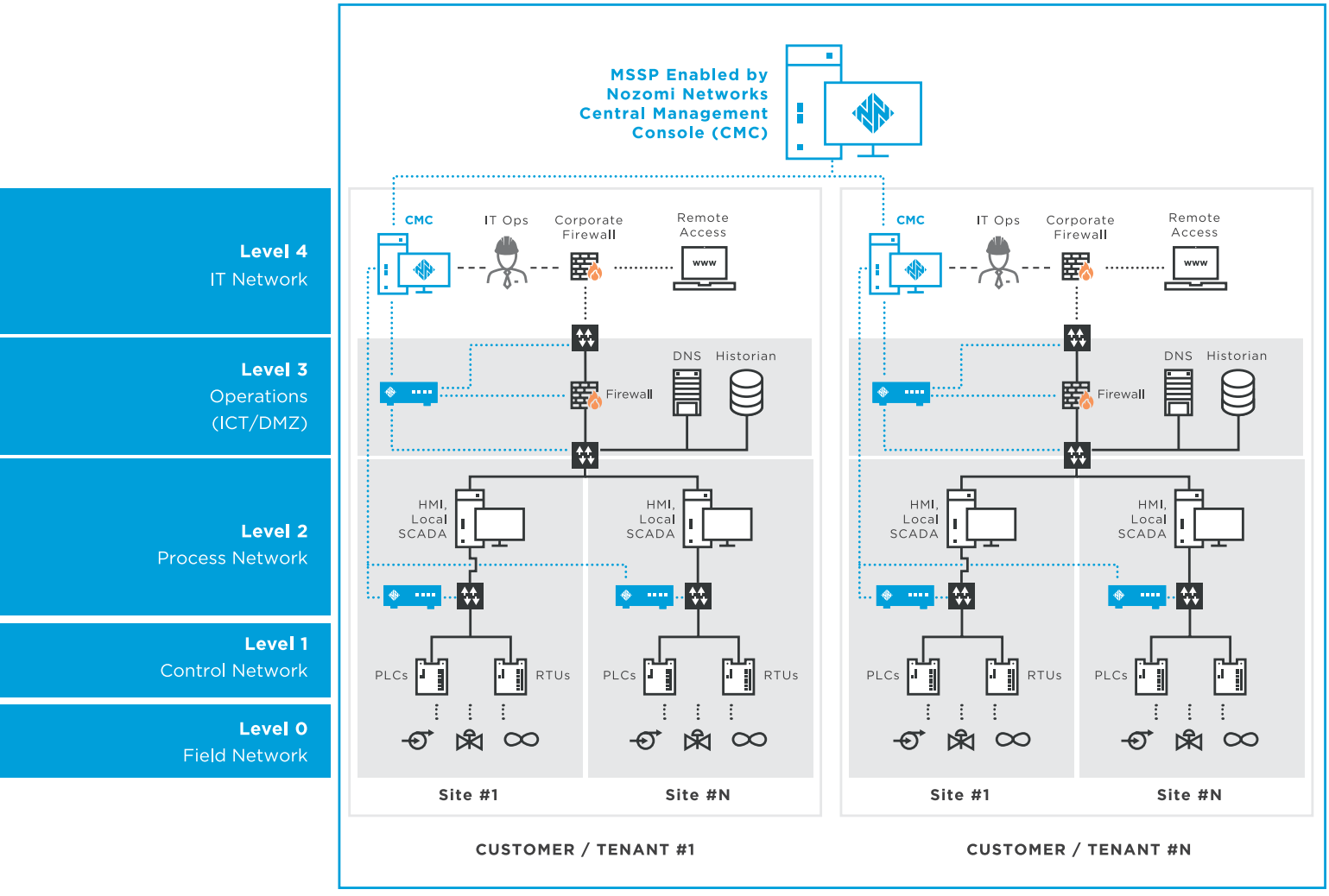
Improved Reliability and Availability

- Addresses the key concern of ICS operators – reduced reliability because of cyber incidents
- Identifies not just cyber risks, but process anomalies that could reduce availability, such as malfunctioning equipment

Trusted Partner Now 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



Nozomi Networks Products

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

The Central Management Console (CMC) provides MSSP / MDR SOCs with centralized and remote ICS cybersecurity and monitoring. It is a secure, multitenant application that aggregates data for up to thousands of SCADAguardian appliances.

Multiple SCADAguardian™ Appliance Formats For Every Type of Deployment

Physical Appliances	 **N1000** *A powerful appliance for very large, demanding scenarios*	 **N750** *A rack-mounted appliance for large scenarios*	 **NSG-L-250** NEW *A rack-mounted appliance for medium scenarios*	 **NSG-L-100** NEW *A rack-mounted appliance for small scenarios*	 **R50** *A ruggedized, DIN-rail mounted appliance for small scenarios*	 **P500** *A portable probe for temporary analysis of network trunks*
Virtual Appliances	 **V1000** *A powerful appliance for very large, demanding scenarios*	 **V750** *A virtual appliance for large scenarios*	 **V250** *A virtual appliance for medium scenarios*	 **V100** *A virtual appliance for small scenarios*	 **V50** *A virtual appliance for very small scenarios*	

For: Complete appliance specifications and options • List of the dozens of supported ICS vendors, ICS protocols and IT protocols • Protocol SDK information, visit **nozominetworks.com**.

The Virtual, Multitenant CMC is Easy to Deploy and Scalable

Summary	Multitenant ICS visibility and actionable threat intelligence for MSSPs and MDRs.		
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 the infrastructure | Visit **nozominetworks.com** for the latest technical specifications.

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

MSSP-SB-8.5x11-002