

SOLUTION BRIEF

Cyber Resilience for Critical Infrastructure

AI-powered visibility and monitoring, trusted industrial technology, lifecycle cybersecurity services and regulatory expertise

Critical infrastructure operators are connecting more assets, systems and teams while facing expanding cyber risk and regulatory scrutiny. Security programs must improve visibility and response without compromising the safety, availability or deterministic performance of essential operations.

Protecting reliability in an increasingly connected world

To help operators meet these challenges, Nozomi Networks and SEL have long partnered to deliver joint solutions and services — along with continuing innovations — spanning cybersecurity software, industrial hardware and networking, control solutions, implementation and lifecycle services, and specialized technical and regulatory expertise.

Nozomi contributes AI-powered asset intelligence, visibility, threat detection and risk analysis across OT, IoT and cyber-physical systems. SEL contributes trusted industrial computing and networking, power-system engineering, cybersecurity services and deep regulatory expertise. The joint approach assists regulated electric utilities preparing for internal network security monitoring requirements under NERC CIP-015-1 and organizations addressing NIS2 requirements in the EU, while also supporting critical infrastructure organizations in other sectors.

At a Glance

Comprehensive internal network security monitoring technology

Network, endpoint and wireless visibility with threat detection, asset intelligence and AI-powered analysis.

Flexible deployment options

Cloud, on-premises and ruggedized edge options, including deployment on and integration with SEL hardware and software.

End-to-end implementation services

Risk assessments and compliance audits through architecture, integration and implementation.

Lifecycle services and response

Health checks, training, threat monitoring, incident response and continuous improvement.

Streamline ongoing operations

Combine lifecycle services with coordinated Nozomi and SEL support to sustain the solution, reduce operational friction and strengthen response readiness.

From Technology to Operational and Compliance Outcomes

The joint Nozomi-SEL solution combines richer operational context, flexible deployment and sensing options, and end-to-end services, to deliver measurable results.

Use the control layer to inform monitoring

The OT-SDN integration adds authoritative network intelligence from SEL's control layer to passive monitoring telemetry collected by Nozomi Networks sensors. The Nozomi Networks platform can use that context to deepen asset and communication visibility and strengthen threat and anomaly detection, which improve AI-powered risk analysis and remediation recommendations.

Deploy and monitor in difficult environments

Organizations can select sensing and installation options according to site, scale, connectivity, environmental and data-governance requirements. A Nozomi Network sensor on SEL-3355 provides a ruggedized network-monitoring option at the edge, while cloud and on-premises central management systems can aggregate and manage distributed sensors. Endpoint and wireless sensors, along with remote collectors, provide coverage in every corner.

Combine technology with end-to-end services

SEL services help customers move from assessment and regulatory planning through architecture, implementation and system hardening. Lifecycle health checks, training, threat monitoring and incident response help scale and sustain the solution and continuously improve the security program after deployment.

Accelerate NERC CIP-015 INSM and NIS2 readiness

The joint solution helps organizations translate regulatory obligations into a monitoring architecture and sustainable operating model, allowing them to exceed baseline requirements.

- For applicable electric utilities, the approach supports internal network security monitoring through network visibility, behavioral and signature-based detection, investigation context, reporting and evidence workflows.
- For organizations subject to NIS2, the combined technology and services can support cyber-risk management, incident handling and evidence-driven governance. Compliance remains dependent and tailored to each organization's scope, documented processes and implementation.

Nozomi Guardian on the SEL-3355 Computing Platform

The SEL-3355 is a versatile computing platform built to withstand harsh environments in utility and industrial applications. It can ship with the Nozomi Guardian sensor operating system installed bare-metal, simplifying deployment and configuration complexity and improving sensor performance while using hardware tested to the same IEC standards as SEL's protective relays, and backed by SEL's standard worldwide, ten-year warranty.



A Flexible, Integrated Technical Architecture

The joint architecture gives customers multiple ways to sense, analyze and manage industrial environments, while integrating with SEL infrastructure and surrounding the technology with the services required for successful adoption.

Flexible sensing and AI-powered management

Nozomi Networks provides complementary sensor options for different assets, networks and site conditions. Nozomi Guardian monitors industrial network communications; Remote Collector extends network visibility to smaller or remote locations; Arc adds endpoint visibility; and Guardian Air monitors wireless networks and devices. Customers can manage distributed sensors through the on-premises Central Management Console or use the cloud-based Vantage platform for centralized visibility, asset intelligence, threat detection and AI-powered analysis.

Joint technology and deployment options

Nozomi Guardian on SEL-3355

Nozomi Guardian can run on the SEL-3355 computing platform, creating a ruggedized monitoring option for demanding industrial locations.

Direct Integration Between the Nozmoi Networks Platform and SEL's OT-SDN

To harden the benefits of our joint solution, the Nozomi Networks platform is now directly integrated with SEL's OT Software-Defined Networking (OT-SDN). OT-SDN provides authoritative network intelligence from the control layer, including real-time information about assets, communications, traffic flows, network policies and physical topology. By incorporating this intelligence directly into the Nozomi Networks platform, organizations gain deeper visibility into managed environments while enhancing threat detection, anomaly detection, asset intelligence and AI-powered risk analysis across OT, IoT and cyber-physical systems.

SEL Blueframe ecosystem

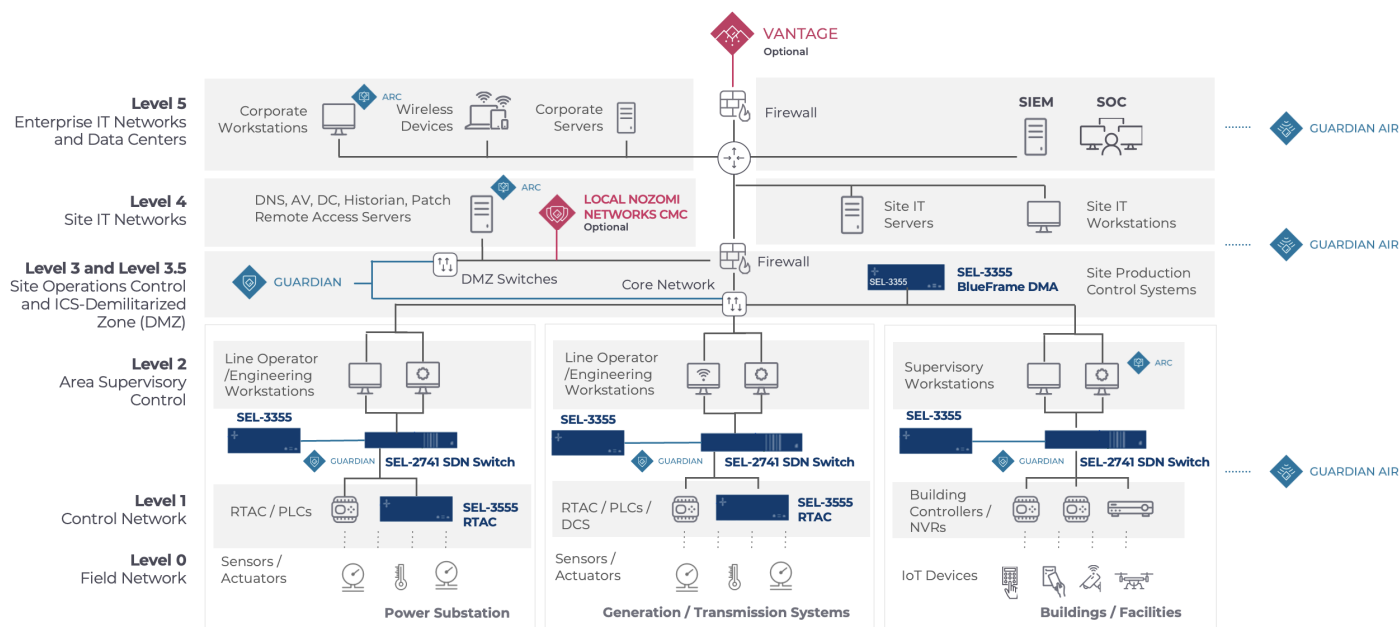
SEL Blueframe systems and applications can be represented within the broader architecture for application hosting and controls.

Services wrapped around the architecture

SEL cybersecurity and regulatory expertise helps tailor the solution to the organization's environment, obligations and goals, then supports implementation, hardening, operations and incident response.

Built around the organization

The architecture is designed to adapt to the customer's installed environment, operational constraints, regulatory scope and preferred management model rather than forcing a single deployment pattern.



Nozomi Networks and SEL Reference Architecture



About SEL

SEL invents, designs and builds digital products and systems that protect power grids around the world. Its technology helps customers improve power-system reliability, safety and economy.

www.selinc.com



About Nozomi Networks

Nozomi Networks protects the world's critical infrastructure from cyber threats. Its platform combines network and endpoint visibility, threat detection and AI-powered analysis for faster, more effective incident response.