CHECK POINT + NOZOMI NETWORKS
SECURE INDUSTRIAL NETWORKS

Benefits

• Provides up-to-the minute intrusion
detection and situational awareness
for industrial networks as part of an
end-to-end security solution
• Automates the identification of
industrial assets, topologies, and
communications
• Operates non-intrusively, with no
downtime or disruption to industrial
networks requiring high availability
• Rapidly identifies industrial
cybersecurity and process anomalies
• Understands industrial protocols and
applies Deep Packet Inspection to
analyze communications and identify
issues
• Facilitates pre-emptive action or fast
incident mitigation by automatically
updating Check Point security
infrastructure
• Allows real-time querying of any
aspect of industrial network or ICS
performance, significantly reducing
manual efforts
• Scales across hundreds of sites while
delivering optimal performance

CHALLENGES IN SECURING INDUSTRIAL NETWORKS

The industrial networks that provide communication for vital Industrial Control
Systems (ICS) such as those in power, water and transportation systems, as well as
for manufacturing systems, differ from IT systems in many ways. They typically have
very high availability requirements, communicate via unique industrial protocols, and
connect a wide variety of equipment that can have lifespans of 30 years of more.

Historically protected by isolation, these networks have ridden a decade-long trend
towards system connectedness, and have had a dramatic increase in industrial cyber-
attacks and vulnerability disclosures. This means that securing ICS is now urgent. The
challenge has been the lack of easy-to-deploy, non-disruptive solutions that address
Operational Technology (OT) requirements and that integrate with end-to-end IT
systems.

INTEGRATED END-TO-END SECURITY

The integrated Check Point and Nozomi Networks’ solution adds ICS intrusion
detection and passive OT monitoring to the comprehensive Check Point security suite.
Standard Check Point Security Gateways and 1200R Rugged Security Appliances
secure perimeters, the IT to OT connection and zones within industrial networks. In
addition, Check Point Endpoint Security Agents secure PC assets in the industrial
network.

Nozomi Networks’ SCADAguardian connects to SPAN or mirror ports on standard
Check Point Security Gateways or Check Point 1200R Rugged Security Appliances
and automatically identifies industrial assets and network activity plus provides real-
time monitoring of cybersecurity and process anomalies. ICS anomaly information is
aggregated into meaningful alerts and communicated to the Check Point security
management infrastructure.

With our unified reporting, you can detect any threat to the application, process or
network, providing granular visibility of SCADA traffic and facilitating attack forensics.
Integrated network and endpoint threat forensics reveals the entire sequence of an
attack event. When security events are centrally managed, you get a complete view
across your enterprise and control networks.
NOZOMI NETWORKS’ ADVANTAGE

Real-Time Cyber-Security and Visibility
Nozomi Networks’ SCADAguardian solves an important part of the ICS security problem by providing comprehensive, real-time cybersecurity and visibility for industrial control networks. It does it in a way that is completely non-intrusive and safe for ICS networks and it integrates with Check Point’s security architecture.

Rapid Identification of Anomalies
Examples of the type of incidents SCADAguardian detects include:
- Malicious cyber threats such as zero-day attacks with no fixed signature or pattern
- Scanning and MITM (Man-In-the-Middle) attacks
- Unintentional cyber incidents such as device-generated traffic storms
- Suspicious behavior such as remote access, configurations, or downloads by unauthorized users
- Misconfigurations and process anomalies
- Any issue that might impact availability, safety or security of ICS

Advanced ICS Monitoring
Reduce Troubleshooting and Remediation Efforts
Instead of spending days decoding network data and manually aggregating information from various sources, use SCADAguardian’s deep and centralized analysis to quickly arrive at real-time answers to industrial issues and incident investigations. You save time and reduce costs.

Preempt Corrective Maintenance
By combining centralized monitoring and continuous process anomaly detection, you get notified of failing equipment and can conduct less costly preventive maintenance.

Save Time and Avoid Regulatory Compliance Fines
SCADAguardian provides detailed, automated business reports, eliminating the need for time consuming, manual data aggregation and avoiding regulatory penalties.

Easily Monitor Remote Sites from a Central Location
Take advantage of visibility across multiple plants and large geographic areas using the Nozomi Networks’ Central Management Console. Remotely troubleshoot and respond to incidents faster and reduce onsite support costs.

CHECK POINT ADVANTAGE

Align IT and OT Security
Deploy our security platforms across your enterprise IT and OT networks for a unified end-to-end security architecture to protect critical assets from threats. Threats to IT networks are protected from OT networks that are not updated or patched as frequently as enterprise systems and do not have the same level of security. OT networks are protected from Advanced Persistent Threats that target IT networks.

Enable Boundary Defenses
Implement granular protection to segment and isolate connectivity to and between facilities and production areas, following the IEC 62443 (ISA-99) zones and conduits model. Ensure the security of the SCADA network devices perimeter and interface points. Ensure that all endpoints and portable equipment used for management is secured with port control protection and free from malware. Our complete IT-OT security solution protects the corporate perimeter, the bridge between IT and OT networks and operator workstations and SCADA devices within the OT network.

Broad ICS/SCADA Protocol Support
Check Point Application Control has broad support for specialized SCADA and ICS protocols with granularity for over 800 SCADA specific commands. Support for additional protocols is available on request. This enables protocol-specific controls with directional awareness. For instance administrators are able to create a policy to prevent monitoring and reporting systems from performing write operations to control systems. Our protocol decoders enable granular control at the command level, for example read/write/get for specific units, function codes and address ranges.

Wide Range of Appliances
Hardened appliances complement our extensive appliance family to support a diverse range of deployment environments and meet specialized requirements. Our 1200R Rugged appliance complies with industrial specifications such as IEEE 1613 and IEC 61850-3 for heat, vibration and immunity to electromagnetic interference (EMI).
SUMMARY
Up to now, it’s been difficult to implement comprehensive, real-time visibility and protection in ICS networks, its devices and process status. Without that insight, protecting the control network from cyber-attacks and avoiding operational disruptions is a challenge. Nozomi Networks’ innovative technology in combination with the Check Point portfolio of firewall products solve this challenge and does it in a way that is completely non-intrusive and safe for ICS and SCADA networks. The combination of Nozomi Networks’ passive OT monitoring solution with Check Point’s active packet filtering devices at key points in the network (see Sample Architecture) provides industrial networks with strong cyber protection and cyber resiliency.

ABOUT CHECK POINT
Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyber-attacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

ABOUT NOZOMI NETWORKS
Nozomi Networks Inc. (www.nozominetworks.com) provides innovative cybersecurity and operational visibility solutions for industrial control systems (ICS). Its technology delivers immediate insight into ICS networks, devices, and process status, rapidly identifying and enabling fast remediation of cyber-attacks and process anomalies. Deployed in some of the world’s largest industrial installations, operators trust Nozomi Networks’ products to enhance cybersecurity, maximize uptime and deliver real ROI.