Protect your control networks from cyberattacks and operational disruptions with SCADAguardian. It rapidly detects cyber threats and process anomalies, providing unprecedented operational visibility.

SCADAguardian automatically discovers the industrial network including its components, connections and topology. It develops security and process profiles and monitors the system in real-time for any changes.

**SCADAguardian uniquely provides:**

- Comprehensive, hybrid ICS threat detection that combines behavior-based, rules, signatures and artificial intelligence analysis
- Superior incident capture and forensic tools
- Easy integration and sharing of ICS and cybersecurity information with IT/OT environments
- Enterprise-class scalability when deployed with the related Central Management Console

Find out how major customers have improved reliability, safety, cybersecurity and operational efficiency with SCADAguardian.

**Contact us today at nozominetworks.com/contact**
Five Modules Deliver **ICS Cybersecurity and Operational Visibility**

**Network Visualization and Modeling**  
- Improve system and process awareness with a visualization interface that shows all assets and links

**Asset Inventory**  
- Auto-discovery of assets saves time and is always up-to-date  
- Asset views make it easy to visualize, find and drill down on asset information

**Vulnerability Assessment**  
- Automated identification of device vulnerabilities saves time and improves cyber resiliency

**Dashboards and Reporting**  
- Custom dashboards, detailed reports and ad hoc querying provide real-time visibility that improves both cybersecurity and operational efficiency

---

**ICS Threat and Anomaly Detection**  
- Rapidly detect cybersecurity threats, risks and process anomalies  
- Hybrid threat detection combines best-in-class behavior-based anomaly detection with rules-based threat detection (YaraRules, Packet Rules and Assertions) and artificial intelligence analysis  
- Detect intrusions: Scanning and MITM attacks  
  - Complex or zero-day attacks  
  - Known malware files or packets and more  
- Detect unauthorized behavior: Remote access  
  - Configurations  
  - Downloads  
  - Controller logic changes  
  - Edits to PLC projects and more  
- Detect states of concern: Misconfigurations  
  - Weak passwords  
  - Missing updates  
  - Open ports  
  - Communication failures  
  - Malfunctions and more

---

**Sample Deployment Architecture**

---

**Level 4**  
**IT Network**

**Level 3**  
**Operations (ICT/DMZ)**

**Level 2**  
**Process Network**

**Level 1**  
**Control Network**

**Level 0**  
**Field Network**

---

**Central Management Console (CMC)**  
**SIEM**  
**SOC**  
**Corporate Firewall**  
**Historian**  
**Firewall**  
**DNS**  
**Local SCADA & HMI**  
**Local SCADA & HMI**  
**Local SCADA & HMI**  
**PLCs**  
**RTUs**  
**PLCs**  
**RTUs**  
**PLCs**  
**RTUs**  
**Site #1**  
**Site #2**  
**Site #N**
Value Delivered to **Multinational Operators**

Automated ICS Modeling
- Installs passively and non-intrusively by connecting to network devices via SPAN or mirror ports
- Learns and models large heterogeneous ICS
- Identifies all assets and triggers alerts on changes

Dynamic Learning
- Switches from learning to protection mode automatically, starting anomaly detection quickly

Operational Visibility
- Provides real-time network visualization, including topology
- Monitors assets, communications and processes
- Presents actionable information in dashboards
- Allows real-time querying of any aspect of network or ICS performance, reducing spreadsheet work

Easy Integration with IT/OT Environments
- Includes built-in integration with:
  - SIEMs: HPE ArcSight, IBM QRadar, Splunk, etc.
  - Firewalls: Check Point, Fortinet, Palo Alto Networks, etc.
  - User Authentication: Active Directory, LDAP, etc.
- Exchanges data with other IT/ICS applications via an Open API
- Includes built-in support for dozens of protocols, extends to others via the Protocol SDK
- Exports data for analysis and presentation in other applications
- Adapts for each installation with many customizable components

Fast ROI
- Deploys quickly, with no network changes
- Delivers value at numerous customer sites, with centralized monitoring of tens of thousands of industrial devices

---

### Multiple SCADAguardian™ Appliance Formats to Meet Your Needs

<table>
<thead>
<tr>
<th>Description</th>
<th>Form Factor</th>
<th>Monitoring Ports</th>
<th>Max Throughput</th>
<th>Max Protected Nodes</th>
<th>Storage</th>
<th>HxWxD (mm/in)</th>
<th>Weight</th>
<th>Max Power Consumption</th>
<th>Power Supply Type</th>
<th>Temperature Ranges</th>
<th>RoHS Conformity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PHYSICAL APPLIANCES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N1000</td>
<td>A powerful appliance for very large, demanding scenarios</td>
<td>1 Rack Unit</td>
<td>8</td>
<td>1 Gbps</td>
<td>5,000</td>
<td>240 Gb</td>
<td>43 x 426 x 356</td>
<td>10 Kg</td>
<td>260W</td>
<td>110-240V AC</td>
<td>0 / +45º C</td>
</tr>
<tr>
<td>N750</td>
<td>A rack-mounted appliance for large scenarios</td>
<td>1 Rack Unit</td>
<td>4</td>
<td>500 Mbps</td>
<td>1,000</td>
<td>180 Gb</td>
<td>43 x 426 x 356</td>
<td>10 Kg</td>
<td>260W</td>
<td>110-240V AC</td>
<td>0 / +45º C</td>
</tr>
<tr>
<td>NSG-L-250</td>
<td>A rack-mounted appliance for medium scenarios</td>
<td>1 Rack Unit</td>
<td>5</td>
<td>200 Mbps</td>
<td>400</td>
<td>64 Gb</td>
<td>44 x 438 x 300</td>
<td>8 Kg</td>
<td>250W</td>
<td>110-240V AC</td>
<td>0 / +45º C</td>
</tr>
<tr>
<td>NSG-L-100</td>
<td>A rack-mounted appliance for small scenarios</td>
<td>1 Rack Unit</td>
<td>5</td>
<td>100 Mbps</td>
<td>150</td>
<td>64 Gb</td>
<td>44 x 438 x 300</td>
<td>8 Kg</td>
<td>250W</td>
<td>12-36V DC</td>
<td>0 / +45º C</td>
</tr>
<tr>
<td><strong>NEW</strong> R50</td>
<td>A ruggedized, DIN-rail mounted appliance for small scenarios</td>
<td>DIN Mountable</td>
<td>4</td>
<td>50 Mbps</td>
<td>200</td>
<td>64 Gb</td>
<td>80 x 130 x 146</td>
<td>3 Kg</td>
<td>60W</td>
<td>110-240V AC</td>
<td>-40 / +70º C</td>
</tr>
<tr>
<td><strong>NEW</strong> P50</td>
<td>A portable probe for temporary analysis of network trunks</td>
<td>Portable Form Factor</td>
<td>5</td>
<td>200 Mbps</td>
<td>250</td>
<td>180 Gb</td>
<td>93 x 202 x 200</td>
<td>5 Kg</td>
<td>100W</td>
<td>110-240V AC</td>
<td>0 / +50º C</td>
</tr>
</tbody>
</table>

(*) Plus other limitations
**Broad Support for Industrial Control Systems and ICS / IT Protocols**

**ICS Vendors**
- ABB, Allen-Bradley/Rockwell, Bristol Babcock, Beckhoff, Emerson, General Electric, Honeywell, IBM, Mitsubishi, Motorola, Rockwell Automation, Schneider Electric, Siemens, Yokogawa

**ICS Protocols**

**IT Protocols**
- ARP, BROWSER, BitTorrent, CDP, DCE-RPC, DHCP, DNS, DRDA (IBM DB2), Dropbox, eDonkey (eMule), FTP, FTPS, GVCP, HTTP, HTTPS, ICMP/PING, IGMP, IKE, IMAP, IMAPS, ISO-TSAP/COTP, Kerberos, KMS, LDAP, LDAPS, LLDP, LLNR, MDNS, MS SQL Server, MySQL, NetBIOS, NTP, OSPF, POP3, PTPv2, RDR, STP, SSDP, RTCP, RTP, SSH, SNMP, SMB, SMT, STP, Syslog, Telnet, VNC

Support for additional systems and protocols is constantly being expanded. Visit [nozominetworks.com](http://nozominetworks.com) for the latest technical specifications. Further protocols can be quickly added using the Protocol SDK.

**Nozomi Networks Products**

**SCADAguardian** is a physical or virtual appliance that provides real-time cybersecurity and operational visibility of industrial control networks. The **Central Management Console (CMC)** aggregates data from multiple sites, providing centralized and remote cybersecurity management.

Together they deliver comprehensive ICS cyber resilience and reliability.

**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](http://www.nozominetworks.com)