



New
SCADAguardian 17.0

SCADAguardian is a real-time cybersecurity and operational visibility solution for industrial control networks that provides:

- Auto-Discovery and Visualization of Industrial Assets
- Asset Inventory **New!**
- Real-time Network Modeling
- Process and Asset Monitoring
- Vulnerability Assessment **New!**
- ICS Process Anomaly Detection
- Dynamic ICS Behavioral Learning **New!**
- Cybersecurity Intrusion and Risk Detection
- Incident Correlation and Management
- Dashboards & Compliance Reporting
- Ad-hoc Queries, Forensics & Troubleshooting Tools

Version 20**17.0**



Asset Inventory

Improve your organization's cybersecurity posture with an always up-to-date asset inventory. Track your assets in dedicated diagram or list views. Know the configurations and firmware versions of network and ICS devices and receive alerts when they change.

Vulnerability Assessment

See all the vulnerabilities for your assets in a single view. Know whether devices need to be patched or updated to be protected. Your assets are analyzed with comparison to a state-of-the-art ICS vulnerability repository.



Dynamic Learning

SCADAguardian uses machine learning and AI to model your ICS. Previously you had to decide when to close the learning phase and switch the product into protection mode. Now, SCADAguardian automatically switches to protection mode and can do so by network segment, protecting stable segments quickly and others over time.

Asset Inventory

- Automated identification of assets saves time and is always up-to-date.
- Dedicated views make it easy to visualize, find and drill down on asset information.
- Extensive asset attributes, including customized fields, provide comprehensive details on each asset. Includes vendor, firmware and configuration information for common industrial devices such as PLCs and RTUs.
- Customizable alerts provide notification of changes to hardware, software and devices.

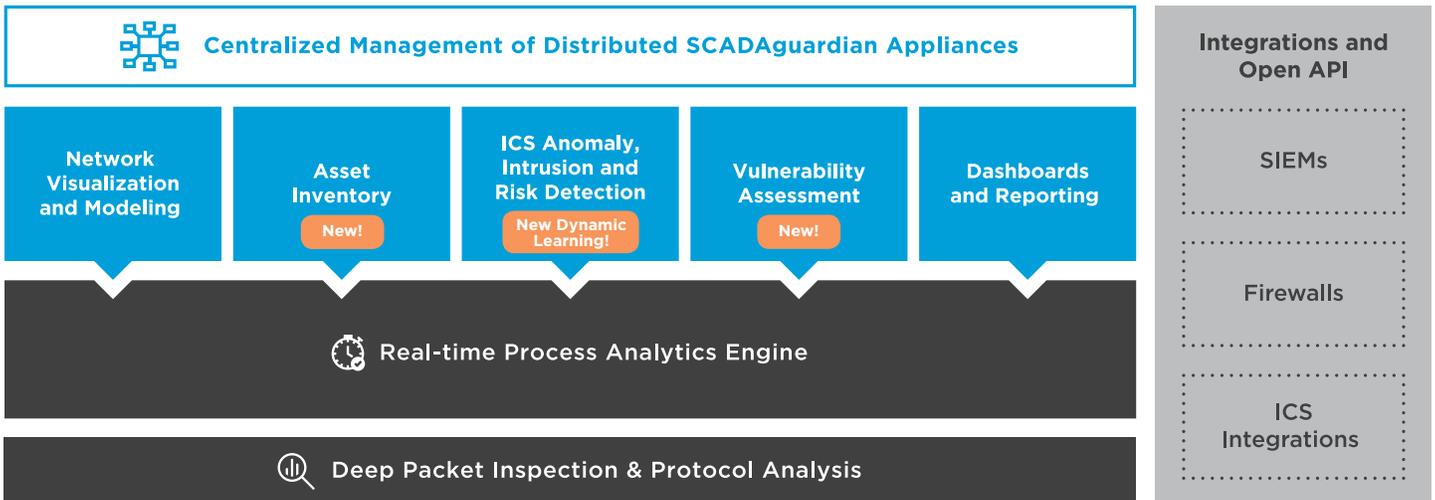
Vulnerability Assessment

- Automated identification of devices with vulnerabilities saves times and improves cyber resiliency.
- Dedicated view of all vulnerabilities and their severity facilitates fast remediation. Allows the identification of vulnerable devices and software by vendor or other attributes.
- State-of-the-art repository checks your system against current vulnerabilities, providing clear visibility of your ICS risk.
- “Mute” vulnerability allows site specific risk management practices.

Dynamic Learning

- Anomaly detection begins as quickly as possible since SCADAguardian automatically switches from learning to protection mode for stable network segments.
- Easy deployment because manual input is not needed to initiate cybersecurity monitoring / anomaly detection.

The Nozomi Networks' Solution Architecture



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 meet the unique challenges of critical infrastructure operations. Nozomi Networks delivers both cybersecurity and process anomaly detection along with industrial network visualization and monitoring, asset inventory, and vulnerability assessment. Deployed in the world's largest industrial installations, customers benefit from enhanced cybersecurity and improved operational reliability with one end-to-end solution. Nozomi Networks is headquartered in San Francisco, California. www.nozominetworks.com