SOLUTION BRIEF

Converged Network; TCP/IP Serial and Analog Security Monitoring for Industrial Control Systems

Extend visibility, situational awareness, and threat detection across operational technologies with Nozomi Networks and Cynalytica.

Organizations operating industrial control systems (ICS) are challenged with monitoring a diverse set of legacy and modern technologies. Adding to this complexity, security risks are increasing as both the frequency and sophistication of cyberattacks on these OT systems accelerate. While Nozomi Networks has developed a leading solution for TCP/IP-based network traffic and threats, more is often required for non-IP based serial bus and analog connections found in ICS environments which are essential for field-level connectivity and legacy systems.

For this reason, Cynalytica and Nozomi Networks have partnered to introduce a solution for visibility and security monitoring of both Ethernet and non-IP systems. The joint solution's key benefits are effectiveness, deployment flexibility, and scalability, across all equipment within a rapidly changing OT environment. The solution ensures real-time visibility and anomaly detection that provides actionable information to respond to incoming threats, no matter what class of system is involved.

> Cynalytica is critical in some of our largest accounts who rely on serial communications alongside Ethernet TCP/IP in their operational networks. Our combined visibility and threat detection—including intrusion detection via the AnalytICS Engine—ensures that all potential threats are captured and simplifies remediation efforts through our platform integrations. Cynalytica providing both on-prem and SaaS serves as a fantastic fit with Nozomi Networks' flexibility of Guardian and Vantage platforms.
>
> *Chet Namboodri*
>
> *SVP of Business Development, Nozomi Networks*

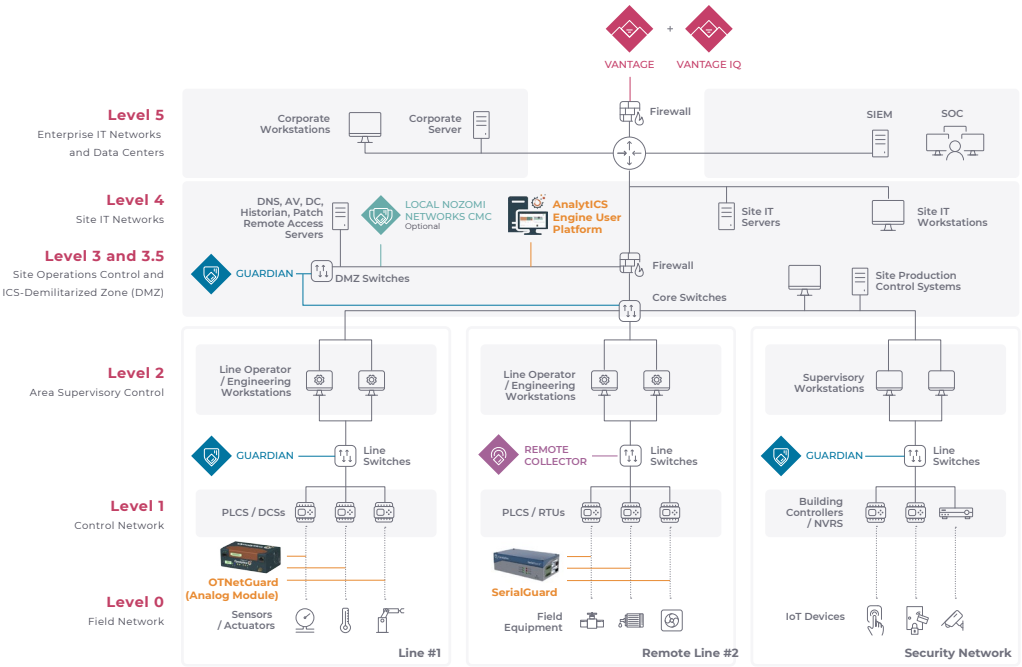
Simplifying the Challenge of Addressing Security Across Dynamic OT Environments with Both Legacy and Modernized Technologies

Converged Monitoring of Ethernet-based and Serial-based Systems

The convergence of IT and OT technologies and the explosion of IoT devices within the OT environment pose an unprecedented risk for organizations to monitor from a central location, including increased attack surface and lack of full visibility and control. The joint solution allows for organizations to gain visibility and threat detection into Ethernet, analog and serial communications that OT equipment runs on. The identified findings are aggregated into the Nozomi Networks Central Management Console (CMC) or the Vantage SaaS-based security platform and the Cynalytica AnalytICS Engine.

The combined visibility across network environments can simplify threat detection, monitoring and remediation efforts, while ensuring a complete view across all assets.

Sample OT Deployment – Nozomi Networks and Cynalytica



Sample Deployment Architecture for Substations SOC

Converged Security Monitoring Across an Unlimited Number of Facilities and Systems from a Central Location

Anomaly Detection and Corroboration of Process Variable Values

Nozomi Networks and Cynalytica improve operational resilience by monitoring process variables sent between OT devices and alerting on any anomalous activity. The joint solution can monitor process variables between Ethernet-based devices as well as analog and serial-based controllers to identify when variables such as setpoints and flowrates shown to operators do not match the commands being issued to running equipment.

The joint solution also flags when process variables deviate from normal ranges or if the process values change unexpectedly, all of which can cause operational issues and be indicators of an ongoing OT security incident or equipment malfunction.

Flexible and Scalable On-Premises Monitoring with Centralized Alerts

The joint solution is designed to deploy into all forms of OT environments and monitor an unlimited number of sensors, devices, and facilities. Nozomi Networks Guardian sensors can be deployed as appliances, VMs or container applications to monitor Ethernet traffic in network switches. Cynalytica OTNetGuardian and SerialGuard devices can be deployed where systems use analog and serial communications for operations, and all sensor management and alerts are consolidated into a single dashboard. Management can be from a corporate office, SOC or in the cloud, giving organizations a scalable and flexible way to monitor all facilities and OT equipment.

Let's Get Started

Schedule a demo with our experts to understand how Nozomi Networks and Cynalytica can provide full visibility and security monitoring for your Ethernet and Legacy systems.

Book a Demo

nozominetworks.com/demo

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com