

Achieve Converged IT, IoT, and OT Visibility with Tripwire and Nozomi Networks

With increasing convergence of IT, IoT, and OT environments, organizations need a consolidated view of their security and compliance posture. Cybersecurity risks don't exist in silos, and organizations are adopting converged strategies for securing their IT, IoT, and OT environments. Tripwire brings more than 20 years of IT security and compliance expertise to customers. Nozomi Networks provides in-depth security visibility for OT/IoT environments. Together, Tripwire and Nozomi Networks deliver a unique set of capabilities to customers.

Nozomi Networks: The Leader in OT and IoT Security and Visibility

Nozomi Networks Guardian provides operational visibility and rapid detection of cyber threats in OT and IoT networks. Its automated discovery process maps network topology, assets, connections, protocols, and SCADA/ICS commands. It monitors network behavior for risks and supplies the information stakeholders need to respond quickly to prioritized threats.

Nozomi Networks Threat Intelligence continuously updates Guardian sensors with rich data and analysis so you can detect and respond to emerging threats faster. Guardian correlates threat intelligence information with broader environmental behavior to deliver maximum security and operational insight.

This solution enables cybersecurity executives and professionals to:

- » **See** all OT and IoT assets and network behavior on a single dashboard
- » **Detect** cyber risks, vulnerabilities, and anomalies for faster, targeted responses

- » **Unify** security, visibility, and monitoring across all operational assets for improved resilience

Nozomi Networks Guardian is available as an appliance or an application on a virtual machine. Multiple Guardian sensors can be unified and managed with an on-premises Central Management Console appliance or a SaaS-based Vantage solution.

Tripwire® Enterprise uses the Nozomi Networks information for a comprehensive and converged management of IT, IoT, and OT networks.

Detect Change and Assess Compliance with Tripwire

Tripwire Enterprise is the industry standard for integrity monitoring, change detection, and compliance validation. With Tripwire Enterprise, organizations can effectively baseline the configuration of assets throughout their environment, and then detect any changes that occur, including detection in real-time. Accurate and comprehensive change detection is key to preventing and responding to incidents.

Tripwire Enterprise uses the configuration data collected to assess systems against a wide variety of security and regulatory standards, such as PCI, NERC-CIP, HIPAA, CIS, and NIST. Ensuring that systems are hardened and in compliance with standards reduces the risk of both security incidents and audit findings.

The Value of Partnership

Combining Tripwire’s best-in-class compliance offering with Nozomi’s industry leading solution for industrial cybersecurity creates an integration that provides a more comprehensive view of your IT, IoT, and OT assets. Through this integration, your team will have a single viewpoint into asset inventory, security posture, change reconciliation, and compliance status across your environment.

Organizations using this integration will experience:

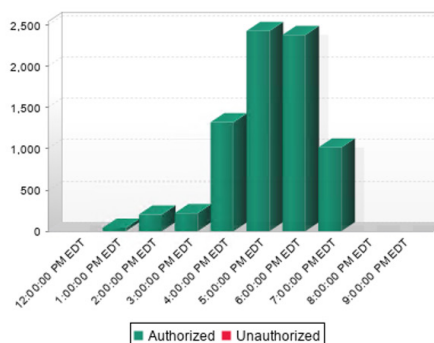
- » Consolidated view of policy compliance across IT, IoT, and OT
- » Comprehensive IT, IoT, and OT asset inventory across the organization
- » Improved visibility into IoT and OT information for IT personnel
- » Consolidated change reconciliation and workflow for IT, IoT, and OT

Implementing consistent security controls across IT, IoT, and OT environments results in lower overall risk, but these environments often require different technical implementations. Integration between Tripwire and Nozomi Networks allows organizations to implement the right tools for the job, but maintain a consolidated view and consistent workflow across diverse environments.

Schedule Your Demo Today

Let us take you through a demo of and answer any of your questions. Visit tripwire.me/demo

Changes to Plant Systems - Nozomi



Details

Interval	Authorized	Unauthorized	Total
8/10/21 12:00:00 PM EDT	0	0	0
8/10/21 1:00:00 PM EDT	42	0	42
8/10/21 2:00:00 PM EDT	203	0	203
8/10/21 3:00:00 PM EDT	220	0	220
8/10/21 4:00:00 PM EDT	1,324	0	1,324
8/10/21 5:00:00 PM EDT	2,432	0	2,432
8/10/21 6:00:00 PM EDT	2,384	0	2,384
8/10/21 7:00:00 PM EDT	1,017	0	1,017
8/10/21 8:00:00 PM EDT	0	0	0
8/10/21 9:00:00 PM EDT	0	0	0
Totals:	7,622	0	7,622

Fig. 1 Tripwire Enterprise report detailing authorized and unauthorized changes to plant systems detected by Nozomi Networks Guardian sensors.



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. nozominetworks.com



Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world’s leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations’ digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. [Learn more at tripwire.com](http://tripwire.com)

The State of Security: News, trends and insights at tripwire.com/blog
Connect with us on [LinkedIn](#), [Twitter](#) and [Facebook](#)