DATASHEET

Achieve Full Visibility Across IT and OT

Tripwire Enterprise and Tripwire Industrial Sentinel Integration

Industrial organizations can now achieve in-depth visibility and monitoring spanning both IT and OT assets with the integration of Tripwire® Enterprise and Tripwire Industrial Sentinel, powered by Forescout. Together, these integrated solutions provide organizations with advanced IT/OT asset inventory, vulnerability management, and other key controls required to keep industrial systems secure and compliant without disrupting productivity.

Integration Highlights

- Get alerted on misconfigurations across IT and OT without risk to production
- Stay ahead of emerging industrial compliance policy mandates
- View one asset inventory that covers both IT and OT
- Detect configuration drift for both IT and OT
- Leverage agentless monitoring for IT devices within OT environments

Holistic Cybersecurity Intelligence

Unifying security intelligence across IT and OT environments is proving to be one of the biggest cybersecurity challenges of the 2020s. Those responsible for operational technology environments now must find a way to apply security controls to their increasingly connected industrial systems to stay ahead of emerging attack vectors. Organizations need to begin taking a more holistic cybersecurity approach wherein both IT and OT environments get the same level of scrutiny.

This integration takes the best of Tripwire Enterprise—secure configuration management (SCM) and file integrity monitoring (FIM)—and now applies it to the OT environment. This allows organizations to be alerted to misconfigurations across IT and OT environments without system disruption, in turn staying compliant and within approved baseline configurations.

While disparate network types like Ethernet and Fieldbus traditionally didn't mix— that is no longer the case. Industrial control systems (ICS) are now increasingly intertwined with IT devices and business processes, multiplying the risk of compromise to their command and control functions. That's why leading organizations are taking advantage of the ability to monitor their combined environments for misconfiguration and configuration change with the new Tripwire offering.

Industrial environments are now a complex mix of traditional IT assets (control system management server for example) as well as unique industrial OT assets (PLCs, robots, conveyor systems, etc.). Bridging the IT/OT gap helps organizations not only helps to achieve budgetary and resource efficiencies, but it also strengthens security postures by improving reporting, maintaining production time, and providing a more holistic view across your landscape.

Secure OT Assets Without Impacting Production or Safety

Using purpose-built tools for the OT and IT side of your organization can be made more efficient—it's time to bridge the IT/OT gap with solutions that span both environments and play well with the other solutions you already have in place. Tripwire Enterprise and Tripwire Industrial Sentinel work together to help you keep intruders out and meet compliance requirements without causing costly system downtime.

Tripwire Enterprise

Tripwire Enterprise is a cybersecurity suite that provides fully integrated solutions for policy, file integrity, configuration management and remediation management for both IT and OT assets. You can now safely apply the same security practices traditionally used for IT assets to your industrial assets as well.

With a single interface management system, Tripwire Enterprise offers operators a security workflow that can be accessed from virtually anywhere, providing a comprehensive picture of security issues across the entire infrastructure. Tripwire Enterprise gives you the ability to identify and remediate configuration issues, such as a PLC that has been left in a risky state like remote-program mode.

Tripwire Enterprise

Tripwire Enterprise is well-known for its ability to enforce security controls within IT environments, but it reaches beyond traditional infrastructure to encompass operational environments for a comprehensive IT/OT cybersecurity program as well.

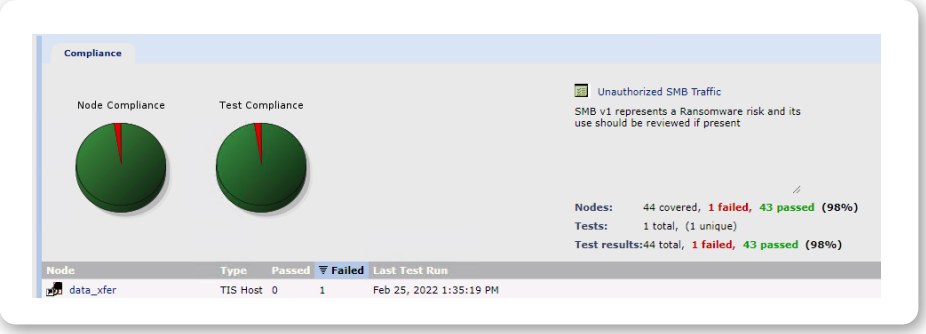

Fig. 1 Tripwire Enterprise dashboard displaying node and test compliance results.

Tripwire Industrial Sentinel

Tripwire Industrial Sentinel is a non-intrusive network monitoring and situational awareness platform that provides in-depth visibility and cyber resilience for industrial control systems (ICS) and SCADA networks, providing visibility to and protection from events that threaten safety, productivity, and quality.

Tripwire Industrial Sentinel combines patented anomaly detection and deep packet inspection (DPI) with a library of thousands of ICS-specific threat indicators and a continuously growing library of 3,500+ indicators of compromise (IoCs) to protect asset owners from advanced cyberattacks, network misconfigurations, and operational errors. Tripwire Industrial Sentinel natively interfaces with enterprise systems such as SIEMs, firewalls, IT asset management, malware analysis, authentication servers and third-party platforms.

How the Integration Perfectly Aligns to OT Needs

You can now apply the same stringent cybersecurity controls to your OT environment that you may have traditionally thought of as IT processes, such as SCM, asset inventory and management, vulnerability management, and others. But how does this occur within the specific needs of industrial operators, where process integrity—the ability to keep systems safely up and running—is just as important as file and configuration integrity?

Here are three ways this integration rises to the challenge:

- **Vendor Agnostic:** To be effective, cybersecurity solutions deployed in industrial environments need to be able to communicate with all the other solutions already in place. Tripwire's industrial solutions play well with the array of device types and vendors found within your OT environment—just like they do in your IT environment. Tripwire Enterprise also integrates with ServiceNow, BMC, Jira, Cherwell, and many other vendors in your tool stack.
- **Offline Analysis:** It is crucial to maintain the safety and availability of OT systems, so cybersecurity tools that disrupt either of those things are a risk to the organization. Tripwire Enterprise conducts analysis offline by gathering data from Tripwire Industrial Sentinel, avoiding costly or dangerous disruptions to system availability.
- **Simplified OT Compliance:** With automated, continuous monitoring across different types of operating systems, industrial devices, and applications, industrial organizations rely on this integration as a simplified and cost-effective solution for maintaining system hardening against policies.

Whether you are simply looking to achieve best practices for your environment or working to provide continual proof of compliance, the integration can help with standards such as:

- International Electrotechnical Commission (IEC) 62443
- International Organization for Standardization (ISO) 27001
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- National Institute of Standards and Technology (NIST)
- Center for Internet Security Industrial Control System Critical Security Controls (CIS ICS CSC)

Summary

Organizations with both IT and OT assets to monitor can do so using the integration between Tripwire Enterprise and Tripwire Industrial Sentinel. Using these two advanced solutions together bridges the cybersecurity gap common in industrial organizations. This integration not only serves to protect your organization against breaches and human error—it also helps industrial operators prove compliance with the industrial compliance standards on which they may be audited. Get unmatched visibility into the configuration and vulnerability states of both the IT and OT sides of your organization at once.

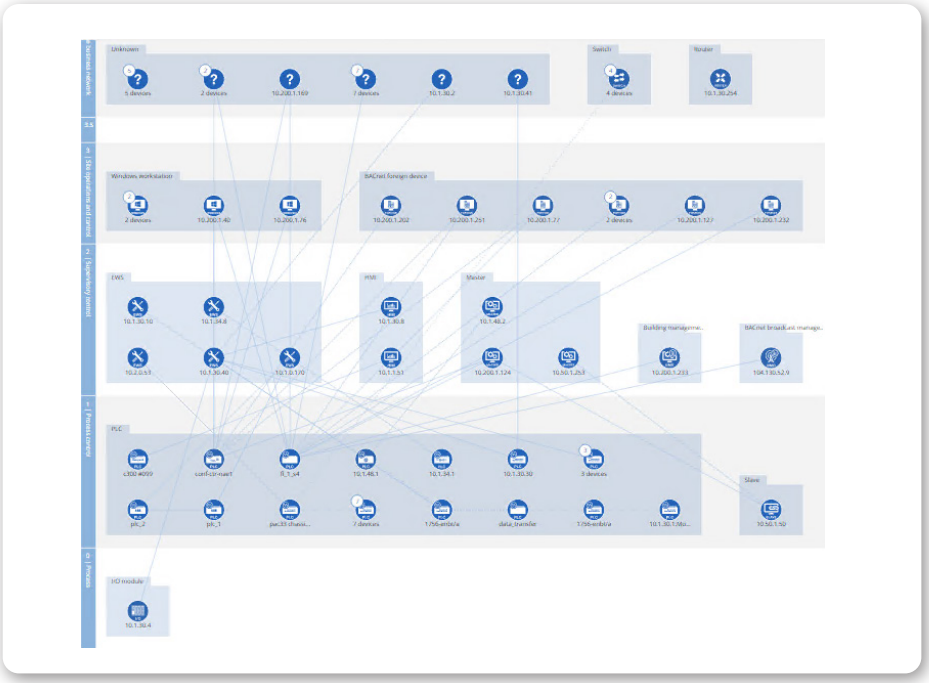

Fig. 2 Tripwire Industrial Sentinel network topology map.

Schedule Your Demo Today

Let us take you through a demo of this integration, where we'd be happy to answer any of your questions. Visit **tripwire.me/demo**

tripwire® by HelpSystems

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**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

©2022 Tripwire, Inc. Tripwire, LogCenter, IP360, Tripwire Axon and others are trademarks or registered trademarks of Tripwire, Inc. All other product and company names are property of their respective owners. All rights reserved.
TETISI1a 2203