SOLUTION BRIEF

Bridging the IT/OT Cybersecurity Gap

Tripwire Enterprise and Tripwire Industrial Visibility Integration

Key Integration Benefits

- » Get alerted on misconfigurations across IT and OT without risk to production
- » 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
- » Stay ahead of emerging industrial compliance policy mandates

With notable industrial cyber events on the rise, the 2020s are shaping up to be a challenging time for operational technology (OT) operators concerned with the safety, security, and compliance of their operational technology networks. To protect their OT environments, everyone from plant managers to CISOs is facing increased pressure to deploy effective cybersecurity solutions. However, professionals in the cybersecurity industry are continuously developing new technology to try to keep up with advancements in illegal cyber activity, and there are a growing number of ways to apply security controls to both your IT and OT environments.

Tripwire's tried-and-true file integrity management (FIM) and security configuration monitoring (SCM) suite, Tripwire® Enterprise, extends across both the IT and OT sides of your organization. And in order to help organizations bridge the IT/OT gap, it now integrates with another powerful solution designed with specific industrial use cases in mind, Tripwire Industrial Visibility.

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. This integration mitigates cybersecurity and production risk for both IT and OT assets.

The IT/OT Challenge

Industrial environments are 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 gain budgetary and resource efficiencies in managing one combined asset inventory.

Traditionally, disparate network types like Ethernet and Fieldbus didn't mix—but 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. This situation is accelerating due to the rapid proliferation of IIoT (industrial internet of things) devices that connect to IT networks.

To stay a step ahead of malicious actors, organizations need to begin taking a more holistic cybersecurity approach wherein both IT and OT environments get the same level of scrutiny and investment from their cybersecurity leadership.

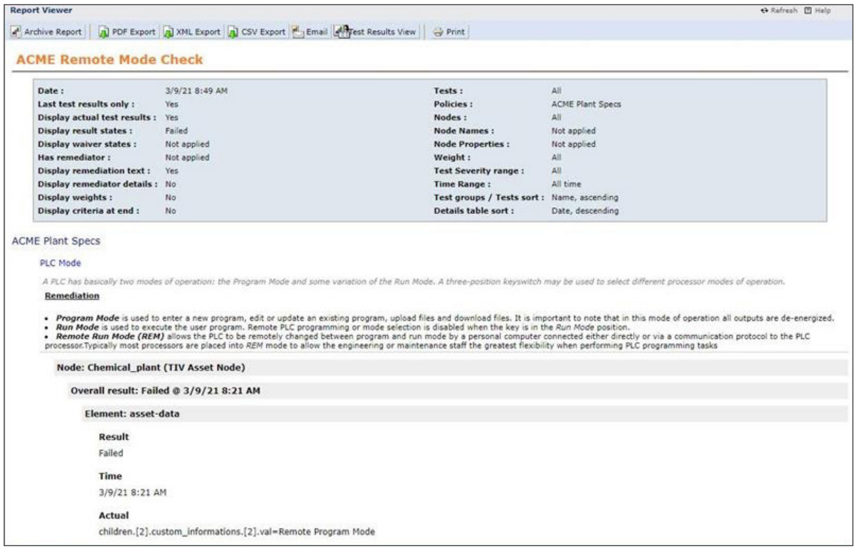
Tripwire Enterprise

Tripwire Enterprise is a cybersecurity suite that provides fully integrated solutions for policy, file integrity, and remediation management for IT and OT assets. It provides an innovative approach for industrial organizations to assess configurations, security, and status in their environments. With a single interface management system, Tripwire Enterprise offers operators an agentless security workflow that can be accessed from virtually anywhere, providing a comprehensive picture of security issues across the entire infrastructure. Tripwire Enterprise gives operators 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 Industrial Visibility

Tripwire Industrial Visibility is a security tool specifically built for OT to protect ICS networks by providing extreme visibility, continuous threat, and vulnerability monitoring, and deep insights into ICS devices and networks. The use of passive deep packet inspection (DPI) technology specifically designed to ensure safe, secure, and reliable operations in complex industrial networks—ensuring minimal impact to the underlying operational processes along with improved cyber resiliency.

It is designed to tap into the native protocols on the OT network in such a way that it extracts data without affecting operations that may be sensitive to latency and bandwidth change. Our deep understanding of the many protocols used by OT systems makes this possible. Tripwire Industrial Visibility integrates with Rockwell FactoryTalk AssetCentre, MDT AutoSave, Eaton IMS, and Kepware.



ACME Remote Mode Check

Date :	3/9/21 8:49 AM	**Tests :**	All
Last test results only :	Yes	**Policies :**	ACME Plant Specs
Display actual test results :	Yes	**Nodes :**	All
Display result states :	Failed	**Node Names :**	Not applied
Display waiver states :	Not applied	**Node Properties :**	Not applied
Has remediator :	Not applied	**Weight :**	All
Display remediation text :	Yes	**Test Severity range :**	All
Display remediator details :	No	**Time Range :**	All time
Display weights :	No	**Test groups / Tests sort :**	Name, ascending
Display criteria at end :	No	**Details table sort :**	Date, descending

ACME Plant Specs

PLC Mode

A PLC has basically two modes of operation: the Program Mode and some variation of the Run Mode. A three-position keyswitch may be used to select different processor modes of operation.

Remediation

- ***Program Mode*** is used to enter a new program, edit or update an existing program, upload files and download files. It is important to note that in this mode of operation all outputs are de-energized.
- ***Run Mode*** is used to execute the user program. Remote PLC programming or mode selection is disabled when the key is in the *Run Mode* position.
- ***Remote Run Mode (REM)*** allows the PLC to be remotely changed between program and run mode by a personal computer connected either directly or via a communication protocol to the PLC processor.Typically most processors are placed into *REM* mode to allow the engineering or maintenance staff the greatest flexibility when performing PLC programming tasks

Node: Chemical_plant (TIV Asset Node)

Overall result: Failed @ 3/9/21 8:21 AM

Element: asset-data

Result

Failed

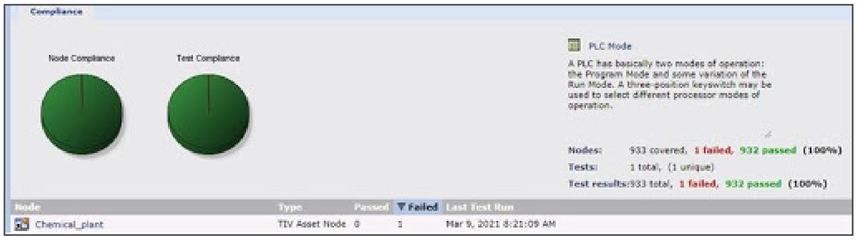
Time

3/9/21 8:21 AM

Actual

children.[2].custom_informations.[2].val=Remote Program Mode

Fig. 1 Tripwire Enterprise Report Viewer displaying a Remote Node Check.



PLC Mode

A PLC has basically two modes of operation: the Program Mode and some variation of the Run Mode. A three-position keyswitch may be used to select different processor modes of operation.

Nodes: 933 covered, 1 failed, 932 passed (100%)
Tests: 1 total, (1 unique)
Test results:933 total, 1 failed, 932 passed (100%)

Node	Type	Passed	▼Failed	Last Test Run
Chemical_plant	TIV Asset Node	0	1	Mar 9, 2021 8:21:09 AM

Fig. 1 Tripwire Industrial Visibility dashboard displaying Node and Test Compliance results.

Tripwire Enterprise

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

Addressing OT Compliance

With automated, continuous monitoring across different types of operating systems, industrial devices, and applications, industrial organizations rely on it as a simplified and cost-effective solution for maintaining system hardening and continual proof of compliance for 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 Visibility. Using these two advanced solutions together bridges the cybersecurity gap common in industrial organizations. 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. 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. It also aligns systems to best practice frameworks like the CIS ICS CSC. Get unmatched visibility into the configuration and vulnerability states of both the IT and OT sides of your organization at once.

Schedule Your Demo Today

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

tripwire®

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