

Tripwire Industrial Visibility

Automated ICS Network Mapping for Maximum Uptime

Bringing Industry 4.0 to the shop floor presents OT professionals with new cybersecurity concerns.

Tripwire Industrial Visibility is the only industrial cybersecurity solution on the market that provides true, real-time visibility for levels 1–5 without disrupting operations.

If you're in charge of keeping an industrial control system (ICS) secure, you know how difficult it is to get an accurate picture of what's happening on all your network devices—especially when you've got both legacy and modern technology at play. Tripwire® Industrial Visibility solves operational challenges with continuous threat monitoring and advanced logging intelligence that gives you deep, granular ICS visibility.

Tripwire Industrial Visibility gathers threat data that could threaten the safety and availability of your OT environment by analyzing network traffic and conducting deep packet inspection. It's fluent in over 42 of the native industrial protocols commonly found in ICS—the highest number of protocols covered by any solution in the industry—making sense of the floods of data produced by your entire range of IIoT-connected industrial devices.

It taps into OT network communication by listening through the SPAN port of routers and switches connected to the network segment, opening data packets and interpreting protocols without disrupting normal operations. As you know, legacy OT networks can be sensitive to latency and bandwidth change—which is why Tripwire Industrial Visibility uses agentless monitoring and an integrated combination of passive and active asset discovery that leaves your network undisturbed.

Get an Accurate Map of Your Network

So what does Tripwire Industrial Visibility do with the data it gathers? Over a period of weeks, it uses machine learning to construct a baseline of normal operations which is then used to detect anomalies. By reading network traffic, it isolates all assets on your network and maps the flow of traffic between them. This data is then used to create graphical network maps that make it easier to visualize activity and to notice unplanned changes before any damage is done.

It also simulates attacks on critical assets to help you understand their exposure. Taken together, these features help Tripwire Industrial Visibility secure ICS networks in a way that's perfectly optimized for OT applications. Tripwire Industrial Visibility is the only industrial cybersecurity solution on the market that provides true, real-time visibility for levels 1–5 without disrupting operations.

Proactively Fix Vulnerabilities

Once you know what's really going on in your OT environment in terms of connected devices and network traffic, you can use Tripwire Industrial Visibility to drill down and look at common vulnerabilities and exposures (CVEs). These CVEs are publicly available and continuously updated in a centralized clearinghouse where emerging vulnerabilities are posted and verified. If you're using a particular version of firmware or device model, you'll be equipped with actionable information about any known cybersecurity risks associated with it.

Detect Threats Sooner

Unlike IT networks, OT networks have a preponderance of repetition and predictable, consistent behavior. For example, a manufacturing environment may have to deliver thousands of the same candy bar every day. Electrical utilities must deliver electricity within a narrow window of performance.

This repetition makes it easier to distinguish normal from abnormal behavior. When Tripwire Industrial Visibility uses machine learning to understand what "normal" looks like on your network, it creates a secure baseline and generates actionable alerts anytime unexpected behavior occurs. Inappropriate changes in configuration and unusual commands are compared against baseline behavior to identify intruders.

For example, if files start disappearing or data begins offloading, the suspicious behavior triggers an alert providing immediate situational awareness. This baselining approach means you'll be alerted when an adversary is on your network. Social engineering and other methods of passwords exfiltration traditionally make it hard to catch invalid users. However, Tripwire Industrial Visibility can flag intruders even if they've successfully stolen legitimate credentials—their login info may look unremarkable, but their behavior will deviate from normal.

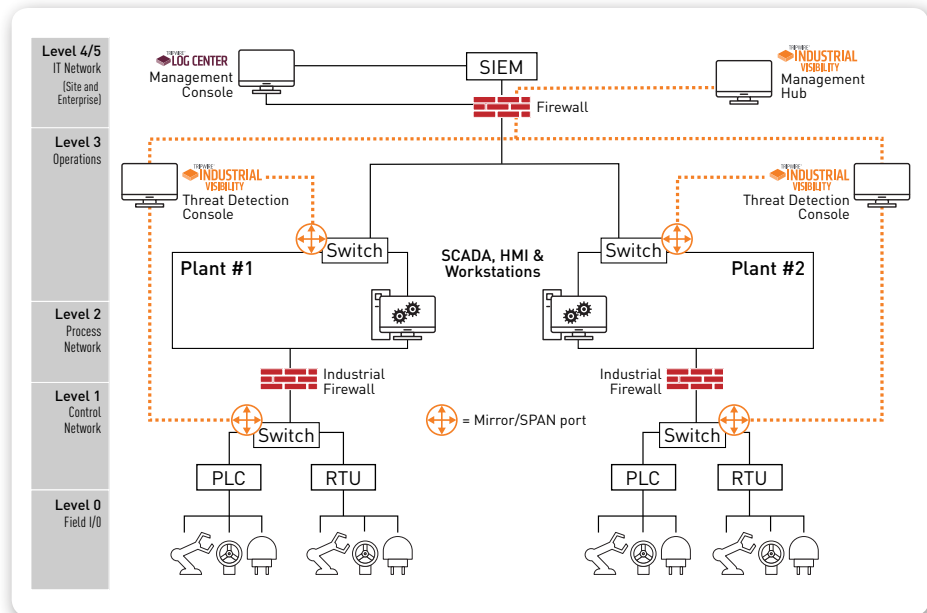


Fig. 1 Tripwire Industrial Visibility employs sensors throughout your OT network to provide complete visibility to provide integrity and resilience.

Block Attack Vectors

ICS attackers have a number of motives. You need to be ready for a broad range of breach scenarios, such as disgruntled employees wanting to compromise productivity, competitors attempting intellectual property theft, and even state-sponsored or organized criminal attacks on critical infrastructure. Tripwire Industrial Visibility helps you pinpoint your most sensitive assets and understand how they can be reached through various attack vectors in your network.

For example, someone overseeing a shop floor in an oil refinery may know that their most sensitive asset is the system that maintains oil temperatures. A hacker enters an email server by way of an internet-connected device. How do they get from the email server to their target? The hacker needs to follow a path to their target from IT to OT using crackable devices as stepping stones. That's why ICS operators need to have an accurate network map that details each device's known vulnerabilities. You can use that information to block

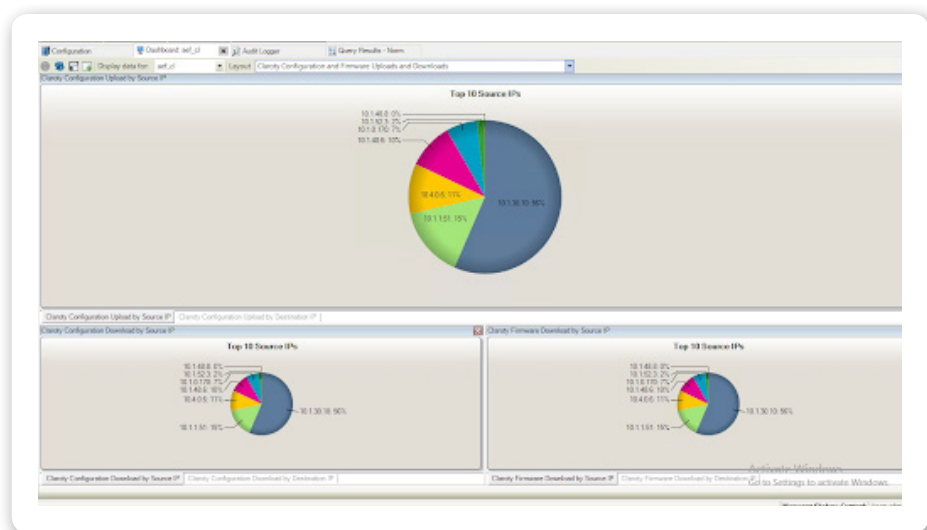


Fig. 2 Top destination and source IPs.

the hacker's path to your most sensitive asset.

Essentially, you can use Tripwire Industrial Visibility's threat modeling feature to learn what devices are connected to your sensitive assets and break the links your adversaries could use to reach those assets. When you highlight a sensitive asset, Tripwire Industrial Visibility will then posit attack vectors that could be executed against it.

Tripwire Industrial Visibility's log management feature helps bring your ICS into alignment with industrial cybersecurity best practice standards like IEC 62443 and NIST.

Automate Security Controls


Tripwire Industrial Visibility leverages change management, event logging, passive monitoring and active scanning. Tripwire and its parent company, Belden, offer over 20 years of experience in leading global cybersecurity solutions, and over 100 years in supporting the world's largest industrial businesses.

Change management

Tripwire Industrial Visibility reads configuration changes as they're made to log and report modifications. You'll be able to detect a suspicious change—such as credential escalation—before it results in real harm to your OT environment's process and product.

Event logging

Logging change events makes it possible to reset a penetrated system to its last known good state, reducing mean time to repair. Tripwire Industrial Visibility includes Tripwire Log Center™, which gathers and aggregates event logs across multiple devices. Tripwire Log Center normalizes the data carried by varied devices and Syslog inflows. It then correlates events from that data,



The screenshot shows a web interface titled "Event Details" with a search bar and a table of event logs. The table has columns for ID, DESCRIPTION, TYPE, and TIMESTAMP. The data is as follows:

ID	DESCRIPTION	TYPE	TIMESTAMP
10771	MODBUS: Schneider command - Get PLC Status	BaselineDeviation	18/06/2018, 16:45
10772	MODBUS: Schneider command - Query Diagnostics	BaselineDeviation	18/06/2018, 16:45
10773	MODBUS: Schneider command - Keep PLC Reservation	BaselineDeviation	18/06/2018, 16:45
10774	MODBUS: Schneider command - Read Memory Block (Block: 10)	BaselineDeviation	18/06/2018, 16:45
10775	MODBUS: Schneider command - Read Memory Block (Block: 20)	BaselineDeviation	18/06/2018, 16:45

Fig. 3 Event data obtained from device communications is normalized and presented as an event log.

displaying actionable insights in a clear dashboard view.

Advanced scanning

The solution uses a combination of passive monitoring and active scanning to avoid disrupting sensitive legacy systems. A strategic combination of agentless and agent-based scanning keeps legacy systems up and running. Unlike traditional vulnerability management (VM) and security configuration management (SCM) products, it employs no-touch sensing that can be used when legacy systems would otherwise crash when polled.

Because operations vary from organization to organization, Tripwire helps you manage your network based on its specific requirements. This includes passive monitoring, active scanning, or and hybridized approach—all without network disruption.


Summary

Tripwire Industrial Visibility provides ICS operators total clarity into the devices and activity on their network. It uses change management, event logging, and threat modeling to help you keep your most sensitive assets out of reach of intruders. By using sophisticated scanning and detection, the solution protects the core integrity and cyber resilience of your OT environment to keep you operating at peak availability and uptime.

Ready for a Demo?

Let us take you through a demo of Tripwire Industrial Visibility and answer any questions you have.

Visit tripwire.com/contact/request-demo.



As a Belden company, Tripwire is uniquely positioned to bridge the cybersecurity gap between your IT and OT environments. Tripwire solutions integrate seamlessly with the industrial products you already have in play, like Tofino firewalls and Hirschmann switches.



Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at [tripwire.com](https://www.tripwire.com)**

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