Tripwire Industrial Solutions Catalog

Cybersecurity for the Modern Industrial Control System






FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT/OT OPERATIONS

See It, Stop It and Monitor It, From the Top Floor to the Shop Floor

Whether your security strategy is driven by complex compliance standards such as NERC CIP, NIST and NEI, your organization seeks to follow industry best practices such as the Center for Internet Security's CIS Controls, or even if you're just beginning exploring how to implement cybersecurity strategies for your OT environment, Tripwire offers a suite of trusted security solutions for your Industrial Control Systems.

Tripwire provides deep visibility through a comprehensive suite of highly-integrated products to detect cyber threats and breaches, prevent future incidents by discovering and prioritizing risks, and continuous monitoring to help keep your security program on track.

Trusted by half the Fortune 500, 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. Call us today at 1.800.TRIPWIRE.

The Three Principles of ICS Security

- **Visibility**: You need to know what's on your network to secure it. Tripwire solutions deliver superior visibility and asset detection, reading 135 industrial protocols and mapping protocol communication patterns.
- **Prevention**: Tripwire solutions enforce security controls to harden your ICS against anomalous behavior and keep you compliant with standards such as NERC CIP and IEC 62443.
- **Monitoring**: Tripwire solutions are non-disruptive while reading configuration and log changes, and provide actionable alerts in real time so you always know what's happening on your network.

Tripwire compliance policies support the frameworks of over 42 entities, including:

IEC · NEI Nuclear Energy Institute · ISO 27001 · American Water Works Association · NERC North American Electric Reliability Corporation · NIST

TRIPWIRE®
ENTERPRISE

Tripwire Enterprise is an industry leading security configuration management (SCM) suite that provides a full integrated solution for configuration policy, file integrity and remediation management. With compliance polices that support the framework of more than 42 entities, the suite lets IT and OT cybersecurity, compliance and IT/OT operations teams rapidly achieve a foundational level of security throughout their IT and OT infrastructures by reducing the attack surface, increasing system integrity and delivering continuous compliance.

The suite has an unprecedented number of configuration policies from regulatory and industry guidelines such as IEC 62443, NIST 800-53, ISO 27001, and many others. To help provide holistic visibility to which assets are running within your ICS, Tripwire Enterprise integrates with Rockwell Automation FactoryTalk AssetCentre, MDT Autosave, and KEPServerEX, as well as industrial protocol support with Modbus TCP and Ethernet/IP CIP. This is also inclusive of leveraging other agentless data collection mechanisms with SNMP and web user interfaces.

Download the Tripwire Enterprise Datasheet

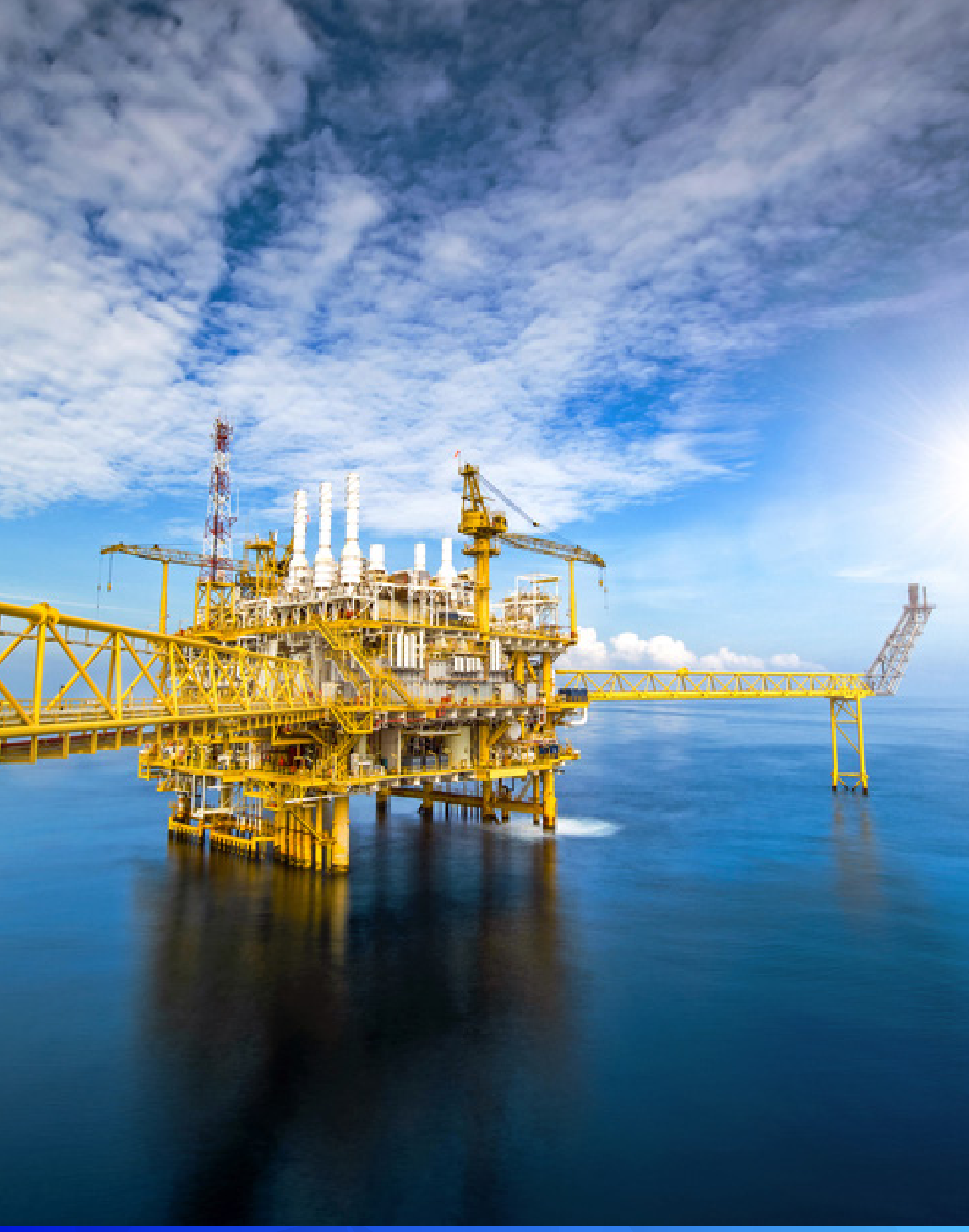
TRIPWIRE® INDUSTRIAL VISIBILITY

Tripwire Industrial Visibility gathers asset inventory and threat data to improve the safety and availability of your OT environment. It does so by analyzing network traffic and conducting protocol deconstruction to inventory assets, create network topology, and more. It's fluent in over 135 of the native industrial protocols commonly found in ICS—the highest number covered by any solution in the industry—making sense of the floods of data produced by your entire range of IIoT-connected industrial devices.

Tripwire Industrial Visibility analyzes network communication by listening through mirror or SPAN port of your industrial switches, interpreting and dissecting protocols without disrupting normal operations. Legacy OT networks can be sensitive to latency and bandwidth change—which is why Tripwire Industrial Visibility uses agentless monitoring to help keep your network undisturbed.

Tripwire Industrial Visibility provides ICS operators with holistic visibility into the devices and activity on their network. It can detect controller configuration and mode changes, comes with event logging capabilities for trending/dashboards, and performs threat modeling to help you keep your most sensitive assets out of intruders' reach. This solution protects the core integrity and cyber resilience of your OT environment, using sophisticated monitoring and detection to keep you operating at peak availability and uptime.

Download the Tripwire Industrial Visibility datasheet



TRIPWIRE®
LOG CENTER

Tripwire Log Center™ collects, analyzes and correlates log data from devices, servers and applications. Why does this matter in an ICS context? ICS create a staggering amount of data, and Tripwire Log Center helps you cut through the noise and focus only on what matters by pre-processing data before filtering it into your security information and event management system (SIEM). This data can be extremely helpful when creating a proactive maintenance strategy—for example it can send an alert if a patch cord is about to fail.

Tripwire Log Center's passive asset discovery capability allows you to discover previously unidentified assets through analysis of their log data. After discovery, the assets can then be added to your environments for further monitoring.

You can think of Tripwire Log Center as a cyber historian for the industrial network, in that it can captures and analyzes log diagnostic and cybersecurity information the helps you stay operational. Log management is a best practice that is referenced by many ICS cybersecurity frameworks and regulations (including but not limited to IEC62443, NERC CIP and NIST SP 800-82.

Download the Beginner's Guide to Industrial Tripwire Log Center Deployments

TRIPWIRE® IP360

While your assets in the lower levels of the Purdue model (cell/area zones) may not be suitable for active scanning techniques, devices like HMIs and engineering workstations in the manufacturing zone and DMZ will benefit from an in-depth vulnerability scan from a vulnerability management tool like Tripwire IP360™.

Tripwire IP360's unique scanning methodology produces the most granular and accurate vulnerability score prioritization in the market. The use of multiple scoring systems allows for audience-specific reporting, and it offers an open API for custom integrations.

The quality of the data collected is at the heart of any vulnerability management tool. Tripwire IP360 finds more vulnerabilities with greater accuracy, period. And it will show you exactly how it detected every condition. Automated discovery, profiling and scanning save security teams time and resources.

The actionable analytics and reporting available in Tripwire IP360 are backed by a dedicated world-class Vulnerability and Exploit Research Team (VERT).

Download the Tripwire IP360 datasheet

Tofino Xenon Industrial Security Appliance

In a class by itself, Tofino Xenon is versatile, rugged and is an ideal solution for protecting the operation of industrial control systems. It is so much more than an industrial firewall. Not only can it perform deep packet inspection (DPI) on industrial protocols to ensure, for example, that Modbus traffic is writing and reading to the right set of registers, it can also do protocol anomaly detection without the need for signature updates to stop zero day attacks. From initial installation to ongoing operation, the one purpose is to keep the industrial process running. Network architecture changes are not required, as the Tofino Xenon operates at the data link layer (layer 2 of the OSI network model) and is therefore transparent on the network as it does not have an IP address. Control engineers can define rules that specify which devices are allowed to communicate and which protocols they may use.

Tripwire offers the only product that can detect a Tofino Xenon—together they provide unparalleled monitoring and detection of anomalous behavior for any industrial automation environment such as manufacturing plants, oil & gas, water/water waste, etc.

Download the Tofino Xenon Industrial Security Appliance datasheet

ICS Professional Services from Tripwire

Many industrial organizations lack the robust security team necessary to implement and maintain rigid ICS security controls. Tripwire offers a range of professional services customized for industrial environments.

Industrial Security Assessments

Conducting a network vulnerability assessment on your industrial organization has changed from a beneficial activity into a necessary one. Tripwire's skilled team of engineers identifies weaknesses and prioritizes them. We collect data from automated vulnerability scanners, proprietary tools and manual assessment efforts to create a normalized list of identified exposures.

Download the Industrial Cybersecurity Assessment services brief

Penetration Testing

Penetration tests—pen tests—are a type of ethical hacking used to regularly evaluate the security of a network. Our team of highly-skilled cybersecurity experts utilizes a combination of tactical and strategic approaches to discover and exploit vulnerabilities in your IT systems through penetration testing and assessing your security program.

Download the Penetration Testing Assessments services brief

Resident Engineers

Tripwire resident engineers serve as an expert-level, dedicated on-site resource to manage your Tripwire solution. Our resident engineers are focused on ensuring that you get the most value out of your Tripwire investment as it relates to your business, security and compliance objectives.

Download the Tripwire Professional Services Overview brief

Request a Demo

Ready to learn more? Let us take you through a demo of these industrial security solutions. We'll show you powerful features and answer any of your questions.
Visit tripwire.com/contact/request-demo or simply call us at 1.800.TRIPWIRE.






Tripwire Product Selection Chart

Feature	Tripwire Enterprise	Tripwire Industrial Visibility	Tripwire Log Center	Tripwire IP360	Description
Asset Discovery and Inventory					
Active Data Collection	✓	✓		✓	**Tripwire Enterprise** achieves active data collection by discovering and inventorying devices through native protocols, Modbus TCP and Ethernet/IP CIP. Tripwire Industrial Visibility achieves this as well through over six industrial protocols.
Passive Data Collection		✓			**Tripwire Industrial Visibility** dissects a copy of network traffic via a SPAN, mirror port, or network TAP.
Hybrid Data Collection	✓	✓			**Tripwire Enterprise** through integrations with Rockwell Automation FactoryTalk AssetCentre, Kepware and MDT Autosave.
Vulnerability Assessment	✓	✓		✓	**Tripwire Enterprise** does through integration with FactoryTalk AssetCentre. **Tripwire Industrial Visibility** achieves through passive and hybrid data collection. **Tripwire IP360** is an active scanning/polling technology, and is an overall vulnerability management solution.
Configuration Assessment or Configuration Compliance	✓				**Tripwire Enterprise** can assess configuration against industrial IEC 62443, NIST 800-53, ISO 27001 and the CIS Controls.
Change Detection	✓	✓			**Tripwire Industrial Solution:** Tripwire Enterprise detects changes to monitored assets. **Tripwire Industrial Visibility:** Configuration and other changes detected in network traffic can be detected by Tripwire Industrial Visibility.
Log Management		✓	✓		**Tripwire Log Center** collects and stores log messages, including those provided by **Tripwire Industrial Visibility**.
Network Devices & SCADA Systems	✓	✓			Network devices can be scanned actively with **Tripwire Enterprise**, network device logs can be collected by **Tripwire Log Center**. **Tripwire Industrial Visibility** detects flow of traffic through a network, and activity related to the network assets.
Reporting and Analytics	✓	✓	✓	✓	**Tripwire Enterprise** (Tripwire Industrial Solution) and **Tripwire Log Center** (Tripwire Industrial Visibility) have available reports. **Tripwire Whitelist Profile**r (a Tripwire Enterprise extension, part of the Tripwire Industrial Solution) includes additional Tripwire Enterprise reports.
Centralized Operations	✓	✓			**Tripwire Industrial Solution:** FIM and SCM data from Tripwire Enterprise and Tripwire Whitelist Profiler. **Tripwire Industrial Visibility:** Log data and network alerts from Tripwire Log Center and Tripwire Industrial Visibility.

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 or 1.800.TRIPWIRE**

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

BRTISC2a 1906