DATASHEET

Tripwire Industrial Visibility

Full Visibility and Fundamental Controls for OT Environments

Digitalization initiatives have transformed enterprises, causing once-isolated operational technology (OT) networks to become interconnected with their information technology (IT) counterparts. The result is the rise of converged IT-OT corporate networks that IT security teams are increasingly responsible for protecting. The challenge is the OT portions of these networks typically comprise proprietary protocols and unfamiliar assets, making them incompatible with IT security tools and invisible to IT security teams.

Tripwire® Industrial Visibility was designed to overcome this challenge. It extends the same controls IT security teams utilize for minimizing risk in IT environments to OT environments.

These controls cover:

- Automatically discovers and manages all OT assets
- AI-driven network zoning and segmentation
- Known and zero-day threat and anomaly detection
- Exact match vulnerability detection
- Change detection
- Log management
- Managed services
- Firewall integration
- Monitors changes to process values
- Asset Management

Tripwire Industrial Visibility leverages the broadest and deepest OT protocol coverage in the industry and unmatched passive, active, and AppDB scanning capabilities to provide comprehensive OT visibility and asset management controls. Tripwire Industrial Visibility offers a high caliber of visibility across all three OT dimensions integral to effective risk calculation and reduction:

1. **Asset visibility:** This encompasses all assets on an OT network, including serial networks, as well as extensive attributes about each asset, including model number, firewall version, and card slot, among others.
2. **Session visibility:** This includes all OT network sessions along with their bandwidth, actions taken, changes made, and other details relevant to OT network sessions.
3. **Process visibility:** This includes tracking of all OT operations, as well as the code section and tag values of all processes with which OT assets are involved.

Threat and Anomaly Detection

Tripwire Industrial Visibility utilizes five detection engines to automatically profile all assets, communications, and processes in OT networks, generate a behavioral baseline that characterizes legitimate traffic and weeds out false positives, and alerts users in realtime to

Key Benefits

- Extends fundamental IT security controls to OT environments
- Provides complete visibility into previously invisible networks
- Continuously detects anomalies, known threats, and zero-day attacks
- Root-cause analysis and risk-based scoring for all alerts
- Prebuilt customizable reports and dashboards
- Seamless integration with IT security infrastructure
- Features both active and passive data collection methodologies

Tripwire Enterprise Integration

Tripwire Industrial Visibility now integrates with Tripwire Enterprise, bringing all OT assets into one view. This integration allows you to use Tripwire Enterprise and Tripwire Connect reporting capabilities on OT assets and run Tripwire Enterprise policies to ensure alignment with OT best practice frameworks and standards like IEC-62443.

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

anomalies and both known and zero-day threats.

OT specific threat intelligence: Tripwire Industrial Visibility includes OT-specific threat intelligence that is updated in real-time to support swift detection of malware-related threats.

Contextual alert risk scoring: This single metric is based on the unique context in which each alert is triggered, enabling users to easily filter out false positives and quickly understand and prioritize alerts for triage and mitigation.

Root cause analysis: This feature groups all events related to the same attack or incident into a single alert, providing a consolidated view of the chain of events, as well as a root-cause analysis. The result is a higher signal-to-noise ratio, fewer false positives, reduced alert fatigue, and thus more efficient and effective triage and mitigation.

Network Segmentation

The extensive OT visibility Tripwire Industrial Visibility provides enables it to automatically map and virtually segment OT networks into virtual zones, which are logical groups of assets that communicate with one other under normal circumstances.

- Cross-zone violations yield real-time alerts that are automatically scored based on risk to help security teams prioritize
- Customers without existing physical or logical segmentation can use virtual zones as a cost-effective alternative
- Customers seeking to implement physical or logical segmentation accelerate such initiatives using virtual zones as the blueprint
- Customers can integrate Tripwire Industrial Visibility with their existing firewalls and network access control (NAC) products to proactively enforce policy-based segmentation and mitigate active attacks

Vulnerability Management

Tripwire Industrial Visibility automatically compares each asset in an OT environment to an extensive database of insecure protocols, configurations, and other vulnerabilities tracked by Tripwire, as well as to the latest common vulnerabilities and exposures (CVE) data from the National Vulnerability Database. As a result, users can identify, prioritize, and remediate vulnerabilities in OT environments more effectively.

Exact-match vulnerabilities: The complete OT visibility, including granular details about each asset, provided by Tripwire Industrial Visibility facilitates easy and accurate identification of exact-match vulnerabilities.

Attack vector mapping: This feature identifies and analyzes all vulnerabilities and risks in an OT environment to automatically calculate the most likely scenarios in which an attacker could compromise the environment. It also provides mitigation recommendations for each scenario.

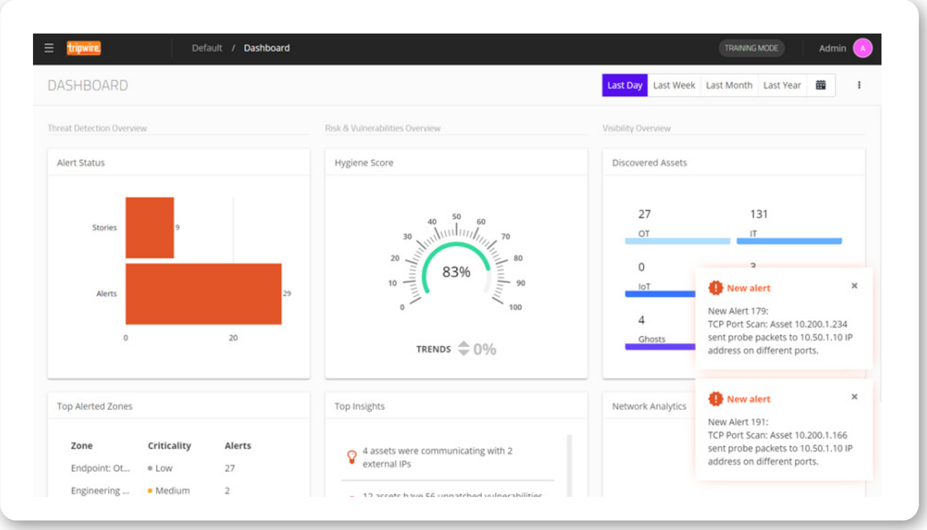
Risk-based prioritization: All vulnerabilities are automatically evaluated and scored based on the unique risk they pose to each OT environment, enabling more efficient and effective prioritization.

Log Management

Your instance of Tripwire Industrial Visibility comes bundled with Tripwire Log Center™, a powerful aggregation tool with built-in intelligence that inspects logs for devices and IP addresses. Tripwire Log Center gives you granular asset discovery on an ICS scale, and it does so without interfering with plant performance, unlike other asset discovery solutions on the market. Tripwire Log Center helps you get started quickly with security solution packs for the following situations:

- Insider threats
- Breach detection
- DDoS detection
- Authentication
- User audits
- Intrusion detection

Tripwire Log Center integrates with your existing infrastructure, including Hirschmann switches and Tofino security appliances, and includes a growing library of available correlation rules, empowering your team to monitor, detect and quickly respond to threats in your environment. It can also find industrial network misconfigurations by highlighting master clock sync issues, duplex mismatches, and CRC errors with not only your Hirschmann switch



New alert

New Alert 179:
TCP Port Scan: Asset 10.200.1.234 sent probe packets to 10.50.1.10 IP address on different ports.

New alert

New Alert 191:
TCP Port Scan: Asset 10.200.1.166 sent probe packets to 10.50.1.10 IP address on different ports.

Zone	Criticality	Alerts
Endpoint: Ot...	● Low	27
Engineering ...	● Medium	2

4 assets were communicating with 2 external IPs

12 assets have 56 unpatched vulnerabilities

Fig. 1 The default Tripwire Industrial Visibility dashboard presents a Threat Detection, Risk & Vulnerabilities and Visibility overview, with drill-down capabilities. Dashboards and associated widgets can be customized to meet your specific needs.

infrastructure, but with other switch vendors as well. This also drives maximum uptime and efficiencies throughout your industrial control networks.

Managed Services

Tripwire ExpertOps^{SM} Industrial Visibility is a managed services version of Tripwire Industrial Visibility. A single subscription provides personalized consulting from trained experts and hands-on tool management to help you achieve and maintain compliance and critical asset security. It gives stretched security teams an alternative to the difficult process of purchasing, deploying, and maintaining products.

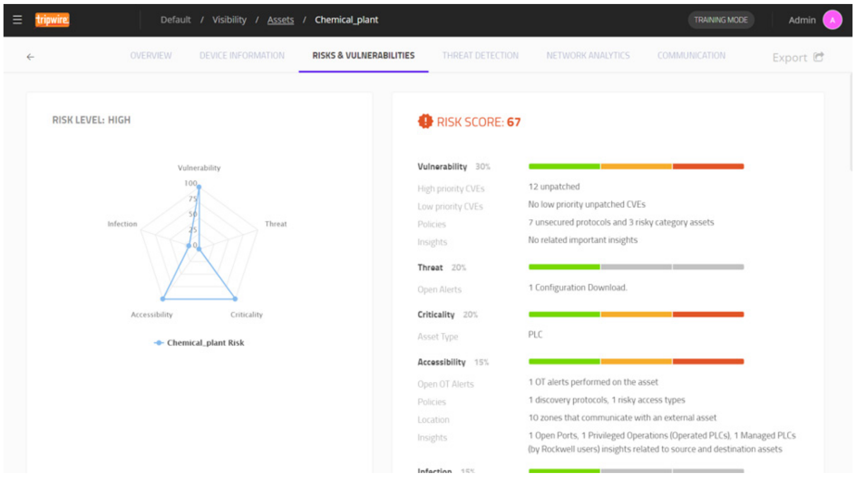
- **Ongoing support:** You'll be matched with a designated Tripwire expert who serves as an extension of your team by providing personalized advice, incident assistance, and audit support. You'll receive recommendations and organizational grading to maximize the value of Tripwire Industrial Visibility, as well as regular alerts and reports in your inbox.
- **System transparency:** How can your security team prioritize which system changes to address if they don't have deep visibility—let alone a detailed understanding of which changes are relevant? Tripwire ExpertOps Industrial Visibility provides you with security and compliance visibility.

Firewall Integration

The sensor technology of Tripwire Industrial Visibility is now embedded within the Hirschmann Eagle Firewall. This makes it so you don't need to set up a SPAN or mirror port on your switch. Take advantage of more out-of-the-box functionality and less setup effort. The Hirschmann multiport EAGLE40 next-generation firewalls expedite intrusion detection using DPI and SPI for hardened cybersecurity under the stringent conditions of today's industrial environments.

Summary

Tripwire Industrial Visibility provides extreme visibility, continuous threat and vulnerability monitoring, and deep insights into industrial control system networks. It's specifically designed to verify safe, secure and reliable operations in complex multi-vendor industrial networks—ensuring no impact to the underlying operational processes along with improved cyber resiliency. It extracts precise details about each asset on the industrial network, profiles all communications and protocols, generates a fine-grain behavioral baseline, and alerts you to network changes, threats and new vulnerabilities.



RISK LEVEL: HIGH

RISK SCORE: 67

Vulnerability 30%	
High priority CVEs	12 unpatched
Low priority CVEs	No low priority unpatched CVEs
Policies	7 unsecured protocols and 3 risky category assets
Insights	No related important insights
Threat 20%	
Open Alerts	1 Configuration Download.
Criticality 20%	
Asset Type	PLC
Accessibility 15%	
Open OT Alerts	1 OT alerts performed on the asset
Policies	1 discovery protocols, 1 risky access types
Location	10 zones that communicate with an external asset
Insights	1 Open Ports, 1 Privileged Operations (Operated PLCs), 1 Managed PLCs (by Rockwell users) insights related to source and destination assets
Infection 15%	

Fig. 2 The Risks and Vulnerabilities detailed view of an individual asset or zone is presented in a spider web chart that highlights five categories: Vulnerabilities, Threats, Criticality, Accessibility, and Infection. Details are provided to the right.

Schedule Your Demo Today

Let us take you through a demo of Tripwire security and compliance solutions and answer any of your questions. Visit **tripwire.com/contact/request-demo**

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