



Why Energy Utilities Can Count on Fortra's Tripwire

Energy Utility Cybersecurity Capabilities

As an energy industry professional, you understand the consequences of subpar protection and the need for reliable, iron-clad security controls. Evaluating new cybersecurity software to protect your energy environment shouldn't involve guesswork, especially when you are trying to match capabilities to your particular needs.

This datasheet provides a quick view of Tripwire's energy solution. See why so many of the world's leading energy utilities count on us to secure their environments with cost-effective, reliable, and user-friendly cybersecurity solutions.

CAPABILITY	FORTRA'S TRIPWIRE
File integrity and system state monitoring (E-FIM)	✓
Security configuration management (SCM)	✓
Automated multi-policy compliance, custom policy creation, and customizable reporting	✓
Dynamic software reconciliation for automatic file change validation against patch manifests	✓
Real time change intelligence with side-by-side change comparison	✓
Allowlisting with automated validation	✓
Automated NMAP scanning	✓
Vulnerability management with granular, prioritized risk scoring	✓
Comprehensive asset detection and system visibility	✓
High-volume log management for IT and OT devices with log correlation and normalization	✓
Non-disruptive monitoring for maximum uptime	✓
Integration with other IT and OT products	✓
Extensive API integrations making it fast and easy to add new devices	✓
Managed service offerings available	✓
Expert professional services and product training	✓

Leading the Way in Energy Cybersecurity and NERC Compliance

Tripwire is committed to meeting and exceeding the needs of our energy customers, and we do so with a multi-pronged approach that ensures a high level of support, education, and optimization:

NERC CIP Dashboard

The NERC CIP Dashboard within Tripwire Enterprise (TE) provides a centralized view of your compliance status across various NERC CIP requirements and offers insights into your NERC CIP baseline, reducing the required labor of the monitoring process.

Get real-time insights into security configurations to see where your organization is falling short of compliance.

COCR Rules

Tripwire helps energy customers use Command Output Capture Rules (COCR) to automate compliance tasks through scripting. Create customized scripts to consistently enforce security policies across your systems.

Rich Integration

Tripwire readily integrates with change management ticketing systems, GRC, CMDB, ITSM, SIEM, and more.

Advanced Scalability

Unlike most of our competitors, Tripwire scales right along with your organization's growth. Adding new network devices, for example, is a quick and simple task with Tripwire. Whether you have tens — or tens of thousands — of devices, Tripwire easily scales to environments of any size. Tripwire is uniquely positioned to baseline virtually anything; if there's a way to get the data, it can be integrated into your baselines.

Customizable Compliance Reporting

Tripwire's customizable compliance reporting is designed with NERC CIP auditors in mind, providing the exact types of proof points they look for to speed up the audit process and ensure success.

Multi-Policy Compliance

In addition, you can apply best practice frameworks like MITRE ATT&CK, NIST, and the CIS Critical Security Controls to further improve your security posture and shrink your attack surface. Tripwire has the broadest policy content library in the industry, so please let your Tripwire account manager know if there are other policies you are interested in.

Compare Patches to Manifests

Tripwire allows you to compare changes detected to the patch manifests to ensure the last stretch of the supply chain is secure. and helps you comply with CIP-010 specifications around BES cyber system baseline configuration requirements.

Professional Services

Tripwire's extensive professional services are here to help you implement and refine your cybersecurity and compliance programs with tailored assessments and training sessions led by cybersecurity and NERC CIP experts.

"Tripwire has helped us further increase our security presence and reduce our risk. I've been really impressed with it. I'm usually vendor agnostic, but I tell people: 'Go Tripwire.'"

— Energy Utility Information Security Supervisor

Tripwire Solutions for Energy Utilities

Tripwire stands apart from the rest because no other solutions provide equivalent breadth and depth of coverage — from more types of environments and assets covered to more policy and platform combinations (4,000+ and counting). There isn't much you can't do with Tripwire powering your cybersecurity and NERC CIP compliance programs.

Tripwire Enterprise

Tripwire® Enterprise is the leading compliance monitoring solution, using file integrity monitoring (FIM) and security configuration management (SCM).

- **File integrity monitoring:** Originally introduced by Tripwire, this security control now encompasses much more than files — tracking changes against a secure baseline across enterprise assets and environments.
- **Baselining capabilities:** Deviations from compliance and cybersecurity best practice alignment are detected using the reference of a secure baseline state.
- **Security configuration management and policy compliance:** Continuously harden your systems against intrusion by maintaining proper configurations across your environment.
- **Side-by-side comparison of changes:** Side-by-side comparison helps illustrate the potential impacts of a particular change.
- **Real-time change detection:** Rather than intermittent scanning, Tripwire Enterprise detects changes in real time to alert you right away.

- **Contextual change data:** See what changed, where, when, and who made the change. This deeper context helps you act quickly to stop threats in their tracks.
- **Dynamic software reconciliation:** Tripwire Enterprise hides routine changes to eliminate excess alert noise for your staff.
- **Support for the entire enterprise:** Monitor the integrity of on-premises, cloud, hybrid, virtual, and OT industrial environments.
- **Dashboards and reports:** Detailed reporting offers insight into risk patterns across your organization, from the whole company to individual business units or departments.
- **Custom policy creation:** Create and enforce your own compliance policies to match internal organizational standards.

Tripwire's Allowlisting Solutions

Tripwire's allowlisting solutions ensure the compliance and security of your network by monitoring the system against lists of what's allowed to run. Aside from securing your network, the automated report generation will save you time on preparing for audits and money by reducing findings within those audits.

- **Allowlisting:** Defines records in centralized allowlist configuration files
- **Validation:** Automates the validation of detected system configurations against your allowlist
- **Reporting:** Generates detailed system configuration reports

Tripwire LogCenter

Tripwire LogCenter® centralizes log management with reliable and automated log collection, analysis, storage, and delivery. It seamlessly integrates with Tripwire Enterprise and Tripwire's vulnerability management solution to identify and address anomalies and suspicious activities, differentiating the valuable insights from the surrounding noise. It collects, analyzes and correlates log data from network devices, controllers, SCADA, servers and applications.

- **Agent-Based and Agentless Coverage:** The Tripwire Axon® agent ensures that the log data it collects is safe in the event of system failure, and Tripwire LogCenter supports agentless log collection where necessary as well.
- **Event Correlation:** Its correlation engine uses prebuilt rules made for your existing platforms, security use cases, and compliance needs — and even allows you to create your own custom rules.

Vulnerability Management

Fortra provides a leading vulnerability and security risk management system that enables organizations to cost-effectively measure and manage their network security risk.

- **Asset Discovery and Management:** Get total visibility into what's on your network on-premises and in the cloud, along with devices and their vulnerabilities.
- **Vulnerability Scanning:** Agentless and agent-based scanning allows you to find vulnerabilities in dynamic IP endpoints, containers, and more.
- **Vulnerability Risk Scoring:** Granular risk scoring system enables you to tackle the most potentially damaging risks fastest.

Tripwire Managed Services

Tripwire's managed cybersecurity service offerings equip you with the advice and support needed to protect your data from cyberattacks while keeping up with regulatory compliance.

- **Managed Service Option:** Take advantage of all the capabilities of Tripwire Enterprise and/or vulnerability management as a managed service, with a dedicated Tripwire expert running your solution(s) while supporting you every step of the way

Summary

With more than 25 years of experience on the front lines of cybersecurity and compliance development, Fortra's Tripwire has had time to listen to hundreds of energy customers and use their real-world experience to optimize our solutions and build in a holistic range of capabilities unmatched by other providers. Schedule a personalized demo at www.Tripwire.com/demo.

FORTRATM

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.