



CASE STUDY (TRIPWIRE)

Fortune 250 Electric & Gas Utility Trusts Tripwire for Unbeatable Accuracy

Scalable, Automated NERC CIP Compliance

Electric and gas utilities and other industrial organizations take solution procurement seriously because they know what's at stake if they fail a North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) or a TSA pipeline security audit, or become the target of a cyberattack. With many cybersecurity and compliance solutions to choose from, it can be hard to know where to start. So why did one Fortune 250 Energy Company select Fortra's Tripwire solution suite for their 1,000+ NERC CIP assets, 2,000 IP addresses, and thousands of industrial assets?

Following a challenging NERC CIP audit, this energy company determined it needed an automated, industry-standard solution to reduce compliance risk and manual efforts. They needed solutions that could accurately handle monthly configuration baselining of the assets for NERC CIP-010 R1 and R2, perform discovery for all unauthorized changes, and achieve 90%+ automation.

For security configuration management (SCM) and baselining, their previous solution was too cumbersome to manage. It wasn't scalable and did not deliver on the automation capabilities that were originally promised. The process was too manual, and the solution required a lot of continuous attention. For vulnerability management and asset discovery, there were difficulties with scanning extremely sensitive control systems using a cloud-based solution that had negative consequences to the control systems. The existing reporting tool was also difficult to use, with too much data and not enough prioritization.

Like many customers migrating to Tripwire, they attributed their decision based largely on experiencing inaccurate results as compared to Tripwire for software changes, version changes, install dates, ports and services reporting, and monitoring "new" asset types for NERC CIP. They made the decision to transition because of Tripwire's solution approach and trusted leadership in the energy and industrial control systems market.

AT-A-GLANCE

Industry	Electric & Gas Utilities
Headcount	10,000+
Customer Since	2016

KEY SOLUTIONS

Tripwire® Enterprise, Tripwire IP360™, Tripwire State Analyzer, Tripwire LogCenter®

BUSINESS NEEDS

- Highly accurate compliance data for NERC CIP, the TSA Directive, and PCI
- Increased granularity of change detection process
- Defined baseline configurations for components across the entire infrastructure
- Enterprise scalability beyond industrial control systems

RESULTS

- Granularity of detail in reports
- Time savings from automation capabilities
- Deep integration with the company's other existing security hardware and software
- Broad and deep continuous monitoring

Following the success of the Tripwire deployment for NERC CIP compliance, this customer has continued to expand the use cases of Tripwire to address the TSA Directive for its gas assets, its IT assets for PCI compliance, and its Distribution Operations assets for industrial cybersecurity.

Business Needs

- Highly accurate compliance data for NERC CIP, the TSA Directive, and PCI
- Increased granularity of change detection process to avoid any unplanned or significant remediation challenges
- Defined baseline configurations for components across the entire infrastructure, including devices and other endpoints
- Enterprise scalability beyond industrial control systems; ability to cover both OT (Operational Technology) and IT (Information Technology) with a single solution

Tripwire Solutions

Tripwire offers truly scalable and easy-to-use solutions that are automated and have deep visibility, risk prioritization, and reporting capabilities. Tripwire Enterprise is the leading compliance monitoring solution, using file integrity monitoring (FIM) and security configuration management (SCM). Backed by decades of experience, it's capable of advanced use cases unmatched by other solutions in both IT and OT environments. For vulnerability management, industrial organizations use Tripwire IP360 to get complete visibility into their networks, including all devices and their associated operating systems, applications, and vulnerabilities.

To help with defining the project scope, schedule, requirements and cost estimate, Tripwire and the customer conducted a Professional Services Design & Architecture Engagement to thoroughly cover all the applicable technology with stakeholders, map the technology to a real

solution in the context of the environment, and capture all of this in a detailed document deliverable. The Design & Architecture Engagement helped this company overcome prior experiences with other projects that were not properly scoped and resulted in expensive re-design work.

“Tripwire has easier extended coverage. Tripwire supports protocols, not specific devices, so it is easier to extend what Tripwire is covering.”

Results

In addition to the added automation capabilities, this company's time is now better spent analyzing its data rather than manual efforts required by its previous solutions. Tripwire's rich integration ability made it easy for this company to not only fully integrate Tripwire but also its other existing security hardware and software. With Tripwire, this energy company can build enterprise scalability beyond industrial control systems that covers both IT and OT environments with a single solution.

The following results were achieved quickly upon implementing their Tripwire solutions:

- Granularity of detail in reports including the Tripwire IP360 heat map and risk prioritization
- Time savings from automation capabilities: time is now better spent analyzing the data rather than on manual efforts required of their previous solution
- Deep integration with the company's other existing security hardware and software
- Broad and deep continuous monitoring, plus high flexibility to easily configure monitoring of one-off assets

FORTRA™

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.