SOLUTION BRIEF

Tripwire Solutions for Industrial Automation

Hybrid "No-Touch" Approach to ICS Security with Tripwire and Rockwell Automation

Highlights

Tripwire delivers a new, innovative approach for assessing devices down to the PLC for vulnerability, changes and attacks, in a non-disruptive, non-invasive way that will appeal to automation and control engineering teams.

Industrial automation and process control systems largely run our world. However, cyber risks to industrial networks, endpoints and control systems are on the rise and protecting highly specialized plant environments can be very challenging for industrial businesses and critical infrastructure.

Cyber threats have been shown to come from simple employee or contractor error, malicious insiders or outside adversaries. Regardless of the source of cyber risk, cyber actions can have a physical impact within industrial sites ranging from disruption to damage.

In the best of cases, cyber risk should be assessed, prioritized and compensated for as a business risk issue for both plant and corporate sites. When gaps exist in the plant, protective steps can then be taken using defense-in-depth strategies for keeping Industrial Control Systems (ICS) such as programmable logic control systems (PLCs), remote terminal units (RTUs), intelligent electrical devices (IEDs), distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems safe.

A New "No-Touch" Hybrid Approach to ICS Security

Tripwire uses patented agentless technology ideally suited to a "no-touch" approach to ICS security. Tripwire® Enterprise interfaces with Rockwell Automation FactoryTalk AssetCentre to monitor and baseline project files within AssetCentre, and lets AssetCentre manage its assets, changes and communications with Rockwell Automation ICS and SCADA. This gives ICS automation and process control engineers assurance that production will be predictably available and undisrupted. Tripwire can deliver a monitored, secure system state baselined against best practices, processes and changes of interest with built-in guidance on what is happening and what to do about it.

"Hands-Off" ICS Security

One of the most foundational ICS security practices is to have a maintained asset inventory. Rockwell Automation provides this for the assets it knows about through FactoryTalk AssetCentre.

Industrial sites often have limited overall visibility to the degree of cyber risk inherent in plant operations and field or remote locations. ICS security risk is also difficult to measure and report upon.

Most ICS operations teams do not have the time, technology or training to identify and resolve cyber risks – after all, this is a much lower priority when compared to the requirement for smooth-running operations to meet production and business requirements. How much cyber risk does your plant or critical infrastructure site have in the environment? How would you know, and if you did know, what should you, or could you do about it?

ICS Configuration Assessment and Security Monitoring

Tripwire pioneered the technology used in monitoring the integrity of files, system configuration parameters, Windows registry, services such as remote access, DLL and OS changes etc, and then distilling this information down to appropriate operator alerts. This expertise is applied to monitor the integrity of FactoryTalk AssetCentre's project files and can give similar monitoring and assessment for an array of other vendor equipment present within industrial sites.

Often if a Demilitarized Zone (DMZ) (or Industrial DMZ – IDMZ) is present to separate plant and corporate networks, assets may be placed there such as historians, shared databases, web servers, Active Directory, email servers, remote access systems, patch management and Manufacturing Execution System (MES). To Tripwire, these and other systems in lower levels such as Human Machine Interface (HMIs), engineering workstations, operator consoles and various system and application servers can be assessed and monitored for changes of interest, vulnerabilities, weak or misconfigured settings and potential opportunity to advise how to harden those systems against cyber risk.

Tripwire also tracks ICS-CERT security advisories, Rockwell Automation vendor alerts, Cisco/Stratix vendor alerts, and combines them to provide intelligent vulnerability searches with guidance built in so plant teams do not have to be cybersecurity experts to understand whether a risk applies to your environment. This saves time and increases efficiency.

Know Your Assets and Reduce Cybersecurity Risks

- » Increase plant resilience
- » Lower cost of security
- » Use built-in templates and guidance
- » Stay on top with alerts and advisories

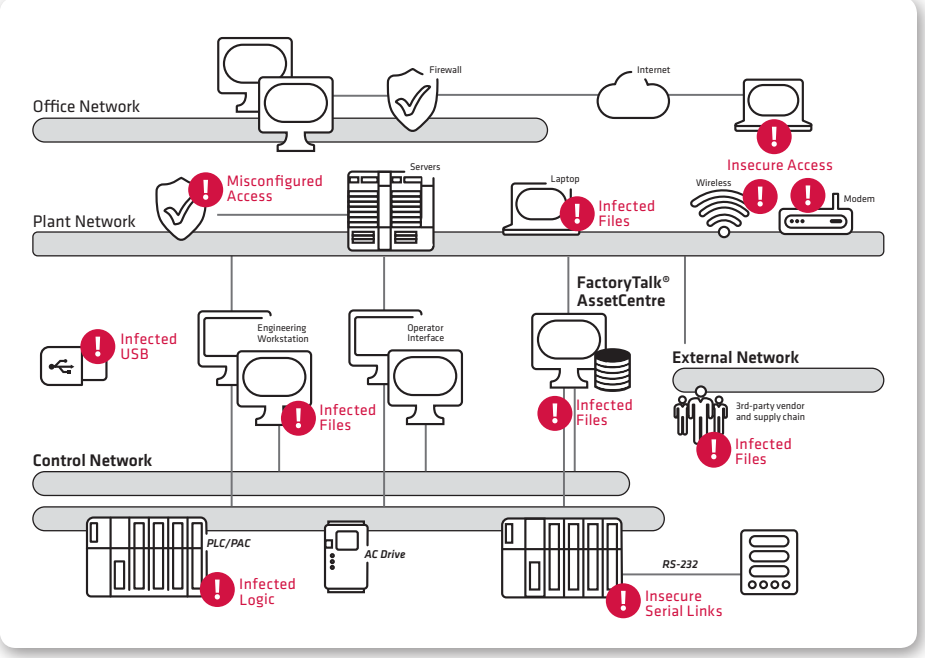

Fig. 1 Common industrial control vectors include misconfigurations, changes of interest, infected USB, insecure remote access, unauthorized access and more.

Industrial Standards and Best Practices Reduce Cyber Risk

Tripwire has known and validated best practices and industrial standards templates, both built-in and "out of the box." Such standards give organizations something to compare to and reach for in terms of growing their industrial cybersecurity awareness and skills. Important guidance, reference architectures and advice is given within most of the industrial standards. Examples of common industrial security standards and best practices in Tripwire are:

- IEC 62443
- NERC CIP
- NIST SP800-53r4
- ISO 27001
- The Center for Internet Security's CIS Controls (formerly the Top 20 Critical Security Controls)
- NEI 08-09 and others

Tripwire also includes a custom editor for creating your own rules and modifying existing templates. This provides for when specialized or legacy equipment needs unique policies to allow exceptions or waivers.

Tripwire Enterprise also has the ability to communicate via standard industrial protocols such as:

- Modbus TCP
- Ethernet/IP CIP
- SNMP v1, v2, v3

Another unique feature is Web Retriever, which allows Tripwire Enterprise to scrape web page configuration data.

Summary

Tripwire can extend the capabilities of Rockwell Automation® FactoryTalk® AssetCentre by adding Tripwire® Enterprise for Industrial Devices. This integrated solution allows engineers to monitor industrial automation networks, endpoints and control systems for secure configurations. It identifies unauthorized changes, cyber threats and security vulnerabilities and provide prioritized guidance to reduce risks without affecting operational availability, reliability or safety. Tripwire combines industry standards, Rockwell alerts, ICS-CERT advisories and other threat research to highlight the greatest areas of risk.

Please contact us to learn more, view a demo or to consider an evaluation of our unique approach to ICS cybersecurity at tripwire.com/contact.

COBIT 5 AN ISACA® FRAMEWORK

industrial internet CONSORTIUM

NIST

CIS Center for Internet Security®

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

American Water Works Association

ISO 27001

DISA

IEC 62443

HIPAA Health Insurance Portability & Accountability Act

NEI NUCLEAR ENERGY INSTITUTE

PCI Security Standards Council®

Tripwire paired with Tofino's Xenon malicious traffic detector provides deep visibility and configuration management insight not previously possible

- The only industrial security appliance that is 100% undiscoverable and undetectable
- Integration with Tripwire Log Center provides real-time visibilty to assets communicating through the Xenon and which packets are being blocked
- Complies with NERC CIP, ISA/IEC-62443, IEC 60870-5-104, ATEX, ISA-12.12.01 Class 1 Div.2, EN 50121-4, Germanischer Lloyd

Learn more at tripwire.com

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**

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