The Tripwire ICS Cyber Resiliency Suite

Tripwire is proud to offer the industry's most complete solution for reducing cyber risk in operational technology (OT) environments across industries such as energy, utilities, chemicals, transportation and manufacturing. Our ICS Cyber Resiliency suite is a holistic set of software applications that assess, harden and monitor plant environments to drive availability, safety, and resilience from cyber incidents.

Problems Solved

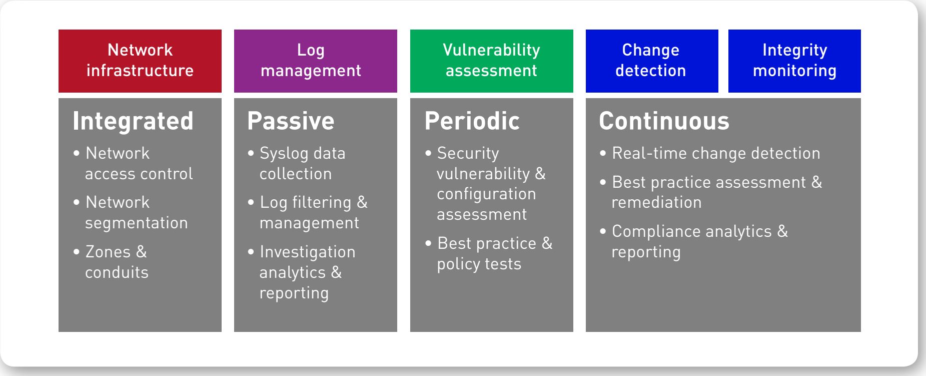
This software suite helps you address security in plants and industrial environments in ways that no one has done before. Just a few problems common to ICS and how we address them are provided in the following table.

Issue	Impact	Solution
No visibility into vulnerable hardware and software that could be exploited to damage or shut down plant operations	Cyberattacks typically exploit known vulnerabilities to inject malware that damages target systems	Continuous assessment of hardware and software vulnerabilities that need to be addressed
Intrusive security tools that could adversely impact plant performance	Standard security approaches that actively scan networks can take them down	Unique no-touch approach to identify and report on potential weaknesses
No monitoring of hardware and software changes that could adversely impact plant performance	Unauthorized configuration changes, whether accidental or intentional, can cripple plant operations systems	Change data collection via passive (device syslog) or active (real-time monitoring) approach to support incident investigation
Manual efforts to collect and summarize proof of compliance with regulatory requirements	Extra work required from plant operations and compliance teams reduces productivity	Automated data collection, and predefined alerts and reporting aligned to industry regulations or standards (e.g. NERC CIP, IEC 62443, NIST 800-53)

Table 1 Common ICS issues and how the Cyber Resiliency Suite addresses them

Security that Scales with Your Needs

When it comes to ICS security, we recommend that you "bake in" basic security as you build your plant network, using zones and conduits for network segmentation along with secure network components. From there, we support you in implementing security—based on your needs as they grow over time—from passive collection for analytics and incident investigation to advanced monitoring and reporting that addresses the most stringent security and compliance requirements.



Integrated
- Network access control
- Network segmentation
- Zones & conduits

Passive
- Syslog data collection
- Log filtering & management
- Investigation analytics & reporting

Periodic
- Security vulnerability & configuration assessment
- Best practice & policy tests

Continuous
- Real-time change detection
- Best practice assessment & remediation
- Compliance analytics & reporting

Fig. 1 A security continuum, from built-in to passive and advanced solutions

How the Suite Works

Our cyber resiliency suite integrates with the plant network equipment and factory automation systems you already own to help you find, fix and monitor security to prevent and detect cyber incidents.

Passive approach: Syslog data collected from in-scope devices and applications funnels to a centralized log management tool. Think of this as a security data historian.

Continuous approach: Windows-based data collectors provide ongoing visibility into vulnerabilities and configuration changes that could open the door to cyber incidents. Think of this as security SCADA.

These capabilities can be operated independently or in an integrated way to act as your HMI for security across your operations environment.

Next Steps

To learn more how Tripwire helps you address security issues that could adversely impact your ICS environment, please visit **www.tripwire.com/solutions/industrial-control-systems/**

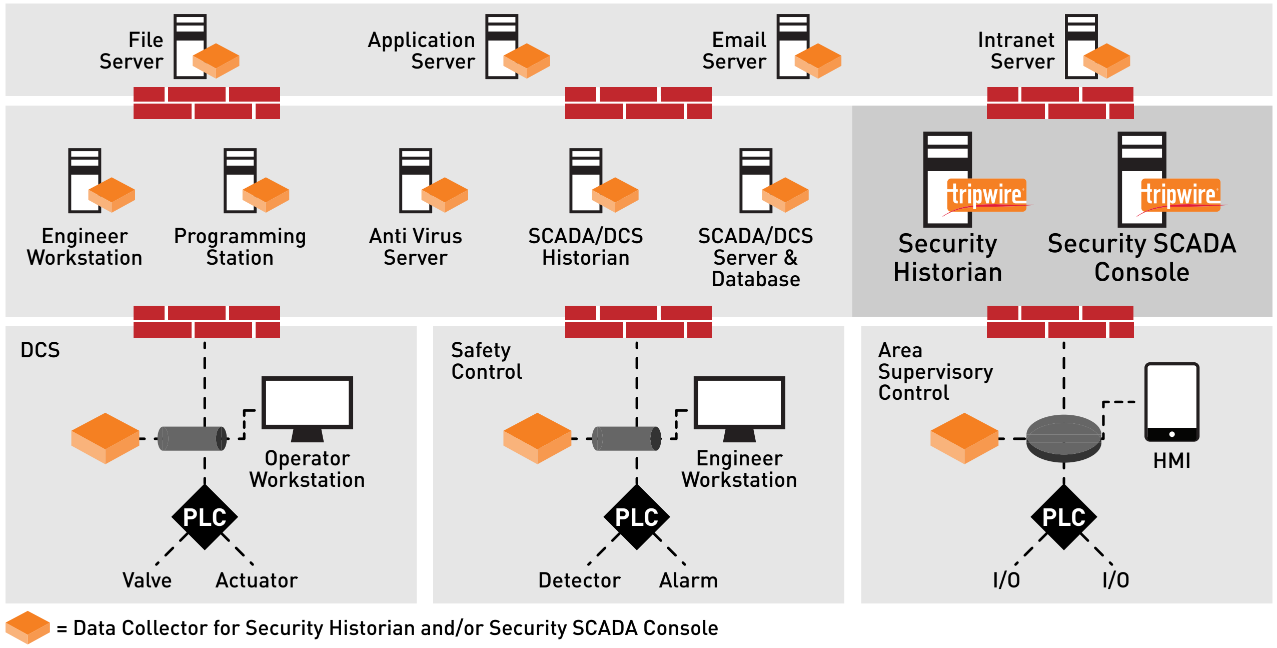


Fig. 2 Tripwire's flexible data collection works throughout your network to help ensure availability, security and resilience

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc