SOLUTION BRIEF

Maximize ICS Availability with Tripwire Industrial Visibility

Deepen Your Industrial Control Systems Security Assessments

Unplanned downtime costs between $30,000–$50,000 per hour in industrial environments. That means increasing your availability by even a single tenth of a percent can result in huge financial savings.

You're responsible for keeping an operational technology (OT) network running in the face of security challenges. The welfare of workers, the general public and the company depend upon you. Your network has to be resilient against cyber attacks. Your job is made harder still by the increasingly connected OT networks. To overcome these challenges, you need to gain deep visibility into your network to find signs of intrusion.

Tripwire Industrial Visibility is designed to tap into the native protocols on the OT network in such a way that it extracts data without affecting operations that may be sensitive to latency and bandwidth change. Our deep understanding of the myriad protocols used by OT systems makes this possible.

Industrial Control Systems Run Our World

Industrial control systems (ICS) are the workhorses of the critical infrastructures that keeps society running. Networks in critical infrastructure segments must be reinforced to establish cyber resilience:

- Energy
- Chemical
- Transportation
- Water & wastewater
- Dams
- Nuclear
- Defense
- Government
- Emergency services
- Financial services
- Food & agriculture
- Healthcare
- Smart cities
- Critical manufacturing
- Information technology

OT network challenges

OT environments present unique challenges:

» **Latency & bandwidth:** OT systems are sensitive to latency and bandwidth changes. Many of them were initially deployed on dedicated networks that performed well under known loading conditions. IT security system designers assume that network bandwidth is abundant and network speeds are high. When OT applications and hardware are placed under excessive load due to these emerging IT systems, they have the potential to starve critical applications of needed resources, causing them to crash.

» **Protocol proliferation:** ICS often have dozens of protocols in play. The variety and complexity of these protocols provides cover for a hacker's activities. To prevent malicious activity on the OT network that could impact availability, it is necessary to understand what an intruder is doing. Tripwire Industrial Visibility is able to passively collect and parse these protocols and isolate abnormal activity. Tripwire Industrial Visibility has no impact on either latency or bandwidth of the network.

OT network advantages

But it's not all doom and gloom. OT networks also have unique tools that can be used to secure ICS if operators know where to look:

» **Consistency:** OT systems strive for repeatability. This reduces the variability of activity on the network and makes it harder for an intruder to hide in the noise. By modeling "normal" behavior of each device on the network, you can recognize abnormal activity caused by intruders who are probing and experimenting.

» **Fewer applications:** There are also relatively few applications running on an OT network as compared to IT. This makes it easier to listen to the conversation and determine if a user is doing what they should be.

» **DPI:** Deep packet inspection (DPI) makes it possible to open communication packets and read their contents. This information can then be used to understand what is happening as it happens.

» **Protocols:** Protocols are both a hindrance and a helper in ICS. The protocols used to communicate between ICS devices can be used to directly monitor actions occurring on the system. Understanding a large number of vendor protocols improves overall network visibility.

Why Is Cyber Resilience So Important?

You can think of your cyber resilience strategy as a shock absorber for your ICS network. It's unrealistic to assume that you won't be breached. The more practical approach is to have every possible mechanism in place to make sure a breach doesn't cause downtime. Don't let a breach bring your business to a standstill.

According to MITRE, "The challenge for companies is to maintain critical functions in the face of these inevitable breaches. Although traditional defenses remain essential, organizations need additional technology so they can complete their missions *despite* successful attacks."

How Tripwire Industrial Visibility Works

Optimized specifically for ICS, Tripwire Industrial Visibility can understand more than 40 of the most important ICS protocols. This can be compared with baseline behavior to identify intruders. Let's take a deeper dive into the ways you can use Tripwire Industrial Visibility to get the most safety, quality, and uptime possible from your OT environment.

Complete network visibility

By reading the network traffic, Tripwire Industrial Visibility can isolate all assets on your OT network to understand the

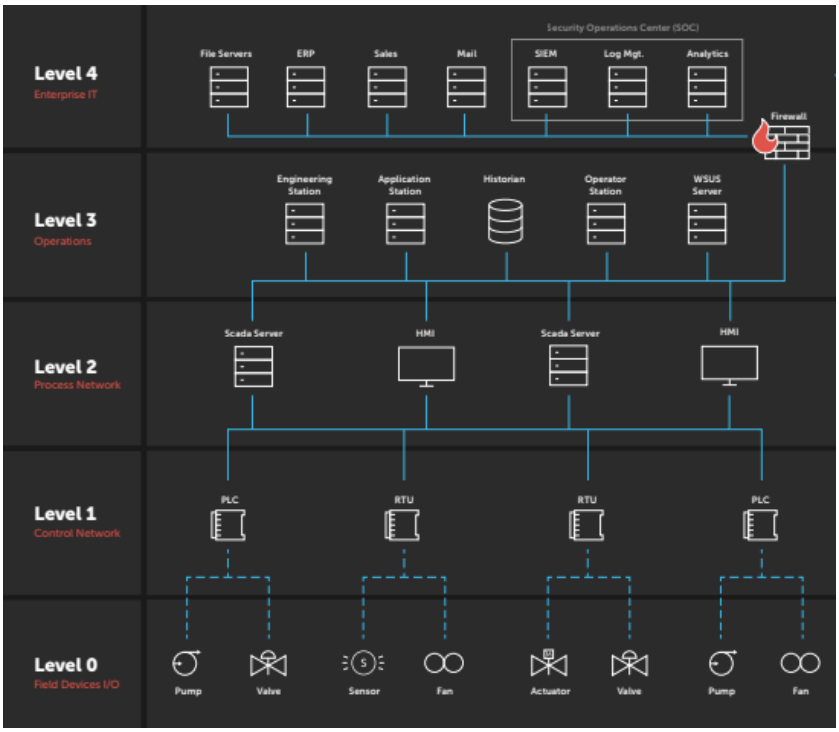

Fig. 1 Network assets are grouped for quick interpretation: Level 0 (Field Devices), Level 1 (Control Networks), Level 2 (Process Network) and Level 3 (Operations) comprise the OT network. A firewall separates the OT network from insecure Level 4 (Enterprise IT) devices.

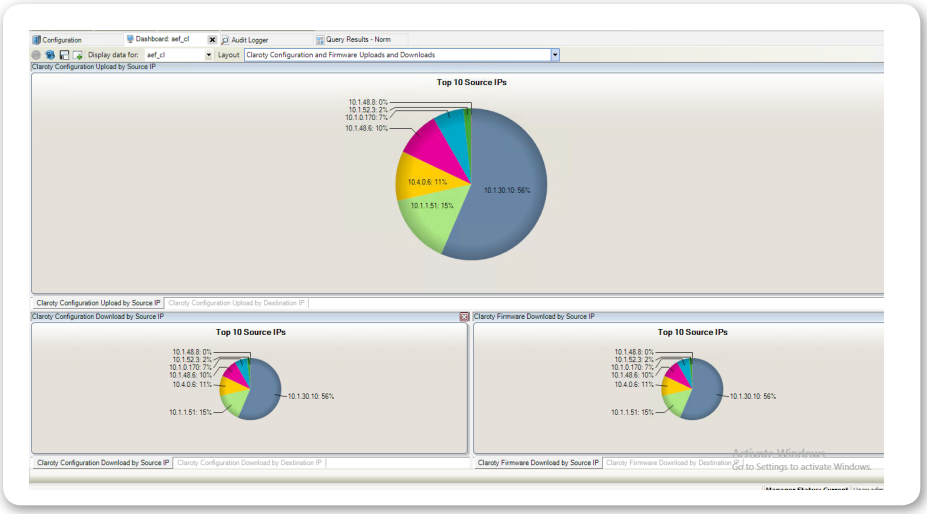

Fig. 2 Top destination and source IPs.

flow of traffic between them. This data is then used to create graphical network maps that make it easier for operators to visualize activity and to notice anomalies. It taps into OT network communication by listing through the SPAN port of routers and switches connected to the network segment, and uses deep packet inspection to open data packets and interpret protocols.

Downtime prevention

One of the primary benefits of Tripwire Industrial Visibility is its ability to stop bad actors in their tracks. Attackers intending to infiltrate your network to cause damage are recognized quickly, enabling their rapid removal. You'll also have quicker recognition of system penetration, as hackers can be detected before attempting to upgrade access permissions, modify system configurations, or change files.

Machine learning

Tripwire Industrial Visibility employs machine learning in a number of ways. It creates a baseline of expected behavior from good actors. When a bad actor deviates from a baseline, it flags them to operators. Even bad actors using legitimate credentials can be easily detected. Unlike IT networks, OT networks have far more consistency in the behavior of users. Machine learning is applied to understand what is normal and then alert when unexpected behavior occurs.

In addition to user behavior, network activity can also be monitored for "normal" behavior. The traffic from a correctly-behaving network is fed into a machine learning system, and the system learns to recognize normal activity. Whenever something unusual occurs, an alert is generated. This saves you time and prevents you from being responsible for evaluating each and every data point.

Attack simulation

Tripwire Industrial Visibility uses vulnerability data to hypothesize a series of attacks that could be executed against your OT network. This information helps executives fully understand security holes and to scale the impact of a potential breach. Users can highlight a sensitive asset and the system will posit attack vectors that could be executed against it.

Event logging

Tripwire Industrial Visibility includes Tripwire Log Center®, which provides secure and reliable log collection from multiple sources to help you investigate outages and correlate events of interest. Its automated normalization engine parses log data to help you quickly identify what data is most relevant and build actionable correlation rules. An intuitive visual interface lets you customize log data rules around your specific use cases. This function also allows you to pre-filter information before it reaches your SIEM.

Passive scanning

Tripwire Industrial Visibility works smoothly with legacy ICS technology, using passive scanning to maximize uptime. This is due to the fact that a strategic combination of agentless and agent-based passive scanning keeps legacy systems up and running during scans. Unlike traditional vulnerability management and security configuration management (SCM) products, it employs no-touch sensing that can be used when legacy systems would otherwise crash when polled.

Summary

Tripwire Industrial Visibility provides deep, ongoing network assessment for OT operators in industrial control systems. Because Tripwire understands the complex challenges posed by increasingly-connected legacy technology, we've developed a way for you to see exactly what's going on in your OT environments at all times using native industrial protocol communications.

Ready for a Demo?

Let us take you through a demo of Tripwire Industrial Visibility and answer any questions you have. Understand how Tripwire's suite of security and vulnerability management products and services can be customized to your specific OT security and compliance needs. Visit **tripwire.com/contact/request-demo/**

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

SBTIV1a 1808