Tripwire Industrial Sentinel

Continuous Operational Cyber Risk Assessment for Maximum Network Resilience

Tripwire® Industrial Sentinel 4.2 is a non-intrusive network monitoring and situational awareness platform that provides in-depth visibility and cyber resilience for industrial control systems (ICS) and SCADA networks, providing visibility to and protection from events that threaten safety, productivity, and quality.

Highlights

- Discover and inventory every asset within your industrial control network
- Baseline normal network commutation between devices and alert upon deviation, enabling real-time operation and cyber risk management
- Find indicators of compromise in network traffic and protocol messages through a comprehensive industrial threat library
- Assess and report on industrial device vulnerabilities, exposure to cyber threats and existing networking and operational problems
- Analyze network traffic through deep packet inspection for all common industrial protocols and vendors
- Transform raw data into actionable information helping to facilitate root cause analysis to minimize mean time to repair metrics.

Tripwire Industrial Sentinel combines patented anomaly detection and deep packet inspection (DPI) with a library of over 2,400+ ICS-specific threat indicators and a continuously growing library of 3,500+ indicators of compromise (IoCs) to protect asset owners from advanced cyberattacks, network misconfigurations, and operational errors. It natively interfaces with enterprise systems such as SIEM, firewalls, IT asset management, malware analysis, authentication servers and third-party platforms.

Asset Inventory and Network Map

- Automatic asset, communication and vulnerability inventory with full device fingerprinting and deep packet inspection (DPI) of industrial protocols
- Customizable Purdue-level or network-based visualization network maps and communication patterns
- Interactive visualizations of threats and risks
- Optional active query component driven by the passive system to collect information such as open ports, PLC information, services, applications and patches
- Device properties, activity and configuration change log
- Impact-based security and operational risk scoring framework

Threat Hunting Framework

- Comprehensive search for indicators of incidents in network traffic and protocol messages
- Automatic threat intelligence ingestion and back-in-time threat detection
- 2,400+ threat indicators like protocol compliance checks, CVEs, and proprietary behavioral checks for cyberattacks, network issues, and operational errors
- Flexible framework for definition and identification of recurring suspicious behavior

Network and Process Monitoring

- Patented DPI for IT & OT protocols, monitoring protocol correctness and process values
- Self-configuring network and process whitelists
- Software Development Kit (SDK) for advanced customizations
- Easy development of complex network- and process-specific checks
- Quick support for new protocols and custom integrations

Investigation & Forensics

» Records and provides a packet capture of raw traffic associated with each alert, to enable forensic analysis

» Analyzes files transferred over the network against known signatures (YARA rules) or hashes where malicious files, up to a certain size, can be included in the alerts for download and further analysis

Dashboards and Reporting

» Dashboards and widgets for easy collaboration among users on asset and threat visibility, including alert trends, asset charts etc.

» Rich alert details to enable root cause analysis and incident response

» Automated generation of editable graphical reports

New Command Center GUI

The Command Center features a new graphical user interface that covers the most important capabilities for asset inventory and alert analysis, and is designed to make user workflows smoother and analysis faster and more effective.

» Several usability improvements have been applied to the map, including increasing the number of visible assets and the visualization of groups and clusters

» Language and locale can now be customized to each user's preference—users can choose among the available languages or load additional language packs

Advanced Alert Aggregation

Advanced Alert Aggregation helps you better understand your risk posture and operating status for faster and more cost-effective response to cyberthreats. It offers the ability to aggregate and create multidimensional alert groups to better uncover trends in the network. Functioning like a pivot table, alerts are aggregated by multiple dimensions according to source IP, type of vulnerability, sensor, etc. This feature reduces noise and helps analysts focus on the highest priority alerts.

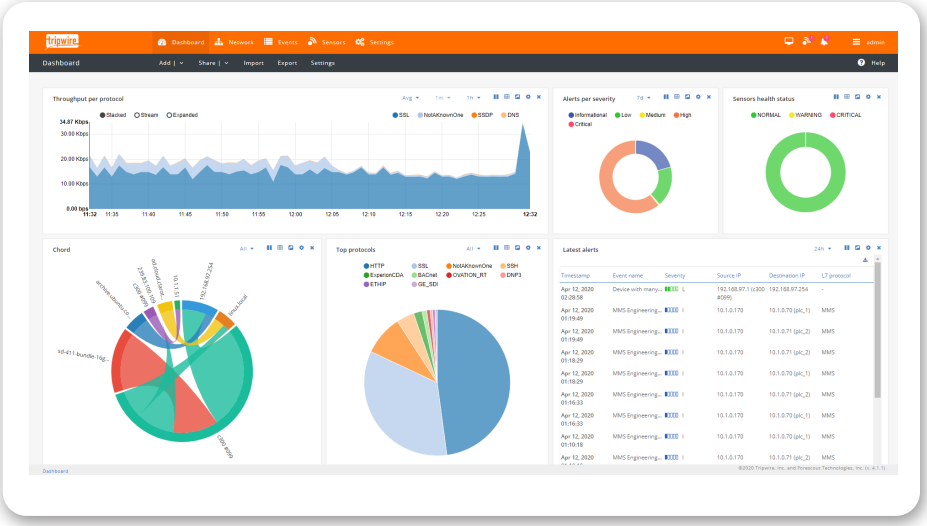


Fig. 1 Interactive Tripwire Industrial Sentinel dashboards display customizable widgets that provide visualization of alerts, throughput per protocols, and sensor status.

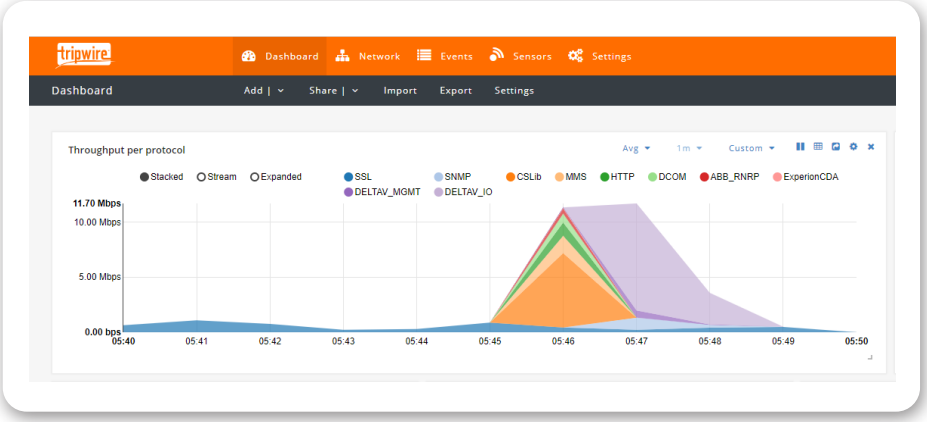


Fig. 2 Tripwire Industrial Sentinel dashboard display displaying throughput per protocol.

New Vulnerabilities Table

The Tripwire Industrial Sentinel Command Center (CC) and Enterprise Command Center (ECC) offer a dedicated table and chart to enable effective vulnerability management and analysis. These enable assets to be filtered based on vulnerability severity and vulnerabilities to be sorted by CVSS score, and determine how many and which assets are affected by which vulnerability. The table also describes how each vulnerability can be exploited by an adversary, possible consequences of the exploit, and whether a fix is available from the asset vendor. This information allows analysts to quickly define and prioritize response and mitigation.

Asset Baselining & Reporting

The Asset Baseline allows users to define granular compliance policies for assets, and to identify and analyze compliance deviations. For example, it allows users to define which OS, firmware version, or open ports are allowed for assets from a specific vendor or of a specific type (e.g. PLCs, HMIs, etc.), and report non-compliant assets through dedicated views. It also enables automation of compliance verification and reporting tasks for both internal and external audits.

Active Sensor Improvements

The following improvements and new capabilities are now available for Active Sensors:

- **SEL devices (IP-enabled and serial):** Two new types of Active Sensor queries are now available, enabling users to quickly retrieve details of SEL IEDs or RTAC devices and connected IEDs (including serial).
- **Improvements in Windows active query:** the active Windows query now exploits WinRM in combination with the original WMI query to retrieve more accurate Windows software and patches.

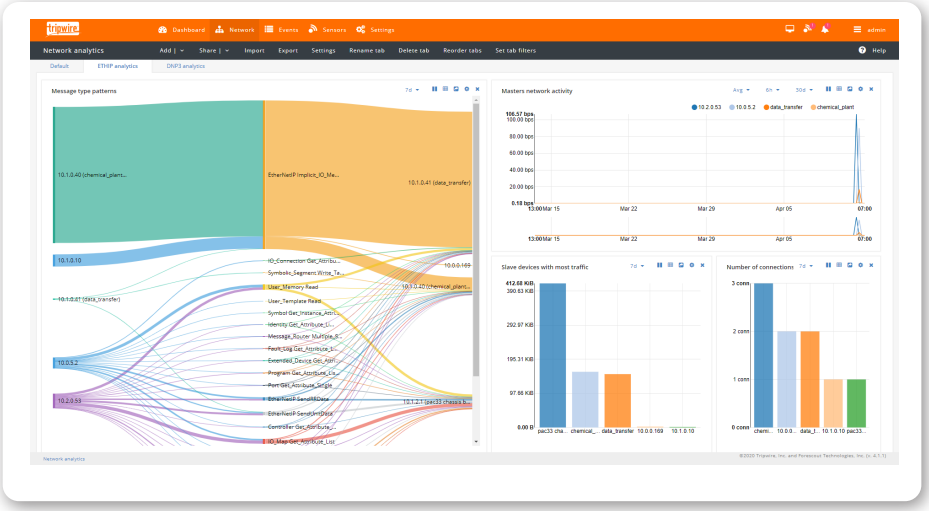


Fig. 3 Tripwire Industrial Sentinel industrial protocol analytics provide visibility into protocol message types and connection summaries for Ethernet/IP CIP. Addtional template-based and customizable OT protocol analytics dashboards are also available.

Federal Information Processing Standards Compliance

All tools and functions of Tripwire Industrial Sentinel adhere to the security requirements of FIPS 140-2 Level 1 for securely implementing cryptographic algorithms, encryption schemes, handling critical data, and working with various operating systems.

Data Encryption at Rest

Tripwire Industrial Sentinel encrypts sensitive information stored on Tripwire Industrial Sentinel sensors. This enhanced level of security protects asset data from cyberattacks—of critical importance for sensors deployed in unmanned and/or remote locations.

Coverage Expansion

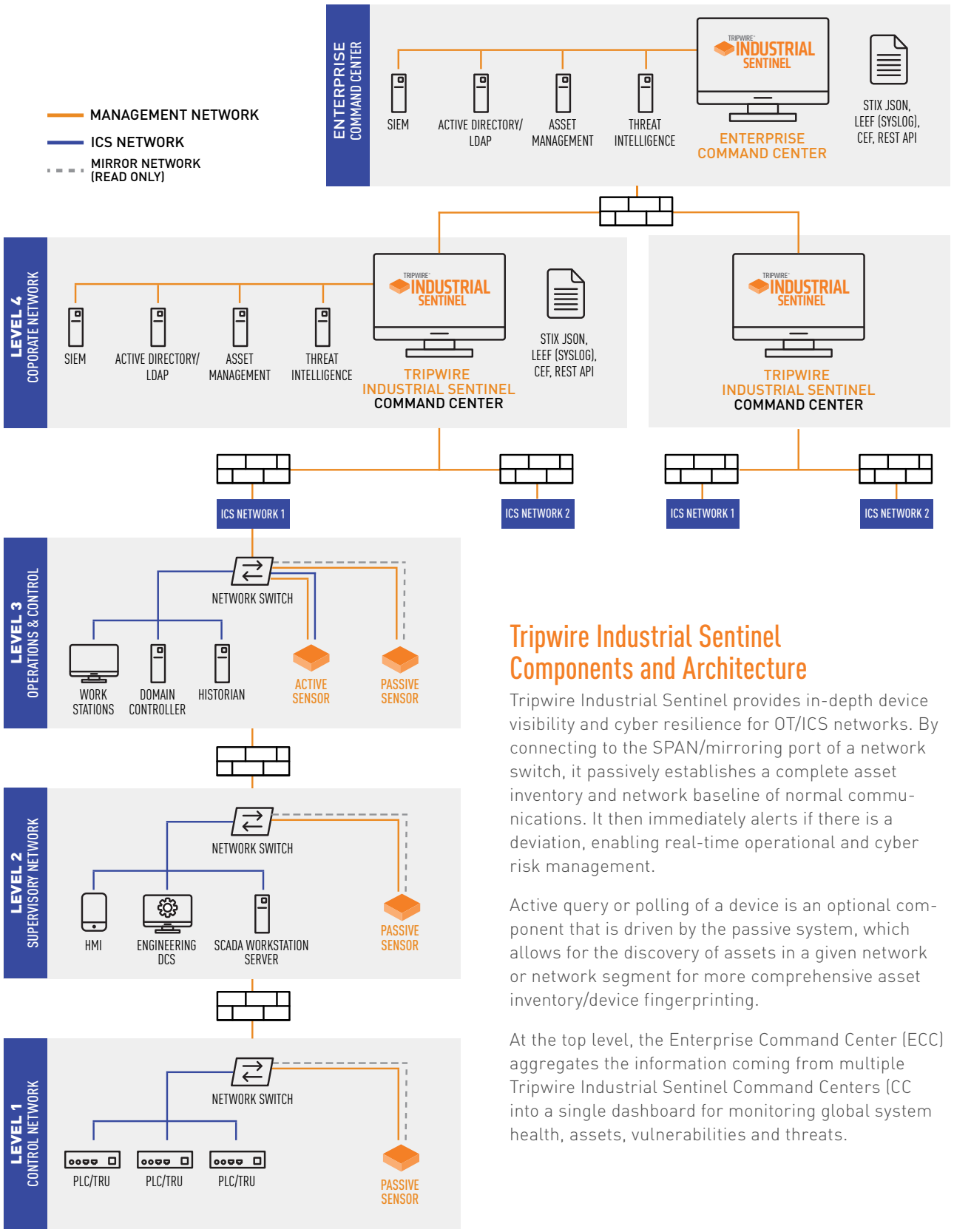
Tripwire Industrial Sentinel also increases its device visibility and threat detection reach with the additional support of 30+ new industrial protocols, improved auto-classification, and 140+ additional behavioral checks. Please refer to the Tripwire Industrial Sentinel Protocol Support datasheet for more information.

Backwards Compatibility

Tripwire Industrial Sentinel 4.2 Command Centers are compatible with 4.1.x sensors, making it easier to plan incremental updates of large systems while maintaining active protection.

Ready for a Demo?

Let us take you through a demo of Tripwire Industrial Sentinel and answer any of your questions.
Visit **tripwire.com/contact/request-demo**.



Tripwire Industrial Sentinel Components and Architecture

Tripwire Industrial Sentinel provides in-depth device visibility and cyber resilience for OT/ICS networks. By connecting to the SPAN/mirroring port of a network switch, it passively establishes a complete asset inventory and network baseline of normal communications. It then immediately alerts if there is a deviation, enabling real-time operational and cyber risk management.

Active query or polling of a device is an optional component that is driven by the passive system, which allows for the discovery of assets in a given network or network segment for more comprehensive asset inventory/device fingerprinting.

At the top level, the Enterprise Command Center (ECC) aggregates the information coming from multiple Tripwire Industrial Sentinel Command Centers (CC into a single dashboard for monitoring global system health, assets, vulnerabilities and threats.

Fig. 3 Tripwire Industrial Sentinel deployment architecture for multiple sites provides holistic coverage across your industrial landscape.

TRIPWIRE CUSTOMER TESTIMONIAL

> “The Tripwire name is trusted in the industry and has never gave reason to doubt it. [The] continued development and listening to customers only strengthens this fact.
>
> — IT Systems Analyst, Fortune 500 Energy & Utilities Company

Source: IT Systems Analyst, Fortune 500 Energy & Utilities Company

Validated Published: Jul. 24, 2020 TVID: 613-7B8-00A

tripwire | TechValidate by SurveyMonkey

tripwire

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at** tripwire.com

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