



SCADAfence

PROFITAP

Solution Brief

INDUSTRIAL NETWORK VISIBILITY & SECURITY WITH PROFITAP AND SCADAFENCE



VISIT WWW.PROFITAP.COM

The Challenge

The integration of advanced Operational Technology (OT) and Information Technology (IT) networks, high tech automation, supervisory control and data acquisition systems (SCADA), and physical processes, are some of the main elements characterizing the 4th industrial revolution, better known as the Industry 4.0 or the Industrial Internet of Things (IIoT). IIoT connects the physical machines and equipment in a factory, smart products, and the whole supply chain to the digital world of cloud, IoT devices, data analytics, and artificial intelligence. Connectivity however opens to vulnerability issues like cyber-threats and operational incidents. The use of Internet Protocols networking in OT systems can open any industrial environment to network attacks, and can create backdoors into organizations' enterprise IT networks, putting both electronic infrastructures and the information they contain at high risk. Managing these risks is complicated by the differing missions of the two systems, and the fact that most OT network environments and devices are not monitored directly by security personnel. Consequently, the Industrial Control System (ICS) networks are harder to monitor and secure as they're very diverse, and most of the time, they operate with an increased risk of industrial-specific vulnerabilities.

Common challenges in monitoring and securing OT and IT environments include:

- ▶ Achieving real-time network monitoring
- ▶ Managing cyber threats effectively
- ▶ OT and IoT security in one place
- ▶ Detecting networking and operational issues before they cause downtime
- ▶ Preventing unplanned downtime due to equipment failure
- ▶ Remote access control
- ▶ Remote troubleshooting (intermittent) issues on hard to reach locations
- ▶ Centralized automated governance of industry regulations for OT & IoT

The Solution

SCADAfence's non-intrusive platform for deep packet inspection (DPI) together with Profitap's network test access points (TAPs) and Network Packet Brokers (NPB) solutions, work together to bring unprecedented network traffic visibility, security, asset inventory management in real-time and compliance to all OT & IoT industry regulations.

By amplifying visibility into OT and IT networks, and through continuous monitoring organizations gain:

- ▶ Full control over their industrial environments
- ▶ Excellence in network monitoring infrastructures
- ▶ Real-time detection of malicious activities
- ▶ Significant reduction of cyber risks
- ▶ Proactive mitigation

How It Works

Accessing the Network Traffic

Deploying network traffic access points (TAPs) throughout the Industrial Ethernet framework ensures safety, uptime, and improved efficiency. Installing TAPs for all monitoring feeds guarantees 100% of the network traffic is copied and transmitted to monitoring tools, achieving real-time network monitoring, and detecting operational issues before they cause downtime.

Profitap TAPs in industrial environments provide:

- TSN support, low jitter
- Low failover time
- High resolution timestamping
- Accurate packet capture
- High fidelity traces
- 24V models available
- Once TAPs are in place in the network, the monitor ports can be connected and disconnected at will without disrupting the network link

Managing & Optimizing Data Flow

Network Packet Brokers are placed between the monitoring and security tools and network TAPs or other sources. They orchestrate the traffic coming from multiple network links and can perform advanced, intelligent traffic management, such as slicing, timestamping, deduplication, decryption, and more to ensure that monitoring tools receive the appropriate packet data. Deploying a Network Packet Broker adds a layer of intelligence to optimize the monitoring architecture and decreases load on monitoring and security tools so they can focus their processing power on their primary functions.

Data Capture and Analyzing OT Traffic

With the traffic access and data flow in order, SCADAfence starts to monitor the OT network activities. With passive DPI analysis and optional active polling, SCADAfence discovers all the assets in the network and their relevant industrial characteristics. The platform completely digitalizes the asset inventory and network communications mapping. In addition, an adaptive baseline is created to capture the current operational behavior of the environment.

SCADAfence algorithms offer real-time detection of malicious activities and anomalous behavior. This is based on deviations from normal behavioral profiles, rule-based capabilities, signature-based alerts and proprietary threat intelligence, the platform detects abnormal activities that threaten the network. This includes cyber-attacks and non-malicious threats.

Asset Management

Generate a complete asset inventory and advanced network map that visualizes traffic patterns with The SCADAfence Platform. By digitalizing your asset inventory with automatic asset discovery and network mapping, users can replace outdated and manually obtained spreadsheets with updated real-time information about their environment.

Continuous Monitoring

The SCADAfence Platform continuously monitors the network architecture for an accurate view of your security posture and insight into real-time events. This enables complete and continuous control over your most critical business assets.

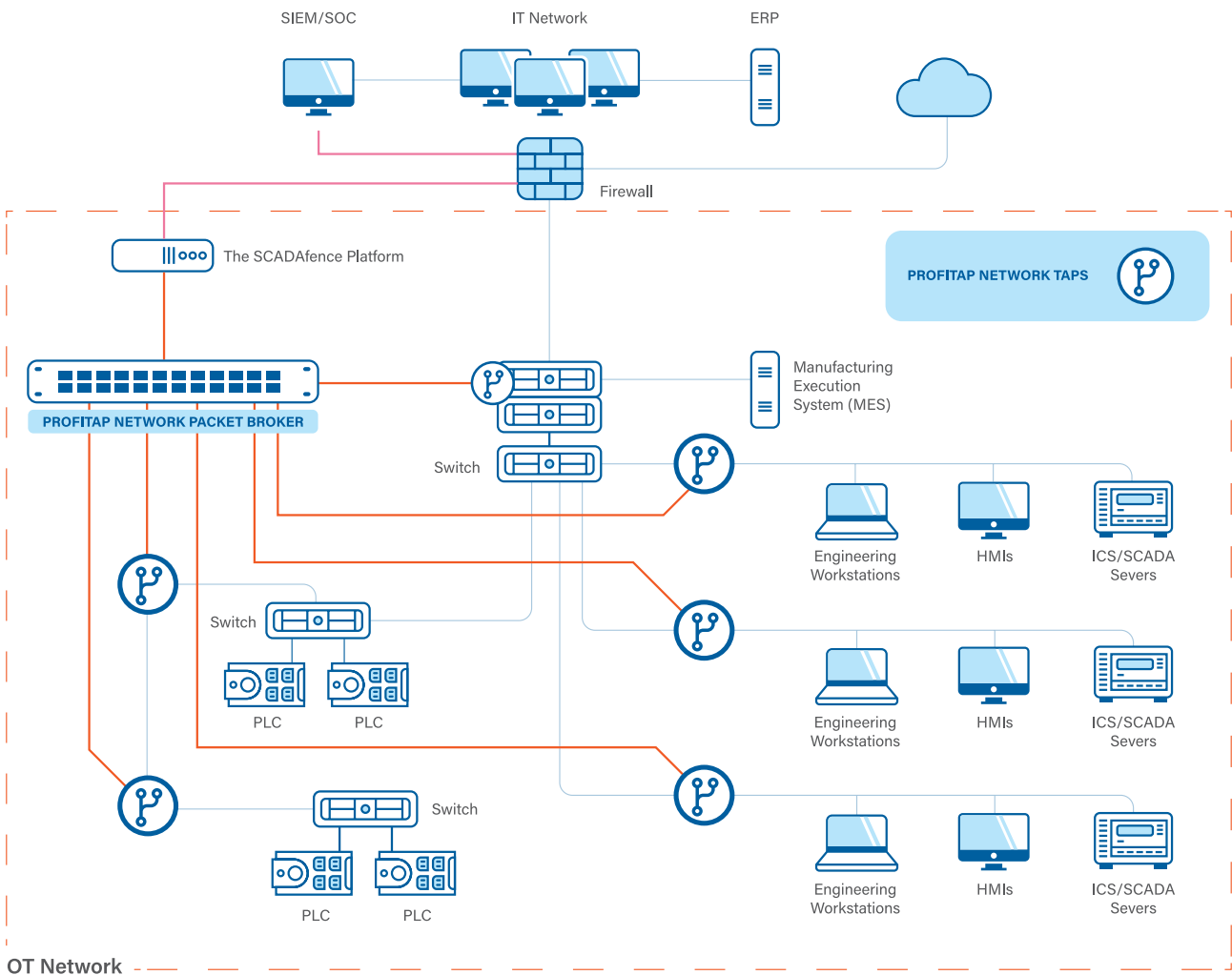


Detection of Malicious Threats

Uncover malware and ransomware that threaten operational continuity. Early detection of threats enables effective response before damage occurs, preventing unplanned operational downtime.

Centrally Manage Compliance to Regulations

The [SCADAfence Governance Portal](#) provides a governance solution portal that enables IT and OT departments to centrally define and monitor their organization's adherence to OT-related regulations and security policies.



About SCADAfence

SCADAfence is the global technology leader in OT & IoT cyber security. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access and IoT device security. A Gartner "Cool Vendor" in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing and building management industries to operate securely, reliably and efficiently. To learn more, visit our [website](#), check out our [blog](#), or follow us on [LinkedIn](#).




Profitap develops and manufactures Copper and Fiber Network TAPs, Network Packet Brokers and Portable Field Service Troubleshooters. These solutions are designed with the security, forensics, deep packet capture and network performance monitoring sectors in mind. Profitap network solutions help eliminate network downtime and add security to existing and new networks all over the world, assist in lawful interception applications and reduce network complexity. All of Profitap's network monitoring tools are highly performant, secure and user-friendly, and provide complete visibility and access to your network, 24/7. Learn more at profitap.com

PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS

sales@Profitap.com
www.Profitap.com

 Profitap

 @Profitap

 Profitap-international