INTEGRATION BRIEF

PROTECT CRITICAL ASSETS AND OT NETWORKS WITH CLAROTY AND FEND

The Industrial Cybersecurity Challenge

The past decade has seen exponential growth of newly connected Operational Technology (OT) and other Extended Internet of Things (XIoT) network components, the benefit of which has been felt across all industries and geographies. The problem with this innovation in hardware design is that it has outpaced manufacturers' ability to provide adequate security for the devices they produce.

With each additional unmanaged device, organizations expand their vulnerability to external threats. It can be easy to fall into the trap of chasing greater efficiencies and control over processes without pausing to consider the impact these devices may have on the overall security posture of the enterprise. Legacy systems, unpatched vulnerabilities, and lack of network controls are common–creating opportunities for cybercriminal and malicious attacks to occur. Claroty and Fend are partnering to help ensure cyber and operational resilience in industrial environments.

Claroty and Fend Joint Solution

Claroty's integrated OT cybersecurity suite and Fend data diodes address inherent shortcomings in legacy OT networks to protect the safety of people, industrial assets, and critical processes from cybercrime and malicious attacks.

Claroty Continuous Threat Detection (CTD)

CTD was created to help both IT and OT teams overcome challenges associated with digital transformation and a converged IT/OT network environment. As the foundation of The Claroty Platform's comprehensive industrial cybersecurity capabilities, CTD is backed by an unmatched library of industrial protocols, three unique asset discovery methods, proprietary DPI and virtual segmentation technology, and the renowned Claroty research

Joint Solution Benefits

- **Centralized OT Asset Visibility:** Unified view of assets, activities, alerts, and access control
- **Continuous Threat Detection:** Continuous threat and vulnerability visibility with deep insight into OT networks
- **Secure Data Transfer:** Deterministic, one-way transfer of Claroty CTD instances to Claroty EMC using Fend's OT data diodes
- **Remote Monitoring:** Monitor CTD instances across multiple sites at a central location
- **Air Gap:** Physically prevent threats from entering the OT network through a data transfer

group, Team82. This solution empowers customers to reveal and protect their XIoT assets, detect and respond to the earliest indicators of threats, and seamlessly extend their existing enterprise security and risk infrastructure and programs to harden their industrial networks. CTD extends the same controls IT security teams use to minimize risk in IT environments to OT environments.

Fend Data Diodes

Data diodes from Fend provide a secure, physically-enforced one-way path from Claroty CTD instances to the Claroty Enterprise Management Console (EMC) - the centralized dashboard of a multi-site CTD deployment. This one-way communication approach architecture allows monitoring of CTD instances across multiple sites at a central location while preventing any possibility of malware or other threats from entering OT networks. Fend data diodes enable safe, one-way communication of log files or raw network traffic to Claroty CTD, while maintaining isolation of an OT network segment, in architectures where the CTD components will reside outside of a data diode-protected OT network segment. Fend's rugged, compact devices can be placed in equipment cabinets or remote locations and perform across a wide variety of environmental conditions.

Site Protected by Fend Data Diode

Single Site Data Diode Scenario

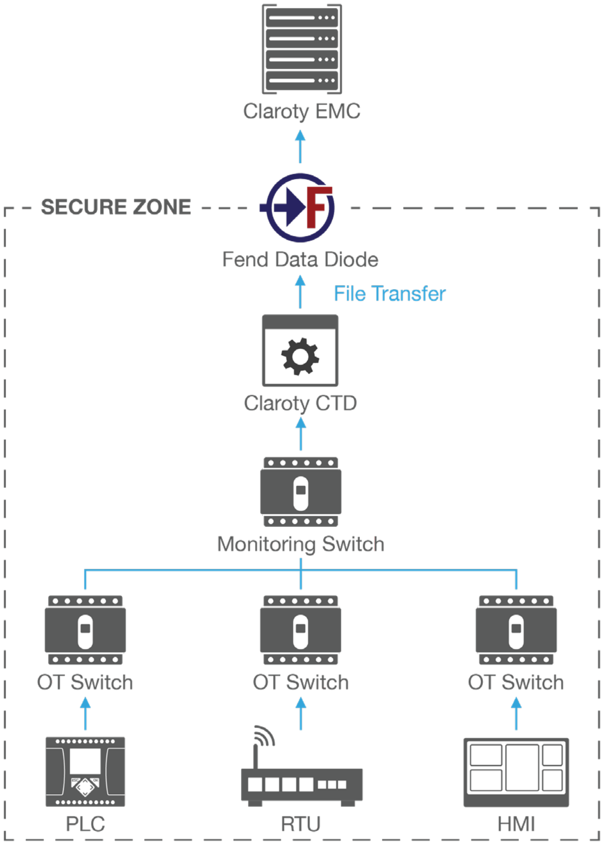

Figure 1: Combining Claroty CTD with Fend data diodes enables continuous monitoring of networks while maintaining the security of an air gap.

Multiple Sites Protected by Fend Data Diodes

Multi-Site, Multi-Data Diode Scenario

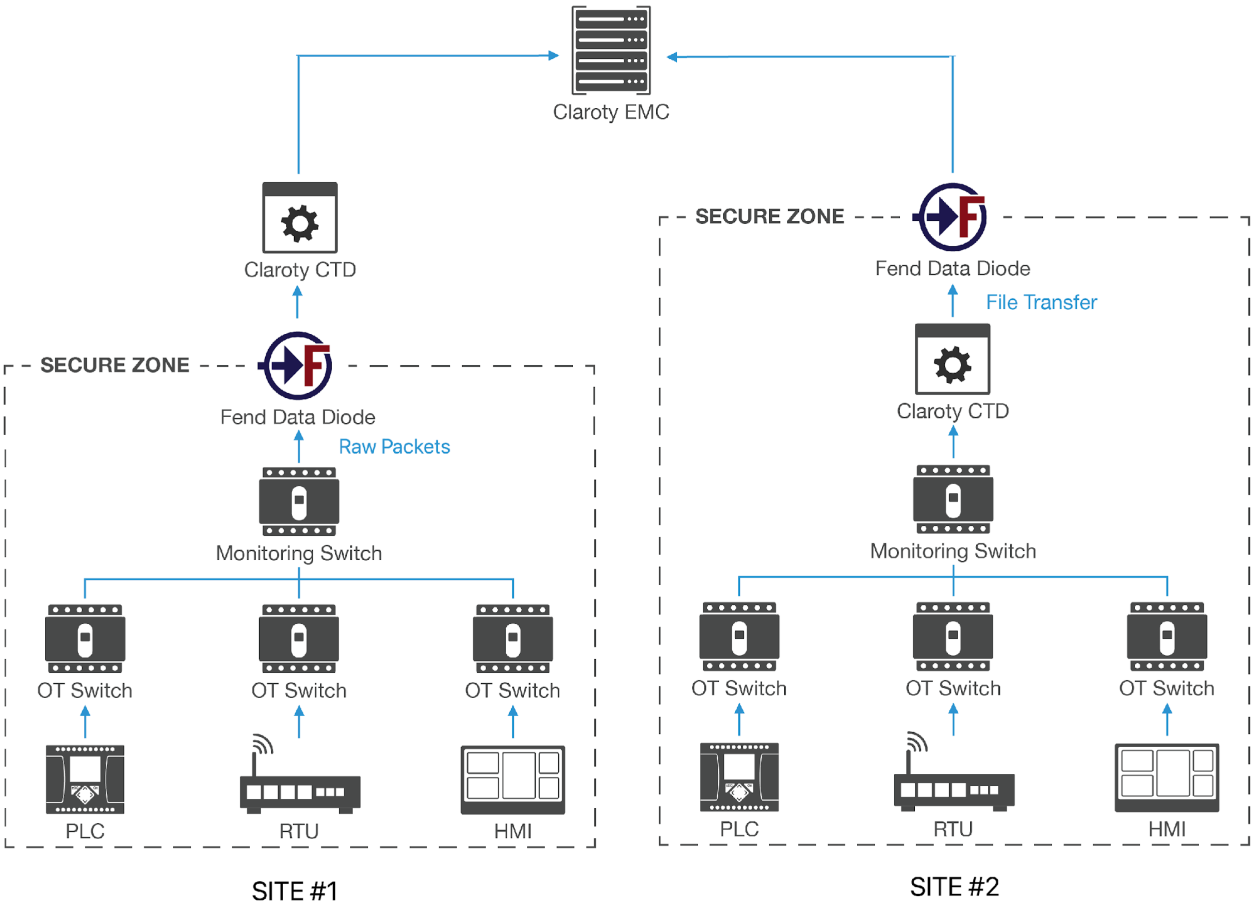

Figure 2: The Claroty + Fend solution scales rapidly across large deployments, delivering enterprise-scale visibility.

About Fend

Fend's data diodes (also known as unidirectional gateways or one-way communication diodes) are cybersecurity hardware devices that facilitate one-way communication of data. Fend products are built from the ground up for the protection of industrial control systems and OT networks. The company is headquartered in Arlington, Virginia. Fend's products have been tested by the US Army, Navy, Air Force, and General Services Administration and are designed and built in the USA. Segment and defend your networks effortlessly to protect even the most sensitive data and assets with Fend.

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, network protection, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.

CLAROTY | FEND