SOLUTION BRIEF

Fortinet and Claroty Comprehensive ICS & SCADA Cybersecurity Solution

Higher Visibility and Faster Time to Value for Automated, Integrated Security Monitoring and Access Control

Digital Transformation and Increasing Cyber Risks

Industrial organizations are embracing digital transformation (DX) to move faster for increased production and reduction in costs. The transition includes adopting internet- connected networks, industrial control systems, and Internet-of-Things (IoT) devices that can often increase cyber risks in operational technology (OT) environments. Cyber criminals leverage industrial DX and IoT cyber risks to aggressively target OT networks and assets.

Traditional IT solutions are unable to address risks met by industrial control networks, processes, and assets in production environments. And, many industrial companies discovered that even with the OT networks not directly targeted, organizations can experience millions in losses through disrupted productivity in plants and factories.

Fortinet and Claroty have partnered to assist industrial organizations with adapting their OT networks to the evolving cyber risks to ensure safety, reliability, and production.

The Claroty and Fortinet Joint Solution

The partnership between Claroty and Fortinet leverages the Fortinet Security Fabric to extend broad OT visibility and IoT coverage deep into the lowest levels of industrial

Networks, resulting in more coverage, faster deployment, and less noise. The comprehensive solution combines Claroty Continuous Threat Detection (CTD) with Fortinet's Security Fabric, including FortiGate and FortiSIEM.

Integration with Fortigate

The integration of Claroty Continuous Threat Detection (CTD) with FortiGate, Fortinet's next-generation firewall (NGFW), enables a seamless transformation of CTD's OT asset inventory with detailed attributes, virtual zones, and reduced alerts into enforceable firewall policies.

- CTD's Virtual Zones are sent to FortiGate and automatically create Address Groups. These Address Groups can then be used by FortiGate users to create firewall policies, which are no longer based on minimal information such as an asset's IP or MAC address, but can now be managed within a rich OT context as an asset type (PLC, HMI, RTU, etc.), vendor and model, firmware version, OS, applicable CVEs, zone, criticality, and much more.
- CTD's alerting policies automatically create firewall rules in FortiGate and provide the needed enforcement of policies to block unwanted or malicious communications, and to serve as a complete segmentation tool.

Joint Solution Components

- Fortinet Security Fabric, FortiGate, FortiSIEM
- Claroty Continuous Threat Detection (CTD), Enterprise Management Console, CTD Sensors

Joint Solution Benefits

- Real-time and unified, full-spectrum visibility and protection across IT, OT, and IoT networks
- Faster detection, response, and resolution across a broader array of OT and IoT assets, and protocols and communications in SCADA
- Agentless discovery of OT and IoT assets and vulnerabilities
- Enhanced OT network and asset threat contextual information to FortiGate for controlling and enforcing policy and protection across precise points in OT networks
- Asset inventory and alert context from CTD to FortiSIEM for centralized visibility, correlation, and automated response and remediation
- Safe, secure, and reliable operations in large, complex industrial networks with strengthened IT, OT, and IoT security

FABRIC-READY

Integration with FortiSIEM

Fortinet's security information and event management (SIEM) tool, FortiSIEM, is fully compatible with CTD's asset inventory and alerts that are shared via syslog. With this integrated and automated capability, customers can leverage their existing SIEM-based workflows and monitoring processes to perform efficient security operations activities for their OT networks, in the same fashion as they do for their IT networks. Syslog messages that require configuration can automatically be sent by the system for:

- Alerts and alert resolutions
- Events (related to the alerts)
- Baselines and deviations
- System status checks
- System health monitoring information

The joint solution with FortiGate secures the gateway between IT and OT networks, and through its integration with FortiSIEM, enables rapid, informed response with OT asset details and threat context.

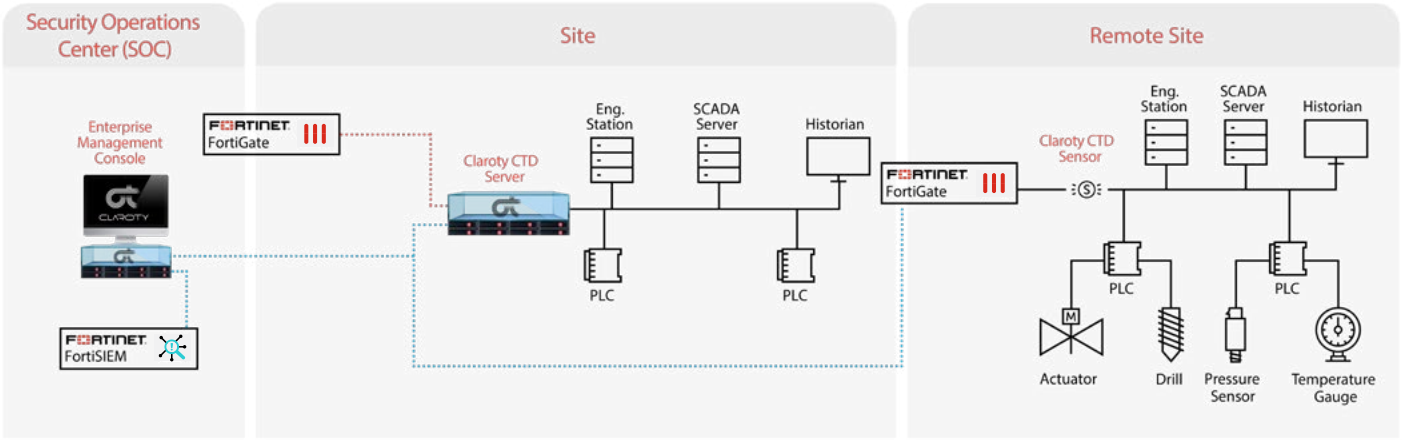

Figure 1: The figure above illustrates an example deployment showing CTD components in a widely distributed environment with local monitoring and remote sites communicating with Claroty's Enterprise Management Console (EMC), commonly found in an IT-OT SOC.

Claroty Platform

The Claroty Platform consists of multiple integrated software applications that work in concert for the best visibility and OT security available. Those most directly involved in the integration with the Fortinet Security Fabric are:

- Continuous Threat Detection (CTD)—This server software can be run as a virtual machine, a physical appliance within the network (such as a 1RU rack mounted or din-rail device), or configured to run on a ruggedized PC-type of platform that meets Claroty-published server requirements. CTD deeply inspects all OT network traffic without agents or impact to operations.
- CTD Sensors—These sensors provide a secure and easy deployment, as well as powerful services for rapid, reliable, and bandwidth-optimized communication. Lightweight sensors provide full visibility into remote/segregated network segments by capturing, analyzing, and forwarding traffic back to the CTD server.
- Enterprise Management Console—The Enterprise Management Console (EMC) is usually located at the security operations center (SOC) or in the corporate site. It displays information aggregated from all sites on its web interface or integrates with

other applications. The EMC displays the network diagram, statistics, and alerts for each site and overall NetFlow statistics. The interface provides a unified, global dashboard, consolidating data from multiple sites, showing their assets, activities, alerts, and access requests.

Fortinet Security Fabric

The Fortinet Security Fabric allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network. FortiGate is the foundation of the Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet Security products and Fabric-Ready Partner solutions.

About Claroty

Claroty is the world's leading industrial cybersecurity company. The Claroty Platform provides full-spectrum visibility across a rapidly growing and opaque operational technology (OT) attack surface. Claroty's technology delivers award-winning OT threat detection, continuous asset monitoring and management, and risk assessment. Founded in 2014, Claroty is headquartered in New York City and is backed by global investment leaders in cybersecurity, technology and industrial manufacturing, including Bessemer Venture Partners, Temasek Holdings, and the investment arms of Siemens, Rockwell Automation, and Schneider-Electric among others. For more information, visit www.claroty.com.

September 14, 2021 2:55 PM

MacintoshHD:Users:austin:Dropbox(RedRider):Clients:Fortinet:SolutionBriefUpdates:WorkingGroup2:sb-FA-fortinet-and-claroty-comprehensive-ics-and-scada-cybersecurity-solution:sb-FA-fortinet-and-claroty-comprehensive-ics-and-scada-cybersecurity-solution

513420-0-0-EN