SOLUTION BRIEF

Fortinet and Waterfall Security Solution

Safely monitor your OT from the comfort of your IT environment

Executive Summary

Fortinet and Waterfall Security, two of the leading operational technology (OT) cybersecurity technology companies, have joined forces to offer an advanced security solution for replicating industrial servers to the IT network and visualizing OT security and event data within the Fortinet FortiSIEM platform. With the integration of these technologies, industrial customers can securely retrieve OT server updates and other event data from OT collectors to the enterprise network and into the FortiSIEM platform without any exposure to internet-based cyberthreats. Additionally, the technology integration allows for seamless monitoring of a customer's fleet of Waterfall devices from within FortiSIEM.

The Challenge

Industrial organizations want to retrieve data from and have visibility into their OT environments. Security monitoring is a mature discipline on IT networks but provides limited visibility into OT and industrial control system (ICS) networks. Companies must connect their OT and IT networks and fully integrate OT monitoring devices with the enterprise SIEM to acquire access to their industrial performance. This merging contradicts network segmentation requirements and presents a large challenge to gaining full visibility of OT networks. Linking industrial networks to internet-connected enterprise networks and cloud platforms can sometimes create a serious security risk that must be overcome before data can arrive safely for enterprise and SIEM users.

Joint Solution

Fortinet and Waterfall Security have partnered to offer an advanced and robust solution that delivers a physically enforced unidirectional transfer of OT event data to FortiSIEM. Following the Purdue model for ICS security, industrial organizations will segregate the OT network from internet-connected devices and logically build a perimeter between OT and IT environments. Most OT sites resist any attempt to open additional paths through their industrial firewalls, even to permit monitoring data and alerts to pass through to their SIEM. Therefore, an additional layer of perimeter protection is added as unidirectional gateways.

Solution Components

Waterfall Security's unidirectional security gateways can physically send information in only one direction—from the industrial network to an external network. If no data can be sent back to the industrial network through the unidirectional gateways, no attacks can be sent back. Unidirectional gateway software replicates industrial servers to the IT networks and emulates the syslog devices to communicate events safely to FortiSIEM.

Solution Components

- Fortinet FortiSIEM
- Waterfall Security Unidirectional Security Gateway

Solution Benefits

- Maintains OT/IT segmentation following the Purdue model for ICS security and IEC62443 recommendations, assuring no data can flow from lower-security zones to higher-security zones
- Unbreachable hardware-enforced unidirectional protection for the OT network
- Real-time OT data flows seamlessly to FortiSIEM for analytics and incident management
- Complies with government regulations and standards for OT network segregation within critical infrastructure
- Receive alerts and notifications for Waterfall devices along with all OT assets from within the FortiSIEM platform
- Unparalleled security protection using the Fortinet Security Fabric

FORTINET FABRIC-READY

Fortinet FortiSIEM is designed to be the backbone of your security operations team, delivering capabilities ranging from automatically building your inventory of assets to applying cutting-edge behavioral analytics to detect and respond to threats rapidly.

Solution Integration

Large industrial customers often deploy multiple Waterfall unidirectional gateways across their various sites. To limit the different platforms required for OT asset monitoring, Waterfall and Fortinet have integrated the ability to visualize the unidirectional gateway performance from within FortSIEM. A unique dashboard has been added to FortiSIEM for the unidirectional gateway logs as an optional enhancement to the existing toolset.

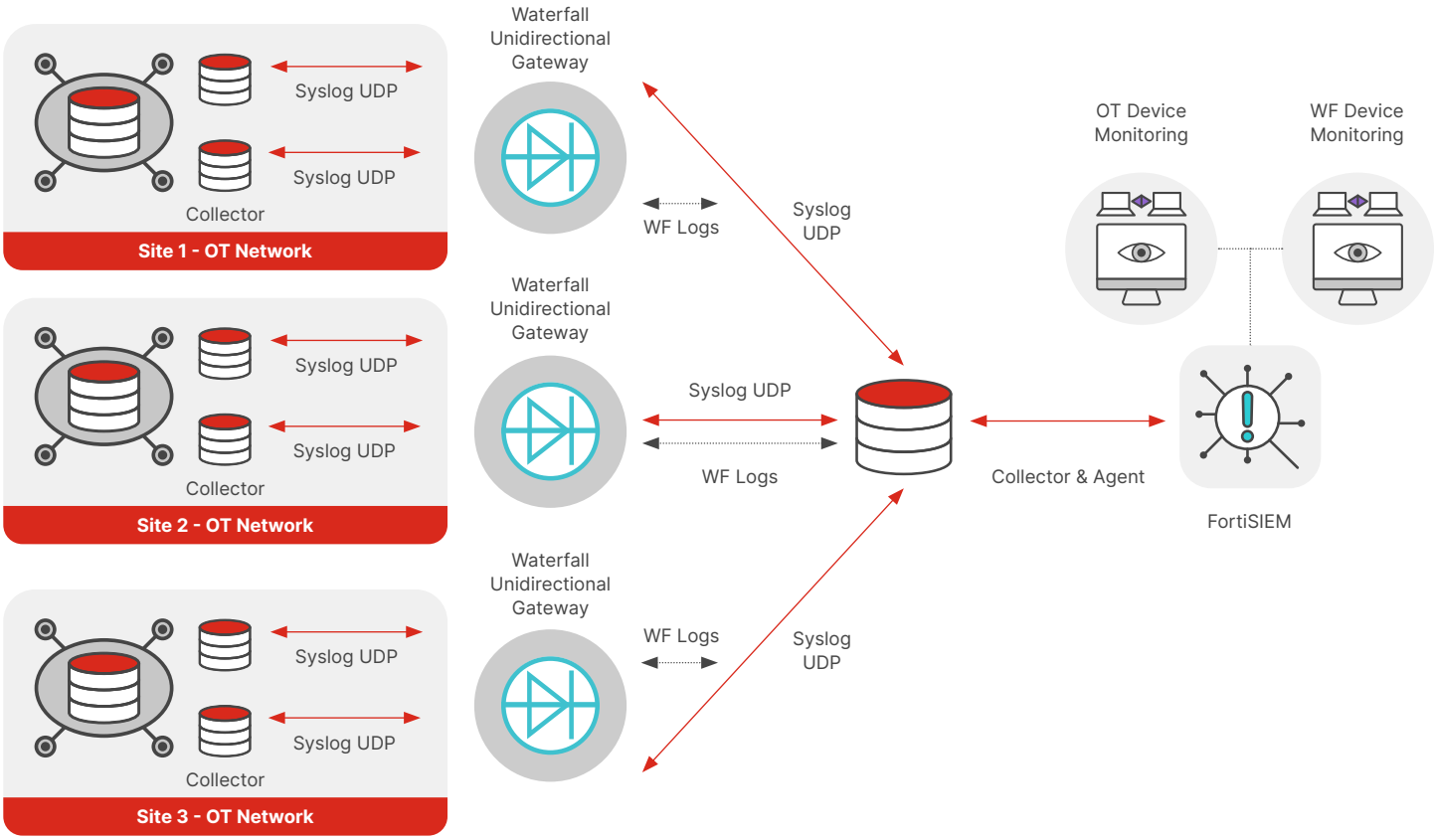

Figure 1: Waterfall Security and Fortinet integration

Use Cases

An oil and gas company needs to receive industrial data and remotely monitor incidents from its SIEM while maintaining absolute OT/IT segmentation. Additionally, the company would like to have real-time visibility on the performance of its fleet of Waterfall Security devices across all sites.

Challenge: Internet-enabled enterprise networks and cloud platforms can introduce cyber vulnerabilities into the critical OT network. The company has, therefore, adopted a strict policy forbidding any bidirectional cross-over from internet-connected devices to its OT assets. At the same time, it requires real-time updates of the supervisory control and data acquisition (SCADA) performance and live access to the event logs in its FortiSIEM interface.

Solution: The company deployed Waterfall unidirectional security gateways at each site to protect the OT networks from internet-based attacks. At the same time, they still receive updates and alerts from their OT devices. All relevant data is sent from the OT to the IT environment in real time without breaking their strict segregation policy and exposing their OT networks to cyberattacks.

About Waterfall Security Solutions

Waterfall Security Solutions' unbreachable OT cybersecurity technologies keep the world running. For over 15 years, critical industries and infrastructure have trusted Waterfall to guarantee safe, secure, and reliable operations. The company's growing list of global customers includes national infrastructures, power plants, nuclear reactors, onshore and offshore oil and gas facilities, refineries, manufacturing plants, utilities, and more. Waterfall's patented Unidirectional Gateways and other revolutionary products combine the benefits of impenetrable hardware with unlimited software-based connectivity, enabling 100% safe visibility into industrial operations and automation systems.

October 22, 2024 11:27 PM / MKTG-165-0-0-EN