WATERFALL®
Stronger Than Firewalls

WATERFALL FOR SECURITY MONITORING

SAFE OT NETWORK MONITORING

Opening paths through industrial firewalls to allow monitoring data to pass through to SOCs is problematic – all connections through firewalls introduce attack opportunities.

Unidirectional Gateways replicate servers and emulate devices, most commonly database servers, OPC servers as well as SNMP, Syslog and other security monitoring data sources. Enterprise users access the replica systems normally, without risk to the original OT network. The replica servers and devices provide central SIEM systems with the data that central SOCs need to diagnose and respond to OT intrusions. Waterfall for Security Monitoring enables safe and seamless universal security monitoring and IT/OT integration.

Unidirectional Gateways also facilitate safe and convenient OT network IDS sensor deployments. The gateways replicate network traffic captures from industrial mirror and SPAN ports to IDS sensors deployed on IT networks. With IDS sensors deployed on enterprise networks, those sensors can easily be updated and managed from a central SOC. Unidirectional Gateways provide the sensors with industrial traffic captures, while ensuring that the sensors are physically prevented from sending any packets or attacks back into the monitored OT switches and networks.

BENEFITS OF USING WATERFALL FOR SECURITY MONITORING

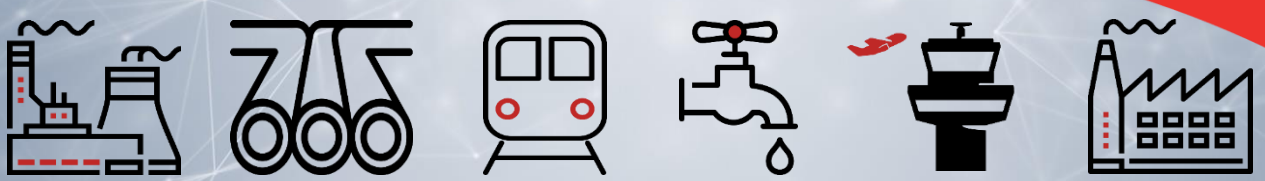
Secure replication of SNMP and Syslog alerts, and other security monitoring information

Simple deployment – the connector runs entirely in the Unidirectional Gateway with a simple web user interface

Eliminates remote control cyberattacks and online malware propagation

Facilitates compliance with NERC CIP, NIST 800-82, ANSSI, IEC 62443 and more

Safe visibility into ICS networks and systems from central and cloud-based SOCs



Power | Pipelines | Rail | Water | Facilities | Manufacturing

WATERFALL®
Stronger Than Firewalls

WATERFALL FOR SECURITY MONITORING

Central OT security monitoring is focused on alerts encoded as log files, Syslog or SNMP traps and sometimes other data sources and formats, such as OPC-DA or historians. Waterfall for SNMP captures SNMP traps according to user-configured rules and pushing those traps through unidirectional hardware to enterprise SIEMs. Waterfall for Syslog is a standard Syslog server on a protected industrial network, gathering Syslog messages from that network, again pushing them through unidirectional hardware into the enterprise network. Waterfall's OPC-DA, OPC-UA, and the many historian connectors similarly replicate those data sources to enterprise networks for easy access by enterprise and cloud-based SIEMs.

Waterfall for IDS is a hardware-enforced, physical barrier that prevents remote attacks, malware, DOS attacks, ransomware and human errors originating on IT networks from compromising or impairing physical operations, while enabling seamless interoperability with intrusion detection system platforms. Together, this family of solutions enables safe, seamless monitoring of OT networks from enterprise and cloud-based Security Operations Centers (SOCs), without the risks that always accompany firewalled access to sensitive OT networks.

FULLY-FEATURED & ROBUST SUPPORT:

- Replicates Syslog clients and SNMP devices to central SIEM systems and Security Operations Centers
- Supports industry-leading SIEMs and Intrusion Detection vendors including: Trellix, ArcSight, QRadar, Radiflow, Dragos, ForeScout, Splunk & Splunk Universal Forwarder
- Standard 1-10Gbps connectivity
- Flexible configurations do not require new hosts or software installed on OT networks
- Optional aggregation of multiple industrial clients and sites into a single enterprise server

Trellix DRAGOS QRadar IBM splunk> Radiflow CyberRes ArcSight FORESCOUT

INFO@WATERFALL-SECURITY.COM | WWW.WATERFALL-SECURITY.COM

ABOUT WATERFALL

Waterfall Security Solutions' unbreachable OT cybersecurity technologies keep the world running. For more than 15 years, the most important 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 generators, onshore and offshore oil and gas facilities, refineries, manufacturing plants, utility companies, and more. Waterfall's patented Unidirectional Gateways and other solutions combine the benefits of impenetrable hardware with unlimited software-based connectivity, enabling 100% safe visibility into industrial operations and automation systems.