WATERFALL®
Stronger Than Firewalls

WATERFALL FOR SECURITY MONITORING

SAFE OT NETWORK MONITORING

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

Unidirectional Gateway software replicates servers and emulates devices, most commonly database servers, OPC servers as well as SNMP & Syslog devices. Enterprise users access the replicas normally, without risk to the original OT network. The emulated/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

Elimination of remote control cyberattacks and online malware propagation

Facilitating compliance with NERC CIP, NIST, CFATS, ANSSI, UK DfT and more

Safe visibility into industrial control system networks and systems from central and cloud-based SOCs

Simple deployment, off-the-shelf solution

Rails

Oil & Gas

Manufacturing

Water

Power

Chemicals

WATERFALL®
Stronger Than Firewalls

WATERFALL FOR SECURITY MONITORING

Central security monitoring is focused on alerts encoded as Syslog or SNMP traps. Waterfall for SNMP captures SNMP traps according to user-configured rules. Trap content and metadata are forwarded through Waterfall's Unidirectional Security Gateway hardware to one or more central Network Management Systems or Security Operations Centers. These central systems may be hosted on an enterprise network or in an Internet-based cloud without risk to operations.

Waterfall for Syslog is a standard Syslog server on a protected industrial network, gathering Syslog messages from that network. Syslog alert content and metadata are forwarded through Unidirectional Gateway hardware. On the external network, new Syslog alerts are formulated and sent to a central or cloud-based SIEM or SOC without risk to operations..

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. Unidirectional OT traffic capture replication further enables OT IDS sensors to be deployed safely and conveniently on IT networks, while monitoring OT network traffic, without introducing new attack vectors into OT networks.

FULLY-FEATURED & ROBUST SUPPORT:

- Emulates Syslog clients and SNMP devices to central SIEM systems and Security Operations Centers
- Supports the following industry-leading SIEMs and Intrusion Detection vendors: FireEye Helix, McCaffee ESM, HP ArcSight, IBM QRadar, Radiflow, Dragos, CyberX, ForeScout, Splunk & Splunk Universal Forwarder
- Flexible hardware configurations include options where no new hosts or software need be introduced to sensitive ICS networks
- Enables secure, real time monitoring of critical assets across the organization
- Optional aggregation of multiple industrial clients and sites into a single enterprise server

McAfee Enterprise Security Manager · QRadar IBM · DRAGOS · splunk> · radiflow · hp ArcSight · CyberX · FireEye · FORESCOUT

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

ABOUT WATERFALL SECURITY SOLUTIONS

Waterfall Security Solutions is the OT security company, producing a family of Unidirectional Gateway technologies and products that enable enterprise-wide visibility for operations, with disciplined control. Waterfall products represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, off and on shore oil and gas facilities, refineries, manufacturing plants, utility companies, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases and protocols in the market. For more information, please contact info@waterfall-security.com