WATERFALL®
Stronger Than Firewalls

# WATERFALL FOR SECURITY MONITORING

## SECURE REPLICATION OF SYSLOG AND SNMP DATA

Opening paths through industrial firewalls to allow data and alerts to pass through to Security Operations Center (SOCs) is problematic – all connections through firewalls introduce attack opportunities. Waterfall for Security Monitoring is based on Waterfall's Unidirectional Gateway technology, enabling visibility into networks without introducing connectivity risks.

Unidirectional Gateway software replicates servers and emulates devices, such as SNMP and Syslog devices. Enterprise users access the replicas normally and bidirectionally, without risk to the original OT network. The replica servers provide central Security Information and Event Monitoring (SIEM) systems with the data that central SOCs need to diagnose and respond to OT intrusions. Waterfall for Security Monitoring enables safe, universal security monitoring and safe, seamless IT/OT integration.

Waterfall's simple installation, configuration and monitoring tools make it easy for users. Comprehensive diagnostics include real-time alarms that alert the user of fault conditions via Syslog, Windows logs, email, SNMP traps, log files, and Waterfall's monitoring console.

## 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 | Pharma

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..

## FULLY-FEATURED & ROBUST SUPPORT:

- Replicates Syslog and SNMP alerts and indexes in real-time
- Supports the following SIEMs: FireEye Helix, McCaffee ESM, HP ArcSight, IBM QRadar, Splunk & Splunk Universal Forwarder
- Enables secure, real time monitoring of critical assets across the organization
- Optional aggregation of multiple industrial clients and sites into a single enterprise server
- Standard 1Gbps connectivity
- Fully transparent to users

### SNMP

- Emulates SNMP devices to central Network Management Systems and Security Operations Centers
- Supports SNMP versions: 1, 2 and 3
- Optional encryption
- Replicates an unlimited number of managed devices

### SYSLOG

- Emulates Syslog clients to central SIEM systems and Security Operations Centers
- Supports both TCP and UDP-based Syslog clients and servers
- Optional encryption
- Support for and partnered with a wide range of SIEM and log analysis providers

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

## ABOUT WATERFALL SECURITY SOLUTIONS

Waterfall Security Solutions is the global leader in industrial cybersecurity technology. The company's expanding portfolio of customers includes national infrastructures, power plants, nuclear plants, offshore oil and gas facilities, rail transport, 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. Please contact: info@waterfall-security.com

Waterfall's products are covered by U.S. Patents 7,649,452, 8,223,205, and by other pending patent applications in the US and other countries. "Waterfall", the Waterfall Logo, "Stronger than Firewalls", "In Logs We Trust", "Unidirectional CloudConnect", and "CloudConnect, and "One Way to Connect" are trademarks of Waterfall Security Solutions Ltd. All other trademarks mentioned above are the property of their respective owners. Waterfall Security reserves the right to change the content at any time without notice. Waterfall Security makes no commitment to update content and assumes no responsibility for any mistakes in this document. Copyright © 2019 Waterfall Security Solutions Ltd. All Rights Reserved. www.waterfall-security.com