waterfall

WATERFALL FOR HP ARCSIGHT

SECURE REPLICATION OF HP ARCSIGHT DATA

Opening paths through industrial firewalls to allow data and alerts to pass through to Security and Information Event Managers (SIEMs) is problematic – all connections through firewalls introduce potential attack opportunities. Waterfall for HP ArcSight is based on Waterfall's Unidirectional Gateway technology, enabling visibility into networks without introducing connectivity risks.

Unidirectional Gateway software securely replicates HP ArcSight Enterprise Threat and Risk Management (ETRM) SIEM servers to business networks. Enterprise users access the replicas normally and bidirectionally without risk to the original OT network. The replica servers provide central SIEM systems with the data that they need to diagnose and respond to OT intrusions without the connectivity risk. Waterfall for HP ArcSight enables secure universal security information and event monitoring with safe 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 HP ARCSIGHT

Secure replication of HP ArcSight alerts

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

Eliminates remote-control cyber attacks and online malware propagation

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

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

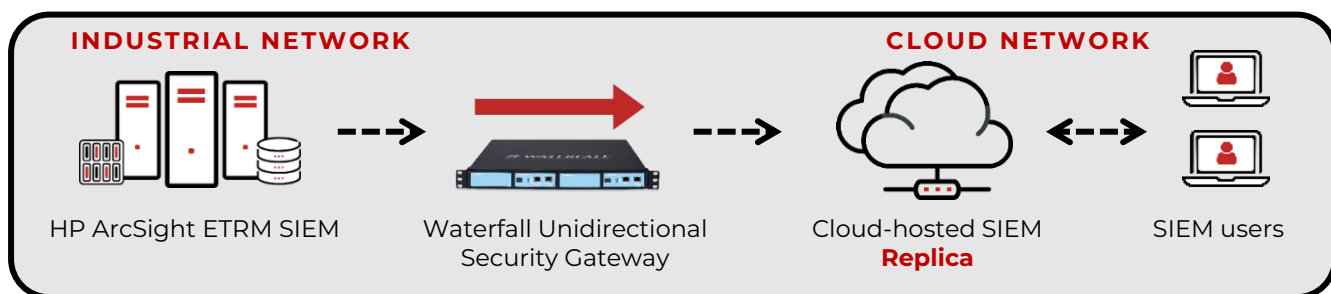Power   Oil & Gas   Rail   Facilities   Water   Manufacturing   Government

WATERFALL FOR HP ARCSIGHT

Waterfall addresses the need for making ArcSight SIEM visible on the business network, while guaranteeing the absolute security of the critical operational network. Waterfall's physical hardware-based isolation protects operational assets by eliminating any threat of cyber-attack, incoming malware or human errors originating from external networks back into the critical network. Waterfall for HP ArcSight gathers data from the HP ArcSight ETRM SIEM located in the Industrial (OT) network, and forwards HP ArcSight alert content and metadata through Unidirectional Gateway hardware. On the external (IT) network, new alerts are formulated and sent to a central or cloud-based SIEM or SOC without risk to operations.

The Waterfall Unidirectional Gateway appliance deployed between IT and OT networks includes TX hardware containing a fiber-optic transmitter/laser, and RX hardware containing an optical receiver but no laser. The Gateway hardware makes it physically impossible for attacks to flow from the corporate network towards the industrial network, eliminating any threats of online attacks, malware or human errors.

INDUSTRIAL NETWORK   **CLOUD NETWORK**

HP ArcSight ETRM SIEM   Waterfall Unidirectional Security Gateway   Cloud-hosted SIEM **Replica**   SIEM users

FULLY-FEATURED & ROBUST SUPPORT:

» Replicates HP ArcSight alerts and indexes in real-time

» Enables secure, real-time monitoring of critical assets across the organization

» Optional aggregation of multiple industrial clients and sites into a single enterprise server

» 1-10 Gbps standard throughput

» Fully transparent to ArcSight SIEM users

» Waterfall for ArcSight tested and benchmarked by HP

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.