WATERFALL®
Stronger Than Firewalls

WATERFALL FOR SIEMENS SIMATIC S7

SECURE ENTERPRISE MONITORING OF SIEMENS SIMATIC S7 DEVICES

Industrial enterprises frequently need enterprise-wide access to data from devices supporting the Siemens Simatic S7 industrial communications protocol. Connecting enterprise networks to Simatic S7 devices through firewalls is high risk. All software can be hacked and all firewalls and Simatic S7 implementations are software.

The Waterfall for Siemens Simatic S7 connector gathers snapshots of state information on Siemens Simatic S7 devices in real time, sends those snapshots through the Waterfall unidirectional hardware and emulates Siemens Simatic S7 devices on the enterprise or SCADA network. Enterprise & SCADA users and applications access the emulated devices bi-directionally, as if they were still communicating with the original devices. The Waterfall unidirectional hardware physically prevents any attack or malicious command from reaching the protected devices.

SIEMENS

BENEFITS OF USING WATERFALL FOR SIEMENS SIMATIC S7

Secure, real-time unidirectional emulation of Simatic S7 devices to external SCADA and enterprise networks

External users and applications interact normally with accurate, timely replicas of Siemens Simatic S7 devices

Eliminates all remote attacks and malware propagation from external networks

Facilitates and simplifies compliance with NERC CIP, NIST, CFATS, ANSSI, UK DfT & more

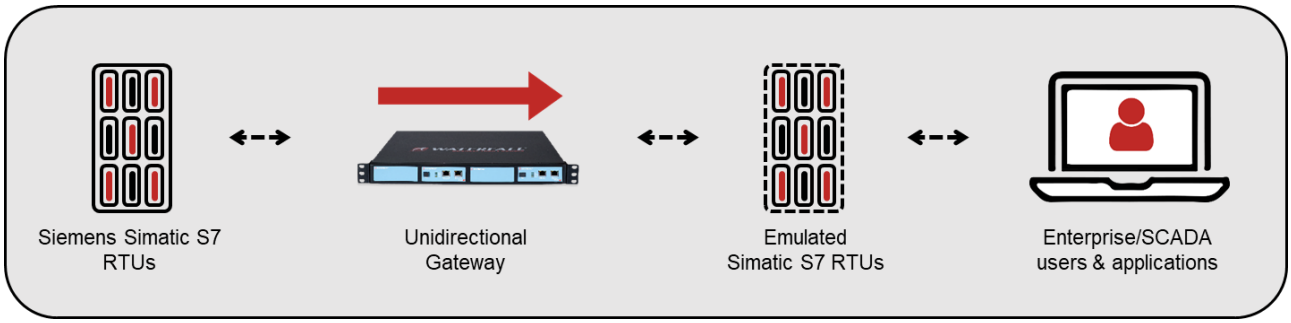
Simple deployment, off-the-shelf solution

WATERFALL®
Stronger Than Firewalls

WATERFALL FOR SIEMENS SIMATIC S7

The Waterfall for Siemens Simatic S7 TX connector is a Simatic S7 master and uses Simatic S7 polls and report-by-exception events to gather a snapshot of the state of Simatic S7-enabled devices. The TX Host module sends this snapshot to the RX Host module through the unidirectional hardware modules. The RX Host module is a Simatic S7 slave, which waits for polls from the Simatic S7 master, or reports by exception to that master station. The RX software serves as a faithful emulation of the enabled devices in the protected network, responding to interactions with the master in the same way as the emulated device would have responded, without permitting any messages back into the protected network. Enterprises deploying the Waterfall for Simatic S7 connector benefit from increased visibility of industrial data, reduced compliance costs and dramatically reduced cyber risk and incident costs.

The Waterfall Unidirectional Gateway hardware deployed between both networks includes a TX hardware module containing a fiber-optic transmitter/laser, and an RX hardware module containing an optical receiver. The gateway hardware makes it physically impossible for attacks to flow from the external network towards the protected network, eliminating any threats of online attacks, malware or human errors.



FULLY-FEATURED & ROBUST SUPPORT:

- Real-time device emulation of Siemens Simatic S7 protective relays, RTUs, IEDs, and other Simatic S7 equipment
- Replicates many Simatic S7 devices on a single host
- Supports both Simatic S7 master and slave emulation
- Supports all Simatic S7 data types and point types
- 1 Gbps throughput standard & High Availability option
- Fully supported with Waterfall Unidirectional Security Gateway software

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