Waterfall One Way – Unidirectional connectivity for securing critical networks

Colin Blou
Sales Director

The material in this document was prepared for the purpose of potential business and is proprietary to Waterfall Security Solutions Ltd. This document is strictly secret and confidential and is provided with the understanding that it will be held secret and confidential. No part of this document may be disclosed to any third party, copied, reproduced or stored on any type of media or otherwise used in any way without the express, prior, written consent of authorized officers and/or executives of Waterfall Security Solutions Ltd.
Introducing: Waterfall Solutions Ltd

- A private company specializing in network and data security
- Located in Rosh-Ha’ayin, Israel
- Product first launched in 2004, following Israeli MOD requirement
- Waterfall spun off as a company at end of 2006
- Successful sales in Israel, Europe and North America (hundreds of operational systems deployed)
- Patented technology for unidirectional security in SCADA environments
Main Threat Scenarios:

- **Scenario I - Critical & Corporate Networks**: The critical (operational, control) network is required to send online information to the business/administrative networks.
  - Via these connections,
    - Attackers can *gain access to the critical network* and carry out remote, online attacks into it.
    - Malware can be introduced from the Corporate network into the Control network.

- **Scenario II - Remote Monitoring**: A Control Center or Operations Center is remotely monitoring a critical network.
  - The Center may be monitoring many *other networks/systems*.
  - Hackers can now move between networks, and attack networks and connected assets as well as the control centers.
Existing Security Approaches

- **The Traditional Approach – IT Security:**
  - Firewalls, intrusion detection and prevention systems
  - Anti-viruses and content filters
  - Encryption and authentication

- **IT Security is not enough here:**
  - All IT Security products suffer from software vulnerabilities, bugs and miss configuration – thus, can be hacked and circumvented
  - Attackers are financially backed up and highly motivated
  - Hacking information and know-how is out there, and plentiful

- **The Strict Approach – Total Segregation**
  - Fully segregate the SCADA network from the outside world
  - Business processes will not work, or will be drastically impaired
Unidirectional Gateway Approach

- Security promise
  - Hackers on the outside have no physical hacking path
  - The secured NETWORK is protected (with all internal assets)
  - Hacking sessions are impossible
  - Absolutely no data transfer in the “wrong” (i.e. RX→TX) direction
Waterfall One-Way™ includes connectors for:

**Leading Industrial Applications/Historians**
- OSIsoft PI, GE iHistorian, GE iFIX
- GE OSM, Siemens WinTS, SINAUT
- Instep eDNA (final stages of development)

**Leading Industrial Protocols**
- Modbus, OPC (DA, HDA, A&E)
- DNP3, ICCP

**Leading IT Monitoring Applications**
- Log Transfer, SNMP, SYSLOG
- CA Unicenter, CA SIM, HP OpenView
- Matrikon Alert Manager

**Remote Screen View™**
- Unidirectional transfer of real-time screen display capture

**Other connectors**
- UDP, TCP/IP
- Video/Audio stream transfer
- Mail server/mail box replication
- IBM WebSphere MQ series
- Antivirus updater, patch (WSUS) updater
- Remote Print server

**File/Folder Mirroring**
- Folder, tree mirroring, remote folders (CIFS)
- FTP/TFTP/SFTP/FTPS/RCP
Waterfall One-Way™ Regulations’ support:

Relevant regulations and guidelines

- 10 CFR 73.54
- NRC RG 5.71
- NIST
  - 800.53 - Security Controls for Federal Information Systems and Organizations
  - 800.82 - Guide to Industrial Control Systems Security
- NERC
  - CIP 002 to 009

“provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in Title 10 of the Code of Federal regulations (10CFR) Part 73, Section 73.1.”

“implementation of state-of-the-art defense-in-depth protective strategies” RG73.54c(2), whose aim “to ensure that the functions or tasks required to be performed by the critical assets ... are maintained and carried out” RG73.54c(4) and “to prevent adverse effects from cyber attacks” (10CFR 73.54c(3)).

Detailed whitepapers

- Waterfall for NRC Compliance with regard to NIST 800.53 and 800.82
- Waterfall NERC Compliance with regard to NERC CIP
WF-SME for OSIsoft PI/GE i Historian and more

Business Network
Historian online Replica Server

Online replication of tens of thousands points

Industrial Network
Historian Serve Master

Site A
Site B
Site C
Site D
Site N

Internet
WF SME for OSIsoft® PI™

Business Network
- Waterfall for OSIsoft PI
  - RX Server

PI Database Subsystem

PI Snapshot Subsystem

Industrial Network
- Waterfall for OSIsoft PI
  - TX Server

Master PI Server

Replica PI Server

Real-time replication of
- Tags database changes (APS)
- Tags data (snapshots)
Replicating a Modbus (SCADA) server - Solution

OPC, DNP3, ICCP and many more protocols are supported
File Transfer – Separating the Critical Network

- **Schematic Solution Configuration:**

- **Supported:** Simple file transfer, Folder tree replication, FTP, FTPS, MQ, and more
Waterfall Remote Screen View (WF-RSV):

- Enabling secure external display of control rooms and monitoring centers screens
- Enabling simplified and now secure remote assistance and maintenance
- Real-time unidirectional replication of workstation or server display screens, to external networks.
Unique Advantages

- Unidirectional Security Gateway™ - A comprehensive Solution and not just a data diode component/s.
- Patented technology for SCADA security
- Designed and built to meet CNI needs
- Enables compliance with relevant requirements found in NERC-CIP, NIST 800.53 and 800.82, RG 5.71
- Host hardware invariance - server agnostic, hardware independence
- Simple hardware maintenance
- Off the shelf integral support for Historians, SCADA protocols, file transfers and streaming.
- OSIsoft Partner – benchmark and certification
- Full PI support
- High Availability support - hardware and software
- 1GB support –hardware and software
- Inherent buffering mechanisms
Solution Highlights – Thinking Outside the Box!

- **Absolute protection** against outside hackers and data theft
- Protection for data, network and network-connected assets
- Unidirectional core is **fully future-proof**
- Flexibility through the software agents
- Advanced administration and monitoring capabilities
- Extensive protocol and application support
- Immune to human error or mis-configuration

**Sleep well!!**

**Waterfall is unbreakable!!!**

**Nobody can change the law of physics!!!**
_deployed at*:

- CPNPP – Luminant
- Progress Energy – Nuclear Fleet installation
- USA Nuclear Power Plants in MI, PA, NY and NC.
- Fossil power plants in Canada (NB power)
- Israel Electric Corporation (IEC)
- Mekorot – Israel’s national water utility
- Egypt-Israel natural gas pipeline (INGL)
- Eilat-Ashkelon oil pipeline
- Government organizations worldwide
- Banks and financial organizations

* Select Examples
THANK YOU!