Waterfall® for Software Updates

Secure Distribution of Software Updates

- Hardware-enforced security for absolute protection
- Eliminates vulnerabilities inherent to all firewalls
- Dramatically reduced risk due to online attacks and human errors
- Supports all major antivirus vendors, MS WSUS, and OPSWAT kiosks
- Validates updates against vendor's cryptographic signatures
- Simplifies NERC-CIP, ANSSI, NIST, and other regulatory compliance
- Supports Waterfall's FLIP® configuration
- Optional high availability (HA) configurations
- Full Gigabit throughput

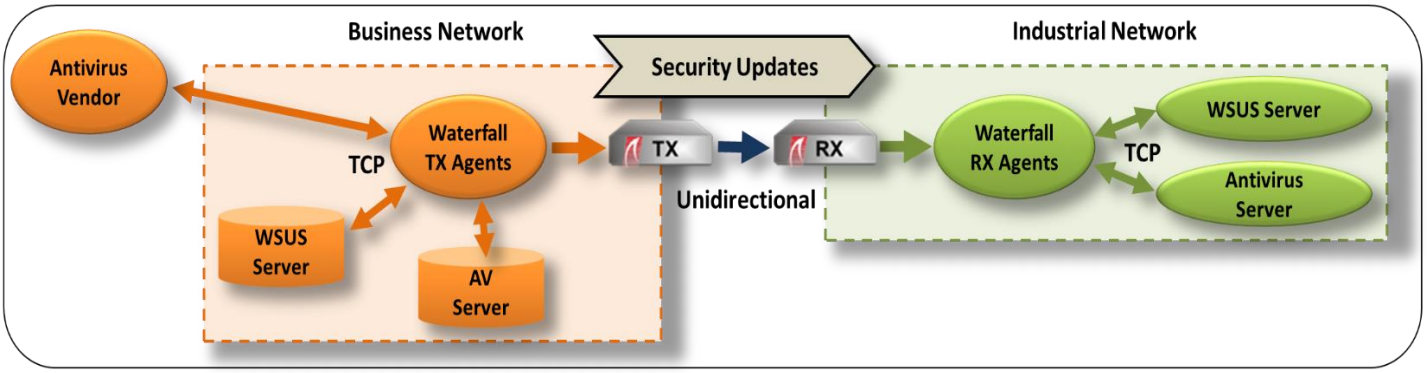
Overview

Installing security updates, such as operating system and antivirus signature updates, are an important practice that organizations must take to protect critical assets. These updates have traditionally been done through firewalls or by removable media, such as USB sticks; however, both are prone to security issues and put industrial environments at significant risk jeopardizing the safety and reliability of the environment. When permitted through firewalls, a two-way connection is made from an external system with no reliable way of knowing if it has been compromised, including the update files. If it has, the firewall provides a direct path to the industrial network regardless of whether the connection is encrypted or not. A similar threat exists using removable media as it is often used on many systems on both the industrial and business networks. Undetected malware on any of these systems can propagate to the industrial network using the USB stick as an easy way to hop between networks - including air-gapped networks.

Waterfall for Software Updates, part of Waterfall's Unidirectional Security Gateway family of products, provides a secure and reliable method of replicating update files in real-time without the cyber-security risks that always accompany firewalls and removable media.

Stronger Than Firewalls: Waterfall for Software Updates

Waterfall's software update solution is a combination of hardware and software where, unlike traditional security solutions, security is enforced through the hardware eliminating the possibility of an attacker launching a remote control or command and control attack into the industrial network from the compromised business system. By enforcing security through the hardware, all software updates go through the unidirectional fiber optic link physically preventing any form of two-way communications. In addition, vendor cryptographic signatures are checked before the updates enter the industrial network.



Waterfall for Software Updates Unidirectional Replication

Waterfall's solution for software updates enables real-time replication of antivirus signatures and operating system updates securely into the industrial environment eliminating the risk of remote control and command and control attacks, common with today's threats, thus putting the safety and reliability of the environment at risk. On the business network, Waterfall software is a client of the corporate antivirus and/or WSUS servers, or even the vendor's antivirus repository if preferred, and receives the update files once they have been made available. On the industrial network, the Waterfall software is also a client of the organization's antivirus and/or WSUS servers and receives the replicated updates through the unidirectional fiber optic link before pushing the updates to the industrial antivirus and/or WSUS servers for distribution. Bi-directional communications still take place between the corporate antivirus/WSUS servers and the Waterfall software as well as between the industrial antivirus/WSUS servers and the Waterfall software on the industrial side; however, with the unidirectional gateways, the data can physically only flow inbound and has no capability of receiving anything back.

Highlighted Unique Features

Waterfall for File Transfers includes a wide variety of features, such as:

- Real-time replication of antivirus and OS updates
- Supports major antivirus vendors and OPSWAT kiosks
- Validates updates against vendor cryptographic checksums prior to entering industrial network
- Minimal changes required to existing infrastructure
- Modular, scalable, and user-serviceable hardware
- Full Gigabit throughput
- Optional high-availability (HA) configurations
- Advanced content policy control with Waterfall's Application Data Control option for data filtering

Regulatory Compliance and Certification

No misconfiguration of Unidirectional Gateway software can impair the security provided by the gateway hardware. This results in dramatically reduced perimeter operating costs and costs of compliance with NERC-CIP, ANSSI, NRC, CFATS, NIST, ISA-SP99, and other standards, guidance, and regulations. The gateway solution is certified Common Criteria EAL4+, resistant to high attack potential. Waterfall's Unidirectional Gateways are the only unidirectional solution to pass a cyber-security assessment by Idaho National Labs.

For further information, please contact us or visit our website: www.waterfall-security.com

USA T: +1 (212) 714-6058 F: +1 (212) 465-3497

International T: +972 3-900-3700 F: +972 3-900-3707

Information: info@waterfall-security.com
Sales: sales@waterfall-security.com