WATERFALL®
Stronger Than Firewalls

WATERFALL BLACKBOX®
In Logs We Trust®

Prevents Manipulation and Deletion of Logs During an Attack
Ensures Reliable Forensics for Attack Analysis
Facilitates Effective Incident Response

FEATURES & BENEFITS

Secure Storage

- Hardware-enforced unidirectional protection of logged data
- Tamper-proof storage for logs, transactions & configuration files
- Reliable forensics, incident response & recovery, and audits
- Encryption and authentication of logged information
- No possibility of leaking information between sites

Wide Variety of Data Sources

- Syslog, SNMP traps, Windows logs
- FTP, SFTP, CIFS/SMB, drag & drop and many other file sources
- System Backups
- SQL Server, Oracle and other relational databases
- Network traffic and NetFlow statistics

Secure Log Data Retrieval

- Logs accessed via dedicated out-of-band port
- Powerful graphical data management and retrieval applications
- Full or partial retrieval with search and filter capabilities

Data Management

- All logs unified and stored in internal relational database
- All recorded data time-stamped and encrypted
- Cyclic & never-overwrite data management options
- Version management for configuration and other files
- Real-time statistics display
- Optional compression

How do you stay one step ahead of an attacker who seeks to erase all evidence of an attack?

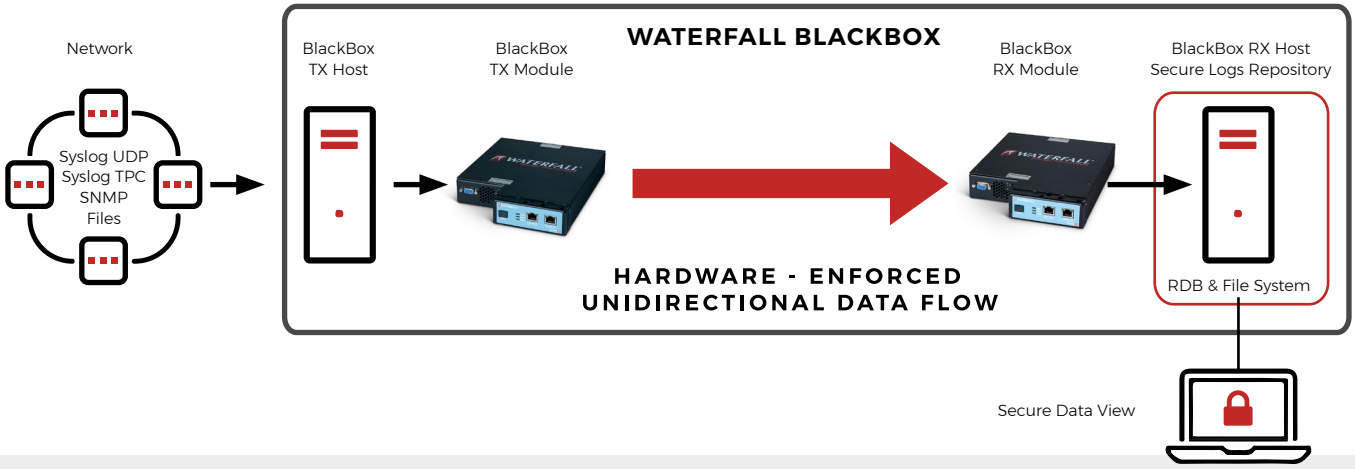
The Waterfall BlackBox prevents attackers from covering their tracks. Modern cyber attackers routinely erase or compromise logs to hide evidence of wrong-doing. All network repositories, including central SOCs and cloud backups, can be accessed and so can be breached. The Waterfall BlackBox provides a tamper-proof, online repository which can survive a cyber attack.

How can you recover from a cyber attack if you can't trust your log information?

The Waterfall BlackBox facilitates effective incident response. Incident response after an attack is only as good as the integrity of the data used to analyze what happened. Reliable backups, transaction records and device configurations are essential to post-incident recovery and business continuity. Incident response teams are tasked to clean the network and close the door through which the attacker entered the network in the first place – all of which depends on their ability to analyze the logs.

What do you do after an attack when you need to know what happened?

Waterfall BlackBox ensures reliable forensics for attack analysis. When investigating ongoing or past cyber incidents, security experts need to know that log information is reliable and trustworthy. Network, application and security activity logs are essential for understanding how a network has been breached and misused post-breach. The Waterfall BlackBox is like a "flight recorder" for cybersecurity.



FORM FACTORS

The BlackBox is available to fit your mission's requirements. It comes in two form factors: **1u Rack Mount** and **Carry-On**.

The 1u rack mount Waterfall BlackBox is permanently installed on a network topology and deployed before an attack; continuously collecting important forensic information.

The Carry-On form factor can be transported from site to site by incident response members and field personnel. The Carry-On serves to capture the details of an attack in progress, especially when attackers are trying to defeat such an investigation

HOW IT WORKS

Waterfall Security's patented BlackBox leverages Waterfall's-market-leading, hardware-enforced unidirectional technology to securely gather, store, and transmit transaction, log and other data into a storage repository located securely "behind" a Unidirectional Gateway. All data sent to the storage respository is stored physically outside of the monitored network, inaccessible and untouchable.

SECURE DATA VIEW

Access to stored data is possible only via the Secure Data Access port. The Waterfall BlackBox faceplate hardware physically blocks the Secure Data Access Port when the port is not in use.

As an airplane black-box survives a crash, the Waterfall BlackBox survives a cyber attack – keeping your logs untampered and secure.

Specifications		
	1u Rack	Carry-on
External Host	2 core/16 G 128 G Flash	2 core/16 G 128 G Flash
Protected Host, Standard	2 core/16 G 500 G Flash	2 core/16 G 500 G Flash
Protected Host, Expanded	2 core/16 G 8.5 TB Flash	2 core/16 G 8.5 TB Flash
Monitored Network	1Gbps copper	1Gbps copper
Configuration Port	1Gbps copper	1Gbps copper
Secure Data Access	1Gbps copper	1Gbps copper
Dimensions	43x50x4.4cm	42x18x40cm
Weight	9kg	13.1kg
Power Supplies	2 per side (4)	1 per side (2)

ABOUT WATERFALL SECURITY

Waterfall Security Solutions is the global leader in industrial cybersecurity technology. Waterfall products, based on innovative unidirectional security gateway technology, represent an evolutionary alternative to firewalls. The company's expanding array of customers includes national infrastructures, power plants, rails, nuclear plants, onshore and offshore oil and gas facilities, 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. For more information, visit www.waterfall-security.com.