WATERFALL®
Stronger Than Firewalls

IN LOGS WE TRUST®

WATERFALL BLACKBOX®

PRODUCT BROCHURE

THE CHALLENGE

What do you do after an attack when you need to know what happened? How can you recover from a cyber attack if you can't trust your information? 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, and prevents attackers from covering their tracks.

FEATURES & BENEFITS

- **TAMPER PROOF LOGS REPOSITORY**
  Preserves copies of logs, packets & other data before and during a cyber attack
- **ENABLES EFFECTIVE INCIDENT RESPONSE**
  Reliable forensics facilitate post-attack analysis of a cyber attack and ensure businesscontinuity
- **SECURE STORAGE**
  Hardware-enforced unidirectional protection of logged data with encryption and authentication of logged information
- **SECURE DATA RETRIEVAL**
  The BlackBox appliance can only be accessed physically via a dedicated out-of-band port
- **MULTIPLE FORM FACTORS**
  BlackBox is available in 1U Rack Mount form factor for permanent pre-attack deployment

1

SECURE FORENSICS

store logs, transactions & configuration files out of hacker's reach

2

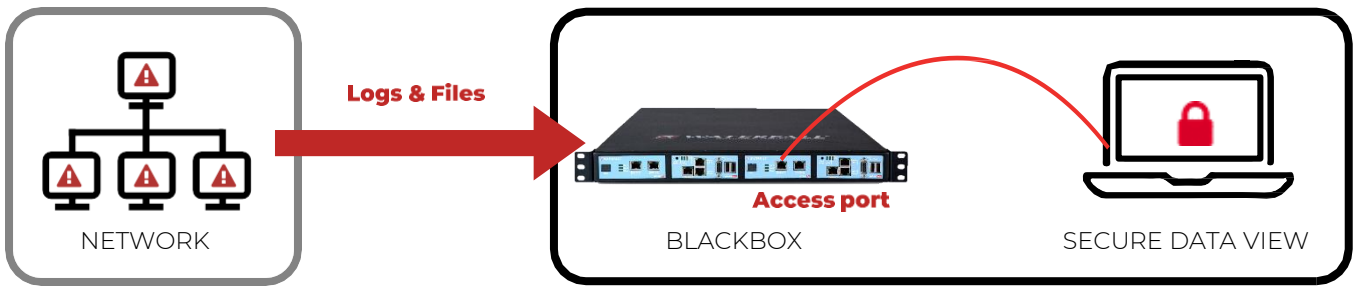
DISABLE ATTACKERS

who seek to maniplate logs & cover their tracks

3

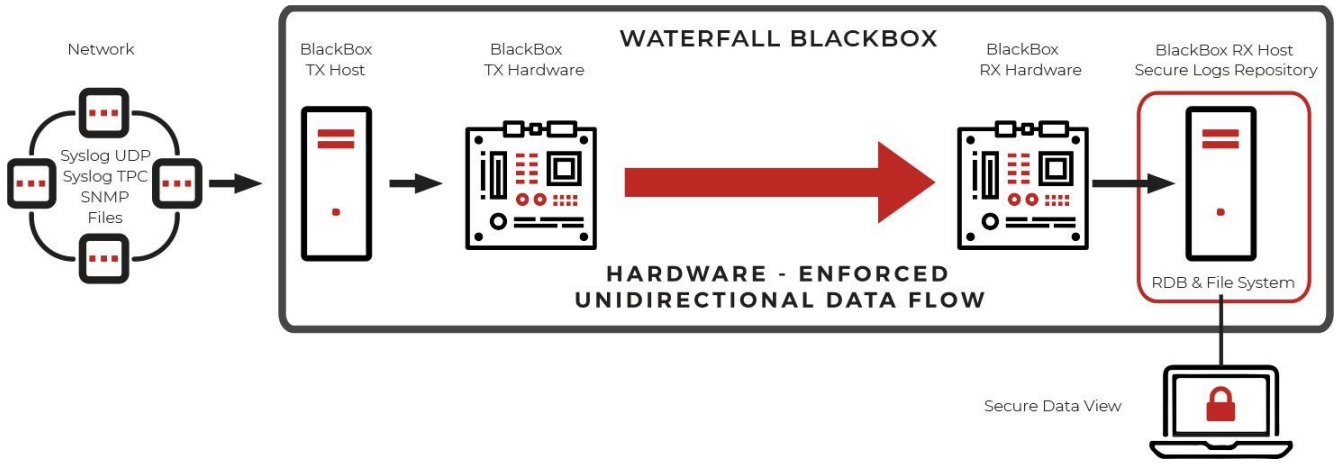
INVESTIGATE & RECOVER

from a cyber attack with reliable and trust-worthy information



WATERFALL®
Stronger Than Firewalls

THEORY OF OPERATION



AS AN AIRPLANE BLACK-BOX SURVIVES A CRASH, THE WATERFALL BLACKBOX SURVIVES A CYBER ATTACK, KEEPING LOGS INTACT AND SECURE.

Inside Waterfall's BlackBox is a high-speed, high-capacity logging and analysis system able to record attack information, attempted changes, manipulation of records and abnormal logging and recording conditions. When necessary, data can be retrieved and inspected securely by physically accessing the BlackBox appliance via the Secure Data Access port.

Unidirectional Gateway technology contains both hardware and software components. The hardware components include a TX side, containing a fiber-optic transmitter/ laser, and an RX side, containing an optical receiver, but no laser. The gateway hardware can transmit information from a signaling system network to the BlackBox data manager, but is physically incapable of sending any status, feedback or any signal at all back to an attacker who might seek to subvert the recording system.

WIDE VARIETY OF DATA SOURCES

Syslog, SNMP traps, Windows logs, FTP, SFTP, CIFS/SMB, System backups, relational databases, network traffic, NetFlow Statistics and more

INFO@WATERFAL-SECURITY.COM | WWW.WATERFAL-SECURITY.COM

ABOUT WATERFALL SECURITY SOLUTIONS

Waterfall Security Solutions is the OT security company, producing a family of Unidirectional Gateway technologies and products that enable enterprise-wide visibility for operations, with disciplined control. Waterfall products represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, off and on shore 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. Please contact: info@waterfall-security.com