FORCEPOINT
POWERED BY Raytheon

Datasheet

SimShield™

BI-DIRECTIONAL FIXED-FORMAT DATA FILTERING AND DISGUISE

FEATURES AND BENEFITS

- **Commercial-off-the-shelf** solution
- **Included** on the U.S. UCDMO Baseline list
- **The only accredited** TENA guard available
- **Provides** fully automated, predictable, controlled and audited two-way communication and sanitization of events across security domains
- **Supports** near real-time cross domain Live, Virtual, and Constructive (LVC) Training with best-in-class performance
- **Enables** the interconnection of RDT&E networks at different sensitivity levels, which moves system tests earlier in the lifecycle
- **Provides** a user-friendly interface for classification filter rule creation
- **Enables** interoperability between previously discrete testing and training activities eliminating redundancies and costs
- **Natively supports** DIS, HLA, TENA, RTP, and MPEG2-TS protocols
- **Allows** object model and/or protocol changes without affecting security posture

Secure Information Sharing for Training and Testing Events

Mission readiness for agents, troops, and equipment is essential to warfighter and national security. Connecting training (live, virtual, and constructive - LVC) and testing environments in a real-world manner – across security boundaries – allows for more effective training activities and more efficient test events resulting in overall cost savings, a better trained warfighter and more thoroughly and quickly tested equipment. Training cost savings are realized through the ability to train multiple groups at the same time, be they different national agencies or multinational forces (for example, U.S. and Coalition). Testing cost savings are realized through earlier detection and correction of issues and errors. For example, an unclassified rail gun can be tested with a ship's classified communications system before the gun is mounted on the ship and is deemed "classified" which reduces the potential for rework and improves implementation time.

SIMSHIELD™

SimShield™ is an accredited commercial-off-the-shelf (COTS) fixed-format data guard with the capability to label, segregate, protect, and exchange data between systems executing at different sensitivity or classification levels. SimShield meets the data format, near real-time performance and low latency requirements for distributed simulation operations, live training exercises, and test events.

In the LVC training environment, SimShield provides secure interoperability across networks at multiple classification levels, which

DATA TYPE OR PROTOCOL	DESCRIPTION
TENA LROM	Test and Training Enabling Architecture Logical Range Object Model Used for live training and testing environments.
HLA FOM	High Level Architecture Federated Object Model Provides the ability to interconnect two or more HLA Federations operating at different security classification levels.
DIS	Distributed Interactive Simulation Typically used for virtual training and simulation.
RTP	Real-Time Transport Protocol
MPEG2-TS	MPEG-2 Transport Stream
MPEG-PES, MPEG-PSI	MPEG Packetized Elementary Stream MPEG Program –Specific Information Stream
MPEG-Video, MPEG-Audio	MPEG Video and Audio Elementary Streams
KLV Metadata	Key-Length-Value

Table 1: Data Types and Protocols

allows the most realistic and beneficial training exercises for U.S. and Coalition troops. The use of SimShield in these exercises enables training assets that operate under different security classification levels to fully communicate and securely interact, creating the most realistic training exercises possible.

In the Research, Development, Test & Evaluation (RDT&E) environment, SimShield allows tests on distributed components to be performed in near real-time and analyzed in a matter of hours. This drastically reduces testing cycle time, which provides large financial benefits. SimShield is listed on the U.S. Unified Cross Domain Management Office (UCDMO) Baseline list as an approved cross domain transfer solution. Because SimShield is an operationally accredited system, the Certification and Accreditation (C&A) process is streamlined for individual installations. SimShield consists of two components: the Policy Editor™ and the Trusted Bridge™ (Figure 1).

POLICY EDITOR™

The Policy Editor is a stand-alone system on which security classification and domain experts build and review re-classification rules that govern the intercommunication between single level networks. The graphical user interface provides for human review and approval in addition to automated system checkpoints to ensure that the rule set is built accurately before being loaded into the Trusted Bridge.

The Policy Editor:

- Supports security domain and data experts in defining classification filtering and sanitization rules between networks communicating through the Trusted Bridge;
- Provides persistent storage for rules and associated reclassification justifications, and;
- Provides an intuitive, user-friendly interface.

TRUSTED BRIDGE™

Trusted Bridge, the SimShield guard component, provides the solution's multilevel security and bi-directional filtering capabilities. The administrator installs and implements the approved Policy Editor rule set on the Trusted Bridge to check the data for type and content. The rule set enforces separate and distinct filter rules before passing, failing, or sanitizing (disguising) the data flowing from high to low and from low to high.

The Trusted Bridge provides a near real-time automated secure two-way data transfer between networks at different security levels in DIS, HLA or TENA environments.
The most important challenge with two-way data transfer is ensuring that classified data is labeled, segregated, and protected to prevent the transfer and disclosure of classified information to a network that is not authorized to access the data.

Data Types and Protocols
SimShield natively supports many data types and protocols for the cross domain transfer of video, audio, and metadata streams concurrently with live and virtual training, simulation, and testing data.

For all protocols and data types, SimShield provides deep format validation, integrity checking, content inspection, and content sanitization at its most granular level of decomposition (i.e., the

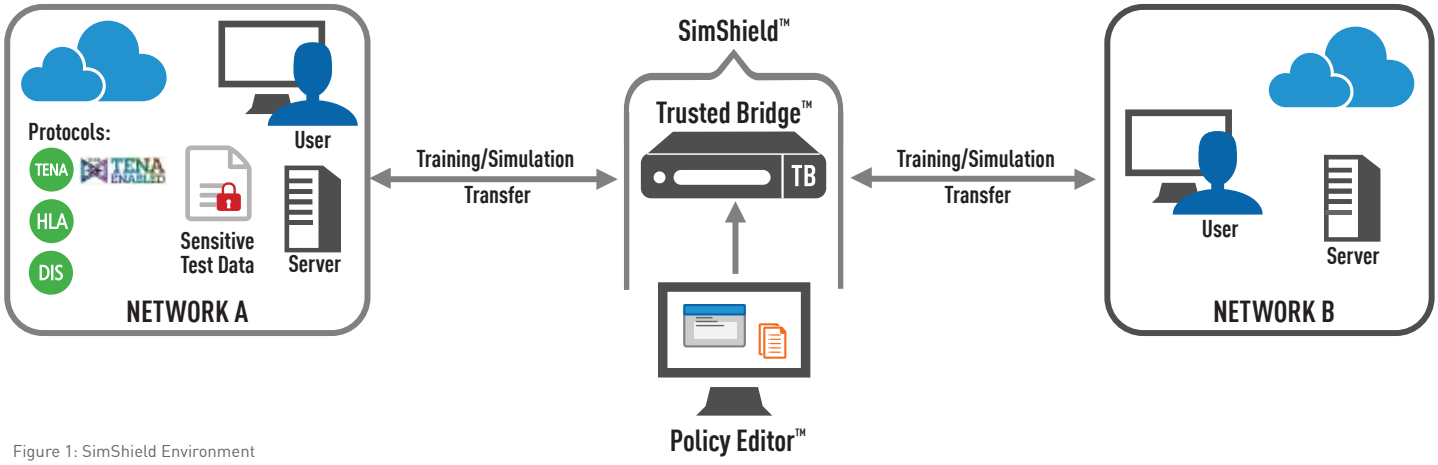

Figure 1: SimShield Environment

content's lowest independently addressable data structure).

ADMINISTRATION AND MANAGEMENT

Logging and Auditing

SimShield provides automatic logging within the Trusted Bridge for user and system activities. When enabled, Trusted Bridge logging is redirected to a remote syslog server at (and only at) the high side.

This capability allows for central logging and archiving. Additionally a logwatcher utility sends administrators email alert notifications and/or displays the alerts on-screen in real time.

Certification and Accreditation (C&A)

SimShield is engineered to satisfy cross domain security requirements for the Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) C&A processes. RTCS products are installed and accredited in operational systems around the world.

SimShield is the only SABI and High Performance Computing Modernization Program Office (HPCMPO) approved TENA guard. SimShield allows for the secure data transfer between the Defense Research and Engineering Network (DREN) and the Secret Defense Research and Engineering Network (SDREN).

"The DREN is a high-speed, high-capacity, low-latency nationwide computer network for computational scientific research, engineering, and testing in support of the DoD's Science and Technology and Test and Evaluation communities. The DREN connects scientists and engineers at the HPCMP's geographically dispersed high performance computing (HPC) user sites."[1]

CONCLUSION

Forcepoint™ develops the most secure, yet flexible, data sharing technologies for military, defense, intelligence, and civilian agencies throughout the U.S., Five-Eyes nations, and NATO member countries. SimShield provides a secure solution to the difficult problem of enabling secure and seamless training and testing across different security classifications. With the most enterprise-wide deployments throughout the world, our proven solutions deliver the right data, to the right people, at the right time to maximize efficiencies and reduce costs. Forcepoint also offers an experienced professional services team to guide customers through the technical implementation and C&A processes.

1 http://en.wikipedia.org/wiki/High_Performance_Computing_Modernization_Program

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

INTERNAL REFERENCE #IIS2013-200 [DATASHEET_SIMSHIELD_EN] 100025FED.011416