EVERFOX

DATASHEET

SimShield

Bi-directional fixed-format data filtering and disguise

Benefits

- Included on the US NCDSMO Baseline list
- First Everfox solution to meet NSA's Raise-The-Bar guidelines
- The only authorized TENA guard available
- Natively supports multiple protocols and data types to include: DIS, HLA, TENA, RTP, and MPEG2-TS
- Enables interoperability between previously discrete testing and training activities, eliminating redundancies and costs
- Supports near real-time cross- domain Live, Virtual, and Constructive (LVC) Training with best-in-class performance
- Provides fully automated, predictable, controlled, and audited two-way communication and event sanitization across security domains
- Provides a standalone user-friendly interface for filter rule creation
- Allows object model and/or protocol changes without affecting security posture

Everfox 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.

Enable multilevel training and testing missions

Connecting training—Live, Virtual, and Constructive (LVC)—and testing environments across security boundaries and in a real-world manner allows for more effective training activities and more efficient test events. The result is 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, whether different national agencies or multinational forces; 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 and deemed "classified," reducing rework and improving implementation time.

Everfox SimShield

Everfox 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. Everfox 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, enabling training assets that operate under different security classification levels to fully communicate and securely interact, creating the most realistic and beneficial training exercises possible.In the Research, Development, Test & Evaluation (RDT&E) environment, Everfox SimShield allows tests on distributed

SimShield Environment

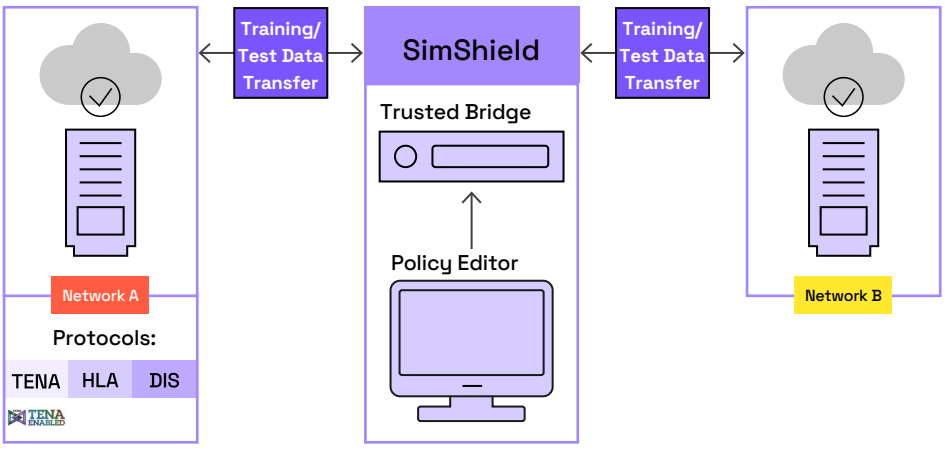


Figure 1: Everfox SimShield Environment

components to be performed in near real time and analyzed in a matter of hours. This drastically reduces testing cycle time, which provides significant financial benefits.

SimShield is listed on the U.S. National Cross Domain Strategy Management Office (NCDSMO) baseline list for Secret and Below Interoperability (SABI) environments and meets current NSA Raise-The-Bar guidelines for an approved cross-domain transfer solution. Because SimShield is an operationally accredited system, the Assessment and Authorization (A&A) process is streamlined for individualinstallations. SimShield consists of two components: Policy Editor and Trusted Bridge (Figure 1).

Everfox Simshield Policy Editor & Trusted Bridge

The Policy Editor is a stand-alone system in which security classification and domain experts define and build classification filtering and sanitization rules that govern the network communications and data flows through the Trusted Bridge. The graphical user interface (GUI) provides for human review and approval, in addition to automated system checkpoints, to ensure the rule set is built accurately and locked down before loading into the Trusted Bridge. Policy Editor also provides persistent storage for rules and associated reclassification justifications for system and security auditing.

The Trusted Bridge is the guard component of SimShield and 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.

Data types and protocols

Everfox 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,Everfox SimShield provides deep format validation, integrity checking, content inspection, and content sanitization at its most granular level of decomposition (i.e., the content's lowest independently addressable data structure).

Administration and management

SimShield architecture divides policy administration tasks and critical data transfer tasks onto separate hardware platforms: Trusted Bridge (guard) and Policy Editor. This separation provides strict security protection on the guard and prohibits filter policy generation on the guard system. Filter policies and rules are defined and generated on the Policy Editor system. A two-person control policy is rigorously enforced when moving the filter policies and rules from the Policy Editor to the Trusted Bridge.

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

System integrity: SimShield uses various mechanisms for file system integrity checking and local configuration monitoring. Integrity validation can occur at any interval as specified by customerpolicy, typically hourly for most critical cross-domain solution files and daily for normal system files.

Data Types & Protocols

Data Type/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 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 exercises
RTP	• Real-Time Transport Protocol • Used for video and audio streaming
MPEG-2 TS	• MPEG-2 Transport Stream • Enables multiplexed video and audio streaming
MPEG-PES, MPEG-PSI	• MPEG Packetized Elementary Stream & MPEG Program-Specific Information Stream • Used in conjunction with MPEG-2 for video and audio data transfer
MPEG-Video, MPEG-Audio	• MPEG Video and MPEG Audio Elementary Streams • Used for video and audio data transfer in basic format
KLV Metadata	• Key-Length-Value • Used for KLV data inspection and security mark check, which might be embedded in the MPEG-2 TS stream

Table 1: Data Types & Protocols

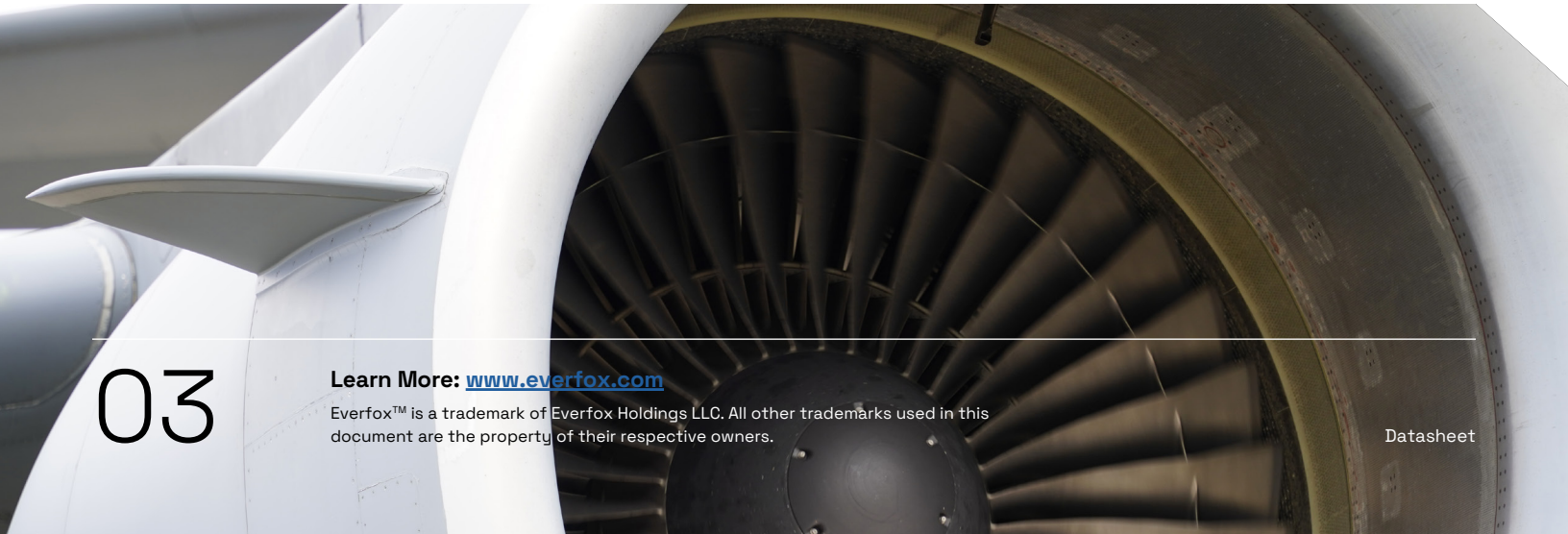
Assessment & Authorization (A&A)

SimShield is engineered to satisfy cross-domain security requirements for the Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) A&A processes to include meeting NSA's RTB guidelines. Everfox 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. This permits SimShield to securely transfer data between the Defense Research and Engineering Network (DREN) and the Secret Defense Research and Engineering Network (SDREN).

Conclusion

Everfox's Cross Domain Solutions have a proven track record of proactively preventing organizations from compromise, while fostering the secure access and transfer of information. This allows agencies to strike the right balance between information protection and information sharing—a vital component to national security.



Learn More: www.everfox.com