EVERFOX

DATASHEET

High Speed Guard

Automated, High-Performance Data Transfer from Enterprise to the Tactical Edge

Benefits

- → Sustains fast transfer rates of more than 9 Gb/s on 10 Gb networks with latencies as low as 1.3ms.
- → Meets the NCDSMO baseline requirements for a CDS since 2001 and is designed to meet current Raise-The-Bar guidelines.
- → Customer maintainable for simplified configuration and management.
- → High Speed Guard SP implementations support tactical and mobile forces and meet SWaP-C requirements.
- → Enables video streaming while providing granular control and auditing.
- → Supports multiple application protocols and adaptability for custom interfaces.
- → Provides highly customizable data validation rules for maximum flexibility.

Rapid Data Transfer for Mission Critical Operations

Intelligence loses value the moment it stops moving. Sensitive data must be santitized and made available to services, agencies, forces, and coalition partners quickly enough to act on, while data collected in austere environments has to reach protected enclaves for processing and analysis. That movement now feeds AI and advanced analytics as well as human decision makers, which raises the volume and tempo at the same time. Doing this between networks at different sensitivity levels has historically been inefficient, ineffective, and insecure. The persistent threat of cyber attack, penetration, and data loss means the path the data travels has ot be trusted, not just fast.

Everfox High Speed Guard & High Speed Guard SP

Everfox High Speed Guard is an integral part of many authorized systems, enabling highly complex, bidirectional, automated data transfers between multiple domains (Figure 1). High Speed Guard and High Speed Guard SP, for special-purpose implementations, support both large enterprise environments and austere environments with specific size, weight, power, and cost (SWaP-C) considerations, with comparatively low administration overhead.

A typical deployment sustains transfer rates of more than 9 gigabits per second (Gb/s) on a commodity server, and High Speed Guard has demonstrated sustained bidirectional transfer rates at this level. The operating system is derived from Red Hat Enterprise Linux with Security Enhanced Linux (SELinux) modules. High Speed Guard is included on the United States National Cross Domain Strategy Management Office (NCDSMO) Baseline list as an approved transfer solution, and because it meets the NCDSMO baseline requirements, the A&A process is streamlined for individual installations.

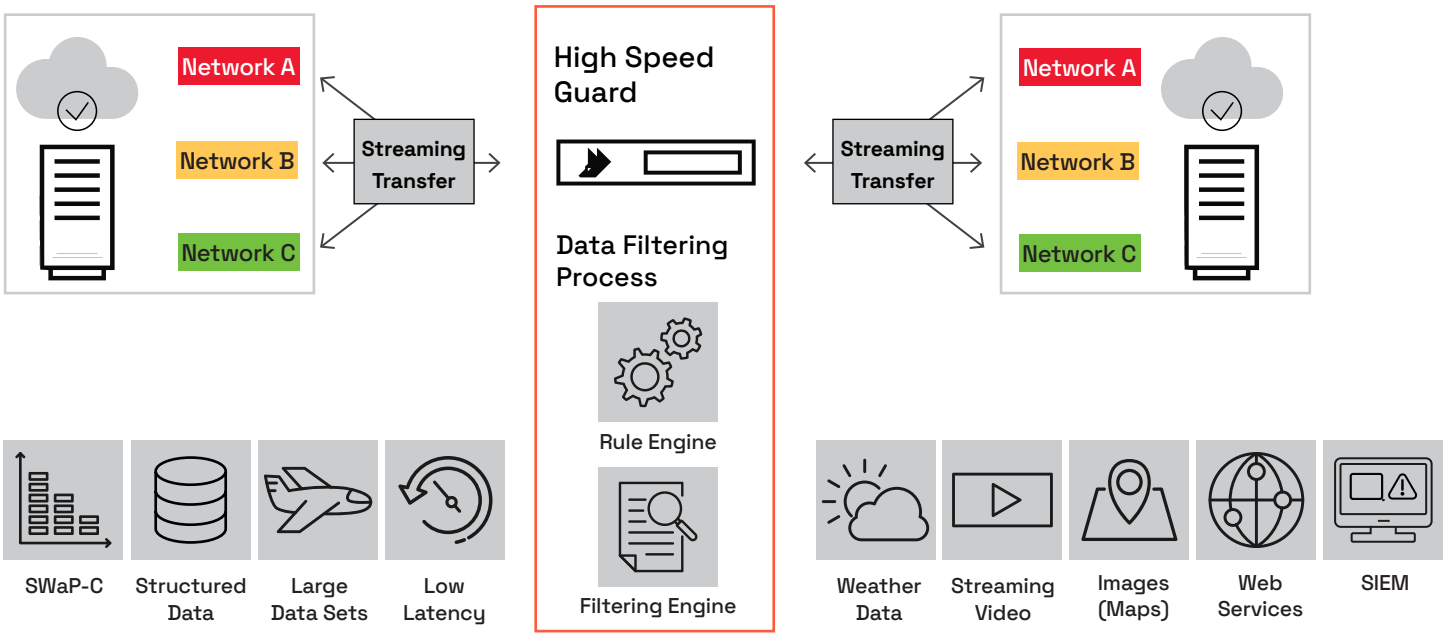

Figure 1: Everfox High Speed Guard Architecture

A Flexible Approach

High Speed Guard supports a wide variety of data transfer scenarios through flexible transfer mechanisms and extensive data support, including web services, streaming MPEG-2 video, imagery in multiple formats, imagery metadata files, inter-system messaging, and a wide variety of proprietary data formats. Numerous transfer mechanisms and a wide array of inspection capabilities together form strong, deployment-specific security policies.

Security Policy Enforcement

High Speed Guard provides built-in redundant filtering delivered by two engines: the Rule Engine and the Filtering Engine. Each provides consistent policy enforcement across all transfer mechanisms. Instead of pre-packaged point-and-click policies, the engines support full customization of inspection capabilities, enabling specific inspections and constraints for each deployment rather than generic controls based on file type. Almost any security policy can be expressed through the engines' user-configurable interface languages, which also allow new data formats to be added without product modification.

Transfer Mechanisms

High Speed Guard transfer mechanisms provide a variety of fixed security protections and secure transfer methods. Everfox works with each customer to determine which mechanisms best support their requirements; many customers run multiple mechanisms on a single system to reduce solution size and cost (Figure 2). Any combination can provide multiple flows through a single system, each independently managed with its own security policy and configuration.

Streaming Video

High Speed Guard provides granular control and auditing of MPEG Transport Stream video, supporting MPEG-2, MPEG-4, and H.264 encodings along with STANAG 4609 (NATO Standardization Agreement) compliant data. Built-in MPEG capability validates that received data is properly formatted, processes multiplexed streams individually, and extracts, audits, and validates key length value (KLV) metadata within the stream, such as classification and release caveats. The mechanism supports unicast and multicast and can send each input to multiple destinations across multiple networks.

Service-Oriented-Architecture Web Services

Using HTTP with or without SSL, High Speed Guard has built-in support for web services and is well suited to SOAP over HTTP. It supports inspection of HTTP headers and a full suite of parsing capabilities for the HTTP payload, with extensive support for data sanitization and re-write, enabling the guard to deliver data that differs from what was submitted. The mechanism automatically parses and validates MIME segments and natively supports SOAP with Attachment (SWA) services.

Adaptable Lightweight Messaging for Ultra-High Data Rates (UDP & TCP)

High Speed Guard supports almost any UDP- or TCP-based protocol, with or without SSL. Many customers use this capability for cross domain transfer of custom protocols, including broadcasts and high-performance Java Messaging Service (JMS) traffic. Messaging latency can be as low as single-digit milliseconds or lower, supporting low-tolerance systems.

High-Performance File Streaming

The Joint Architecture Study Data Transfer Protocol (JAS/DTP), jointly defined by the National Geospatial-Intelligence Agency (NGA) and its mission partners, provides standardized high-performance data dissemination across a wide variety of networks and systems. High Speed Guard supports repeatable transfer rates of over 9 Gb/s with this protocol, ideal where FTP-style delivery is appropriate but higher performance is required.

Cross Domain Simple Network Management Protocol (SNMP)

Cross Domain SNMP provides the means to extend network management across domains. With this capability, enterprise network status can be received by a controlling domain.

Streaming Video	• Provides enhanced security controls for video • Live MPEG video transport streams
SOA Web Services	• Standards-based interoperability through SOAP/HTTP • Cross Domain Web Services
Adaptable Lightweight Messaging (UDP & TCP)	• Custom messaging integration; easy integration into existing TCP/IP, UDP/IP systems • Supports latencies as low as 1.3ms • High-throughput UDP messaging (Xtreme rate UDP)
High-Performance File Streaming (JAS/DTP)	• Ideal for time-sensitive, large payload transfers • USG standard for product transmission
Cross Domain SNMP	• Extending network management across domains • Supports enterprise network management from a controlling domain

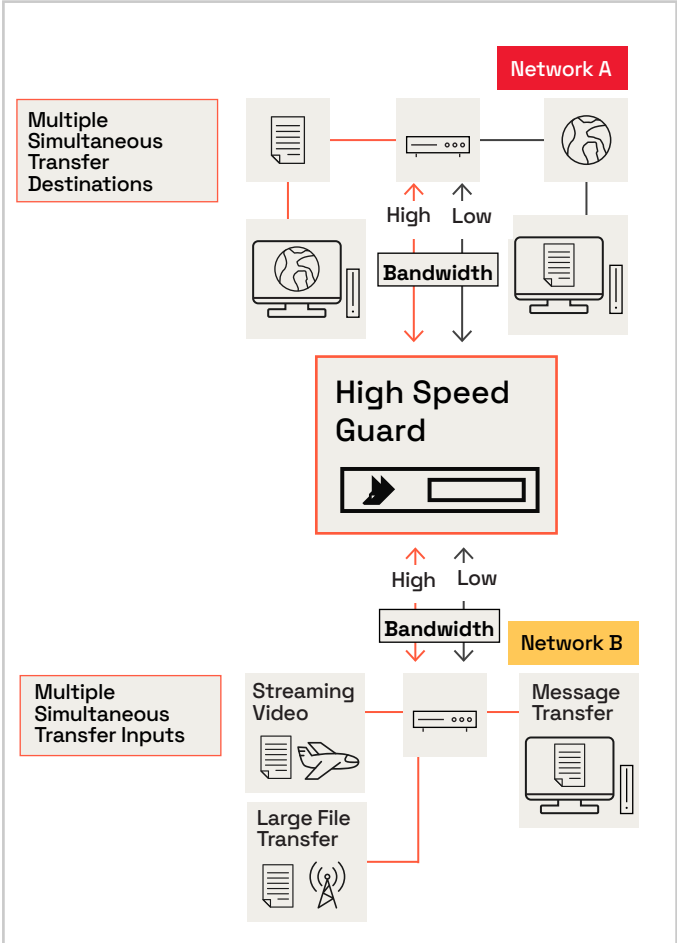

Figure 2: High-Performing file streaming

Automated Secure Transfer (AST)

The AST mechanism provides a standard file "drop box" transfer capability that allows High Speed Guard to monitor external file servers for files to transfer. Using AST, High Speed Guard can monitor and re-create subdirectories, monitor multiple source directories, and transfer to multiple destinations across multiple domains. A unique feature of AST is the ability to send files that fail validation to a specific destination. For example, failed files could be automatically redirected to another guard such as Everfox Trusted Gateway System. High Speed Guard may also redirect failed files to a problem or trouble queue on the source system for further review. AST supports both Secure Copy (SCP) and FTP transfers.

Administration and Management

High Speed Guard architecture divides administrative tasks from critical data transfer tasks on separate hardware platforms. This separation permits the guard to be highly minimized and locked down, while administrators have complete access to the Administration Server for performing functions such as backup, restoration, configuration, logging, auditing, real-time alerting, and administrator account management. A single Administration Server supports 10 or more guards depending on the deployment. Consolidated logging and real-time alerting for the enterprise can be managed from a central area. The Administration Server itself can be accessed directly or remotely, depending on customer configuration requirements.

Logging and Auditing

High Speed Guard is deployed with an audit configuration that meets standard requirements across the cross domain community. Each deployment is enhanced with auditing specific to the data flows and security policies for that deployment. This unique auditing is driven by the Rule and Filter Engines, permitting the security policy to send any data deemed appropriate to the audit trail at any time. High Speed Guard supports local and remote log consolidation of the standard operating system syslog, binary auditing, and data transfer logging. Log and audit data is actively collected, parsed, and reduced for immediate administrator notification of security events and can be sent at line speed to a collection server.

System Integrity

High Speed Guard uses various mechanisms for file system integrity checking and local configuration monitoring. Integrity validation can occur at any interval as specified by customer policy, typically twice a day. Integrity failures result in a full server halt or service termination (i.e., transfer mechanisms are stopped), depending on customer policy.

Configuration Management

Administration Server contains built-in configuration management functionality. The configuration management system preserves a controlled baseline of all High Speed Guard configurations. System modifications are tracked through the configuration manager which runs in a deciated area on the server. Use of configuration management enforces the maintenance of prior configuration versions and ensures strict adherence to two-person integrity controls.

Assessment and Authorization (A&A)

High Speed Guard is engineered to satisfy cross domain security requirements, including current NSA Raise the Bar guidelines. Everfox High Speed Guard is deployed worldwide and is part of systems authorized under Department of Defense (DoD) Risk Management Framework (RMF) IT, ICD 503, and National Institute of Standards and Technology 800-53 and 8500.01/RMF security controls.

Conclusion

Everfox Cross Domain Solutions connect what mission partners cannot otherwise connect, moving intelligence between networks, domains, and allies without exposing either side. High Speed Guard delivers that connection at the speed and volume AI, analtyics, and mission requirements demands, so the data feeding those decisions arrives trusted, and protection and information sharing stop being a tradeoff.

About Everfox

Everfox delivers trusted connectivity to protect the world's most critical environments and safeguard the sensitive data powering decision advantage.

Built for mission - critical operations, Everfox protects what matters most by securing how data moves, how users access it, and how threats are neutralized across every domain. We enable mission speed and secure collaboration across networks, domains, and allies, while ensuring the data powering AI and advanced analytics remains trusted and protected.

We don't just defend systems; we deliver decision dominance.