Forcepoint Enables Secure Sharing of Threat Information

Secure information sharing between entities (agencies, countries, networks)

Publicly Available Information. This document does not contain information (e.g., technical data, technology) that is controlled under U.S. International Traffic in Arms Regulations (ITAR) technical data or Export Administration Regulations (EAR). EXIM Document ID - FIERCE-928.

Forcepoint

forcepoint.com/government

Whitepaper

George Spencer
GSpencer@forcepointgov.com
Senior Capture Manager – Civilian
Global Governments and
Critical Infrastructure

Table of Contents

Introduction

As governments, agencies, and the private sector focus on the need to collaborate and share critical information, protecting and improving how that information is distributed between various secure and sensitive domains becomes paramount. Our customers' most sensitive intelligence must often be sanitized and made accessible to various services, agencies, forces, and coalitions as quickly as possible. Simultaneously, data from a wide variety of sources is transferred to larger protected data center enclaves for processing and analysis. The sharing and movement of this data is essential to the rapid, accurate, and precise execution of our customers' missions. Unfortunately, the persistent threat of cyber-attack, penetration, and data loss requires that only the most secure methods are utilized to enable automated secure information sharing and transfer.

Dissemination of new information needs to carefully balance the need-to-know by consumers with the responsibility-to-share by providers. The right amount of sharing, governed by policies defining what information can cross domain boundaries, when, and under what circumstances, is highly context-dependent and dynamic. Dynamic management of those policies is a key challenge. The result is a high-speed, efficient, cost-effective sharing process for even the most challenging data environments.

Herein, we describe the Forcepoint High Speed Guard (HSG) as a key solution that aligns closely with NIST Special Publication 800-150 for implementing a technical vision enabling automated and collaborative enterprise cyber threat enrichment using HSG secure cross-domain information-sharing capabilities focused on providing the right information to the right stakeholder, at the right time. Thus, we can enhance threat-informed decision-making and enable a more rapid, qualitative security posture.

Threat-sharing environments

Digital transformation has driven unprecedented connectivity throughout government agencies. Users want to work in dynamic applications that reside on premises, in the cloud, or in a hybrid environment. They also expect access to data, including Controlled Unclassified Information (CUI), from anywhere—and from any type of device without frustrating users, overwhelming administrators, or mistaking good actors with bad actors. These challenges also drive the narrowing of defenses from wide network perimeters to NIST's Zero Trust initiative 800-207 (2019). This is in direct response to less controllable enterprise trends which include the vast growth of remote users and cloud-based assets not located within an organization's enterprise-owned/controlled network boundary.

Digital transformation has driven unprecedented connectivity throughout government agencies.

In this new era, it is imperative for the federal government to provide better, more efficient service for its citizens in the most cost-effective, but secure manner. To accomplish such modernization, agencies must rethink traditional cybersecurity approaches. Furthermore, per NIST Special Publication 800-150 "Guide to Cyber Threat Information Sharing" (2016), cyber threat information (i.e. indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents) is vital to the security of government agencies. Forcepoint's automated and integrated risk-mitigation solutions uniquely focus on individuals and their behaviors to better protect access to data, networks, devices, analytics, and applications.

Noteworthy is that programs to coordinate the sharing of threat information within government and public sectors have been established before. For example:

- → **Information Sharing Analysis Centers (ISACS)** provide repositories for gathering cyber threat information relevant to critical infrastructure while also providing two-way information sharing between the private and public sectors.
- → **The Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP)** is a public-private data-sharing and analysis platform that facilitates the timely bi-directional sharing of unclassified and classified threat information among energy sector stakeholders.[1]
- → **The Department of Homeland Security's (DHS) Automated Indicator Sharing Program (AIS)** is a free capability that enables the exchange of cyber threat indicators between the federal government and the private sector at machine speed.[2]

NIST Special Publication 800-150 outlines best practices for cyber threat information sharing and how to establish proper partnerships with stakeholders. These recommendations include: Safeguarding Sensitive Information and Protecting Classified Information.

Cross-domain solutions (CDS) were specifically developed to address these security safeguards, while simultaneously addressing the usability, through cross-domain automation, and the expense and resourcing of hardware duplication challenges that arise from physically separated networks.

Across Civilian Agencies, DoD, and the Intelligence Community (IC), Forcepoint has deployed proven and secure CDS transfer solutions to protect the transfer of federated data across multiple classification levels.

The Forcepoint High Speed Guard (HSG) is a secure transfer solution that solves the difficult problem of satisfying security needs while enhancing the speed and latency of structured information sharing. Forcepoint HSG provides the automated, high-performance transfer of information securely between and within many classification levels. Forcepoint HSG is designed to satisfy the highest information assurance-accrediting community requirements and mitigate potential leaks and risks. All Forcepoint cross-domain solutions have been designed to meet or exceed extensive and rigorous security Certification and Accreditation (C&A) testing by multiple agencies, organizations, and services for simultaneous connections to various networks at different security levels.

Over 1,100 Forcepoint HSGs have been deployed to locations across the globe and the Forcepoint HSG is currently accredited for use within Civilian, DoD, and IC environments. It resides on the National Cross Domain Services Management Office (NCDSMO) "Raise The Bar" (RTB) list of approved CDS for Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI). As a commercial COTS company, these accreditations coupled with Forcepoint's ongoing commitment to NSA's RTB current and future standards, ensures that HSG deployments and accreditations are low-risk, cost-effective, and efficient for our customers.

1 https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf
2 https://www.us-cert.gov/ais

Forcepoint HSG is a multi-level guard solution which enables rapid, bi-directional, automated transfer of highly complex data between multiple domains (Figure 1). HSG supports large enterprise systems with comparatively low administration costs, making it the ideal choice for large-scale deployments that require large-volume, automated data transfers. The Forcepoint HSG delivers the industry's fastest bi-directional transfer rates of more than 9 gigabits per second (Gb/s) with 2ms latency or less and is provided as a Commercial-Off-The-Shelf (COTS) solution. Another of HSG's key features is its customer configurability, which enables simplified operations and maintenance, the elimination of costly and time-consuming manual data transfers, and most importantly, the ability to perform byte-level data inspection on virtually any structured data format.

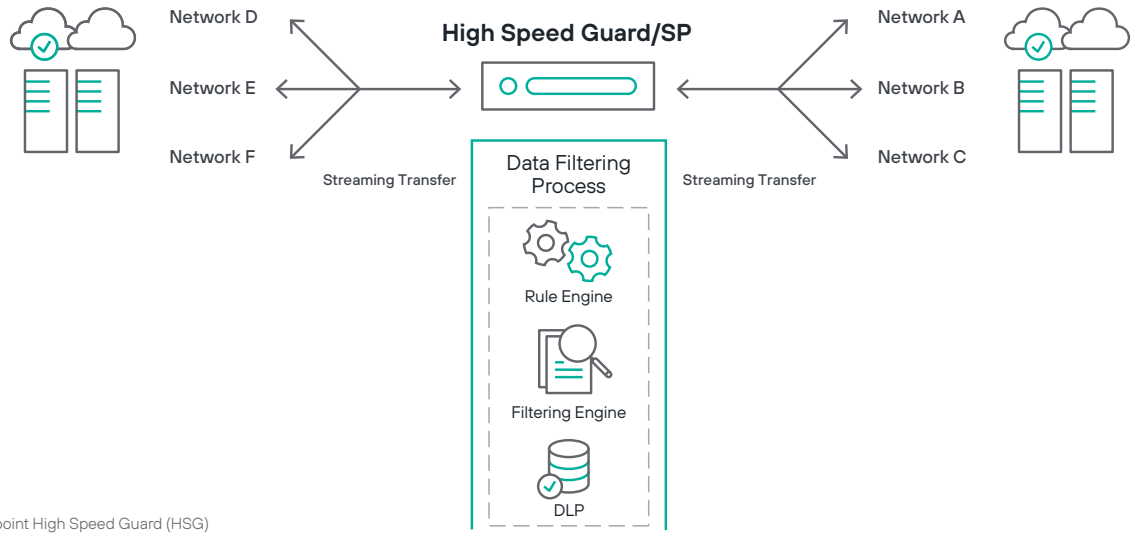

Figure 1: Forcepoint High Speed Guard (HSG)

Furthermore, Forcepoint Data Loss Prevention (DLP) safeguards data from accidental and deliberate actions. Forcepoint's implementation of DLP uniquely enables users to follow data (e.g. controlled unclassified information (CUI), personally identifiable information (PII) and threat information across networks and devices—both at rest and in use while creating and enforcing policies that provision the access and movement of data to prevent data breaches and help ensure compliance. Forcepoint supports current and future efforts of agencies and public entities participating in threat information-sharing environments. Forcepoint implements a combined, Zero Trust-based cross security domain and a DLP solution to better visualize and correlate cross-domain data movement in order to protect information from unauthorized disclosure or modification.

Forcepoint's implementation of DLP uniquely enables users to follow data, personally identifiable information, and threat information across networks and devices.

Table 1 below describes our features and benefits to threat information-sharing environments.

FEATURE	DESCRIPTION	VALUE
Flexible Open Architecture	› Adaptable to wide variety of data types and security policies › Multiple application protocols, adaptable to custom interfaces › Advanced virus scanner for optimized virus inspections that can complete within milliseconds › Highly customizable data validation rules for maximum flexibility	› Configurable for simplified operations and maintenance › Sustains the industry's fastest transfer rates: 9Gb/s on a 2-CPU platform allowing personnel to focus on mission › No impact to current operations given latencies as low as 1.3ms
Transfer Mechanism	› Extensive support for highly complex automated transfer requirements of big data between multiple sensitive networks or clouds › Flexible data inspection engine applies the same rule engine for all data inspections › Bi-directional and unidirectional data flows › Any combination of transfer mechanisms can be used to provide multiple flows through a single system › Large and small payload, time sensitive, and periodic operation	› 22+ security domains, supports many data flows with a single server › Eliminates costly and time-consuming manual data transfers and analysis › Automation of manual processes and reduction of administrative burden improves the capability to expedite information sharing across secure information-sharing programs like CRISP, AIS, etc.
Administration and Management	› HSG architecture divides administrative tasks from critical data transfer tasks on separate hardware platforms › A single Administration Server supports 10 or more guards depending on the deployment › The Administration Server itself can be accessed directly or remotely, depending on customer configuration requirements	› System administrators manage users, set configurations, manage alerts seamlessly › Simplified operations and maintenance › Full on-site control from a single point enables effective management of the technology
Accredited Cross-Domain Solution	› Listed on NCDSMO Baseline since 2010 › Current ATOs: SABI, TSABI, ICD 503, DCID 6/3, etc.	› Minimizes Assessment and Authorization costs/risk and reduces time to achieve IATO and ATO › Enables customer to more easily expand into the SABI environment in future implementation phases with the same technology and user experience

Table 1: Feature and Benefits of the Forcepoint HSG

Figure 2 below describes the Forcepoint Zero Trust Cyber protection layer afforded customers that require cross-domain visualization and analysis of data and the behaviors associated with the use of that data. Hence, transitioning threat information programs to leverage a modern, secure, and cost-effective CDS platform like the HSG is critical to driving information sharing and delivering unique predictive intelligence and analysis to operators and decision-makers at all levels. Forcepoint's HSG effectively and efficiently enables sharing and processing of cyber threat information between the classified and unclassified threat indicator repositories. Further, the ability to bring sensor and other data sources across boundaries will enable the more effective use of classified analytics and data sources to improve information-sharing environments.

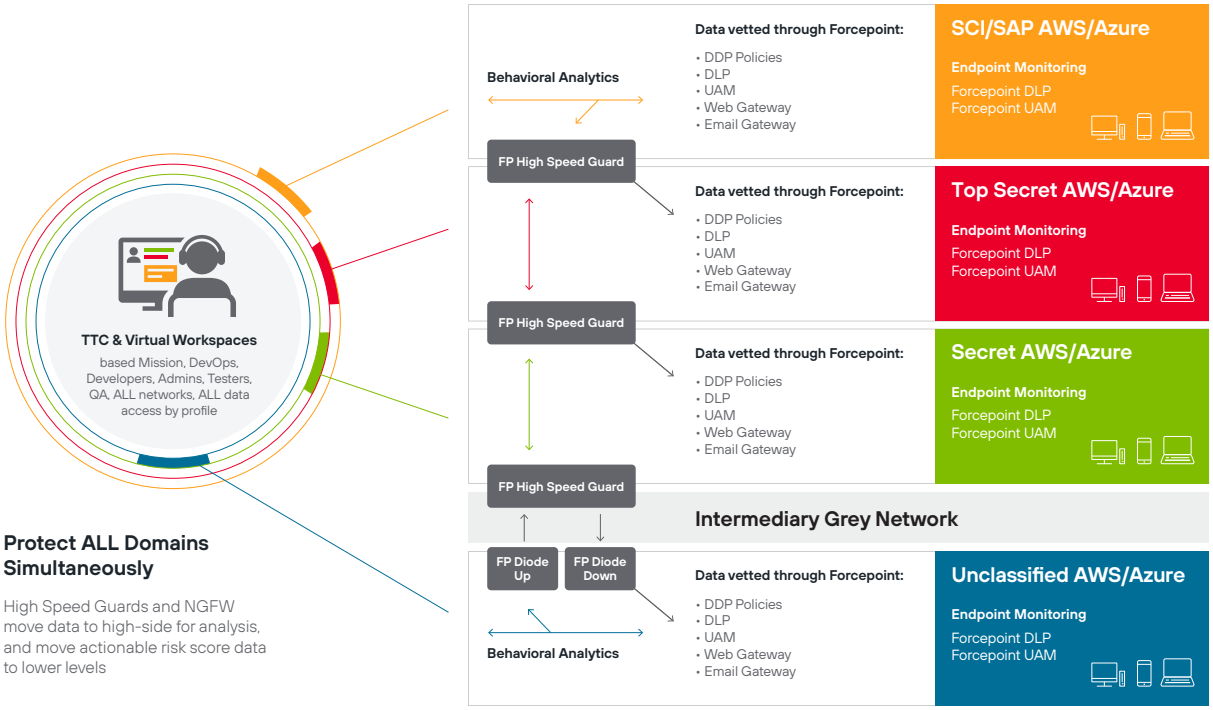

Figure 2: Cross-Domain, Zero Trust Protection

Mapping Cross-Domain Transfer to The Operational Environment

Balancing the protection of data with the mission requirements for information sharing is essential to the threat information mission and commitments to collaborating with government and industry partners. Cyber threat information must be sanitized and made accessible to various services, agencies, forces, and coalitions as quickly as possible. At the same time, data from a wide variety of sources must be transferred to protected enclaves from austere environments for processing and analysis. The sharing and movement of this data is essential to the rapid, accurate, and precise execution of our customers' missions. The persistent threat of cyber-attack, penetration, and data loss requires that only the most secure methods are used to maintain the highest standards of security.

Fortunately, the fundamental combined purposes of cyber data protection and mission information sharing are improved by integrating HSG and DLP together into a Zero Trust-based threat information-sharing environment along with the existing network infrastructure for enabling a scalable, secure, seamless, and interoperable service to automate secure data transfer with the HSG and delivering uncompromising security and usability while addressing data exfiltration.

The Forcepoint HSG contains highly flexible, plain-text rule sets and filters that provide the ability to validate nearly limitless types of structured data. The flexible rule language, combined with the high performance of Forcepoint HSG, allows the consolidation of multiple data flows onto fewer physical systems, which reduces costs, improves efficiency, and reduces the risk to cross-domain vulnerabilities. These rule sets and filters are also adjustable by customers. Forcepoint has trained numerous customers to be self-sufficient on rule set creation and modification. There are currently a number of enterprise HSG deployments where the systems are completely managed by the customer.

Forcepoint's HSG cross-domain solution can be integrated to transfer Structured Threat Information Expression (STIX) data between different security enclaves, domains, or classifications. This integration can be performed using the Trusted Automated eXchange of Indicator Information (TAXII) protocol or via another unique means. The HSG utilizes its standard-based XML inspection and verification engine to validate STIX data and enforce appropriate security policies.

In addition to the technical advancement in capability, several other benefits would be realized, including:

- → **Improved productivity** due to the automation of formerly manual processes leading to cost reduction.
- → **Reduced backlog** of manual transfer approvals.
- → **Redirection of staff** into higher-value and more strategic work as a benefit of eliminating mutual administrative tasks.

Forcepoint ThreatSeeker Intelligence

Forcepoint has expertise in threat information sharing beyond enabling solutions (e.g. Forcepoint HSG, DLP). The Forcepoint ThreatSeeker Intelligence, managed by Forcepoint Security Labs, provides the core collective security intelligence for all Forcepoint security products. It unites more than 900 million endpoints, including inputs from Facebook, and, with Forcepoint Advanced Classification Engine (ACE) security defenses, analyzes up to 5 billion requests per day. This expansive awareness of security threats enables the Forcepoint ThreatSeeker Intelligence to offer real-time security updates that block Advanced Threats, malware, phishing attacks, and lures and scams, while also providing the latest web ratings. The Forcepoint ThreatSeeker Intelligence is unmatched in size and in its use of ACE real-time defenses to analyze collective inputs.

Summary

Forcepoint provides the most comprehensive and widely used collection of multi-level access and cross-domain transfer products available today which strike the right balance between information protection and information sharing. Forcepoint's cross-domain secure information-sharing solutions have a proven track record of proactively preventing government and commercial organizations from being compromised, while fostering the secure access and transfer of information. This allows Forcepoint's cross-domain solutions to strike the right balance between information protection and information sharing—a vital component to national security.

As information systems evolve and are more deeply integrated into mission success, we need to continue to work together to secure our key critical infrastructure systems. Our critical infrastructure of the future will be connected, we know that. We need to also ensure we take the steps to make the systems internationally interoperable, provide information assurance, and leverage their networked environments for resiliency.

Partnerships that help organizations, government agencies, and nations effectively minimize cyber risk to safeguard information and critical infrastructure are paramount. Forcepoint is committed to active participation in this global imperative and to delivering our proven capabilities in secure information-sharing and cybersecurity to meet the current and evolving challenges.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[Forcepoint-Enables-Secure-Sharing-of-Threat-Information-Whitepaper-US-EN] 21May2020