FORCEPOINT

Solution Brief

Is Your Guard Compromising Your Agency's Mission?

Is Your Current Solution Forcing Risky, Non-Compliant Workarounds for Your Team?

Protecting and streamlining how data is distributed between separated networks, is essential to efficient and secure data sharing and collaboration. Sharing and moving data are essential to the rapid, accurate, and precise execution of defense departments, intelligence communities and other federal government 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.

Outdated Solutions Decrease Efficiency, Increase Risk

Your current guard probably meets basic requirements such as supporting flexible data transfer mechanisms (file based, UDP streaming, TCP, HTTPS, et al.) and multiple concurrent data flows; has a substantial data type library; it may even meet the minimum Raise the Bar requirements. But what about video, the ability to make custom rule sets specific to your mission and the ability for end users to set and deploy new data flows in the solution? Lack of these crucial features will lead to your team finding risky workarounds that may not be compliant or timely.

To ensure technology robustness and enable efficiency in your agency, your guard should be able to answer "yes" to the following questions:

- Can it sustain transfer rates of more than 9Gb/s on 10Gb networks with message latencies of less than 10 ms?
- Can it support Raise the Bar-compliant Full Motion Video (FMV) transfers and transcoding?
- Is it Raise the Bar-compliant for imagery (jpg, png, bmp) transcoding?
- Does it have flexible data inspection engines that utilize dynamic Rule Sets to manage security and mission needs?
- Are end users able to deploy new data flows and data type filters without contractor support?
- Does it offer additional support tactical and mobile forces and meet SWAP-C requirements?

Forcepoint High Speed Guard answers "yes" to the questions above. It supports a wide variety of data transfer scenarios through the use of flexible transfer mechanisms and extensive data support. These include web services, real-time Moving Pictures Experts Group (MPEG2) video, transfer imagery of multiple formats, imagery metadata files, inter-system messaging, and a wide variety of proprietary data formats

High Speed Guard delivers the most robust combination of security, flexibility, usability and reduced total cost of ownership. An independent, Forrester study at an intelligence agency customer demonstrated a 389% return on investment (ROI) over a 2 month payback period by significantly increasing data transfer speeds (automating a manual process) and allowing for better use of skilled personnel time.

Forcepoint High Speed Guard

Industry's fastest transfer rates

Sustain the industry's fastest bi-directional data transfer rates of more than 9 GB/s, with latencies as low as 1.3 ms.

Employ a product accredited on NCDSMO Baseline

Included on the U.S. National Cross Domain Strategy Management Office (NCDSMO) Baseline for TSABI & SABI environments since 2001, and designed to meet NSA Raise the Bar guidelines.

Move data in all environments: enterprise to battlefield

High Speed Guard enables most U.S. enterprise cross domain data transfer capabilities; High Speed Guard SP delivers those capabilities to tactical and mobile forces.

Forcepoint High Speed Guard: Secure rapid data transfer between segmented networks

Achieve O&M savings with Commercial Off-the-Shelf (COTS)

- Standard commercial software development and maintenance practices provide savings in operations and maintenance (O&M) over Government-Off-The-Shelf (GOTS).

Eliminate manual processes and re-deploy personnel

- By securely automating manual data transfer and verification tasks, highly skilled personnel can be redeployed to mission-critical tasks.

Reduce admin overhead in multilevel environments

- Streamline alert and monitoring processes (e.g., SIEM) by moving data from lower levels to a single higher level for a full operational picture.

Employ R.A.I.N. principles

- Dual filtering engines and robust security controls ensure that any security critical action is Redundant, Always invoked, Independent, and Non-bypassable (R.A.I.N.).

Enforce robust administration, logging, and auditing

- Separate hardware platforms for critical data transfer tasks (the guard) and administrative tasks (admin server) to enforce strong process and role separation.

forcepoint.com/contact

© 2019 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners
[IS YOUR GUARD COMPROMISING YOUR AGENCY'S MISSON-SOLUTION BRIEF-US-EN] 700027.090619