How to Ensure Inter-Agency Collaboration

Compare capabilities and assure security for multi-level networks with Cross Domain Solutions

Forcepoint

Cross Domain Buyer's Guide

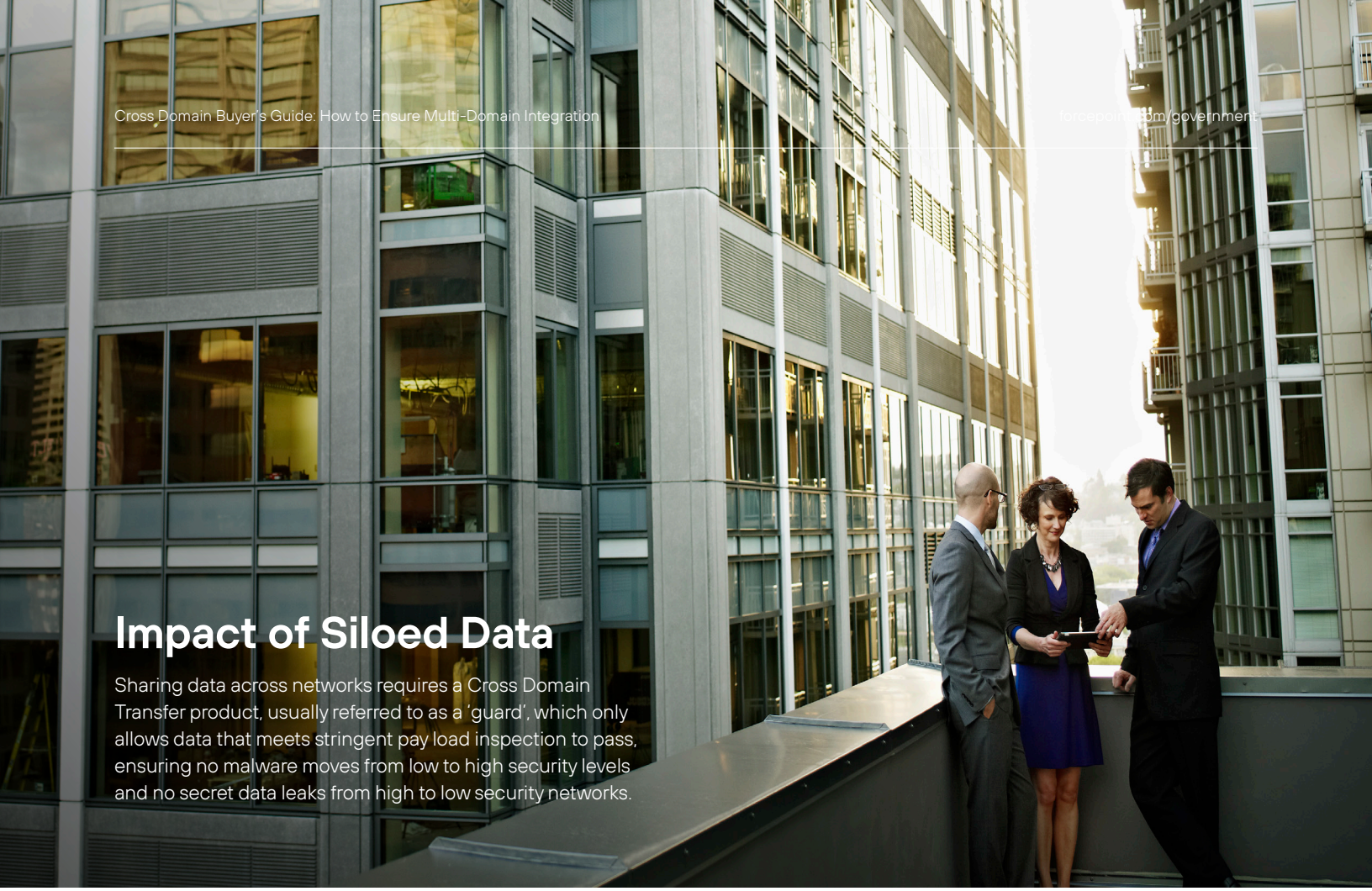
Challenges with the Current Environment

45% of military respondents from a March 2020 Government Business Council (GBC) survey noted siloed data as a challenge to their organization's ability to collect and disseminate data.

Without secure data sharing capabilities across agency networks, some decision making will hinge on an incomplete picture of information.

Challenges in collaboration increased with telework as 25% of federal employees noted a fear of compromised data as a reason for limited remote access in their agencies. For government agencies who transfer data among sites and with other agencies across the globe, it's created a greater gap in the capability for digital collaboration.

Agencies being globally dispersed increases the risk of data leakage during transfer and introduces an enlarged attack surface that agencies need to protect. Often, agencies are left trying to piece together data sharing solutions from multiple providers, which result in scale and performance limitations. They can't meet the capacity or connectivity needs of expanded set of network domains as the organization grows. And they are unable to effectively transfer the types of data at the performance requirements of the agency. The time to fortify and scale security for transferring critical information is now.



Impact of Siloed Data

Sharing data across networks requires a Cross Domain Transfer product, usually referred to as a 'guard', which only allows data that meets stringent pay load inspection to pass, ensuring no malware moves from low to high security levels and no secret data leaks from high to low security networks.

Reduced or stagnated collaboration within and among agencies and partner organizations

Secure access and sharing of data, PII and high-value assets (HVAs) between agencies and mission partner environments (MPEs) is critical to their progress, research, and development. Without the ability to safely and securely transfer data, organizations such as the Department of Energy, Department of Health and Human Services and the Department of Justice cannot succeed. They won't effectively collaborate or they will be forced to stop projects completely.

Critical information misses the window to impact Inter-Agency Collaboration

Inter-Agency Collaboration depend on real-time communications across air, land, sea, and space . They remain key to our military operations and retaining our military advantage.

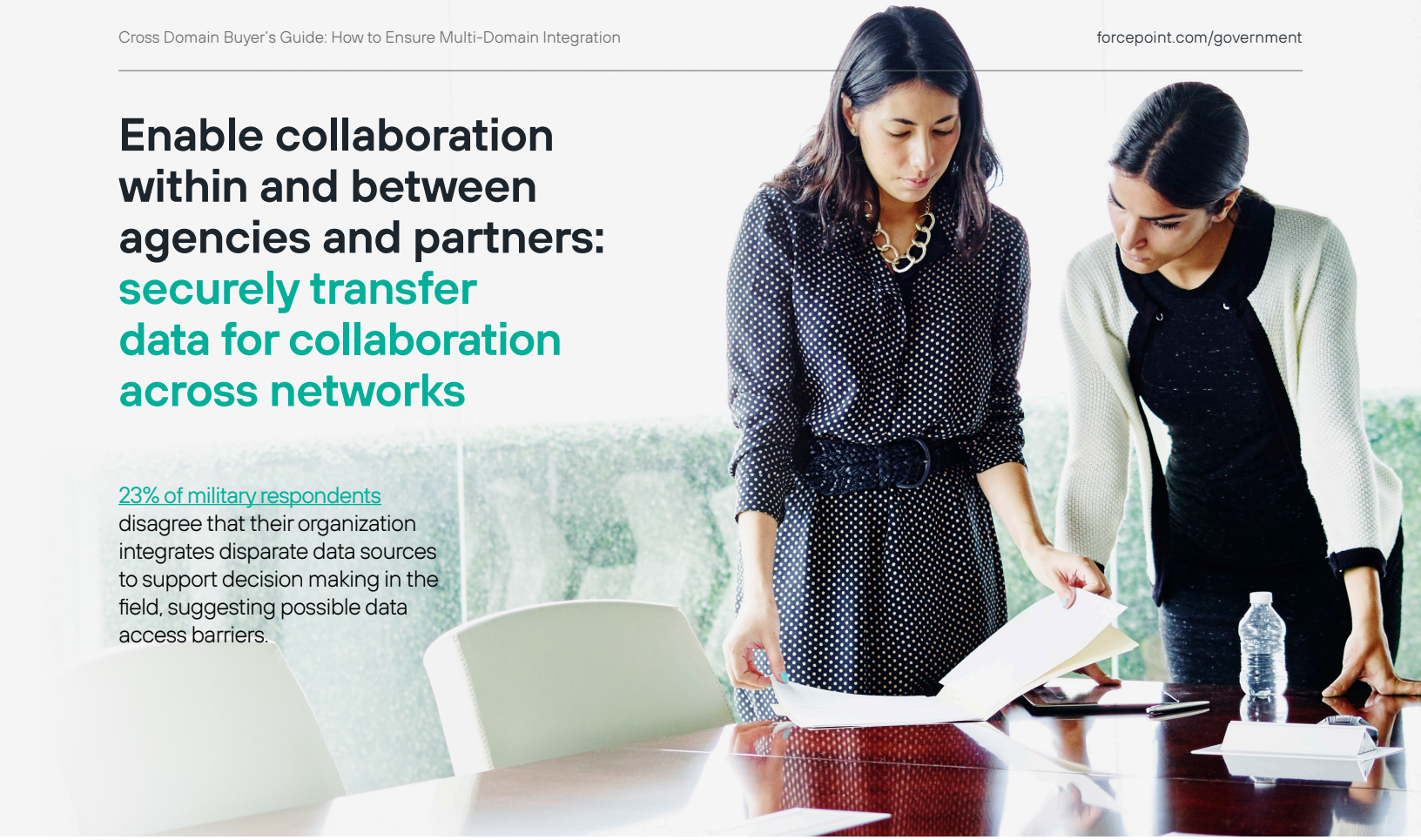
"The interoperability of various, different systems, that's really where we are struggling," said Air Force Brig. Gen. David Kumashiro at a Defense One conference in 2020. Although the DoD is making great strides to improve interoperability, it remains an opportunity for modernization.

Agencies have struggled to allow classified and unclassified data to transmit across domains. For example, until recently, the two most advanced Air Force jets could not transmit data to one another, as these aircraft—the F-35 and F-22—have different data links that lack interoperability to receive and send data to one another securely.

Manual workarounds can introduce new threats

People tend to find new ways to get the job done when experiencing roadblocks, and Sneakernet is no exception. Sneakernet refers to the transfer of data by physically moving media such as USB flash drives or external hard drives between computers, rather than transmitting it over a network. Information transferred from a high threat network (such as the internet) into a controlled or secret network via Sneakernet (or other methods), could introduce malware or malicious code. Pieces of malicious code can be hidden in large files such as images or videos— introducing risk to the next network.

Enable collaboration within and between agencies and partners: securely transfer data for collaboration across networks



23% of military respondents disagree that their organization integrates disparate data sources to support decision making in the field, suggesting possible data access barriers.

To increase agency success, you should find a Cross Domain Solution provider that:

- → Employs the largest staff of highly cleared service professionals to support installation, A&A, and Site Based Security Assessment (SBSA) and can provide training for your team or flexibility to manage the environment for your organization.
- → Enables secure high speed data transfer between segmented networks in all environments: from HQ to tactical edge.
- → Is trusted by the U.S. DoD, IC Community and Civilian Agencies for 20+ years.
- → Is included on the U.S. NCDSMO Baseline for TSABI and SABI environments.
- → Meets NSA Raise the Bar guidelines and testing.
- → Sustains the industry's fastest bi-directional transfer rates (> 9 GB with latency as low as 1.3 ms).

Forcepoint

Chosen by the U.S. Military and the U.S. Government's largest federal systems integrators to support their missions.

Secure global missions efficiently and effectively—any network, anywhere.

Forcepoint offers Cross Domain Transfer solutions including High Speed Guard, Data Diodes, and Trusted Gateway Systems that are purposely built for rapid file transfers, optimized by data type. These solutions provide for multi-directional data movement, customizable inspection capabilities, and best-in-class transfer rates and latency. They allow for robust policy creation, ensuring security while delivering performance.

Beyond that, Forcepoint offers the only endpoint that allows for proper access to multi-domain capabilities as you travel with a Cross Domain Access solution, whether on campus or remote. Any mission, any network, from a single device with Trusted Thin Client and Trusted Thin Client Remote.

As your environment grows and changes based on connecting to additional networks or accessing additional data, Forcepoint offers enterprise level management of your CDS environment with Forcepoint Control Center. Pull and push configuration, view CPU and memory utilization for a clear picture of current capacity, ensuring proper growth with your organization.

All of this is built on the mindshare of the largest group of highly cleared cross domain experts in the world, who can support installation, A&A, and Site Based Security Assessment (SBSA), and provide deployment, implementation, support for accreditation, and training for your organization. With over 20 years of experience in cross domain, -and trusted by the U.S. Military and U.S. Governments largest federal system integrators to support their missions—Forcepoint is the leader in Cross Domain Solutions.

Efficiency and security for segmented network environments

Want to learn more about Cross Domain Solutions?

- → Learn more about Raise the Bar and Forcepoint solutions
- → Find out why Forcepoint is The Leader in Cross Domain
- → Forcepoint Global Government Cybersecurity

Forcepoint Cross Domain Solutions

Forcepoint is the leader in Cross Domain Solutions, with over 20+ years' of experience and the largest workforce of highly cleared cross domain specialists. We are ready to advise for accreditation, and training for your organization.

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 humanly-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.

[Cross-Domain-Buyers-Guide-How-to-Ensure-Inter-Agency-Collaboration-Brochure-EN] 11AUG2021