FORCEPOINT
POWERED BY Raytheon

Datasheet

Cross Domain Solutions for Mobile Forces

PROVIDING STREAMLINED AND SECURE INFORMATION SHARING TO TROOPS ON THE MOVE

FEATURES AND BENEFITS

- **Maximize** security while minimizing footprint
- **Meet requirements** for size, weight, power, and cooling (SWaP-C)
- **Commercial-Off-The-Shelf** (COTS) software solutions that provide industry-proven capabilities
- **All solutions** are included on the UCDMO Baseline list

Cross domain solutions have been used within the Department of Defense and Intelligence Community for decades to foster secure data access and information sharing. Most of these deployments have focused on traditional office environments, such as permanent buildings or stationary outposts. These environments use customary hardware devices (servers, workstations, etc.) that meet their needs perfectly well. However this leaves mobile forces, whether they are ground-based, airborne or afloat, with the burden of finding creative ways to fit these devices into already limited space. This often results in unmanageable conditions, jerry-rigged solutions or simply going without; which can compromise mission assurance.

The move toward thin clients and smaller computing devices, combined with more powerful servers, data centers and cloud computing necessary to harness virtualization technologies, has made it easier to bring cross domain to mobile forces. With the advent of smaller, faster, reliable hardware – thin clients, slim servers, and tablets – cross domain software solutions can be implemented to meet mobile forces' requirements for size, weight, power, and cooling (SWaP-C) while ensuring that information assurance and mission requirements are met.

STREAMLINING DATA ACCESS

No longer does a cross domain access solution require a lot of desktop hardware and wiring that takes up space and increases weight. Whether in an airframe or submarine, space is at a premium. It is not uncommon to find much of this space taken up with computer components; typically one workstation or external hard drive per network – and all the associated wiring and peripherals. Not only does this require a great deal of space, it also results in the operator wasting a lot of time rebooting machines or switching from one workstation to another. Forcepoint Trusted Thin Client can address these issues. Forcepoint Trusted Thin Client is the cross domain enterprise solution of choice for mobile forces needing to access multiple networks while increasing efficiencies. Through a hardware or virtual thin client, operators can access multiple networks at one time – without rebooting or moving from machine to machine. Because Forcepoint Trusted Thin Client does not save any data on the thin client, the device itself remains unclassified when not

in use. There is no risk of data being lost or stolen should the device fall into the wrong hands. Operator productivity is enhanced and administration time is reduced. Forcepoint Trusted Thin Client is renowned as a flexible cross domain solution, able to be tailored to meet a variety of customer requirements and hardware configurations.

FORCEPOINT TRUSTED THIN CLIENT IN ACTION

Bringing Cross Domain Access to a US Air Force Airframe

This US Air Force customer is responsible for evolving the nation's key battlefield intelligence aircraft. Before deploying Forcepoint Trusted Thin Client, each of the three enclaves the operators needed to access required three separate network connections and three separate workstations. All of this equipment made the already limited interior space of the aircraft even more confining. In addition to limited space, there was the issue of limited power and the need for cooling.

The Air Force elected to retrofit the aging operator workstations with Forcepoint Trusted Thin Client. Because Forcepoint Trusted Thin Client is a cross domain solution it allows the aircrew to access every enclave at every operator position within the aircraft. They deployed the Forcepoint Trusted Thin Client Virtual Access Implementation to make use of existing hardware. Forcepoint Trusted Thin Client Virtual Access Implementation has all of the security features and capabilities of the traditional thin client implementation maintaining the requisite network data separation. The thin client software image is installed within a virtual machine through which the user accesses each network via a separate window and there is no cut and paste allowed between the networks. This Air Force customer utilizes existing hardware onboard the aircraft to run Forcepoint Trusted Thin Client, reducing space requirements and cooling and power needs. Eliminating all the extra wiring alone saved approximately 1,700 lbs. of weight – directly contributing to better fuel consumption. The operators are now able to gain secure access to all information necessary to fulfill their mission. By running Forcepoint Trusted Thin Client in a virtual machine, limited space, power use, and cooling requirements onboard the aircraft are no longer the Air Force's biggest concerns. Operator productivity is enhanced and administration time is reduced.

ENHANCING INFORMATION SHARING

Remove the need for "sneaker net" and increase data transfer efficiencies

In many cases, mobile forces' missions are focused on data collection from a variety of sources. Once that data is collected it must be moved and shared between the appropriate recipients – human or machine. This can mean deploying many different transfer solutions for a single type of data depending on the sources and intended destinations for that data.

Forcepoint provides several low-overhead cross domain transfer solutions, or guards, to address the secure information sharing need. All are software-based and can work independently, together or within a Forcepoint Trusted Thin Client environment. Forcepoint High Speed Guard is ideal for filtering and delivering sensor data, including full motion video, at the highest demonstrated industry transfer rate of 9 Gigabits per second. Forcepoint Trusted Gateway System is a web-based application that specializes in releasing or upgrading files, such as Microsoft Office files or images, through a workflow interface that enforces Reliable Two-Person Human Review (where required by policy). WebShield, one of the most widely-used guards throughout the Intelligence Community, provides a secure mechanism for on-demand web search and browse-down to lower level networks, providing transparent protection of the entire network.

FORCEPOINT TRUSTED GATEWAY SYSTEM IN ACTION

Bringing Cross Domain Transfer to tactical, operational, and theater-level commanders and staff

Army commanders require rapid receipt and movement of intelligence information, where and when they need it, to plan and conduct full spectrum operations in counterinsurgency environments and across the full range of military operations. This US Army customer chose Forcepoint Trusted Gateway System to meet this need. Forcepoint Trusted Gateway System is deployed in humvees, with a goal of housing servers in transit cases, to protect information and data created on a high-side network that needs to be securely transferred to a lower domain for use by another agency or organization and vice versa. Forcepoint Trusted Gateway System is also optimized to move large quantities of data or information from a lower level network to a higher level network without human interaction. The bi-directional nature of Forcepoint Trusted Gateway System allows for the transfer of intelligence-related data rapidly between commanders, analysts, and warfighters operating at multiple network levels. Forcepoint Trusted Gateway System ensures that data is available and capable of being operationally integrated, reducing analytical production time. This provides analysts in the field the ability to maintain situational awareness and to disseminate intelligence across the enterprise. Running on servers at the edge, Forcepoint Trusted Gateway System integrates web-based intelligence

architecture with data access which provides analytic centers the means to deliver operational information to and from deployed forces.
For almost two decades, Forcepoint has been at the forefront of the information security industry. Forcepoint develops the most secure, yet flexible, data sharing technologies for military, intelligence, and civilian agencies throughout the US, 5 Eyes nations, and NATO member countries. With the most enterprise-wide deployments throughout the world, our proven solutions deliver the right data, to the right people, at the right time. When protecting sensitive data, choose the global leader – Forcepoint.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

INTERNAL REFERENCE #IIS2012-071 [DATASHEET_CROSS_DOMAIN_MOBILE_FORCES_EN] 100026FED.030117