Enabling Remote Operations on Multiple Network Classifications Using Cross Domain Solutions and CSfC

Forcepoint

TECHNOLOGIES
Accelerating Simplicity

forcepoint.com

Solution Brief

Forcepoint
August 10, 2020
Forcepoint Proprietary

Secure Remote Access to Mission-Critical Data Across Multiple Domains for a Growing Remote Workforce is a Pressing Challenge for Government Agencies

Technical and financial constraints associated with **T**ype 1 hardware encryptors and other traditional remote access solutions **call for a reasonable approach to securing sensitive information**.

In response to these constraints, the National Security Administration (NSA) introduced the Commercial Solutions for Classified (CSfC) program. Once seen as an enabler for a very specific set of mission-focused activities, the CSfC program has grown significantly in relevance as it amplifies the benefits of commercial innovation. Moreover, CSfC solutions enable significant cost savings, the flexibility to complete missions from anywhere, and the ability to move away from difficult and costly hardware encryption implementations.

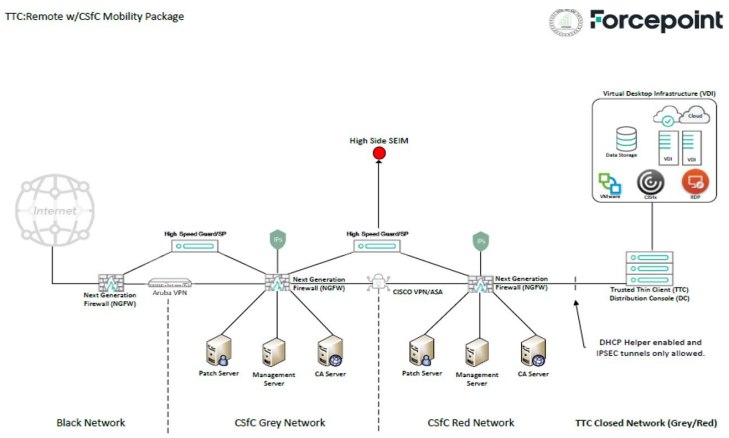
Securing Remote Multi-Network Missions with a Multi-Enclave Remote Workforce Solution (MERWS)

A specifically relevant application of CSfC is in combination with a Cross Domain Solution (CDS). A CSfC-enabled CDS is the optimal choice in meeting the above requirements for providing access to multiple networks through secure, encrypted communications to fundamentally transform remote access to government IT enterprises. Forcepoint and ID Technologies have successfully created a Multi-Enclave Remote Workforce Solution (MERWS). ID Technologies' Archon ZV running Forcepoint's Trusted Thin Client and CSfC mobility access capability package provides a secure multi-network access solution that satisfies security needs while enhancing user productivity, regardless of the user's physical location. With this trusted client solution, an agency allows users to work from home or in the field just as if they were in the office.

Current global conditions have underscored the absolute necessity for multi-domain remote operations, including work from home, to be scaled to the enterprise level for government agencies.

Archon | Forcepoint Multi Enclave Remote Workforce Solution Benefits:

- Supports both hardware- and software-level disk encryption.
- No evidence or trace of data resides on the laptop. All data and work products are saved at the agency's data center, not on the endpoint device.
- Allows secure remote re-key of the entire platform including certificates, retransmission device firmware, and Forcepoint TTC software.
- The Archon laptop is a standard Dell 5410 Ultrabook with a secure RTOS for enhanced security.
- Archon is provisioned at the factory to eliminate provisioning the system onsite.
- The laptop can be treated as Unclassified Data at Rest per NSA CSfC guidelines.
- A true multi-level solution/Virtual Desktop Infrastructure (VDI) solution for enterprise deployment for classified work from home users requiring access to multiple domains.
- Trusted Thin Client endpoint software runs natively as the secure host operating system.
- A standardized CSfC solution designed to support all transport capability packages that is straightforward to register with NSA and accredit internally.



MERWS Enables Mission-Critical Remote Workforces with a Seamless UX, Reduced Costs, and Maximum Security

Forcepoint and ID Technologies' MEWRS meets the needs of agency end users, administrators, and leadership tasked with securing remote access across distributed networks at a low cost while accelerating speed to mission. End users can access mission critical data wherever they are with an office-like experience while having no fear of data compromise if their laptop is misplaced. Administrators experience a seamless extension of the standard Trusted Thin Client software, allowing for easy expansion from a Trusted Thin Client-only environment to also support Workstation users. Leadership can enable secure access to multiple networks while reducing costs by eliminating Type 1 encryption hardware, reaping the benefits of more agile commercial solutions.

These solutions strike the right balance between information protection and information sharing - a vital component to global and national security. They are designed to meet or exceed extensive and rigorous security Assessment & Authorization (A&A) testing for simultaneous connections to various networks at different security levels. Forcepoint and ID Technologies as a Trusted Integrator (TI) offers an experienced Professional Services team to guide customers through the technical implementation, A&A, and the CSfC processes and documentation.

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.

www.idtec.com

About ID Technologies

ID Technologies is dedicated to developing, delivering and integrating forward-thinking, proprietary, reliable solutions to government customers in the Intelligence, Civilian and Federal markets. Trusted with over 20 Government Contracts and partnering with industry leaders and innovators, ID Technologies pairs market leading technologies and supportive acquisition strategies with agility, expertise and mission-understanding to enable government agencies to achieve mission success.

[Title-of-File-USorA4-LanguageCode] [Status]20 Aug. 20