As the boundaries that define the work environment become more pliable – or non-existent – security practices must keep up with this mobility in order to support work flexibility as well as constituent expectations. No longer is it acceptable for agents in the field to wait hours to obtain critical data or for the business of government to halt due to an extreme weather event because they are without access to sensitive networks.

Trusted Thin Client® Remote Access resolves this problem by extending secure multi-network access outside of the traditional physical security perimeter without compromising security. Trusted Thin Client Remote Access utilizes the standard, accredited Trusted Thin Client solution, with additional endpoint and communication security technologies, to permit roaming access from standard-issue laptops and hybrid devices.

**USER EXPERIENCE**

Trusted Thin Client Remote Access is installed directly on the host machine which allows for efficient use of all capabilities inherent in the hardware – video playback acceleration, multiple monitor support, audio, webcams and smart cards.

An authorized user starts the laptop, provides an initial decryption password.
Trusted Thin Client Remote Access

**ADMINISTRATOR EXPERIENCE**

Trusted Thin Client Remote Access is a seamless extension of the standard Trusted Thin Client software, allowing for easy expansion from a Trusted Thin Client Remote Access-only environment to also support thin client and workstation users. This also provides seamless inclusion of Remote Access users within an existing Trusted Thin Client deployment. Forcepoint™ Professional Services will install the appropriate licenses and activate additional features on the Distribution Consoles to support the additional capabilities.

**DEPLOYABLE SECURITY**

Trusted Thin Client Remote Access provides a completely validated boot process that ensures full integrity of the system and runtime environment. Utilizing a process that seals and validates various boot stage and system hashes within the onboard Trusted Platform Module (TPM) allows for an immediate stop to the boot process if a discrepancy is found. Once the boot process completes, the hardware is locked down, including access to the computer’s internal or external hard drives, CD-ROM/RW, other USB or SATA ports, and interfaces – with the exception of the components required to establish secure access to the organization’s networks and any additional networks that the user may need to perform his or her mission or task. Services and applications are tightly controlled.

Trusted Thin Client Remote Access endpoint and communication security meets the National Security Agency (NSA) Commercial Solutions for Classified (CSfC) Mobile Access or multi-site connectivity package guidance for simultaneous access to networks of different sensitivity or classification levels. This solution provides field agents and
other remote workers a means of securely connecting to multiple backend networks or security zones from the field, home office or some other remote location with no risk of data leakage.

A deployed Trusted Thin Client Remote Access instance contains commercial-off-the-shelf (COTS) components, such as Suite B, validated by the CSfC program to be used in layered solutions protecting classified data within National Security Systems (NSS).

These components adhere to two capabilities packages:

- **Mobile Access** - "Meets the demand for mobile data in transit solutions (including Voice and Video) using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as Suite B algorithms, are used to protect classified data using layers of COTS products."

- **Data at Rest** - "Enables customers to implement two independent layers of encryption for the purpose of providing protection for stored information while the End User Device (EUD) is powered off or in an unauthenticated state."

### USE CASE EXAMPLES

#### Ruggedized, Tactical Deployments

The Department of Defense (DoD) has the need to deploy highly mobile computer systems in theater. These systems need to fit in very small areas (such as tanks or other armored vehicles) and be impervious to the elements while providing access to applications and data on multiple networks with varying sensitivity levels.

Without an approved multi-network security solution in place, additional hardware is required. For example, in order for a user to access three different network domains, three endpoint devices and three encryptors are necessary. Each endpoint can only access one network.

To access all required networks, the user must switch from machine to machine. This is highly impractical in-theater and virtually impossible in vehicles with limited space.

When Trusted Thin Client Remote Access is deployed in such environments, the necessary equipment in each vehicle can be reduced by two thirds (including the elimination of encryptors), reducing size, weight, power, and cooling (SWaP-C) costs and overhead. Each endpoint is able to simultaneously access all allowed networks without the need for users to switch between devices.

#### Agents in the Field

Many agencies have employees who work primarily in the field, such as law enforcement and field agents. These employees require secure access to their agency networks from unsecure areas. In the case of covert agents, they require this access to be undetectable.

With Trusted Thin Client Remote Access, agents can work from their standard issue laptop and easily boot the secure Trusted Thin Client workspace. The Trusted Thin Client workspace provides the mechanism to support dual tunnel access (eliminating the need for hardware encryptors), which provides agents access to multiple sensitive networks, applications and data required to fulfill their missions. When the agent shuts down the Trusted Thin Client, no sensitive data is present or accessible. Utilizing Trusted Thin Client Remote Access provides these agents fast, secure and undetectable access to any authorized agency network regardless of location. This decreases their risk of discovery and increases the reliability and accessibility of information gathered and shared.

#### Teleworkers

More and more agencies are preparing to meet the telework mandate. Weather-related events can close offices for a week or more, increasingly longer commutes, rising traffic congestion and the price of fuel all contribute to employees wanting to perform their work duties from home or satellite offices. While this trend delivers many benefits – it also poses significant security challenges. Nowhere is this more pronounced than with federal and civilian government agencies. These workers frequently require access to data that resides on multiple sensitive networks and the risk of having this data resident on laptops is too great.

Trusted Thin Client Remote Access can provide a simple solution to this problem, allowing secure access to an agency’s data center from an agency-provided laptop. From the data center, workers gain access to all authorized networks required to do their jobs. They can now work from any location without fear of data compromise or data loss. All data and work products are saved on the appropriate network at the agency’s data center, not on the endpoint device.

---

CONCLUSION
Trusted Thin Client Remote Access is a secure multi-network access solution that solves the difficult problem of satisfying security needs while enhancing user productivity regardless of the user’s physical location. Trusted Thin Client Remote Access is the same client software that is designed to satisfy information assurance accrediting community requirements, eliminate potential leaks and risks, and provide users with a familiar Windows® desktop environment. Trusted Thin Client is included on the United States Unified Cross Domain Services Management Office (UCDSMO) Baseline list. Forcepoint 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. These solutions strike the right balance between information protection and information sharing—a vital component to global and national security. And 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 offers an experienced professional services team to guide customers through the technical implementation and A&A processes.

ABOUT FORCEPOINT
Forcepoint™ Federal is a trademark of Forcepoint LLC. Trusted Thin Client® is a registered trademark of Forcepoint Federal LLC. SureView®, ThreatSeeker® and TRITON® are registered trademarks of Forcepoint LLC. Raytheon is a registered trademark of Raytheon Company. All other trademarks and registered trademarks are property of their respective owners.

INTERNAL REFERENCE #FFP-B2016-109 [DATASHEET_TRUSTED_THIN_CLIENT_REMOTE_EN] 100051FED.061716

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.