Secure Telework for Mission Critical Resources

Trusted Thin Client Remote

Single-level remote access deployed in days with easy transition to multi-level

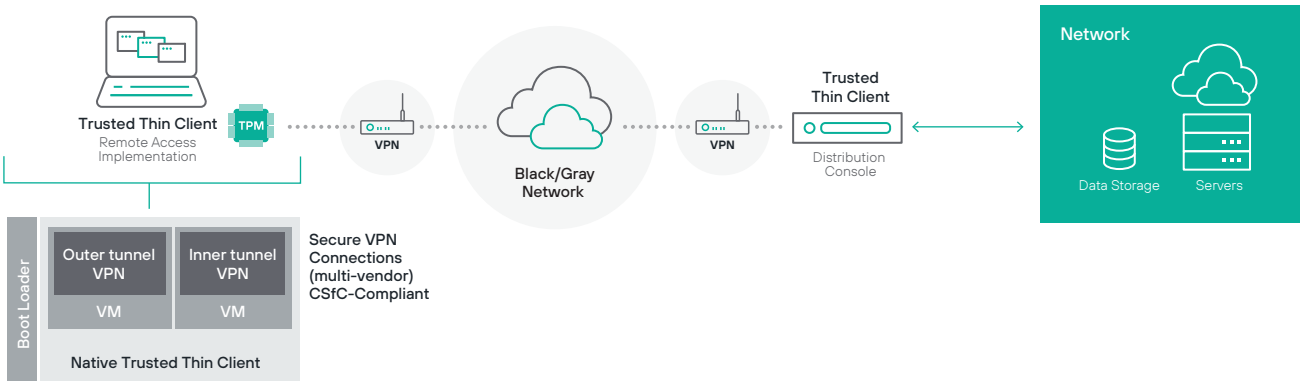
Agencies today face the immediate challenge of enabling secure, remote access to mission-critical resources. Trusted Thin Client Remote (TTC-R) provides a simple solution to this challenge, allowing secure access to an agency's data center from laptops and hybrid devices.

Telecommuting office 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, allowing for the use of clients on any authorized network from home, the field, or anywhere there is connectivity to a mission network. Leveraging CSfC capabilities, single-level network connectivity can allow for rapid operationalization (within weeks) of remote access to classified networks without long accreditation time required on multi-level networks, but allowing for that accreditation at a later time.

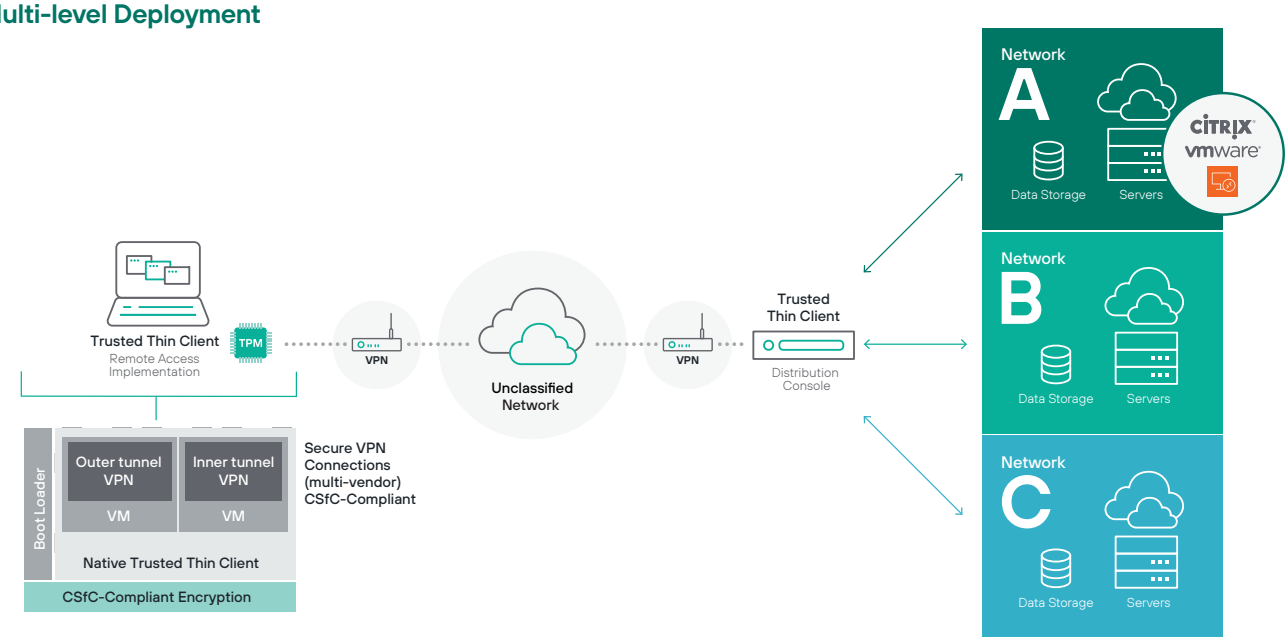
Trusted Thin Client Remote is a CSfC solution that can have your people up and running remote within days. Disconnected communications won't slow your organization down - keep smart card authenticaion, access applications, work with local content and work offline - sync data when connection is re-established, without losing work.

KEY BENEFITS AND FEATURES	
Work Offline with no loss of work	Sync when communications reconnects
Deploy within weeks	Supports both hardware- and software-level disk encryption
No evidence or trace of data resides on the laptop. All data and work products saved at the agency's data center, not on the endpoint device	Performs tamper-proof hardware verification
Deploy single-level (e.g., Secret) leveraging current CSfC stacks	Allows secure remote updates of TTC Remote software
Uses CSfC-approved dual VPN communication stack encryption	Supports all Trusted Thin Client applications, capabilities, and security of accessories including webcams, smart-cards, and unified communications
Utilizes Forcepoint's registered NGFW Commercial Solutions for Classified (CSfC) solution	Supports flexible Linux or Windows outer and inner tunnel VPN client deployment options
Unclassified at rest	Uses off-the-shelf (approved/qualified) laptop and hybrid devices
No SABI or TSABI accreditation required	Future support for simultaneous access to multiple classification levels, leveraging the same infrastructure
Easy transition to a true multi-level solution/ Virtual Desktop Infrastructure solution for enterprise deployment at any time	Trusted Thin Client endpoint software runs natively as the secure host operating system

Single-level Deployment



Multi-level Deployment



User experience

Trusted Thin Client Remote 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 to allow hardware-based system integrity validation, and initiates secure VPN connections to their organization. He or she then authenticates to the data, applications, and networks that reside solely in the organization's data center. (Refer to the Trusted Thin Client datasheet for more details.) Trusted Thin Client Remote protects the data and ensures that **no evidence or trace of data resides on the laptop.** If the device is lost or stolen, no evidence of the client software or secure connection methods are present on the device or hard drive and no data can be compromised. This allows for the access of classified data on systems in hotels, homes, etc. with a significantly reduced risk posture. Should government employees not have access to their traditional workplace, TTC-R can provide similar single- or multi-level access from their remote work environments.

Administrator experience

Trusted Thin Client Remote is a seamless extension of the standard Trusted Thin Client software, allowing for easy expansion from a Trusted Thin Client Remote-only environment to also support thin client and workstation users. This also provides seamless inclusion of Remote 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 ensures full system and runtime integrity by utilizing the onboard Trusted Platform Module (TPM). Trusted Thin Client Remote security features tightly control all the services and applications and lock down the hardware, including access to the computer's internal or external hard drives, optical drives, other USB or SATA ports, and interfaces. Trusted Thin Client Remote endpoint and communication security meets the National Security Agency (NSA) Commercial Solutions for Classified (CSfC).

A deployed Trusted Thin Client Remote instance contains commercial-off-the-shelf (COTS) components, validated by the CSfC program to be used in layered solutions protecting classified data within National Security Systems (NSS).[1] TTC-R supports MACP in multiple configurations, including in combination with the DARCP, or in a Thin EUD implementation, depending on security requirements defined by the Authorizing Official. It adheres to Mobile access requirements and "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.[2]

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 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, 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. If agent endpoint loses communication connection, they can work locally, syncing at reconnection, with no loss of work. Utilizing Trusted Thin Client Remote 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

It has become imperative that agencies meet the telework mandate. Weather-related and national emergency events can close offices for a week or more, while 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 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 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 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 National Cross Domain Strategy Management Office (NCDSMO)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.

1 Commercial Solutions for Classified Handbook version 3.0 November, 2017 https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/csfc-customer-handbook.pdf
2 Mobile Access Capability Package, version 1.1; 19 June 2018 https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/capability-packages/MACPv2_1.pdf

Forcepoint

forcepoint.com/contact