Remote location. When booting a laptop from a USB memory stick, for example, an authorized user initiates a secure VPN connection (through protected, unchangeable means) to their organization. He or she then authenticates through the client to the data, applications, and networks that reside solely in the organization’s data center.

Trusted Thin Client Remote Access protects the data and ensures that no evidence or trace of data resides on the laptop or memory stick. 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 solution provides field agents and other remote workers a means of securely connecting to multiple backend networks or security zones with no risk of data leakage.

Implementation Management
Trusted Thin Client Remote Access is a seamless extension of the standard Trusted Thin Client software. This allows for ease of inclusion within an existing Trusted Thin Client deployment and new Trusted Thin Client Remote Access-only environments. Raytheon Professional Services installs the appropriate license, activates additional features on the Distribution Consoles, and installs a Provisioning Server.

The Provisioning Server is a separate Linux* machine or bootable drive that runs the Raytheon-provided provisioning software. The Provisioning Server is used to format and create the end user’s delivery device endpoint (external or internal drives, USB devices, etc.), registers the endpoints and works in conjunction with the Distribution Console security policies.

Deployable Security
Trusted Thin Client Remote Access is designed to lock down the user’s hardware and disallow 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.

Encrypted USB Memory Stick or SD Memory Card
USB memory sticks and SD memory cards provide access to the organization’s approved desktop image and multiple networks from most any available x86-based device with USB media boot capability.

Laptop, Netbook, Ruggedized Device, or x86-based Tablet
For organizations that provide mobile devices to users and do not want to use USB media, the client image can be installed directly on the device in replacement of the standard operating system.

Complementary Security Mechanisms
Trusted Thin Client Remote Access can be configured to leverage an organization’s PGP encryption protocols or hardware-based encryption for additional protections to meet Federal Information Processing Standard (FIPS) 140-2 (level 1 and level 3 respectively).
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 a cross domain solution in place, access to multiple networks requires additional hardware. For example, in order for two users to access three different network domains, six endpoint devices and three encryptors are necessary. Each endpoint can only access one network. To access all required networks, users 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 the Size, Weight, Power, and Cooling (SWaP-C) costs and Cooling (SWaP-C) costs and reducing the Size, Weight Power, and Cooling (SWaP-C). This reduces the cost of ownership, improves mission readiness, and enhances user productivity.

Trusted Thin Client is supported on tactical ruggedized systems that meet or exceed the relevant specifications from MIL-STD-810G for environmental conditions, MIL-STD-461E for EMI/EMC conditions and MIL-STD-1275D for operating with direct current (DC) vehicle power.

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 insecure 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 normal laptop and easily boot into the secure Trusted Thin Client workspace. The Trusted Thin Client workspace provides the mechanism to support dual Suite B tunnel access (eliminating the need for hardware encryptors), which provides agents access to multiple sensitive networks, applications and data required to fulfill their mission. When the agent shuts down the Trusted Thin Client workspace the laptop returns to its original state from which the standard operating system can be started. 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, longer and longer commutes, increasing traffic, and the price of fuel all contribute to more and more 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 a home computer or 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.

Conclusion

Trusted Thin Client Remote Access is a secure 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 desktop environment. Trusted Thin Client is included on the United States Unified Cross Domain Services Management Office (UCDSMO) Baseline list. Because Trusted Thin Client Remote Access is delivered on an encrypted bootable USB memory stick, SD memory card, embedded hard drive, or SSD, it provides users with simultaneous access to any number of secure networks, at different classification levels from any location.

Raytheon’s 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. This allows Raytheon’s secure access and transfer solutions to strike the right balance between information protection and information sharing — a vital component to global and national security. Raytheon’s secure information sharing solutions are designed to meet or exceed extensive and rigorous security C&A testing for simultaneous connections to various networks at different security levels. Raytheon offers an experienced professional services team to guide customers through the technical implementation and C&A processes.

For further information contact:

Intelligence, Information and Services
Cyber Products
12950 Worldgate Drive, Suite 600
Herndon, Virginia
20170 USA
866.230.1307
www.raytheon.com/cyberproducts