FORCEPOINT
POWERED BY Raytheon

Datasheet

Trusted Thin Client®

SECURE ENTERPRISE ACCESS TO MULTIPLE DOMAINS FROM A SINGLE CONNECTION POINT

FEATURES AND BENEFITS

- **Accredited** and evaluated by authorities in the US (SABI, TSABI, ICD503) and Five-Eyes nations
- **Commercial-Off-The-Shelf** (COTS) solution
- **Simultaneous** access to multiple domains from a single terminal and wire
- **Significant ROI** through reductions in infrastructure, hardware, office space, power consumption, and administration
- **Increased** user productivity
- **Multiple** implementation options: thin client, thick client (repurposed PCs), virtual (Type 1 and Type 2 hypervisors), and mobile (laptops and tablets)
- **Streamlines** administration through robust enterprise management capabilities, while increasing enterprise and data security
- **Supports** a wide array of hardware; agnostic for both servers and endpoints
- **Redisplay** technology agnostic (Citrix®, Microsoft®, Virtual Bridges™, VMware®); supports numerous peripherals
- **Supports** the use of Common Access Card (CAC), smartcard, SAC card, and SIPRtoken for identity management and access authorization to back end Microsoft® Windows® servers.
- **Collaboration** technology support including, webcam redirection through Citrix HDX RealTime Optimization Pack for Microsoft Lync
- **Supports** Suite B cryptographic algorithms for all encrypted communications on the client network
- **Supports** lower resource-intensive office automation applications and high performance graphic-intensive analytical applications

SECURE ACCESS TO SENSITIVE DATA, APPLICATIONS, AND NETWORKS

Entities throughout governments, intelligence communities, departments and ministries of defense, law enforcement, and industry have the need to ensure security, trusted collaboration, mission and enterprise agility and scalability, while also reducing costs. No longer is it acceptable to maintain data and intelligence in singular stove pipes; information must be shared between national entities (public and private) and between national, coalition, and allied partners in order to protect citizens and systems from threats large and small. Secure information sharing – getting the right data to the right people at the right time – involves permitting a diverse user population “need-to-know” access to an increasing amount of sensitive data frequently maintained on disparate networks. The most efficient way to support these enterprises and users is to provide secure simultaneous access to all authorized networks from a single endpoint with streamlined administration. Only one comprehensive suite of access solutions delivers robust security, flexibility and reduced total cost of ownership – Trusted Thin Client® from Forcepoint™.

TRUSTED THIN CLIENT

Trusted Thin Client is comprised of two components, a Distribution Console and thin client software. The Distribution Console is the solution’s server component and provides the physical connection to one or more single level networks, maintaining separation between each.

The Distribution Console requires the Common Criteria evaluated (EAL4+) Red Hat®

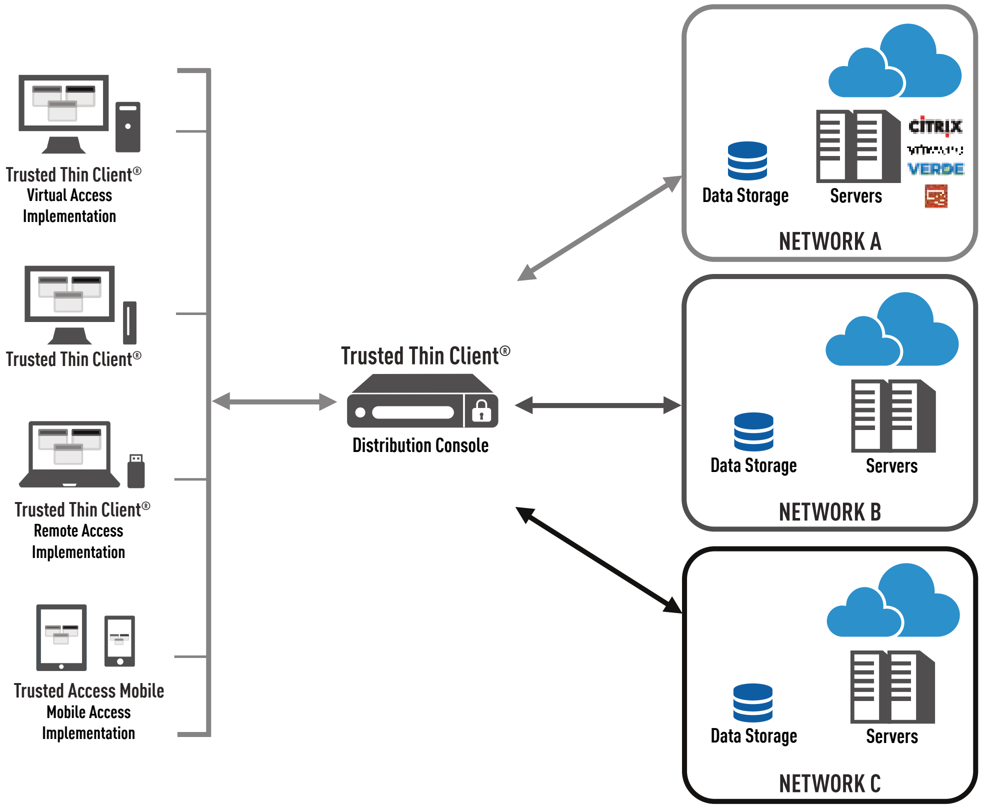


Figure 1: Trusted Thin Client Architecture

Enterprise Linux® operating system with Security-Enhanced Linux (SELinux) to provide stringent security controls and maintain the necessary network/data separation. The client software communicates directly with the Distribution Console and provides secure, simultaneous access to permitted networks, applications, and data. While providing connectivity to multiple security domains through common virtualization and desktop and application redisplay technologies (e.g., Citrix®, Microsoft®, Virtual Bridges™, VMware®), each network has a separate physical network interface connection on the Distribution Console that is assigned the classification level of the domain. Security protections prevent data from being transferred between classification levels. The Distribution Console silently rejects all communications from unauthorized systems, reducing risk exposure to the enterprise.

Trusted Thin Client has a proven positive return on investment through the elimination of desktop hardware, reduced power consumption, decreased administration, increased user productivity, reduced infrastructure and reclaimed office space.

BUILT FOR THE ENTERPRISE

Designed and built to meet the needs of any enterprise deployment, Trusted Thin Client is the most secure yet flexible access solution available today, providing robust centralized management for multiple form factors, globally dispersed sites and thousands of users. Administrators are equipped with centralized administration and monitoring, scalability to easily add networks and clients, and the flexibility to enable access to users in offices, in-theater, and in the field from virtually any device.

CENTRAL ADMINISTRATION AND MONITORING

The Distribution Console is the solution's administration and monitoring hub. All Distribution Consoles, endpoints and users are administered through the solution's Management Console and administrators can monitor Distribution Console and endpoint performance (locate or remote) through the Performance Monitor.

Additionally, the Distribution Consoles serve as a centralized audit repository for the client software to track use and activity. This audit data can also be pushed to a centralized enterprise audit storage location.

THE MANAGEMENT CONSOLE

The Management Console is used to establish and maintain licensing, users, authorized clients, the client network and virtual local area network (VLAN), and desktop and application redisplay services. The Management Console provides the ability to administer any Distribution Console from any other Distribution Console in the enterprise from a single location, greatly reducing the need for on-site resources and the cost to transport administrators from site to site.

It is recommended that all deployments utilize multiple Distribution Consoles to address server outages, scheduled maintenance and unexpected hardware failures. Through the Management Console, administrators configure clients to failover to redundant Distribution Consoles when necessary, allowing work to continue unabated. Depending on environmental needs, the failover configuration can include the ability for clients to failover to off-site Distribution Consoles.

PERFORMANCE MONITORING

The Performance Monitor option, when enabled, allows the Distribution Console to send environment performance information (Distribution Console and clients) to a separate server. This option is designed to collect generic system information (network usage, drive space, memory) as well as Trusted Thin Client-specific information such as number of users logged in and the session security levels being accessed.

Administrators can retrieve snapshots of the environment state and historical data through third-party tools such as HP® OpenView.

CLIENT USER MANAGEMENT

The Distribution Console provides all necessary configuration information for client initialization and communication services. This information contains relevant security data and allows the user to access the backend environments. When a network at another security level or a new backend server is added to the Distribution Console, the information is automatically sent to each client, removing the need to locally manage or update individual clients.

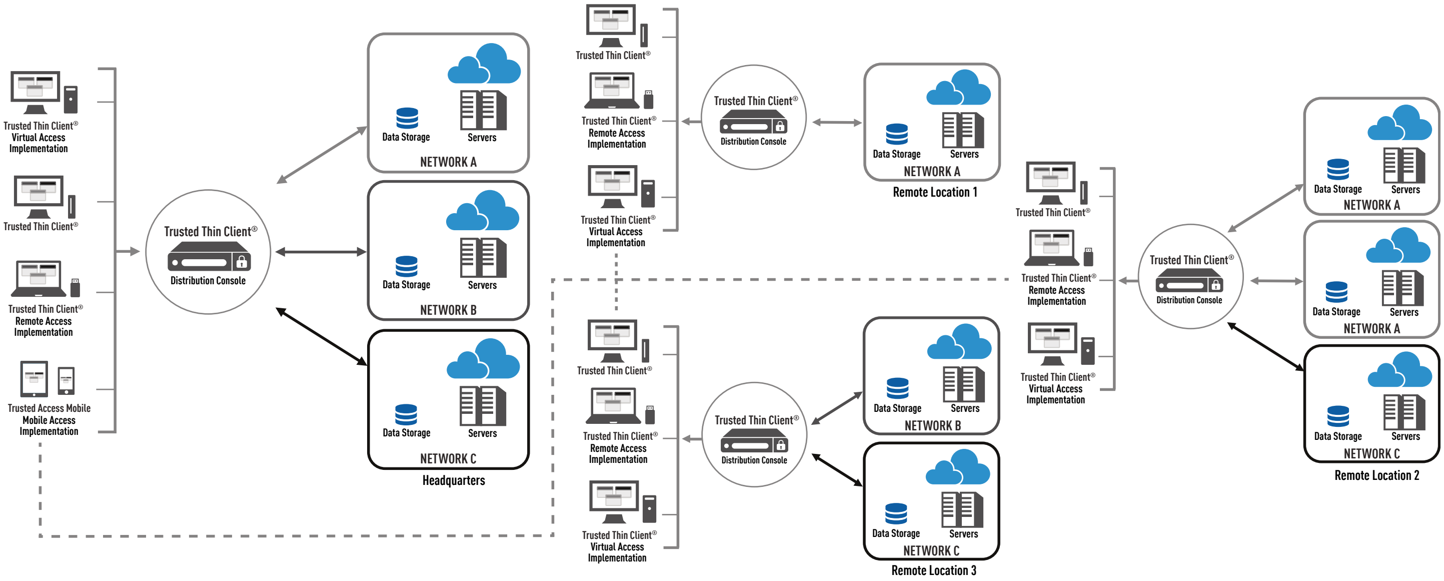
User access controls (username, password, and clearance level) are validated by the Distribution Console through either hosted Lightweight Directory Access Protocol (LDAP), external high-side LDAP, or external high-side Microsoft Active Directory®. Utilizing a pre-existing LDAP or Active Directory server eliminates the need to manage user accounts on the Distribution Console, thus reducing administrative overhead.

SUPPORT FOR MULTIPLE ENDPOINT TYPES

In support of the variety of missions and users that make up an enterprise, the same client software can be implemented on different form factors: thin client hardware, repurposed PCs and laptops, a virtual machine resident on a host operating system, a bootable encrypted memory stick (or other approved removable device), and mobile devices. All recommended hardware is certified in-house by Forcepoint engineers.

All endpoint form factors run a read-only, stateless, SELinux multilevel secure (MLS) operating system that meets the most stringent certification,

Figure 2: Trusted Thin Client Distribution Console Spanning


Trusted Thin Client® Virtual Access Implementation
Trusted Thin Client®
Trusted Thin Client® Remote Access Implementation
Trusted Access Mobile Mobile Access Implementation
Trusted Thin Client® Distribution Console
Data Storage
Servers
NETWORK A
NETWORK B
NETWORK C
Headquarters
Remote Location 1
Remote Location 2
Remote Location 3

accreditation, and evaluation requirements. Users interact with the security-enabled and labeled (visual and code-based) graphical windowing system, which provides immediate access to simultaneous presentation-layer clients (Citrix, Microsoft, VMware, Virtual Bridges) at one or more sensitivity levels on one or more monitors (generally up to 8, portrait, landscape, and touchscreen). The windowing system also provides for client-side rendering of various streaming multimedia protocols enabling an unsurpassed distributed computing experience. Through the client, users can obtain support for different peripherals including: card readers, USB headsets, microphones, webcams, printers, scanners, and multi-head monitor displays.

Over 80,000 users worldwide

Risk exposure is greatly reduced as no user data is stored on the client and there is no risk of downloading or executing malware. Due to the strict network and virtual desktop session separation, and the fact that Trusted Thin Client only provides a redisplay of data from the data center, no malicious code can move from one network to another greatly reducing the risk to the overall infrastructure. Other similar solutions introduce additional risk because of the possibility that end points can access any data on multiple networks and those networks have access to anything on the host operating system.

Additionally, if a foreign or unapproved device is introduced to the client network, there is no mechanism for that device to retrieve a session from the Distribution Console because of Access Control List (ACL) verification. The system is completely controlled and isolated through the enforcement provided by the trusted operating systems on which the client and Distribution Console run and through the use of digital certificates.

CERTIFICATION AND ACCREDITATION (C&A)

Trusted Thin Client is recognized by the US Unified Cross Domain Services Management Office (UCDSMO) and is included on the UCDSMO Baseline List. Trusted Thin Client is designed and developed to meet or exceed Intelligence Directive (ICD) 503 up to the highest Protection Profiles for securing the most sensitive information. Trusted Thin Client has been accredited and evaluated by authorities in the US (Top Secret/SCI and Below Interoperability (TSABI), Secret and Below Interoperability (SABI), and National Institute of Standards & Technology (NIST) 800-53 requirements) and Five-Eyes nations.

CONCLUSION

Forcepoint'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 Forcepoint'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. Trusted Thin Client solves the difficult problem of satisfying security needs while enhancing user productivity. It provides users with secure simultaneous access to any number of sensitive networks through a single device, in support of an enterprise-ready trusted collaboration experience that brings people, data, security, policy, and governance into alignment.

Trusted Thin Client is designed to satisfy the information assurance accrediting community requirements, eliminate potential leaks and risks, and provide users with a familiar desktop environment. Forcepoint'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. Forcepoint offers an experienced professional services team to guide customers through the technical implementation and C&A processes.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

INTERNAL REFERENCE #IIS2014-098 [DATASHEET_TRUSTED_THIN_CLIENT_EN] 100020FED.011416