Cross Domain Security

Trusted Thin Client

Secure enterprise information access to multiple domains from a single device

Key Benefits

- Assessed and Authorized by authorities according to NIST guidelines in the US and Five-Eyes nations
- Supports DoD and IC VDI initiatives such as DoD Joint Information Environment (JIE): Mission Partner Environment (MPE)
- Commercial-Off-The-Shelf (COTS) solution
- Simultaneous access to multiple networks/clouds from a single endpoint
- Significant ROI through lower ownership costs (infrastructure, office space, power consumption and administration)
- Maximized security, usability and adaptability
- Flexible implementation options to meet the needs of your organization
- Streamlined administration through robust enterprise management capabilities
- Redisplay technology integration with industry standards such as Citrix
- Supports the use of Personal Identity Certificate (PIV), Common Access Card (CAC), SAC and SIPRtoken smartcards for identity management and access authorization to back end Microsoft Windows servers
- Supports Suite B cryptographic algorithms for all encrypted communications on the client network

Enabling secure access to sensitive data, applications, and networks

Government agencies know better than most how pervasive and costly (in lives, trust and money) cyberattacks and breaches can be. One basic method of defense is to ensure complete compartmentalization and data separation through physically separate network architectures. This security best practice is commonly referred to as "network segmentation."

While network segmentation does not ensure that hackers "stay out" it keeps them in one place should they breach the perimeter. Damage is therefore contained and only one domino can possibly "fall," not five, ten or 20,000. This is the essence of successful cyber risk management and resiliency."

As agencies have discovered, working in this secure-by-design environment has also led to high costs (hardware, power, and administration) and usability and endpoint security burdens by requiring one computer per network for each user.

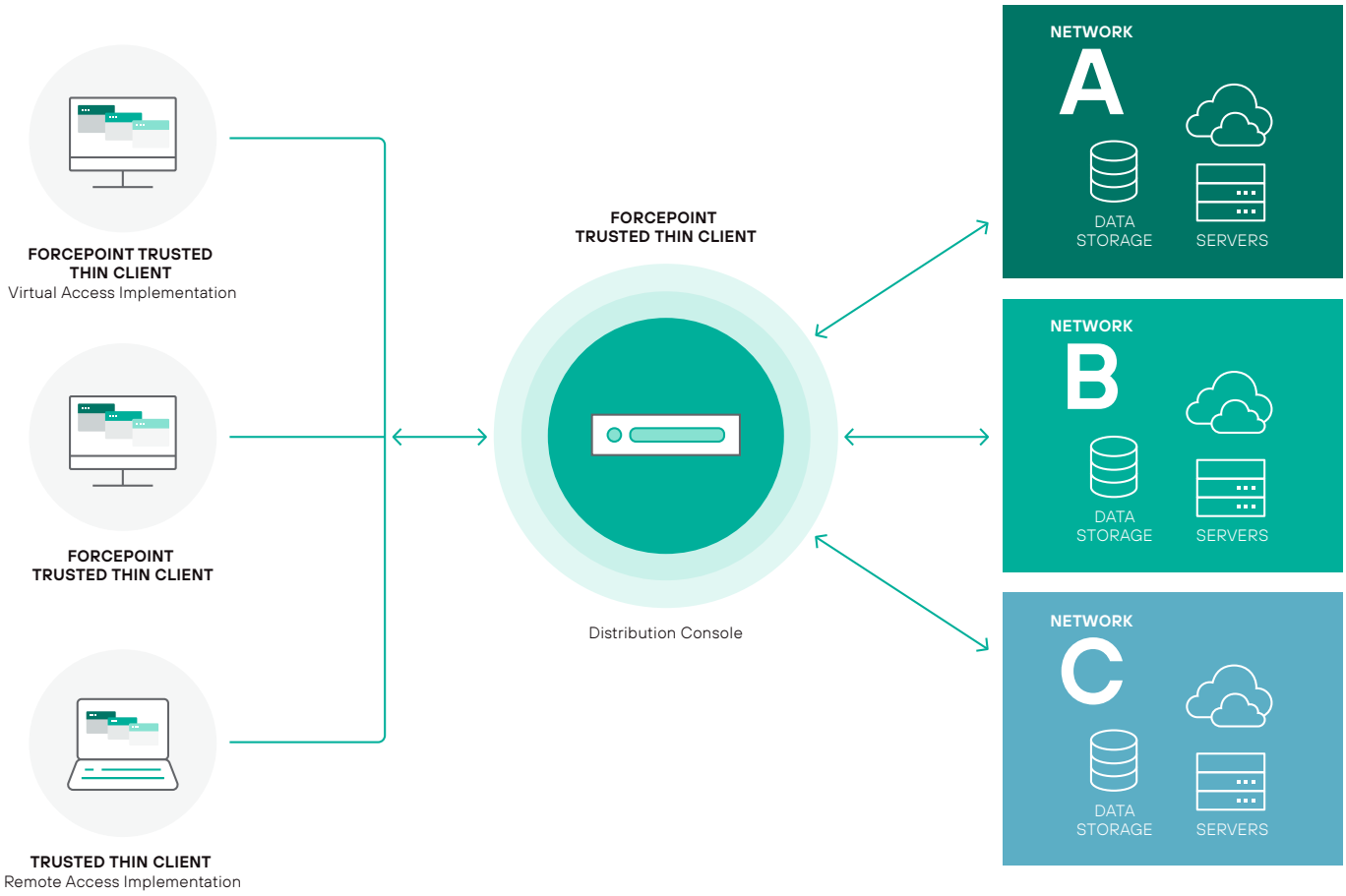
This is no longer the case. Due to the increased adoption of virtualization to move desktop, application and data resources back into the datacenter and increase operating system security and physical separation can be maintained while permitting secure simultaneous access to allowed networks from a secure endpoint device. Forcepoint Trusted Thin Client, delivers the most robust combination of security, flexibility, usability and reduced total cost of ownership available to enable secure access to multiple sensitive networks.

Forcepoint Trusted Thin Client

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

The Distribution Console leverages the Common Criteria evaluated (EAL4+) Red Hat 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, VMware), each network has a separate physical network interface connection on the Distribution Console that is assigned the classification level of the domain.

Forcepoint Trusted Thin Client Architecture



Security protections prevent data from being transferred between classification levels. The Distribution Console rejects all communications from unauthorized systems, reducing risk exposure to the enterprise.

Built for the enterprise

Designed and built to meet the needs of any enterprise deployment, Forcepoint 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.

Restricted, high-risk installation environments

Environments that provide connection to high-risk networks, such as unclassified networks or the open Internet, are required to operate in a restricted manner. To enforce this requirement, Forcepoint Trusted Thin Client installation is modular based on your environment. Restricted, high-risk environments are installed with some features removed. (Table 1).

Central administration, monitoring and auditing

The Distribution Console is the solution's administration and monitoring hub from which all Distribution Consoles, endpoints and users are administered through the Management Console application. It is recommended that all deployments utilize multiple Distribution Consoles to address server outages, scheduled maintenance and unexpected hardware failures.

FEATURE	SABI AVAILABILITY		TSABI AVAILABILITY	
USB Peripheral Redirection (thumb drive, optical reader/ writer, printer, scanner)	✕		✓	Forcepoint's multi-network access technology: Trusted Thin Client, is currently in operation across a multitude of federal agencies including the DOD, DOJ, and IC with over 160,000 access devices deployed around the globe. It has proven deployments of over 60 classification levels and the ability to easily add more classification levels and endpoints at anytime. All IT resources, including endpoint updates are easily managed through a central management console.
Video Playback through Multimedia Redirection (optimized) and Media Player application	✕	*Video playback is available through Windows VDI sessions	✓	
HDX RealTime Optimization Pack for Lync - Skype for Business	✕	*Skype for Business is available through Windows VDI sessions, non-optimized	✓	
Remote Distribution Console Administration via Private, Administration Network	✕		✓	

Table 1: Features removed from SABI environments

Through the Management Console, administrators can administer any Distribution Console from any other Distribution Console in the enterprise—greatly reducing the need for on-site resources and the cost to transport administrators from site to site. Administrators configure clients to failover to redundant Distribution Consoles (on- or off-site) when necessary, allowing work to continue unabated.

The Distribution Console serves as a centralized audit repository for the client software to track use and activity. This audit data can be pushed to a centralized enterprise audit storage location.

Administrator role and account separation

Additional security controls are provided through granular administrator role and account separation. Each account is permitted only one role on the system, thus enforcing the requirement that multiple personnel provide checks and balances for privileged actions, system changes and system data access.

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 virtual environments. When a network at another security level or a new 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, further reducing administrative overhead.

Support for multiple endpoint devices

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, PCs, laptop and hybrid devices, or a virtual machine resident on a host operating system. All recommended hardware is certified in-house by Forcepoint engineers.

All endpoint devices run a read-only, stateless, SELinux multi-level secure (MLS) operating system that meets the most stringent security 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) at one or more sensitivity levels on one or more monitors (up to 8, portrait and landscape orientation).

Risk exposure is greatly reduced due to the read-only device, strict network and virtual desktop session separation, and the fact that Forcepoint Trusted Thin Client only provides a redisplay of data from the data center. Should malicious code make its way to a virtual desktop, these factors prevent it from moving from one network to another greatly reducing the risk to the overall infrastructure.

With DC spanning you can connect to anywhere in the world, from anywhere in the world. For example, personnel located in in Virgina can connect to a network in Korea. See Figure 2. Multi-Enterprise Spanning Architecture (MESA) enables agency owners, or sub agencies to create and share independent private/coalition enclaves across the enterprise with enhanced security and capability for C2 actions.

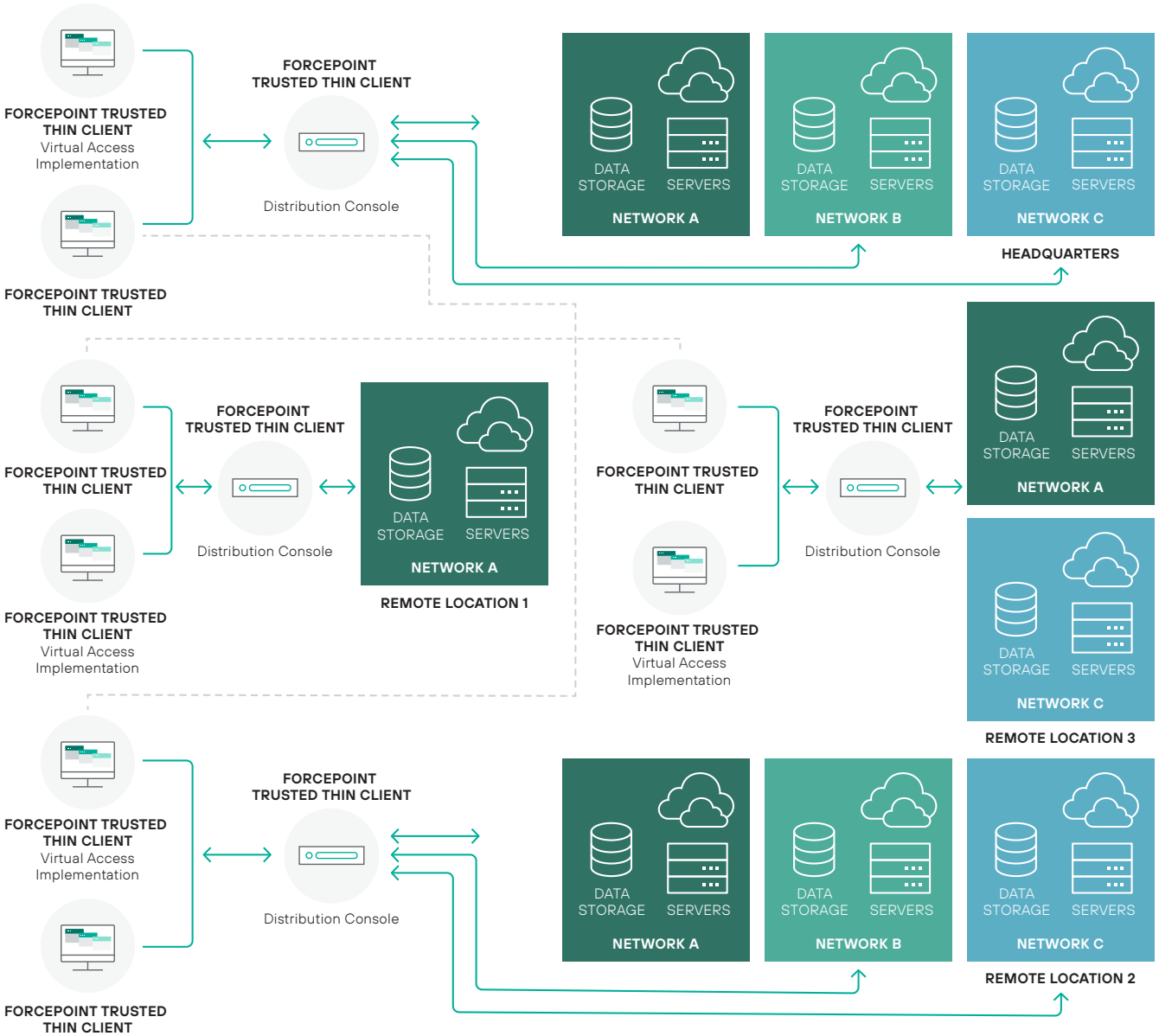


Figure 2: Forcepoint Trusted Thin Client Distribution Console Spanning

Additionally, if a foreign or unapproved device is introduced to the client network, that device is prevented from communicating with the Distribution Console. The system is completely controlled and protected through the enforcement provided by the trusted operating systems on which the client and Distribution Console run and through the use of digital certificates.

Assessment and Authorization (A&A)

Forcepoint Trusted Thin Client is recognized by the National Cross Domain Strategy Management Office (NCDSMO) and is included on the NCDSMO Baseline List. Forcepoint Trusted Thin Client is designed and developed to meet or exceed National Institute of Standards & Technology (NIST) 800-53 and 800-37 (SP), the Committee for National Security Systems (CNSS) Instruction 1253 requirements, and the Risk Management Framework (RMF) as required by Intelligence Community Directive (ICD) 503 and Department of Defense (DoD) IT for securing the most sensitive information. Forcepoint Trusted Thin Client has been assessed and authorized by authorities in the US – Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI)–and Five Eyes nations.

Conclusion

Forcepoint's cross domain multi-level solutions have a proven track record of proactively preventing enterprises from compromise, while enabling collaboration through secure information access and transfer. 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. Forcepoint 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.

Forcepoint Trusted Thin Client is designed to satisfy information assurance requirements, eliminate potential leaks and risks, and provide users with a familiar desktop environment. Forcepoint's multi-network access technology: Trusted Thin Client, is currently in operation across a multitude of federal agencies including the DOD, DOJ, and IC with over 160,000 access devices deployed around the globe. It has proven deployments of over 60 classification levels and the ability to easily add more classification levels and endpoints at anytime. All IT resources, including endpoint updates are easily managed through a central management console. Forcepoint's cross domain multi-level solutions are designed to meet or exceed extensive and rigorous security 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.

forcepoint.com/contact

Forcepoint

[Trusted-Thin-Client-Datasheet-EN] 27Jan2021