EVERFOX

DATASHEET

Trusted Thin Client

Cross Domain Security: Secure enterprise information access to multiple domains from a single device

Benefits

- Evaluated against Raise-The-Bar standards and is a NCDSMO baselined solution
- Supports DoD and IC VDI initiatives such as DoD Joint Information Environment (JIE): Mission Partner Environment (MPE)
- Commercial-Off-The-Shelf (COTS) solution for maximum security, usability and adaptability
- Simultaneous access to multiple networks/clouds from a single endpoint
- Significant ROI through lower ownership costs (infrastructure, office space, power consumption and administration)
- Fully scalable solution that can connect over 100 networks and over 100,000 clients
- Streamlined administration through robust enterprise management capabilities
- Cloud ready system with Azure Virtual Desktop capability
- 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) cyber attacks 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 adversaries "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), usability and endpoint security burdens by requiring one computer per network per user.

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

Everfox Trusted Thin Client

Everfox 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 client 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 application technologies (e.g., Citrix, Microsoft and VMware), each network has a separate physical network interface connection on the Distribution Console assigned the classification level of the domain.

Everfox Distribution Console and Client software is a customized software op-erating system based on Red Hat En-terprise Linux with Security-Enhanced Linux (SELinux) to provide stringent security controls and maintain the necessary network/data separation. Our software is evaluated in lab-based assessment against the most rigorous security standards in the industry - Raise-The-Bar - and our product is on the National Cross Domain Manage-ment Office (NCDSMO) baseline list.

Security protections prevent data from being transferred between classi-fication levels. The Distribution Console rejects all communications from unau-thorized systems, reducing exposure risk to the enterprise. Data from these networks is never stored on the clients themselves, further reducing risk.

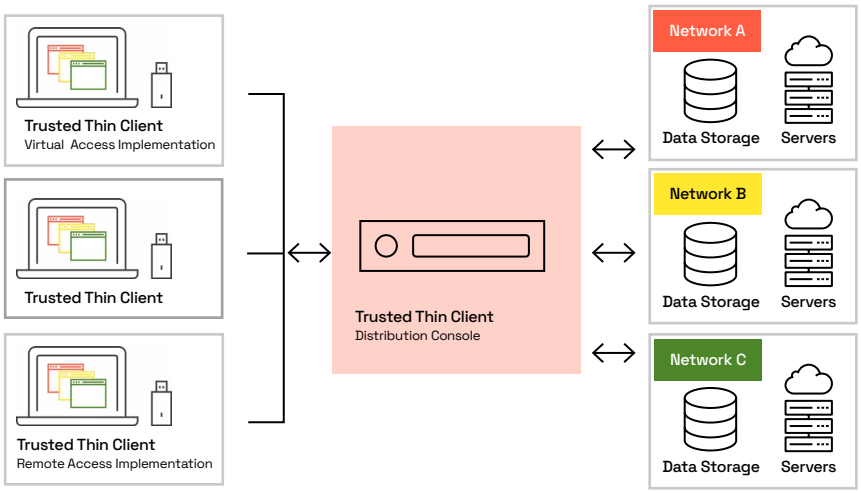
Built for the enterprise

Designed and built to meet the needs of enterprise deployments, Everfox Trusted Thin Client is a secure, flexible and scalable access solution. The solution provides robust centralized management for multiple form factors, globally dispersed sites, and easily scales to over a hundred networks and tens of thousands of users. Administrators are equipped with centralized tools for administration and monitoring, with the ability to easily add networks and clients. Administrators also have flexibility to enable access to users in offices, in-theater, and in the field from virtually any device.

Central administration, monitoring and auditing

The Distribution Console is the solu-tion's administration and monitoring hub, all Distribution Consoles, end-points and users are administered through the Management Console application. It is recommended that all deployments utilize multiple Distri-bution Consoles to address server outages, scheduled maintenance and unexpected hardware failures.

FIGURE 1: EVERFOX TRUSTED THIN CLIENT ARCHITECTURE



Through the Management Console, administrators can administer any Distribution Console from any other Distribution Console in the enter-prise—greatly reducing the need for on-site resources and the cost to transport administrators from site to site. Administrators can configure clients to failover to redundant Distri-bution 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 activ-ity. This audit data can be pushed to a centralized enterprise audit storage location.

Administrator role and account sepa-ration

Additional security controls are pro-vided through granular administrator role and account separation. Each ac-count is permitted only one role on the system, thus enforcing the require-ment 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 communica-tion services. This information contains relevant security data and allows the user to access the virtual environ-ments. When a network at another security level or a new server is added to the Distribution Console, the infor-mation is automatically sent to each client, removing the need to locally manage or update individual clients.

User access controls (username, pass-word, and clearance level) are validat-ed 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 Con-sole, further reducing administrative overhead.

Easily scale to over 100 networks and over 100,000 users. Implement anywhere critical data must be accessed.

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.

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 graphical windowing system, which provides immediate access to simultaneous 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 Everfox Trusted Thin Client only provides a redisplay of data from the data center. Should mali-cious 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. Additionally, users can only see resources they have been assigned and you can further assign restrictions based on the devices themselves.

With DC spanning you can connect to anywhere in the world, from anywhere in the world. For example, personnel located in Virginia can connect to a network in Korea. See Figure 2. Soon: Expanded Trusted Thin Client capabilities will be available with a Multi-Enterprise Spanning Architecture (MESA Partner Clusters) feature that will increase options to secure controlled collaboration across various agencies, commands, and partners while maintaining full control of their own resources. This publish-subscribe capability will allow granular access control with the flexibility to spin-up and spin-down access so that collaboration can happen at the speed needed to respond to rapidly changing mission requirements.

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)
Everfox Trusted Thin Client is recognized by the National Cross Domain Strategy Management Office (NCDSMO) and is included on the NCDSMO Baseline List. Everfox Trusted Thin Client is designed and developed to meet Raise-the-Bar requirements, 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. Everfox Trusted Thin Client has been assessed by the NCDSMO, and is on the NCDSMO baseline list.

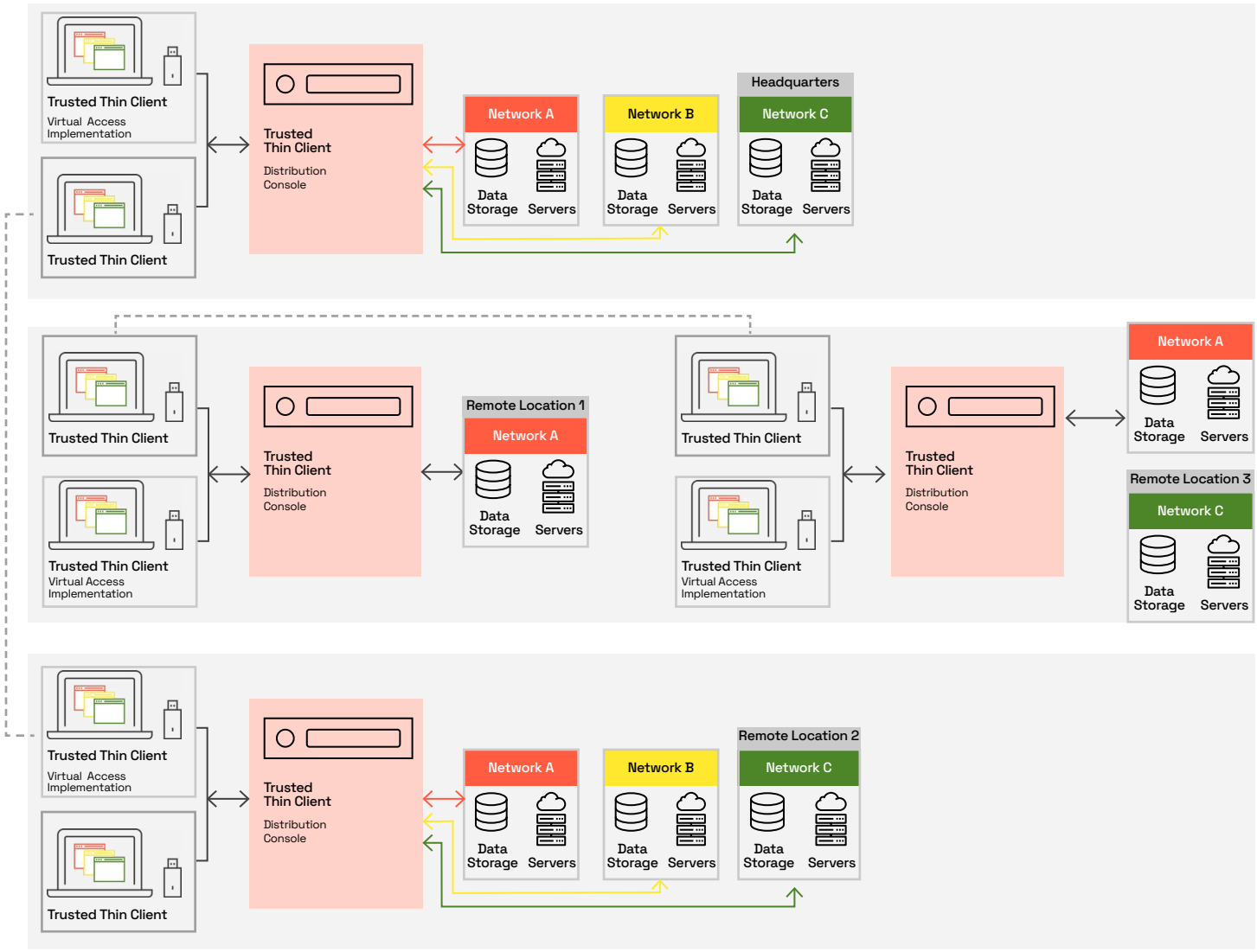


Figure 2: Everfox Trusted Thin Client Distribution Console Spanning

Conclusion

Everfox's Cross Domain multi-level solutions help prevent enterprises from compromise, while enabling collaboration through secure information access and transfer. Everfox is continually able to push forward with innovation and meeting stringent security standards, such as the ever-evolving Raise-The-Bar requirements. Everfox's secure access and transfer solutions strike the right balance between information protection and information sharing — a vital component to global and national security. Everfox Trusted Thin Client satisfies 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.

Everfox Trusted Thin Client is designed to satisfy information assurance requirements, eliminate potential leaks and risks, and provide users with a familiar desktop environment. Everfox's multi-network access technology 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 with proven deployments of over 60 classification levels. Easily add more networks, entire locations and endpoints or updated endpoints through a central management console.

Everfox Cross Domain multilevel solutions are designed to meet extensive and rigorous security A&A testing for simultaneous connections to various networks at different security levels. Everfox offers an experienced professional services team to guide customers through the technical implementation and A&A processes.

Learn More: www.everfox.com