WHITEPAPER

MESA Partner Networks: An Evolution in Information Access

EVERFOX

MESA Partner Networks: An Evolution in Information Access

The Department of Defense (DoD) and intelligence communities face unique challenges in sharing sensitive information between organizations while maintaining the highest levels of security and control. Traditional methods of information sharing often require extending network boundaries, exposing internal networks, data and IT systems to potential risks. This approach can be time consuming and may compromise the security and integrity of sensitive information, which puts mission success and decision dominance at risk. The adoption of Data-Centric Security and Zero Trust will help to address some of these challenges within an organization. However, organizations will remain limited to managing the data, information technology, and cybersecurity they control. Everfox has developed a new technology solution that will allow individual organizations to extend their secure environments to authorized partners for collaboration and information sharing.

The Everfox Multi-Enterprise Spanning Architecture (MESA) built on the Trusted Thin Client (TTC) Partner Cluster technology represents an evolution in information access between environments owned and operated by different organizations. It replaces legacy VPNs and point-to-point network connections that are expensive and expose program data to unnecessary risks. Through MESA, organizations can choose what information can be accessed and who is authorized to access it while retaining full control over their infrastructure and data.

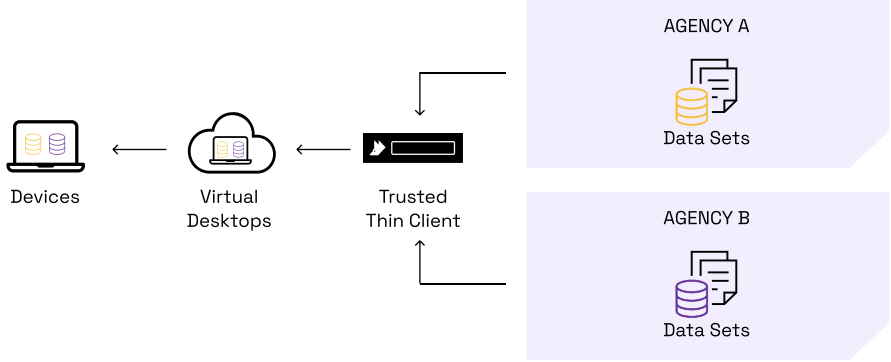


Fig. 1: TTC Access to Multiple Agencies

High Level Benefits

Reduces Costs

- → Reduces infrastructure costs
- → Minimizes COMSEC hardware and management overhead
- → Consolidates the number of user devices

Reduces Risk

- → Improves Operational Security (OPSEC)
- → Retains full control of infrastructure and data
- → Eliminates data exfiltration channels
- → No data resides at the desktop

Increases Speed and Agility

- → Scales horizontally over time
- → Rapid deployment timeframe
- → Centralized and simplified management through software

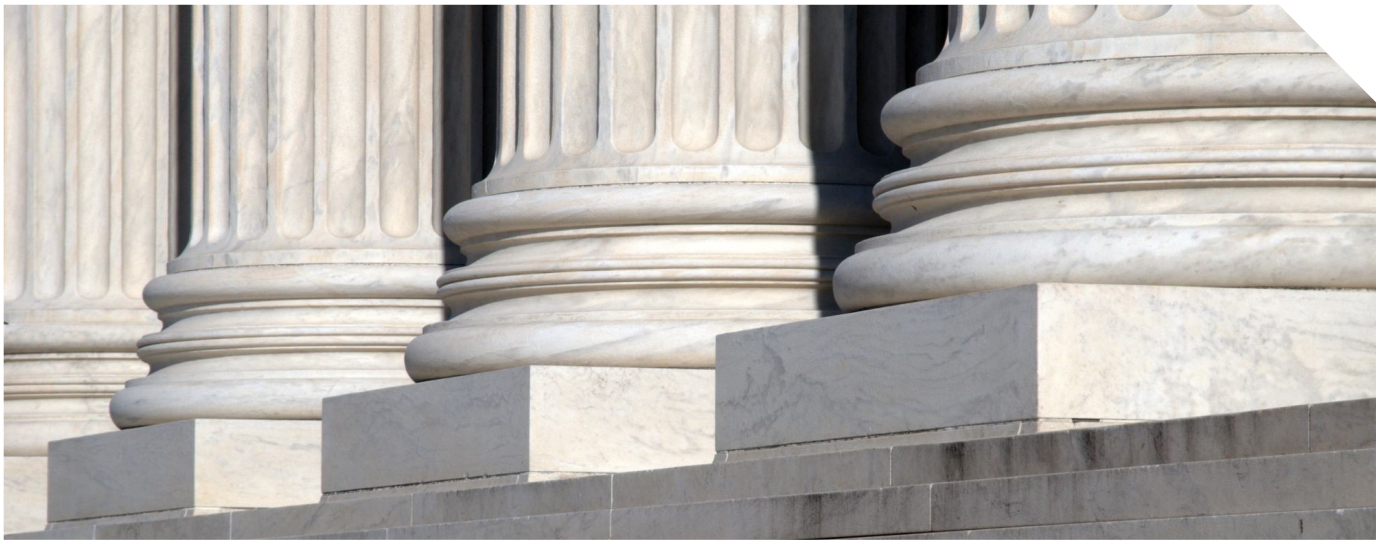
TTC is an Access Cross Domain Solution (CDS) which enables a single TTC End User Device (EUD) to access information from multiple isolated security domains (i.e. environments). TTC EUDs access applications and desktops remotely so that data always remains in a protected physical space such as an on-premises datacenter or cloud.

A single TTC user device may “view” data from multiple domains simultaneously by leveraging Virtual Desktop Protocols to display pixels to the user device, not the actual data files.

Everfox Trusted Thin Client (TTC) provides this transformational CDS functionality within many DoD and IC organizations today. TTC is on the NCDSMO CDS baseline list and meets NSAs Raise the Bar (RTB) requirements.

MESA enables multiple independent TTC environments to be connected together into a single distributed access network referred to as the MESA Partner Network.

The MESA Partner Network will allow TTC systems managed by separate organizations to interconnect, enabling each organization to selectively authorize partner-level access to collaboration tools and information without the need to modify the security of their internal networks, data, or IT systems.



Access between Partners before and after MESA

Before TTC

Sharing Access to Data requires changes to the Security Boundary

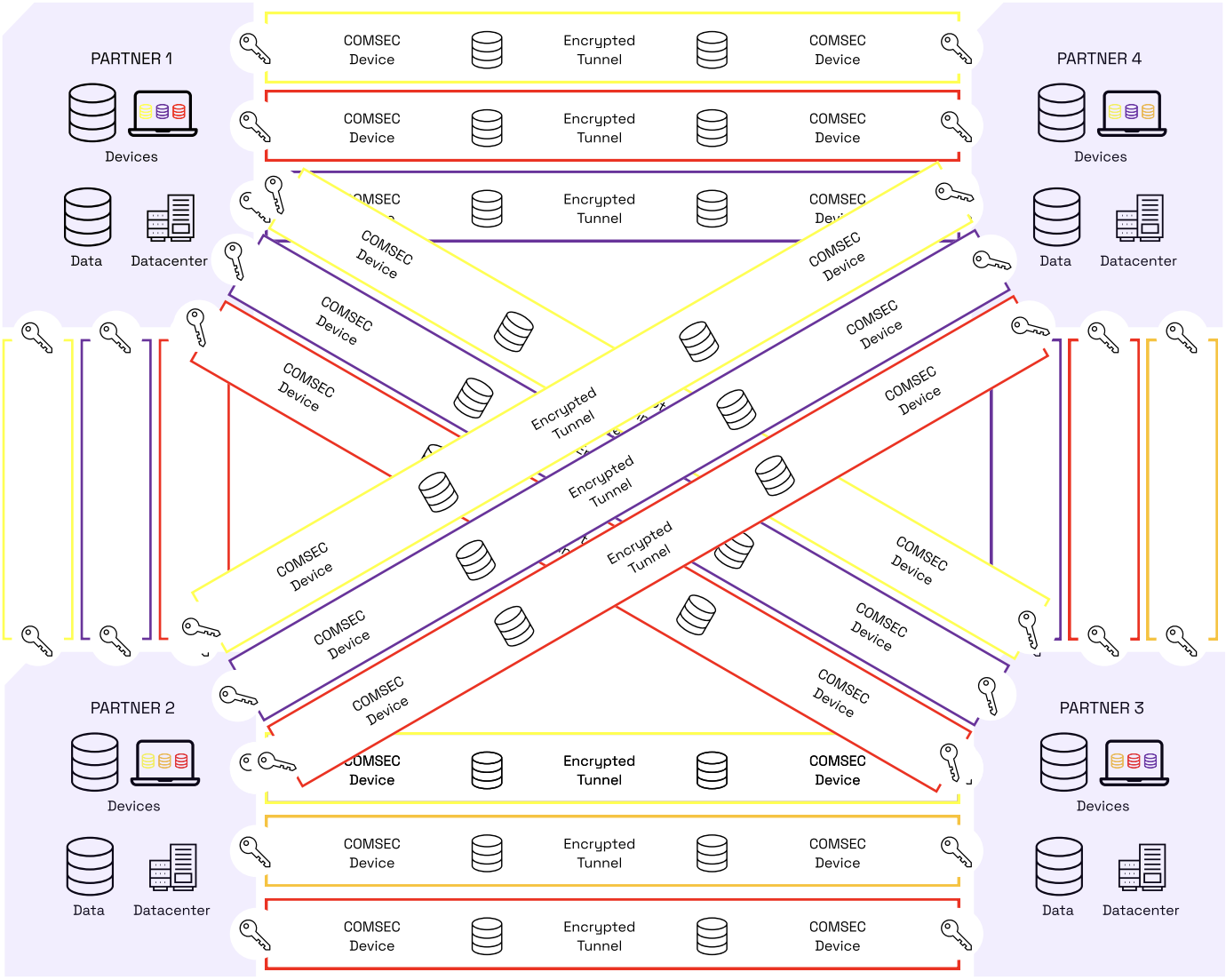


Fig. 2: Information Access Comparison

After TTC with MESA

Partners share Access to Data without changing their Security Boundary

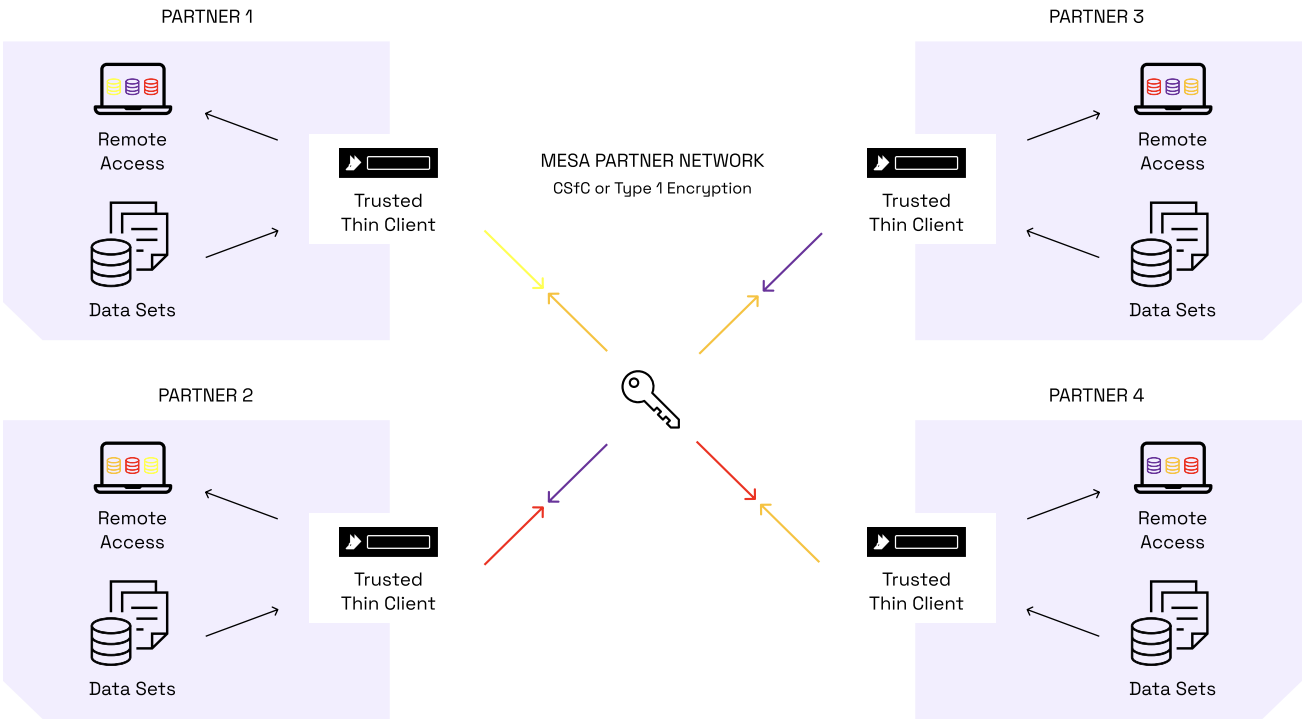


Fig. 2: Information Access Comparison

MESA: How it works

The MESA Partner Network establishes a multi-tenant collaboration and information access network that is managed through TTC software. To employ MESA, an organization must have at least one TTC server located within an on-premises or cloud datacenter configured with connectivity to one of more security domains hosting virtualized desktops or applications. A dedicated MESA network interface on each TTC server must be configured with an IP address that is reachable from partner organizations that will be authorized to connect through the MESA Partner Network.

The MESA Partner Network begins to function when one organization configures the necessary policy to authorize remote users and devices from a partner organization to access a resource (i.e. application or desktop) they have decided to publish.

Sharing access to virtualized desktop and application resources through the MESA Partner Networks requires coordination between publishing and subscribing organizations. Both the publisher and the subscriber must control at least one TTC server that is connected to a common network. The publisher will configure the connection details that enable access to a shared resource.

Once the resource is configured the publisher will be provided an ”authenticity proof” and passphrase from their TTC server that must be sent to the subscriber through an out-of-band method such as secure encrypted email. The subscriber will enter the information into their own TTC Server that is connected to the Partner Network. The authenticity proof will be used to ensure the authenticity of the publisher and the passphrase is sent electronically to the publisher so it can validate the identity of the subscriber.

Once this process has been completed, the users and devices that the publishing organization has authorized will be able to connect to the published resource. This process can be repeated for any number of subscribing organizations so that users from multiple organizations may be authorized to access the published resource through the shared Partner Network. The MESA publish and subscribe model only allows authorized users and devices to access a resource.

Each organization may maintain their own fully independent authentication and access management capabilities along with additional privileged access management and data security controls that are hosted within the boundary of their own environment. if desired, organizations may choose to utilize a federated Identity, Credential, and Access Management (ICAM) solution to manage user authorization through MESA.

MESA: Reduces Cost

Historically, the costs associated with standing up new netwrok infrastructure, deploying Type I encryption, and maintaining the new infrastructure have been a barrier to establishing shared collaboration and information access between partner organizations. MESA leverages existing network infrastructure to remove these barriers. Organizations will be able to leverage an existing circuit-based transport such as MPLS or modern SD-WAN to establish connectivity through MESA.

By way of example, two organizations that want to share access to information with each other might deploy up to four Type I encryption devices, one on either end of a network transport for each domain the organizations intend to share with the other (see figure 2). Each organization would then be responsible for maintaining the COMSEC associated with their respective end to end encrypted transport. Additionally, to protect their respective environments, each organization may also furnish dedicated user devices to the other organization to ensure that endpoint and data security are effectively managed at the remote end of the transport.

Access without MESA Partner Networks

- Requires new Type 1 encryption for each network classification that is shared
- Requires separate COMSEC management for each new classification
- Requires furnishing and managing remote user devices

By comparison, if both organizations utilize the MESA Partner Network, they can establish shared collaboration and information access through TTC software. Within minutes, a subscribing organization could access the virtual desktops or applications published by another organization. TTC user devices would remain compatible between organizations, alleviating the need to furnish equipment to remote users. Organizations that publish resources on the MESA Partner Network would be able to retain full control over their data and infrastructure protection from end-to-end. Utilizing MESA obviates the need to deploy additional Type I encryption devices or to expand COMSEC management duties. New organizations would have the option to connect their TTC cluster to an established MESA Partner Network and begin sharing resources immediately.

Sharing with MESA Partner Networks

- Utilize existing MPLS or other circuits to establish a single consolidated encrypted transport for collaboration and information access across multiple domains.
- Reduce the amount of COMSEC management overhead
- No need to furnish or manage remote user devices
- Dynamically add and remove new organization partnerships without standing up new network infrastructure.

MESA: Reduces Risk

Many organizations have unique concerns when it comes to protecting their respective data, users, and IT security. MESA addresses these concerns by providing organizations with greater control over their environment, how it is accessed, and by whom.

Authentication and authorization is managed via a two-tier system with the first tier being managed through the TTC and the second tier being managed through the virtualized application and desktop layer managed within each organization. Through TTC software, organizations can choose which resources to make accessible and which users (and devices) can view or attempt to access a resource.

Within each organization's environment, they retain full control over their cybersecurity and data layer security controls. Confidentiality is assured through multiple encryption layers. Type 1 encryption or CSfC encryption can be utilized for the outer layer of the MESA Partner Network. The TTC provides an additional layer of encryption and data encapsulation built into the RTB compliant and NCDSMO approved operating system platform.Within the TTC inner layer, data is isolated based on classification of each individual resource so that multiple security domains may traverses the MESA Network simultaneously.

OPSEC Benefits:

- Hides information about multi-lateral relationships between various partners
- Hides portions of data based on need-to-know
- Supports access control based on functional role (e.g. development, finance, funding, management, testing, engineering, etc.)

IT and Data Security Benefits:

- No data stored at the Thin Client endpoint. Information is sent to remote user devices as pixels – data never leaves the publishing organization's datacenter
- Organizations do not have to furnish or manage end user devices for partners
- Each organization retains full control over their IT and data security boundary
- Organizations maintain a level of isolation from one another that mitigates the potential liability of being exposed to IG inspections as a result of potential security incidents
- Access to organizations can be limited per user and per device

User Security Benefits:

- Organizations may manage their own identity and access management service or use a federated ICAM
- Organizations may manage their own user monitoring and logging service or utilize shared enterprise services
- Each organization retains administrative control over which users may access published services and can revoke access on demand through TTC software without modifying hardware and networks

MESA: Increases Speed and Agility

Traditional methods for establishing collaboration and information access between organizations is not only costly but also time consuming. It can take several months to over a year to acquire, deploy, and approve the necessary infrastructure. With MESA, access to information is managed through software and leverages existing infrastructure.

The time required to access information between organizations can be reduced to days, and in some cases within hours. Organizations will benefit from this time savings by redirecting funds, engineering, and management resources toward other mission-oriented tasks.

MESA is designed to grow horizontally meaning that new organizations and resources can be added without changing the underlying infrastructure or interrupting services that are currently being delivered. New organizations simply connect a compatible TTC server to the shared MESA Partner network and publish or subscribe to resources when necessary.

Likewise, organizations that already operate on the MESA Partner network can add or remove virtual desktop and application resources without having to coordinate with other organizations or make changes to the underlying network infrastructure that MESA utilizes. Coordination between organizations is only necessary when a publishing organization has configured their access controls and is ready for a subscriber to begin accessing their published resources.

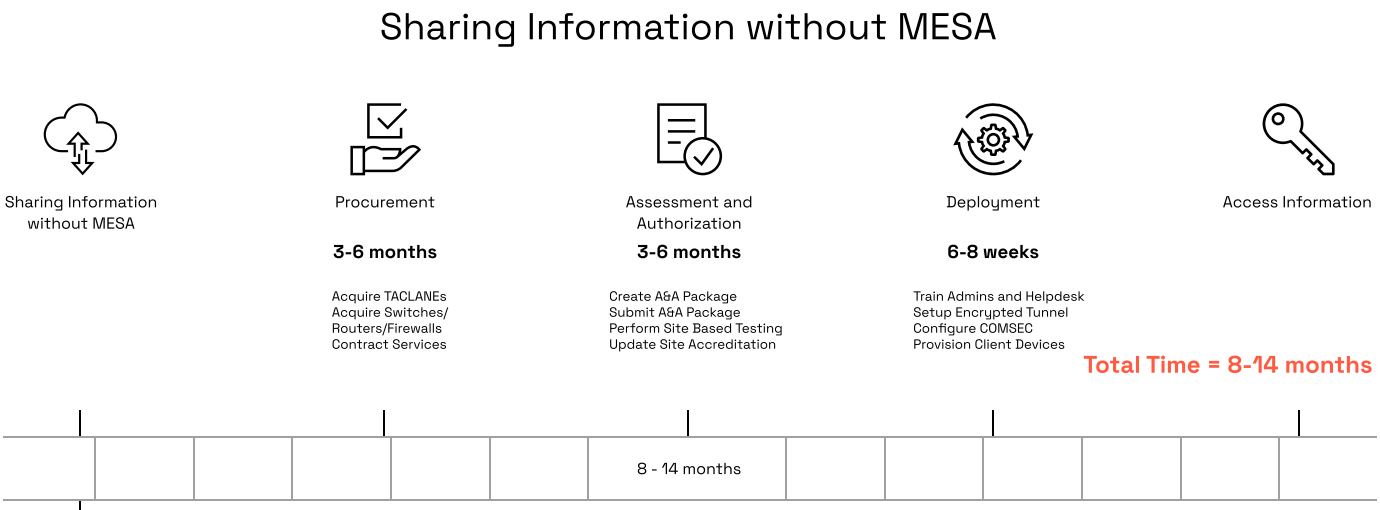


Fig. 3: Timeline for sharing Information without MESA

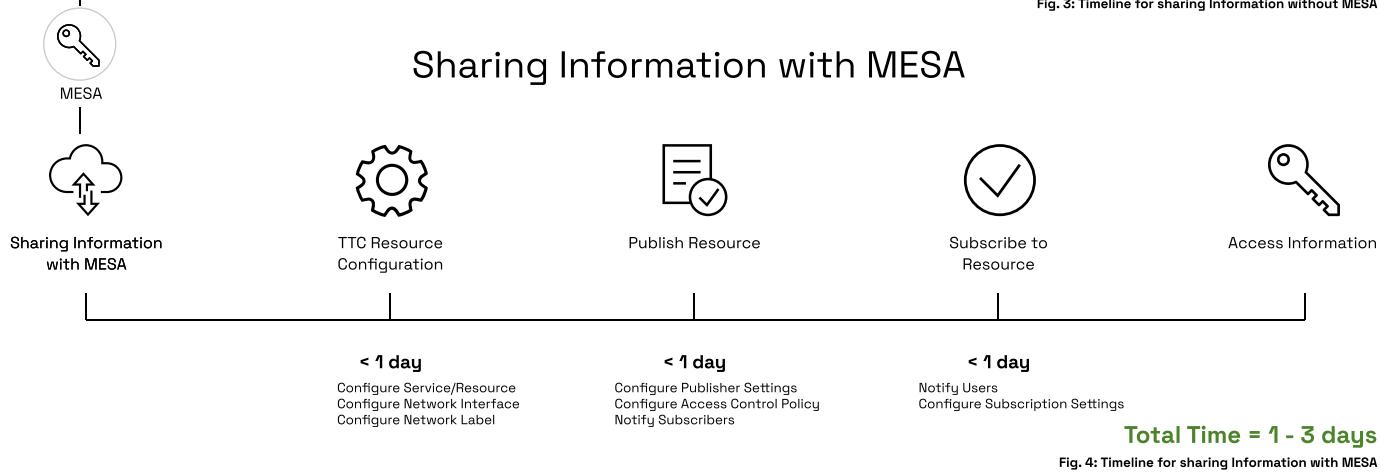


Fig. 4: Timeline for sharing Information with MESA

MESA: Realizing the Benefits

Organizations can begin realizing the benefits provided by TTC and MESA in a timeframe and within a budget that fits their unique needs. The benefits of TTC as a means for consolidating the number of user devices and bloated netwrok infrastructure can be realized on any scale, large or small. The TTC Access CDS is currently deployed in environments with geographically distributed datacenters and to over 200k users with organizations ranging in size from less than 50 users to as large as 45k users.

Each TTC server has the capacity to support up to 1000* user devices and up to 15** different network classifications. A single server in a datacenter can have an immediate and sizable impact on operational capability. Adding additional servers to a TTC cluster allows for easy expansion to support an unlimited number of user devices and security domains.

*this number is estimated based on certain factors such as the volume of concurrent VDI connections and server configuration
**this number is based on server configuration

An established MESA Partner Network will be available to new organizations that deploy TTC and will be ready for integration when needed. As more organizations begin joining their TTC servers onto the MESA Partner Network the speed of information access throughout the network will increase rapidly.

MESA provides a game-changing solution for DoD and Intelligence agencies, enabling secure controlled, and scalable collaboration and information access while maintaining the highest levels of security and control.

By leveraging MESA, these agencies can redefine how they securely share information, protect security domains, and maintain control of data security, ultimately enhancing mission success and decision dominance.

About the Author

Chris Finch is a Solutions Architect with Everfox. He works closely with industry thought leaders, customer stakeholders and the Everfox team to help develop innovative cybersecurity solutions that protect the government cyberspace.

By leveraging his wealth of over 20 years of operational experience in cyber and Cross Domain Solutions, Chris has helped position Everfox as a leader in multi-domain security for the government.

Following his service in the United States Air Force, Chris obtained his Bachelor of Science in Computer Information Systems. His early career began as a Systems Engineer delivering Cross Domain Solutions across the DoD and Intelligence Communities. He built upon these experiences by obtaining his CISSP and CCSP certifications.

In these positions, Chris gained extensive experience in cybersecurity and Cross Domain Systems, in leading technical innovation and in translating customer needs into impactful requirements that drive the design process.

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.

Learn More

www.everfox.com