FORCEPOINT

Solution Brief

Multi-Enterprise Spanning Architecture (MESA)

Advanced Networking, Collaboration and Security

Challenge

The current global security landscape demands that organizations share information quickly both internally and with trusted mission partners while maintaining strong security.

For example: US Indo-Pacific Command (USINDOPACOM) works with mission partners to further objectives throughout the Indo-Asia-Pacific region. Five of seven U.S. Mutual Defense Treaties exist in the USINDOPACOM Area of Responsibility, which translates to five alliances of national militaries that must operate together daily as a unified force and through all phases of planned operations. Sharing information currently is done via methods such as email or sneakernet which results in slow communication, often proves ineffective, and comes with inherent security risks.

NEED: A secure, timely, and efficient way to share information internally and externally across mission partners.

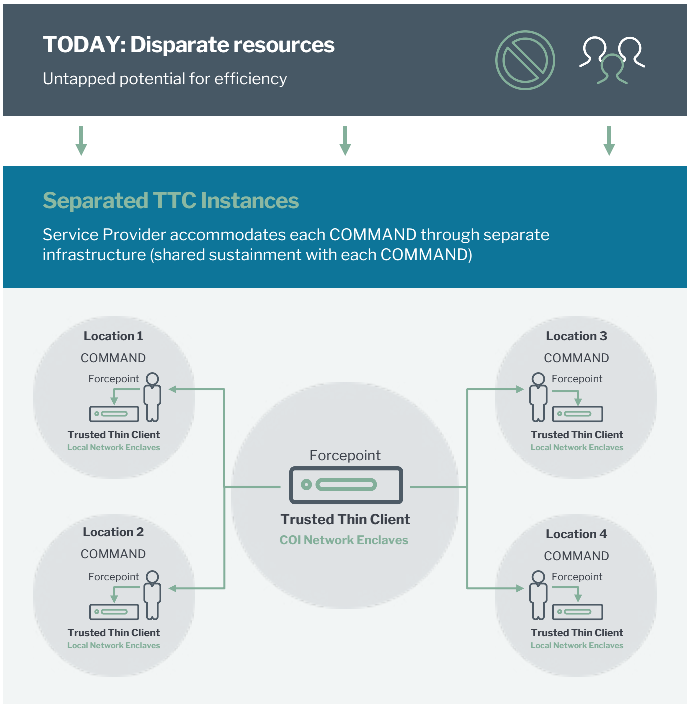


Figure 1. Today's landscape: disparate groups and networks unable to collaborate efficiently to accomplish the mission

Solution

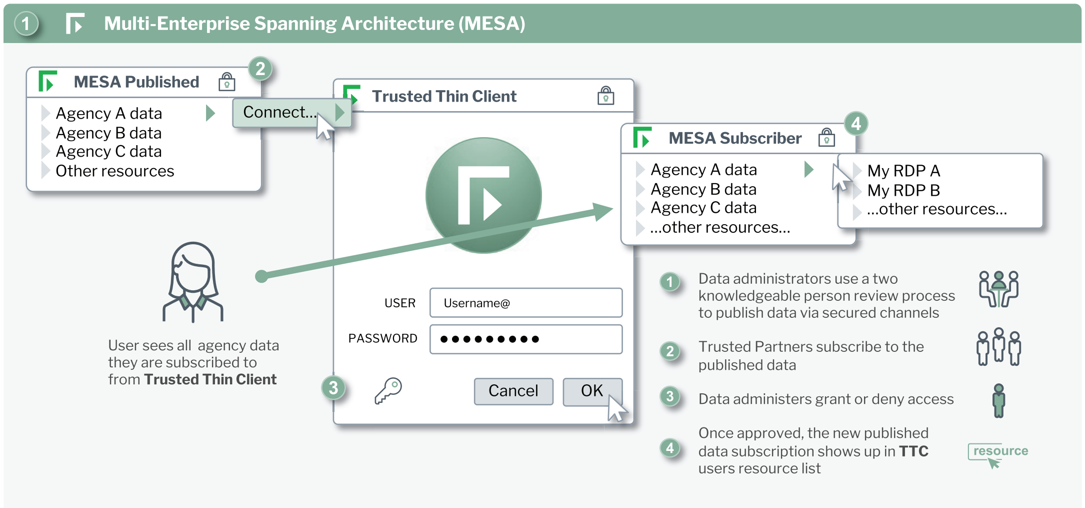
Forcepoint Trusted Thin Client (TTC) solves the difficult problem of satisfying security needs while enhancing user productivity. It provides users with secure simultaneous access to any number of sensitive networks through a single device, in support of an enterprise-ready trusted collaboration experience.

Forcepoint's TTC Multi-Enterprise Spanning Architecture (MESA) takes that access to the next level. MESA provides advanced networking, collaboration, and security features on TTC's proven foundational technologies.
By leveraging pre-existing TTC solutions, a web of independent Coalition Partner private clouds with enhanced security and capability for Command and Control actions during exigent and emergent circumstances can be created. Each independent Coalition Partner, private cloud, or TTC Distribution Console node could also be expanded to include integration with commercial FedRAMP-certified CSP networks. Depending on the requirements of each domain regarding the security levels necessary for the CSP, NIPRNet-based solutions could use FedRAMP-certified IL5 for file, application, virtualization, web, information sharing, or application access. Classified solutions could use FedRAMP-certified IL6 for file, application, virtualization, web, information sharing, or application access.

How It Works

MESA provides on-demand access to any permitted network (internal or external to your organization) from any location around the globe from an approved client device. The MESA publish-subscribe model enables a service provider to publish any community of interest (COI) network or application to any authorized consumer (user). This model also provides users access to VDI services (as subscribed to) on-demand—command to command, agency to agency, partner to partner (as authorized). For example, a service provider can consolidate and manage access to an unlimited number of secure enclaves throughout every command, including coalition enclaves such as Battlefield Information Collection and Exploitation Systems.

Just as important is the ability to "tear down" these connections and configurations quickly and easily using centralized management. This is important for not only standing up multinational collaborative austere deployment, but also for decoupling from the services quickly and with minimal cost at mission end, with the assurance that the owning organization of each retains access to resources.



User sees all agency data they are subscribed to from **Trusted Thin Client**

1. Data administrators use a two knowledgeable person review process to publish data via secured channels
2. Trusted Partners subscribe to the published data
3. Data administers grant or deny access
4. Once approved, the new published data subscription shows up in **TTC** users resource list

Figure 2. Future: MESA publish-subscribe model enables a service provider to publish any COI network or application to any authorized consumer (user)

Key Functions

- Organizations maintain complete and discreet administrative control of their published VDI resources
- Administrative processes and approval workflows remain unchanged—each participating group stands alone with its own administrative domain
- Each organization's administrators have final access authority for participating organizations
- Granular access at user level
- Two knowledgeable person review process
- Ongoing non-security relevant configuration changes to published services are automatically updated (i.e., broker IP address change within existing network range, etc.)
- Unlimited sharing to authorized remote entities
- Local users gain access to remote entity VDI services
- Peering model is many-to-many
- Built-in redundancy and fail-over
- Network aware least-cost routing
- Applications
  - Disparate, multi-entity mission groups and entities located remotely that need to share resources
  - Allows easy sharing between disjointed security levels

Outcomes

MESA's publish-subscribe model enables a service provider to publish any COI network or application to any authorized consumer (user). Enabling end users from different environments to access, display, and interact with multiple network security enclaves with a single computing device and single network connection.

Benefits

- Share information at mission speed with maximum security
- Joint interoperability access environment to all coalition partners
- Secure interchange and access services and data on each independent network
- Rapid COI network deployment (multi-coalition forces, Joint Task Force, etc.)
- Rabid tear-down capability
- Share common applications and collaboration tools
- Reduced capital expenditure (CapEx)
- Reduced operational expenditure (OpEx)
- Increased mission effectiveness & operational efficiencies through streamlined access to critical information.

MESA continues to raise the bar in security and presents customers with the power to leverage the innovation and resources of their mission partners to optimize their cross-domain access investments.

forcepoint.com/contact