Virtual Desktop Infrastructure (VDI) is a form of desktop virtualization that's popular for consolidating and centralizing desktops, streamlining management and costs and securely enabling access to virtual desktops anytime, from anywhere. User desktops can be run inside virtual machines on servers in datacenters and provide users with personalized desktops and the simplicity of centralized management. A mission critical agency within the DoD utilizes multiple networks to support its mission and functional requirements.

ManTech was tasked with designing, implementing and testing a new network architecture for its three sites. This design replaced the legacy infrastructure to support the agency's mission and consisted of a new network infrastructure (LAN and WAN), Computer Network Defense (CND) architecture, compute, virtualization, and storage environments (NAS or SAN). As part of the project, ManTech engineered a Virtual Desktop Infrastructure (VDI) solution across all the network sites.

VDI is an emerging practice of replacing traditional desktop operating systems with virtual machines residing on centralized servers. VDI allows for significant CAPEX and OPEX savings, and more importantly enhances enterprise security and allows ease of remote management. Utilizing highly redundant and scalable network infrastructure, certified COTS software and zero client desktops, ManTech designed, deployed and configured an enterprise-wide VDI solution that met the requirements of the DoD customers' mission.

For this project, ManTech used VMware Horizon View as the solution to provide VDI capability. VMWare Horizon is a software VDI framework that delivers virtualized desktops and applications through a single platform, giving end-users enterprise access through one unified workspace.

- VMware vCenter Server was used in conjunction with VMware Horizon to present end-user desktops from VMs running on ESXi hosts.
- After a desktop is provisioned, authorized end-users use Clearcube zero clients or locally installed client software to connect securely to the centralized virtual desktops.
- These virtual desktop images were STIG-hardened to comply with all DoD mandates.
- VMware Horizon used the existing Microsoft Active Directory infrastructure for user authentication and management.
- Horizon View Connection Server was used to authenticate users to the existing Active Directory infrastructure before directing the request to the appropriate virtual machine.
- Horizon View Administrator was used to configure the Connection Server and manage the remote desktops and applications.
- CAC Authentication was configured for role-based access to resources.
- View Composer was used to provide the ability to deploy multiple VMs from a single image, resulting in significant savings in storage requirements.

This approach of using a single baseline image allowed for ease of patching and performing upgrades and enhancements. Changes to a single master image triggers the View Composer to apply the updates to all cloned desktops. View Agent Service was also installed on all VMs to allow communication between the View Connection Server and the VM. The View Agent service provided features such as connection monitoring, virtual printing and persona management (persistency across multiple sessions). Deploying the above VDI solution throughout the enterprise allowed for ease of management, high availability, enhanced security, user mobility and overall CAPEX and OPEX savings for the customer.