Delivering Secure Remote Access to Classified Networks

KEY BENEFITS

- Offers risk-adaptive cybersecurity for remote access
- Offers a commercial off-the-shelf (COTS) solution
- Delivers Zero Trust security to classified networks
- Is Raise the Bar ready and recognized by the National Cross Domain Strategy Management Office (NCDSMO)
- Integrates with VMware SDDC technologies
- Enhances the audio and video experience for Microsoft Teams
- Supports modern hybrid and multi-cloud architectures

Government agencies at every level have had to reimagine how best to achieve mission outcomes, protect information, and improve employee engagement in the new distributed workplace. Enabling secure, remote access to classified networks for remote workers has become especially important as many government agencies don't see remote work going away. *An SAIC survey* of 300 federal IT decision-makers found that they expect remote work to increase in the future.[1] Additionally, the U.S. Air Force estimates *one-third of its workforce will remain working remotely* after the pandemic subsides.[2] IT departments need to ensure these remote devices meet strict compliance requirements (e.g., NIST, FIPS), applications are available to users and updated in a timely manner, and that applications and data are secure from unauthorized access.

With many traditional tools unable to scale or adequately fulfill their requirements in this distributed, disconnected model, agencies must modernize how they deliver, manage and secure access to government resources. A Zero Trust approach to security—in which the security architecture limits access to resources via strict identity and device verification procedures—is one way for agencies to meet these challenges.

Providing Zero Trust security for the digital workspace

A critical tool for delivering secure remote access to classified networks is virtual desktop infrastructure (VDI). With VDI, desktops run in the agency's data center with users connecting to the desktop from an endpoint device, meaning the user only sees an image of their desktop. No actual data is downloaded or stored on the endpoint device, just pixels. Using VDI, agencies can provide a complete Windows desktop with all of the applications the user will need, without having to touch the user's device or risk agency information being lost or stolen with the device. This enables users to connect to authorized networks from any location.

VMware Horizon® securely delivers virtual desktops and apps from a single control plane, with rapid provisioning, automation and simplified management to extend the best digital workspace experience to end users. Leveraging best-in-class management capabilities and deep integrations with the VMware technology ecosystem, the Horizon platform delivers a modern approach for desktop and app management that extends from on premises to hybrid and multi-cloud environments. This results in fast and simple virtual desktop and application delivery that extends the best digital workspace experience to all applications.

1. SAIC and Market Connections. "The Federal Agency Response to the War on COVID-19." October 20, 2020.
2. Association of Defense Communities. "One-Third of Air Force Workers May Remain Remote Permanently." September 17, 2020.

NIAP ACCREDITED

The National Information Assurance Partnership (NIAP) oversees evaluations of commercial IT products for use in national security systems. Accredited products must meet stringent requirements from NIAP, FIPS and ISO. The following VMware products are NIAP accredited and listed on the CSfC components list, ensuring they can easily be implemented into a classified network's architecture:

- VMware ESXi™
- VMware Workspace ONE Unified Endpoint Management
- VMware Workspace ONE Boxer

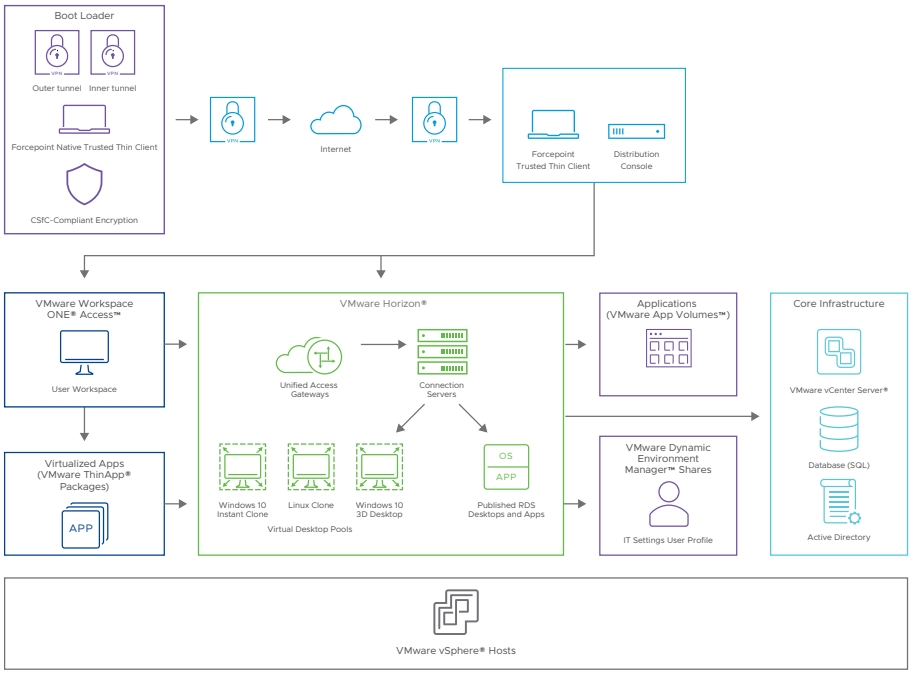

FIGURE 1: Deployment architecture.

Unique integration with VMware technology

Leveraging VMware's virtualization heritage and leadership in SDDC and digital workspace technology, Horizon delivers unique benefits across management, networking, security and user experience. Built on VMware Cloud Foundation™, Horizon can leverage the market-leading capabilities of VMware vSphere®, VMware vSAN™, and VMware NSX® to deliver real-time desktops and applications, strengthen security, and simplify and automate Day 2 operations.

VMware Workspace ONE® utilizes FedRAMP Moderate Authorized instances of key Workspace ONE technologies: VMware Workspace ONE Unified Endpoint Management and VMware Workspace ONE Access™. Combining Zero Trust conditional access control with industry-leading modern management, Workspace ONE helps IT proactively secure their digital workspace of users, apps and endpoints. Workspace ONE manages endpoint devices, ensuring updates are delivered to off-network machines and that security baselines are met, such as enforcing passwords/PINs. Workspace ONE enables IT to provision new agency government-furnished equipment (GFE) out of the box, anywhere in the world, from the cloud in minutes. IT can also onboard new employees with all apps to GFE in less than an hour without tickets or help desk calls. Workspace ONE PIV-D Manager supports derived credential authentication without the need for additional hardware smart-card readers.

Additional security features are woven into VMware technologies across the network and supported by Horizon, such as VMware NSX® Advanced Load Balancer™ and VMware SD-WAN™. With next-generation endpoint protection from VMware Carbon Black products, IT can further improve security on virtual desktops and apps. These intrinsic elements help provide a Zero Trust access security model across users, apps and endpoints that empowers employees without sacrificing security.

KEY CAPABILITIES

- Supports VDI initiatives from the Department of Defense (DoD) and the U.S. Intelligence Community, such as DoD's Joint Information Environment (JIE) and Mission Partner Environment (MPE)
- Provides hardware- and software-level disk encryption
- Performs tamper-proof hardware verification
- Deploys at single level (e.g., secret), leveraging current CSfC stacks
- Supports Personal Identity Verification (PIV), Common Access Card (CAC), Special Agreement Check (SAC), and SIPR token smart cards

Forcepoint Trusted Thin Client Remote

To meet government requirements for remote access to secure networks, VMware partners with Forcepoint. The Forcepoint Trusted Thin Client and Trusted Thin Client Remote solutions layer on top of the Horizon VDI to add required capabilities, such as dual VPN communication stack encryption leveraging current National Security Agency (NSA) Commercial Solutions for Classified (CSfC) stacks.

Trusted Thin Client Remote is installed directly on the endpoint device, allowing for efficient use of the device's native hardware capabilities, such as video playback acceleration, multiple monitor support, audio, webcams, and smart cards. An authorized user starts the laptop, provides an initial decryption password to allow hardware-based system integrity validation, and initiates secure VPN connections to their organization. The user then authenticates to the data, applications and networks that reside solely in the organization's data center. The native security capabilities of Workspace ONE and Horizon ensure that no data leaves the data center, removing the risk of data breach should the device be compromised, lost or stolen.

A Horizon-based instance of Trusted Thin Client Remote contains *COTS components validated by the CSfC program* to be used in layered solutions to protect classified data within national security systems.[3] Trusted Thin Client Remote supports the *CSfC Mobile Access Capability Package* (MACP) in multiple configurations, including in combination with the Data-at-Rest Capability Package (DARCP) or in a thin end-user device implementation, depending on security requirements defined by the authorizing official. It adheres to mobile access requirements and meets the "demand for mobile data in transit solutions (including voice and video) using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components."[4] The solution enables access to multiple sensitive networks from a single secure endpoint device.

Forcepoint is the only COTS developer with access and transfer solutions recognized by NCDSMO. Forcepoint Trusted Thin Client and High Speed Guard are the widest deployed access solutions within the DoD, the U.S. Intelligence Community, and the civilian federal government.

3. National Security Agency/Central Security Service. "Commercial Solutions for Classified Handbook, Version 3.0." November 2017.
4. National Security Agency/Central Security Service. "Mobile Access Capability Package, Version 2.1." June 26, 2018.

LEARN MORE

For more information, visit the *VMware Federal Government IT Solutions page*.

Supporting remote work and beyond

It has become imperative that agencies support remote working. While providing many benefits, remote work also poses significant security challenges, especially with federal and civilian government agencies. These workers frequently require access to data that resides on multiple sensitive networks, and the risk of having this data reside on laptops is too great. VMware provides a simple solution to this problem, allowing secure access to an agency's data center from an agency-provided laptop. From the data center, workers gain access to all authorized networks required to do their jobs. They can work from any location without fear of data compromise or data loss. All data and work products are saved on the appropriate network at the agency's data center, not on the endpoint device.

This solution can also be applied to the highly mobile computer systems the DoD deploys in theater. It reduces the amount of equipment that needs to be carried in each vehicle, and enables each endpoint to simultaneously access all allowed networking from one device. Agents that work primarily in the field also benefit from the solution. They can easily boot to the secure workspace from their standard-issue laptop, providing agents with fast, secure and undetectable access to any authorized agency network, application or data needed to fulfill their mission—regardless of location. This decreases their risk of discovery, and increases the reliability and accessibility of information gathered and shared.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: 696857aq-so-sec-rem-acc-clsfd-ntwks-uslet 2/21