National Defense-ISAC

The Role of VDI for CMMC

October 2025

Focused on securing Controlled Unclassified Information, this work highlights how Virtual Desktop Infrastructure (VDI) reduces endpoint risk and aligns with CMMC requirements across the defense industrial base.

DIB Sector Coordinating Council
National Defense ISAC

TLP:CLEAR

EXECUTIVE SUMMARY

Organizations across the Defense Industrial Base (DIB) continue to face pressure to protect Controlled Unclassified Information (CUI) while maintaining productivity and collaboration across a diverse and distributed supply chain. Many of the greatest challenges stem from the need to enable access from systems or users outside an organization's compliance boundary such as subcontractors, suppliers, or remote personnel without introducing additional cybersecurity risk.

Virtual Desktop Infrastructure (VDI) offers a secure way to meet this challenge. When implemented within a compliant, centrally managed environment, VDI allows users to securely interact with CUI without ever storing, processing, or transmitting that data on the endpoint device. The endpoint becomes merely a conduit for encrypted keyboard, video, and mouse traffic, sharply reducing the attack surface while preserving collaboration. VDI does not remove the need for trusted access or endpoint security controls; it complements them by minimizing the consequences if an endpoint is compromised or operating in a less-trusted location.

Aligned with NIST SP 800-171 and CMMC Level 2 requirements, VDI supports multiple control families (including Access Control, Identification and Authentication, System and Communications Protection, and Audit and Accountability) by centralizing management, enabling detailed monitoring, and enforcing consistent policy application. When layered on top of FedRAMP-authorized cloud infrastructure, this model allows organizations to inherit a strong baseline of security while tailoring configurations for CMMC-specific compliance.

For defense manufacturers and contractors, VDI provides a pragmatic path to secure digital collaboration without resorting to cost-prohibitive and risky "swivel seat" setups or expanding the compliance boundary to every external device. Properly designed, it strengthens both the security and usability of CUI access, providing a scalable and adaptable foundation for compliance across today's connected defense ecosystem.

Principal authors of this document include the members of the DIB-Sector Coordinating Council VDI Working Group. ND-ISAC is the administrative and operational arm of the DIB SCC.

DISCLAIMER

TABLE OF CONTENTS

INTRODUCTION

Organizations across the Defense Industrial Base (DIB) are continually challenged to protect Controlled Unclassified Information (CUI) while enabling collaboration across complex supply chains. In practice, this often means working with external partners, subcontractors, and remote users whose endpoint devices may not meet the organization's compliance or configuration standards. The question is not whether these participants will need access (they already do) but *how* to provide that access securely and responsibly.

Virtual Desktop Infrastructure (VDI) provides one practical answer. When properly implemented, VDI confines all CUI interaction to a compliant, centrally managed environment, keeping data from being processed or stored on local endpoints. In this model, the endpoint simply becomes a conduit for encrypted keyboard, video, and mouse traffic. This approach does **not** eliminate the need for access control, device hygiene, or trusted locations; rather, it complements them by sharply reducing the attack surface and limiting the exposure of CUI to non-compliant systems.

The intent of this paper is to clarify how VDI can **mitigate** risk, not bypass it, particularly for organizations navigating the Cybersecurity Maturity Model Certification (CMMC). By drawing a clear compliance boundary around the virtual environment, organizations can collaborate effectively without expanding their certification scope to every partner device. This paper explores the role of VDI in protecting CUI, supporting CMMC-aligned controls, and enabling secure collaboration across a distributed defense supply chain.

UNDERSTANDING THE CHALLENGE

ENDPOINT CUI USE DEVICES

Endpoint devices comprise a range of form factors from Microsoft Windows, Apple Mac, and Linux computers to mobile devices including Android and iOS tablets and phones. These endpoints can introduce vulnerabilities into an organization's IT environment when they lack necessary security controls, or be infected with malware, or be susceptible to unauthorized access. When such devices are used to access sensitive information, they can compromise the confidentiality, integrity, and availability of data.

Endpoint devices may be non-compliant or outside the scope of control for an organization's CMMC-compliant IT environment under many circumstances. Most commonly, the endpoints may be owned and managed by external organizations such as subcontractors, suppliers, partners, customers, etc. Additional examples may include IT environments of the same organization, but in a different management scope, such as foreign subsidiaries or commercial subdivisions. Since these endpoints are non-compliant with CMMC, or cannot be trusted, they are not permitted to access CUI and other sensitive information.

However, in many real-world scenarios, these users still need to access information or participate in collaboration. In such cases, technologies like Virtual Desktop Infrastructure (VDI) can provide a controlled means of access, bridging the gap between operational necessity and compliance by allowing interaction with CUI without expanding the organization's boundary of responsibility or increasing endpoint risk.

CMMC COMPLIANCE

The CMMC framework is designed to enhance the cybersecurity posture of organizations within the Defense Industrial Base (DIB) serving the U.S. Department of Defense (DoD). It establishes a set of cybersecurity practices and processes across three maturity levels, with Levels 2 and 3 focusing on the protection of CUI. Achieving CMMC compliance requires organizations to implement stringent security controls to safeguard CUI from cyber threats and vulnerabilities. Endpoints fall under the scope of CMMC compliance when they store, process, or transmit CUI. They must be secured according to a set of 110 controls and assessment objectives defined by National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171r2).

USE CASES FOR ENDPOINTS AMONG ORGANIZATIONS SEEKING CERTIFICATION (OSC)

Collaboration: Organizations often need to share unstructured data such as documents and email that may contain CUI (e.g. Request for Proposals). They may also host meetings and messaging where sensitive information may be exchanged. It is common that recipients of this information are outside of the scope of control for the OSC, especially for external users at subcontractors, suppliers, partners, customers, etc. Collaboration often results in many copies of data circulating outside the compliant environment.

Application Access: Applications include supplier management, enterprise resource planning (ERP), human resources systems and other enterprise solutions. If the applications contain CUI, they must reside behind a firewall in a CMMC compliant IT environment. This will effectively block access to non-compliant endpoints.

Digital Engineering: Digital engineering environments include centralized IT environments hosting data and applications such as product lifecycle management (PLM), computer-aided design/modeling solutions (CAD or CAM) and often have a requirement for high-performance computers. The endpoints for digital engineering require minimum system specifications and often need to download or print information (e.g. blueprints) that is prohibited if non-compliant. This results in data being exported and shared through collaboration channels.

Manufacturing Shop Floor Access: End-users may require access to CUI from the manufacturing facility. This may be from a kiosk located on the shop floor, a portable tablet, a secure printer, or endpoint devices integrated with manufacturing equipment (e.g. CNC mill),

etc. As with digital engineering, non-compliant endpoints result in data being exported and shared through potentially non-compliant collaboration environments.

THE ROLE OF VIRTUALIZATION / VIRTUAL DESKTOP INFRASTRUCTURE

WHAT IS VDI?

VDI is a technology that allows users to access a virtualized desktop environment hosted on a centralized IT environment. Instead of running applications and storing data on local endpoint devices, users interact with a virtual desktop that resides in a secure and compliant data center. This approach provides security benefits, particularly when dealing with non-compliant endpoint devices.

Examples of VDI solutions include:

- Microsoft Azure Virtual Desktop (AVD)
- Windows 365 (W365)
- Amazon Workspaces
- Google Cameyo
- VMware Horizon
- Citrix Workspaces
- Nutanix XI Frame

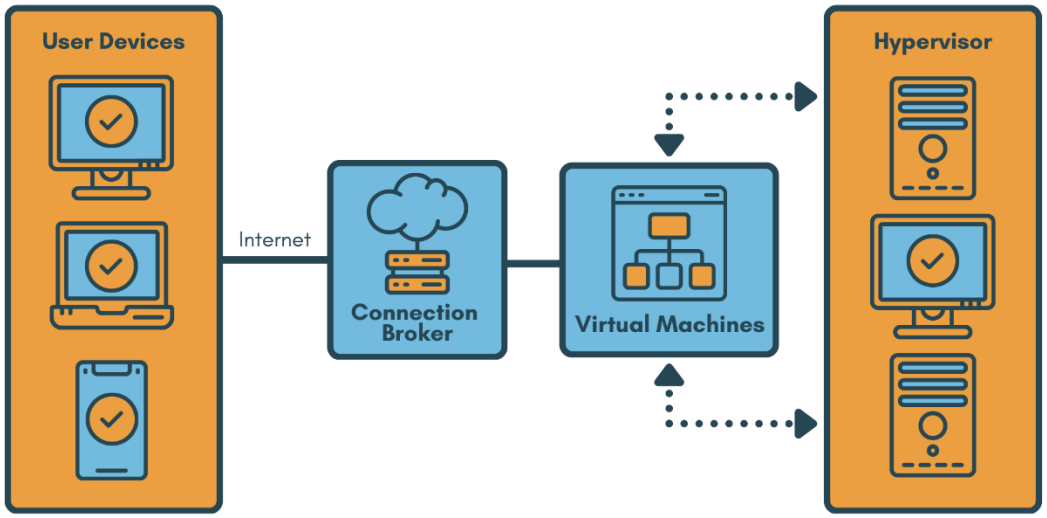

Figure 1.1
Source: Helpwire.app

KEY BENEFITS OF VDI

Centralized Management and Control: VDI enables centralized management of virtual desktops, allowing IT administrators to enforce security policies, apply patches, and monitor activity from a secure and compliant location. This reduces the risk of security gaps that may exist on individual physical devices.

Isolation of Sensitive Data and CUI: By keeping sensitive data within the virtual desktop environment, VDI prevents data from being stored on potentially compromised physical devices. This isolation ensures that even if a physical device is compromised, the sensitive data remains protected.

Granular Access Control: VDI supports access control mechanisms, including multi-factor authentication (MFA), role-based access control (RBAC) and conditional access policies. These controls ensure that only authorized users can access the virtual desktop environment from allowable locations.

Secure Remote Access: VDI provides a secure solution for remote access, allowing employees to work from anywhere without compromising security. FIPS 140-2 compliant encrypted connections and secure gateways protect data in transit, reducing the risk of interception by malicious actors.

Rapid Incident Response: In the event of a cyber incident, VDI allows for quick isolation and remediation. IT administrators can easily disconnect compromised virtual desktops, investigate the issue, and restore clean environments without impacting the entire network.

High Performance Compute: VDI is capable of hosting desktops and applications with minimum system specifications (e.g. GPU) for digital engineering and mission-critical solutions (e.g. GenAI).

IMPLEMENTING VDI FOR CMMC COMPLIANCE

BOUNDARY AND SCOPE OF CMMC

VDI provides a clean boundary for protecting CUI by containing sensitive information in a centralized and compliant IT environment while prohibiting the processing, storage, or transmission of CUI by non-compliant endpoint devices. According to the CMMC Scoping Guide for Level 2 version 2.13 dated September 2024:

"An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset." (Source: DoD CMMC Level 2 Scoping Guide, Version 2.13, September 2024)

Historically, organizations have had to issue compliant endpoint devices to users operating outside the compliance boundary, such as external partners or commercial users. This often resulted in a cumbersome "swivel seat" setup, where individuals were forced to manage multiple user accounts across different physical devices: One for compliant work, and another for day-to-day tasks. Not only is this approach cost-prohibitive due to the need for additional hardware, and licenses but it also introduces operational inefficiencies and potential security gaps.

"Swivel seating" is especially risky in situations where the physical location of the CUI-containing device is untrusted or exposed to insecure networks. By contrast, VDI helps mitigate this risk by keeping the desktop environment and the CUI it contains within the secure compliance boundary. The endpoint device serves only as a conduit for input and output (keyboard, video, and mouse), with no data ever stored or processed locally. In effect, the user is simply viewing pixels, hearing audio, and sending keystrokes, dramatically reducing the attack surface and improving security without the need for costly secondary hardware.

ALIGNING VDI WITH CMMC REQUIREMENTS

Compliance with NIST SP 800-171r2 supports compliance with CMMC and other standards. To achieve CMMC compliance, organizations must implement specific security controls outlined in NIST SP 800-171r2. VDI can help meet these requirements in at least four of the fourteen control families:

Access Control (AC): VDI supports the implementation of access control policies by limiting system access to authorized users and processes. It ensures that only authenticated users can access the virtual desktop environment, aligning with AC.L2-3.1.1 and AC.L2-3.1.2.

Identification and Authentication (IA): VDI enhances identification and authentication processes by integrating MFA and secure login mechanisms. This aligns with IA.L2-3.5.1 and IA.L2-3.5.2, ensuring that users are properly authenticated before accessing sensitive information.

System and Communications Protection (SC): VDI provides secure communication channels and encryption for data in transit, meeting the requirements of SC.L2-3.13.8 and SC.L2-3.13.11. It also supports boundary protection and secure remote access, as outlined in SC.L2-3.13.1 and SC.L2-3.13.12.

Audit and Accountability (AU): VDI enables comprehensive logging and monitoring of user activities within the virtual desktop environment. This supports the implementation of audit controls, such as AU.L2-3.3.1 and AU.L2-3.3.2, ensuring that all actions are traceable and accountable.

RECOMMENDATIONS FOR VIRTUALIZATION / VDI IMPLEMENTATION

To maximize the security benefits of VDI and achieve CMMC compliance, organizations should consider the following security recommendations:

FedRAMP authorization: For VDI solutions provided as Cloud Services Offerings (CSO), the Cloud Service Provider (CSP) offering must be FedRAMP Moderate or '*Equivalent*'. For example, Microsoft Azure, Amazon Web Services, and Google Public Cloud offer FedRAMP Provisional ATOs (PA) found on the FedRAMP Marketplace. (Source**:** *FedRAMP Moderate Baseline and CSP Customer Responsibility Matrix (CRM) guidance, b*ased in part on FedRAMP Moderate Baseline documentation and standard CSP Customer Responsibility Matrix (CRM) guidance.)

Shared scope of responsibility for compliance: FedRAMP authorized cloud services include a Control Implementation Summary (CIS) and Customer Responsibility Matrix (CRM) with a shared set of security responsibilities between the CSP and the OSC. For VDI, many components are CSP-managed, but desktop session hosts and supporting services are the responsibility of the OSC. For example, the desktop hosted by VDI must be configured and managed for CMMC compliance. This may be similar to how a physical desktop is configured and managed but includes additional components for VDI such as session hosts, pools, virtual networks and conditional access controls.

Conduct a risk assessment: Perform a thorough risk assessment to identify potential threats and vulnerabilities associated with non-compliant and untrusted endpoint devices. Use this assessment to inform the design and implementation of the VDI solution. For example, if the device and VDI client originates from a prohibited location (e.g. Section 126.1 embargoed nations), conditional access policies may be implemented to block the connection.

Implement strong authentication: Enforce MFA, Role-Based Access Control (RBAC) and conditional access policies to ensure that only authorized users can access the virtual desktop environment from a trusted location/device. Regularly review and update access controls to maintain security.

Disable CUI download and print: Configure the VDI client to prohibit the clipboard (*copy-and-paste*) from the VDI desktop to the endpoint device. In addition, disable connectivity to local functions including drive, USB and printer redirection. Screen capture should also be disabled.

Note: it's possible to allow the clipboard to upload content to the endpoint should the IT risk profile allow for it.

Enable a Cloud Print Solution as Needed: It is possible to deploy a cloud printer solution that may be attached to the VDI desktop to print remotely (e.g. to a secure and compliant printer in the same location as the VDI client). One such solution is Microsoft Universal Print. This is especially useful for manufacturing companies that need to print specifications and blueprints on the shop floor. The transmission of the print data is encrypted between the VDI and the receiving printer/print proxy. This keeps any networks in the middle out of scope, only expanding the scope to the printer/print proxy and the paper CUI itself.

Configure CSP Security Services: CSPs offer security services to manage vulnerabilities, assess compliance, and strengthen the overall security of the VDI environment. Examples include Microsoft Defender for Cloud, AWS' GuardDuty, and VMWare Carbon Black Cloud. Many CSPs also offer virtual Trusted Platform Module (vTPM) support for VM hosts. Consider implementing the vTPM-enabled security features, such as Microsoft Trusted Launch.

Encrypt data in transit and at rest: Use FIPS 140-2 validated encryption to protect data both in transit and at rest within the virtual desktop environment. This ensures that sensitive information remains secure, even if intercepted. CSPs encrypt data at rest and in transit with FedRAMP Authorized offerings. However, we recommend additionally encrypting storage with OSC-managed encryption keys. For example, Virtual Machine (VM) disks may be double-encrypted at rest, with both the CSP-managed encryption keys and the OSC-managed encryption keys. Taking it another step further, internally encrypting the VM connected disks is an extra layer of that binds disk encryption keys to the VM's vTPM (e.g. Microsoft BitLocker). This encryption makes the disk content accessible only to the VM. Integrity monitoring allows cryptographic attestation and verification of VM boot integrity and monitoring alerts if the VM didn't boot because attestation failed with the defined baseline.

Implement confidential computing if supported: Confidential computing protects data in use by performing computation in a hardware-based, attested Trusted Execution Environment (TEE). CSPs already encrypt data at rest and in transit. Confidential computing helps protect data in use, including cryptographic keys. It helps organizations prevent unauthorized access to data in use, including from the CSP itself, by processing data in a TEE. When confidential computing is enabled and properly configured, the CSP cannot access unencrypted data. (*Concepts summarized from Microsoft Azure Confidential Computing documentation*)

Regularly Update and Patch: Keep the VDI infrastructure up to date with the latest security patches and updates. Regularly review and apply patches to address known vulnerabilities.

Monitor and Audit Activities: Implement comprehensive logging and monitoring in accordance with CMMC to track user activities within the virtual desktop environment. Regularly review audit logs to detect and respond to suspicious activities.

Establish maximum inactive time and disconnection policies: Sign out users when they are inactive preserves resources and prevents access by unauthorized users. We recommend that timeouts balance user productivity as well as resource usage. For users that interact with stateless applications, consider more aggressive policies that turn off machines and preserve resources. Stateless applications are applications that do not retain any information about previous interactions or sessions. Stateless applications do not need to remember what a user did last time and do not store data about the user session on the virtual machine itself. Disconnecting long running applications that continue to run if a user is idle, such as a simulation or CAD rendering, can interrupt the user's work and may even require restarting the computer.

Set up screen locks for idle sessions: Prevent unwanted system access by configuring the VDI client to lock a machine screen during idle time and require re-authentication to unlock it.

Establish tiered admin access: In most cases, do not grant users admin access to virtual desktops. If software packages must be installed, we recommend making them available through configuration management utilities (e.g. Microsoft Intune, Jamf Pro, Ivanti Endpoint Manager). In a multi-session environment, do not let users install software directly.

Consider which users should access which resources: Consider session hosts as an extension of the existing desktop deployment. We recommend controlling access to network resources the same way other desktops would in the environment, such as using network segmentation and filtering. By default, session hosts can connect to any resource on the internet. There are several ways to limit traffic, including using a firewall, Network Virtual Appliances (NVA), or proxies. To limit traffic, make sure to add the proper rules so the VDI desktops can function properly.

User profile security: User profiles can contain sensitive information. Restrict who has access to user profiles and the methods of accessing them, especially when using profile management services (e.g. Microsoft FSLogix Profile Container, VMware Dynamic Environment Manager, Citrix Profile Manager, Ivanti Environment Manager) to store user profiles in a virtual hard disk file on an SMB share. Follow the security recommendations for the provider of the SMB share. For example, if leveraging Microsoft Azure Files to store these virtual hard disk files, use private endpoints to make them only accessible within an Azure virtual network.

VDI SECURITY BOUNDARIES

Security boundaries separate the code and data of security domains with different levels of trust. For example, there is usually a security boundary between kernel mode and user mode. Most VDI software and services depend on multiple security boundaries to isolate devices on networks, virtual machines (VMs), and applications on devices. The following table lists each security boundary and what they can do for overall security, depending on implementation.

Security boundary	Description
Network boundary	An unauthorized network endpoint cannot access or tamper with code and data on an endpoint device.
Kernel boundary	A non-administrative user mode process cannot access or tamper with kernel code and data. Administrator-to-kernel is not a security boundary.
Process boundary	An unauthorized user mode process cannot access or tamper with the code and data of another process.
AppContainer sandbox boundary	An AppContainer-based sandbox process cannot access or tamper with code and data outside of the sandbox based on the container capabilities.
User boundary	A user cannot access or tamper with the code and data of another user without being authorized.
Session boundary	A user session cannot access or tamper with another user session without being authorized.
Web browser boundary	An unauthorized website cannot violate the same-origin policy, nor can it access or tamper with the native code and data of the web browser sandbox.
Virtual machine boundary	An unauthorized virtual machine cannot access or tamper with the code and data of another virtual machine; this includes isolated containers.
Virtual Secure Mode (VSM) boundary	Code running outside of the VSM trusted process or enclave cannot access or tamper with data and code within the trusted process.

Table 1.1, VDI Security Boundaries via Microsoft,
"Security Recommendations for Azure Virtual Desktop"

IT administrators need to make certain choices about security boundaries on a case-by-case basis. For example, if a user needs local administrator privileges to install apps, they need a personal (single instance) desktop instead of a shared session host. We do not recommended giving users local administrator privileges in multi-session pooled scenarios because these users can cross security boundaries for sessions or data permissions, shut down multi-session VMs, or do other things that could interrupt service or cause data losses.

Users from the same OSC, like knowledge workers with apps that do not require administrator privileges, are great candidates for multi-session session hosts (many desktops hosted on a single VM server). These session hosts reduce costs for the organization because multiple users can share a single VM, with only the overhead costs of a VM per user. With user profile management products like Microsoft FSLogix paired with Azure Virtual Desktop (AVD), users can be assigned to any VM in a host pool without noticing any service interruptions. This feature also lets organizations optimize costs such as shutting down VMs during off-peak hours.

In cases where users from external OSCs connect to VDI, we recommend isolating the infrastructure from the internal environment, such as hosting the VDI in a separate cloud subscription with a firewall configured between virtual networks. Such as the case with Zero-

Trust Architectures (ZTA), this will "micro-segment" the VDI networks to limit the blast radius when vulnerabilities are introduced.

In many cases, multi-session environments are an acceptable way to reduce costs, but whether recommended depends on the trust level between users with simultaneous access to a shared multi-session instance. Typically, users that belong to the same organization have a sufficient and agreed-upon trust relationship. For example, a department or workgroup where people collaborate and can access each other's personal information is an organization with a high trust level.

OS software (e.g. Microsoft Windows) leverage security boundaries and controls to ensure user processes and data are isolated between sessions. However, the OS still provides access to the instance the user is working on.

Multi-session deployments benefit from a defense-in-depth strategy that adds more security boundaries that prevent users within and outside of the organization from getting unauthorized access to other users' personal information. Unauthorized data access happens because of an error in the configuration process by the system admin, such as an undisclosed security vulnerability or a known vulnerability that hasn't been patched out yet.

The following table summarizes recommendations for each scenario.

Trust level scenario	**Recommended solution**
Users from one organization with standard privileges	Use a multi-session OS (e.g. Microsoft Windows Enterprise).
Users require administrative privileges	Use a personal host pool and assign each user their own session host.
Users from different organizations connecting	Separate cloud subscription

Table 1.2, VDI Trust Level Solutions via Microsoft "Security Recommendations for Azure Virtual Desktop"

VIRTUAL APPLICATION DELIVERY

Virtual Application delivery is a middle-ground security strategy that allows users to access specific applications (rather than full desktops) in a controlled, virtualized environment. In this model, the application runs on a centralized server, and only the visual interface is delivered to the user's device. The actual data and processing stay on the server, meaning the user's device never directly interacts with or stores sensitive information. For organizations handling CUI, this approach helps contain data within the application environment and minimizes the chance of accidental or intentional data sprawl.

While this method does not offer full containment of VDI, it still provides significant risk reduction. Since users interact only with the application window (and not an entire desktop) it is easier to limit functionality such as copy/paste, file download, or data redirection. This keeps CUI and other sensitive data relegated to the application itself and eliminates the need to trust the user's endpoint device. Virtual Applications are particularly helpful when users require access to a specific tool or system, but full desktop access would expose unnecessary risk. It is a scalable, cost-effective way to balance usability and security in environments where protecting sensitive data is critical.

BROWSER-BASED VIRTUALIZATION

Virtualization and browser-based limited access solutions provide a middle-ground security measure for organizations managing sensitive information. By delivering applications or desktop environments through a browser session, these solutions significantly reduce the risk of data leakage or unauthorized access. Since no data is stored locally on the end-user device and all activity occurs in a controlled, centralized environment, it limits the exposure of sensitive data to only what is needed for the session. This model helps to contain the data within a secure enclave and prevents users from inadvertently downloading, copying, or storing CUI across unmanaged or personal devices.

While browser-based virtualization is not as robust or isolated as full Virtual Desktop Infrastructure (VDI) implementations, which offer complete desktop environments with stricter controls and deeper system integration, it still serves as an effective tool to minimize CUI sprawl. It allows organizations to enforce least privilege access and limits the user's ability to manipulate or exfiltrate data. By reducing where CUI can live and how it can be interacted with, browser-based access helps organizations stay compliant and lowers the overall attack surface. It is a practical risk-reduction step, especially in environments where VDI may not be feasible or cost-effective for all users.

(Concepts from Virtual Application Delivery and Browswer-Based Virtualization summarized from Microsoft Azure, VMware Horizon, and Citrix VDI documentation.)

EXAMPLES OF VDI AND VIRTUALIZATION IMPLEMENTATIONS

The VDI and virtualization implementations are cited for illustrative purposes only and do not constitute product endorsements by the contributors or the ND-ISAC or the DIB SCC.

NAVY NAUTILUS VIRTUAL DESKTOP FOR FLANKSPEED (NVD)

The Navy Nautilus Virtual Desktop (NVD) is a service under the Flank Speed program designed for users who do not have access to government-furnished equipment (GFE). It provides a secure, virtual desktop environment that mirrors the Navy Marine Corps Intranet (NMCI)

workspace, the legacy network environment being transitioned to the Navy's Next Generation Enterprise Network (NGEN) under the Flank Speed initiative.
https://www.peodigital.navy.mil/News/Article/4124328/strengthening-digital-operations-flank-speed-and-hyperion-designated-as-don-ent/

Through NVD, users can access key applications like Microsoft Outlook, Teams, and other essential tools without being physically connected to NMCI hardware. The platform allows users to maintain their NMCI account, access encrypted email, collaborate via Teams, and manage files within a controlled and compliant environment. Access is requested via a Flank Speed account, and account creation typically takes 1-3 days.

In practice, NVD helps address common challenges like sending encrypted emails or accessing NMCI-restricted websites and documents from non-GFE devices. When logged into the NVD portal, users experience an environment similar to an NMCI machine but within a secure, isolated virtual session. File transfer to and from the portal is restricted to preserve security, but users can move files through approved services like Microsoft OneDrive. This implementation ensures that users without Navy-issued hardware can still securely access sensitive systems and collaborate effectively across the Navy network.

Source*: U.S. Navy FlankSpeed Program documentation (NVD overview, 2024)*

EXAMPLES OF REMOTE BROWSER ISOLATION (RBI) IMPLEMENTATIONS

While RBI (Remote Browser Isolation) and VDI (Virtual Desktop Infrastructure) are distinct technical solutions, both are occasionally mentioned in the context of CMMC control implementation. While the primary focus on this paper is on VDI, RBI is covered only where relevant for comparison or supplemental risk mitigation.

Remote Browser Isolation (RBI) lets users access a full desktop environment that runs on a remote server, often in a data center or in the cloud. RBI adds a layer of isolation by sandboxing or hosting browser activity in a remote container. Only safe rendering output is sent to the endpoint and the local device never directly interacts with web content. The application is usually integrated into secure web gateways or Zero Trust frameworks. No local cache/file store is allowed if the endpoint is to remain out of scope.

Using RBI can help prevent phishing and malware attacks from websites and help protect users from risky websites and help enforce secure web access policies.

PRISMA ACCESS BROWSER (PALO ALTO NETWORKS)

Prisma Access Browser is a cloud-delivered secure browser solution built into Palo Alto Networks' Prisma Access platform. It provides users with secure web browsing capabilities by

isolating web traffic in a remote, cloud-hosted browser session, so potentially harmful content never reaches the user's device. Rather than sending the actual web content to the user's endpoint, Prisma Access Browser sends only a safe, visual representation of the site, helping prevent malware, zero-day exploits, and phishing attempts from reaching the endpoint.

The solution integrates with Prisma Access' broader Zero Trust Network Access (ZTNA) model, enabling organizations to enforce granular policies around web usage and access based on user identity, device posture, and risk level. It supports scenarios where users access SaaS apps or websites without requiring full VPN access or exposing internal assets. Admins can define policies that determine which websites or categories require isolation, block uploads and downloads, and prevent clipboard or screenshot actions. Because it's cloud-native and browser-based, Prisma Access Browser doesn't require endpoint agents, making it a viable option for remote users.

Source*: Palo Alto Networks Prisma Access Browser product documentation.*

ISLAND SYSTEMS COMPLIANCE ISLAND

This solution provides a secure enclave by deploying Azure Virtual Desktop environments within an organization's Azure tenant, preferably in Azure Government and Microsoft 365 GCC-High for enhanced security. This approach can isolate different types of information (example: Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)), to help reduce the scope and complexity of compliance efforts.

An example implementation involves creating a dedicated, compliant enclave where users access secure Windows 10 desktops equipped with Microsoft Office 365. These virtual desktops are accessible via secure Remote Desktop sessions, ensuring that no sensitive data resides on local devices. The solution includes comprehensive system-specific compliance documentation, policy frameworks, and management services such as risk, change, and incident management. This integrated approach enables organizations to meet compliance requirements efficiently, often within a few days, while minimizing costs and operational disruptions.

Source*: Island Systems marketing overview (2024).*

CHALLENGES OF VDI IN MANUFACTURING ENVIRONMENTS

While VDI is beneficial in managing data security and workflow efficiency in many production environments, its applicability may be limited in some aspects of manufacturing. However, there is an opportunity to manage risk early in the process in a manufacturing environment using VDI.

LIMITATIONS OF VDI IN MANUFACTURING ENVIRONMENTS

Workflow mismatch in traditional manufacturing environments: Not all manufacturing facilities have transitioned to a fully digital workflow. Many still rely on printed data for various aspects of the production process.

Infrastructure and integration challenges: Deploying a VDI solution requires network infrastructure and compatible endpoint devices. Manufacturing sites with older or less integrated IT systems may face challenges in adopting VDI.

Cost and complexity: The initial setup and ongoing support of a VDI solution may be costly. Training and process flow adjustments may be required, adding to the overall complexity of a workflow transition.

However, even manufacturing firms with manual shop floor processes may have an opportunity for VDI:

BENEFITS OF VDI IN MANUFACTURING ENVIRONMENTS

Improved data security: When a customer sends a specification via email, the file is typically stored in the manufacturer's environment, on premise or in the cloud. Once the specification is sent for quoting purposes, the data is out of the customer's control. Using VDI, documents can be accessed temporarily in a controlled session without being permanently downloaded onto local devices or workstations. If a bid is not won, the sensitive data remains in the controlled environment and remains managed by the data's owner without leaving copies on a manufacturer's systems. Incidentally, this also lends itself to improved configuration management. Should the manufacturer win the bid, the customer provides more "permanent" access to the data, mitigating the risk of the manufacturing retrieving a previous revision and making the wrong parts.

Streamlined workflow for digital operations: On modern shop floors where operators and programmers use digital devices such as tablets, VDI provides seamless access to real-time data and design specifications.

Centralized data control and auditability: VDI facilitates detailed tracking of who accessed what data and when. This is crucial for maintaining data integrity and meeting compliance requirements.

VDI presents a compelling solution for enhancing data security and operational efficiency in manufacturing environments, particularly for digital workflows. While its advantages are best realized in environments that are already leveraging digital tools, there are opportunities for VDI to be implemented within business operations practices to help mitigate risk at different points within the workflow. A tailored approach, combining traditional methods with selective digital enhancements, offers the best opportunities.

CONCLUSION

Virtual Desktop Infrastructure (VDI) offers a powerful approach to securing IT environments, especially when organizations must accommodate non-compliant or untrusted endpoint devices. By centralizing management, isolating sensitive data, and enforcing robust access controls, VDI helps reduce the footprint of Controlled Unclassified Information (CUI) and lowers overall cybersecurity risk.

When implemented in alignment with frameworks like the Cybersecurity Maturity Model Certification (CMMC), VDI not only strengthens an organization's security posture but also provides a scalable, flexible solution for today's dynamic IT environments. As cybersecurity standards evolve, technologies like VDI also support the principle of inheritance, enabling organizations to build on existing controls rather than reinventing the wheel.

This same model is already being leveraged with Cloud Service Providers through programs like FedRAMP, and it can accelerate compliance in international or fast-track scenarios. Ultimately, adopting VDI is not just a tactical move for security, it's a strategic foundation for long-term compliance and operational resilience.

To learn more about the National Defense ISAC go to: www.ndisac.org
Interested in joining our community? Contact info@ndisac.org