CDM and VMware Workspace ONE

Responding to Today's Remote Work Challenges

End-user computing environments face unprecedented challenges in 2020. VMware Workspace ONE® provides a complete platform for productive and secure remote work.

The spread of COVID-19 has prompted all types of organizations, including federal agencies, to shift employees to remote work. As remote work continues, agencies must address cybersecurity challenges and optimize the performance of their newly expanded teleworking communities. Simultaneously, agencies face these challenges under new budget constraints.

To strengthen the cybersecurity posture of government networks and systems, the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program enables federal agencies to prioritize security risks based on potential impacts and focus on the most critical problems first. Today, the challenges are addressing the overnight surge in the number of teleworkers and confronting the adversarial tactics being used to exploit the new operating environment, all while adhering to federal cyber guidelines. To address these immediate pressing needs, agencies can use the CDM program, along with funding from the Coronavirus Aid, Relief, and Economic Security (CARES) Act, toward new investments in end-user computing technologies.

The Challenges of 2020 and Beyond

In early 2020, agency IT administrators worked around the clock to enable employees to continue their mission via telework. Many user roles, devices, and applications that were not intended to function remotely are for the first time being used to perform work outside of agency facilities.

While the initial priority was rapidly enabling work from home, attention is now turning to the security and optimization of the new environment. Workarounds, reduced visibility, and inadvertent security gaps that might have been acceptable for a few weeks during the initial emergency time period are now no longer sustainable. Malicious actors are actively seeking to take advantage of the chaos caused by the transition. It is imperative that these risks now be mitigated.

Agencies face a range of challenges. With employees accessing many more applications from mobile devices and personal devices, agencies must ensure that these devices are secure and adhere to federal cyber-hygiene guidelines. Laptops are now remote all the time, and agencies must ensure that they remain patched. The network perimeter has expanded beyond recognition, and agencies must find a way to ensure that all access requests are legitimate and that bad actors are kept out. Users are increasingly turning to cloud services for remote collaboration. Agencies must be aware of this usage and make sure that it is properly sanctioned to protect identities and data.

Malicious actors are actively seeking to take advantage of the chaos caused by COVID-19. Mitigate the risk now.

To have visibility and control over this new environment, agencies must reexamine the technology stack used to support mobile and remote employees and consider adopting modern end-user computing solutions, such as:

- Unified endpoint management for visibility and policy control on all types of mobile devices, including personal devices
- Conditional access policies based on zero trust concepts, which evaluate the context of the user, device, transport, authentication strength, app, and data before every request
- Cloud-based modern management for laptops to ensure that they can be patched and compliant no matter where they are without relying on a connection to the agency network
- Workflows to onboard new employees, provision devices, and provide ongoing support when in-person contact is limited

Integrating all these features—and more—into a holistic platform is key to achieving end-to-end visibility, from the user and the device all the way to the application and data center.

Unfortunately, these concerns come at a time when many sources of government funding are being diminished or repurposed.

Addressing Telework Technology Needs with CDM and CARES

The Department of Homeland Security created the CDM program with the goal of establishing a foundational cyber posture for all federal agencies, as well as improving visibility through aggregation and reporting of data. CDM initially focused on four capability areas: asset management, identity and access management, network security management, and data protection management. The framework gives agencies the flexibility to identify their most critical needs and then address them according to their own priorities in the context of a rapidly evolving landscape.

Beyond technical cybersecurity and management mandates, the CDM program includes a funding and acquisition mechanism that enables projects to be implemented much faster than traditional processes. CDM DEFEND (Dynamic Evolving Federal Enterprise Network Defense) task orders have been awarded to system integrators to implement CDM projects. Agencies can work with the CDM Program Management Office to drive prioritized requests for service through their CDM system integrators. This model brings the benefit of working with an integrator that is already familiar with an agency's infrastructure, standards, policies, and constraints. Furthermore, the 2020 CARES Act, passed in response to the coronavirus pandemic, can serve as a source of funding for CDM projects.

These rapid acquisition and funding support mechanisms—along with the flexibility of CDM—allow agency stakeholders to quickly implement prioritized cybersecurity capabilities as they see fit, such as platforms to address the cybersecurity and mobility challenges created by COVID.

VMWARE FOOTPRINT

- VMware Workspace ONE
- VMware Workspace ONE Unified Endpoint Management
- VMware Carbon Black
- VMware NSX

Using VMware to Support Remote Work and CDM Requirements

VMware Workspace ONE®, VMware Carbon Black, and the company's software-defined data center product VMware NSX® provide a comprehensive platform for addressing agencies' remote-work needs. This platform approach layers intrinsic security, from remote workers' devices into the agency data center, to create a holistic telework cyber posture using CDM-approved solutions. You can also extend VMware platforms to support the upstream CDM reporting requirements.

The cornerstone of the VMware remote-work offering is the Workspace ONE platform. Workspace ONE Unified Endpoint Management supports a wide range of asset management options, including solutions for BYOD and modern management of Windows 10 devices. These capabilities can directly address the security and management issues that arise from increased usage of mobile devices, as well as the challenges of managing remote laptops with traditional PC lifecycle management products.

The comprehensive Workspace ONE platform includes authentication and zero trust conditional access capabilities; policy enforcement, analytics, and automation; and the ability to integrate existing best-of-breed security investments—delivering across the full range of CDM capability areas.

VMware Carbon Black brings intrinsic security to the workspace through its cloud native endpoint protection platform. Carbon Black further addresses CDM capabilities for asset management and identity and access management.

VMware NSX, which includes microsegmentation capabilities, extends control into the data center. It addresses the risks caused by the increasing number of mobile devices accessing resources within the data center and adds layers of virtual firewalls to reduce east-west attacks. NSX addresses identity and access management, network security management, and data protection management.

By combining the Workspace ONE platform with Carbon Black and VMware's software-defined data center platform, you can address a much broader range of CDM use cases than with individual point solutions.

VMware for a Secure and Productive Remote Work Environment

End-user computing environments face unprecedented challenges in 2020. VMware Workspace ONE provides a complete platform for productive and secure remote work, and addresses the full range of capability areas defined by the Department of Homeland Security CDM program.