CTG Federal & Broadcom:

Securing and Modernizing Federal Networks Across Multiple Clouds

CTG FEDERAL

vmware by Broadcom

WHITEPAPER

Federal agencies are increasingly relying on multi-cloud IT environments to power their digital operations. As of 2024, over 90 percent of federal agencies have adopted multi-cloud strategies to enhance operational efficiency and security. This trend continues to accelerate as the Department of Defense (DOD) expands its Joint Warfighter Cloud Capability (JWCC) initiative, a program awarded in December 2022, enabling secure, multi-cloud operations.

By 2025, nearly 95 percent of enterprises have adopted hybrid or multi-cloud environments to optimize workload distribution and security. The drivers for these strategies remain clear: they provide agencies with greater flexibility, improved redundancy, and access to cutting-edge technological capabilities.

The challenge for agencies, however, is that multi-cloud environments introduce increased complexity in security, compliance, and administration. According to recent federal IT surveys, more than 75 percent of agency executives cite managing a multi-cloud environment as one of their top five challenges through 2025.

A primary concern is that each cloud service provider (CSP) enforces unique networking and security policies, leading to integration and visibility gaps. These discrepancies can cause performance bottlenecks, create security blind spots, and increase operational costs as agencies try to bridge the differences between cloud providers.

VMware NSX for Consistent Security

VMware, now under Broadcom, continues to offer NSX solutions, albeit with a renewed focus on enterprise cloud security and AI-powered compliance monitoring following the company's 2023 acquisition.

VMware NSX enables federal agencies to establish consistent security and networking policies across private on-premises and multi-cloud environments from a unified management console. This allows IT teams to be more efficient, reducing the need for redundant configurations across multiple cloud providers.

VMware NSX, remains a strong security solution, with a growing emphasis on AI-powered threat detection and compliance automation. It enhances network segmentation, prevents lateral attacks, and ensures real-time security enforcement across multiple cloud environments.

One of the key innovations of VMware NSX is network micro-segmentation, which applies security policies at each partition—effectively restricting lateral movement for attackers. Even if a security breach occurs, NSX isolates threats to prevent further compromise.

The family of VMware NSX solutions include NSX Data Center, NSX Cloud, and NSX SD-WAN:

NSX DATA CENTER

VMware NSX Data Center is a network virtualization and security platform that enables the virtual cloud network, a software-defined approach to networking that extends across data centers, clouds and application frameworks. With NSX Data Center, networking and security are brought closer to the application wherever it's running, from virtual machines (VMs) to containers to bare metal. Benefits include:

- Protection for applications with micro-segmentation at the workload level and granular security
- Reduced network provisioning time — from days to seconds — and improved operational efficiency through automation
- Consistent management of networking and security policies independent of physical network topology within and across data centers and native public clouds
- Detailed application topology visualization, automated security policy recommendations, and continuous flow monitoring
- Advanced, lateral threat prevention on east-west traffic using the built-in, fully distributed threat prevention engine
- Even if a federal agency has not yet moved to the cloud, it can deploy NSX® Data Center to unify its on-premises environments.

NSX CLOUD

When a federal agency is ready to migrate workloads to the cloud, it can seamlessly extend security and networking policies from the data center to the multi-cloud environment through NSX Cloud and treat the data center and the cloud as if it's one single environment. This capability delivers greater flexibility for agencies as they migrate applications and data from one cloud to another because they can maintain the same security and networking policies and configurations throughout.

VMware NSX Cloud delivers consistent networking and security for applications running natively in the public cloud. NSX Cloud uses the same management plane and control plane as VMware NSX Data Center, enabling a single networking and security solution from the private data center to the public cloud. Together with the VMware NSX family, VMware NSX Cloud enables a virtual cloud network, which is a software-defined approach to networking that extends across data centers, clouds, and end points. Benefits include:

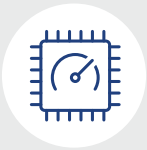
- Common networking and security across public clouds
- Greater scalability, control and visibility — with lower OpEx
- Deployment flexibility using NSX constructs or native public cloud constructs
- Simple scalability across virtual networks, availability zones, regions, and public clouds
- Precise control of security and networking services brings protection and standardization to applications
- End-to-end visibility of networking and security ensures the health and compliance of applications in public clouds

NSX SD-WAN

VMware SD-WAN essentially removes the need for dedicated, telco-managed circuits by deploying wide-area network (WAN) circuits between your regional offices as software in the cloud. All that's needed is standard ISP connectivity. So it saves agencies considerable cost by doing away with dedicated circuits, the management of those circuits, proprietary routers, and networking gear. In addition, the software-defined WAN is far more flexible and smarter in terms of how it operates, creating big benefits for highly distributed agencies.

VMware SD-WAN is built on software-defined networking principles to address end-to-end automation, application continuity, branch transformation, and security from the data center and cloud to the edge. It uses packet steering to select the best path for each application, ensuring consistent performance and overcoming quality issues and outages. Other benefits include:

Simplified WAN management with zero-touch deployments, simplified operations, one-click service insertion



Assured application performance, including transport-independent performance for the most demanding applications, leveraging economical bandwidth

Direct cloud access with performance, reliability, and security

Conclusion

Federal agencies are becoming more distributed and cloud-dependent than ever before, requiring modernized security frameworks that span across multi-cloud environments. With Broadcom's recent acquisition of VMware, NSX solutions continue to evolve with new AI-driven security enhancements, making it easier for agencies to automate security controls and simplify compliance management in multi-cloud environments.

Broadcom has a wide array of VMware solutions for multi-cloud, Kubernetes and container orchestration, and software-defined networking. Other VMware NSX-related products include: NSX Service-Defined Firewall, NSX Intelligence, NSX Distributed IDS/IPS, NSX Advanced Load Balancer, NSX-T 3.1, vRealize Network Insight, and SmartFabric Director.

To learn more about how CTG Federal and Broadcom can help, please visit www.ctgfederal.com/partners/vmware/ or contact us at contact@ctgfederal.com.

Nutanix 2024 Enterprise Cloud Index Report
https://www.nutanix.com/blog/federal-government-eci-report-2024#

About

CTG Federal, a Cohesive Technology Group company, is an SBA-certified small business that excels in servicing dozens of federal defense, intelligence, and civilian organizations with best-in-class information technology. Our experienced team of sales and engineering professionals design and deliver IT hardware and software solutions that save time and money for our customers. Headquartered in Virginia, we have dedicated resources in all regions across the continental United States.

Broadcom's VMware software manages cloud complexity so customers can modernize infrastructure, accelerate app development, and protect workloads, wherever these reside. Our private cloud solutions deliver the security and agility enterprises need, supported by solutions for applications, edge infrastructure and private AI.

Carahsoft is The Trusted Government IT Solutions Provider®, supporting Federal, State and Local Government and Education and Healthcare organizations with IT products, services and training through our partners and contracts.

Contracts

DUN & Bradstreet: 080932836
UEI: G2D4Q7UKR5P5
CAGE Code: 7ZHE9
NAICS Code(s): 541519

NASA SEWP V

Contract Number: NNG15SD12B
Group: Group B_Small Business

GSA Multiple Award Schedule (MAS)

Contract Number: 47QTCA25D003P

DOE ICPT

Contract Number: ICPT CISCO BOA 4I-30062-0008A

Dell Technologies ICPT Agreement

Contract Number: 4I-31841 Small Business

Horizon ELA

Contract Number: W519TC-25-D-A005

Smart | Secure | Scalable

(703) 278-3885
contact@ctgfederal.com
1818 Library Street, Suite 500
Reston, VA 20190

www.ctgfederal.com