CTG Federal and VMware:

Securing and Modernizing Federal Networks Across Multiple Clouds

CTG FEDERAL

vmware®

Whitepaper

Federal agencies are increasingly relying upon multi-cloud IT environments to power their digital operations into the future. More than 80 percent of federal IT decision-makers surveyed said their agency is already using multiple cloud platforms.[1] And those percentages continue to climb higher as the Defense Department pursues a multi-cloud strategy under its recently announced Joint Warfighter Cloud Capability program.

In fact, by 2022, over 90 percent of global enterprises will rely on a mix of on-premises, dedicated private clouds, multiple public clouds, and legacy platforms, according to global market intelligence firm IDC.[2] The drivers for multi-cloud strategies are clear: They give agencies more flexibility, more choice, as well as access to the newest technological capabilities.

The challenge for agencies, however, is that multi-cloud environments present added management and administration burdens for agency IT staffs. In fact, 75 percent of federal executives surveyed said that managing a multi-cloud environment will be among their top challenges in the next five years.[3]

Key among those challenges is that each cloud service provider (CSP) has its own proprietary networking and security policies, configurations, and constructs. Having disparate networking and security configurations from one cloud to the next can lead to glitches in performance or security blind spots when applications or data that reside in different places interact. Managing those different environments can be a monumental chore that expends significant staff, time, and budget resources. And it requires that IT staffs be experts in the networking and security regimes of numerous infrastructure enclaves when it comes to deploying or tweaking application workloads.

The best approach is to have a single, uniform network and security construct that applies to all operations, regardless of where a particular application is manage their applications across multiple CSPs.

VMware NSX for consistent security and networking — everywhere

VMware's NSX suite of products lets federal agencies overcome these challenges by managing consistent networking and security policies across private on-prem and public clouds from a single pane of glass.

This enables agency IT teams to be more efficient because they're handling everything as one synchronized environment. Staff require less training because there is only one set of networking and security policies and configurations to learn. And IT operations become far easier to manage and synchronize. VMware NSX also significantly improves visibility across entire operation because everything is accessible from a single screen.

VMware NSX dramatically improves security by putting all operations on the same security plane, so there are no gaps as applications or data cross from one cloud or on-prem enclave to another. In addition, VMware NSX® dramatically decreases lateral security vulnerabilities through its innovative use of micro-segmentation. VMware NSX® pioneered network security micro-segmentation by creating compartmentalized networks and applying security policies at each partition — called virtual Network Interface Controllers (NIC) — instead of just at the perimeter. That means that, if an intruder does get into the network, their ability to move freely about is severely limited because there are security gates throughout the infrastructure.

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 operations are becoming more distributed than ever before, and agencies must rely far more on cloud-based services and capabilities to keep pace. With VMware NSX solutions, CTG Federal can help your agency embrace, optimize, and secure any multi-cloud environment for the most advanced digital operations.

VMware has a wide array of 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.l, vRealize Network Insight, and SmartFabric Director.

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

About

CTG FEDERAL

CTG Federal serves dozens of federal defense, intelligence, and civilian organizations with IT expertise and solutions. We bring extensive expertise, experience, and professionalism in helping federal clients meet their IT modernization needs. Our experts keep current on the leading edge so we can provide our clients with the best solutions to s`erve their specific IT goals and objectives most efficiently and effectively. Headquartered in the greater Washington area, CTG Federal has satellite offices throughout the United States.

vmware

VMware Government Solutions provide the digital foundation for the evolution and transformation of government IT, enabling agencies to improve mission outcomes and meet constituent expectations for modern, efficient and cost effective services.

carahsoft

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
CAGE Code: 7ZHE9
NAICS Code(s): 541519

Available contracts via teaming:

- SEWP
- CIO-CS
- GSA
- DHS FirstSource II
- Army CHESS
- FAA SAVES
- DoE ICPT
- DoE SCMC
- Air Force NETCENTS-2
- Navy SPAWAR C2 MAC
- Multiple Direct Marketplace Engagements
- DLA SOE Troop Support
- 8a Small Business Direct Award
- Agency Specific BPA's & Marketplaces

CTG FEDERAL

A small business reseller specializing in Federal IT infrastructure that is scalable, secure, and affordable.

(443) 270-6535
contact@ctgfederal.com
1818 Library Street
Suite 500
Reston, VA 20190

www.ctgfederal.com

Footnotes

1 Three Out of Four Feds Say Managing a Multi-Cloud Environment Will Be One of Their Agency's Top Challenges Over the Next Five Years, Meritalk press release, Dec. 2, 2019: https://www.meritalk.com/wp-content/uploads/2020/02/JugglingTheClouds_PressRelease.pdf

2 Marco Attard, IDC: 2021 is the Year of Multi-Cloud, IDC, April 3, 2020: http://www.it-sp.eu/index.php?option=com_content&view=article&id=4631:idc-2021-is-the-year-of-multi-cloud&catid=39:cloud-computing&Itemid=102

3 Three Out of Four Feds Say Managing a Multi-Cloud Environment Will Be One of Their Agency's Top Challenges Over the Next Five Years, Meritalk press release, Dec. 2, 2019: https://www.meritalk.com/wp-content/uploads/2020/02/JugglingTheClouds_PressRelease.pdf