ZIVARO

BRILLIANT IT

Cisco Gets the Early Lead for Government SD-WAN

Glenn Smith
President and Co-Founder

INTRODUCTION:

Cisco recently announced that the U.S. government's Federal Risk and Authorization Management Program (or FedRAMP as it is commonly known), issued Cisco the In-Process designation for its Viptela SD-WAN (software-defined WAN) cloud solution. FedRAMP is the government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[1] Receiving FedRAMP's approval is an arduous but required step in order for government agencies to consume cloud-based technologies. Providers must build and operate the underlying cloud infrastructure environment with extensive policy and security controls then pass an extensive 3rd party audit against those controls.

Cisco is the first major OEM to receive the designation among SD-WAN providers, making it the early-leader to capitalize on the next frontier of networking for the federal government. In addition, Cisco has several other solutions at the FedRAMP Authorized level spanning collaboration, security and now, for the network itself.

Ultimately Cisco's SD-WAN solution holds the promise of streamlining network architecture, reducing costs, and automating network operational tasks in the name of mission speed and error reduction. The agencies that will succeed will be those that are already implementing cloud-centric transformations and recognize the network as that next evolution in their strategy.

Before we get too deep, here is a quick primer on government technology adoption.

Government agencies plan, implement, and operate technology through a similar phased approach to those conducted by private commercial organizations, but they are typically held to more stringent evaluation, selection, procurement, and compliance requirements.

Large acquisitions can take months and sometimes years to budget, plan, architect, procure, deploy and implement. This process reinforces the commitments made to certain technology stacks, good or bad, and creates more difficult hurdles once implemented for future automation or net-new integration requirements. The technology silos that can form over time constrict future flexibility from an architectural perspective.

The decision to move to SD-WAN is significant for most organizations, requiring rigid inspection and evaluation before investing in such a significant technology architectural shift which may have to satisfy interoperability with historical technology investments.

1. Fedramp/gov/faqs/

THE CHALLENGE:

The greater civilian population tends to think that the government shares the same monolithic empire of infrastructure and applications - nothing could be further from the truth.

Government agencies are not only typically siloed from one another, but their semi-autonomous sub-agencies (e.g. Department of Interior and sub-agencies such as Bureau of Land Management, Bureau of Reclamation, etc.) operate with a high deal of independence.

This independence can lead to deep-rooted technology cultures where investments in technology infrastructure (and the networks connecting them) are disparate, acquired on different timelines, and serve different mission functions making underlying commonality either scarce or nonexistent. People also often think that the government is behind the technology curve. This is a misconception. Many agencies are forward-thinking, adopting cloud and emerging technologies to solve unique challenges, and in other cases developing their own software to do the same. It's fair to say that many agencies suffer from the same challenges as commercial enterprises; advanced in certain areas and hindered by past investments and technology commits (technical debt) in others.

There, are however, some commonalities when comparing certain agencies.

The DoD (Department of Defense) and DoE (Department of Energy) share similar attributes; both have large personnel and location footprints, both require high levels of cybersecurity operations, both run hundreds of applications, and both generally have more complex IT architectures serving their missions.

In contrast, smaller agencies or sub-agencies have smaller, less-complex IT environments and less stringent cyber requirements. The difference helps paint a picture of who might be early adopters of SD-WAN – agencies with the easier path to adoption who stand to make the fastest gains from a more application-intelligent WAN.

Despite these stereotypes, the federal government has been quite adept at moving to cloud hosted and delivered applications, capitalizing on what is currently over two-hundred vendors (and counting) with approved FedRAMP cloud solutions available to consume.

The most significant partnerships to date are those with the major public cloud players AWS and Azure. These partnerships are reflected in recent headlines with the Pentagon's $10 billion JEDI (Joint Enterprise Defense Infrastructure) cloud contract awarded to Microsoft but still under appeal from Amazon.

BACKGROUND

Government agencies provide more critical services than most people know. The department of defense, for example, manages intelligence collection, missile warning, missile defense, satellite sensor command and control, and global cyber defense, to name just a few.

Adding to the list, civilian agencies manage and protect our food, land, water, and provide disaster monitoring and response among many more critical citizen and asset services.

The agencies that own these missions face the same IT-related challenges as the rest of corporate America, and ultimately gain the same benefits from building flexible, cloud-based solutions to securely connect applications and users regardless of the complex premise and cloud architectures which may be deployed.

The cloud journey is an iterative transformation of the underlying program applications to cloud-based delivery, where application performance and user experience can thrive.

SOLUTION:

Cisco's SD-WAN solution will ultimately be authorized at the FedRAMP Moderate control level, creating the ultimate network backbone for securely connecting enterprise data centers, public clouds and SaaS providers to campuses, branches and remote users.

The solution enables anyone, anywhere, to-any-application connectivity, which is the nirvana of today's multi-cloud strategies. The U.S. government has been adopting and expanding cloud initiatives for almost ten years, highlighting its willingness to create flexibility in how, where, and when its employees can access the applications and resources necessary to execute on their agency missions. The deeper opportunity for federal agencies is to provide standardization within programs to run services, and architect capabilities with speed and agility, which is where Cisco's SD-WAN solution is timely.

For example, rapidly standing up and tearing down networks at a specific global location (in response to emerging hostile activity) is a key capability needed from defense networks.
Building, maintaining, and sustaining networks are people-intensive activities, and stand to benefit from the intelligence and automation available through Cisco's SD-WAN solution. As agencies migrate applications to the cloud, having a cloud-ready WAN creates the intelligent, responsive network fabric to exponentially improve performance, scalability, policy control, and user-experience while reducing or eliminating what might be extensive manual tasks today.

Cisco SD-WAN won CRN's 2019 Product of the Year Award, honored for these connectivity capabilities improving network speed, security and efficiency.[2] Of the Fortune 100, seventy organizations are already using Cisco SD-WAN and the interest keeps growing. The primary issue preventing the government from capitalizing on the SD-WAN movement was FedRAMP authorization. With that now underway, what are the biggest benefits from Cisco SD-WAN for agencies to consider?

SECURITY: Probably the biggest advantage for Cisco is the integrated security across their other leading tools for the multi-cloud environments SD-WAN connects.
Cisco provides a complete suite of network security capabilities integrated with the SD-WAN

2. https://www.crn.com/slide-shows/mobility/crn-s-2019-products-of-the-year/20

management framework, including enterprise firewall, IPS, URL Filtering, end-to-end segmentation, advanced malware protection, SSL proxy and secure internet gateway.[3]

Customers can enable some of this functionality through routers running the SD-WAN fabric or through the Cisco Umbrella cloud. This integrated stack means simpler policy enforcement across the entire environment and a security strategy thoughtfully applied for multi-cloud requirements. The overall elegance of Cisco's SD-WAN solution is the fact that the architecture is thought out with security at all layers rather than facing bolt-on security components later.

PERFORMANCE: A primary objective of any network is application performance, and Cisco's SD-WAN solution excels at performance design. The solution addresses concerns on data loss over circuits, delay and jitter, network latency, and traffic prioritization. Cisco's WAN-Edge routers play a pivotal role in determining the quality of service delivering application performance across the WAN. They can employ QoS to prioritize more critical application traffic, as well as perform traffic-shaping and policing, further enforcing SLA objectives.

CLOUD OPTIMIZATION: Cisco SD-WAN onRamp is a multi-purpose tool allowing the SD-WAN environment to choose the best-performing path when users are connecting to SaaS applications. For connecting into cloud providers where infrastructure (IaaS) is consumed, Cisco SD-WAN automates the extension of the WAN to the public cloud to seamlessly extend the WAN fabric and apply consistent policies to those workloads. The onRamp feature for co-location automates deployment of virtualized network services in co-location facilities and consolidates internet access for branch locations using regional network hubs.[4]

MANAGEMENT: The Cisco vManage console is the cloud-based management dashboard specifically built for managing Cisco SD-WAN resources. Administrators can create the SD-WAN overlay fabric through the console to define all locations (data centers, campuses, branches, etc), perform centralized configuration, establish network and security policy definition, and provide ongoing monitoring activities. Branch locations can be configured, deployed and managed remotely including the critical security policies to secure the branch traffic. Cisco vManage brings together both NetOps and SecOps objectives through its single, role-based interface.

ZIVARO: Zivaro, Inc. provides industry-leading consulting and technology services to help clients realize measurable business value from their technology investments. Clients leverage Zivaro for a broad range of consulting, deployment, and operational support across hybrid cloud infrastructure, application development, security operations, and workforce collaboration tools. With deep roots in network infrastructure, Zivaro helps plan, build and operate complex, multi-cloud architectures with an emphasis on security policy and control for public sector and regulated environments.

Zivaro has many Public Sector customers operating mission capability in Impact-Level (IL)-2, IL-4, and IL-5 cloud environments. Our public sector clients obtain favorable Authorization to Operate (ATO) decisions based on Zivaro's securely delivered Managed Services. Zivaro has substantial skills and expertise architecting, designing, implementing, and validating complex cloud environments to meet

3. Doyle Research, Key Aspects of Security and Multicloud in the SD-WAN Transformation, 2020
4. Cisco SD-WAN Cloud OnRamp video, https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/cloud-onramp.html

mission requirements and fulfill cybersecurity requirements identified in FedRAMP policies and the DoD Cloud Computing Security Requirements Guide.

Zivaro routinely implements secure hybrid-cloud architectures and effectively operates the environments to maintain operational integrity. Through collaborative client planning Zivaro can specifically help define Identity and Access Management, Enterprise Network, Vulnerability Management, Patch Management, Security Information and Event Management (SIEM), compute, and storage requirements for public cloud architecture to ensure agency missions are secure and successful.
To further strengthen SD-WAN practice capabilities, Zivaro has partnered with Criterion Networks to provide a comprehensive and structured approach to SD-WAN evaluation and adoption. Public sector entities can greatly benefit from the Criterion Networks' cloud platform and its full suite of on-demand learning, design validation and sandboxing capabilities for Cisco SD-WAN. These as-a-service solution environments would also serve as developer environments for ongoing release/software testing addressing the full lifecycle needs.

Criterion Networks offers an industry-leading Enablement Cloud to accelerate network transformation strategy, called the Criterion SDCloud® platform. Through the platform Zivaro can help customers build custom test and evaluation environments to meet lifecycle needs across learning, planning, design, proof-of-concept, deployment and operations. The Criterion SDCloud® platform supports requirements for all networking use-case solutions of interest including SD-WAN, Security, VNS, Container Networking and 5G Network Services. Given the complexity and unique attributes from agency to agency, the Criterion platform is purpose-built to help entities really evaluate features and obstacles on the path to full SD-WAN adoption.

CONCLUSION:

We all stand to benefit as citizens and consumers of government services from advancements in the capabilities of our underlying federal and state agencies. Cisco SD-WAN offers a tremendous opportunity to accelerate the quality, security, efficiency and delivery of applications for employees and citizens to leverage. With the hurdle of FedRAMP authorization nearly complete, our government agencies can now begin the next major transformation underway in enterprise infrastructure.