SD-WAN Delivers Reliability and Efficiency for the Public Sector

velocloud™
Now part of VMware

The modernization act is driving network innovation

The time to modernize government agency networks is here, yet many agencies have been struggling to carry out their missions using outdated IT infrastructure. With the Modernizing Government Technology (MGT) Act, federal agencies have a mandate to modernize their applications and networks and to serve both office workers and those in the field. Many government agencies have been planning their IT initiatives and searching for solutions. Upgrading the network has been a critical focus point.[1]

The General Services Administration (GSA) is helping agencies move forward with network modernization, and they are encouraging the use of software-defined wide area network (SD-WAN) and 5G technologies. The GSA is also warning them not to delay. On March 31, 2020, the GSA will limit the use of the extended contracts for agencies that have not made a task, delivery, or call order for supplies and/or services placed against an established contract, blanket purchase agreement (BPA), or basic ordering agreement to vendors for delivery of a solution.[2]

Cloud services and SaaS

A requirement to increase access to applications and cut costs has come with the mandate to modernize. This means that agencies are moving to modern applications in the cloud and getting away from outdated applications that run on servers in the local office. The goal with the migration to the cloud is that government workers can quickly and easily access their applications from any office or from remote sites using mobile devices.

To comply with the mandate, the Air Force wants to accelerate its use of software as a service (SaaS). They are implementing Microsoft Office 365, as they want to be responsive to the needs of users and make their applications more available. The Air Force recognizes the need to keep current with the capabilities that a modern cloud application can bring.[3]

Likewise, the Army Corps of Engineers has decided to accelerate cloud adoption. As the Corps shifts to a more mobile workforce, it is increasingly turning to SaaS tools so that users can access the data they need wherever they are.[4]

1. https://fedtechmagazine.com/article/2017/12/how-mgt-act-will-spur-agencies-it-investments-2018-and-beyond
2. https://fedtechmagazine.com/article/2019/05/where-do-agencies-eis-network-transition-plans-stand
3. https://fedtechmagazine.com/article/2019/05/air-force-wants-accelerate-saas-deployments
4. https://fedtechmagazine.com/article/2018/03/why-army-corps-engineers-believes-saas

KEY TAKEAWAY

According to the Federal IT Dashboard the federal government is planning to spend about $87.7 billion on IoT in fiscal 2020.

IoT is having an impact on the network

The Internet of things (IoT), which allows devices to link and exchange data, is a particular focus in the effort to modernize and spending on it is growing. The federal government is planning to spend about $87.7 billion on IoT in fiscal 2020, according to the Federal IT Dashboard.[5]

According to analysts from the Immix Group, by 2021, over 20 billion Internet-connected devices worldwide will make up a market for IoT worth over $2.5 trillion. Government agencies will be a large part of this market.[6]

As the number of IoT devices grows, the network must grow with it and the network capabilities must expand to handle the vast amounts of data generated in remote locations. This is creating the need for edge computing capabilities in the network.

Traditional PSTN services are going away

Telecom providers want to decommission legacy telecom services on the public switched telephone network (PSTN), and they are petitioning the Federal Communications Commission (FCC) for permission to do so. Telecom providers will migrate their offerings to over the top (OTT) applications, and this will accelerate the need to decommission legacy private branch exchanges (PBXs) deployed at government offices. It's time for federal agencies to move to voice over internet protocol (VoIP).

Security requirements change with access to the cloud

With increased access to the cloud, the nature of the network has changed. There is a need for more connections to the Internet and additional peering between networks. As a result, new types of security must be implemented. There is also a need for security services on the remote device, both natively, as well as the ability to run applications locally, and link to security services in the cloud. This requires a rewriting of the rules for network connectivity. Fortunately, progress is being made.

On Dec. 14, 2018, the Office of Management and Budget (OMB) issued draft guidance that updates the Trusted Internet Connection (TIC) program, giving agencies increased flexibility to maintain secure Internet connections. The new policy allows agencies to use modern security capabilities and ensures that the initiative is "agile and responsive to advancements in technology and rapidly evolving threats," according to the draft.[7]

Video and multimedia require network changes

Organizations are increasingly adopting video conferencing and multimedia applications, and each of these need more bandwidth, which their existing network services cannot provide.

The network needs to modernize to serve the cloud

The performance of these new applications will rely on a WAN that can reliably connect to applications with good performance. This effort is going to stress legacy networks that weren't built to handle applications in the cloud. This situation is made worse if the applications are hosted in just a few regional cloud data centers, increasing network latency.

5. https://itdashboard.gov/
6. https://blog.immixgroup.com/2018/10/26/yes-the-public-sector-is-embracing-iot/
7. https://fedtechmagazine.com/article/2018/12/omb-revamps-tic-program-boost-agencies-flexibility

KEY TAKEAWAY

By 2021, over 20 billion Internet-connected devices worldwide will make up a market for IoT worth over $2.5 trillion.

Many agencies have admitted that their networks are outdated and in need of an upgrade. Agencies must update their networks to succeed with a migration to the cloud. A modernized network is necessary so that agency personnel can access these applications securely and enjoy a high-quality experience, even when using their mobile devices.[8]

Legacy networks won't enable the transformation

Agencies won't be able to efficiently complete a digital transformation if they are using a legacy network approach. A legacy network is expensive to change and manage. Upgrading requires buying more expensive legacy routers. The traditional network is bandwidth constrained. It won't serve the needs of newer applications. The legacy network uses an inefficient topology where traffic is taken to the data center and then out to the cloud.

Backhaul is expensive and ineffective. Branch breakout is difficult to manage and does not provide optimization. Many public sector organizations don't have a lot of IT staff to get things done. They need an easy way to manage devices and a solution that provides streamlined access to the cloud, increased performance, and allows for policy-based networking.

As agencies depend more on applications in the cloud, they need reliable access, without outages; dual links from remote locations; traffic steering over the best link; service chaining to services in the cloud; and a way to ensure that VoIP traffic gets priority. On top of this, they need to be able to integrate security with access to applications on the Internet.

This requires a new type of networking. Both physical and virtual appliance choices are needed. There needs to be the option for a network functions virtualization (NFV) infrastructure for fast deployment of devices in remote locations, with a centralized orchestration system that can easily manage all devices. Data management and analytics, especially around application performance, are important. There also needs to be a way to manage IoT data from remote sensors.

SD-WAN is the solution to network modernization

The Defense Information Systems Agency (DISA), which provides IT and secure communications services across the Department of Defense (DOD) and military service branches, is exploring how the Pentagon can modernize its networks through software-defined networks. DISA thinks that SD-WAN will help make the DOD's networks more secure and flexible, and less expensive to deploy and manage, according to Lt. Gen. Alan Lynn, DISA's director. This technology offers partner agencies and foreign governments better control and sharing of the network, so they are more likely to participate in joint activities that involve sharing of information.[9]

8. https://fedtechmagazine.com/article/2017/12/why-network-must-lead-it-modernization-charge
9. https://fedtechmagazine.com/article/2017/11/why-sdn-hot-pentagon

Indications that you need SD-WAN

When evaluating SD-WAN, there are several events that indicate that it is a good solution for network modernization. If your public sector organization is doing any of the following, SD-WAN could be the right solution for your modernization initiatives.

- Aggressively moving applications to the public cloud as a part of a federal initiative
- Using SaaS applications, such as Microsoft Office 365 to reduce the load on IT staff
- Seeking to reduce the operational complexity of the existing WAN to better serve remote locations
- Looking to improve the cost, performance, and availability of the WAN
- Negotiating a contract renewal with a network service provider for WAN services
- Refreshing WAN edge devices, such as routers or WAN optimization controllers
- Supporting many small to midsize field sites and remote or mobile connections
- Looking to reduce operating costs by embracing automation of network services
- Deploying video or other high-bandwidth, real-time applications to remote locations
- Seeking to maintain limited or no IT personnel on-site in remote locations

Benefits of SD-WAN for federal agencies

Budget Stability – SD-WAN provides a predictable operating expense model that makes annual budget planning easier. Since SD-WAN is available as a virtual appliance and as hardware on a subscription, upgrading technology across the entire deployment is simple and fast. This means that the phase-out of hardware isn't necessary, as software updates keep the network operating with the latest technology and devices can be replaced as needed with a simple upgrade.

Flexibility – SD-WAN makes integration with the network simple. Integrating a new edge application or cloud platform or adding a new data center won't disrupt the network performance. SD-WAN enables speed and greater adaptability for new technology.

Transformation – The capability to integrate with multiple platforms—from security and IoT to 5G and new learning platforms—can make all the difference. SD-WAN makes this a possibility for government agencies by enabling them to use the latest technologies. This means agencies can adopt the newest platforms and have confidence they'll get the performance they need from their network.

Multi-Vendor Environments – SD-WAN platforms are built to handle multi-vendor network environments. With an agnostic approach, your network can connect to different carriers, specific applications for agency headquarters, classrooms, and diversified security appliances based on the clearance level of each location.

Globally Managed – SD-WAN comes with a simple orchestration layer that makes management more accessible and effective than ever. No matter how many locations are connected to the network, a single management platform can initiate changes, update configurations, change carrier preferences and review overall reporting. This allows IT departments to manage remote locations without having to be on-site.

VMware SD-WAN

Edge devices reliably connect sites and reduce costs

A VMware SD-WAN™ by VeloCloud® deployment starts with placing a VMware SD-WAN Edge device at each location, such as a branch office and a larger hub device in the data center. VMware SD-WAN Edge devices are available as a hardware appliance, a virtual instance that can run on common hardware, or they can run as a virtual instance and a universal customer premises equipment (uCPE) from various vendors. With the virtual appliance model, the VMware SD-WAN Edge device can be deployed as software over the network and installed remotely.

The VMware SD-WAN Edge connects sites to the WAN and to the Internet. It connects to where the applications are, whether in data centers, hosted at a service provider or in the cloud. A smaller device at the remote location communicates with the larger hub device in the data center to deliver optimized traffic between them.

VMware SD-WAN Edge devices are auto configured so it's quick and easy to install them. The cost to deploy these devices is much lower than with a typical router that must be configured manually device by device. The VMware SD-WAN Edge devices offer flexible deployment options to fit with any device management plan. They can coexist with a switch or router to support a legacy connection. The VMware SD-WAN Edge can be the default device and failover to the L2 device using the Virtual Router Redundancy Protocol (VRRP). It can coexist at Layer 3 and use a routing protocol such as Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF) and failover to the router.

The VMware SD-WAN Edge devices can be standalone and replace the existing router, if it is time to replace it. This can lead to greater cost savings by eliminating the router.

Centralized VMware SD-WAN Orchestrator eases device management

The VMware SD-WAN Orchestrator manages the provisioning of the VMware SD-WAN Edge devices, saving time in setting up new sites and in keeping devices configured correctly. The VMware SD-WAN Orchestrator makes it easy to push out a predefined configuration and avoids the need to access each device and type in commands, like with older systems. Together, they handle your application traffic effectively.

The VMware SD-WAN Orchestrator does health checks on the VMware SD-WAN Edge devices and it can restore configurations that are out of spec. This means that devices can operate at their best and if something happens, it can quickly be put right. The VMware SD-WAN Orchestrator is available from the cloud, hosted by VMware or it can be installed on-premises for deployments where the highest levels of control and security are required.

VMware SD-WAN Gateways are an on-ramp to the cloud and SaaS

A design benefit of the VMware SD-WAN solution is high performance access to hosted applications. This is done by connecting remote locations thorough a VMware SD-WAN Gateway to applications in the cloud. The VMware SD-WAN Gateway can be hosted by VMware, by a service provider or by the organization that is using it if that is required for additional security and control.

Instead of a connection going back to a legacy data center location and then going out to the cloud hosted application, the traffic is sent directly to the application in the cloud. The VMware SD-WAN Gateway provides optimization between it and the VMware SD-WAN Edge device in remote locations.

In this way the VMware SD-WAN Gateways are an on-ramp to the cloud. They provide faster, more reliable access to cloud hosted applications by handling traffic coming in over multiple links and providing mitigation for network issues.

VMware SD-WAN provides you with two options for connecting. You can connect over the Internet using Internet protocol security (IPSec) for a secure connection without any VMware SD-WAN device on the other end. With this option, you get optimization between the branch VMware SD-WAN Edge device and the VMware SD-WAN Gateway. You can also do an optimized connection using VMware SD-WAN and connecting with a virtual edge in the cloud. The VMware SD-WAN Edge device is available on the popular cloud marketplaces such as Amazon Web Services (AWS) and Azure.

Security, virtual appliances and service chaining

The VMware SD-WAN solution provides several ways to implement security. There is a built-in firewall on the VMware SD-WAN Edge device that provides adequate security for less secure sites.

A software firewall can also be installed as a virtual network function (VNF) using the network function virtualization (NFV) infrastructure. VMware has partnered with many vendors of firewalls and tested the integration of these services.

Traffic through the VMware SD-WAN Edge device can be directed to security services in the cloud using the built-in service chaining capability. These cloud security services can provide many types of protection, such as URL filtering, firewalling or access control. Automated configuration of the tunneling to the cloud sites eliminates the need for site by site configurations. Single-click application-aware policies can be used for service insertion so that you can ensure the security of traffic going over the Internet.

Network segmentation and data isolation

VMware SD-WAN provides segmentation to ensure traffic isolation and security. Segmentation can be used to extend logical connections from the VMware SD-WAN Edge device to the enterprise data center. Segmentation can be done using virtual local area networks (VLANs) or virtual routing and forwarding (VRF). Network services such as quality of service (QoS) and firewall policies can be set per segment. If the network services multiple agencies, their traffic can be isolated. The solution provides for overlapping IP addresses as well, so no changes are required for addressing.

With VMware SD-WAN, data can be identified by its type, such as payment card information, which is commonly used in commerce. Selected data can be isolated from other types of data to protect privacy and prevent fraud. This can be done with segment aware policies. You can set policies to isolate guest WiFi traffic or to isolate point of sale system data. You can configure multi-segments, for example, if you have a department for which you need to provide secure access to an application. If your company acquires another company and you need to provide overlapping IP addresses, you can do that, too. Network services such as QoS and firewall policies can also be set per segment.

Visibility, monitoring, continuous diagnostics and mitigation

The VMware SD-WAN Orchestrator makes it easy to monitor your devices and the performance of your applications on the network. The VMware SD-WAN Orchestrator can save hours of time spent on device management because it can configure all devices at once from the central console using policies. It is used to set policies for prioritization of applications on the network to make sure that your most important applications get the top priority. The VMware SD-WAN Orchestrator provides a user interface to monitor the performance of network connections and of your applications, so you can see the benefits of VMware SD-WAN firsthand. The VMware SD-WAN Orchestrator can be used to provide continuous diagnostics and mitigation. The application monitoring features in the VMware SD-WAN Orchestrator will allow you to troubleshoot issues in much less time, preventing poor application performance and saving you on application downtime.

Using the VMware SD-WAN Orchestrator, you can:

- View overall health of a remote site
- Quickly assess link quality
- Drill down on application usage to see what applications are consuming bandwidth

IoT and real time edge processing

IoT requires real time processing of data traffic, such as control data, and summary reports. Edge computing is required for efficient processing of IoT data. Edge computing involves putting services in the branch offices, allowing for distributed compute at locations close to where the data resides. The VMware SD-WAN Edge device has capabilities for edge compute and the processing of IoT data. By enabling IoT processing at the edge, agencies can save on bandwidth and core processing and have more timely data provided to them.

Why VMware SD-WAN

VMware has worked with many government customers, including the Food and Drug Administration (FDA), Federal Reserve, General Services Administration (GSA), and the Federal Aviation Administration (FAA). We have government sales specialists who understand your requirements. VMware can work with your agency over the evaluation and purchase cycle. VMware has technical experts who can help with doing a proof of concept (POC). We can provide solutions architects to help with the network design.

VMware SD-WAN components can be installed on-premises for added security and compliance with agency regulations. We can handle large scale, complex deployments to meet the needs of the most demanding projects.

VMware has experts who can train agency IT staff to ensure that they can take over and manage the deployment successfully. We have extensive staff to provide post-installation support to ensure that the deployment is reliable and performs well. VMware stocks spare devices and components in depots for fast delivery in the case of an equipment failure.

VMware SD-WAN is sold by approved suppliers with an EIS contract. Our resale partners include AT&T, Mitel, Harris and Dell.

For more information visit, *www.velocloud.com*

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2020 VMware, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: sdwan-650-sdwan-delivers-reliability-efficiency-for-public-sector-so-0220 5/19