Market Connections®
Research you can act on.

JULY 2021

Finding the Best Way to Securely Connect the Modern Hybrid Workforce

EXECUTIVE SUMMARY

The 2020 pandemic response significantly impacted the budgets of state and local governments. As a result, they're now facing the challenges of reduced tax revenues, increased expenditures for unemployment assistance, and an increased need to deliver services digitally.

For leaders in government IT, this new economic reality, as well as the historic expense of running technology in-house, is driving the move to a cloud-smart approach that can increase efficiency in both operations and budgets.

PRESENTED BY

CISCO

PREPARED BY

Market Connections, Inc.
11350 Random Hills Road, Suite 800
Fairfax, VA 22030
TEL 703.378.2025
www.marketconnectionsinc.com

SHARE THIS STUDY

This focus is not entirely new since governments have been shifting apps (like email) to the cloud for some time. Yet it's clear the pandemic response is accelerating the IT modernization in government that was already in process, especially in regard to facilitating a modern hybrid workforce. Equally clear is that this will impact the future of IT transformation.

To learn from, and apply the results of, the government IT response over the past year, we asked the following questions:

- What did IT teams learn from rolling out 19 million branches overnight and transitioning to a fully remote workforce?
- How will those learnings help agencies secure resources as they implement a hybrid work environment over the next few years?

To help answer these questions, Cisco commissioned market research firm Market Connections to explore where vulnerabilities may still exist and what steps should be taken next.

THE PRE-PANDEMIC SHIFT

Before examining the pandemic lessons specifically, it's important to look at what was already happening within the IT environments of state and local government.

For years, they have been adopting cloud-based applications and technologies to power remote work and improve responsiveness to the needs of citizens. As they did so, fewer applications were being run from their own data centers. Instead, they were running in cloud environments like Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP).

This shift to a multi-cloud approach for application management (on-prem, off-prem, and cloud-based) has had several impacts on their IT infrastructure. Network security has been forced to respond by also shifting to the cloud as users, their data, and their connected end-devices leave the physical office. The need for reliable and secure access anywhere, anytime has become clear with all the newly connected end-devices. State and local governments are also having to find new ways to deal with the growing network workloads. This includes simplifying management, increasing efficiencies, and holding a line on costs.

One thing has become clear—a centralized security approach is no longer practical. Unnecessary backhaul costs and decreased performance due to exploding user traffic, as well as data latency issues, have demanded a response that moves security closer to the edge. And that security must be holistic, providing deeper visibility into the behaviors of users, such as what applications and areas of the networks they're accessing.

Traditional virtual private networks (VPNs) that have long been a favorite for securing remote access, have also been more frequently exploited in recent years. Unless they offer strong security that is part of a larger, holistic approach, VPNs may fail to serve state and local governments well in our evolving zero trust world [1]. At the same time, running Internet traffic through a security stack is important. Endpoint security technologies like Cisco Secure Endpoint have evolved since the "anti-virus" days, and they offer highly advanced capabilities to protect users from hackers and their exploits.

[1] Source: CISA Alert (AA20-073A): Enterprise VPN Security. Updated April 15, 2020. Website accessed May 18, 2021: https://us-cert.cisa.gov/ncas/alerts/aa20-073a

TOP FINDINGS

One question that is still unanswered is whether state and local government employees will continue to work remotely once safe and trusted workplaces are available. While respondents expect the majority of staff to return to the office, it is likely that significantly more people will decide to work remotely in the future due to the flexibility it provides them.

According to the survey, only 5% of respondents expect to go back to the office full time. The majority (67%) will work remotely three or more days per week, and 28% will work remotely one or two days per week. The establishment of such a long-term hybrid work environment will impact security. It is critical for state and local governments to understand how and respond proactively.

The survey also reveals that only 11% feel their cybersecurity posture remained secure, safe, and strong over the last year. Nearly two-thirds (62%) say remote work has somewhat or greatly increased vulnerabilities and another 28% say it has stayed about the same. Yet, despite the increased vulnerabilities, 41% say the pandemic didn't affect the agency's cyber plans. While these responses seem to contradict each other, agencies may have been planning for better security around remote work prior to the pandemic and recognize there is still much more to do.

Nearly All State and Local Government IT Employees Expect to Continue Remote Work

2/3 expect to work remotely **3+ days** a week

1/4 expect to work remotely **1-2 days** a week

And only **5%** expect to go back to the office **full time**

Another question is what methods IT managers are using to protect remote workers' computers and devices from threats. The majority (69%) require an endpoint security agent on every device—a surprising finding considering that means almost one third of respondents are leaving some devices unprotected. Two thirds are protecting computers and devices via direct Internet access with some cloud-based security (such as cloud email security, secure Internet gateway, and multifactor authentication).

A Hybrid Work Environment Will Continue to Impact Security

NEARLY **2/3** say remote work has **increased vulnerabilities**

Accessing Government Applications Securely

AMONG STATE AND LOCAL REMOTE WORKERS

1/3 of respondents are **allowed to access** some cloud-based applications **without VPN**

2/3 of respondents are **required to log into agency VPN** for all government applications

Agencies are also leveraging VPNs. Two thirds of respondents (65%) say they protect remote workers' computers and devices from threats by VPN backhaul using their own security infrastructure. And for 66% of respondents, remote workers are required to log into the agency VPN for all government applications. But one third (34%) allow remote workers to access some cloud-based applications, like Office 365, without going through the agency VPN.

One state government respondent said: "Because of COVID-19, the majority of IT related work is happening remotely and the same is the case with us. Hence safety, security, flexibility, and efficiency of our department's IT infrastructure becomes much more important. The VPN connection for employees to be able to connect to the network needs to be extremely secure and should have the ability to handle the load of hundreds and thousands of employees."

While this is a typical response to the primary decision to use VPN, it is not the only option, nor is it the most user friendly and cost effective, especially as more workers continue working remotely.

HOW SASE ADDS VALUE

"I feel there is a gap in the industry for cost effective tech tools to support VPN, security, and related issues." —COUNTY GOVERNMENT RESPONDENT

The secure access service edge (SASE) concept was originally defined in 2019 with Gartner. It works by combining modern SD-WAN networking with cloud-based security like web content filtering, cloud-delivered firewall, cloud access security broker, and more. The pandemic cemented the need for a SASE approach because it can add value for governments by improving security, efficiency, and user experience.

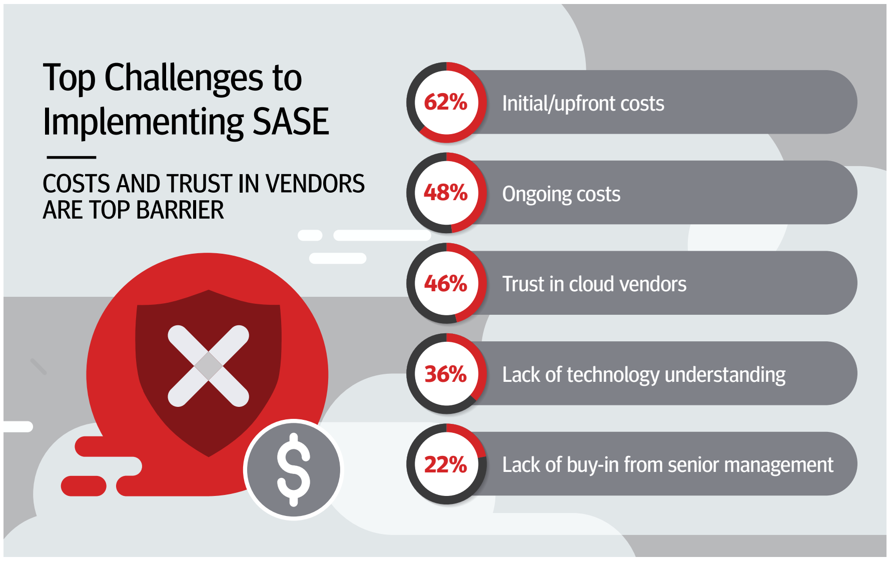
"The data shows that two out of three agencies are spending too much money, placing too much load on their VPN, and degrading the remote user experience," said Steve Caimi, Cisco Industry Solutions Specialist for U.S. Public Sector Cybersecurity.

He adds that securely connecting a hybrid workforce is not about eliminating VPNs—they are an important security tool. SASE allows agencies to limit VPN use to those who absolutely, positively need it. SASE means there are fewer VPN ports and boxes to buy and maintain, preventing potentially harmful Internet traffic from accessing an internal network. Plus, there is an overall better user experience.

When considering an IT provider (including SASE vendors) to help them meet cyber goals, respondents cite several factors as being important. None of the top three are surprising: flexible pricing/usage models (69%); advanced, modern security capabilities (69%); and ability to leverage existing investments (67%).

Other top considerations revolve around the vendor's flexibility and agility, including the ability to secure all users and devices anywhere (64%) and the ability to manage a mixed environment (61%).

The top challenges and barriers to implementing SASE mirror the top considerations. Initial/upfront costs are the biggest barrier (62%). Almost half of respondents also cite ongoing costs. Trust in cloud vendors (46%); lack of technology understanding (36%); and lack of buy-in from senior management (22%) are also barriers. Caimi notes it is interesting that cost is perceived as the top challenge when SASE is actually cost-effective within the overall cyber strategy.



SECURING CONNECTIVITY IS MORE IMPORTANT THAN EVER

> **"Future generations would see more cloud integrations, more need to make everything secure."** —CITY GOVERNMENT RESPONDENT

The data shows respondents are not interested in ripping and replacing existing technology. And they don't need to. Nor do they need to move everything to the cloud. In fact, securing certain assets with traditional tools will often serve the agency better—which is the benefit of SASE.

SD-WAN provides the network at a fraction of the cost of Multiprotocol Label Switching (MPLS), and cloud-based security can effectively connect government workers with the systems they need. SASE provides secure connectivity to applications, data, and SaaS resources, regardless of where they reside.

SASE is a cost-effective choice as it allows you to go directly to the cloud instead of routing all traffic back to the headquarters via VPN. But network elements are important too because many state and local governments have applications at headquarters running in their data center. Users need to be able to access those applications using a secure method like a VPN. The VPN also provides a secure path to centrally control security on remote devices. The network will continue to be relevant for most agencies because they are going to retain applications and data inside the enterprise. In general, the fastest, most efficient, and secure paths will be used. But these are risk-based decisions that will have to be made by the network administrator by giving them the ability to direct traffic granularly and with path optimization. That means the elements of network security, like visibility into the network traffic and internal segmentation, matter.

The key is to be "cloud smart." This means creating a manageable approach that recognizes both premise-based traffic and cloud traffic—then provides the optimal path, based on cost, efficiency, and user experience, for every packet. Cloud smart is the future of government IT, especially as remote access expands. Why? Although cloud solutions offer many benefits such as rapid deployment, flexibility, and ease of use, some agencies may decide cloud solutions don't fully address their needs for all applications. They may choose to keep some on-premises to save money, control security, accommodate legacy applications, or for other reasons.

CONCLUSION

Successful cyber programs effectively manage risk. As state and local governments transition to a hybrid work environment requiring cloud-based applications, their networks are open to more risks. Adopting a SASE approach lets you better manage those risks by enhancing your cyber program, reducing costs, and improving your user experience.

By implementing SASE, leaders in government IT can optimize the delivery of services to users, keep agency and citizen data more secure, and even positively impact citizens' faith and trust in government. These outcomes will expand, change, and evolve over time as your community of users changes or unexpected events occur. That's why it is so important to avoid "checkbox compliance" and focus on flexible actions you can start today and that will evolve with your program.

It is important for state and local government IT leaders to understand that VPNs are not the only option. It often makes little sense to push all traffic through the state agency and then out through the Internet. When more government workers eventually go back into the office, agencies may want to choose whether to optimize the path so traffic can go through the VPN or connect users directly to applications like Office 365 and their other cloud apps using a SASE approach based upon agency needs. Managing and securing traffic in a unified, automated environment is important as you direct the best path for each packet.

As state and local governments seek to secure IT networks in transition, it is critical that they partner with an experienced and trusted provider of IT services and solutions. By leveraging the value of the private sector, the public sector can speed the shift to a multi-cloud environment while preserving the value they've already invested in their on-premise infrastructure, and together, build the next-generation of government to better serve the people of their communities.

ABOUT THIS STUDY

The blind, online survey of 300 state and local government IT decision makers included 42% state government, 34% city/municipal government, and 24% county government respondents. The population of nearly half (47%) of state respondent's states was more than 10 million and was 5 to 9.9 million for 30%. Nearly one third (32%) of county respondents are in counties with populations of 1 to 4.9 million, and 60% were under 1 million. These numbers are similar for city governments: 34% and 61%, respectively. All respondents have some involvement in their government's IT operations and management and IT security solutions and services: 48% are on a team that makes decisions; 41% manage or implement solutions; 39% develop solution requirements; 38% evaluate or recommend products and services; 38% assess risk and identify improvement areas; and 31% make the final decision.

ABOUT CISCO

As the largest enterprise cybersecurity company in the world, we lead the way with solutions that are driving the industry in SASE, XDR, and zero trust. Integrating it all is Cisco SecureX, our security platform that provides simplicity, visibility and efficiency across your security infrastructure.

Learn more about how Cisco can help you on your SASE journey by visiting www.cisco.com/go/SASE

ABOUT MARKET CONNECTIONS, INC.

Market Connections delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations, and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications; healthcare; and education.

For more information visit: www.marketconnectionsinc.com

DOWNLOAD THE WHITE PAPER AND INFOGRAPHICS

www.marketconnectionsinc.com/cisco-modern-hybrid-workforce/

SHARE THIS STUDY