# The New Work Reality: Securing Remote Access for the Long Term

## MARKET TRENDS REPORT

govloop paloalto NETWORKS | verizon

# Executive Summary

Remote work has been gaining popularity among federal agencies for several years, but the current pandemic has put it front and center. As a result, many agencies are preparing for a future where telework will be a viable option for everyone. To make that happen, they must find ways to deploy more scalable, secure solutions that support remote workers.

While many agencies have long had technology in place to allow for sporadic teleworking, those technologies often don't support the cloud-intensive work environment employees must interact within daily. Today, agencies need more than remote access — they need secure access to cloud applications and the internet that employees can safely use on their mobile device of choice.

To help agencies meet these goals, the federal government has worked hard to upgrade its Trusted Internet Connections (TIC) guidance. The latest version provides use cases just for remote workers. By combining TIC guidance with the right tools, technologies and approaches, agencies can provide the type of flexible, scalable and secure access their remote users need.

To learn more about how agencies can best accommodate a growing number of remote workers, GovLoop teamed with Palo Alto Networks, which offers a cloud-delivered secure remote access solution, and Verizon, which helps organizations prepare their networks to accommodate large-scale remote workforces. This report will discuss the challenges agencies are facing in accommodating a growing number of remote workers without compromising on performance, manageability and security, and how to best address them.

# By the Numbers

68%

**of teleworking employees want to increase their telework.**

51%

**of federal data in the cloud is considered sensitive.**

34%

**growth is expected in software-defined wide-area networking, or SD-WAN, tools by 2023.**

78%

**of security teams plan to deploy zero-trust network access.**

30%

**of public sector agencies currently have a formal zero-trust approach to IT security.**

63%

**of cyber incidents are caused directly by employees through accidental disclosure, social engineering scams, inadvertent ransomware infection and even malicious intentional behavior.**

**"In the federal enterprise of tomorrow, we know there's going to be more work performed off the enterprise network than on it. We know there's going to be more workloads running in the cloud than through traditional data centers, and more traffic in the cloud than in the data center itself. What's exciting to me is how we're moving the [TIC 3.0] program forward to support those enterprise solutions of tomorrow.**

– Sean Connelly, TIC Program Manager, Cybersecurity and Infrastructure Security Agency (CISA), Homeland Security Department (DHS)

# Remote Work Shows Need for a Better Approach

## Challenge: Performance, Latency and Security

Remote employees need the same secure access to applications and data as office-bound workers. Typically, agencies have been able to provide access to internal network resources and the internet for remote users by using remote access virtual private network (VPN) devices combined with mobile device management (MDM) for policy enforcement.

In times of major growth or event-based activities — like the current pandemic — this model falls short. When demand increases significantly, the remote VPN device can quickly reach a saturation point.

"Enterprises typically don't account for having 100% of their traffic committed to a VPN at any given time. So when the need arises, the system can overload quickly," said Dan Beaman, a district manager at Palo Alto Networks.

With the traditional VPN model, latency becomes a bigger issue when demand is high because it essentially forces all traffic, regardless of destination, through the VPN concentrator. The combination of limited geographical redundancy of access points and limited bandwidth at the internet access point can cause bottlenecks.

Cost is another unanticipated concern. Organizations typically buy enough VPN licenses for a certain percentage of the workforce to work concurrently, but in times of major spikes, those licenses don't go very far. That may cause an organization to have to buy more licenses very quickly.

Explosive demand and growth can stretch VPNs to the limit. For example, if users get frustrated enough by performance and access issues, they may choose to bypass the VPN and go directly to the internet, risking exposure. In other cases, misconfigurations may create unintended vulnerabilities that could allow users to unintentionally share sensitive data with those who shouldn't have it.

## Solution: TIC + SASE Proves a Winning Combination

TIC 3.0, the latest version of the Cybersecurity and Infrastructure Security Agency (CISA) — guidelines, focuses squarely on these issues by providing templates and guidance for secure remote access. The ultimate goal of TIC 3.0 is to provide a better user experience and performance in the most secure way, while paving the way for the adoption of emerging technologies.

TIC 3.0 is just that, though — guidance. Providing the right level of access, performance and security for remote workers using the cloud requires solutions that can scale virtually infinitely. That's the only way for agencies to be able to add users and capacity rapidly without compromising performance, manageability and security.

One modern approach takes advantage of the increasingly popular secure access service edge (SASE) model, a cloud-based network architecture that combines wide-area networking and network security services. The SASE model fits the TIC 3.0 remote user use case well. It provides both the mechanism for secure VPN access to the data center and the security necessary for access to internal data, cloud and the larger internet.

"Traditionally, the VPN was one piece, and the security services were the other pieces, which required traffic to be funneled through a security stack," said Wayne LeRiche, a systems engineer at Palo Alto Networks. "SASE converges these functions through one interface, which results in a secure VPN with distributed security services that give users the same experience, no matter where they are."

The cloud-based SASE model also supports a related TIC 3.0 use case on remote and branch offices, which encourages the use of SD-WAN technology to connect traffic to the internet directly. By choosing a SASE solution that includes SD-WAN capabilities, agencies can help ensure secure, application-aware routing of resources on demand instead of relying on more expensive multi-protocol label switching connections.

# Best Practices in Providing Remote Access

## Keep remote access in line with TIC 3.0 guidelines.

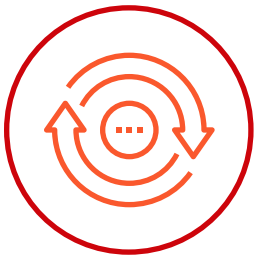
When choosing solutions, dig deep and ask the hard questions. Is the solution scalable and flexible to allow for surges? Will it scale as users shift geographically? Does it have robust logging and granular controls for tailored use cases? Will it work well with your existing technologies? Will it allow you to incorporate new technologies and requirements?

## Leverage SASE.

Combining elements of secure networking and security in one cloud-based solution is attractive for many reasons. Not only is it more efficient and cost-effective than traditional solutions, but it is less complex, provides greater access control and produces the type of immediate, uninterrupted access users need, no matter their location. Most importantly, it includes a host of network security services that are increasingly important today, including zero-trust network access and the multi-mode cloud access security broker (CASB).

## Don’t lowball security.

“Nothing is more important than having up-to-date security in every part of the stack,” Beaman said. “If you are getting signatures that are being updated every 10 seconds via a cloud-based system, you’re getting the newest data in real time. If you have some sort of intrusion protection system onsite and you’re doing a pull every few days or so, those signatures are too old to be of much help.” Beaman recommends a SASE solution that includes zero-trust network access, Domain Name System security, threat prevention, firewall as a service, a cloud-secure web gateway to block malicious sites and a CASB for full governance and data classification. A SASE solution with these capabilities can cover every area of security.



## Insist on agility, flexibility and ease of use.

Remote workers who are unable to access the resources they need will inevitably find other ways to get that information, which may not be as secure or in line with their agency’s policies. To avoid these issues, look for platforms that provide centralized administration, web-based interfaces with preconfigured profiles and streamlined workflows, and automated updates. Most importantly, make sure that all parts of the platform are engineered specifically for the cloud. Such platforms will ensure that you benefit from upgrades and changes instantly.

# Case Study: Productivity, Pandemic Style

During the early days of COVID-19, as agency after agency began requiring employees to work from home, the challenges of the new reality became crystal clear. Employees were having problems accessing the information they needed to do their jobs, and were hampered by slow network connections, along with capacity and performance issues. For one defense health agency, those problems required an immediate solution. Without any change, the agency's day-to-day business would come to a halt.

The agency had been using VPN concentrators with agents installed on user devices to manage traffic and provide user access, but the concentrators were failing as demand skyrocketed. They needed a better solution — one that could accommodate traffic bursts quickly and scale as high as necessary on-demand.

After evaluating several options, the agency settled on Prisma Access from Palo Alto Networks, a SASE solution that provides cloud-based connectivity and security for remote users. With this solution, users spin up their own network infrastructure on demand, and the infrastructure is always in compliance with the agency's policies. When users finish using the resources, they spin back down.

Today, as personnel continue to work remotely, the value of the SASE-based solution has become even more clear. No matter how long the pandemic continues or how many employees will continue working remotely in the future, latency, capacity and performance will never again be major issues.

## HOW PALO ALTO NETWORKS AND VERIZON HELP

Palo Alto Networks provides federal agencies with data protection, network security and cloud security solutions. Its Prisma Access SASE product, based on zero-trust security, provides granular user and application visibility and control, along with content inspection. Prisma Access addresses many of the TIC 3.0 use cases, including SD-WAN architectures, and integrates with existing trusted internet connection access provider (TICAP) and managed trusted internet protocol service (MTIPS) technology. Palo Alto Networks is committed to complying with federal certifications.

Verizon provides agencies with solutions for IT modernization, mobility, business continuity and transitioning to GSA's Enterprise Infrastructure Solutions program. It is also a major provider of TIC 2.2 and TIC 3.0 technologies and currently holds several federal contracting vehicles, including Global Network Services, EIS, Connections II, DTS-P II, Networx and WITS3, along with a full GSA schedule program.

Together, Palo Alto Networks and Verizon work to address cloud, branch and remote user solutions for federal agencies. For example, Prisma Access integrates seamlessly with Verizon's MTIPS and SD-WAN solutions used by many agencies to allow them to gain more visibility and granular detail from their solutions.

***For more information, contact Palo Alto Networks at TIC@paloaltonetworks.com.***

# Conclusion

TIC 3.0 provides agencies with important guidance on how to improve network and data security while still enabling remote users to get their work done. Combined with technology like SASE and modern SD-WAN capabilities, agencies can keep worker productivity on course while ensuring that data remains fully protected and in full compliance with all applicable regulations.

By adopting this type of modern, flexible, cloud-based approach to network and data security, agencies are also positioning themselves for whatever comes next. Whether that's greater incorporation of artificial intelligence/machine learning, Internet of Things (IoT) or 5G-based capabilities, having the right structure in place will ensure that agencies can make the most of the capabilities these new technologies may afford.


## ABOUT PALO ALTO NETWORKS

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

For more information, visit www.paloaltonetworks.com.


## ABOUT VERIZON

For more than 100 years, Verizon has been at the center of the communications revolution. Verizon is one of the largest communication technology companies in the world. We help people, businesses and things communicate better. The digital world promises consumers a better, more connected life, and we're the ones delivering it. We make it possible for people to stay in touch and businesses to connect with their customers. We're also bringing technology and hands-on learning opportunities directly to kids who need it most. Our goal is to inspire tomorrow's creators to use technology to build brighter futures for themselves, their families and the world.

For more information, visit www.verizon.com/business/solutions/public-sector/


## ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop