A **CENTER FOR DIGITAL GOVERNMENT** WHITE PAPER | WINDSTREAM ENTERPRISE

Meeting **Modernization** Goals with SASE

Remote work, changing customer expectations, new security threats and ongoing talent shortages are driving organizations to modernize.

Many state and local governments are adopting Secure Access Service Edge, referred to as SASE (pronounced "sassy"), to meet their modernization goals. A SASE approach provides a simplified but powerful security deployment with synchronized technologies. By converging network and cybersecurity components into a comprehensive cloud-based framework, SASE enables secure, reliable access to network resources and users regardless of their location.

"Convergence offers significant advantages, especially for organizations that are trying to simplify, be cost efficient and offer more seamless user experiences," says Deborah Snyder, senior fellow for the Center for Digital Government.

With the right strategies, organizations can roll out a flexible SASE solution at their own pace while meeting their modernization priorities.

Many state and local governments are adopting **Secure Access Service Edge**, referred to as SASE.

Misconceptions about SASE

Myth: **SASE is expensive.**

Truth: **It's exceptionally cost effective when you look at the total cost of ownership.**

In a traditional non-converged solution, software-defined wide area networks (SD-WANs), firewalls, cloud access security brokers (CASBs), Zero Trust network access (ZTNA) controls and other tools run on different platforms. Hardware redundancies and the need for IT to support each technology stack separately drive up costs.

"While there may be initial costs with SASE, it's important to consider the long-term benefits. Government agencies should conduct a thorough cost and benefit analysis that considers the savings you can achieve through reduced hardware, simplified management and improved operational efficiencies," Snyder says.

Myth: **SASE is a "rip and replace" model.**

Truth: **It's "wrap and refresh." It's easy to add SASE components on top of what you already have, and you can do so at your own pace.**

"The fact that agencies can phase in SASE gradually — which then allows them to adapt and grow the solution as their budgets and requirements evolve — gives them flexibility on the cost issue as well," Snyder says.

Combining SD-WAN and SASE

An SD-WAN uses real-time data about network conditions to automatically route data along the best available path at any given moment. By doing so, it helps optimize application performance and manage bandwidth usage costs.

Traditionally, SD-WAN and security solutions are separate components, leading to complexity and fragmented architectures. By converging the two, organizations reduce the number of disjointed devices and services they need to manage.

"With SD-WAN and SASE, you get enhanced network performance and robust security without compromising either one," Snyder says.

Converged network solutions centralize network management as well as the monitoring and management of cybersecurity controls. With a single engine that integrates and correlates log data from multiple components, security teams get end-to-end visibility and greater control over the activity on their systems.

> "Convergence offers significant advantages, especially for organizations that are trying to simplify, be cost efficient and offer more seamless user experiences."
>
> *— Deborah Snyder, Senior Fellow, Center for Digital Government*

The Benefits of a Converged Solution

A comprehensive network security solution provides better protection against cyber threats and ensures regulatory compliance. It also increases redundancy and failover capabilities, which help services remain available during a network or system failure.

The main network and security components of a converged infrastructure include:

Secure web gateway (SWG). This gateway sits between users and the internet. It automatically detects and blocks any user's attempt to access potentially malicious applications or websites. Together with SWG, remote browser isolation allows users to safely browse any website.

CASB. A CASB sits between users and cloud services or other cloud resources. It applies the organization's privacy, security and compliance policies as users access these resources. To fortify a CASB, include data loss prevention, which secures sensitive information, and security-as-a-service, which integrates third-party software-as-a-service apps with defined security policies.

ZTNA. ZTNA is a user-centric approach based on the premise that it's not sufficient to focus on protecting individual locations or technology itself. It focuses on dynamically granting access to users based on their identity, location, device type and other qualifiers.

Firewall-as-a-service (FWaaS). FWaaS is similar to an on-premises firewall device, but its network security capabilities are available anywhere. These features include URL filtering, an intrusion prevention system, malware and threat detection, and managed detection and response.

Beyond security improvements, a converged system can save costs. SASE providers manage and maintain the solution, alleviating the in-house burden and operational costs of updates, patches, upgrades and hardware replacement. Additional savings include freed-up square footage, electricity and staff resources.

Advanced security practices and improved internal operations also streamline the constituent experience.

Beyond security improvements, a converged system can save costs.

CUSTOMER SPOTLIGHT

How a Modern Solution Evolves with a Growing Student Body

When its multiprotocol label switching (MPLS) network could no longer keep up with network demands, a large college in the Southern United States found a fast fix with an SD-WAN and managed network security solution.

The college serves more than 6,000 students online and across five campuses. The network is critical to the institution, yet its legacy MPLS solution lacked the bandwidth to support a growing student body and the profusion of devices used by students. Managing the legacy system and routers was complex and time consuming. The college also experienced four major network outages a year.

The college deployed high-availability SD-WAN managed services provided by Windstream Enterprise at each campus to strengthen redundancy and resilience. Then, it added the provider's Managed Network Security (MNS) for an extra layer of network protection. MNS has been vital, enabling students and faculty to connect securely from anywhere and on any device for online courses.

Since implementing the updated solution, the college has not experienced a single outage. The network is easier to manage and allows IT staff to move servers and make other changes more agilely. Through one centralized dashboard, staff can run statistics, monitor performance, troubleshoot and mitigate issues.

Moving forward, the college has the network security, performance, resilience and scalability to meet the demands of modern teaching and learning — at a lower cost and without the burden of managing the network and security in house.

Strategies for Success

To successfully adopt a SASE approach, consider these best practices:

Start with a ZTNA approach. End users are your biggest vulnerability, and traditional controls such as virtual private networks don't adequately protect remote or mobile workers. In addition, many ZTNA strategies — such as multifactor authentication and micro-segmentation — are inexpensive to implement.

"ZTNA is the first step that I would recommend," says George Stewart, leader of sales engineering for state and local government and education at Windstream Enterprise. "It's the easiest and lowest-cost component. Get your users — especially your remote workforce — covered because that is the biggest vulnerability."

Conduct a thorough cybersecurity assessment. Assess your current network/IT infrastructure and areas of vulnerability. Understand the problems you want to solve, then identify your modernization goals and the specific outcomes you want to achieve (e.g., enhanced security, improved performance, additional scalability, cost efficiency, better user experience).

Update and patch software regularly. Many attackers exploit well-known vulnerabilities that were reported years ago. Remember to update and patch tools such as browsers, printer drivers and mobile devices.

Review password policies. Implement strong password policies and routinely require users to change passwords. This will help build a culture of cybersecurity throughout the agency.

Keep refreshing your modernization strategy. Modernization is a continuous process. It requires regular assessment, staff training, software updates and more. Provide short, focused training and hands-on learning opportunities to keep staff current on cybersecurity issues and remediation.

Consider IT managed and professional services. In a Center for Digital Government survey, more than 75% of respondents said they were in the early stages of modernization or had made only moderate progress. Respondents' top barriers to modernization were costs/funding (64%) and IT knowledge/technical skills gaps (38%).[1]

IT managed and professional services fill in skills gaps and help with modernization assessments, planning, management and skills development. Partner with proven vendors that can work with your team to create solutions that meet your unique goals.

Creating a Helpful Partnership

When delivered by a proven services provider, a converged network and security solution reduces complexity and costs while improving cybersecurity and network performance. Your provider should be aligned with your modernization goals, security requirements, and budget and staffing constraints.

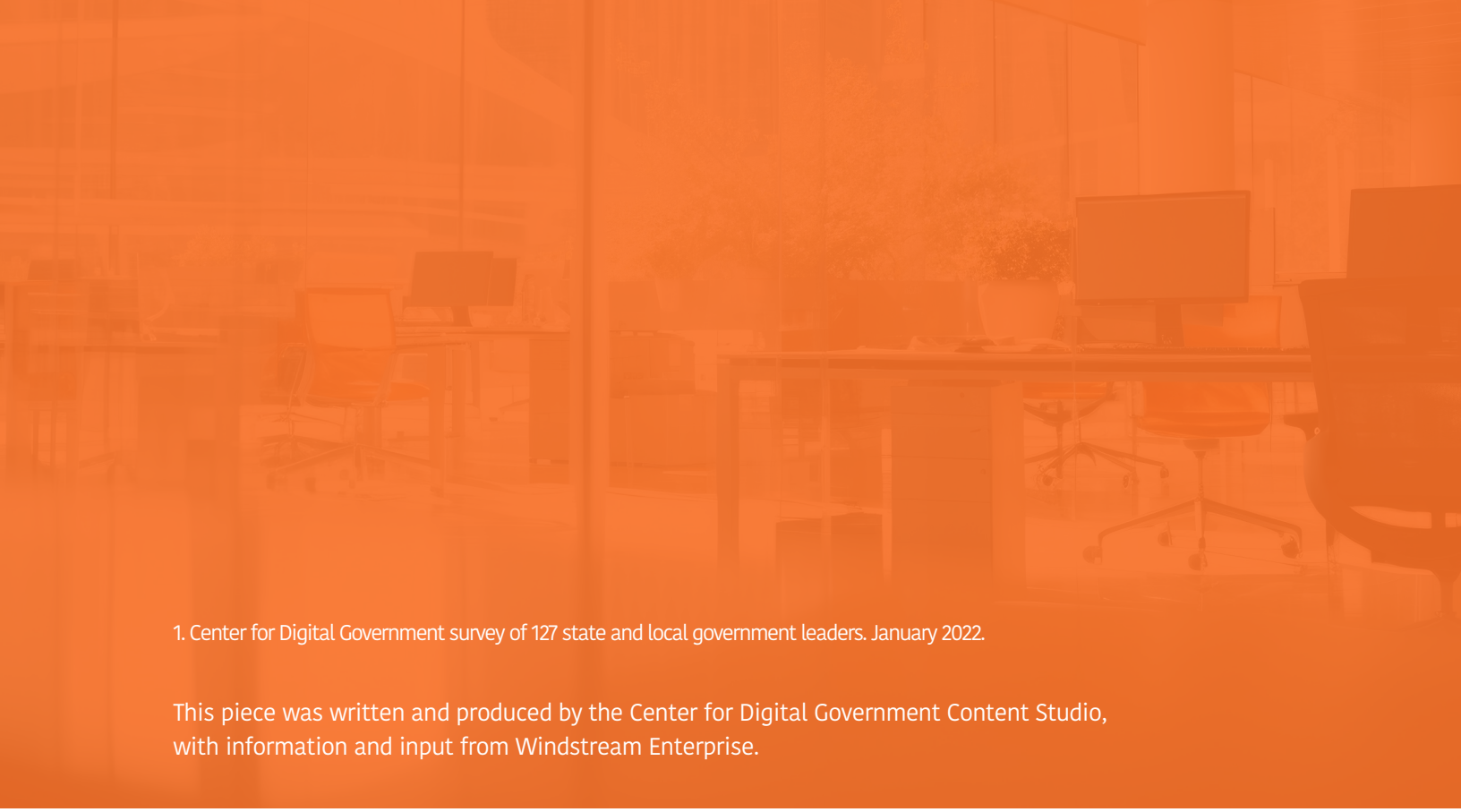
Consider the provider's record of accomplishment in deploying and managing SASE solutions. Be sure its bench includes a team of professionals with deep knowledge of SASE technologies and best practices. Understand the provider's full range of services, which should be tailored to meet your organization's unique needs.

Your provider should have robust security measures in place, including a comprehensive strategy around cybersecurity and incident response. To help ensure continuous availability of services, ask about data center redundancy and failover capabilities. Review service-level agreements and request the provider's actual record of availability. Be sure the provider has sufficiently distributed data centers for rapid recovery and minimal data loss in the event of a region-wide outage.

The provider should be well versed in regulations that impact your organization's specific mission and function, as well as general regulations related to financial transactions, data privacy and data availability. It should also offer a framework and tools for assessing and reporting compliance with regulatory requirements.

While many agencies are eager to modernize, barriers are common and costly. A partner can give organizations of any size the foundation and support they need for their initiatives.

A partner can give organizations of any size the foundation and support they need for their initiatives.



1. Center for Digital Government survey of 127 state and local government leaders. January 2022.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Windstream Enterprise.

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Sponsored by: WINDSTREAM ENTERPRISE

Windstream Enterprise drives organizational transformation through the convergence of our proprietary software solutions and cloud-optimized network to maximize government agencies' return on technology spend. Our end-to-end IT managed services modernize technology infrastructure, optimize operations, eliminate resource constraints and elevate the experience of agencies and the constituents they serve, while safeguarding their critical data and reputation. Analysts recognize Windstream Enterprise as a market leader for our product innovation, and clients rely on our first-in-the-industry service guarantees and best-in-class management portal. Over 2,700 public entities trust Windstream Enterprise as their single source for a high-performance network and award-winning suite of connectivity, collaboration and security solutions — delivered by a team of technology experts whose success is directly tied to fulfilling each organization's mission.

ADOBESTOCK

©2023 e.Republic LLC. All rights reserved.