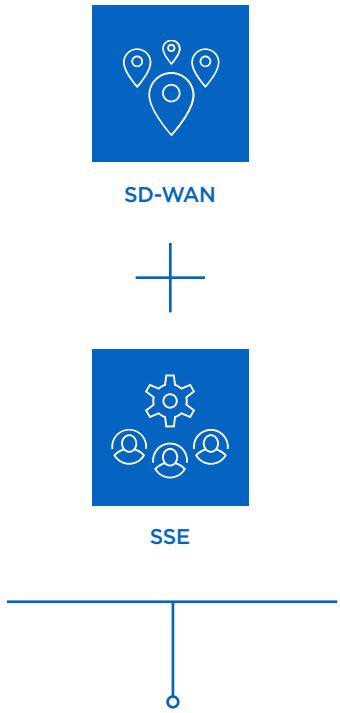
A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER | SPECTRUM ENTERPRISE

Navigating the SASE Evolution

How to move toward a new generation of protection for users across locations, clouds and applications.

Introduction

Secure access service edge (SASE) is often touted as the next generation of cybersecurity for an increasingly dispersed technology environment, but it's about more than ensuring the integrity of users, data and systems. Planning for SASE involves rethinking how you design and manage your overall network infrastructure to meet changing needs and protect users across locations, clouds and applications.



SASE combines SD-WAN and SSE into a single managed service to secure users across locations, clouds and applications.

What is SASE?

SASE is an architectural framework that brings together two key components:

- Software-defined wide-area networking (SD-WAN) for unified access and network controls.
- Secure service edge (SSE), a cloud-based cybersecurity platform centered on the identity of users, devices and operations.

SASE converges networking and security — typically as a cloud-delivered managed service — to safeguard internal networks, users, devices and endpoints connecting via the internet.

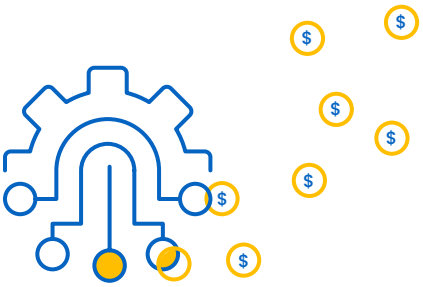
Endpoints continue to proliferate due to the growth of hybrid work and cloud-delivered applications. SASE gives government agencies a single solution to track all users, devices and applications by enabling Zero-Trust architecture and supporting cloud-based control of security and compliance policies. It lets users securely and seamlessly connect whether they are on premises or in the cloud — without increasing the burden on IT staff or adding complexity. Adopting SASE and its underlying components allows agencies to provide a seamless, flexible experience for their workforce and residents.

Strategies for Success

SASE is a combination of technologies, not a single plug-and-play solution. Implementing SASE requires agencies to move toward a modern cloud-based IT architecture. The approach often involves working with a trusted partner that can implement and manage technologies through a cloud-delivered managed services agreement.

Government IT leaders must consider a range of factors when planning, implementing and managing this transition.

Deciding to implement. To determine your readiness for SASE, you need a full understanding of endpoints, users, networks, applications, data, and workforce and constituent needs across the enterprise — a challenge in siloed agencies and departments. You'll also need to assess



Agencies Evolve Their Network Security Approach

State and local government agencies are steadily adopting key building blocks of SASE, such as cloud-based network architecutures and managed security services.

Almost 70% of officials responding to the Center for Digital Government's 2022 Digital States Survey said they were implementing or upgrading SD-WAN technology. More than 50% said they were expanding their use of security as a service.[1]

what cloud environments are in use or may be added, and consider the desired security posture across different users, devices and use cases. A managed services vendor can assist you with this daunting task.

Developing a plan. Adopting SASE is an evolution, so prioritize your organization's greatest needs. An agency that rarely uses remote access might start by deploying an SD-WAN for internal networks. An agency focused primarily on managing access to web applications might begin with SSE.

As you develop implementation plans, determine the extent of integration required for existing hardware, systems and applications. Identify vendors and partners who can manage the transition across multiple physical locations connected by traditional WANs. Also determine the extent to which SASE and its components will be managed in house or by partners through managed services agreements.

Designing your environment. Decide if existing network hardware and applications will be replaced or integrated into the new SASE environment. Work with your technology partners to assess existing and planned use cases to determine the appropriate network capacity. Consider the differing uptime, performance and security needs for all use cases, with the goal of providing the best network experience for users.

Implementing SASE. Even if technology partners play a primary role during implementation, you need to focus on change management for existing staff and workflows. One common challenge is addressing shadow IT within individual departments or offices as siloed operations are brought into the SASE environment. You'll also need to train IT staff to provide service and prepare end users for changes in network access procedures or policies.

Managing and optimizing your deployment. Monitor service-level agreements and customer support provided through managed services contracts. Also monitor network performance and use insights gained from visibility into systems to improve access and control policies. Working with the right managed services partner will simplify these tasks.

Starting the Journey

Expansion of hybrid work and cloud-based applications are accelerating the transition to SASE. Public agencies can start this journey by evaluating their existing network and security infrastructure to identify gaps in how systems are accessed, managed and secured.

Trusted network partners like Spectrum Enterprise can help agencies avoid disruption and achieve faster time to value by providing specialized skills during SASE planning, design and implementation. They can also offer flexible ongoing support.

The result: An IT architecture that provides the security and flexibility governments need in a rapidly evolving world.

This piece was written and produced by the Government Technology Content Studio, with information and input from Spectrum Enterprise.

Visit enterprise.spectrum.com/services/industries/state-local-government.html to learn how Spectrum Enterprise can help your organization with SASE planning, design, implementation and support.

Endnotes

1. https://www.govtech.com/cdg/digital-states/digital-states-survey-2022-results-announced

ADOBESTOCK

Produced by: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.
www.govtech.com

Sponsored by: Charter COMMUNICATIONS | Spectrum ENTERPRISE

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions, Internet access, Ethernet access and networks, voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.