SASE Security Buyer's Guide

How to Choose a SASE Platform that Puts Data Security First

Forcepoint

Buyer's Guide

forcepoint.com

Table of Contents

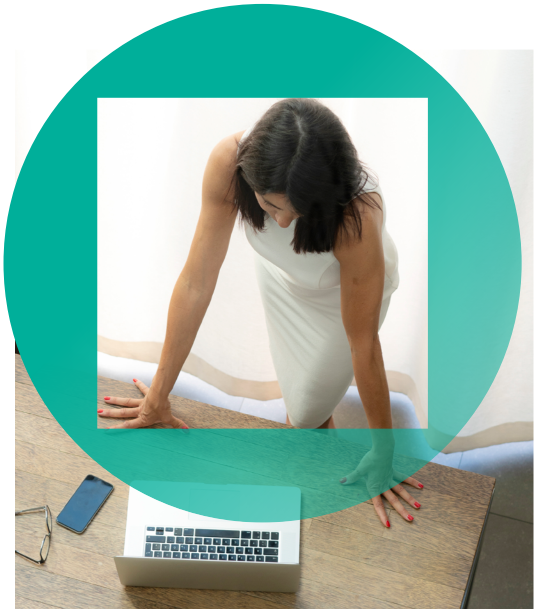
Executive Summary

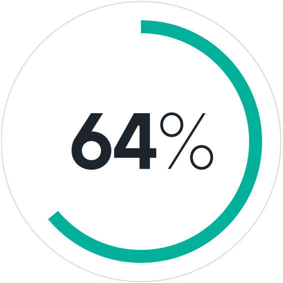
Remote work today means "work anywhere"—at home, in an office, or wherever travel may be permitted. Connecting people to the data they need and delivering consistent security wherever data is used are the new challenges.

With people, applications, and data now frequently beyond the traditional boundaries of the enterprise, security teams must continue to deliver consistent security where it's needed, while supporting productivity for today's anywhere worker and lowering the operational burden. Gartner's Secure Access Service Edge (SASE) architecture is a compelling path forward, designed to bring together disparate networking and security technologies as converged services delivered from the cloud.

Some SASE solutions focus on connecting people to applications; however, access is simply the way people securely obtain the data they need to get their jobs done. Cybersecurity must also protect the usage of that data from the edge to the cloud.

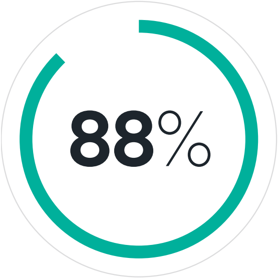
Use this guide to understand the different approaches for SASE security and the capabilities you should expect and trust from a SASE platform.



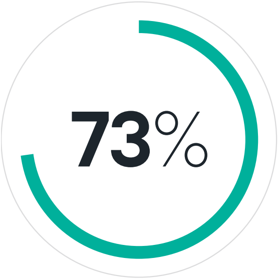


64% of enterprises say network security is more difficult today[1]

53% of employees work remotely, up from 20% prior to COVID[1]



88% of SASE users are confident they have visibility to all cloud usage in the enterprise[1]



73% of mature SASE users will eliminate VPNs[1]

Two Types of SASE

SASE reinvents disparate stacks of networking and security hardware as converged cloud services that primarily follow two schools of thought:

Access-centric SASE

→ **Advantages:** As the name suggests, access-centric SASE security focuses primarily on safely connecting users to applications and data, whether on the web, in the cloud, or in internal private data centers. Typically delivered as a cloud, this type of SASE provides centralized control over who can use crucial business systems and protects against attackers from malware, ransomware, and other advanced threats.

→ **Concerns:** Access-centric SASE tends to focus on getting users connected to the applications they need to interact with business data but doesn't provide continuous control over the usage of that data. Furthermore, some solutions behave as loosely managed point products, requiring multiple endpoint agents for different security services, leading to sprawl and conflicts among the agents.

Data-first SASE

→ **Advantages:** Putting data first in a SASE approach provides continuous control over how data is used in addition to giving users safe access to data. Moreover, some SASE solutions have evolved to understand how users interact with data, digital, and physical systems and identify behaviors that create risk and could lead to breaches. Putting data at the center of SASE enables automated enforcement of security policies based on the risk each user presents in any given moment. The goal of data-first SASE is to make such enforcement uniform everywhere—on endpoints, in the network, on the web, and in the cloud, making this approach ideal for distributed enterprises where employees work and use cloud services beyond corporate walls.

→ **Concerns:** Even though you can implement all SASE platforms one capability at a time, a data-first approach to SASE is most effective when data security is seen as a priority throughout the organization. To get the full benefits of a data-first approach, security policies for sensitive information and intellectual property should be understood and supported by management as well as business processes and procedures.

5 Steps to SASE

1. Protect remote workers in both the web and the cloud

SASE security must enable people to get their jobs done safely, not inhibit productivity. These anywhere workers need the freedom to work safely from any location at any time.

2. Control access to cloud and private apps without VPNs

Each user should only have access to the resources they have explicit permission to use, under the full visibility and control of your business.

3. Safeguard usage of data everywhere

SASE must provide ongoing control of how critical data and intellectual property is used once downloaded from apps. This prevents data from inappropriately going to the cloud, web, or personal accounts—unintentionally or maliciously.

4. Connect and protect branch offices and remote sites

Users at remote sites must have fast, secure access to web, cloud, and private apps without the costs or complexities of private MPLS lines or backhauling traffic to HQ. Easy integration with SASE services is crucial for management at scale.

5. Continuously monitor user risk

Controlling data usage, especially on remote devices and cloud services, requires an ongoing understanding of what people are doing and whether their behavior is creating risks that could become breaches.

What to Look for in Data-First SASE

By converging capabilities in a cloud-delivered platform, SASE fills in the gaps that previously existed from disparate point products, reduces costs, and improves efficiencies by delivering security wherever data is used. The difference between access- and data-centric SASE approaches comes down to whether data is continuously protected after it is accessed. Consider the following capabilities in your evaluation. Look for next-level features that increase automation as well as manageability and always put data first in SASE.

Core capabilities

- → **Data Protection:** Data-first SASE must provide protection for accessing and using sensitive information and intellectual property. Look for SASE solutions that offer a single set of data security policies that can be enforced uniformly from the endpoint through the network, into the web and cloud. Enterprise-class traffic controls ensure that data can't leave employee devices inappropriately, such as being moved to a cloud service or USB stick, printed, or copied.
- → **Threat Protection:** Defenses are layered with a combination of edge protection, deep content inspection, advanced malware detection, and remote browser isolation to protect against external attackers. You can bring branch offices online quickly and securely with comprehensive protection delivered directly from the cloud with no hardware appliances.
- → **Application Security:** SASE was developed to provide visibility and control of applications, Shadow IT, and corporate-managed and unmanaged devices through features like URL filtering, deep content inspection, and cloud app visibility. Blocking the use of any unsanctioned cloud service prevents employees from skirting security policies. Full audit and granular control over app usage and activities simplify compliance in the cloud.
- → **Network Security:** Comprehensive security encompassing cloud- and site-based firewall services enable safe access to the internet, inspection of encrypted traffic, and defenses against advanced network threats.
- → **Network Connectivity:** SD-WAN connects branch offices directly to the internet where SASE services can provide seamless security; an endpoint agent similarly connects remote employees.

Next-level features

- → **Unified data security policies** enable you to define security policies once and enforce them everywhere, from the endpoint to the cloud.
- → **Unified agents** integrate endpoint software for safely accessing resources, enforcing policies, and monitoring activity on users' devices.
- → **Flexible deployment** features integrate rich context-based controls, hybrid enforcement at sites with special requirements (e.g., compliance with data sovereignty regulations), and secure SD-WAN without requiring extra products.
- → **Risk-based policy enforcement** automatically personalizes security according to the risk each user's behavior presents as they use data, apps, and systems.

Key Questions to Consider

1. What steps will be required for you to transition to a hybrid workforce model?

2. How do remote workers access your cloud and private apps today?

3. What did you have to change in your infrastructure or operations to support work-from-home (WFH)?

4. How will you sustain WFH?

5. What cloud applications does your organization sanction today?

6. Do you have visibility into unsanctioned applications that include data sharing capabilities?

7. Do you have control over the cloud/internet security for your remote workers?

8. Are you looking at ways to consolidate hardware at your network's edge (in offices, branches, etc.)?

9. What is your strategy for securing access to internal, private apps?

10. How are you protecting or controlling data, and what are the gaps between regulatory requirements and capabilities?

11. What is your organization's exposure to risk for data being "lost" in the cloud, exposed publicly, or outright exfiltrated?

12. If you had a clean slate, what would you do differently to secure cloud access, data, and networks?

The Upshot: Protecting Data Everywhere

Today's anywhere workers will have more autonomy within your decentralized organization. The world has irrevocably changed to one with seemingly endless options for accessing resources and services and protecting against increasingly sophisticated threats or accidental breaches.

As a security professional, you need to enable transformation without being hemmed in by point solutions that can't scale in this boundary less digital frontier. The fact that you're reading this means that you're trying to find fresh ways to support productivity effectively, while protecting your people and your critical data everywhere. Going cloud-native and hybrid-enforced is the most effective way to do security.

Find a partner who can help you quickly identify the opportunities to create an integrated security framework, step by step. One that gives you the agility to adapt to a continuously evolving environment.

As a security professional, you need to enable transformation without being hemmed in by point solutions that can't scale in this boundary less digital frontier.

Next Steps

Learn more and download our *5 Steps to SASE* whitepaper.

Download Now

[1] ESG Research Insights Report, Quantifying the Benefits of SASE, March 2021

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

Report: THe State of Hospital Cybersecurity 19MAY2021