5 Steps to SASE

Your Executive's Guide to SASE—Enabling the "Anywhere" Worker

Forcepoint

Whitepaper

Table of Contents

Introduction

In today's remote work era, delivering safe access to business resources from anywhere with security policies enforced consistently everywhere are now must-haves for distributed organizations. Converged, cloud-based approaches like Secure Access Service Edge (SASE) enable you to efficiently use web, cloud, and private apps, protected against advanced threats and data loss. But what defines a complete SASE platform? Not access. It's data. More precisely, controlling usage of data.

Unlike access-focused solutions, a data-first approach to SASE boosts productivity and reduces risk, allowing you to improve access to your data, apps and services and secure data everywhere it's used. This guide explains the key benefits of a data-first SASE architecture that combines uniform enforcement of data policies, unified agents, flexible deployment models, and risk-based policy enforcement to continuously protect your critical data and users.

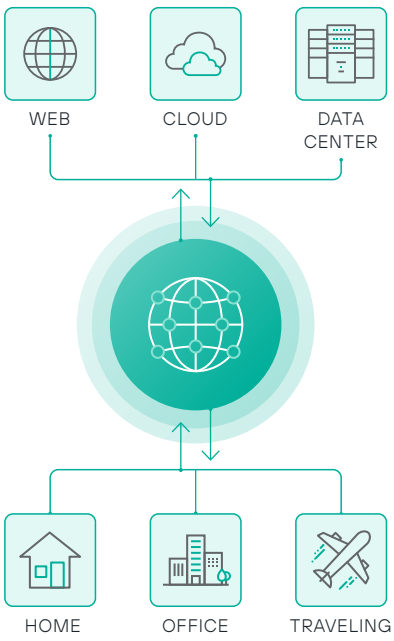
Organizations with existing cloud security, network security or security operations technologies can also use this guide to understand next steps in activating key capabilities in a data-first SASE platform.

Protecting your business starts with protecting users and data—everywhere

Here's the reality of today: your data is in the cloud, your people are working in multiple locations—at home, in the office, and on the road—and security has to join them. Employees, contractors and vendors need to access business data like customer information, cloud services like Office 365 and private applications like ERP, regardless of where they or the data reside.

Interactions between users and critical data expose your people and systems to new types of attacks by digital thieves or nation states that want to steal your sensitive data or intellectual property. Old hardware-based approaches aren't keeping up, creating yet more complexity as the number of moving parts increases.

The security perimeter has shifted from your corporate infrastructure to wherever your people are working and whichever devices they are working on, but your mission remains the same: to give your people access to necessary data and services, without obstructing productivity or putting critical information at risk.



With organizations more distributed than ever before, putting stacks of appliances at every location or using fragmented products for remote workers creates holes for attackers, costs too much, and drains scarce IT resources.

Against this backdrop, Zero Trust is the model for security today: everyone is required to gain explicit permission each time they access resources or use information. A converged, cloud-based approach like SASE is how you can deliver that security. SASE doesn't just move old products up into the cloud—it reinvents them as capabilities within a platform to eliminate redundancies and simplify operations. With people and data now everywhere, security has to address the question: In a distributed world, how do you control access and usage continuously?

The security perimeter has shifted from your corporate infrastructure to wherever your people are working and whichever devices they are working on.

5 Steps to SASE

The path to SASE can really start from anywhere, depending on whether your greatest need is securing user access or keeping data safe. Your priorities might be as diverse as enabling remote workers and protecting branches to preventing IP theft and complying with regulations. In any case, you can start your SASE journey in five key ways and work your way through the other steps as needed:

Protect remote workers in the web and cloud: We're seeing the onset of the new age of "anywhere workers" who have the freedom to work from any location and at any time.

Control access to cloud and private apps without VPNs: You must personalize security so each user can only get to the apps and resources they need, under the full visibility and control of your business.

Safeguard usage of data everywhere: Security's job is preventing critical data from being misused— unintentionally or maliciously—from the endpoint to the cloud.

Connect and protect branch offices: 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.

Continuously monitor user risk: Controlling data usage requires both a Zero Trust approach and an understanding of people's behaviors to determine whether their actions are creating risk that could become breaches.

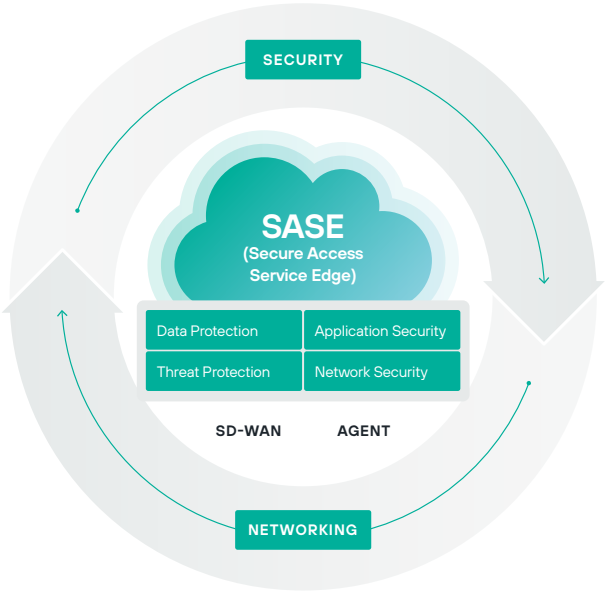
SASE is picking up steam because it replaces stacks of networking and security hardware with converged cloud services that dramatically improve and simplify user and data protection. The goal has shifted from digital transformation to business transformation. Yet the old ways of handling connectivity and security can't keep up.

Access-centric SASE is a start— but not enough

As great as SASE is, some implementations simply bring together products that betray their legacy as infrastructure point solutions:

- → The dependency on single endpoints in the network or the cloud leads to agent sprawl.
- → The lack of unification means security policies become inconsistent, brittle, complex, or outdated.
- → On the other hand, cloud-only services ignore sites needing local, hybrid controls and enforcement.
- → Access-centric SASE focuses too much on content and ignores the context around users interacting with data and systems.

The access-centric SASE approach is too brittle and can't scale to meet the dynamic needs of today's massive remote workforces and business transformation.



SASE replaces stacks of networking and security hardware with converged, cloud-based services.

Data-first SASE security

Ultimately, networking and security is all about enabling people to get to and use business information safely. Access-based SASE should go beyond access to continuously protect how data is used. This is what we mean by putting data at the center of SASE.

Data-first SASE brings together a wealth of connectivity and security capabilities and, importantly, allows you to tackle different problems at different stages. You can seamlessly add cloud-based services in phases, according to your business requirements.

The benefits of data-first SASE

Integrating a data-first approach into your SASE stack uniformly protects data and users and consistently applies policies everywhere:

Web, cloud, and data security in a single cloud service

- → Keep your users safe and productive no matter where they work—at home, in the office, on the road.
- → Reduce risks and prevent data loss as your people use the web and cloud apps from more places than ever before.
- → Protect roaming users automatically with lightweight, unified endpoint software.

Remote access to private apps without VPN pain

- → Bring your remote sites into the cloud era, connecting them directly to the internet and the cloud without having to use VPNs or send traffic back to your HQ.
- → Employees and partners can securely access data, apps, and information without compromising the integrity of corporate networks, systems, and databases.

Risk-based, automated security

- → Eliminate friction and keep people productive by automatically tailoring security to the level of risk posed by each user's actions.
- → Seamlessly enforce policies in the cloud or locally at sites with special data sovereignty needs.
- → When you're ready, you can make sure that the data your people are using stays safe on their laptops and in their cloud apps, and that they aren't taking unnecessarily risky actions.

Operational efficiency, managed from cloud

- → Save your IT teams from chasing never-ending updates and wrestling with inconsistencies in point products.
- → Make policies easy to understand with names of your own users and groups as well as thousands of cloud apps.

Continuously understanding risk and enforcing policies based on risk is the most efficient way to protect and enable distributed workforces.

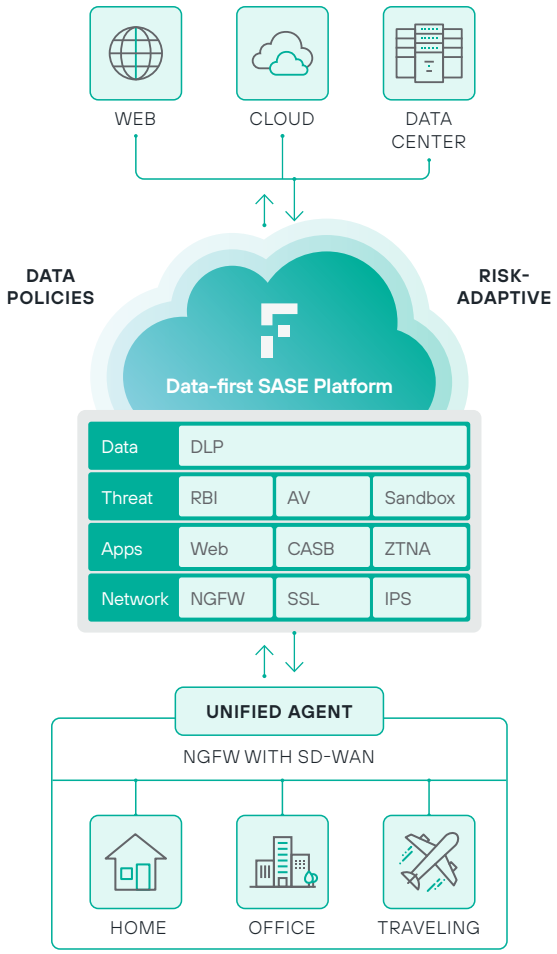
Your people can remain productive regardless of where they or their data reside. Employees and partners can securely access everything they need to get their work done without compromising the integrity of networks and data.

In the end, a SASE approach that puts data at the center also closes the security gaps and redundancies to control costs. Your IT security teams can reduce capital expenses, like hardware, and trim operational expenses as processes and infrastructure change and shift to the cloud.

Access-based SASE solutions focus primarily on securing the door to resources. A data-first SASE platform goes further to continuously protect how data is used.

Secrets to SASE Success

Forcepoint's Data-first SASE platform goes beyond simply providing safe access anywhere—it safeguards the usage of data consistently everywhere. You can write uniform data policies once that are then enforced from endpoints to cloud apps. With data-first SASE, your people can work at home, in a branch office, or even at a customer site, and still be protected by the same security policies. By design, you can activate cloud-based capabilities as you need them to simplify your transformation to the cloud:



Data protection secures data that is now flowing among main offices, data centers, branch offices, remote users, and the cloud. Data-first SASE provides a single set of consistent, seamless data security policies to enforce data loss prevention (DLP). Both cloud-based traffic controls and integrated endpoint data protection ensure that sensitive information doesn't ever go to the cloud or leave employee devices inappropriately. Optional hybrid data protection provides both cloud-delivered and on-premises capabilities.

Threat protection is paramount for anywhere workers using flimsy or non-existent security measures when at home or on the road. The Forcepoint Data-first SASE platform delivers robust edge protection and layers in complex defenses like deep content inspection, advanced malware detection, and remote browser isolation to protect against the most sophisticated external attackers. On-premises appliances become obsolete because you can bring branch offices online quickly and securely with comprehensive protection delivered directly from the cloud.

Application security from SASE helps you gain visibility and control into data center and cloud applications, devices and shadow IT resources. You control the usage of applications and corporate-managed and unmanaged devices through features like URL filtering, deep content inspection, and cloud app visibility and control. Employees can no longer skirt security policies because you can block the use of any unsanctioned cloud service. Additionally, full audit and granular control over app usage and activities simplify compliance in the cloud. With a data-focused approach, you can easily extend DLP to the cloud with seamless integration.

Network security delivers efficient, reliable security using cloud-native firewall and web proxy services for accessing the internet, without the need for hardware at every location. Your branch offices and remote employees can connect automatically using integrated, secure SD-WAN and unified endpoint agents, respectively. And instead of forcing users to deal with painful VPNs for SaaS and private apps, SASE incorporates Cloud Access Security Brokers (CASB) and Zero Trust Network Access (ZTNA) systems that keep out ransomware, while keeping in sensitive data.

Advantages of Forcepoint's Approach to SASE

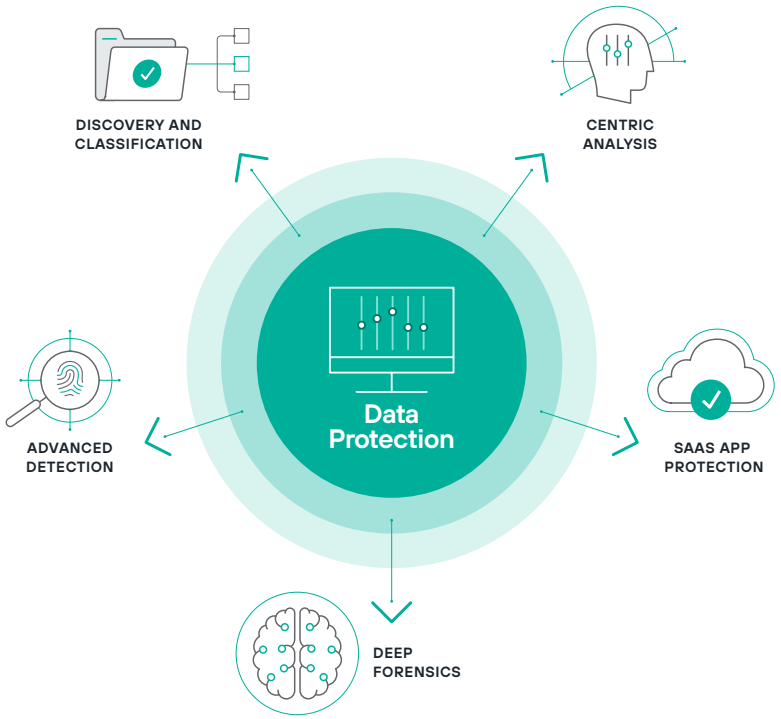
Advantage #1: Unified data security policies
Managing a patchwork of point products is cumbersome and simply doesn't scale, especially as users do more work beyond the corporate perimeter. Forcepoint's Data-first SASE platform enable teams to write security policies once and enforce everywhere from the endpoint through the network into the cloud.

Advantage #2: Unified agents
The Forcepoint platform integrates software for safely accessing resources, enforcing security policies, and monitoring activity on endpoint devices. The architecture eliminates agent sprawl and provides a single piece of software that is easy to deploy and maintain.

Advantage #3: Flexible deployment
True data-first SASE should deliver efficient, safe access to web, cloud, and private resources no matter where your people are working. The platform must integrate rich context-based controls, hybrid enforcement at sites with special requirements (i.e, compliance), and secure SD-WAN without requiring extra products. Don't ever compromise your enterprise just because of a vendor's cloud-only or point-solution based model.

Advantage #4: Risk-adaptive policy enforcement
Consider how often you review your web security or DLP policies. Or how often you should, given how quickly things change. Instead of a static, block-and-allow model that requires security to spell out every possible combination of compromise and remediation, Forcepoint introduced a game-changing approach that automatically adapts security response to risk. We call this risk-adaptive protection. The understanding of risk personalizes enforcement based on people's behavior as they use data, apps, and systems.

- Discover data everywhere
- Classify data with integrations (inc. Microsoft Azure Information Protection, Boldon James, Titus)
- Leverage advanced detection and forensics like fingerprinting, OCR and machine learning
- Quickly build from largest policy templates available for compliance and critical IP protection



"Something Forcepoint does that others don't is converging or consolidating cloud-based and traditional DLP. We see that as a really big story. The enterprise DLP model is not as important with more and more data going to the cloud."

JOHN GRADY, ANALYST, ENTERPRISE STRATEGY GROUP

Related Resources

- → **Your fast ramp to data-first SASE: Schedule a SASE 101 live demo**
- → **View the ESG webinar on-demand: Practical Steps to SASE and Zero Trust**

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.