CATO NETWORKS

iF TECH AG part of connexta

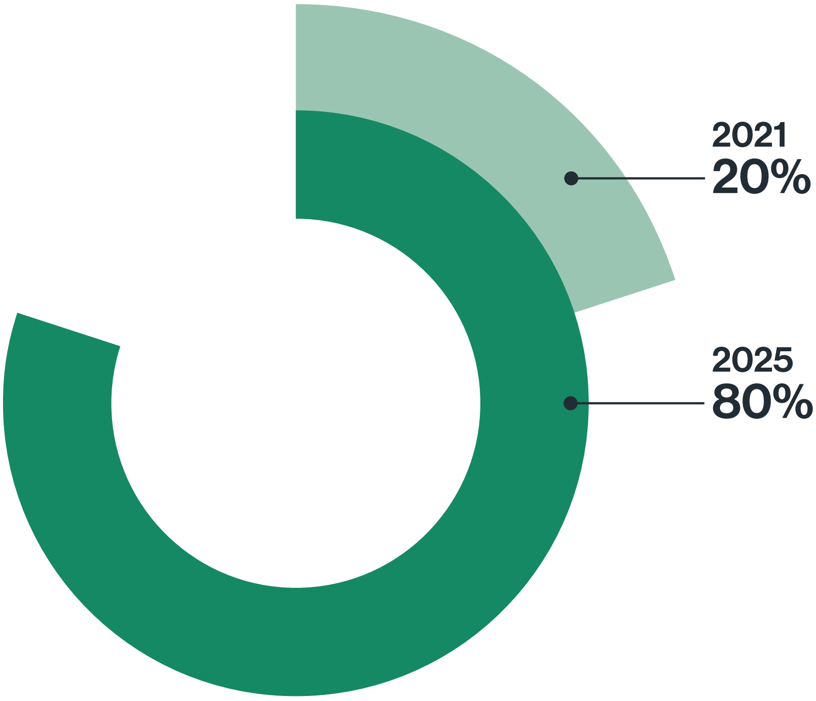
How to Plan a SASE Project

Summary

For decades, enterprises have been stuck on a complex and rigid architecture that has prevented them from fully executing their digital transformation strategies and achieving business agility. But now there is a much more flexible alternative. SASE (Secure Access Service Edge), defined by Gartner in 2019, describes a single architecture converging enterprise networking and security point solutions into a single architecture that is cloud-native, globally distributed, and secure for all enterprise edges – remote users, sites, and cloud resources.

Gartner estimates that by 2025, 80% of enterprises will have adopted a strategy to unify web, cloud services, and private application access using SASE, up from 20% in 2021. There are significant benefits to implementing a SASE architecture, including increased operational efficiency, a more consistent user experience, improved application and network performance, improved security, and much more.

SASE Convergence Strategy Adoption per Gartner



Most organizations need a migration plan to go from traditional hub-and-spoke wide area networking with a legacy security perimeter to a new flexible SASE architecture. Making that shift requires good planning. If your company is just beginning this journey, we offer this game plan for developing a realistic project roadmap toward SASE adoption.

Develop the Team

Your organization may still be functioning with a legacy architecture that has separate security and network operations teams. One team could, in theory, drive a SASE migration – Cato can certainly be deployed by one team to address a particular challenge — but ideally, networking and security groups should work together to design the future network. Security is too essential to network operations today for compartmentalized decision-making, and network operations and performance is too important to the user experience to be ignored.

Depending on your company culture, it may be beneficial to appoint a neutral person to lead the project team, such as a program or project manager or a digital transformation leader who isn't tied to the specifics of security or network architecture. This leader's role is to ensure that all requirements are considered and communicated well to the rest of the team.

Owners of your organization's most strategic applications also may be part of the team. They have a vested interest in the performance and security of the applications and their data assets, as well as the user experience of working with these applications. These are important considerations of the SASE architecture.

Gartner also recommends including personnel involved in workforce transformation and branch office transformation on the project team. This is especially important if your SASE project is part of a larger company-wide digital transformation effort in which business processes and ways of work are expected to change significantly.

Why Do You Want SASE? Define Your Objectives

This document assumes a focus on the transformation journey of a SASE deployment with headquarters, branch offices, remote users, and cloud resources. Of course, your enterprise's specific needs may vary from others.

Among the most common objectives companies cite when planning a SASE implementation are:

Facilitating Work from Anywhere (WFA) and Remote Access

Pandemic lockdowns drove people out of branch offices and into remote work environments. Even today, with most restrictions lifted, remote work continues to be a popular – and possibly long-term – workstyle for many people. Plan to manage secure access requirements for a more distributed workforce for the foreseeable future.

Supporting Global Locations of the Business

Your company must have an affordable and consistent means of transport to connect to physical and cloud datacenters and it must be more reliable and secure than the public Internet.

Enabling Secure Direct Internet Access (DIA)

With a legacy architecture, securing Internet access in the branch office is a tough tradeoff between deploying security appliances everywhere or backhauling internet traffic to a secure location. Branch security appliances come with significant operational complexity – forcing IT teams to manage hardware upgrades at inopportune times to accommodate more traffic or CPU-intensive features – and backhauling traffic adds latency. An efficient SASE architecture enables secure DIA through the provider's nearest Point of Presence (PoP), eliminating the need to deploy a security appliance or backhaul traffic to a distant secure location.

Providing Access to Cloud Resources and Applications

Your organization needs an optimal connection to the cloud from anywhere in the world – i.e., where the users are – not just premium connectivity from your corporate datacenter.

Gather Requirements

Before planning what SASE solution to deploy, you need to determine your requirements in terms of the sites, the people/users, and the cloud resources you need to connect and secure. It's also prudent to design for future considerations in order to minimize disruptions or rework when new requirements arise down the road.

Sites

Work sites, or branch offices, come in many sizes and purposes—from small to large, and from critical functions to a simple home office. You need a network that can adapt to all, offering availability levels to meet the requirements of each type of office. The SD-WAN connectivity portion of SASE creates flexibility by integrating Internet transports such as cable, DSL, fiber, and 4G into the WAN and forming a virtual overlay across all transports. With features like load balancing and measuring the real-time transport quality of each circuit, SD-WAN provides the high uptime your business demands by using a mix of Internet connections.

It's helpful to categorize your various sites by their significance, matching last-mile availability and performance measurements to site importance. Being able to mix and match circuit types and quantity allows you to meet the specific availability requirements of each branch office without overprovisioning. Some examples of connectivity you may choose to meet requirements without overspending include:

Headquarters or critical branch
Redundant fiber with local SLA

Regional branch
A mix of DIA and broadband

Small branch or home office
Redundant broadband

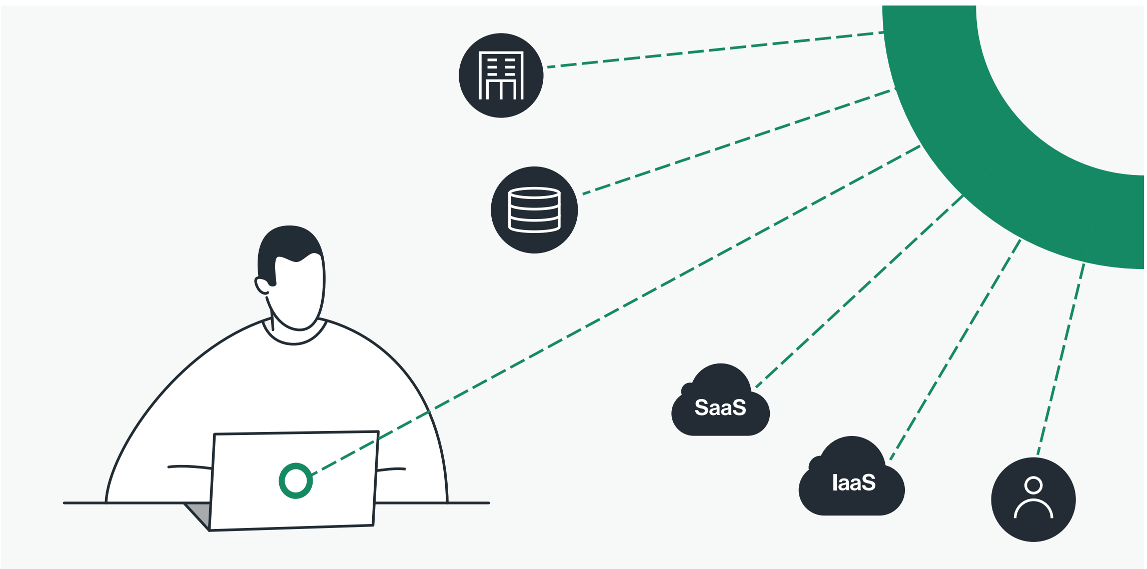
You also may have special transport considerations for applications to ensure their optimal performance. For example, real-time applications such as voice and video deteriorate when there is latency, jitter, or packet loss. It's important to understand what applications are being run in order to plan for better performing circuits and techniques like packet duplication and fast session failover for real-time applications.

You may need to plan for high availability (HA) at the networking and security layers of the infrastructure for certain sites. With SASE being a cloud-delivered service, the primary burden of building HA sits with the service provider. The networking and security logic is in the cloud service, which simplifies HA design for you. Nevertheless, there are some choices your organization can implement to ensure the resiliency of site-based components such as edge connectivity devices.

Users

Remote and mobile users – those who work from anywhere, or WFA – have various requirements pertaining to usability, performance, and security. In SASE parlance, this type of user is just another edge that needs to have similar capabilities as people working in a branch office.

SASE solutions typically require a software agent on the user's device to connect to your network. Some providers may allow a simple browser connection to a URL that enables connectivity. Consider the ease of use needs of your WFA users to make their experience as frictionless as possible.



Map the general locations of these users and compare them to the locations of PoPs offered by SASE providers. You will want to have the PoPs as close to users as possible to reduce latency for better application performance. A standard measure of acceptable latency is 25ms or less for a roundtrip of traffic to/from the nearest PoP. Anything higher will create a frustrating user experience.

WFA users need the same security services as people who work in branch offices. This creates a challenge in figuring out where to put the security stack. Legacy networks have the security stack in a central datacenter, which forces network traffic from remote locations and mobile users to be backhauled to the corporate datacenter where it exits to the Internet through the corporate's security appliances stack. Network responses then flow back through the same stack and travel from the datacenter to the remote user. This twisted path, resembling the bent pipes of a trombone, has a negative impact on latency and therefore on the user experience.

Some SASE solutions recommend hosting security in regional hubs that serve as mini datacenters. This approach reduces the end user performance impact by backhauling to the nearest hub. However, the fundamental issue of managing multiple instances of the security stack remains as well as the need to set up distributed datacenters and address performance and availability requirements.

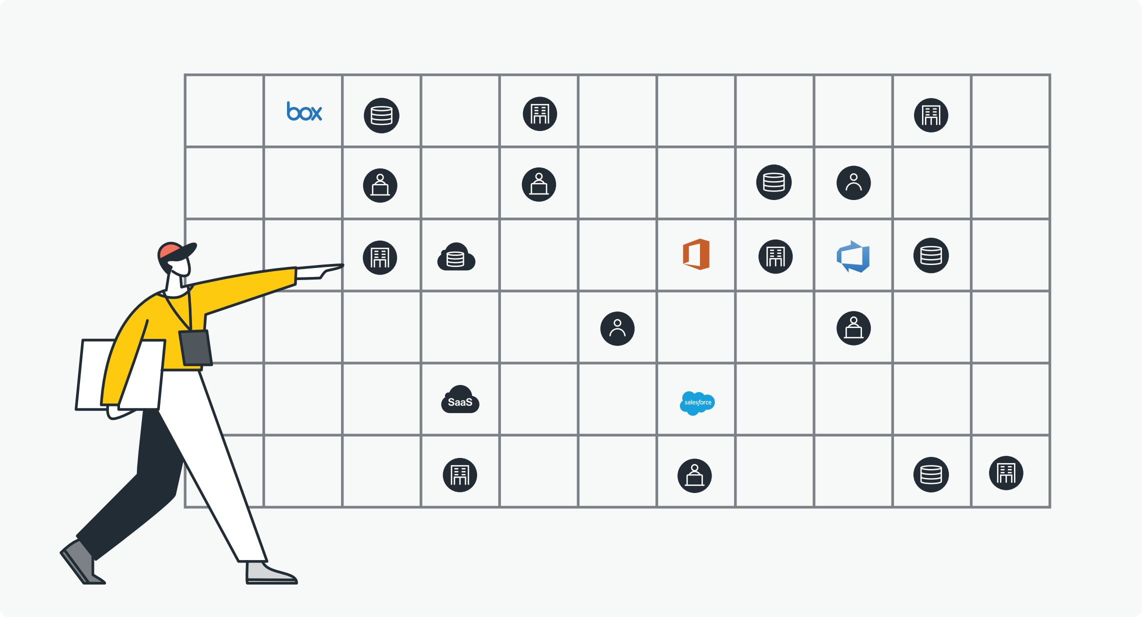
Look for a SASE solution that hosts the security stack in the PoPs where WFA users connect to the network. With security being an integrated component of the PoP, there is no need to maintain and manage separate security appliances. What's more, a single security policy can apply to every user and every edge coming into the PoP.

Cloud Resources

When resources and applications are said to be "in the cloud," few people stop to think that this means they are physically located in a datacenter somewhere in the world. That location is critically important when it comes to latency and performance of applications.

The further the datacenter is away from users, the longer the round trip is for traffic going to and from the application, and the worse performance users can see from the application. Top-tier hosting companies like Equinix, Rackspace, and Verizon, as well as cloud platform companies like Amazon, Microsoft, and Google, have numerous regional datacenters, which allows customers on those platforms to host their applications closer to their users.

An important part of planning a SASE implementation is to map all of the resources your company has in the cloud, including SaaS applications like Microsoft 365, SAP, Salesforce, and countless others. Some applications can actually be located in several different cloud hosting datacenters around the world. Microsoft, for instance, has microservices hosted in numerous distributed datacenters. Knowing these hosting locations, as well as the locations of your users, will help you estimate application latency, which directly impacts application performance.

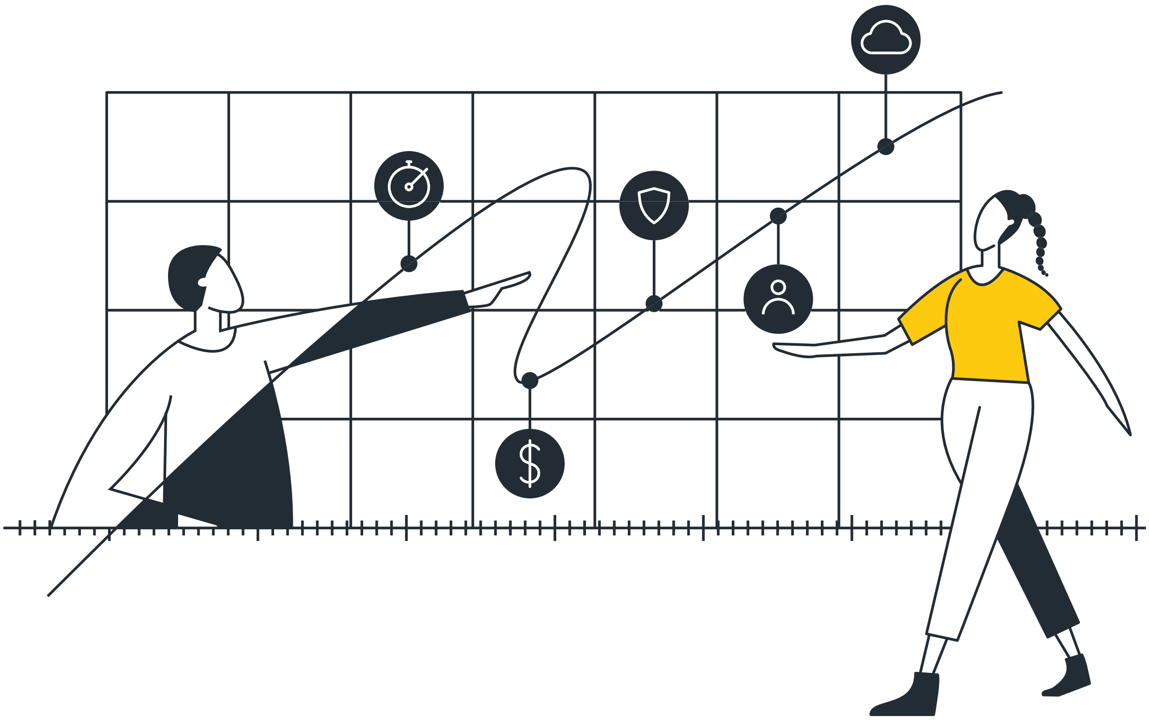


A SASE solution is going to have PoPs in the cloud that serve as on-ramps to SaaS and other cloud services. Some of these PoPs might even be located in the same co-location datacenters (i.e., peer locations) as major SaaS applications – a big advantage for application performance and the user experience – but this isn't always the case.

Thus, you must conduct a thorough identification of the regions where cloud resources reside, and a mapping of those locations onto a SASE solution's ability to interconnect with those regions. Application performance would be greatly enhanced if users connected to a regional PoP can go to the nearest instance of the application, rather than having traffic traverse the network to get to a distant host datacenter.

Future Considerations

Your planning team must “future-proof” the network to accommodate potential business needs—even if they are not yet known. It’s an important exercise to avoid building an inflexible solution that can’t easily adapt as business needs emerge and evolve.



Your company, like most others, probably has growth as a strategic business objective so as not to be overtaken by competitors and becoming irrelevant in your markets. Your technology platforms must be growth enablers that can adapt quickly as business changes.

Some of those changes could involve expanding into new locations, which of course would require secure networking capabilities. A cloud-delivered SASE solution can be turned up in days, whereas it might take months, or longer, to acquire MPLS circuits for traditional networking—if they are even available in the regions of your expansion. Opening a new facility in China, for example, can be troublesome if you need to install the circuits for yourself, or if a specific SASE solution doesn’t have PoPs in that region.

Company growth can come from mergers and acquisitions. When a deal closes, it’s imperative to bring the two companies’ IT systems together as quickly as possible. With a legacy network, integration of the systems can take years, whereas with a SASE platform, turning up new services for the acquired company can be accomplished in days to weeks.

Your organization will probably continue to migrate more and more applications to the cloud over time. As discussed above, where a SASE solution’s PoPs are relative to where applications are hosted in the cloud is critically important to application performance. Look for a SASE offering with a global distribution of PoPs.

In short, a SASE platform converges all the capabilities you need today and tomorrow. By contrast, a non-SASE approach forces you to find, evaluate, buy, integrate, and manage, multiple products to cover each requirement. Think how much time you will save by not doing all this work and just flipping a switch on new capabilities when you are ready.

Write an RFI

Once you have collected your requirements and understand what you want and need from a SASE solution, it's time to reach out to a few vendors with a Request for Information (RFI) to see how they propose to address your needs. This will help you understand the marketplace as well as your options before going forward with a Proof of Concept (PoC) project.

Your RFI should include the following:

Business and IT Overview

You want vendors to understand your environment well enough to tailor their responses to your needs and point out how their solution is specifically valuable in your context. This section covers your business, your SASE project goals, what geographies you operate in, and what network resources are covered. Also include a more detailed overview of your network topology, current networking and security stack, and how you currently connect and secure the different network connected entities.

Solution Architecture

While many SASE offerings include similar capabilities, the way these capabilities are delivered affects cost, complexity, and the overall success of the project. You want to understand the architectural elements—what they are, what they do, where they are placed (branch, device, cloud), how they scale, how they address failures and deliver resiliency, and more.

Solution Capabilities

The aim of this section is to understand the functionality provided by the solution across multiple areas such as SD-WAN, cloud, security, mobile, and more. Choose the requirements relevant to your network.

Support and Services

Get to know a vendor's support structure and available managed services. For global organizations, follow-the-sun support models are essential. And, if you are coming from a telco contract and are used to a fully managed service, this project can create an opportunity to move towards a self-service or co-managed model.

Plan a Gradual Deployment (Sites/Capabilities)

By planning a gradual deployment, you can start small with a few sites and then grow incrementally once you get a good feel for what you are doing.

There are several common use cases that will give you a gradual transition to SASE:

MPLS Migration to SD-WAN

Migrating from MPLS to SD-WAN is made simple with a SASE architecture, as it supports running MPLS in parallel with SD-WAN. This means you can transition only certain sites, turning them down on your own schedule, or even just start with new sites. All legacy security and remote access solutions are left in place, and only the SASE SD-WAN functionality is leveraged. You get the benefits of building flexibility into your last-mile transports but don't gain the simplified security benefits of SASE.

Optimize Global Connectivity

Improving performance across global sites and applications is often a big driver for migrating to a SASE architecture. In this use case, you may choose to keep your MPLS connections for critical WAN applications and eliminate all traffic backhauling. Either way, SASE can be used to improve connectivity to Internet and WAN applications or locations, especially those where MPLS isn't feasible.

Secure Branch Internet Access

Securing Internet access from the branch is another reason to migrate to SASE. If you have MPLS with Internet breakout or direct Internet access with no MPLS, you need edge security. SASE eliminates all edge security devices, including NGFW, SWG, IPS, and AM, by routing all traffic through a cloud-based security stack.

Cloud Acceleration and Control

Sometimes improving performance and control of cloud datacenters and applications drives the move to SASE. With a global network of PoPs, SASE creates a private and optimized network access to cloud datacenters. SaaS applications benefit from advanced routing rules, ensuring that traffic continuously travels across the optimized network, not the unpredictable Internet.

Remote Access

With today's work from anywhere requirements, VPNs struggle to keep up with the business. Here you can turn to SASE to scale your remote users' access quickly, without having to add additional VPN servers or compromise on security. SASE ensures remote users' traffic is secured and optimized by connecting them to a network of global PoPs.

Build the Business Case

Network transformation is a game-changing strategy that helps drive business growth and market acquisition. Thus, a migration to SASE is a decision for your Board of Directors to make. Getting their approval is key to supporting the long-term ability to execute and advance business objectives.

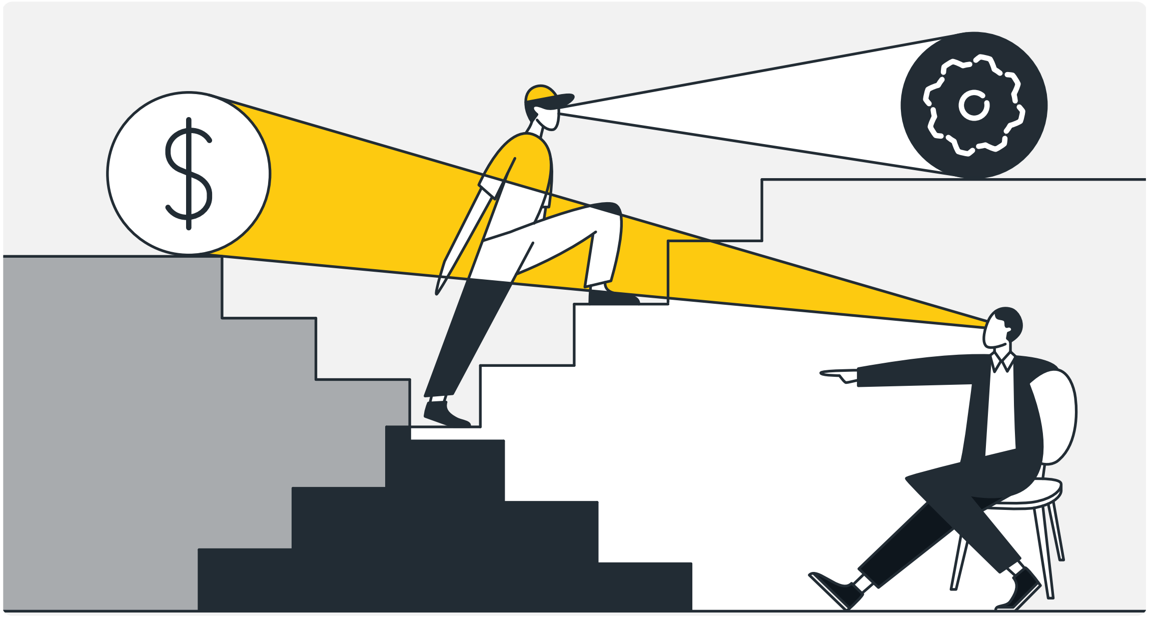
When addressing the board, CIOs must position such technology strategies with critical board-level concerns in mind and discuss them in the context of:

- How this strategy can help the company improve IT responsiveness and the ability to support business growth
- The value the business will realize through this initiative
- The positive security impact of this strategy on critical applications
- How this strategy enables the IT organization to better mitigate increasing security risk
- The short- and long-term financial impact of this initiative
- The impact on the company's current and next generation of IT talent

Core to discussing these strategies is articulating the necessity of simplification, optimization, and risk mitigation in delivering business outcomes through network transformation. And this is where Secure Access Service Edge becomes that strategic conversation for board-level engagement.

SASE is the network transformation strategy that addresses board-level concerns around risk, growth, and financial flexibility. SASE converges networking and security capabilities into a single high-performing cloud-native architecture that allows organizations to scale core business operations through efficiency and performance, while extending consistency in policy and protections.

Boards are laser-focused on the long-term financial performance goals of the business. The board needs to understand how network transformation will improve their balance sheets and customer retention. While many CIOs hesitate to link technology investments to financial performance metrics, articulating the positive impact of SASE on financial performance can position it as an ROI-enabler.

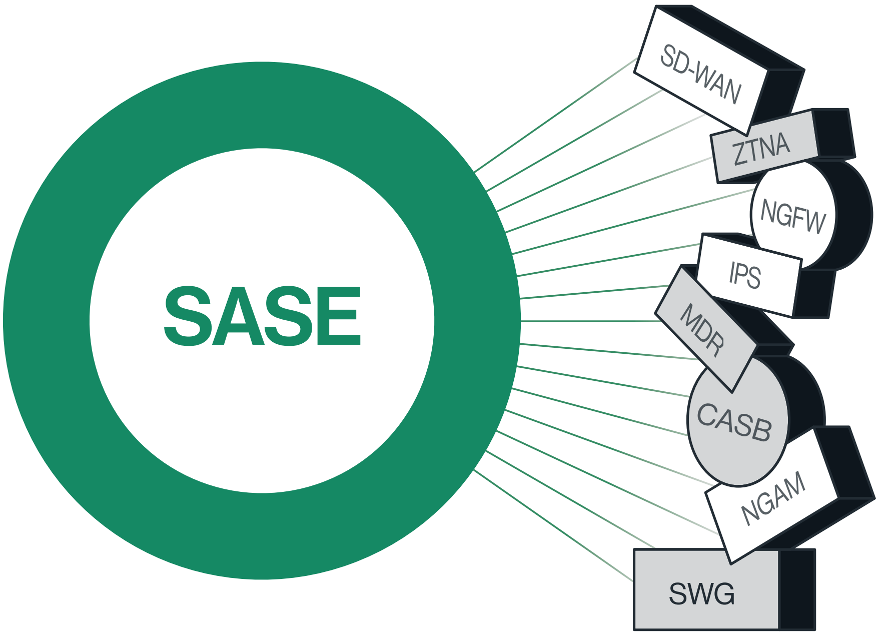


The financial impact of migrating to SASE can vary greatly from one solution vendor to another, and we can't speak for our competitors. However, we can give you a look at the Total Economic Impact of a solution from Cato Networks, with data compiled by Forrester based on in-depth interviews with real Cato customers. Forrester aggregated the interviewees' experiences and combined the results into a single composite organization. In short, the composite customer saw a 246% Return on Investment and Net Present Value of $4.33 million, with an investment payback period of less than 6 months. The Forrester report is a good guide on how to build and present the financial case for any SASE solution.

Build Consensus Within the Networking and Security Teams

Once the decision is made to deploy at least some aspects of SASE, the next challenge is to build consensus among the networking and security teams. Getting their buy-in is crucial, as they may perceive their jobs as being in jeopardy if the technologies they currently support are changing or being eliminated.

An imperative for consensus building is to highlight use cases where SASE proves its strategic value across the entire enterprise. A successful SASE implementation will make it easier to pursue cloud migration, work from home initiatives, Unified Communications as a Service (UCaaS), and global expansion projects, just to name a few. These and other use cases show how SASE not only eliminates networking and security headaches by reducing complexity, but also how it streamlines the efforts of IT teams, allowing them to place more focus on strategic initiatives to support business goals.



SASE offers security professionals the opportunity to reduce risk in their environment—the entire objective of their jobs. Years of acquiring point products to solve point problems have bloated technology environments, resulting in security blind spots, increased complexity, and unmanageable risk. SASE proves its risk mitigation value by simplifying protection schemes, increasing visibility, improving threat detection and response, unifying security policies, and facilitating easier auditing. SASE also has a simplistic Zero Trust access approach to critical applications, delivering consistent policy enforcement across the entire network.

Run the Proof of Concept Project

A SASE solution is unlike the legacy networking and security configuration you have today. What's more, solutions from the various SASE vendors are different from each other. Before you make a commitment to a particular solution, it's best to do a trial run with a Proof of Concept (PoC) project based on one of your use cases. The PoC will give you the experience needed to make a confident decision in your choice for implementation. Keep your PoC plan simple and limit it to no more than two or three vendors, each tested for approximately 30 to 60 days.

Choose a use case or two that closely mirrors your goals for the full SASE implementation. Include branches and users in different geographical locations to get a good feel for connectivity to the PoPs, performance of applications, and the user experience. Be sure to test the different types of circuits that would ultimately be deployed in your full project. Test as much as possible in full production mode. If you intend to leave legacy equipment in place following full implementation of your SASE solution, test how well it can integrate with new components and equipment.

Before beginning the PoC, develop a test plan with a number of scenarios and determine how you will measure success. If you plan to test more than one vendor's solution, determine the metrics you will use to compare the two solutions. To the extent possible, include a cost-benefit analysis to help you estimate expected savings on the full implementation.

Document any issues or failures, including why you believe they occurred. It could be something inherent in the solution you are testing that could indicate this is not the way to go for a broader implementation.

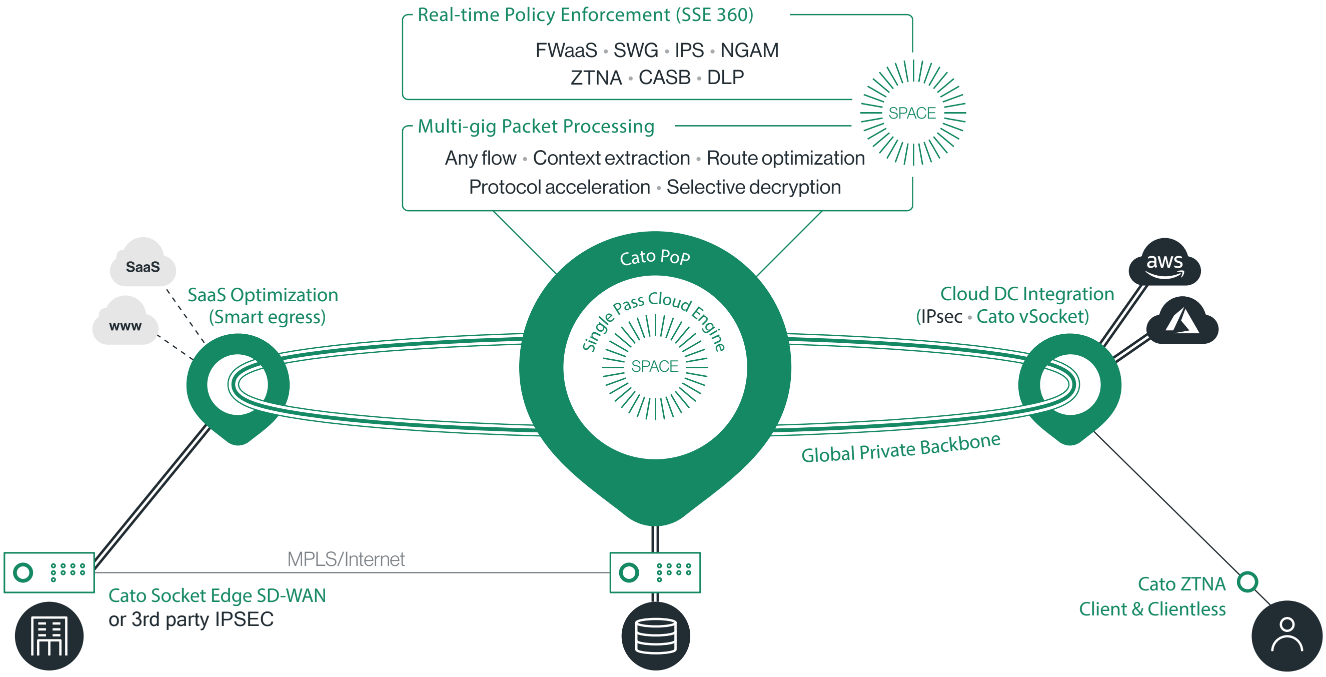
Make the Decision

You know your objectives for migrating to a SASE architecture. You have definite use cases in mind. The Board supports your recommendations for a new approach to how SASE technology can support and further enable the business. Your networking and security teams are anxious to roll this out. You've tested a model or two and know how they perform for you. The cost-benefit analysis hints at the savings you can expect. With all of these chess pieces in place, you can feel confident that you've done your due diligence and can now select your SASE solution.

Cato: The Global SASE Platform for Whatever Comes Next

Cato provides the world's leading single-vendor SASE platform, converging Cato SD-WAN and a cloud-native security service edge, Cato SSE 360, into a global cloud service. Cato SASE Cloud optimizes and secures application access for all users and locations everywhere. Using Cato, customers easily replace costly and rigid legacy MPLS with modern network architecture based on SD-WAN, secure and optimize a hybrid workforce working from anywhere, and enable seamless cloud migration. Cato enforces granular access policies, protects users against threats, and prevents sensitive data loss, all easily managed from a single pane of glass. With Cato your business is ready for whatever's next.

Cato SASE Cloud with SSE 360



For more details, please contact us

Elisa Schumann
IF-Tech AG
Willy-Brandt-Allee 4
81829 München
+4989200066929
elisa.schumann@if-tech.de

IF TECH AG
part of connexta

Cato SASE Cloud

SSE 360

Secure Remote Access

Edge SD-WAN

Global Private Backbone

Multi-cloud / Hybrid-cloud

SaaS Optimization

Cato Management Application

Use Cases

MPLS Migration to SD-WAN

Secure Remote Access

Secure Branch Internet Access

Optimized Global Connectivity

Secure Hybrid-cloud and Multi-cloud

Work From Home

Cato. Ready for Whatever's Next.

SASE, SSE, ZTNA, SD-WAN: Your journey, your way.