citrix

Solution Brief

Accelerate your Secure Access Service Edge (SASE) Journey

Empower your hybrid workforce with a unified, flexible, and comprehensive approach to SASE

Digital transformation, cloud adoption, and the expanding hybrid workforce have fundamentally changed the dynamics of the security and connectivity landscape. Businesses like yours rely on applications, and now more than ever, your employees are using managed and unmanaged devices to access those business apps over the internet. Hybrid work has become the new reality increasing the attack surface and exposing your business to new threats that are coming out at a faster rate than ever before.

With this shift, the corporate network has been redefined. Traditional enterprise architectures and siloed approaches relied primarily on datacenter security, point products, and redundant firewalls in their corporate or branch networks. These approaches don't work for today's dynamic app delivery, connectivity, compliance, and security requirements. Cybersecurity, IT, and networking professionals have been working to maintain and scale security while ensuring business continuity and a great employee experience. Traditional network security approaches have shown to be complex, time-consuming, inefficient, expensive, and could leave enterprises vulnerable to growing cyberthreats.

Key challenges with point products and traditional approaches to security and networking:

- **Insufficient, disjointed, and inconsistent security:** Multiple logins and overlapping security policies can lead to insecure practices and increase security risk
- **Increased IT cost and complexity:** Managing multiple vendors is costly, inefficient, and complex
- **Poor and inconsistent experience:** Poor end-user and IT experience, productivity loss, slow adoption, and shadow IT

To meet modern enterprise needs and empower a secure hybrid workforce, organizations need to rethink their approach to network security, connectivity, and application delivery. That's where Secure Access Service Edge (SASE) plays a role. Embracing SASE will help to address several of the challenges and complexities we face today with traditional and siloed approaches. A comprehensive and fully integrated SASE architecture will help you accelerate your cloud transformation journey and securely enable your modern hybrid workforce.

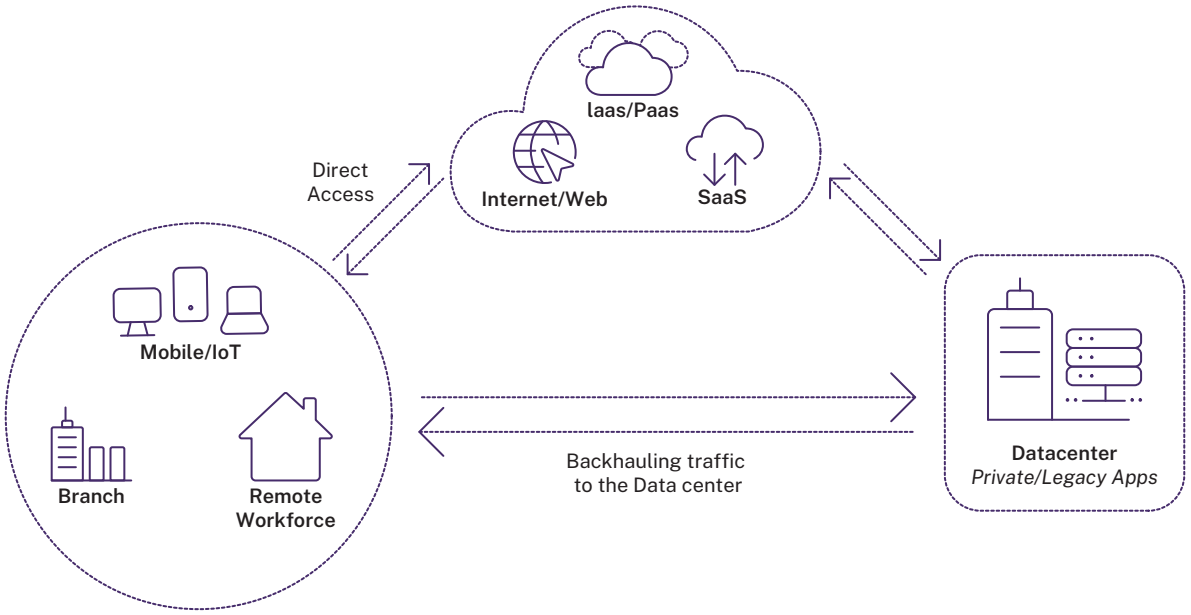

Figure: Challenges with Traditional Network Security Approaches

What, exactly, is SASE?

SASE is a leading architectural framework that can help you reduce complexities in today's distributed enterprise environments and simplify secure access for your hybrid workforce. SASE brings together SD-WAN and comprehensive cloud-delivered security services including zero trust network access (ZTNA), firewall as a service, secure web gateway (SWG), cloud access security broker (CASB),and all other core and recommended technologies into a unified architecture.

When combined into a single solution, SASE enables organizations to provide fast, secure, remote access to all internal and external apps across public and private clouds, web, internet, and software as a service (SaaS), without straining IT. And it's built to meet the complex needs of distributed hybrid workforces.

Historically, networking and security solutions were delivered as individual products that resided in the datacenter and managed in siloes by separate IT teams, creating a bottleneck that affected user experience and increased IT complexity. Solutions that are designed from the ground up with a unified approach to bring simplicity and consolidation of networking and security technologies with a best-fit approach can provide the true value of a SASE model.

Key characteristics of a unified and complete SASE solution:

- Comprehensive cloud-delivered security stack with a zero trust approach
- Optimized application experience through resilient connectivity
- Unified management & orchestration across networking and security
- Global and consistent presence with points of presence
- Customer data privacy to meet compliance and regulatory requirements

Reduce risk and deliver business results faster with a unified SASE architecture

As your enterprise modernizes, implementing a unified and comprehensive SASE solution from a single vendor and a flexible ecosystem that can work with your existing technologies, will help to effectively drive business initiatives forward while reducing risk and complexities.

Here are some key business outcomes and benefits of implementing a unified and comprehensive SASE architecture:

Improve the user experience

- Increase user productivity and optimize application experience
- Deliver resilient connectivity and consistent, secure access on any device
- Eliminate latency from backhauled connections and experience consistent connectivity performance even as internet performance fluctuates

Enhance IT agility and simplify operations

- Reduce operational cost and complexity
- Consolidate vendors across networking and security
- Deeper integrations and unified management to simplify deployment, configuration, reporting, and support services
- Reduce overall hardware footprint and improve architectural elasticity and scale

Ensure business continuity by reducing cyberthreat risk

- Protect all users at any location against all threats at scale
- Zero trust network access with comprehensive cloud-delivered security services to secure access to all types of applications

Accelerate your SASE journey with a business-centric approach

With several vendors and multiple point products offering SASE solutions, it has become difficult for organizations to pick the right solutions. Each organization will have a unique path toward a complete, mature SASE architecture, which won't happen overnight.

SASE could bring a lot of change to your organization. Start planning your SASE journey with a focus on your expected business outcomes and prioritize use cases that will help to address these outcomes so you can plan and execute your SASE implementation strategy with more confidence.

Every SASE journey is unique. After identifying expected business outcomes,assess your current environment to identify technology gaps, available resources, allocated network, and security budgets. You also need to identify critical apps you'll need to support your business to create a baseline for your security strategy. It is important to understand how your IT is going to manage transformation to a SASE architecture operationally and plan to migrate from legacy technologies.

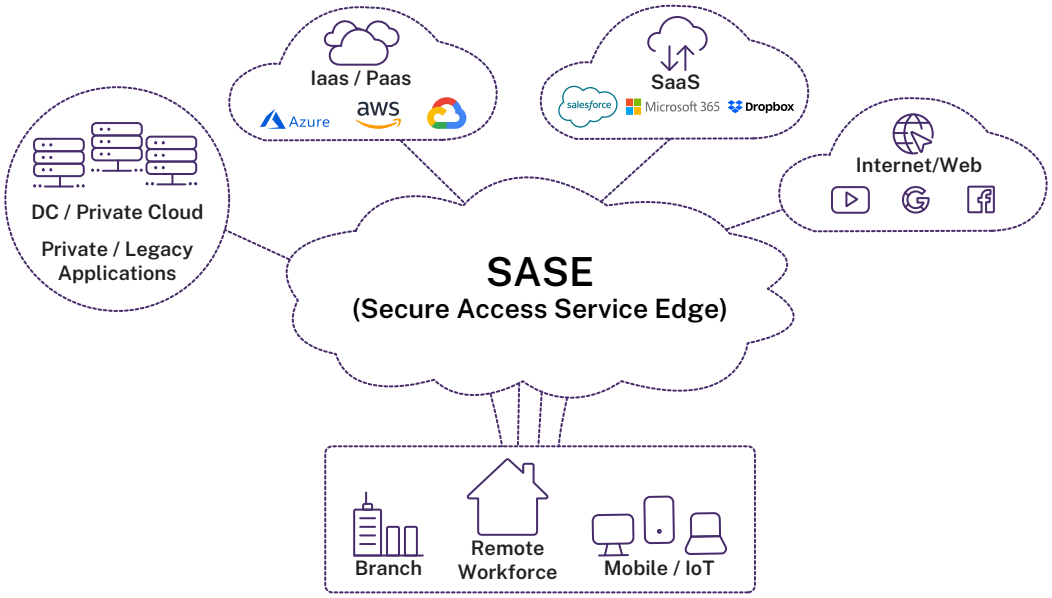

Figure: Embrace SASE for Modern Hybrid Workforce

Each organization may have its unique use cases to empower secure, distributed work. Here are key use cases to consider on accelerating your SASE journey:

Enable secure access to business SaaS and Internet applications

- Without the complexities and expense of datacenter-based security
- Through comprehensive cloud-delivered security to access internet and SaaS app access

Implement ZTNA to secure access to high-risk enterprise sensitive private and IT sanctioned applications

- Zero Trust Network Access (ZTNA) to all IT sanctioned apps
- A Cloud delivered zero trust access to all IT sanctioned apps reduces risk and enables intelligent, adaptive, and consistent security policy for any app, any location, and any device
- It also allows you to reduce dependency on cumbersome VPN solutions

Secure, reliable, and always on connectivity for branch & remote users

- Deliver always-on network and reduce costs by consolidating routing and security hardware in your branch locations.
- Quickly roll out new cloud-based apps, monitor connectivity to these apps from your branch locations, and ensure bandwidth is fully optimized.

A strategic, flexible, and unified approach to SASE

A SASE architecture includes several core and recommended components; flexibility is key to implement and accelerate your journey. Citrix SASE solutions deliver all core and recommended SASE security functionalities within a unified solution and a single-pass architecture for lower latency and better performance.

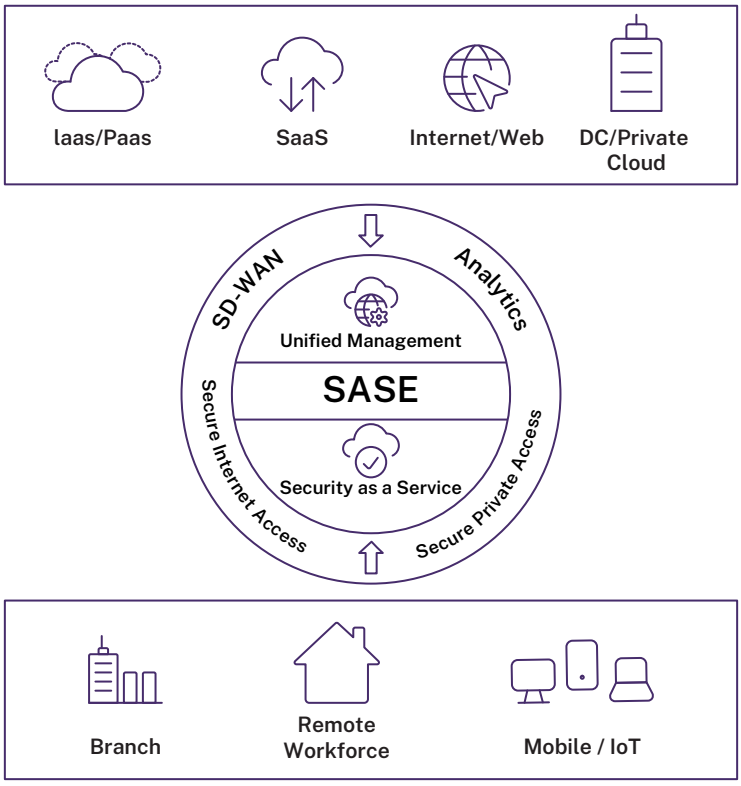

Figure: Citrix SASE architecture overview

SASE is all about enabling a simple and secure access experience for your hybrid workforce while reducing costs and complexity and requiring less effort to manage the environment. The Citrix approach to SASE brings together networking and security into a unified solution that supports a simpler way to enable secure access to apps and data, without complicating the user experience. Citrix's fully unified, ready-to-deploy SASE portfolio delivers flexible and comprehensive core and recommended capabilities.

The solution integrates Citrix Secure Access solution, and resilient connectivity through Citrix SD-WAN to empower your hybrid workforce with the best, most secure access experience through Citrix Workspace and for all apps.

SASE Implementation Methods

Choose the deployment option that best fits your unique needs and business goals. There are core components you might consider deploying first such as SD-WAN, SWG, CASB, ZTNA, FWaaS (with IPS), identity-sensitive data, and malware protection. Also, you might add WAAP, RBI, sandbox, API-based access to SaaS for data context, and support for managed and unmanaged devices.

Considering all these different components might be hard to figure out where to start your journey. The flexible ecosystem and closely integrated components within Citrix's unified SASE architecture make it easy to deploy and enable you to take a logical and flexible path that fits well with your existing environment and technologies. It allows you take different approaches to start your SASE journey.

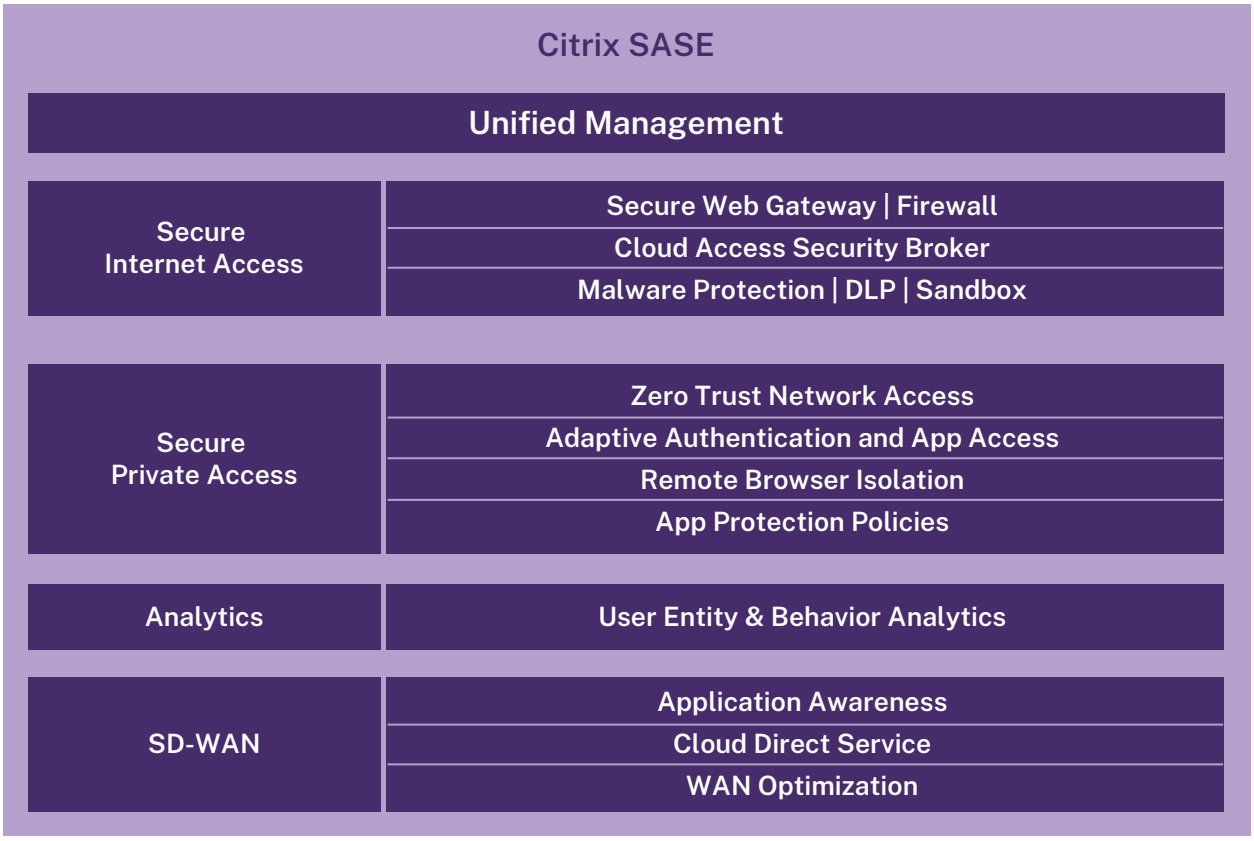

Figure: Citrix delivers unified, flexible, and comprehensive SASE solutions

Security-First Approach

When evaluating security solutions towards a unified SASE architecture, IT and security professionals should consider key factors including how quickly they can enable secure access through a cloud-delivered security stack to protect users, apps, and data with end-to-end contextual security.

Citrix Secure Access Solution

Unlike with traditional approaches and point product solutions, with Citrix Secure Access solution, your applications are continually protected — no matter where employees work, which devices they use, or what your infrastructure looks like. Citrix Secure Access solution provide the fully integrated, automated solutions businesses need to keep applications secure and employees productive:

- Citrix Secure Private Access is a VPN-less solution that delivers Zero Trust access with adaptive authentication and SSO to IT sanctioned applications (web, SaaS, client-based, and virtual applications). It provides security controls for managed, unmanaged and BYO endpoints thus giving end users device choice while improving the overall user experience. Request a demo to see Citrix Secure Private Access in action.
- Citrix Secure Internet Access offers a comprehensive, cloud-delivered security stack so you can empower users with the most secure experience possible — for any app, anywhere, on any device. This complete security platform includes a secure web gateway (SWG), cloud access security broker (CASB), data loss prevention, next-generation firewall (FWaaS), malware protection, sandbox, and more. These security capabilities work together to enable secure access to the internet and SaaS and protect remote users, without the complexities and expense of datacenter-based security. Request a demo to see Citrix Secure Internet Access in action.
- Citrix Web App and API Protection service offers holistic, layered protection against known and zero-day application attacks. This cloud-based service combines a web app firewall, bot management, and DDoS protection to keep all application types secure and help you maintain a consistent security posture. Request a demo to see Citrix Web App and API Protection in action.
- Citrix Analytics for Security uses sophisticated machine learning and artificial intelligence to continuously assess, detect, and prevent risks. Each user is assigned an individual risk profile, with scoring that's adjusted based on real-time activities. When an anomaly or suspicious action is detected, Citrix Analytics for Security acts immediately to proactively prevent unauthorized access to apps. These behavior-based analytics ensure your users can be productive from any location and device, while your company stays protected. Request a demo to see Citrix Analytics for Security in action.

Networking-First Approach

When evaluating networking solutions towards a unified SASE architecture, network administrators and business managers should consider certain factors including ease and speed of deployment, the simplicity of the move to secure hybrid work model, intelligent traffic management, high performance, and an always-available WAN edge solution that provides an exceptional experience, and seamless business continuity.

- Citrix SD-WAN accelerates digital transformation with flexible, secure connectivity for cloud and virtual applications. A comprehensive SASE-ready SD-WAN with automation, policy-based enforcement, zero-touch deployment, and intelligent reporting make it easy to quickly roll out new applications and monitor connections to the cloud. Organizations use Citrix SD-WAN to ensure bandwidth is fully optimized and to increase cost savings by consolidating routing and security hardware in branch locations. Request a demo to see how to deliver a secure, always-on network with Citrix SD-WAN.

Learn more about the core and recommended SASE components: What Does a SASE Architecture Look Like the page.

SASE Maturity Hygiene

Your SASE journey is an adaptive process, choose vendors that will partner with you along the journey to help plan and achieve a complete SASE architecture. You need to be able to continuously monitor SASE hygiene and quickly adapt your access policies or scale up/down your access based on your business needs.You must continuously evaluate your existing security and networking technologies to identify gaps and the best paths forward based on use case priorities and expected business outcomes so you can plan for a phased and gradual SASE deployment.

Citrix's flexible architecture and comprehensive technology portfolio can help you to build a unified SASE deployment strategy through continuous assessment, planning, and deployment of SASE components in multiple phases so you can move forward with confidence.

The solutions eliminate the need to backhaul all traffic for all users and branches through your datacenter security stack. Citrix SASE solutions provide a robust, flexible, and effective model that enables a phased deployment approach and can be partially or fully deployed in your environment today.

Learn more at citrix.com/solutions/sase

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States