7 must-haves for Secure Access Service Edge (SASE) architectures

Converging networking and security for your digital workspace
Fast, consistent, and secure access to all applications for all employees, anywhere

Many reported data breaches are related to security software updates and patches being received by IT teams, but never installed, or by employees accessing corporate assets using devices that are out of compliance. CIOs and CISOs consistently secure business applications that employees are using but are challenged to secure applications they can’t see.
A hybrid multi-cloud strategy is rapidly becoming the preferred way to deploy applications where on-prem data centers, cloud XaaS and SaaS are combined. But as the number of remote workers continues to grow and a more hybrid workforce emerges, maintaining a secure environment creates new challenges.

Solving these challenges with do-it-yourself, best-of-breed, multi-vendor solutions are enticing in concept, but they are burdensome in practice. Each solution must be independently deployed, patched, and scaled. Organizations must keep IT teams frequently updated on the most current best practices and train them on vendor-specific management systems. With increasing levels of encrypted traffic, each vendor solution adds latency in processing the traffic — with each data packet being decrypted and inspected by multiple security engines. In contrast, comprehensive, cloud-delivered security offerings easily adapt to the fluid app delivery environment that is constantly evolving, without the need for constant software updates, hardware upgrades, or significant reconsideration of the architectural approach.

Offering a unified approach for Secure Access Service Edge (SASE) architectures, Citrix delivers comprehensive network and security capabilities to meet the demands of cloud and SaaS adoption, mobility and an expanding, diverse workforce. Read on to see how.
61% of CISOs and CIOs are seeing an increase in risks from the use of non-enterprise devices and software due to more people working remotely.”

PwC’s Workforce Pulse Survey
Introducing Citrix’s unified approach to Secure Access Service Edge

Citrix uniquely converges comprehensive, cloud-delivered security, SD-WAN, zero trust access, data governance and analytics capabilities, into a truly unified SASE architecture through built-in automations and single-pane-of-glass management.
Each of the services in the diagram can be deployed standalone or as a unified approach, depending on your enterprise requirements.
Citrix’s approach is designed to support employee experience, cybersecurity and operational agility needs of modern, cloud- and mobile-first enterprises. For instance, delivering fast and secure direct access to all apps, protecting remote and home-based workers, preventing loss of sensitive data from enterprise networks and gaining full visibility into all user activity, including for mobile users, are just some of the use-cases that benefit from this approach.

With a fully unified approach to SASE from Citrix, you can easily implement a modern networking and security architecture. By integrating the capabilities of Citrix solutions, this global cloud service helps you meet the full security requirements of a modern enterprise. One that enables fast, consistent, and reliable access to your applications — anywhere, anytime, on any device.
Support your business’s technology goals

- Remain protected from zero-day and recently discovered threats through automated security updates from 10+ threat engines

- Empower all employees, regardless of location, with a fast application experience with secure local Internet breakouts through a high-performance, single-pass security cloud

- Ensure a consistent security posture for all employees, regardless of their physical location

- Enhance the Citrix Workspace and Citrix Virtual Apps and Desktops security posture with Citrix SIA and Citrix SWA

- Simplify management across networking and security with unified management interface
7 must-haves for SASE architectures

1 Comprehensive, cloud-delivered security services

Citrix secures access to all applications - web, SaaS and internally managed applications, for all traffic - encrypted and conventional.

For SaaS and web: Citrix offers comprehensive, cloud-delivered security services by converging Secure Web Gateway, Next Generation Firewall, Cloud Access Security Broker, Data Loss Prevention, Malware Protection that’s powered by 10+ threat engines, Sandboxing, and advanced analytics into a unique security architecture. All traffic, including SSL/TLS traffic, is inspected at scale, without performance limitations.

For internally managed applications: Unlike traditional VPN solutions that require end user devices to be managed, provide access at network level and enforce static access control policies, Citrix provides users with a choice to access internally-managed apps on any device, regardless of it being managed or BYO. It provides access at application layer to prevent network level attacks while enforcing contextual access control policies that are driven by continuous assessment and verification of both identity and device posture of the end user. It also provides protection of user sessions from malicious content like keyloggers and screen capturing malware.

For SaaS and web: Citrix offers comprehensive, cloud-delivered security services
76% of enterprises are planning to move security to the cloud.”

PwC’s Global Digital Trust Insights
While much of today’s workforce remains dispersed, mobile and home-based workers expect and require branch-like protection and application performance. Citrix’s approach to SASE delivers consistent security, regardless of user location through globally distributed security points of presence (PoP). High global PoP density ensures PoP availability closer to the user, without the need for backhauled connections, thus reducing application latency. Each PoP offers full security functionality. This ensures consistent protection for all users, regardless of location. Auto-scale and built-in resiliency via the cloud-delivered architecture allows on-demand scale as traffic volume increases.

Security functionality is available as a single-pass architecture — data packets are decrypted and inspected only once, to be used by all policy engines. This minimizes latency in comparison to service chained architectures from a single or multiple vendors wherein each traffic packet may be decrypted and inspected multiple times.
While the benefits of cloud are multifold, the inherent risk of traffic intermixing remains. The Citrix cloud architecture offers private instances and separation of data offering higher levels of privacy and compliance. Dedicated IP addresses ensure that employees appear to be originating from within the company perimeter even when they are mobile. This is critical for upstream integration with cloud services and where IP presence within the country of origin is required by law.

The Citrix cloud architecture offers private instances and separation of data offering higher levels of privacy and compliance.
Even if your employees are doing their best to maintain privacy, high-risk behavior remains a concern. Identifying and remediating security incidents requires deep visibility and forensic capabilities into the behavior of all users and traffic, including mobile and home-based workers.

With Citrix’s approach to SASE, you get full visibility into all traffic and logging for all users, including mobile and identification of usernames associated with activity, full URL and IP information. Intelligent reporting enables you to extract critical information to identify high-risk users and their activities while real-time dashboards and alerts provide information needed for incidence remediation. You can also prevent loss of confidential information with select encryption of logs. With built-in connectors, logs can be exported to SIEM solutions without the need for a separate log streaming service.
As network conditions change and local internet service fluctuates, maintaining a consistent employee experience across your workforce is critical to productivity.

Citrix’s approach to SASE ensures consistent application performance, including application identification, prioritization and optimization, and delivers automated “dual resilient” connectivity between Citrix SD-WAN locations and security points of presence. By peering with thousands of SaaS and UCaaS applications via a dedicated WAN, Citrix SD-WAN improves performance of SaaS, cloud and virtual applications.

Citrix enables enterprises to be agile and efficient in their operations, being able to redirect focus towards delivering new digital services versus having to manage complex architectures. By unifying the management interface across networking and security, Citrix delivers seamless control over cloud-delivered security, SD-WAN, zero trust access and other capabilities. Unique ‘under the hood’ automations and sharing of analytics across networking and security further augment the integrations in the management plane.
Choose the total solution that’s easy to manage

Like for the adoption of any disruptive technology, evaluation of SASE will require an evaluation of your current architecture, strategic priorities and prioritization of more immediate use-cases. Whatever your specific use-case initially, by eventually converging to a unified, single-vendor SASE architecture, you would maximize operational agility, employee experience and cybersecurity.

Citrix unifies all SASE services, across networking and security, with deep integrations, automations and single-pane-of-glass administration. Trusted by 400,000 organizations to create a better way to work, Citrix can help accelerate your networking and security transformation.

Learn more at citrix.com/sase