White Paper

Understanding Secure Access Service Edge (SASE) Architectures

Rethink Network and Security Architectures to Meet Modern Requirements

An Evolution in How People Work

There has been an evolution in how people work. Enterprises must take these evolutions into account to plan future infrastructure investments, architectures, timelines for delivery of new digital services and more. Keeping up with these evolutions is imperative to positively impact tangible indicators of business success, such as operational performance, financial costs, employee engagement and customer satisfaction.

- **Increased usage of cloud applications and services:** Gartner estimates a 34% increase in spending on SaaS applications between 2020 – 2022[1]. These SaaS applications are being adopted for both work and personal use. In either case, people expect consumer-grade experience from these applications – fast access regardless of the application being accessed or the location where the user is situated.
- **Increasing number of remote workers:** COVID-19 forced employers and employees to test out remote work. Based on a survey in June 2020, 72% of employees would like to work remotely at least two days a week even after COVID-19 is no longer a concern[2]. That said, remote workers also mentioned that difficulty collaborating was a key reason for loss of productivity. It's no surprise that 53% employers plan to invest in providing a better mobile experience for work applications and data[3].
- **Increasingly lethal security threats:** USD 3.86 million – that's the average total cost of a data breach[4]. Most data breaches are intentionally orchestrated with malicious intent (versus human error or system glitches). It is imperative for businesses to evolve their security systems and architectures to outrun bad actors. This not only prevents tangible financial loss, but also helps retain customer and employee trust.

IT teams need an underlying networking and security architecture that is capable of supporting fast, consistent and secure access to cloud applications by all, including remote, workers. Unfortunately, hub-and-spoke networking and security architectures in use today were designed for an era of on-premise applications and branch-based workers, connected via private WANs. A change in these underlying architectures is needed to be able to support larger technology trends that can tangibly impact business success.

> **"53% employers plan to invest in delivering a better mobile experience for work apps & data"**

Architectures for a Cloud- and Mobile-first Era

Challenges with traditional architectures

Below are the specific challenges that need to be solved to deliver architectures suitable for the cloud- and mobile-first era.

- **Poor Employee Application Experience:**
  - *Architecture-related challenges:* Hub-and-spoke architectures force backhaul of traffic to the data center for security. This additional traffic hop increases WAN requirements but more importantly, adds avoidable latency and worsens employee experience.
  - *Appliance-related challenges:* As remote workers collaborate and engage through cloud applications, especially encrypted file sharing applications such as Microsoft SharePoint and video conferencing applications such as Microsoft Teams, the load on the underlying infrastructure – data center-based appliances and WAN links, increases considerably. These hardware appliances have compute limitations and the increasing load from encrypted cloud applications worsens performance, affecting employee experience.

- **Inconsistent Security for Remote Workers:** Employees expect branch-like application performance even when working from home. To achieve this, employees often disconnect from VPN clients when accessing web and SaaS applications. This leaves them unprotected and vulnerable to threats. Similarly, workers accessing company data from BYO devices can increase risk for the business. In fact, 61% of CISOs and CIOs say they are seeing an increase in risks from the use of non-enterprise devices and software due to more people working remotely[5]. Hence, enterprises need a way of consistently securing all users, all devices, regardless of location without any impact on employee application experience.

- **Operational Complexity:** Traditional architectures are often made of fragmented, service chained solutions. This makes it difficult to make changes to the architecture without 'breaking' another set of configurations. Also, scaling the architecture with changing traffic patterns often involves an upgrade of the physical appliances to higher capacity limits. This is time consuming and takes away the IT team's focus from being able to deliver new digital services.

Key Functionality for a Modern Enterprise Architecture

- **Direct Internet Access:** Employees need to be able to access all applications via a direct path from the employee to the application. However, this connection must be secured.
- **Security that follows the user:** Data Center-based security does not allow Direct Internet Access. Hence, a security architecture is needed that allows security that is in-path between the employee and the application, regardless of employee location. This can only be delivered via cloud-delivered security services. Expectedly, 76% enterprises are planning to move their security to the cloud[6].
- **WAN services for application performance:** Direct Internet Access shortens the path between the employee and the application. However, it does nothing to mitigate variations in application performance due to unpredictability of commodity or business Internet connections. Hence, enterprises require comprehensive functions such as software-defined WAN (SD-WAN) and WAN optimization to ensure application performance over Direct Internet Access connections.
- **Single-pass architecture:** To eliminate added latency from service chained inspection engines in a typical security stack, enterprises must deploy a single-pass architecture. Single-pass architectures open and inspect the traffic only once for processing by multiple policy engines. For instance, a single-pass architecture would open and inspect an encrypted packet only once for analysis by the malware protection and data loss

prevention engines.

- **Unified management:** Management plane integrations across networking and security must simplify full lifecycle operations – provisioning, policy-based management, visibility and troubleshooting. For instance, IT Administrator teams must have holistic views into the complete enterprise architecture across networking and security, including branch office locations, security points of presence, tunnels and network usage, all on one unified dashboard. This eliminates blind spots and simplifies configurations across the complete architecture, minimizing chances of human error.

“76% enterprises are planning to move security to the cloud”

Secure Access Services Edge

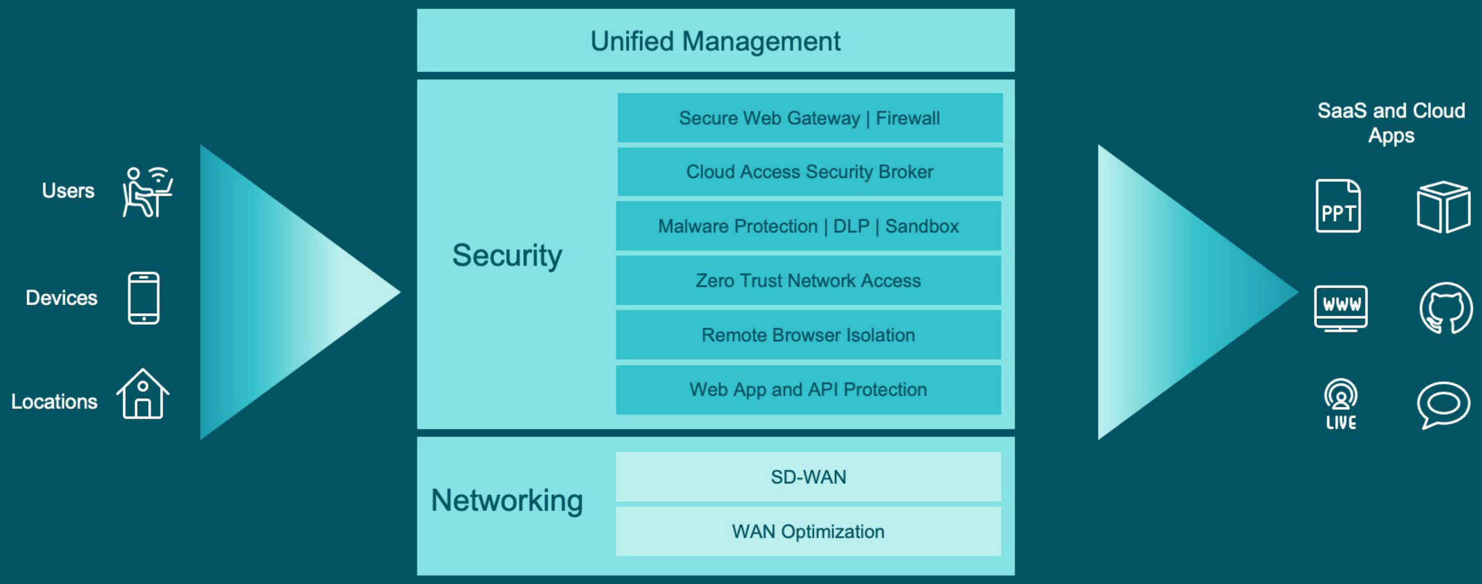
Secure Access Services Edge (SASE) aims to replace traditional, hub-and-spoke architectures with secure Direct Internet Access. Unification of cloud-delivered security, zero-trust access and comprehensive WAN capabilities ensure secure and consistent employee experience, regardless of employee location or where the application is hosted.

SASE services are applied based on the identity of user and real-time context. For instance, an executive in the finance department would receive different access as compared to a 3rd party contractor in marketing. Key services within a SASE architecture include:

- **Secure Web Gateways (SWG)** are enterprise security solutions intended to protect users from web-based cyber threats. They provide the following capabilities:
  - *URL Filtering* – Allows or blocks website access by comparing requested URLs with a filtering database that’s defined per organizational policy.
  - *Anti-malware Protection* – Inspects encrypted and unencrypted web content to identify and block all threats.
  - *Application Control* – Offers visibility into applications being accessed and allows granular control to ensure security and compliance.

SWGs are typically implemented as an inline cloud service, orchestrated as multi-tenant security stacks

SASE converges networking and comprehensive, cloud delivered security with unified management


Users
Devices
Locations
Unified Management
Security
Secure Web Gateway | Firewall
Cloud Access Security Broker
Malware Protection | DLP | Sandbox
Zero Trust Network Access
Remote Browser Isolation
Web App and API Protection
Networking
SD-WAN
WAN Optimization
SaaS and Cloud Apps
PPT
WWW
LIVE

through globally distributed of points of presence (PoPs). Traffic from enterprise users – remote and branch-based – is forwarded to the SWG cloud where it is inspected and secured.

- **Cloud Access Security Brokers (CASB)** help monitor, secure and manage access to sanctioned and unsanctioned SaaS applications. CASB capabilities are built around the following four pillars:
  - *Visibility* – Consolidated view into all applications, including unsanctioned shadow IT applications, being used by enterprise users
  - *Data Security* – Mitigate unauthorized access to and exfiltration of sensitive data
  - *Threat Protection* – Leverage inline proxy architectures, native or integrated threat feeds and behavioral analysis to identify and limit damage from malware and compromised users
  - *Compliance* – Visibility and reporting to show that industry regulations and data residency policies are being met
- **Zero-trust Network Access (ZTNA)** aims to eliminate “excessive trust” by providing “just in time” and “just enough” access between authorized users and sanctioned applications. Unlike traditional VPN solutions which allow a user with a specific IP address to access the entire corporate network, ZTNA allows precise, adaptive, identity- and context-aware access. Here are the primary characteristics of ZTNA solutions:
  - *Identity-aware* - Access is granted based on user identity. ZTNA solutions usually integrate with Identity Providers such as Microsoft Azure Active Directory for Identity information.
  - *Context-aware* - ZTNA solutions take into consideration real-time context parameters such as identity of the user, location and device from which access is being requested, time of day, sensitivity of the specific application being requested, and real-time risk calculation based on inputs from security and monitoring services. Access levels are adaptive - as these parameters change, access can be granted/limited/denied.
  - *Application-level Access* - Authorized users are granted access to the specific application, not to underlying network. This limits possibility of lateral spread of malware within the enterprise network.
  - *Applications Remain Hidden from the Internet* - Data transfer between a user and an application is supported by a ‘broker’ within ZTNA architecture, without the application ever having to expose it’s IP address to the Internet. As a result, the application remains hidden from bad actors that might want to launch DDoS or similar attacks.

ZTNA solutions minimize the enterprise attack surface protecting both users and applications. Since users don’t have to log into a VPN anymore and don’t have to be backhauled via the VPN stack, the user experience improves. Lastly, ZTNA solutions simplify the enterprise security architecture by replacing the VPN stack needed in data centers with a cloud-delivered service, adding to operational agility and efficiency.

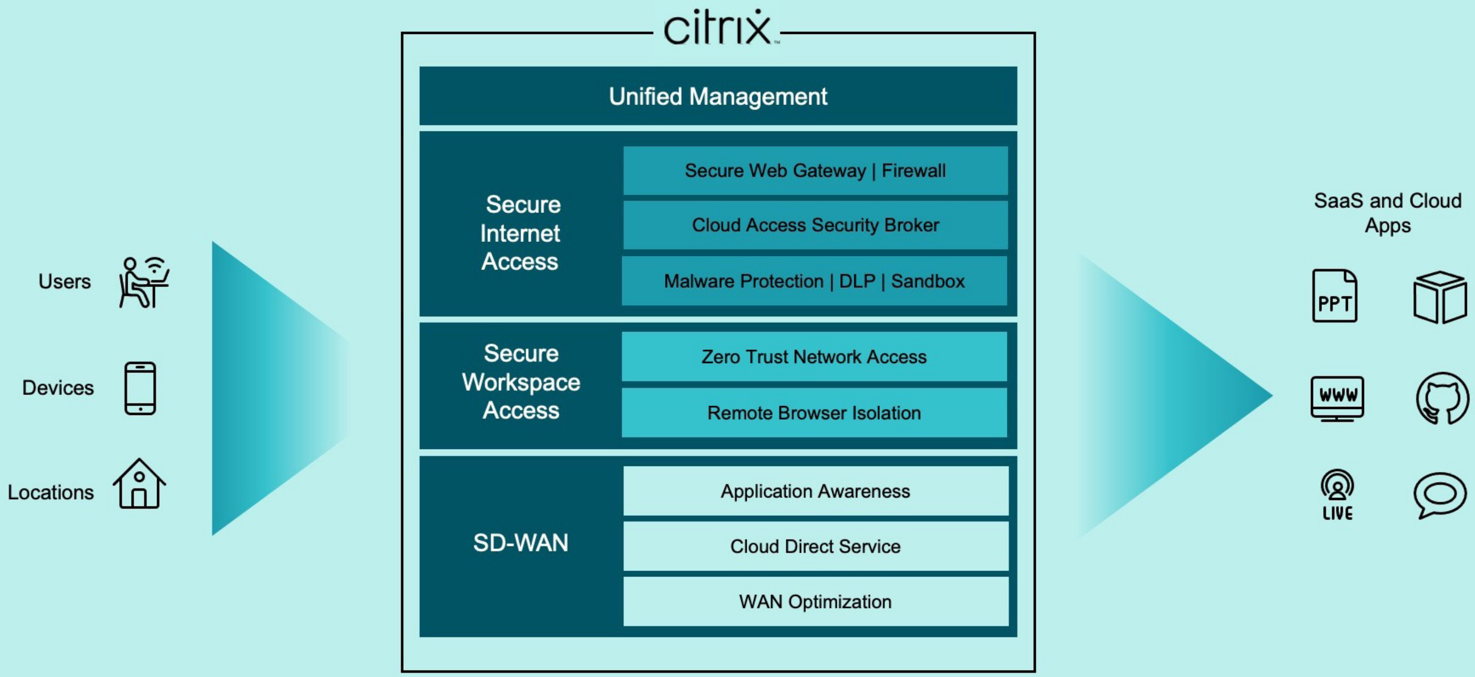
- **Firewall as a Service** – Firewalls act as gatekeepers or filters between the enterprise network and the Internet, by offering bidirectional (ingress and egress) controls to only allow trusted, secure traffic to pass through. Firewalls typically offer capabilities such as Intrusion Detection/Prevention, Anti-malware Protection, Logging and Reporting capabilities. In addition, most modern firewalls also offer Sandboxing, Geolocation and Signatureless (anomaly-based) Threat Detection. A few of these are explained here:
  - *Anti-malware Protection* – Inspects encrypted and unencrypted web content to identify and block all threats.
  - *Intrusion Prevention/Detection System (IPS/IDS)* – IPS/IDS inspects traffic and compares against known threat signatures to identify malicious files. IDS is a monitoring and logging tool that creates an alert when malware is detected. IPS takes this a step further and automatically blocks potentially malicious traffic.
  - *Signatureless/Anomaly-based Threat Detection*

- Anomaly-based detection involves comparing file behavior or potential behavior (by inspecting the code in the file) against typical baselines. For instance, a newly downloaded file trying to disable security controls should likely be quarantined.
- *Network Sandbox* – Suspicious files are sent to the sandbox to run in an isolated environment. If the files are found malicious, information about the files is sent to the firewall to block the files.
- *Geolocation* – Allocation of certain IP address ranges to a specific geography for allowing/limiting/blocking access based on that allocation.

Firewalls are used for protecting enterprise branch locations, data centers and cloud instances from threats. They're often integrated with other security and SecOps (analytics) solutions for creating a more robust, comprehensive threat management 'platform'.

- **SD-WAN:** Software-defined WAN solutions provide low-latency and resilient connectivity from distributed enterprise locations to cloud and on-premise applications, while overcoming the complexity experienced when using traditional router-based networking solutions to manage modern networks. SD-WAN functionality includes more holistic WAN Edge capabilities including:

- *Path Selection* – Identification and dynamic steering of traffic based on administrator-defined policy and real-time WAN health (packet loss, jitter, latency etc.). Path Selection capabilities help ensure that users receive a consistent application experience regardless of changes in network performance.
- *Routing* – Functionality that enables replacement of branch-office routers (BGP, OSPF, multiple topology support).
- *Native Security* – Branch-grade security functionality including IPS/IDS, signature and heuristics-based malware protection, and web filtering. In addition, SD-WAN solutions often simplify the setup of VPN tunnels between branch location and cloud (IaaS/PaaS) instances.
- *Zero-touch Provisioning* – Provisioning and initial configuration of branch SD-WAN appliances can be done remotely by centralized IT team through this capability. It allows SD-WAN appliances to be shipped to a branch location and simply plugged into one or more WAN circuits, without the need for



Citrix SASE unifies functionality for secure and reliable access to applications anywhere, anytime from any device

any complex configurations on site. The SD-WAN appliances download configurations from the SD-WAN control plane and automatically begin tunnel setup with other SD-WAN enabled branch and cloud locations.

The above security capabilities, unified with SD-WAN, enable an enterprise to transform its network and security architectures to meet the demands of cloud, mobility and an expanding, diverse workforce.

Citrix's SASE Solution

Citrix offers a fully unified SASE solution that integrates a comprehensive, cloud-delivered security stack with SD-WAN and zero-trust access to securely empower the workforce with the best experience for any application, anywhere, on any device.

- **Cloud-delivered, Comprehensive Security:**

Citrix Secure Internet Access (SIA) offers comprehensive, cloud-delivered security services. These include Secure Web Gateway, Next Generation Firewall, Cloud Access Security Broker, malware intelligence that's powered by 10+ threat engines, Data Loss Prevention, Sandboxing, AI-powered Analytics and more. Globally distributed across 100+ points of presence (PoP), with each PoP consistently offering all services, SIA protects employees with a full security stack, regardless of their location.

Citrix Secure Internet Access offers comprehensive, cloud-delivered security services

- **Identity-aware, Zero-trust Access:** Citrix Secure Workspace Access provides identity-aware, zero-trust access to all corporate sanctioned applications within a digital workspace designed to streamline employee experience across any device. Built-in Remote Browser Isolation protects endpoints and the corporate network from browser-based attacks. Website data does not directly transfer to the user device, so the experience is secure.
- **Fast Application Experience with SD- WAN:** Citrix SD-WAN is ranked #1 by Gartner for Application Optimization and Deployment Flexibility[7]. Functionality such as packet-level prioritization of traffic with sub-second failovers between WAN links and dual-ended QoS ensures fast ensures consistently fast application performance regardless of network availability.
- **Deep Forensics and Easy Search:** Detailed logging of all users, including mobile users, and their activity, including full URL information (not just domain name) in HTTPS traffic provides unique and deep visibility. AI-powered reporting engines extract critical information for reporting and alerts. In addition to built-in reports, logs can be exported in real-time to SIEM solutions as well.
- **Unified Management:** Citrix offers deep integrations, automations and single-pane-of-glass administration across SD-WAN and SIA for simplified, full lifecycle operations – from initial setup to continual management and troubleshooting.

  - Automated 'dual resilient' connections connectivity between Citrix SD-WAN locations and Citrix SIA
  - Singular view into the full architecture spanning SD-WAN enabled locations, SIA PoPs and connecting tunnels
  - Granular control to on traffic steering and allocation of bandwidth across SIA, cloud providers, and other WAN links, per business needs
  - Eliminate blind spots by integrating reporting across the networking and security architecture

Citrix SD-WAN Ranked #1 by Gartner for Application Optimization & Deployment Flexibility

Benefits of Implementing a SASE Architecture

SASE architectures were designed with the intent of enabling fast, reliable and secure access to cloud applications by mobile and remote workers, while concurrently also improving IT agility. Assuming that enterprises pay attention to the nuances in functionality offered, such as unified management across networking and security, single-pass architectural design and powerful SD-WAN functionality, enterprises can achieve the following benefits from a SASE deployment:

- **Improved User Experience, Collaboration and Engagement** – Direct Internet Access eliminates latency from backhauled connections. However, SD-WAN and WAN optimization functionality within SASE solutions is required to ensure consistent performance even as Internet performance fluctuates. Single-pass architectures ensure that the inspection and policy engines themselves do not added unnecessary latency.
- **Improved Security Regardless of Employee Location** – Identity-aware, zero-trust access is enabled for sanctioned applications. This reduces the attack surface and impedes lateral movement of malware within the enterprise network. For web and unsanctioned applications, comprehensive, cloud delivered security ensures a consistent security posture, regardless of employee location.
- **Simplified Operations with Better IT Agility** – SASE architectures can help consolidate vendors across networking and security. Single-vendor solutions offer deeper integrations and unified management which simplifies deployment, configuration, reporting and support services. Since SASE architectures require moving security to the cloud, overall hardware footprint is reduced which in turn improves architectural elasticity and scale.

Getting Started

Like any disruptive technology, certain enterprises will adopt SASE architectures earlier than others. Replacement of traditional hub-and-spoke architectures, replacement of legacy VPN technologies, migration of applications to the cloud, consistent security for remote workers and the need to improve employee engagement are just some of the likely conversation starters.

The ability to rethink and redesign networking and security architectures will give significant advantages to early adopters, creating a positive impact on indicators of business success, such as operational performance, financial costs, employee engagement and customer satisfaction. To enable this transformation, enterprises must choose their technology partner wisely.

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.

Visit *www.citrix.com/secure-internet* for more information.

Endnotes

[1] https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

[2] PwC’s US Remote Work Survey, June 2020, https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

[3] PwC’s US Remote Work Survey, June 2020, https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

[4] Cost of a Data Breach Report 2020, IBM, https://www.ibm.com/security/data-breach

[5] PwC’s Workforce Pulse Survey, https://www.pwc.com/us/en/library/covid-19/workforce-pulse-survey.html

[6] PwC’s Global Digital Trust Insights 2021, https://www.pwc.com/us/en/services/consulting/cybersecurity/library/global-digital-trust-insights/cyber-defense-technology.html

[7] Gartner, Critical Capabilities for WAN Edge Infrastructure, Gartner, Sept 2020

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