Solution Brief

Cloud-delivered security for the digital workspace

Get Comprehensive Security and Reliable Access to Apps, Anywhere from Any Device with Citrix Secure Access Service Edge

With the adoption of hybrid cloud and the rise in remote work, traditional connectivity models like VPN and MPLS are no longer meeting performance and security requirements. Distributed employees need reliable access to their apps, yet disparate networking and security infrastructure makes it hard for IT to meet expectations.

Traditionally MPLS has been the primary mode of connectivity for the data-centric model because it provides predictable performance. However, MPLS can be expensive especially if you have idle backup links. Adopting direct internet access (DIA) allows users to connect faster to cloud applications, but also requires edge computing services, local access points, and centralized policy management for this new access paradigm. To become more agile, businesses need a new, more modern architecture that simplifies complexity, mitigates security threats, and delivers a better user experience.

Overview of Citrix Secure Internet Access

Citrix Secure Internet Access (SIA) offers comprehensive, cloud-delivered security services for direct internet access. It includes Secure Web Gateway, Firewall-as-a-Service, and Cloud Access Security Brokers, Data Loss Prevention, and Sandboxing functionality. 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. The service includes:

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.

Firewall- as-a-Service 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.

Cloud Access Security Brokers (CASB) help monitor, secure and manage access to sanctioned and unsanctioned SaaS applications.

Data Loss Prevention ensures sensitive data is not lost, exfiltrated or accessed by unauthorized users, e.g., safeguard customer credit card numbers, social security numbers.

Sandboxing safely executes suspicious code in an isolated environment, e.g., run a suspected zero-day threat code in a sandbox.

Converging Network and Security for a Consistent Workspace Experience: Bringing networking and security together at the edge gives businesses the opportunity to simplify their workspace delivery. As a result, a new trend has emerged that brings SD-WAN and security together as a unified cloud-delivered solution. The secure access service edge (SASE) architecture converges comprehensive networking and cloud-delivered security capabilities, in a single-pass architecture with unified management, to:

- Make IT operations more agile through consolidation of fragmented solutions that are complex to manage, limit elasticity and scale, and impede IT agility. In fact, McKinsey states Agility has the potential to improve the customer experience by up to 30 percent and can lead to a potential 20 to 30 percent improvement in employee engagement.[1]
- Empower remote workers by reducing latency due to inefficiencies in inspection and processing of traffic.
- Ensure network reliability by intelligently steering traffic with network outage protection for a consistent experience.
- Employ policy definition and enforcement consistency for all employees, regardless of location or device to ensure security and preserve the employee experience.

McKinsey states, "Agility has the potential to improve the customer experience by up to 30 percent and can lead to a potential 20 to 30 percent improvement in employee engagement.[1]"

Introducing the Citrix Secure Access Service Edge

Citrix Secure Access combines Citrix SD-WAN with Citrix Secure Internet Access (SIA), Citrix Secure Workspace Access (SWA), and Citrix SD-WAN for a fully integrated secure access service edge (SASE) solution. It allows users anywhere to securely access

any virtual, web, or SaaS app, from any personal or corporate device. All users can securely access applications sanctioned within the Citrix Workspace and unsanctioned SaaS and web applications to ensure a secure and consistent experience, regardless of employee location.

- **Citrix Secure Internet Access (SIA)** offers comprehensive, cloud-delivered security services. This includes Secure Web Gateway, Next-Generation Firewall and Cloud Access Security functionality.
- **Secure Workspace Access (SWA)** provides identity-aware, zero trust access for all corporate-sanctioned applications within Citrix Workspace.
- **Citrix SD-WAN** is a next-generation WAN edge solution delivering secure, automated, reliable connectivity to improve performance of SaaS, cloud, and virtual applications and desktops. It reduces network complexity, centralizes orchestration and monitoring, and speeds cloud and on-premises connectivity to applications for users in branches or working from home.

Use Cases:

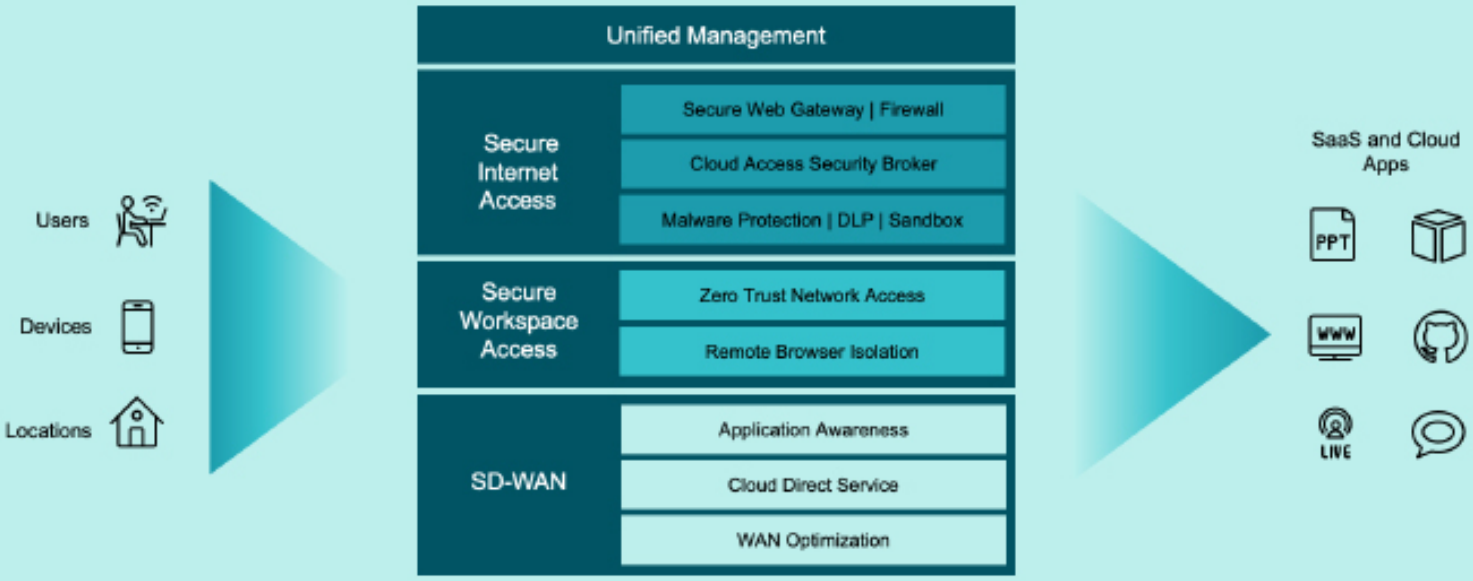
- Users clicking on links
- Users accessing personal applications from a BYO device

Citrix Secure Internet Access Features

The cloud-delivered service offers:

- A comprehensive security service consisting of 100+ PoPs each offering SIA services giving consistent protection for all users, regardless of location.
- Lower latency and improved employee experience with availability close to users with no need to backhaul traffic to centralized hubs/data centers.
- Auto-scale and built-in resiliency via a cloud-delivered architecture that allows on-demand scale as traffic volume increases.
- Inspection and protection for all encrypted and compressed traffic for compliance, malware and data loss prevention without performance limitations typically associated with appliance-based approaches.

Figure 1: Citrix Secure Access Service Edge



- Intelligence from 10+ Threat Engines with highly effective malware, ransomware and signature-less threat protection.
- Privacy and compliance through data segregation based on enterprise and location.
- Increased performance and lower latency with a single-pass architecture, unlike service-chained architectures.

Citrix Secure Internet Access Benefits

Deep Forensics and Easy Search

Citrix SIA provides deep visibility into all traffic and user behavior, including for mobile users, to locate specific security incidents, atypical activity and policy violations.

Full Visibility into All Traffic Logging

for all users, including mobile and identification of usernames associated with activity, full URL and IP information.

AI Powered Reporting

Extract critical information to identify high risk users and their activities while real-time dashboards and alerts provide incidence remediation.

Selectively Encrypt Logs

Encrypt fields such as username, source IP and group prevents loss of confidential information.

Export to Templates, SIEMs

Built-in, schedulable executive reporting templates or real-time export to SIEMs via built-in connectors.

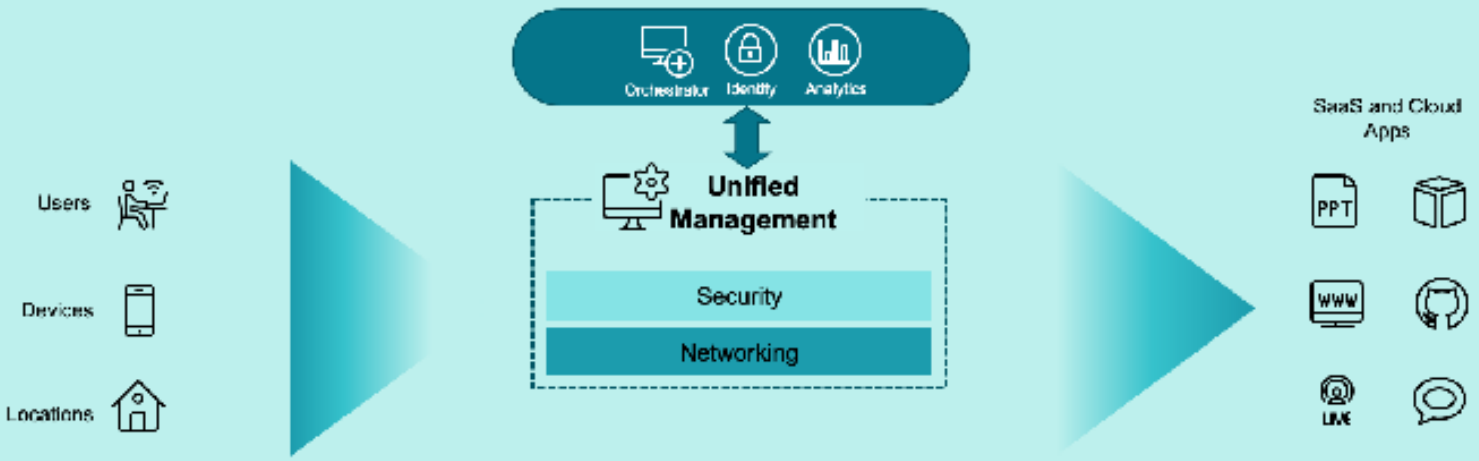
Automated, Resilient Connectivity

Leverage single-click automated tunnel setup between branch locations and Citrix SIA. Dual tunnels to primary and backup PoPs provide continuous monitoring and failover for consistent performance.

Unified Management

Simplifying operations enables businesses to be more agile and efficient so they can redirect focus on delivering new digital services. Ease troubleshooting, deliver consistent security policies, and consolidate infrastructure all through centralized cloud-managed console from a single vendor. Leverage single-click automated tunnel setup between branch locations and Citrix SIA. Dual tunnels to primary and backup PoPs provide continuous monitoring and failover for consistent performance. Gain intelligent bandwidth

Figure 2: Unified Management for Networking and Security



control and leverage real-time reporting with a single cloud-managed interface

Establish one trusted vendor for networking, security and a digital workspace

Re-evaluate your current systems and tools to find new, more cost-effective and consolidated IT models that meet performance expectations. To deliver an exceptional employee experience and security without compromise, look for a single vendor with the most comprehensive SASE framework that allows you to:

- Remain protected from zero-day and recently discovered threats through automated security updates
- Empower remote workers with an architecture that offers the fastest, most reliable experience with comprehensive security
- Enhance the Citrix Workspace and Citrix Virtual Apps and Desktops security posture with Citrix SIA and Citrix SWA
- Ensure consistent policy definitions and enforcement for governance and compliance assurance
- Eliminate IT silos with by creating policies for both SD-WAN and security with a unified interface

Learn more at www.Citrix.com/secure-access

Endnotes

1 Enterprise agility: Buzz or business impact?

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