EDGE7 Networks

Secure access:
A unified and cloud-delivered zero-trust security solution

Contents

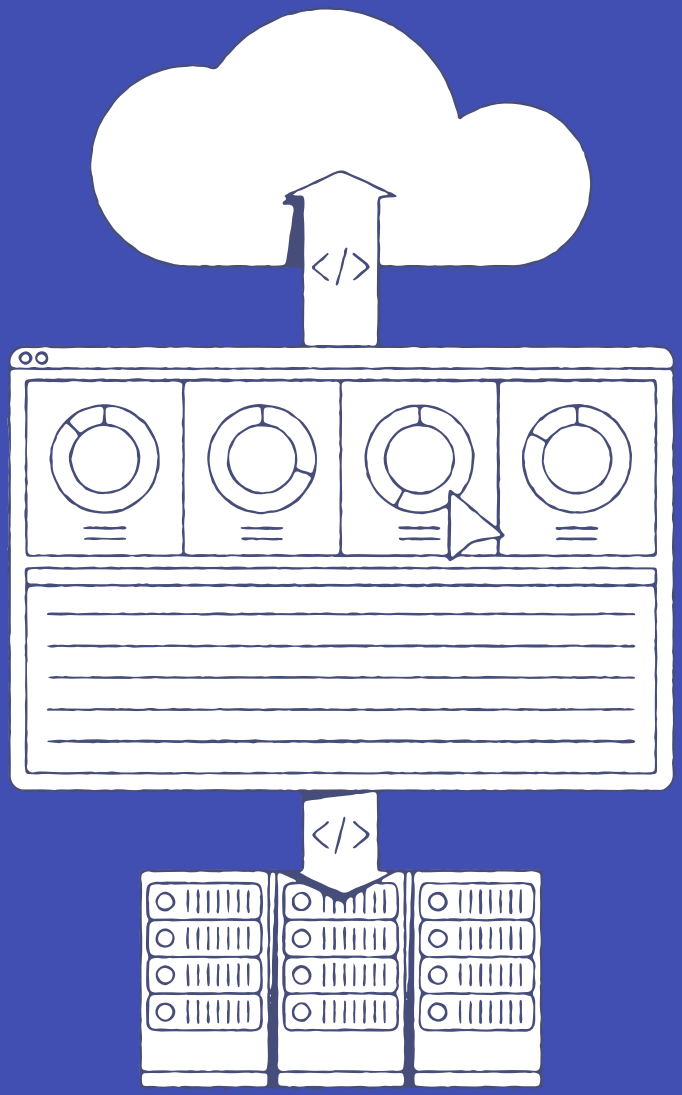
Introduction	3
The pitfalls of appliance-based IT security systems	5
What is a unified secure access solution?	9
Three benefits of a unified secure access solution	10
What characterizes a unified secure access solution?	13
Secure your users, apps, and devices with Citrix	16
FAQs	16

Introduction

As businesses move to hybrid working models where end users—including employees, contractors, and partners—can work from anywhere, IT teams must properly adapt to provide a simple, secure, and productive work experience for their end users.

To do this, businesses are increasingly migrating data and legacy applications to the cloud and developing new applications for the cloud—including software-as-a-service (SaaS) apps. Many IT teams are also allowing employees to access these corporate resources using their own devices and remote networks, as we see IT looking to provide flexibility for employees to keep them productive.

But as businesses transition to the cloud and adopt bring your own device (BYOD) policies to help streamline remote workflows, appliance-based security solutions—such as secure web gateways (SWGs), web app firewalls (WAFs) and virtual private networks (VPNs)—are becoming obsolete. Featuring a rigid infrastructure, these solutions lead to a less than satisfactory end-user experience, a vulnerable security posture, and a lack of scalability.



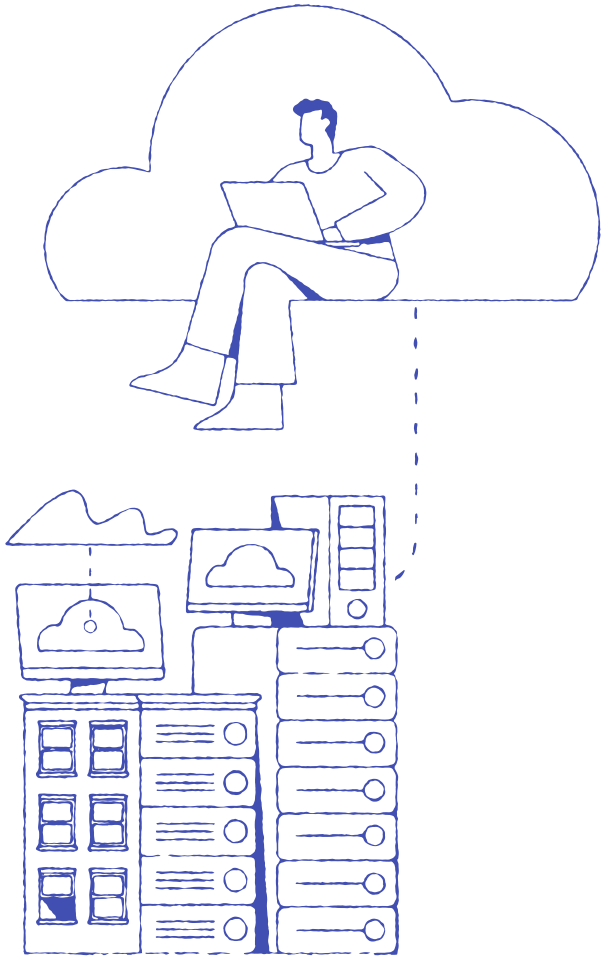
With more employees working remotely and apps continuing to shift to the cloud, IT teams must look beyond appliance-based security solutions to ensure their assets and end users stay productive and protected. Fortunately, a unified secure access solution from Citrix provides cloud-delivered security based on principles of zero trust. Following SASE architecture, this solution allows businesses to rapidly modernize IT while providing a more agile, effective way to reduce security vulnerabilities and deliver the best end user experience.

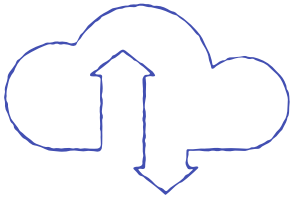
Before we break down just what a unified secure access solution entails, let's take a closer look at the pitfalls of appliance-based IT security systems.

The pitfalls of appliance-based IT security systems

Existing appliance-based, on-premises security solutions like SWGs, WAFs, and VPNs simply cannot protect data or applications in the cloud effectively, as they are constrained with their physical deployments and rigid security policies. Additionally, they enforce backhauling of user and application traffic through already congested datacenter networks and are difficult to scale. This introduces latency that results in poor end user experience, as well as an incomplete security posture that exposes apps to modern-day attacks.

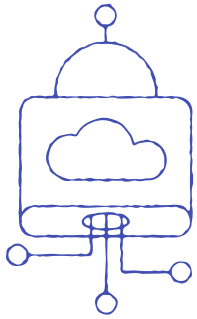
As we move to cloud, having a mix of When it comes to employees using zero trust as well as cloud-delivered BYO and personal devices and public access solutions also result in a networks to access corporate apps poor user experience. For example, in the cloud, many IT teams struggle accessing applications across hybrid to provide the right security posture or multi-cloud environments today against application-level attacks requires end users to use multiple with appliance-based solutions. access mechanisms. Not only does Unfortunately, solutions such as this provide a poor user experience, VPNs have a difficult time detecting if but it means IT teams are forced to malicious content is being transferred to define separate security policies the corporate application infrastructure. and monitoring tools. As this siloed structure presents gaps in the security environment, this could leave their downfalls as workloads move to businesses exposed to modern-the cloud. These devices are often used day attack vectors that lead to to access internet URLs for personal unauthorized access, as well as various use, as well as official work. Because malware and zero-day threats that can IT does not have visibility of all apps go undetected for months.and content end users are accessing, personally identifiable information (PII) can be easily compromised.





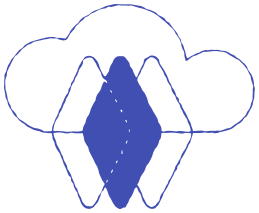
Traditional “castle-and-moat” approach

Traditional appliance-based security solutions like VPNs and SWGs were designed to protect data stored on-premises and protect users on the corporate network. These solutions were based on the principle of a moat surrounding a castle to protect everything in it. But since the valuable assets (i.e., the user, data, and the apps) from the castle have moved out, the moat is an ineffective way to provide security. As applications and data are moving to cloud and more users are remote, this approach enforces the backhauling of all user traffic to the datacenter to enforce security controls. For a user who is working from a remote location and accessing applications in the cloud, this introduces latency and provides a poor end user experience.



Traditional security

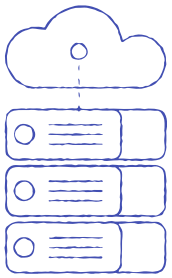
A traditional way of delivering app security relied on the principle of implicitly trusting something that is known, such as a company employee or a whitelist URL. This means that once an employee connects to a corporate network, they can access all the applications and data within that network. Be it an end user, a whitelist URL, or a managed device, this notion of “implicit trust” is exploited by several modern-day cyber-attacks that can take advantage of compromised credentials to gain unauthorized access, infect whitelist URLs with malicious content to further infect IT infrastructure, or use a stolen or compromised device to access information and steal intellectual property.



Complexity of existing infrastructures

Most modern organizations have highly complex infrastructures that are made up of apps, systems, and networks deployed across several IT environments—including on-premises datacenters, public clouds, and private clouds. This has led to organizations maintaining a complicated cybersecurity stack of up to 75 threat detection tools.

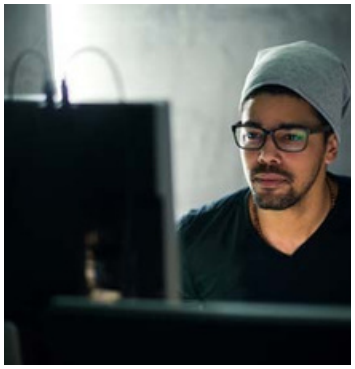
Managing each of these threat detection tools can be challenging, labor intensive, and expensive, especially as an organization grows. It can take days (or even weeks and months) for IT to properly configure and monitor these tools. Even worse, taking such a siloed approach to security can lead to inconsistent configuration and information, as well as general confusion for IT team members. This can be hugely problematic for an organization, as modern-day threats are becoming more sophisticated and take longer to recognize and mitigate in a siloed architecture.



Insufficient protection against modern-day attacks

As applications move to cloud-hosted platforms and are deployed in multiple locations, it is increasingly important to protect them from modern-day application and API-level threats like distributed denial of service (DDoS) and bot attacks, cross site scripting (XSS), SQL injection attacks, and application abuse. Many modern and consumer-facing applications store plenty of consumer data and PII, which means it's more important than ever to protect them.

Existing on-premises solutions cannot always mitigate DDoS attacks completely, especially if the attack is coming at a large scale—such as a volumetric DDoS attack. As on-premises appliances are limited in scalability, these attacks can easily overwhelm an appliance-based solution. These types of attacks must be stopped at the edge before they enter the network—especially as more applications are deployed in the cloud.



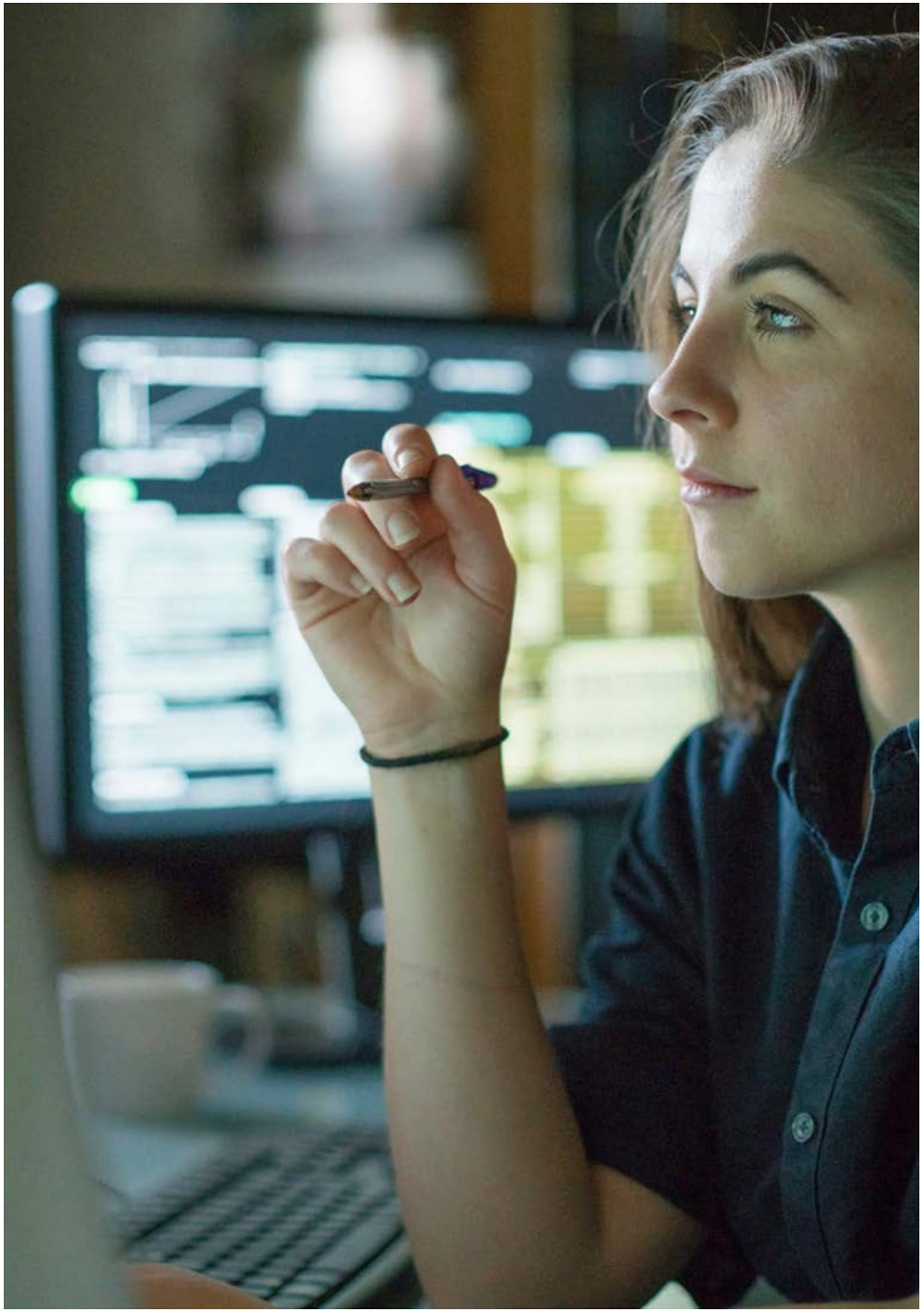
It can take days (or even weeks and months) for IT to properly configure and monitor threat detection tools.

Lack of security breach visibility

Security solutions like on-premises SWGs backhaul all internet-bound traffic through the datacenter, meaning the security controls on traffic going out or coming from the internet are not enforced in real time. This is because it needs to be brought into the datacenter for further inspection by on-premises data loss prevention (DLP) engines. Should a breach occur, the threat cannot be detected at the edge. And, because DLP controls are not closer to the organization's cloud applications, threats or security breaches are not detected in real time.

Shortage of IT skill sets

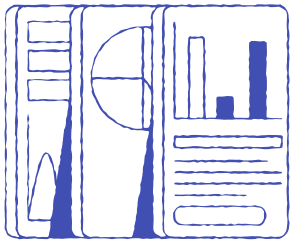
A shortage of IT skill sets is challenging many organizations to continue using and managing older and siloed appliance-based security technologies. There is also a lot of attrition in IT— especially when it comes to cybersecurity. This is primarily due to IT teams looking to diversify their learnings, but not having enough educational opportunities in their existing organizations.



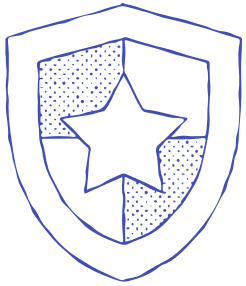
What is a unified secure access solution?

Unlike appliance-based or multi-vendor security strategies that are distributed across several IT environments, a unified secure access solution provides cloud-delivered security based on zero trust via a single, fully managed security stack. Not only does this help to protect end users, apps, devices, and an organization's underlying infrastructure, but it allows IT administrators to manage security for all enterprise-level applications, desktops, and data from a single and a unified management plane.

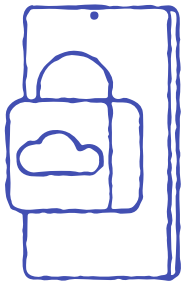
A unified secure access solution from Citrix provides holistic visibility and monitoring controls across all apps, all clouds, and all devices from a unified monitoring dashboard. This allows IT to provide real time and transparent security, as well as the best end user experience for a secure and a hybrid work environment.



Unified monitoring dashboard



Real-time transparent security



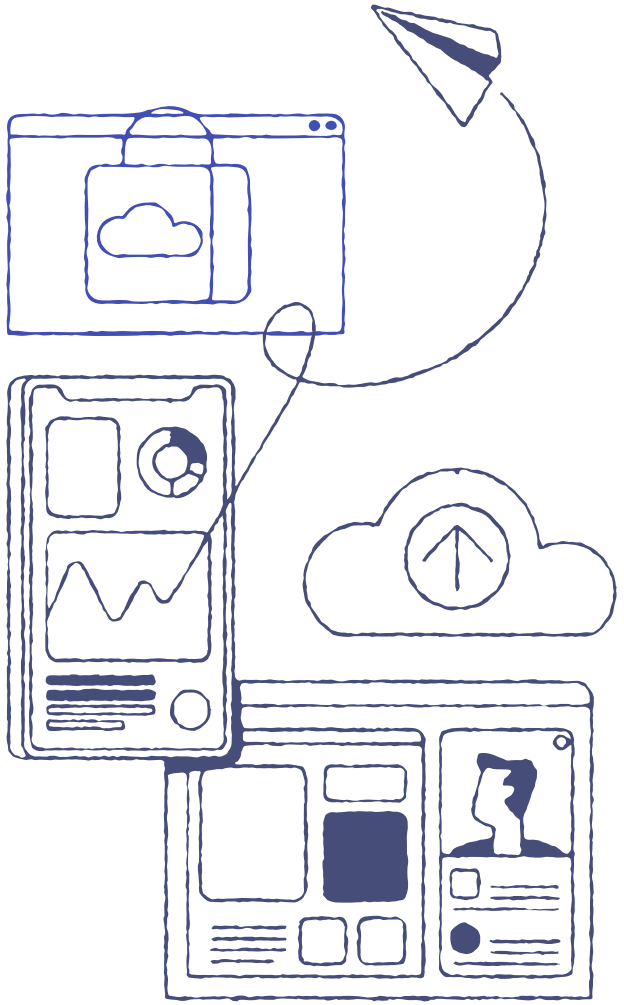
Controls for all apps, clouds, and devices

Three benefits of a unified secure access solution

1

Provides a secure and productive hybrid work environment

With a unified secure access solution, IT teams can easily protect end user access in a hybrid workforce. Featuring unified security and adaptive access for all web, virtual, and SaaS apps and desktops, this solution provides a secure, simple, and productive work environment for remote employees with the flexibility to use any device and work from any location. Not only does this provide continuous monitoring and assessments of user activity and automatic enforcement of security policies, but it also helps protect data stored in both sanctioned and unsanctioned apps from being stolen because of misuse or user error.



Three benefits of a unified secure access solution

2

Modernizes IT and promotes digital transformation

A unified secure access solution ensures IT teams can modernize their infrastructure and promote digital transformation of their organization through a cloud-delivered, zero trust platform. A unified secure access solution provides adaptive and intelligent security policies to help IT simplify security policies, create a consistent end user experience, as well as monitor and track user activities across all apps, devices, and locations from a centralized dashboard.

Additionally, a robust unified secure access solution also provides a rich ecosystem of technology integrations that protects current security infrastructure investments—allowing organizations to define their own journey to implementing a cloud-delivered secure access service edge (SASE) architecture. It also eliminates the operational overhead required to install and manage physical, appliance-based solutions.

Three benefits of a unified secure access solution

3

Prevents cybersecurity threats and mitigates risk

A unified secure access solution not only reduces risk for remote workers, but it also minimizes threats against devices, corporate data, and applications and APIs.

Replacing traditional VPN and SWG security solutions with a cloud-delivered solution built on zero trust allows organizations to provide conditional application access. It also safeguards user credentials and sensitive data from being stolen by keylogger and screen capturing malware.

This protection extends beyond end users. Devices and corporate data are protected via consistent and always-on threat prevention using artificial intelligence (AI) and machine learning (ML) detection methods. This prevents both internal and external threats across all apps, APIs, data, and devices while reducing the overall risk of malware, bots, DDoS, and zero-day attacks.

Furthermore, a unified secure access solution protects applications and APIs by working to block both DDoS attacks on-premises and volumetric attacks and app-layer DDoS attacks in the cloud.

What characterizes a unified secure access solution?

Consolidated access

Access all internal/ external apps, (un)sanctioned by IT.

High performance

Ensures secure and high-performing work environment for the hybrid workforce.

Risk management

Reduces risk across all apps, application APIs, devices, and data from external and internal attacks.

Unified digital architecture

Allows organizations to capitalize on a consolidated networking and security stack to provide a Zero Trust/ SASE security framework.

Minimize training

Minimizes the need for training IT on multiple security strategies/platforms or hiring additional cybersecurity experts, which increases ROI.

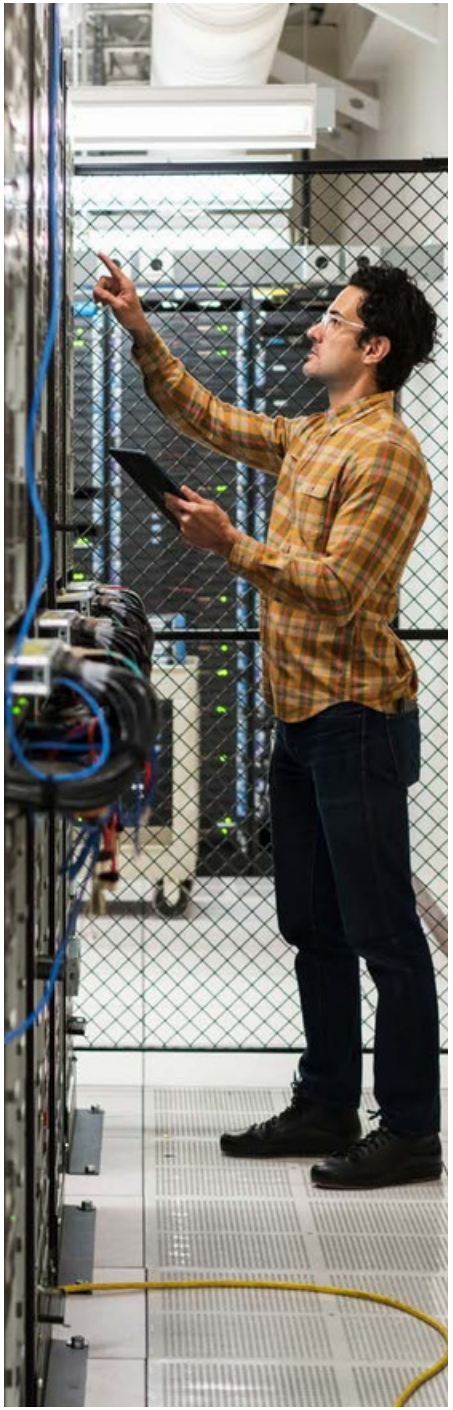
To provide these characteristics, a unified secure access solution should be composed of:

Zero trust network access (ZTNA)

A ZTNA solution expands the traditional security perimeter from the datacenter to be closer to the users and the apps. This allows for continuous verification and adaptive access in real time, including analyzing user, device, and location credentials. A ZTNA architecture uses a reverse proxy connection to establish a secure connection between the user and the app. This ensures end users only have access to the corporate or network resources they need to do their jobs by constantly evaluating contextual, real-time activity and never assuming an identity is trustworthy.

Cloud-delivered security

With a consolidated cloud-delivered security solution, management is centralised while enforcement points are decentralised and distributed. This is an effective way to provide security closer to the user and the apps. IT teams also gain efficiencies in vendor management by focusing on just one vendor to deploy multiple security policies across an entire network. In addition, it allows in-house IT teams to focus on value-driven work, rather than reigning in security solutions from different vendors at multiple sites.



SASE

A SASE architecture makes it easier for organizations to configure, manage, and scale networking and security policies across their entire workforce with better visibility and a consistent user experience. Combining solutions like cloud-delivered security, software-defined wide-area networks (SD-WAN), cloud-access security brokers (CASBs), firewall-as- a-service, SWGs, ZTNA, and more into one unified solution, SASE ensures organizations can provide secure remote access to applications and the internet from a single pane of glass. At their core, they're built to meet the complex needs of today's distributed workforces.

Secure your users, apps, and devices with Citrix

As workloads shift to the cloud and remote workforces grow, IT teams must deploy the proper security solutions to safeguard their corporate infrastructure and employees while promoting a productive work environment. With a unified secure access solution from Citrix, organizations can accelerate digital transformation and modernize IT with a cloud-delivered security stack based on zero trust. Not only does this provide an always-on security posture for all end users, apps, devices, and an organization's underlying infrastructure, but it offers an enhanced user experience that boosts productivity and collaboration.

FAQs

What is a unified secure access solution?

Unlike appliance-based or multi-vendor security strategies that are distributed across several IT environments, a unified secure access solution provides cloud-delivered security based on zero trust via a single, fully managed security stack. Not only does this help to protect end users, apps, devices, and an organization's underlying infrastructure, but it allows IT administrators to manage all enterprise-level applications, desktops, and data from a single pane of glass.

What is adaptive access?

Adaptive access grants or denies app or resource access based on more factors than the user's assigned role, including location, device, type of request, and timing of the request. With adaptive access, IT teams can factor in the 5 Ws of Access—which includes the who, what, when, where, and why into every access and transactional event.

How to secure remote worker access?

Properly securing remote worker access starts with deploying a cloud-delivered unified secure access solution. This type of solution provides a complete security stack for a secure access service edge (SASE) and zero trust network access (ZTNA) architecture. At its core, a unified secure access solution provides true vendor consolidation for all security and networking use cases, including ZTNA, cloud access security broker (CASB), secure web gateway (SWG), data loss prevention (DLP), sandbox, malware protection, firewall, app and API protection, and software-defined wide-area network (SD-WAN).