Provide simpler, more secure access to any app, from any device

Learn how Citrix Workspace goes beyond traditional single sign-on and VPN

With more people working remotely, traditional perimeter security is no longer enough to protect your apps, data, and users. Citrix Secure Workspace Access provides zero trust–based access management capabilities to provide contextual and secure access to on-prem web, virtual, and SaaS applications. Using Citrix Secure Workspace Access, you can consolidate your traditional VPN and single sign-on (SSO) solutions, providing a holistic secure access strategy to all applications. Citrix Secure Workspace Access can help you with the following three use cases.

1. Traditional VPN solution replacement

Unlike a traditional VPN, Citrix Secure Workspace Access is a cloud-based offering that provides secure and contextual VPN-less access with SSO to on-premises web and virtual applications. In addition to SSO, it also provides controls for protecting information shared in web applications. Additionally, it provides security controls like web filtering and an isolated browser environment to protect users accessing malicious links embedded or shared in web apps—adding security as they access web apps from their personal or bring-your-own (BYO) devices. This enables organizations to deliver zero trust outcomes by reducing the attack surface, securing the log-in process, enabling continuous authentication and authorization, providing data and device protection, protecting users from web-based threats, and automating risk prevention.

Why Citrix Secure Workspace Access is a better choice than a VPN

VPNs have a high risk of security breaches

VPNs expose entire networks to threats like DDoS, sniffing, and spoofing attacks. Once an attacker or malware has breached a network through a compromised user device connected to it, the entire network can be brought down. With VPN-less access, users will get single sign-on to both internal apps and SaaS apps. Access is provided at the application layer, thereby removing the risk of any network-level attacks.

VPNs are hard to scale and offer a poor user experience

Most VPNs were deployed to serve a small percentage of a remote workforce. When most of workforce is remote, VPNs become bottlenecks, especially when
delivering traditional client-server applications that consume lot of bandwidth. Citrix Workspace not only helps optimize delivery of these apps, but can auto-scale to serve the entire workforce without configuring and deploying additional appliances.

VPNs are accessed through unmanaged devices
Unmanaged devices introduce risk, as your IT team has no insight into the health of the devices. These devices may be infected with keylogging or screenshot malware, which attackers can use to exfiltrate sensitive data. Citrix Workspace features anti-keylogging capabilities, scrambling keystrokes that are captured by attackers looking to exfiltrate credentials. Attackers will receive only undecipherable text, keeping usernames and passwords safe.

VPNs are not designed to detect breaches
When VPN credentials are compromised, an attacker can enter the network and move freely to exfiltrate sensitive data. VPNS aren’t designed to detect or correct an attacker’s suspicious action. Given the limited resources of most IT departments and the limited insights VPNS provide, monitoring that activity can be overwhelming.

Citrix Analytics for Security will leverage machine learning to understand and monitor end-user behavior across devices, data, networks, apps, and virtual desktops. When it detects risky behavior, it can take proactive, automated action like session recording, logging the user out of their account, or expiring links to shared documents.

VPNs can compromise employee privacy
Connecting to a VPN means all the traffic is backhauled to a datacenter. This includes personal traffic as well business traffic. With Citrix Workspace, employee data stays private because only corporate data is sent through the datacenter.

2. Single-sign on and data governance for SaaS applications
The increase in use of SaaS apps creates security risk as users have to juggle multiple sign-ins for their different services, leading to poor password practices like reusing passwords or creating passwords that are easily hacked.

How Citrix Secure Workspace Access does more than identify and authenticate users

SSO and multifactor authentication (MFA)
Citrix Secure Workspace Access offers SSO to access all of your SaaS and web apps, virtual apps and desktops, and document repositories. MFA can block 99.9% of account compromise attacks. Organizations can implement MFA for users through native, time-based, one-time passwords or through their identity provider.

Security monitoring powered by machine learning
Get a holistic view of how users interact with apps, files, devices, and networks to create a baseline of normal individual behavior. Automated tools can detect when users exhibit anomalous behavior, like excessive file downloads, requesting access from unknown devices, or attempting to sign in from unfamiliar locations.

Cloud App Control
Unlike many other SSO solutions, Citrix provides Cloud App Control, a set of security policies to control user actions within SaaS applications after they successfully sign on. These added security controls pick up where traditional SSO solutions fall short, allowing you to control user behavior, protect company confidential information, and adopt SaaS applications widely by addressing the underlying risks.

3. Secure corporate data accessed through unmanaged devices
Access to applications through an unmanaged device introduces risk, which is why many organizations require device enrollment to deploy a traditional VPN or SSO solution. IT departments have no oversight into the health of a personal or BYO device, which may
be infected with keylogger or screenshot malware. Keylogger malware can harvest critical corporate data like sign-in credentials, allowing attackers to freely access your network. Screenshot malware can be equally dangerous, as any important information that is presented on the screen—such as patient health records or credit card information—can be exfiltrated. Employees can infect their personal devices by browsing to risky websites that unknowingly deliver malware, which puts corporate data at risk later.

How Citrix Secure Workspace Access enables a secure BYO program

Anti-keylogging and screenshot malware protection

Citrix Secure Workspace Access protects against keylogging malware by scrambling the data sent from the keystrokes, turning the sensitive information into undecipherable text. It also defends against screenshot malware, capturing a picture of a blank screen instead of your company’s private corporate data.

Dynamically initiated browser isolation

With Citrix, you can be confident that end users can securely navigate the web with a cloud-based browser that won’t introduce risk to the corporate environment. Threats that may introduced by visiting malicious websites are isolated off the corporate network and device. The browser is discarded at the end of the session, ensuring that any malicious software encountered while browsing the web never reaches your infrastructure.

Web filtering

Web filtering allows you to block users from accessing restricted websites that are known for introducing risk. You can choose to block specific URLs and categories of sites like gambling, social media, torrent, video streaming, and many more.
Summary

Citrix Secure Workspace Access follows the zero trust framework to help consolidate point products that offer VPN, SSO, web filtering, and browser isolation as separate offerings. This not only helps simplify IT’s task and make your environment more secure, but provides for a better end-user experience. For many companies, Citrix Secure Workspace Access serves as a replacement to a legacy VPN or traditional SSO solution, and as a means to provide secure, remote access to corporate resources.

For customers looking to implement just SSO, Citrix Secure Workspace Access is the only service that offers SSO to virtual, web, and SaaS apps.

To learn more about Citrix Secure Workspace Access, visit citrix.com/workspace.