Securing access to internal apps with a zero trust approach

Implement zero trust security with one solution

99% of threats to data security will spring from underlying vulnerabilities already known to the enterprise and its workforce[1]. IT is now responsible for managing a larger attack footprint than ever, thanks to end-users relying on personal devices for work and accessing cloud apps and corporate resources from remote locations. How can you deliver the access your employees need to do their best work while protecting your organization from internal attacks?

Today's security approach must shift from unconditional confidence in users to zero trust fundamentals. A zero trust model relies on contextual awareness to adaptively grant access to authorized users using patterns based on identity, time, and device posture. This tightens the reins on access security while giving your users their choice of devices and apps.

Citrix Secure Workspace Access provides a zero trust approach for accessing corporate, private web, SaaS, and virtual apps securely. With advanced security controls for managed, unmanaged, and BYO devices, it's ideal for IT and employees alike.

99%

of threats to data security will spring from underlying vulnerabilities already known to the enterprise and its workforce.[1]

Simplify and secure user access

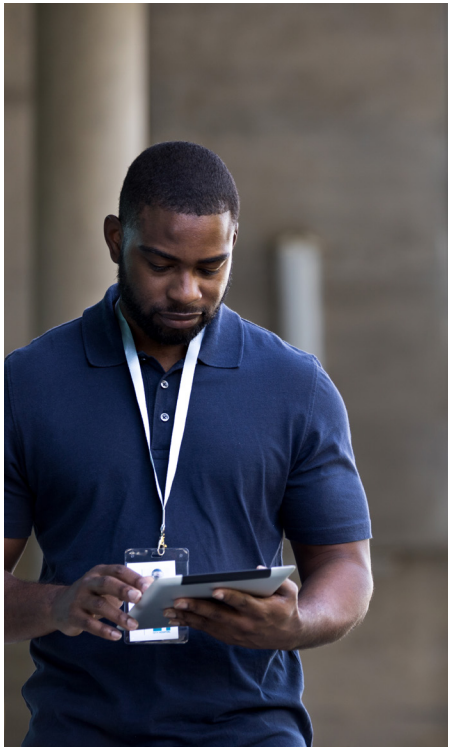
When employees are switching between multiple apps hundreds or thousands times a day, it's no wonder they're reusing the same password—a nightmare scenario for IT. With a unified access control solution for the entire digital workspace, you can improve security and the experience for users and IT. Reduce risk, gain more control over user access and behavior, and get deeper insights across your entire application landscape.

Access everything with a single click

Employees rely on various apps to get work done, but managing access to these apps creates challenges for both end-users and IT alike. Citrix Workspace with Citrix Secure Workspace Access improves the user experience by providing single sign-on (SSO) to SaaS and web apps, no matter where people need to work. Security is improved with fewer passwords for users to manage and hackers to exploit. And IT enjoys integrations with all major identity providers, multi-factor authentication mechanisms, and SSO protocols.

SaaS and web apps, secured

With 84% of organizations saying traditional security solutions don't work in cloud environments[2], it's no longer enough to manage access to SaaS and private apps. Citrix Workspace empowers IT with insight and control into how users interact with the apps to better protect against data exfiltration. Restricting actions users can take such as copying and pasting, printing, and downloading. You can also enable a watermark to appear on sensitive pages that someone tries to print or screenshot.



Provide secure access to private apps with a zero trust approach

Not long ago, network security was still relatively simple: Build a secure perimeter around resources and protect what's inside. Then apps moved to the cloud, employees began to rely on unmanaged devices and your attack surface expanded. As a result, today's organizations need a better way to protect corporate data—one that allows you to monitor access to apps, no matter where they're deployed. That's where zero trust network access (ZTNA) comes in. This VPN alternative offers a better, easier, and more secure way to authorize access to internal private apps.

Reduce your attack surface

As remote work continues to rise, so does the number of exposed VPN services. This is a concern since traditional VPNs connect unmanaged devices to on-premises resources and make trust implicit once network access is granted. The result is open connections, compromised assets, and an increased risk of network-level attacks. And as user traffic goes through your corporate network, any number of the 100,000 daily malicious web-borne threats could be free to roam. With zero trust network access, it's easy to overcome these challenges. By providing access at the application layer, Citrix Secure Workspace Access securely delivers apps and data to your users—without exposing your assets to external discovery.

84%

Percentage of organizations that say traditional security solutions don't work in cloud environments[2]

Securing access on untrusted devices

Personal devices are a critical component to consider for organizations that are cautious about how employees and contractors consume apps and data. Corporate-managed devices go through regular health checks to ensure they meet safety requirements. But most end users don't take the same care with personal devices.

Browsing the internet poses another risk, exposing devices to vulnerabilities in websites, browsers, and browser plug-ins. Malware that lives on employees' devices also poses a threat to corporate resources.

While most users understand they shouldn't visit potentially risky websites on their corporate-issued devices, they might not take the same care as their personal ones. Some organizations completely disallow internet browsing, affecting productivity and limiting BYO programs.

Citrix Secure Workspace Access incorporates a secure, embedded browser capable of applying stringent security policies. When security policies are enabled, the embedded browser is used. These policies include application and user interaction restrictions and advanced capabilities that scramble keystrokes and return screenshots as blank screens, protecting corporate data from keyloggers or screenshot malware.

Contain threats. Enhance productivity.

If restricting access to certain websites gets in the way of productivity for some users, Citrix Workspace offers Citrix Secure Browser. This cloud-based browser, hosted by Citrix, lets users browse the web without restriction. The browser is isolated from your company network, so if someone happens to visit a compromised site, no malicious software will ever reach your network or the user's device. Citrix Secure Workspace Access also protects user credentials and any sensitive information from being hijacked by any keylogger or anti-screen capturing malware.

70%

of all breaches still originate at endpoints.[3]

Improve the user experience

Traditional VPN technologies fall short when it comes to the digital workspace experience. Because they backhaul application traffic to the data center and clog the underlying network, these solutions can't optimize app access in ways that help support productivity. In addition, the routing of both business and personal traffic through corporate IT can potentially infringe on employee privacy. A better option is zero trust network access with SSO and contextual access that can be easily adapted based on individual device activity. This end-to-end contextual access ensures a superior employee experience without exposing your organization to unnecessary risk or creating privacy issues.

Modern solutions to modern challenges

The IT landscape looks drastically different from a generation ago, with many new risks to protect against. With Citrix's unified approach to zero trust, organizations can ensure fast, consistent, and secure access to applications anywhere, anytime on any device. This improves employee and business productivity. Simplified operations allow customer IT teams to focus on rapid delivery of new business-enabling digital services, further accelerating business productivity.

[www.partnersuppliedlink/CTA goes here.]

> **"For all the different kinds of users and roles we have within our company, the user experience still should be good. That's what Citrix is enabling us to do."**
>
> **Marco Stadler**
> Team Leader of Workspace Services, Bechtle

brought to you by

Partner Logo

Partner Badge

This area can be used for a partner-specific message. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eisumod tempor incididunt ut labore et dolore magna aliqua. Quisipsum suspendisse.

Sources:
1. Gartner, Inc., 2020 Data Security Predictions
2. Crowd Research Partners, 2018 Cloud Security Report
3. IDC 2020