citrix

Solution Brief

Citrix Enterprise Browser

Your journey to ZTNA starts with the Citrix Enterprise Browser

Over 400,000 organizations trust Citrix to deliver secure access to virtualized applications and desktops for over 100 million users.

With the rise of hybrid work, cloud migration of applications, and increased use of personal devices for work, organizations need a single and easy-to-administer solution for secure access to any application, from any device anywhere, without impacting user productivity. Traditionally, VPNs were the standard security solution but that is no longer the case.

Today, Zero Trust Network Access (ZTNA) solutions are increasingly replacing legacy VPNs. Citrix offers a unique and powerful approach to ZTNA that begins with the Citrix Enterprise Browser.

Security Risks

Although using VPNs is the most common solution, they have several security issues. VPNs lack granular security and scalability, so as a business grows with more employees in more locations, it will outgrow the VPN solution.

Another issue with VPN-based security solutions is that infected devices can access private applications through the VPN, leaking sensitive data to attackers. Since VPNs tunnel traffic to the entire network, any vulnerability will affect the entire network, making it impossible to isolate threats. Lastly, VPNs may not protect employees who bring their own devices, as old devices with unpatched operating systems and BYO devices do not have the necessary security to protect the device itself from malware attacks.

And security threats are not the only issues that businesses face. With the move to the cloud, applications have created more traffic to data centers, adding latency and inefficiency, reducing performance, and making employees less productive. Cloud SaaS applications can be more secure, but employees can still run into trouble by clicking hyperlinks within 'trusted' SaaS apps, which could lead to the accidental download

Average cost of a data breach 4.35 million*

Breaches affecting organizations with zero trust cost 20.5 percent less*

Breaches of businesses with a mature zero trust model cost 1.51 million less than those early in the zero trust journey*

*Gregory, Jennifer. (2022, September 21) Companies Without Zero Trust Could Lose $1M More During a Data Breach. Security Intelligence. https://securityintelligence.com/articles/companies-zero-trust-lose-data-breach/

of keylogger malware, phishing malware, and screen capture malware. Again, these actions could expose companies to data breaches.

Even accidental actions like sharing the wrong screen or having personal and business data on one machine can expose a business. So how does a business resolve security concerns while maintaining performance? With an enterprise browser.

What is an enterprise browser?

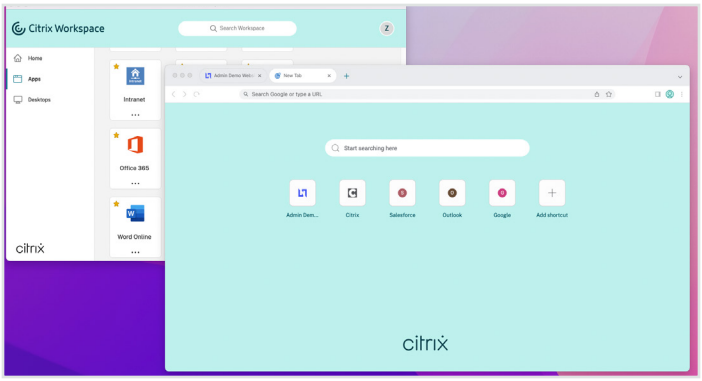
Typical consumer browsers do not offer controls to secure access to sensitive corporate data. To provide secure access IT teams often use a combination of VPNs, firewalls, and endpoint security solutions. While this approach works to protect infrastructure, it is usually insufficient in protecting sensitive corporate data from insider and external threats.

To overcome these challenges, access security must begin at the browser, where applications and data are accessed. An enterprise browser offers powerful security controls that IT can enable on a per-user and per-application basis, to mitigate cyber threats and data loss scenarios, without compromising the user's browsing experience or impacting productivity.

Introducing the Citrix Enterprise Browser

Citrix Enterprise Browser delivers secure, identity and context-aware access to any browser-based application without the need for a VPN. Our enterprise browser enforces 'just enough' access through granular controls for data loss mitigation and threat prevention.

The Citrix Enterprise Browser uses a zero-trust approach to authenticating activity on applications, which enables secure access no matter the users' location, role, device, or risk. The seamless integration with external identity providers also makes it easy for you to connect your existing provider for a consistent employee experience. The Citrix Enterprise Browser also does not require the device to be managed to apply security policies, simplifying your IT environment.



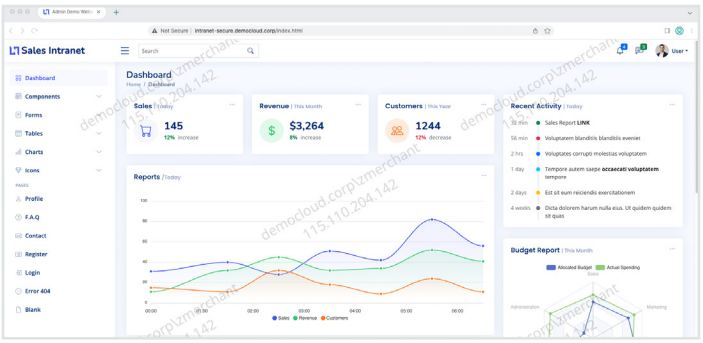
Citrix Enterprise Browser keeps corporate data secure without impacting worker productivity providing the same user experience compared to any consumer-grade browser. Key benefits are:

- **Single Sign On (SSO):** Authenticate users with unified SSO for internally managed web and SaaS applications to minimize passwords that users must remember. Use MFA and context awareness to assign precise levels of 'trust' to each user and device before granting access.
- **Seamless Browser Experience:** Support for tabs, bookmarks, progressive web apps, and video conferencing such as Microsoft Teams, Zoom, Cisco Webex, and more, ensures that users continue to remain productive.
- **Secure User Activity:** All user activity is protected by the configured security policies, no matter what web features are used.
- **Protect corporate-owned, contractor-owned, and personal devices:** Protect corporate-owned, contractor-owned, and personal devices: Reduce the attack surface by standardizing Citrix Enterprise Browser as the preferred enterprise browser to ensure that access from any device is secure.
- **Runs locally on PC or Mac:** No virtualization or infrastructure is required, so IT gets security and manageability without any additional overhead.

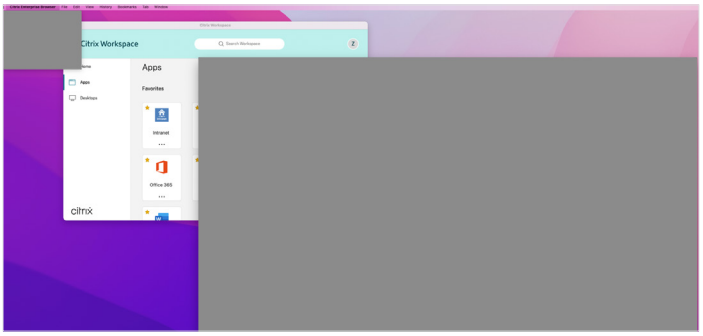
Contextual security policies on Citrix Enterprise Browser

In the age of data breaches, security has become more important than ever, especially when employees regularly handle sensitive information. With Citrix Secure Private Access, (SPA) you can deploy contextual security policies that IT departments can manage for all users, on a per-app basis. SPA works with the Workspace platform on the cloud, and it works with StoreFront on-premises, so the Enterprise Browser integrates seamlessly no matter if you're on-premises, in the cloud, or both.

The contextual security policies included on Citrix Enterprise Browser include copy and paste restrictions, watermarking, screen captures, download, and print restriction abilities. Watermarks indicate proprietary company information. The anti-screen sharing feature returns blank screens in the capture, rendering screenshot malware ineffective. Download and print restrictions can stop the movement of data off of the employee's device.



An example of Citrix Enterprise Browser's watermarking abilities.

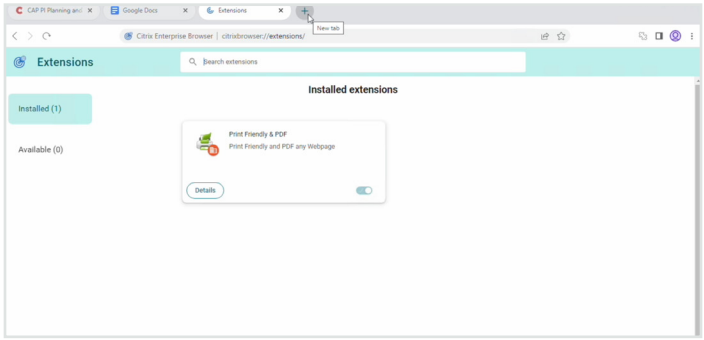


An example of Citrix Enterprise Browser's anti-screen capture feature.

Another security feature of the Citrix Enterprise Browser is built-in anti-keylogging, which scrambles all keystrokes within the browser, including logins, rendering any keylogging malware ineffective. These measures can mitigate data loss whether through an employee's unintentional mistake, or a bad actor intentionally trying to gain access to sensitive information. These security features allow your IT department to regulate exactly who can see, access, and record data.

Enterprise Browser Management

The Citrix Enterprise Browser is designed to replace the consumer browser but retain the same user experience. Our Chromium-based browser has all the functions that users are used to, like extensions, bookmarks, and password manager, but is also equipped with the ability for IT to push specific settings onto users. Extensions are blocked by default on the enterprise browser, but IT can create a forced list of extensions required to be installed on a user's browser or an allowed list where users can choose which to install.



An example of Citrix Enterprise Browser's forced extensions and available extensions list.

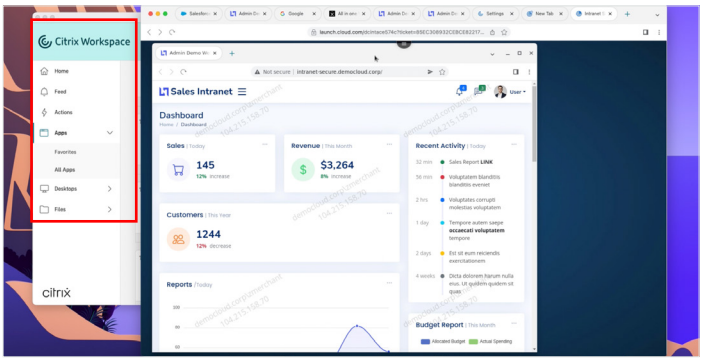
Admins can also allow or block password manager, push bookmark lists, allow or block incognito mode, allow or block developer tools, and more. Browser-level settings like cache, history, autofill, and cookies, can be set to clear automatically when a user quits the browser. Admins can also select the Citrix Enterprise Browser as the default browser to launch SaaS applications. Opening SaaS and web applications through the enterprise browser applies the configured security policies to the SaaS application.

What's most unique about the Citrix Enterprise Browser is that all of these features can be utilized on managed and unmanaged devices. This ability is unique to Citrix, relying on our custom-built policies designed to securely connect unmanaged devices. So if your business has contractors, consulting professionals, or anyone who uses a BYO device, you'll stay secure, while they can easily connect to any application they need.

Remote browser isolation mode

For certain highly regulated industries, the Enterprise Browser provides a solution to allow employees to access applications that need internet connections with strict regulation. It also provides protection from websites compromised by malicious actors. In addition to all the features mentioned earlier, the Citrix Enterprise Browser can also operate in an isolated environment by running on a cloud virtual machine, to securely render sensitive applications and apply the configured security policies. The isolated environment creates a gap between the web or SaaS application and the endpoint. This gap stops malware and prevents leaks of sensitive information.

The advantage of creating this gap is that you can separate the application and the end user. For example, if you had a very secure application, the remote browser isolation would allow the user to interact with the application but remain secure by blocking uploads. It works the same the other way around as well, if you have a user interacting with an unsecured application remote browser isolation prevents the application from downloading anything onto the local device. Many industries, like governments, retail, finance, and healthcare can utilize Remote Browser Isolation for compliance purposes, as well as to secure privileged and personal information.



The Citrix Enterprise Browser Remote Isolation mode.

Isolated browsers are stateless and discarded at the end of each session, making it impossible for any threats from malicious websites to access the corporate network. Applications that are configured by admins to open in remote browser isolation use a Linux-based remote desktop hosted in the cloud by Citrix that is completely discarded once the user is done with the application.

Getting started

Citrix Enterprise Browser is delivered as part of Citrix Secure Private Access, Citrix's ZTNA solution. The Citrix Enterprise Browser can solve critical challenges for your organizations, such as replacing legacy VPNs for secure access to browser-based apps, accelerating employee onboarding, simplifying M&As, or securing access for contractors and BYO devices.

Citrix Enterprise Browser can be downloaded and deployed for use within hours, accelerating your ZTNA implementation by months while significantly reducing IT operational overhead and easing user experience. For more details and a discussion around your specific requirements, please reach out to the Citrix team.

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