citrix

White Paper

Designing for a remote workforce

How to keep your data and intellectual property safe

Do you know what remote employees are doing with your data and intellectual property?

At the start of the Covid-19 pandemic, businesses rushed to give employees remote access to the tools they need to work from home. However, many of these tools won't protect you from threats. Here's what you need to know to keep your data secure—while providing a great user experience.

The #1 cause of intellectual property loss

Although remote work is now necessary, it creates gaps in your data security.

Studies have shown that IP leaves organizations primarily by accident. In fact, 62% of insider threats stem from "negligent insiders" who mistakenly give away company data or put it at risk.[1]

When employees work from home, they use networks and devices that aren't as secure as those in your office. This can make your intellectual property (IP), customer data, and other sensitive information prime targets for hackers.

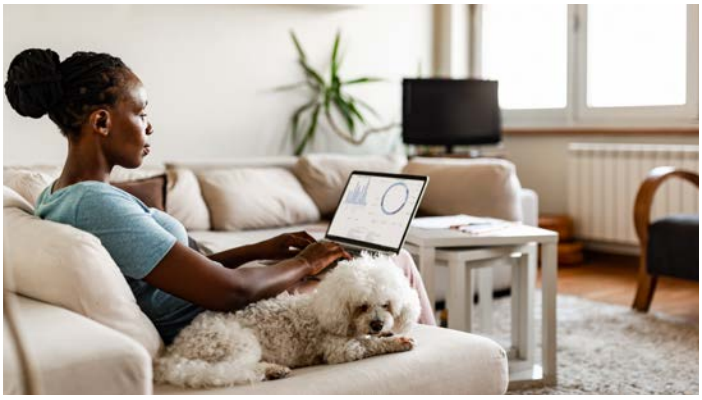
To protect your data and IP, you need a secure remote work environment. Your technologies also must give employees a seamless experience so that they can be productive—no matter where they work or which devices they use.

Unintended consequences: The problems with relying on a traditional VPN

Many IT teams used virtual private networks (VPNs) as a quick, low-cost way to give remote employees access to business apps.

But traditional VPNs do more harm than good.

VPNs require you to trust every device that connects to your network.



Anyone who logs into your VPN gets an all-access pass—even if their role only requires them to use a few applications. Granting free reign increases your threat surface and the probability of an attack.

Since most VPNs only authenticate users when they log in, hackers with stolen credentials can do anything they want after gaining access.

VPNs also don't account for changes in context. If a device is stolen, a VPN won't know if an employee or a criminal is logging in. This lack of context also increases your risk of insider threats, as employees can do anything they want with your data.

Essentially, a VPN is like a moat around a castle. If someone is outside the castle, they must ask a guard to let them in. But once you lower the drawbridge, people can go anywhere on the premises.

An estimated 25%–30% of the global workforce is expected to work from home multiple days per week by the end of 2021.

– Global Workplace Analytics[2]

Protect your corporate data and IP—no matter how or where employees access it

Citrix Virtual Apps and Desktops allows you to give remote employees the same secure experience they would have working in the office—without putting your data at risk.

Both remote and on-site workers can log into all of their business apps with single sign-on. However, context-aware security policies prevent your data from falling into the wrong hands. For example, you can specify that remote workers must authenticate more than employees who work in the office. This added security allows users to access their files and apps without creating the castle-and-moat issues of a VPN.

Meanwhile, your IT team can manage everything from a single platform. The central console gives you greater visibility into your security while allowing you to provision on-premises and cloud resources in minutes.

Here are three ways Citrix Virtual Apps and Desktops protects your IP—while giving users and your IT team a better experience:

1. IT controls the keys to the kingdom

Centralizing your apps and desktops allows you to manage your security policies from a single dashboard.

When you log into Citrix Virtual Apps and Desktops, you will gain complete visibility across all of your organization's apps, users, networks, and devices. Advanced analytics reduce your security blind spots and help you proactively respond to threats that can put your IP at risk.

And, unlike a VPN, nothing runs locally on user devices. If an employee loses their smartphone, you don't need to worry about someone finding it and accessing your IP and other sensitive data.

2. Prevent IP and data loss with zero-trust security

Citrix Virtual Apps and Desktops lets you apply zero-trust security to all of your business tools, including web and SaaS applications. It gives your third-party cloud apps the same level of protection as your published apps and desktops.

With Citrix Virtual Apps and Desktops, you'll go beyond identification and authentication to gain the added protection you need when users work outside of the office.

Use contextual security to control the actions users take within an application based on parameters such as device or location. Your security measures will automatically change based on where someone works. For example, you can block remote users from printing Microsoft Excel spreadsheets but grant them full printing capabilities when they are in the office.

IP theft costs U.S. companies $600 billion a year.

– **Theft of Intellectual Property Commission**[3]

3. Provision resources in just minutes

If you get a VPN, you need to install an agent on all end-user devices. The process is time-consuming and requires constant, ongoing management.

With all of your virtual apps and desktops centralized in a single platform, you can provision resources to workers without touching their devices. Get users up and running quickly—no matter where they are located.

If employees want to access their physical desktops through their mobile devices, we offer a secure connection. Your IT team can automate the installation of a lightweight client on office PCs and give users safe, remote access to their workstations. Meanwhile, you don't need to dedicate your limited IT resources to building out back-end infrastructure.

Do you want to safeguard your company's intellectual property without sacrificing the employee experience?

Discover what's possible with Citrix Virtual Apps and Desktops

Sources:
1. ThreatPost: Work from Home Opens New Insider Threats, June 23, 2020
2. Global Workplace Analytics: Work-At-Home After COVID-19—Our Forecast, 2020
3. CSO: Intellectual property protection: 10 tips to keep IP safe, February 28, 2019

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