Protect your business with AZ-IT and Citrix security

Reduce the risk of a cyber attack with a digital workspace

Are your company assets secure?

Stolen passwords, malware, phishing, denial-of-service attacks, ransomware—there is a long list of possible cyber attacks that can disrupt business and result in significant financial loss. Taking this into account, it's no surprise security is a top concern of business leaders making the transition from working in the office with IT-managed devices and apps to working remotely.

"75 percent of enterprises agree that we need a new security framework to address the threat of cybersecurity."[1]

— Citrix and Ponemon Institute

A **digital workspace is a set of integrated technologies designed to manage and deliver virtual apps and desktops**. It allows employees to access their apps and data in real-time on any device, from any location—regardless of whether the information is accessed through cloud services or in the data center. Security is enhanced with full visibility into network traffic, users, files, and endpoints making it easy to stay ahead of both internal and external threats.

Secure policies and access control across any network

The traditional model of security is to build a fortress around a business with a secure perimeter (firewall) and restrict access to resources (data center) with varying levels of permissions. Then came the need to embrace Bring-Your-Own-Device (BYOD) and allow employees to work on their personal devices. A great convenience for the employee, but IT has no control over these personally-owned devices.

"Information theft is the fastest growing cybercrime costing an average $3.6 million per data breach."[2]

— Microsoft

Left unchecked, IT has to constantly worry about data being saved on a USB drive and falling into the wrong hands, or that confidential information will be printed out and stolen. What about an employee who installs an unauthorized app on their personal device and transmits a virus or malware to the network—or uses a device that hasn't had a security patch installed in years?

With a digital workspace, security is centrally managed independently of the device—personal or company owned—or location, i.e. home network, public Wifi, or back in the office. Now IT can have visibility into all systems and sets policies that control what a user can or cannot do from any device or location—so corporate data is not carelessly or unknowingly put at risk. Real-time security policies define when users can print, upload, and download files, and more. IT can protect files as they are downloaded, detect high-risk activities, or revoke privileges if necessary.

Secure applications accessed from anywhere on any device

Applications are the lifeblood of productivity. Your workforce depends on a mix of applications including Microsoft Office, Windows apps like QuickBooks, and SaaS business apps to do their jobs. Managing this mix of locally installed Windows and SaaS apps is a constant cycle of installing, patching, and controlling for IT.

A digital workspace relies on application virtualization to securely deliver these apps as a cloud service, verses installing them locally on devices. Now IT can centrally manage access to every Windows, web, or SaaS app without ever touching a device—even employee-owned devices. It's seamless for the employees, yet IT gains the ability to protect apps from viruses, malware, keylogging, screen capture, and other attacks. Access to an application can be blocked if suspicious activity is detected, preventing unauthorized copying, sharing, or file download.

"Public clouds experience 60 percent fewer data breaches than on-premises data centers."[3]

— Impact

Secure user access and identity

There is no single, fail-safe method to prevent stolen passwords and relying on employees to create complex, unique ones and store them safely simply doesn't work. Weak passwords are chosen because they are easy to remember, one password is reused for multiple applications, and passwords are not updated regularly, making your corporate data low hanging fruit for hackers and easy to exploit.

"80 percent of hacking-related breaches used weak or stolen passwords."[4]

— Verizon

With a digital workspace, identity and access management is also centrally managed and cloud-enabled. Using single sign-on (SSO), users only need to log on once to access their virtual apps or desktop. This eliminates the need for multiple passwords to access multiple applications—more passwords, more problems—and ensures the passphrase is strong. The password manager automatically configures and maintains downstream application passwords, the user only needs to remember one, which can be made even stronger with two factor authentication.

Secure your company assets with a digital workspace

Business losses resulting from a cyber attack are substantial. Just figuring out how a breach happened can cost $15,000 or more. Virtual apps and desktops hosted in the cloud are inherently more secure than on-premises data centers and experience sixty percent fewer data breaches. In addition, cloud service providers have SLAs with 99.9 percent uptime and the expertise and training to predict, prevent, and respond quickly to any threat.

With a digital workspace your employees can work from anywhere using personally-owned devices with minimal risk of an attack. Users are given levels of access by IT according to their security profile and work requirements—with the right policies applied from day one to keep your valuable data secure at all times.

Start protecting your business today with AZ-IT and a Citrix-powered digital workspace.

Virtual Desktops (VDI)

About AZ-IT (AZ Informatique)

Founded in 2005 by Jean-Pierre Rérat, AZ-IT is a company active in the IT service for SMB, public administration, and industries. From its inception, quality and professionalism have been the hallmarks of the company. Anxious to further the interests of our customers, we resolutely turn to builders and providers of quality services. AZ Informatique strives to maintain the direction, quality, and intentions of its customers, whilst providing advice on the best alternatives available according to their needs.

az informatique

citrix™

Partner
Silver
Solution Advisor

[1]Citrix
[2]Microsoft
[3]ImpactMyBiz.com
[1]Verizon
[1]Fundera

Insert partner legal and trademark disclaimer. Delete if not used. Consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dt aliquip ex ea commodo. hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum.