Manage Risk by Protecting the Apps and Data That Drive Business Productivity

Today you face the challenge of securing a business environment transformed by technologies such as cloud and new workforce requirements such as mobility, BYO and third-party talent. Consider:

Your employees no longer do all their work at a corporate facility during traditional office hours.

Consultants, contractors and other outside parties are frequently part of your core team.

Your sensitive business data is in constant use across countless networks and devices, and must adhere to compliance regulations.

That information is increasingly vulnerable, as new threats and attack vectors emerge every day.

Traditional perimeter-based security has proven ineffective at preventing breaches and data loss. To be successful in this increasingly volatile environment, you need a new approach to information security, one that enables you to protect what matters most – your organization’s apps and data – without compromising productivity.

It’s no surprise that executive-level focus on security is at an all-time high. 1 And consider: In 2016, only 37% of CIOs said security and IT strategy were tightly integrated. Within the next three years, that number is predicted to jump to 80%. 2

Your security strategy needs to:

- Protect your organization’s most valuable assets and data from loss or theft
- Facilitate compliance and regulatory enforcement, while preparing for new and emerging requirements
- Allow people to access the apps and data they need from any device for full productivity
- Ensure the availability and performance of apps and data from any network connection & cloud environment
- Reduce the risk associated with disruptions, whether from planned activities or unexpected situations

Citrix Solutions are Trusted to Protect the Most Sensitive Information

With Citrix, organizations can provide the right level of confidentiality, integrity and availability to data without placing undue restrictions on the ways people choose to work.

The core security pillars of the Citrix offering include:

- **Contextual Access**
  - Gain the controls needed to ensure appropriate levels of access based on the user, end-point, network and security profile of every individual inside and outside your organization

- **Network Security**
  - Provide encrypted delivery of applications and desktops to employees and third parties, enforce network access control and segment networks for compliance and security, and deliver the highest level of service uptime and performance

- **Data Security**
  - Keep information where it belongs: in the data center, encrypt mobile data storage, and prevent data from residing on end points

- **Analytics and Insights**
  - Gain the ability to improve user performance degradation and quickly identify the source, rapidly detect misconfigurations and attacks, better comply with regulations and maximize uptime and productivity

Customers Around the Globe Rely on Citrix for a Secure Digital Workspace

Citrix unifies and enriches end user experience, secures all types of enterprise applications and data, and simplifies it’s ability to manage such environments in a secure, reliable, and consistent manner. Citrix creates a software-defined perimeter that combines secure access to apps and data with contextual control, visibility and behavioral analytics across devices, networks and clouds. By extending control beyond the traditional datacenter to mediate user interactions with apps and data, Citrix can proactively prevent, detect and mitigate risk with intelligence applied to each unique scenario.

With this holistic security and analytics approach, Citrix helps organizations address the growing cybersecurity threats of today by preparing for future requirements.