CITRIX®

5 ways to reduce risk and boost productivity

Citrix Workspace provides the best of both so you can enable new ways of working without sacrificing security

Contents

Balancing security and productivity in a mobile world 3

5 ways Citrix Workspace reduces risk and boosts productivity 4

1. One secure place to access everything 5

2. Contextual access 6

3. App and data security 7

4. Advanced controls for SaaS and the internet 8

5. Visibility and analytics 9

Confidence without compromise 10

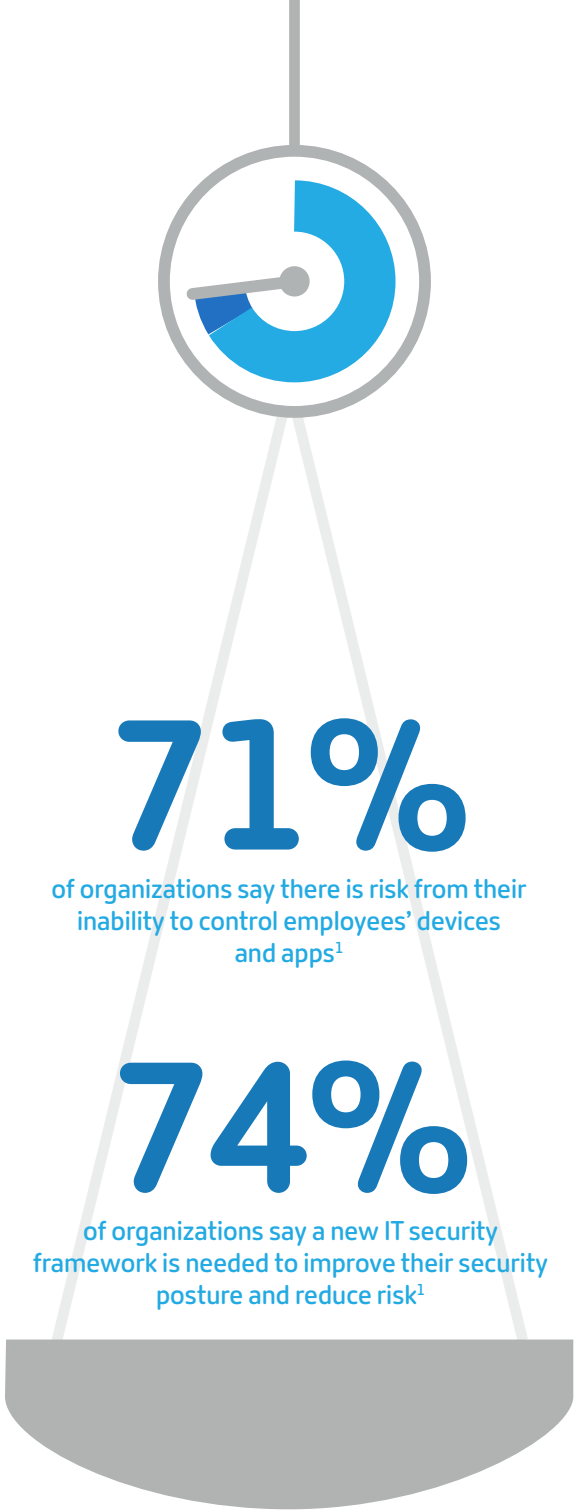
Balancing security and productivity in a mobile world

While IT must enable both the flexibility employees need to be productive and the security the business requires, this balancing act often ends in compromise.

As the center of work shifts to the user and to the cloud, IT is challenged with the complexity of adding and securing new technologies to support business needs and deliver new ways of working. The old way of layering multiple point security solutions is no longer enough to secure users working outside the corporate firewall.

The answer?

A secure digital workspace. It's the simplest, most integrated way to secure your apps and data across the clouds, devices, and networks where business is happening and people are collaborating.



5 ways Citrix Workspace reduces risk and boosts productivity

Click a circle below, or scroll to a section to learn more.

1. One secure place to access everything →

2. Contextual access →

3. App and data security →

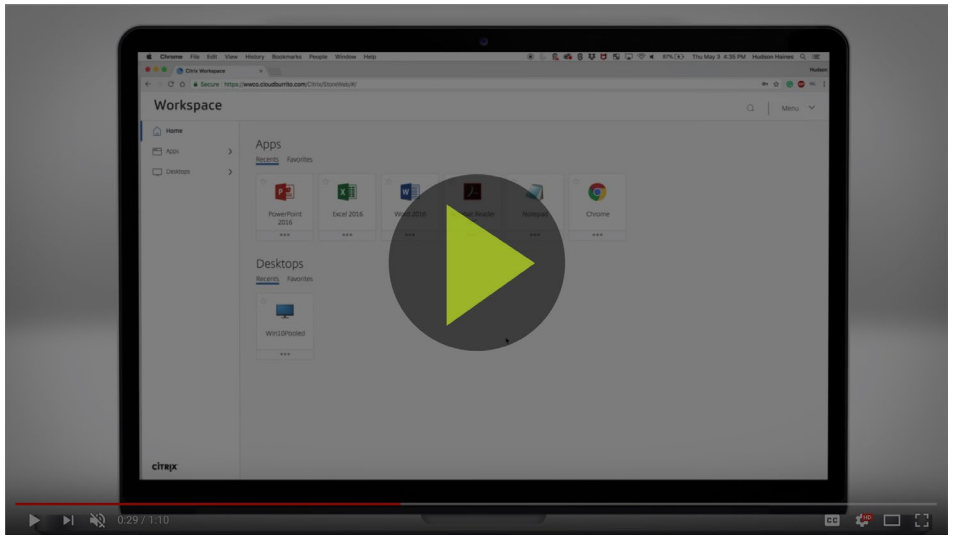
4. Advanced controls for SaaS and the internet →

5. Visibility and analytics →

1. One secure place to access everything

Citrix Workspace provides secure access to everything employees need to be productive. It doesn't matter what type of app they're using, where their data is stored, the network they're on, or the device they're using. Citrix Workspace provides:

- The ability to work anywhere, at any time with secure access to all apps and resources across any data center or cloud
- Single sign-on to apps, desktops, and files from one easy-to-use interface
- Integrated file sharing and approval workflows
- IT control over user accounts and password policies
- Support for SAML 2.0 for federation across applications
- Support for Azure Active Directory and on-premises Active Directory
- Secure access with microVPN and encryption for mobile users



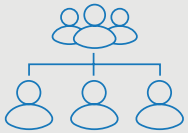
Don't have Adobe Flash Player? No problem. View on YouTube. →

2. Contextual access

Managing user access calls for a balanced approach that's convenient for users and more secure than a simple user name and password combination.

Contextual access is all about adapting to ever-changing situations involving users, devices, locations, data sensitivity levels, threats, and vulnerabilities that are risk-matched to desired business outcomes. It factors in who, what, when, where and why into every access and transactional event.

With automated access controls constantly evaluated and applied dynamically at the point of service, security decisions are consistently applied across all the different ways we work.



Integration with role-based access mechanisms like Active Directory allows you to create predefined access control policies at both the group and user level.

Being able to authorize access based on the device lets you quarantine or grant limited access for devices out of compliance.

Policy orchestration allows enterprise security policies to be applied for all the ways a user will access business resources, while considering the location, device, and other context to provide the best user experience balanced with the most security.

3. App and data security

Even as organizations like yours collectively spend billions of dollars to counter ransomware, malware, and cyber threats, the diversity, volume, and sophistication of those threats continue to expand.

Traditional methods for securing business information have proven insufficient to adequately address the complexities inherent in today's diverse threat landscape. You need a more robust, user-centric approach to keep data out of an attacker's reach and to keep business running as usual.

Citrix Workspace enables you to build defenses against ransomware by:

1. Insulating business data and corporate networks from web-based malware with secure browser services
2. Protecting data on mobile devices with device- and app-level protection
3. Using hypervisor introspection (HVI) to detect ransomware based on techniques, not just patterns, and prevent even unknown attacks and exploits
4. Implementing a robust enterprise data sync and sharing service to keep data out of reach of ransomware, facilitate backups, and maintain clean versions of every file for rapid restoration without the need to pay ransom
5. Providing a web app firewall and DDoS protection to keep web applications and sites safe from both known and unknown attacks, including all application-layer and zero-day threats

4. Advanced controls for SaaS and the internet

With Citrix Workspace, you can confidently allow employees to use the SaaS and web tools they need to be productive.

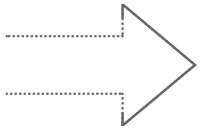
Citrix Workspace provides several capabilities to protect users from malicious websites, including web filtering and browser isolation. Plus, enhanced security policies for SaaS and web apps allow you to control user actions after they successfully sign in — for example, display watermarks on SaaS apps.

You can create policies to restrict:

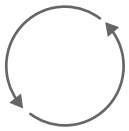
Clipboard access

Printing

Navigation bar



Back/forward buttons



Downloads

Mobile access

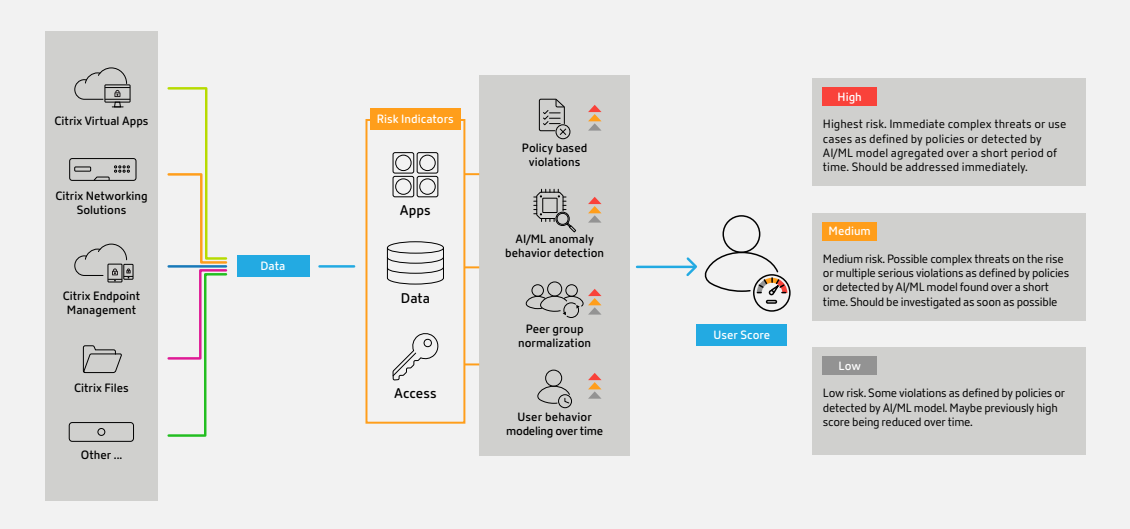
Screen capture

5. Visibility and analytics

Even in the best-secured environment, preventing breaches and maintaining a great user experience can be almost impossible without monitoring and detection. Real-time analytics are a critical tool for helping you identify threats while preventing any disruptions in user productivity.

Citrix Workspace with Citrix Analytics enables you to proactively handle user and application security threats, improve app performance, and support user productivity and continuous operations. Machine learning and advanced algorithms provide actionable insights into user behavior based on risk indicators across users, endpoints, network traffic, and files. If a user anomaly is detected, security policies can be automatically enforced.

- Stop malicious activity and prevent data loss with prescriptive actions to halt attacks
- Detect and prevent ransomware by recognizing the attack is underway and taking prescriptive actions
- Monitor and analyze user access and authentication behaviors



CITRIX®

Confidence without compromise

A secure digital workspace from Citrix combines the freedom and security your business needs to enable new ways of working that advance innovation and growth.

Explore Citrix Workspace

Source:
1. “The Need for a New IT Security Architecture.” Ponemon Institute, sponsored by Citrix, 2017
2. “2017 Cost of Cybercrime Study.” Ponemon Institute, sponsored by Accenture, 2017.
3. “Internet Security Threat Report.” Symantec, 2018.

Sales
North America | 1-800-441-3453
Worldwide | 1-919-745-6111

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

© 2019 Citrix Systems, Inc. All rights reserved. Citrix and Citrix Workspace are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks are the property of their respective owners.