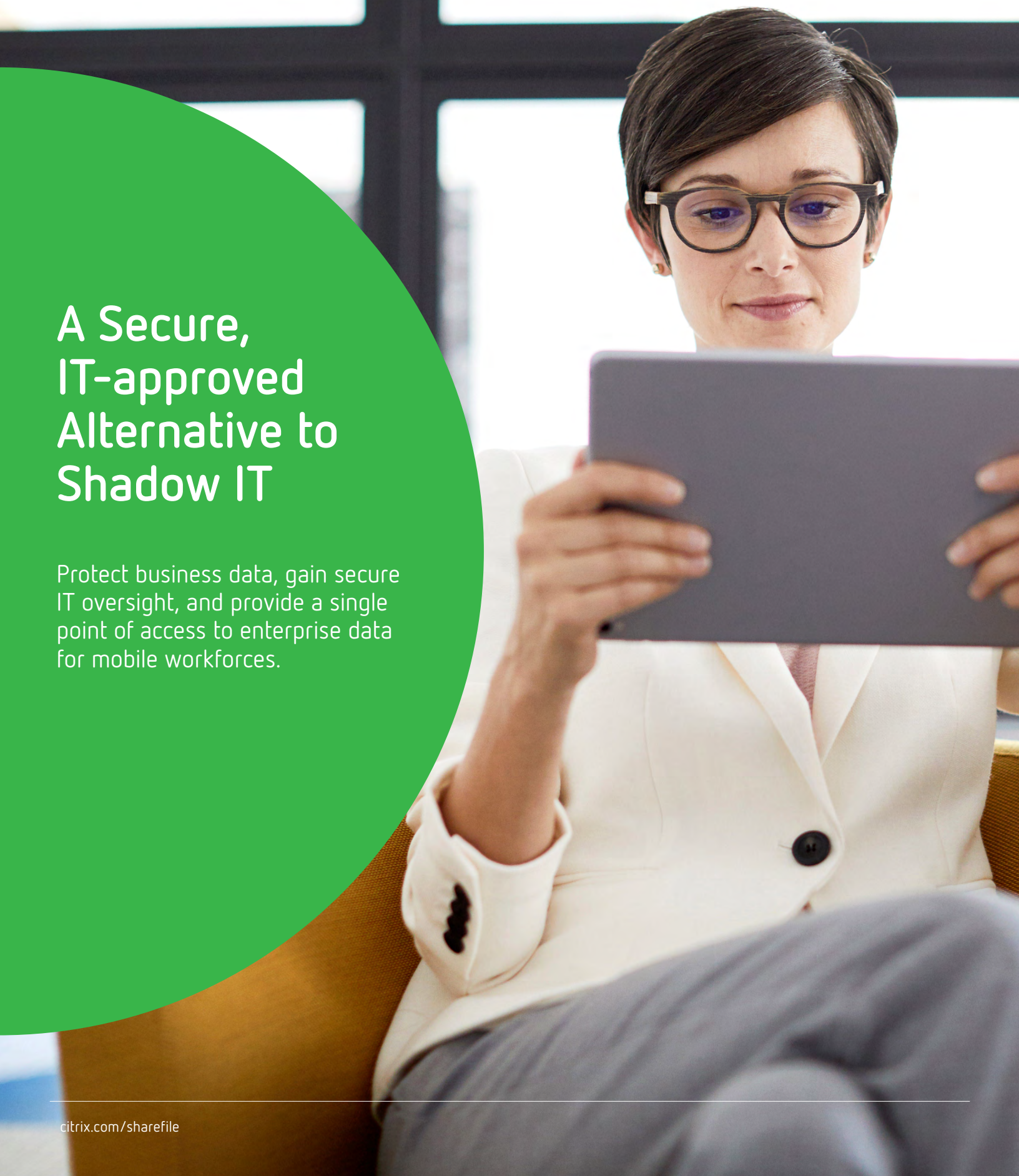
ShareFile®

CITRIX®



A Secure, IT-approved Alternative to Shadow IT

Protect business data, gain secure IT oversight, and provide a single point of access to enterprise data for mobile workforces.

According to an Enterprise Strategy Group report, 70% of organizations know or suspect their employees are using personal online file sharing accounts without formal IT approval[1].

The unauthorized use of personal apps and services—also known as Shadow IT—poses immediate and serious risks for organizations of all kinds. In most cases, employees seek out and use these services not out of malice, but to meet legitimate needs to share files for business purposes. Though personal apps and services have limited functionality and lack built-in security, they promise free storage, quick installation and a simple user experience. This can seem like a good-enough solution—especially for employees who are unaware of the risks associated with these services – but once an employee signs up for a personal account, the problems begin. As files are shared, business data is stored outside the control of IT, potentially exposing the organization to data leakage and breaches. These services also lack granular file control and many compliance certifications, putting organizations at risk of compliance violations in regulated industries like healthcare and financial services. Beyond the potential loss of confidential or proprietary information, the risks of Shadow IT include malware, hacking and other malicious activity. often compounded by embarrassment and damage to the company's brand and reputation.

To avoid such risks and to secure corporate data, apply these five ways to identify and eliminate Shadow IT:

1. Know where the risks are coming from

A recent Ponemon study revealed significant concern around the shift to mobile working. Over two thirds of respondents believe the trend for more employees working outside the office is a risk to IT security infrastructure. Further findings explain why this concern is rife across organizations. Just one-third of companies have a secure mobile strategy for bring your own device (BYOD) schemes, whilst six in ten admit employees or contractors use third-party apps for file sharing or productivity which are not sanctioned by IT.

Invest in effective cybersecurity

66%

of organizations
are expecting their information security budget for 2017 to increase

69%

claim their company has previously made investments in IT security technology which were not successfully deployed.

This creates additional pressure for any investments in 2017 to effectively tackle the main threats jeopardizing organizational security posture today.

Employees need technology which enables them to work in a productive manner and, for a large majority of organizations, this means being able to access corporate data and apps from any device and at any time[3].

2. Invest in effective cybersecurity

Over half of organizations are expecting their information security budget for 2017 to increase from last year, providing an opportunity to invest in security solutions which can address current fears around shadow IT and outdated infrastructure. Yet, over two thirds of respondents claim their company has previously made investments in IT security technology which were not successfully deployed. This creates additional pressure for any investments in 2017 to effectively tackle the main threats jeopardizing organizational security posture today[2].

A complete strategy for security technology encompasses virtualization of applications, desktops and networks; centralization of data to avoid exposure to risk on endpoints; and layered security on data sources to control access. With this secure infrastructure in place, security becomes simpler and more flexible, while people—and connected devices—can work in new ways without putting data and applications at risk.

3. Work with Shadow IT

Employees need technology which enables them to work in a productive manner and, for a large majority of organizations, this means being able to access corporate data and apps from any device and at any time. To combat current concerns around BYOD and shadow IT, businesses must look to invest in robust technology that is secure-by-design in order to protect sensitive business information wherever it is being accessed.

Today's workers need mobility, productivity, and flexibility. It's no wonder they're using consumer apps on the sly. Rather than focus on the consumer apps, IT needs to provide enterprise-grade solutions that allow workers to access information anywhere, including on mobile devices. The way to support file sharing is to say "Yes, we have a solution that's as easy as what you use at home but protects our files at the same time." Already have data stored in a consumer-grade app like Box or Dropbox? "Yes", we have a solution that connects to that data and allows you to share it securely and migrate to a secure storage zone[3].

4. Add additional security measures such as Data Loss Prevention (DLP) and Information Rights Management (IRM)

With the ever growing mobilization of the workforce, data has a tendency to develop legs. Once the recipient has downloaded a file, the authentication and authorization controls no longer apply. They are free to re-distribute that file to anyone using any means (USB drive, email attachment, personal cloud account, etc.). A file you intended to only be seen by one recipient, suddenly has found its way to an unauthorized user that you never intended.

Organizations have been deploying DLP to address regulatory compliance, intellectual property (IP) protection and data visibility and monitoring. Newer solutions that include user entity and behavior analytics, image analysis, machine learning, and data-matching techniques are being used to augment existing solutions.

How can IT ensure that content sent to a recipient is only viewed by that person? This is where Information Rights Management or IRM helps. It's a follow-me security model that allows for security protections to continue being enforced no matter where the data goes.

Information Rights Management applies file-level encryption, authentication and authorization controls to downloaded documents. You set some very simple and straightforward sharing permissions to a file you intend to send to a collaborator.

These could include controls like:

- Whether the document can only be viewed
- Whether it can view and printed
- Or whether it can be view, printed or edited

5. Shift your focus from protection to prevention

Strategies in the past focused on walling in employees with security technologies such as VPN and firewalls to keep ransomware and malware out. IT professionals are realizing that prevention is both costly and nearly impossible. Instead, organizations are investing in advanced security features, security intelligence (analytics and reporting), secure cloud storage solutions, end-point management big data tools in order to rapidly detect, identify and respond.

"Take the money you're spending on prevention and begin to drive it more equitably to detection and response. The truth is that you won't be able to stop every threat and you need to get over it[5]."

Earl Perkins | Gartner Research VP | Gartner's 5 Trends in Cybersecurity for 2017 and 2018

Learn More

As a leader in the 2017 Gartner Magic Quadrant for Content Collaboration Platforms, Citrix ShareFile provides enterprise-grade security capabilities that no consumer service can match, including granular permissions and access control, mobility for all enterprise data, flexible data storage options and integration with existing infrastructure—all with a great user experience designed to enable collaboration and productivity.

With ShareFile, enterprises gain a single point of access to mobilize business data that helps IT protect business data, regain visibility and control, ensure regulatory requirements and data compliance, and enhance employee productivity with a mobile, work-from-anywhere solution.

For additional information, please visit citrix.com/sharefile.

References:

[1]Gartner: 7 top security predictions for 2017

[2]ESG Research Report, Online File Sharing and Collaboration: Security Challenges and Requirements

[3]Citrix Ponemon Research: The need for a new IT security architecture

[4]Gartner: Forecast Analysis: Information Security, Worldwide, 1Q16 Update

[5]Gartner: 5 trends in cybersecurity for 2017 and 2018

CITRIX®

ShareFile

North America | 1 800 441 3453
Worldwide | +1 919 745 6111
United Kingdom | +44 800 680 0621
Australia | +1 800 089 572

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