Tap the Potential of Shadow IT

Give employees tools they love while keeping your company safe

Google for Work

Executive summary

IT and business leaders today are grappling with the ever-increasing use of personal devices and unauthorized apps at the office, often referred to as “Shadow IT.”

This rapidly emerging trend comes as a natural response to employees looking for ways to create and collaborate with the same ease, efficiency and freedom that they do in their everyday lives. While the rise of Shadow IT can pose numerous security risks to companies, it also offers unique opportunities for businesses to rethink their traditional tools and processes in ways that both support productivity and innovation while minimizing risk.

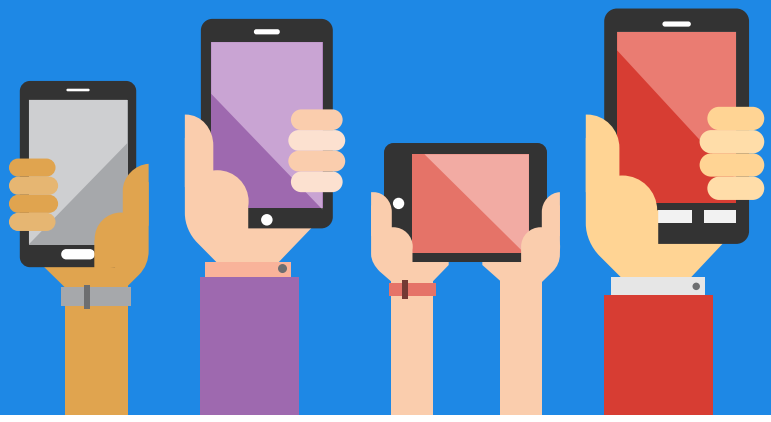
At Google, we believe companies should not have to choose between agility and security. This white paper examines the role of IT in the new landscape, offering insights from IT and businesses that have leveraged Google Apps for Work to empower employees with collaboration tools they know and love while providing robust security and controls that protect data.

Read on to learn more.

The Google Apps for Work team

Tap the Potential of Shadow IT

Give employees tools they love while keeping your company safe



There was a time not too long ago when personalization in the office consisted of bringing in your favorite coffee mug and sharing with co-workers amounted to sending interoffice mail. But with the rise of tablets and smartphones, as well as cloud-based services and apps, the line between life and work has rapidly blurred.

Today, devices and apps for consumers and businesses are virtually interchangeable. Workers who once needed to come to the office to hold a video conference, collaborate on a document or presentation, or talk to someone in another city or country, can now do all those things from anywhere, at anytime with just a few taps on a smartphone.

Given the freedom, speed and simplicity of consumer technology, it's no wonder employees are increasingly turning to their personal devices and apps to be more productive in the workplace. For companies, however, the use of unauthorized apps or "Shadow IT" at the office poses a whole new set of security risks—from data theft and malware infections to compliance violations, competitive threats and reputation damage.

In this new environment, IT managers often find themselves caught in a balancing act: how to manage and safeguard company information while still supporting creative freedom and productivity.

At Google, we believe companies should not have to compromise. This white paper will examine the role of IT managers in the new landscape and show how Google Apps for Work can offer an IT solution that both empowers employees with collaboration tools they know and love and provides robust security and controls to keep valuable data safe.

Who's using Shadow IT?

The short answer? Everyone. Unapproved third-party apps and cloud software services have been making their way to the office for at least a decade, as tech-savvy employees look for faster and easier ways to store, access and share files and connect and collaborate with colleagues. Recent studies estimate that 79% of enterprise businesses have employees who use consumer file sharing or collaboration tools at work, with or without approval.[1]

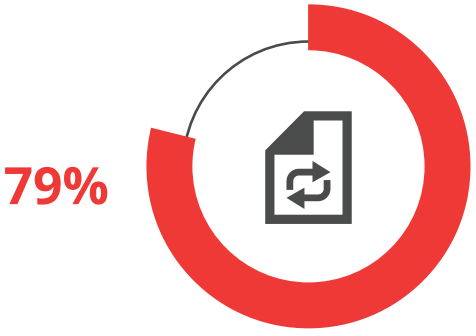
Research firm Gartner reports that 38% of enterprise IT expenditure is already happening outside of the corporate IT budget. That number will reach more than 50% by 2017.[2]

In a 2013 Frost & Sullivan survey of 600 IT and line-of-business employees, more than 80% admitted to using non-approved Software-as-a-Service (SaaS) to do their jobs more effectively and efficiently.[3]

Shadow IT is not limited to one function or service. Consumer apps are being used across the board to provide solutions to a host of everyday workplace issues that companies struggle with—from file sharing without endless versions or attachments to video chat that lets people meet face-to-face from anywhere in the world.

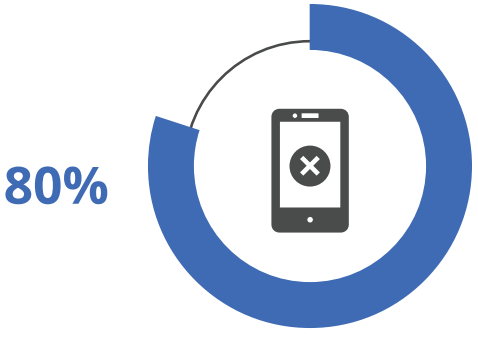
According to a study by Accenture, 44% of employees express dissatisfaction with the devices and software provided by their employer.[4] Nearly half of those say they will end up using consumer applications for work.

It's not just devices, people are also bringing apps to work



79% of organizations have employees using **consumer file sharing and collaboration tools**

Based on data from IDG, *Consumerization of IT in the Enterprise* (CITE), March 2014



80% of end-users use **unapproved** apps

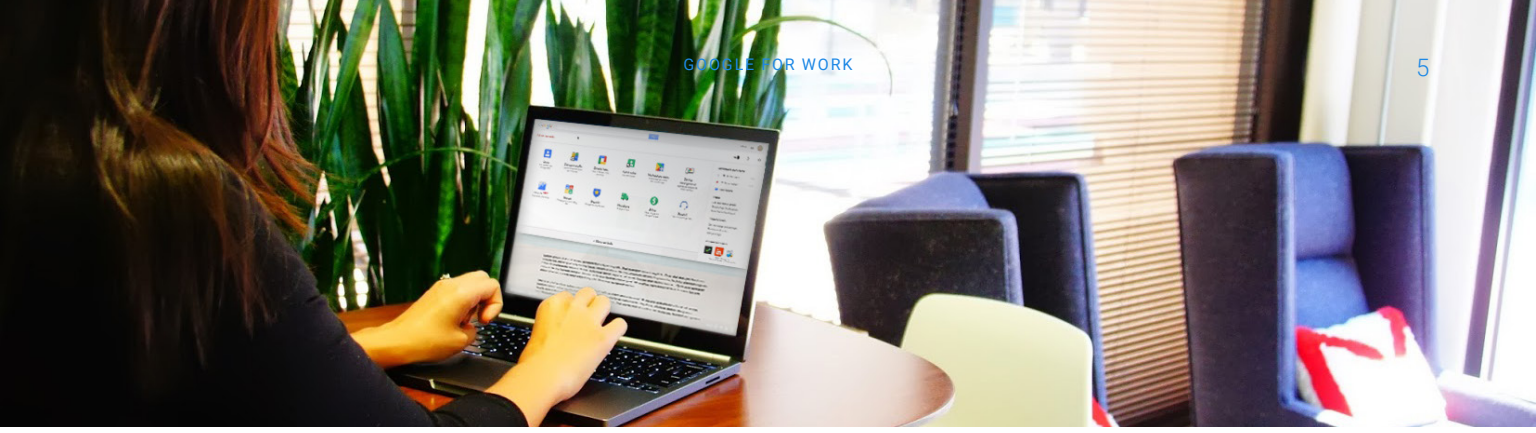
Frost & Sullivan, "*The Hidden Truth Behind Shadow IT*," November 2013

[1] IDG, *Consumerization of IT in the Enterprise (CITE)*, March 2014

[2] Gartner Says Digital Business Economy is Resulting in Every Business Unit Becoming a Technology Startup, October 6, 2014

[3] Frost & Sullivan, "The Hidden Truth Behind Shadow IT," November 2013

[4] Accenture, "Consumer IT: The Global Workplace Revolution has Begun," 2011



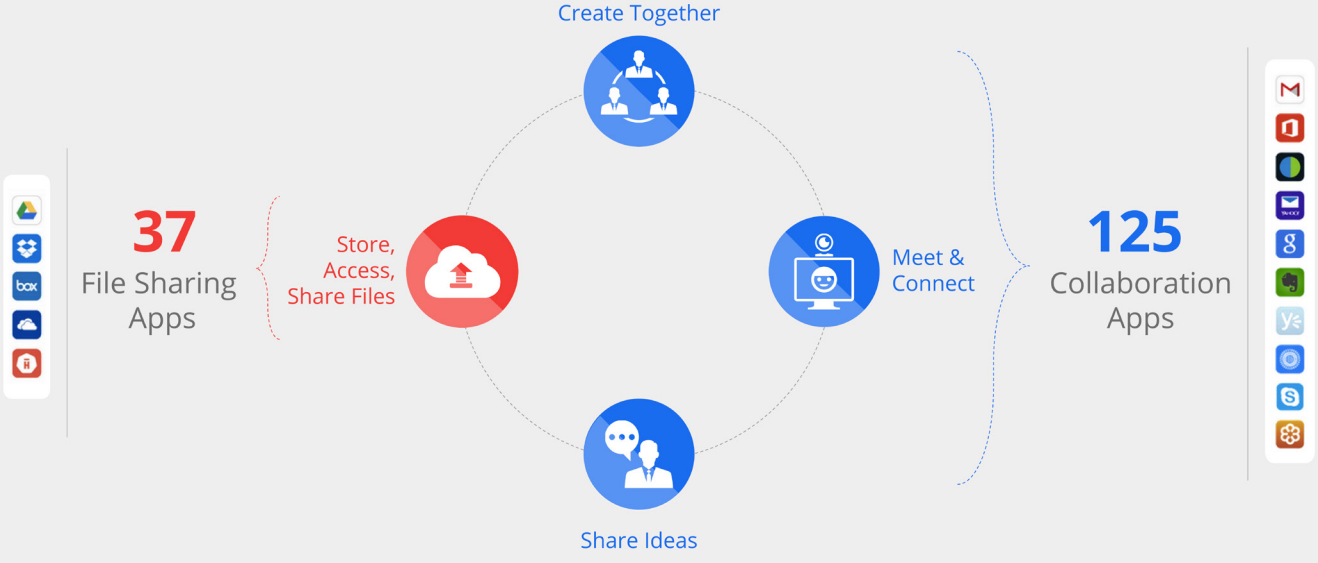
Among the most common problems people are solving with consumer apps at work:[5]

- Backing up and storing data
- Sharing files
- Collaborating on documents
- Accessing work from mobile devices
- Connecting through video conference and messaging
- Sharing ideas through social media

> The right thing to do is to help people be as productive as possible, and the way to do that is … to understand the toolset that people … want to use. To the best of your ability, you need to give them that toolset. When you do that, it creates a completely different organizational culture."

— Ben Fried, CIO, *Google*

While file sharing is the symbol of this phenomenon, collaboration is the broader need



The average mid to large size company uses 37 types of file sharing and 125 collaboration services.

Source: Skyhigh Cloud Adoption and Risk Report - Q3 2014, based on anonymized usage data from over 350 companies

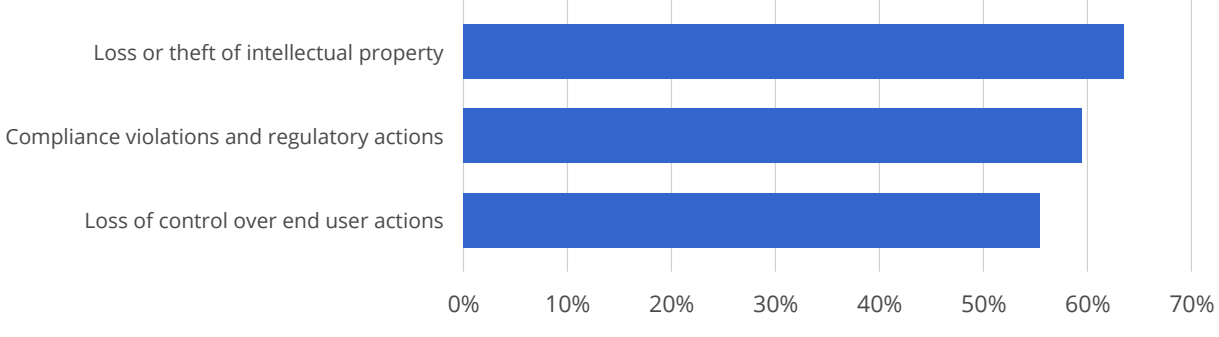
[5] Based on data from IDG, Consumerization of IT in the Enterprise (CITE), March 2014 and Frost & Sullivan, "The Hidden Truth Behind Shadow IT," November 2013

From an IT standpoint, the use of unapproved apps is not just a question of violating company policy. Shadow IT exposes businesses to a whole set of risks ranging from data theft and regulatory compliance to phishing and snooping scams, competitive threats and compromised reputation.

As ominous as this sounds, Shadow IT is not the enemy. It is a natural response to employees who want to work better and faster using tools they already know and love.

Simply put: Employees are looking for ways to create and collaborate in the workplace with the same ease, efficiency and freedom that they do in their everyday lives.

Managers worry most about the use of unauthorized apps



Source: Ponemon Institute© Research, "The Insider Threat of Bring Your Own Cloud (BYOC)," figure 6 (top three results), 2013

Lockdown isn't the answer

Trying to control or put a stop to people using personal apps and devices at work is like the old cartoon where the hapless hero tries to plug a leak in a dam by sticking his finger in the hole. For every leak he plugs, 10 more spring up, until he runs out of fingers and the dam bursts. When you consider that the use of productivity apps grew 121% in 2014,[6] it's clear that the trend of personal devices and apps in the workplace will only continue to rise at ever-increasing rates. According to recent Forrester research, 69% of companies currently endorse a BYOD (bring your own device) policy at work, with 85% expected to implement by 2020.[7]

> If governed, managed and guided appropriately to mitigate the risks, Shadow IT can create a lot of value for the organization. But the opposite is also true, in that, left unguided and controlled, it can destroy value."
>
> — Gartner, *Embracing and Creating Value From Shadow IT,* 2014

[6] Flurry Analytics, 2014 year-end survey of 2.079 trillion app sessions, January 2015
[7] Forrester Telecom & Mobility Workforce Survey, 2013

Source: The Weather Company video

So what's the solution? At Google, we believe companies need to look at Shadow IT from the other side of the equation. Rather than trying to shut down apps and devices in the office, IT decision-makers should be embracing the value cloud technology can bring to the workplace and find ways to both educate employees about the risks of unauthorized apps and empower them with better tools and services that can be managed in a secure environment.

"The conventional wisdom of our industry is that we can't have efficiency and choice, we can't have security and choice," says Google CIO Ben Fried. "I have discovered during my time at Google that is a complete falsehood."

IT, the ultimate enabler

"With the cloud, the power to build new products and features to delight your customers and win future customers can be distributed through your entire business," explains Urs Hölzle, Google's SVP of Technical Infrastructure. "The central IT organization is not a blocker of progress, but the ultimate enabler."

Google Apps for Work is a cloud technology designed precisely around this guiding principle: that companies can empower employees with technology that breaks down barriers to productivity rather than building them up. To do this, they need to be able to safely access the right applications and information, from any location, using any device.

> We've also started using Google Drive to replace personal Box and Dropbox accounts that people had been using to share documents, so we'll have centralized control of our intellectual property."
>
> — Bryson Koehler, CIO, *The Weather Company*

> Managers … must support their employees and help them be productive, but they must also enforce corporate information policies. To succeed, managers need to find a file-sharing solution that is accepted and used by all."[8]
>
> — Larry Hawes, *Gigaom Research,* 2014

[8] Source: Harnessing the tyranny of autonomy: the Dropbox problem and the manager's dilemma A Social Report by Larry Hawes, 2014

This combination of freedom, productivity and security is what convinced Woolworths, Australia's largest retailer, to switch to Google Apps last year. With 3,000 stores and 200,000 employees, the company was looking for ways to help people connect and communicate better and to work more collaboratively across all their stores and offices in Australia and New Zealand.

Using tools such as Google Drive, Docs, Gmail, Calendar and Hangout, as well as a custom-made "tap to support" iPad app built on Google App Engine, Woolworths has transformed the way they do business. Teams in different cities and countries can now collaborate in real time and managers are able to contact the national support office from the shop floor, rather than tying themselves to a laptop in the back office.

"Google has transformed the way our employees interact with technology and collaborate with each other at every level of the organization," says Dan Beecham, Woolworths Limited CIO. "And Google's technology makes it very easy to do things in a secure way, therefore our people do things in more secure ways."

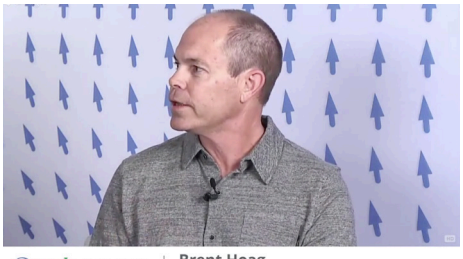
For Briggs & Stratton, a century-old manufacturer of gas-powered engines and generators, Google Apps offered a way to expand into the consumer market and overhaul antiquated systems that were bogging down productivity, hindering their ability to respond to customers and leaving the company vulnerable to security threats.

"When I discovered that 15% of our network traffic was consumed by unsecured content storing and sharing and realized that poor communication was leading to inefficiencies, I pushed for a move to Google Apps," says Brent Hoag, Briggs & Stratton's CIO.

Google Apps enabled businesses to replace things like paper checklists and outdated databases with the simplicity and speed of Google Drive, which lets everyone from the assembly line to the sales office access, sync and share the latest data from any device.

Since making the transition to Google Apps, Briggs & Stratton has not only streamlined its manufacturing and business processes, it's cracked the consumer market with 40 new models of lawn, garden and outdoor power equipment.

WATCH WOOLWORTHS STORY »



WATCH BRIGGS & STRATTON STORY »

"I knew that switching to Google's platform would not only fix our communications problems, but help our 3,000 employees be both more innovative and more effective."

— Todd Teske, CEO, *Briggs & Stratton*

A complete, secure solution

Google Apps for Work offers a holistic solution for businesses like Woolworths and Briggs & Stratton who are striving to become more connected and agile in the changing digital environment. Google Apps for Work is a complete set of business-grade tools—Drive for file storage and sharing, Hangouts for video meetings and chat, Docs, Sheets, Slides—conceived and developed with Google's commitment to performance, security and reliability.

For IT managers trying to steer a course that drives innovation and productivity without sacrificing security, Google Apps for Work offers a clear path forward: advanced and secure infrastructure, monitored around the clock, protected by more than 500 security experts and chosen by more than 5 million businesses worldwide.

Management tools such as advanced audit reporting, customized sharing controls, mobile encryption, built-in archiving and e-discovery provide additional layers of security. And they're all instantly accessible via a simple, centralized admin console.

For a lot of IT managers, this hassle-free management has another benefit: it helps them do what they really love to do. "It frees us from mundane, repetitive tasks that add little value to what we do so that we can focus on enhancing our core competencies and delighting customers in new ways, " says Stanley Toh, Global Director of IT at Avago Technologies, who moved to Google Apps for Work in 2006.

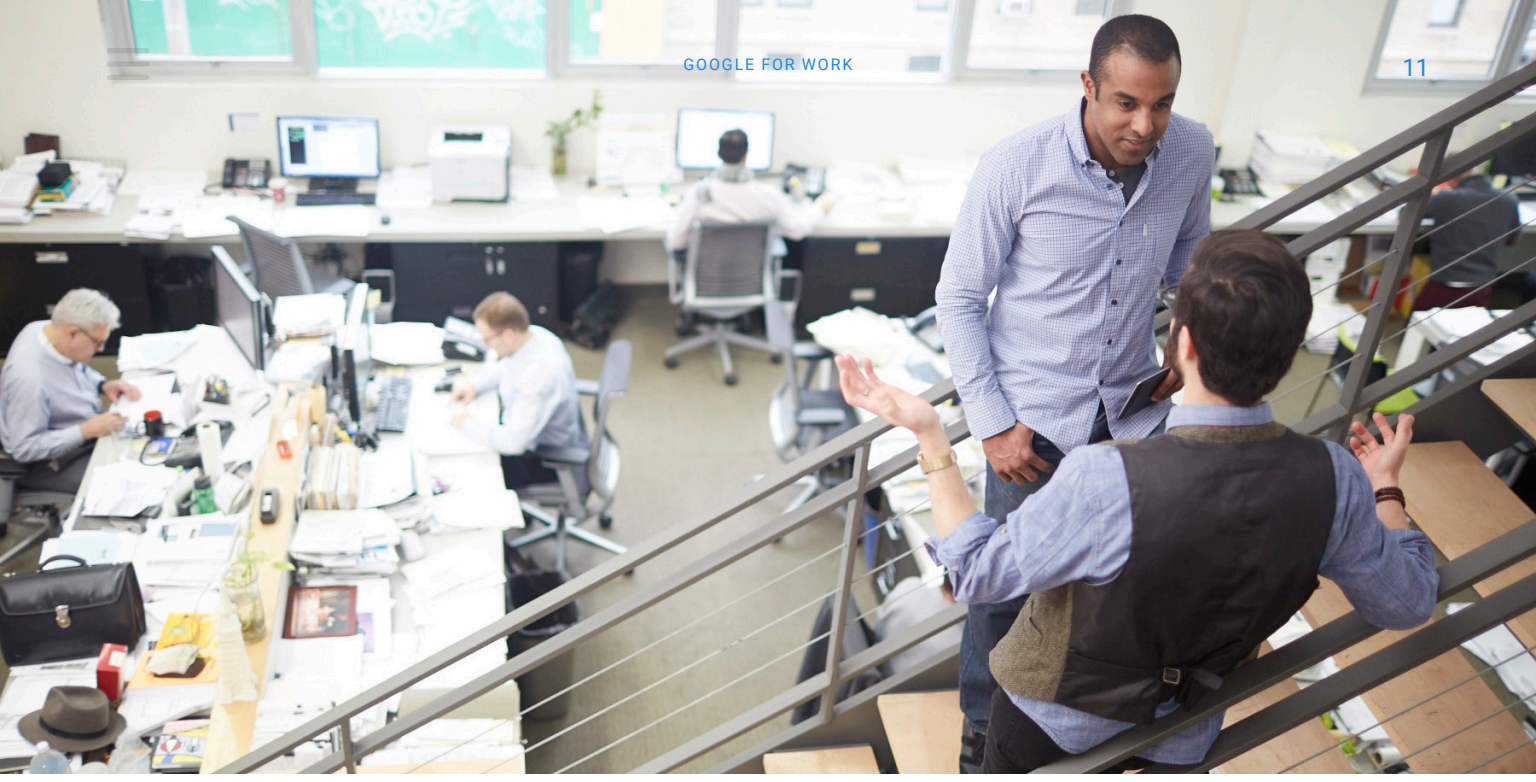
Back up and store data

Share files

Collaborate on documents

Access work from mobile devices

Connect through video conference and messaging



Getting started

The most important lesson we can learn from the use of Shadow IT is that companies no longer have to choose between agility and security. With Google Apps for Work, they can offer an IT solution that both supports employees' needs and minimizes corporate risk. The first step toward tapping the positive potential of Shadow IT is to take an honest look at how employees today collaborate and communicate. This means:

- Evaluating what apps and services are being used
- Understanding what employees are trying to do with these tools
- Educating users about how to keep company data safe
- Identifying better, secure and productive solutions

> "The solution is for [companies] to develop policies that strike the right balance between flexibility and control. IT and business leaders need to work together to create and support policies that enable employees to use the apps they need to be productive, with controls in place to protect data and minimize corporate risk."

— Frost & Sullivan, *The Hidden Truth Behind Shadow IT*, 2013

Want to continue the discussion?

Learn more about Google Apps or call us now at (855) 778-5079.