Shadow IT in the Enterprise

Softchoice SaaS Study 2013

softchoice

Table of contents

Softchoice's SaaS Study 2013 examines the prevalence of Software-as-a-Service (SaaS) applications in today's enterprise environment. Based on an analysis of roughly 7,200 enterprise users across 23 distinct organizations spanning industries including finance, law, health care, and manufacturing, Softchoice's latest audit details the rampant and widespread use of SaaS applications whether organizations know it or not.

Executive Summary

The world of enterprise technology is changing. Between the decentralization of corporate budgets and the consumerization of IT, the IT manager's role has become muddled, at best. The Bring Your Own Device (BYOD) phenomenon and ubiquity of unsanctioned personal cloud applications have created a difficult scenario for technology managers.

On the positive side, employees are more nimble, and are adopting technologies to do their jobs better, faster and from anywhere—hence the mass migration to smartphones and tablets. The work-everywhere mentality hasn't been restricted to hardware. Personal Dropbox accounts and Google Drive are also more common in the workplace.

However, the IT department's best efforts to enforce corporate IT policy are often met with varying degrees of resistance. Further, IT managers must contend with common employee misperceptions that their departments serve as a gatekeeper to remove vital "consumer" software and applications from the enterprise.

Softchoice, a leading North American technology services and solutions provider, regularly conducts proprietary TechCheck audits for enterprise clients, taking a full account of an organization's technology environment. These audits examine how many devices within the company are operating SaaS applications (sanctioned by company policy or otherwise), and which specific applications are in use.

What follows is a deep dive into Softchoice's latest audit, which explores the habits of 7,199 end users across 23 organizations from small to medium-sized enterprises. With a special focus on the most pervasive types of applications used by employees – including remote access, file sharing, online storage and collaboration – this whitepaper will uncover trends to help IT departments navigate the complexities of managing SaaS applications, while keeping employees productive and engaged.

Some key findings from the Study:

- **Over 80% of organizations are using some form of remote access app**, indicating a clear trend towards BYOD and flexible working environments
- **Google's suite of personal productivity apps is king in the enterprise**, with Google Calendar appearing in 83% of businesses, Google Docs in 80%, and Google Drive in 75%
- Contrary to popular belief, **Microsoft SkyDrive is a top contender for online storage** with 79% enterprise penetration – more than double that of Dropbox

Data Collection Methodology

The data collection for this study was made possible through Softchoice's award-winning IT assessment services, specifically its SaaS TechCheck assessment.

This assessment provides detailed IT inventory data from organizations designed to:

- Define the exact cloud application services being utilized throughout the environment
- Identify options for existing on-premise applications
- Develop a baseline for the current state of cloud in the environment

A portion of this data was analyzed in aggregate to produce the findings pertaining to the prevalence and use of SaaS applications among North American organizations.

SaaS Applications: One Family, Multiple Species, Different Breeds

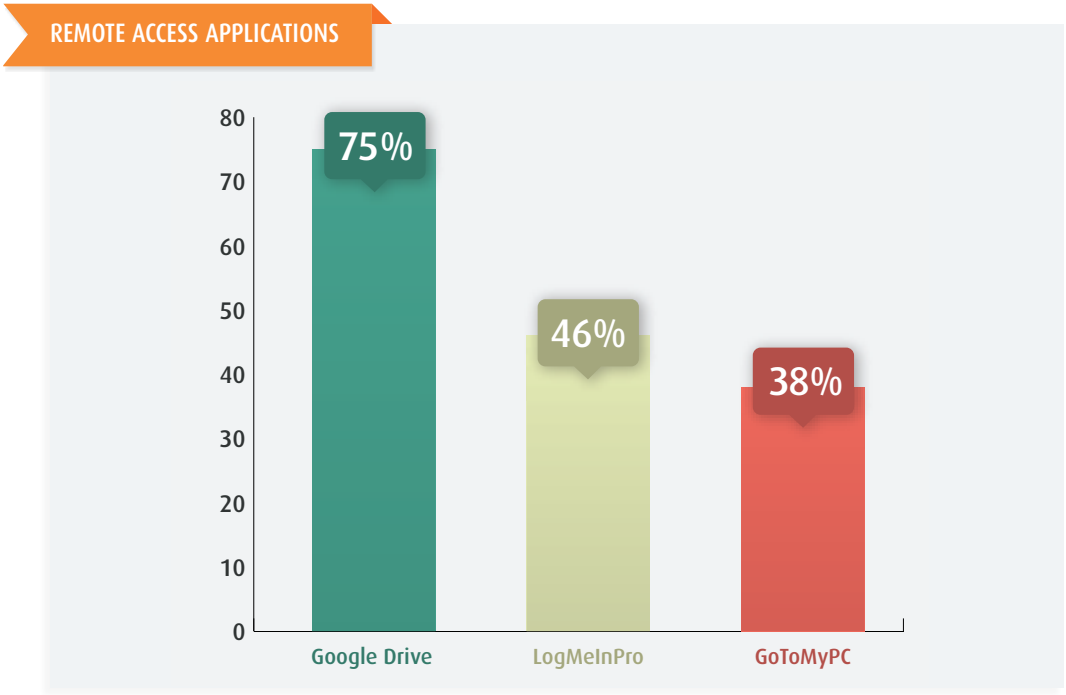
SaaS applications have gained a strong foothold in the enterprise. More than 55 percent of users assessed for the study are currently running SaaS applications on corporate devices. With SaaS growth outpacing the overall software market, this number is expected to increase, while corporate IT departments simultaneously struggle to determine which SaaS applications are safe and which pose threats.

Most organizations have little insight into the SaaS applications employees are using at any given time. This lack of understanding often results in diluted or misguided policies surrounding SaaS applications, including blanket bans, which are ineffective and contentious to employees. Instead, organizations must have a clear and complete picture of not only the applications employees are using, but also, how and why they are using them.

Remote Access: Extending Corporate Data Beyond Office Walls

Prevalent in 83 percent of organizations, remote access SaaS applications allow users to easily access and share files across devices – desktops, laptops, smartphones and tablets – regardless of physical location. With these apps, employees can virtually log in to their corporate-issued computer from any device, even smartphones.

With collaboration features such as group editing and shared storage space, Google Drive is by far the most popular remote access application, used in 75 percent of companies, followed by LogMeInPro in 46 percent of organizations, and GoToMyPC in 38 percent of organizations.



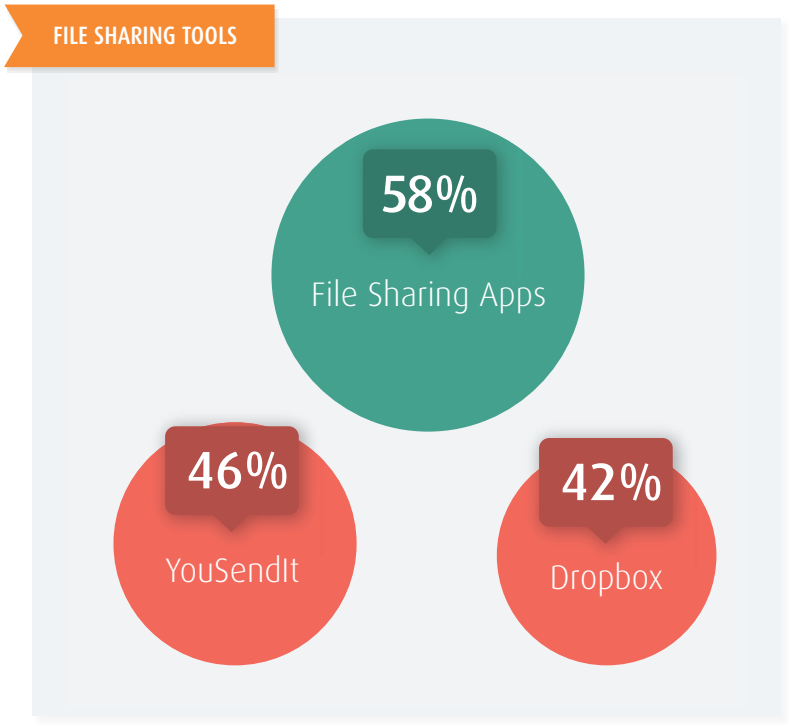
Remote access applications break the traditional ties between employees and corporate-issued PCs and hard drives, providing access to everything from the cloud, including sensitive corporate data. With remote access tools, corporate data journeys beyond the safe confines of an office into the personal domain, blurring the lines between personal and professional, and compromising information security. With Google Drive, as long as the user is logged into Gmail, everything in his or her drive is automatically accessible.

While these tools create significant productivity gains and foster an always-on workforce, they generate more uncontrolled access points susceptible to data leaks or malicious intrusions. This causes headaches for the most well intentioned IT teams. The challenge is how to strike a balance that preserves employee mobility, while adopting policies to safeguard enterprise data.

File Sharing: Don't Let Your Enterprise Become a Data Sieve

Programs like Dropbox and Syncplicity simplify file sharing, especially for documents, presentations and videos that are too large to send via email. File sharing applications are common in 58 percent of organizations and the most popular include Dropbox (42 percent of companies) and YouSendIt (46 percent of organizations), which is now called Hightail.

These programs and applications are easy to use and many incorporate cloud backup and storage capabilities, making them employee favorites. However, they are consumer-grade tools and consequently, prone to widespread account vulnerabilities and outages.

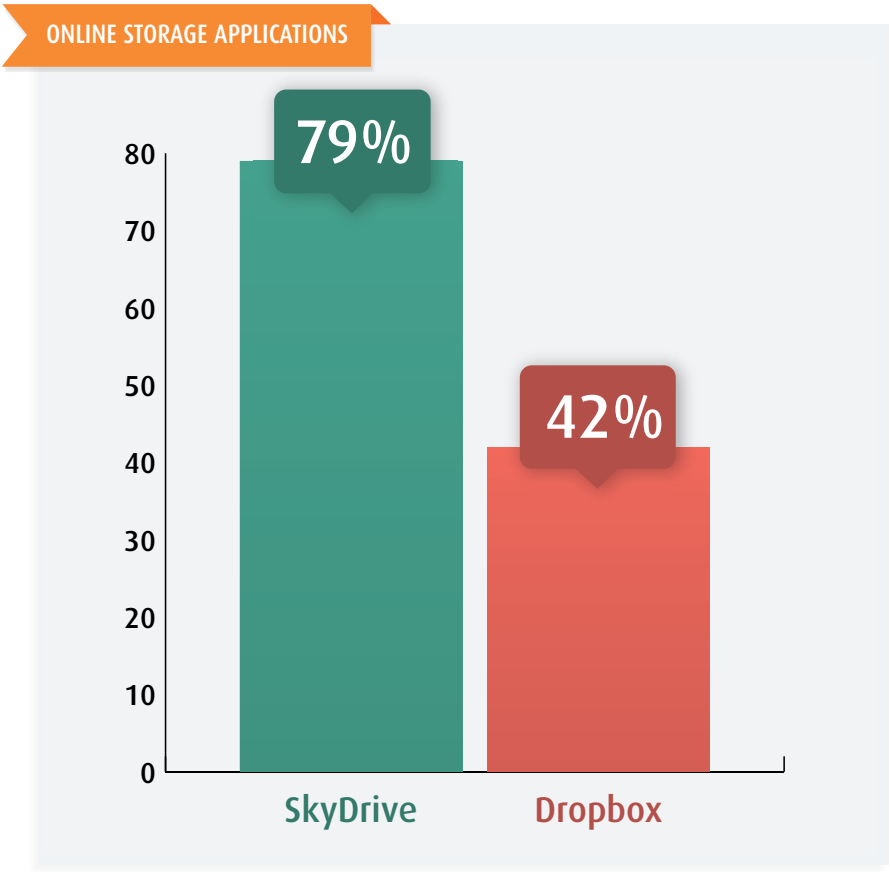


Many IT departments block these programs outright as a result. In the best-case scenario, this authoritarian approach frustrates employees and lowers productivity. At worst, particularly determined employees may find a way to circumvent IT firewalls, exposing the organization to data leaks or attacks. Completely removing consumer-grade file sharing programs is most successful if IT departments offer an alternative, enterprise-grade solution with comparable features and user experience.

Online Storage: Microsoft's Cloud Ambition is No Laughing Matter

Microsoft has been thrown a few curveballs over the last several years, from a lukewarm consumer market reaction to device launches (in particular the Surface tablet and Windows Phone) to slow growth in new user acquisition. Critics have also expressed skepticism in response to CEO Steve Ballmer's public ambition to make Microsoft the largest cloud organization in the world.

Softchoice's data, however, revealed it is too soon to write off Microsoft's cloud capabilities. In fact, the audit found that Microsoft SkyDrive is the most widely used cloud-based storage tool among enterprise users with 79 percent penetration—nearly double that of Dropbox.

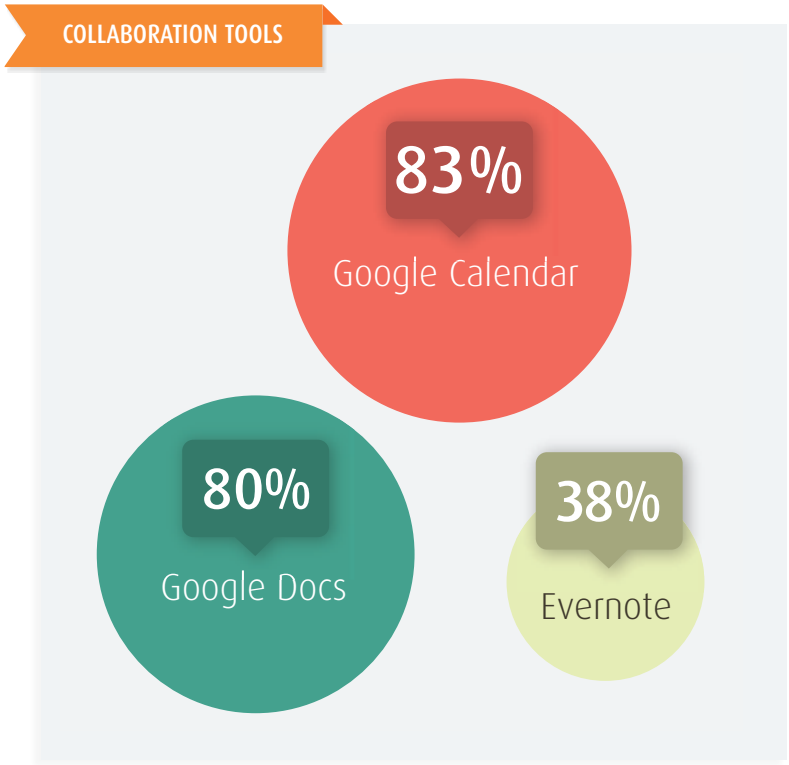


SkyDrive's seamless integration with Office 365, Windows 8, and Hotmail appeals to users but presents a new set of challenges to IT departments. With SkyDrive's tight integration, many users unknowingly transfer and store files in the cloud, posing unintentional risks that IT departments must get ahead of before adoption rates climb higher.

Collaboration: Safeguarding Against Intruders

Collaboration apps such as Evernote and Google Docs have become staples for time management and personal organization improvements. Used in 83 percent of companies, Google Calendar is the most prominent SaaS collaboration application, followed by Google Docs in 80 percent of organizations and Evernote in 38 percent of organizations.

Similar to Google Drive, Google Calendar and Docs create security gaps because the information stored within them is readily accessible as long as the user is logged into Gmail. Along the same lines, Evernote does not default to password protection. Once a user is signed in to an Evernote account, they have full access to any documents or data housed there, making it particularly vulnerable to hackers, as demonstrated by a very public data breach that exposed user data and forced sweeping password resets this past March.



Like file sharing programs, however, user attachment to SaaS collaboration tools makes it difficult to implement an outright ban. Instead, IT organizations must find a way to seal up the end points they expose, or offer on-par alternatives.

Enabling (Not Succumbing to) SaaS

As more SaaS applications enter the corporate space, it is critical that IT departments are aware of everything lurking in and outside of their enterprise environments.

Which SaaS applications are employees using? Are there better, more secure alternatives with comparable features and functionality? Can IT enable productive behavior without compromising security? These are all critical questions IT departments need to address through regular audits to safeguard SaaS applications. IT departments should also consider revising existing policies or drafting new ones that clearly and concisely spell out SaaS guidelines and best practices. This includes providing a "safe list" of SaaS applications approved by the organization with detailed information about why certain applications are beneficial, risky or insecure.

Since new SaaS applications and updates are released frequently, the safe list should remain fluid and updated often, taking into account employee feedback. With a formal process in place, employees can be encouraged to file requests for new applications they want included on the safe list, or evaluated for an alternative. This gives IT more time to vet new SaaS applications before employees begin transferring data. Screening application requests in a timely manner is key to making this process successful, otherwise employees may become impatient and bypass IT by storing corporate information on "rogue" cloud applications.

Third-party providers are another helpful resource for time-strapped IT departments. With specialized experience, third-party providers can conduct routine audits of IT environments to uncover a comprehensive picture of user behavior and SaaS applications. This improves IT decision making and allows IT managers (or third-party providers) to shut down access points during a data breach or deprovision an application when an employee leaves the company, ensuring he or she does not put sensitive corporate data in the hands of competitors. Third-party partners can also help identify and implement highly-secure, enterprise-grade SaaS programs as an alternative to consumer applications like Dropbox and Evernote.

Beyond application audits and security management, business and IT leaders should seek to foster organizational alignment by breaking down silos between IT departments, other lines of business and end users by:

- Enhancing user experience with a consolidated interface and single sign on for all SaaS applications
- Communicating across business units and developing customized usage reports to measure return on investment
- Identifying redundancies across departments and driving standardization to reduce SaaS costs

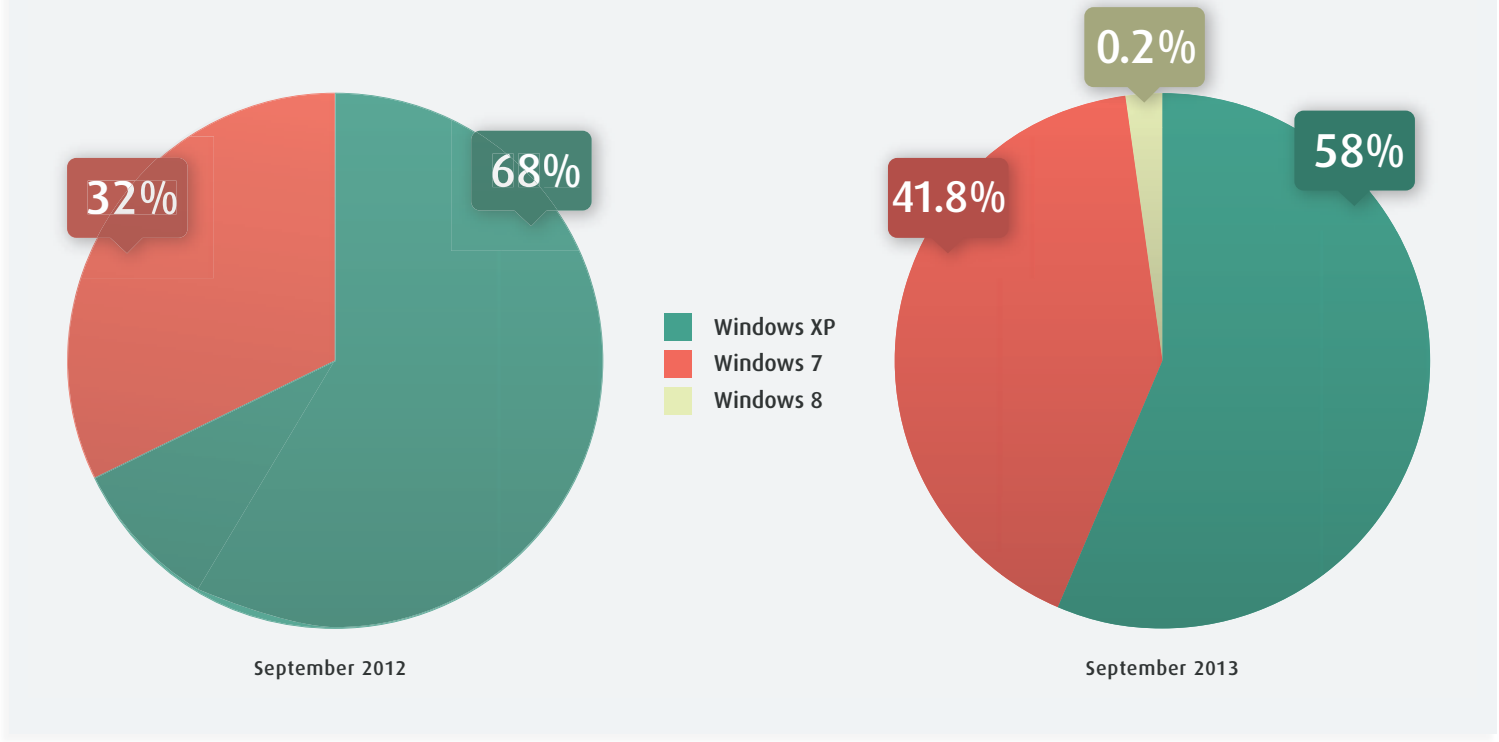
Ultimately, the rise of SaaS applications marks a tipping point for IT's evolution from gatekeeper to service broker. When managed effectively, SaaS applications are powerful drivers for efficiency, productivity and collaboration improvements in the enterprise.

Addendum

Softchoice's research into cloud environments also recorded the prevalence of the different Windows operating systems in the enterprise. With Windows XP end of life approaching in the spring of 2014, the company wanted to see if firms were making progress in migrating to newer operating systems. Often, overhauling an enterprise operating system is accompanied by upgrades to hardware and the software that comes with it. Uncovering where an organization stands with their OS migration plans typically indicates if and when certain SaaS applications will become more predominant in the environment.

In September 2012, Softchoice had found Windows XP made up 68 percent of operating systems across half a million PC devices, and Windows 7 had a 32-percent share. In its most recent evaluation, conducted at the same time as the research for this report, Softchoice found that little progress has been made in migrating operating systems. Windows XP still makes up 58 percent of the enterprise environment. Windows 7 now represents 41.8 percent and Windows 8 has a 0.2-percent share.

WINDOWS OS IN THE ENTERPRISE



Companies need to make concerted efforts to migrate away from Windows XP before the operating system no longer receives vendor support and security patches. Without regular "Patch Tuesday" security updates, cyber-criminals will have an infinite timeline to uncover and exploit vulnerabilities.

At the same time, with a small slice of the enterprise market giving Windows 8 a test drive, companies should start preparing for a new breed of applications (namely SkyDrive and Office 365) to flood the workplace. The more familiar IT departments become with the functionality and security measures behind these apps now, the better prepared they'll be in the event of an office-wide migration.

CONTACT US

To learn more about how Softchoice makes it easier to source, implement and manage the right cloud solutions for your organization, visit us at **softchoicecloud.com.**