EXECUTIVE BRIEF

The Cloud Application Explosion

An Osterman Research Executive Brief

Published April 2013

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

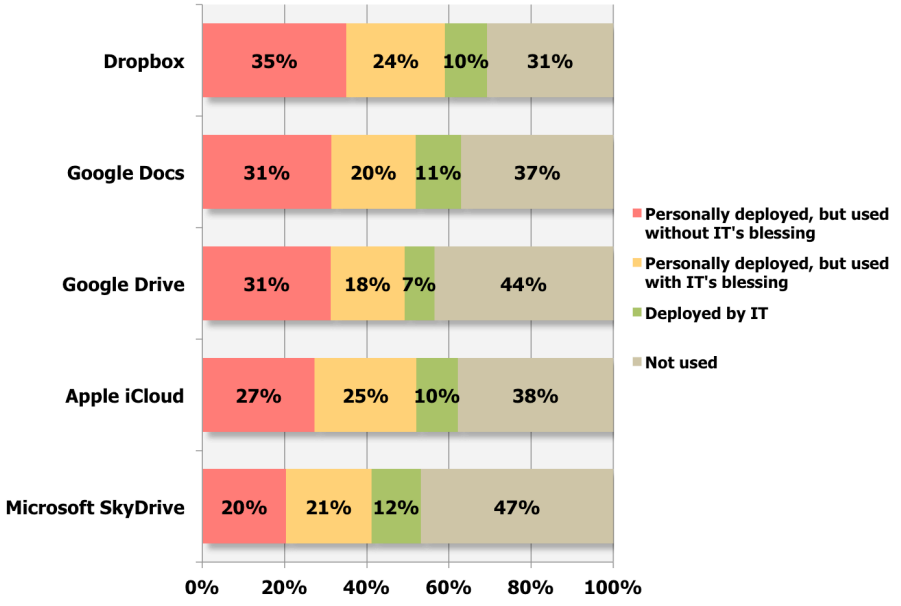
THE CLOUD APPLICATION EXPLOSION: A PROBLEM YOU NEED TO ADDRESS

There are a large and growing number of cloud-based applications being deployed in organizations of all sizes to provide a variety of capabilities, including email, real-time communications, social media, file sharing, file storage, telephony and other services. Among the more popular of these applications are Twitter, Facebook, LinkedIn, Google Plus, Hotmail, Yahoo! Mail, Google Mail, YouSendIt, Dropbox, Box and Microsoft SkyDrive, although there are literally thousands of cloud-based applications in use worldwide. Some of these applications have been approved and/or deployed by in-house IT departments, although most have been deployed by individual users without the authorization – or often the knowledge – of the IT department.

For example, Dropbox is currently used in 68% of organizations, but only 45% of these deployments have the blessing of the IT department. Similarly, Apple iCloud is used in 65% of organizations, but only 57% of these deployments have IT's blessing; while SkyDrive is used in 44% of organizations with only 56% having IT's blessing.

Osterman Research has found that small organizations have the highest penetration of cloud-based applications in use, although these applications are commonly found in even the largest enterprises.

Leading Cloud-Based Applications in Use



WHY CLOUD-BASED APPS?

It is important to note that the vast majority of employees who deploy cloud-based applications do so to solve specific business problems that they cannot easily solve in other ways, such as gaps in the capabilities provided by their internal IT departments. For example, many users will often deploy a file-storage application in order to more easily share content with others inside and outside their organization, or to have all of their critical business files available when traveling or when working from home. Similarly, users will often employ a file-sharing application to overcome file-size limitations in their corporate email system.

Some…applications have been approved and/or deployed by in-house IT departments, although most have been deployed by individual users without the authorization – or often the knowledge – of the IT department.

Fundamentally, cloud-based applications have been deployed by employees with the best of intentions and often as a result of IT's inability to deploy important features and functions that users need in order to remain productive.

THE RISK IS SIGNIFICANT

Although cloud-based applications are most often deployed to enhance users' productivity and to improve business processes, they carry with them a number of serious risks. For example:

- Cloud-based applications typically store large amounts of corporate data – much of it of a sensitive or confidential nature – in data repositories that are outside the control of the organization that owns this data.
- When data is stored in the cloud, it is often not accessible to the organization at large. This creates significant problems when an organization must have access to this information during a regulatory audit, for eDiscovery purposes, or when senior managers otherwise must gain access to it.
- Most of the time, organizations do not control access to these applications or the data they contain, nor do they control the methods of access to them. Moreover, employees typically control access to data stored in the cloud, not the organization itself, creating significant problems if any employee leaves the organization or forgets that data is stored in a particular cloud repository.
- A related problem is that access methods are typically weak, normally requiring only a user-defined username and password for access. For sensitive or confidential information, this form of authentication is unsatisfactorily weak.
- Corporate policies are often ignored or followed incompletely when data is stored in cloud-based applications. This includes policies focused on encrypting sensitive data, establishing expiration periods for files, or determining permissions on certain types of data.
- While many cloud-based providers offer robust security for their customers' data, there have been some well-publicized breaches that have permitted access to customer data by unauthorized parties. For all intents and purposes, organizations are subject to whatever security standards – or lack thereof – maintained by cloud providers.
- IT and other decision makers have little or no visibility into data that resides in cloud-based data stores.
- Because many cloud-based providers do not run malware scanning on their customers' content, cloud-based applications present another means of ingress for malware into corporate networks. For example, a user who accesses his or her Dropbox account from home using a PC whose anti-virus signatures are out of date may inadvertently infect a file, load it back into Dropbox, and then infect the corporate network when accessing the file from his or her work PC.

IMPORTANT QUESTIONS TO ASK

Business and IT decision makers should ask – and properly answer – some critical questions about the use of cloud-based applications in their organizations in order to maintain robust access control and to protect sensitive and confidential data assets:

- **Do you know what applications are in use across your organization?** Many decision makers do not have good visibility into how many users employ personally deployed and managed applications, what these applications are, what data they contain, etc.

Cloud-based applications typically store large amounts of corporate data – much of it of a sensitive or confidential nature – in data repositories that are outside the control of the organization that owns this data.

- **Can access to these cloud-based applications be managed through your current access and identity management infrastructure?**
  If so, are they being managed this way today? If not, will cloud-based applications require an entirely new set of tools?

- **Do you know the risks you face?**
  This includes not only the risks of losing access to important corporate data, but also the risks associated with data breaches and their remediation, violation of federal data protection statutes, increased risks of data spoliation during legal proceedings, etc.

- **Have you quantified these risks?**
  This is an important step in the process of understanding risks, since a single data breach or an inability to satisfy an eDiscovery order can cost hundreds of thousands or millions of dollars.

- **Have you established a plan for managing access to cloud-based applications?**
  In short, have you answered all of the questions above to the satisfaction of your senior IT management, senior business decision makers, internal legal counsel and other key stakeholders and then created a plan to address the risks and costs you face from unmanaged use of cloud-based applications?

RECOMMENDATIONS

Osterman Research offers the following recommendations to organizations that must address the growing use of cloud-based applications in their organizations:

- Understand how and why cloud-based applications are being used in your organization in the context of what they offer that IT does not provide and other reasons that users employ them.

- Refrain from the temptation to impose draconian controls prohibiting the use of these applications. These controls are unlikely to be effective anyway, and imposing them will simply discourage employees and make their work more difficult.

- Implement detailed and thorough policies focused on how cloud-based applications are to be used, the controls that IT should have over them, and how employees should use them.

- Educate users about best practices when using cloud-based applications. This might include not storing highly sensitive data in non-secure repositories, not using personal Webmail during email outages to send data that must be archived or encrypted, or optimal methods for sending very large files that cannot be sent through email.

- Finally, deploy robust access management technologies that will enable IT to control access to cloud-based applications and the data sent through and stored in them.

Implement detailed and thorough policies focused on how cloud-based applications are to be used, the controls that IT should have over them, and how employees should use them.

ABOUT McAFEE SOLUTIONS

Integrated Web and Identity solutions from McAfee provide improved security at every phase of the web experience. Organizations can easily manage cloud application access through a user-friendly single-sign-on portal. Strong authentication through one-time-passwords ensures added security for select or all applications.

Granular control of data exiting the organization through cloud applications using DLP rules along with granular application control ensures consistent policy enforcement across the broad and growing spectrum of cloud applications and providers. Detailed logging and reporting enables visibility of application use and helps demonstrate compliance, regardless of device used or location of the user.

For protection against advanced malware and other hidden threats in returned traffic, McAfee layers numerous threat technologies to provide the most in-depth web security available. From opening content and scanning active elements in real-time to comprehensive signature-based coverage and web reputation, McAfee's layered approach optimizes several technologies for the best combination of security and performance.

Whether looking for the control of an onsite solution, the ease of Security-as-a-Service (SaaS) management or a hybrid combination of the two, McAfee empowers organizations to deploy web access and security the way that best fits current and future needs. McAfee offers true deployment flexibility without forcing organizations to backhaul web traffic to a central location. Shared policy across Web Protection deployments enables the same security profile to be enforced no matter what device is used or the location of that user or device.