# SECURING MICROSOFT OFFICE 365

WHITE PAPER

bitglass

Do a search for trending IT topics today, and it's hard to find one that's more discussed—or more controversial—than cloud services. IT departments love that they can outsource the daily software management grind. Business leaders love the cost savings. And information workers—already accustomed to using online email and mobile apps in their personal lives—see no reason why they shouldn't have the same flexible tools at work.

Everyone, however, has concerns about privacy and security.

According to a 2014 Bitglass survey of 81,253 wide-ranging businesses, about 24 percent of organizations today are embracing online email and productivity suites, such as Microsoft Office 365 and Google Apps. As we discussed in our cloud adoption report, security concerns persist in holding back adoption rates.

But a survey released by Microsoft in March offers an interesting twist on those numbers: While the 24 percent number holds true for "official" cloud users, many IT leaders "simply don't know who is adopting cloud in their organizations."

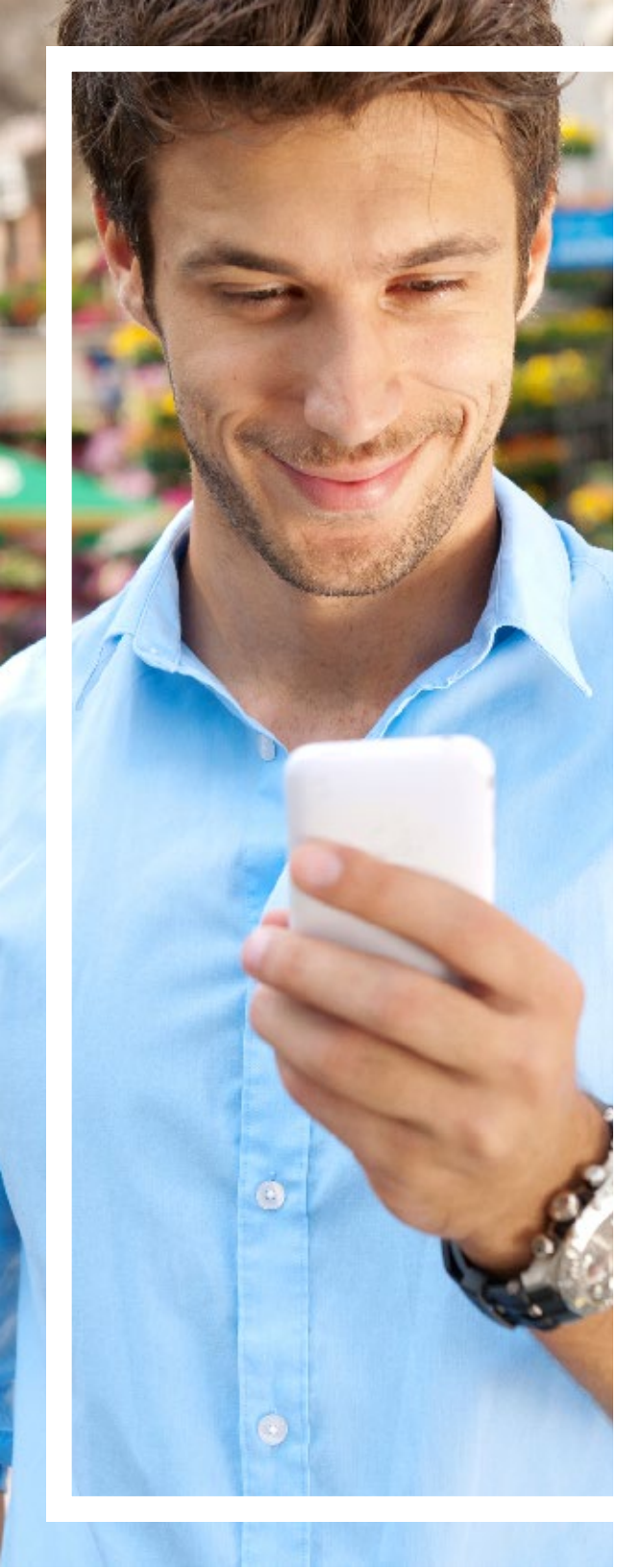
Indeed, some cloud companies actually count on this renegade approach to the corporate world. In May, the CEO of Box told *Wired*, speaking of his company's idea of collaboration: "What we now have is a digital space that has no connection with the corporate hierarchy, that is actually the way that work gets done."

That attitude is entirely understandable, given the enormous flexibility and cost efficiencies in the cloud—but it also brings to mind the proverbial ostrich putting its head in the sand. The risk inherent in cloud investments is huge, and passively relinquishing control over the ways that company employees collaborate and share information seems foolhardy, at best.

**44%**
**OF EXECUTIVES**
admit that there are a lot of off-budget purchases or implementations of cloud taking place within their enterprises.

**ONE IN FIVE**
indicates that there is even a 'significant' amount of shadow IT spending on cloud resources taking place under their noses.

**— *Forbes***, March 20, 2014,



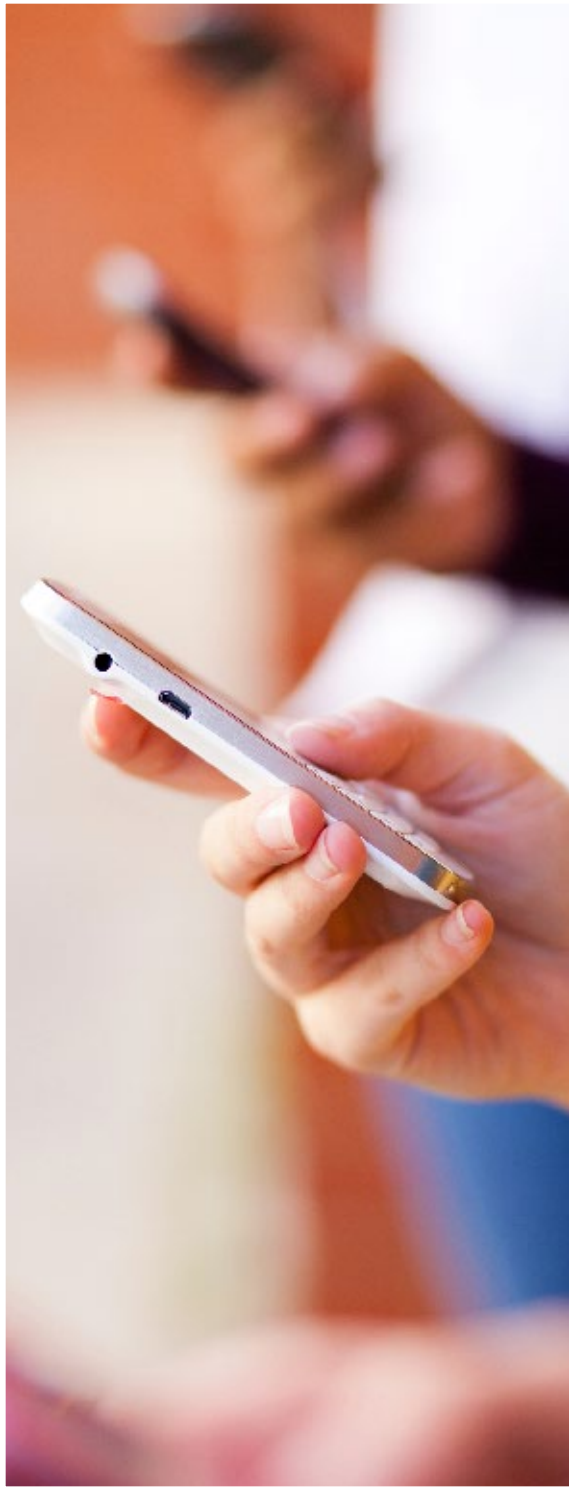


# Microsoft to the Rescue?

As much as Silicon Valley startup execs love to portray Microsoft as a dinosaur, the very fact that so many enterprises are slow to strategically embrace the cloud indicates that they are holding onto the familiar tools and broad functionality that the Office productivity suite offers. As IT organizations start to face up to employees' subterranean embrace of the cloud, Office 365 offers a promising compromise: Bring cloud-based productivity tools under the company's security umbrella so that people can work the way they want to, without sending sensitive company data astray.

The idea that you can simply shift responsibility for your company's data security to Microsoft, however, couldn't be further from the truth. The Office 365 team includes highly trained security experts who excel at protecting their infrastructure—they're all over SSL, data redundancy, and backup systems. But the Microsoft team has no control over your devices. They can't tell you who is accessing your data or when. And they have no idea what happens when your data leaves their servers.

You can achieve Office 365 data security... but only through a partnership that involves, at its core, a comprehensive in-house security plan, together with Office 365's built-in security functionality. Before you can rest easy about company data in the Office 365 cloud, you must address these key problem areas:

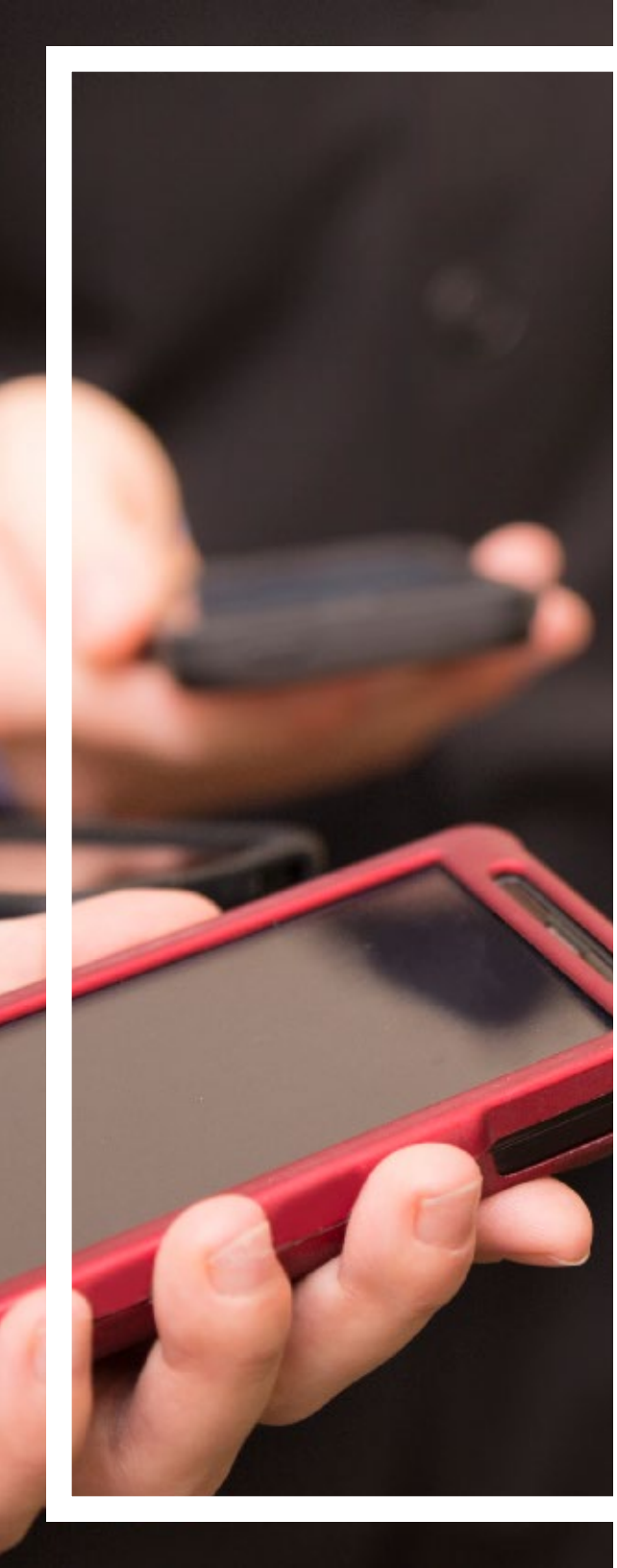


# **ONE:** Identity Sprawl

Hastily put-together cloud app deployments often don't integrate with corporate identity systems such as Microsoft Active Directory. Users end up with too many passwords and accounts to keep up with—a situation that causes endless frustration, productivity loss, and help-desk calls. Employees with too many passwords are also more likely to reuse them or write them down on sticky notes, adding to the likelihood of compromised passwords.

## **THE SOLUTION:** SINGLE SIGN-ON (SSO)

Deploy an SSO system so that employees have just one password to remember and manage. SSO allows you to manage every account through Microsoft Active Directory, so that if you deactivate an account there, the user is automatically locked out of all company systems. No more worrying about what information employees may have squirreled away in their cloud apps after they've left the company.



# **TWO:** Suspicious Activity

Office 365 doesn't offer any audit logging or visibility into user activity within applications. Microsoft can't tell you that "Dave" logged into Office 365 from New York at 1:30, and then someone purporting also to be "Dave" logged into your Salesforce.com account from San Francisco at 1:34. But it happens, and you need to know about it.

If you're in financial services, healthcare, or any other regulated industry, visibility into employee activity takes on additional urgency, allowing you to operate in compliance with regulations and to survive audits.

## **THE SOLUTION:** A CLOUD ACCESS SECURITY BROKER

Complete visibility into corporate activity across all company cloud apps may be more easily achievable than you think. When you implement a cloud access security broker, all data from your cloud apps, including Office 365, flows through the proxy and is recorded for you. To make sure high-risk activities don't get lost in the noise, invest in one that offers alerts and gives you information in plain English, rather than offering an audit log of unreadable transactions.



# **THREE:** Data Leakage

You read the news, so you know the risks and consequences of losing control of sensitive data. But if your CEO carries around next quarter's financial projections on his iPhone, you certainly can't blame Microsoft when that information accidently makes its way onto a reporter's desk. While you can easily prevent such behavior with on-premises software, a move to the cloud complicates matters considerably.

To prevent data leaks, we recommend a three-pronged approach:

## SOLUTION #1:
### CONTROL WHO CAN ACCESS DATA

This is where your company's security policies come into play. Decide who can do what inside of Office 365, and then set up rules that automatically enforce those policies. Ideally, you want to be able to control access according to the app, group, device type, and geographic location.

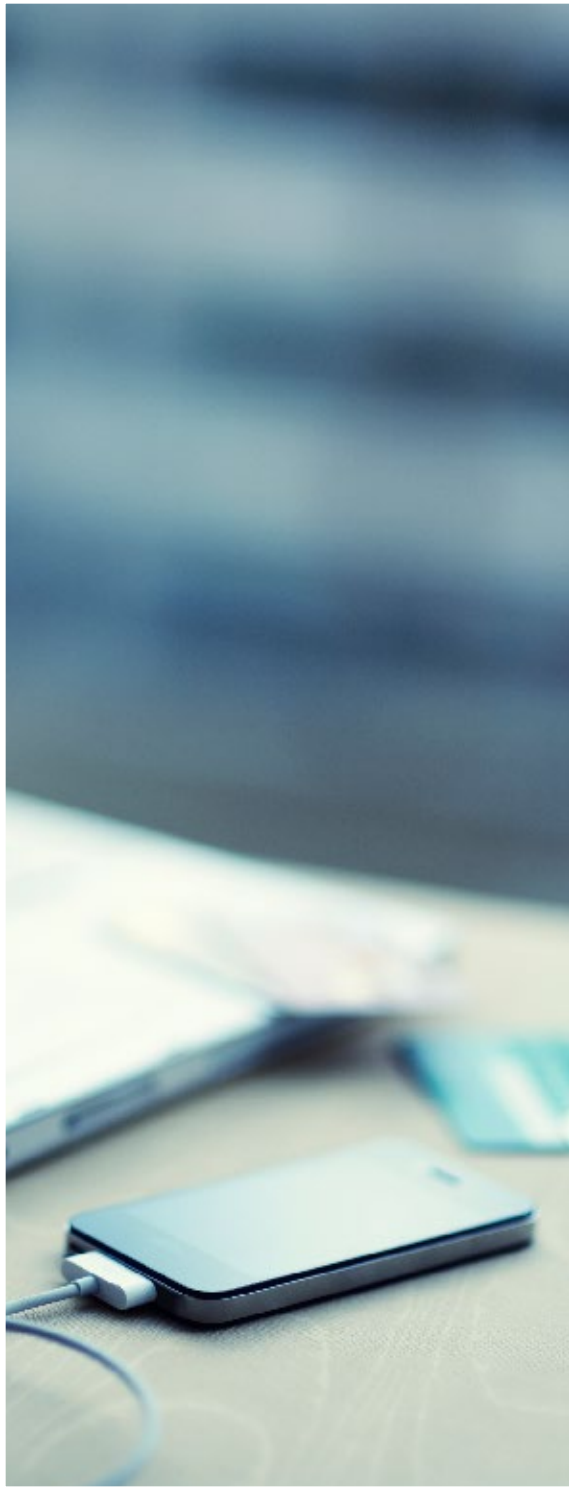
## SOLUTION #2:
### LOCK UP IMPORTANT DATA

All data is not created equal. Marketing materials, for example, are meant to be shared. Credit card numbers and company secrets must be kept secure at all times. Much corporate data falls somewhere between those two extremes, along a spectrum where varying levels of security are appropriate.

Spend some time thinking about the kinds of data you deal with, and deploy a solution that automatically removes highly sensitive information from emails and attachments before they can be downloaded from Office 365.

## SOLUTION #3:
### TRACK IMPORTANT DATA

Just as it's possible to track paper money through the use of watermarks, it's now possible to digitally watermark corporate data and track it wherever it goes. Put hidden identifiers on each piece of data in that "highly sensitive" category, and every time it's downloaded, you'll know who accessed it, and when they did so.



# **FOUR:** Lost Mobile Devices

Mobility is a fact of life in the modern world and, like it or not, your employees must be able to download corporate data to their devices in order to remain productive. Office 365 is available from nearly anywhere, which means that just about any device, whether it's company-managed or not, can access your data. Mobile device management (MDM) systems work only when you know about the device, and many employees object to the privacy implications of MDM solutions.

## **SOLUTION:** CLIENTLESS SELECTIVE WIPE

Today, you can protect your data without installing software on individual devices or invading employee privacy. When a device gets lost or stolen, or when an employee leaves the company, you can wipe company data from the devices in question, whether or not your IT department ever set eyes on them.

# You Can't Outsource All of Security

A move to Office 365 can help you gain control over company data and online employee activity, but only if you go into it prepared to rethink IT security, to take advantage of the innovative technologies available now. Today, you can build a virtual firewall around your data instead of trying maintain a secure perimeter around apps and devices you no longer control or manage.

Just remember that any security solution you put into place must be virtually invisible to users. You don't want employees going rogue and working around IT because security is inhibiting their workflow. You also have to make sure the whole thing pencils out financially. If the cost of security wipes out the economic gains of moving data to the cloud, you're back at step one, aren't you?

Learn more about how security technology has advanced to match innovations in the cloud at www.bitglass.com.

Want to hear what the analysts are saying about Bitglass and CASBs? Reach out to Neil MacDonald or Peter Firstbrook at Gartner.

bitglass

## About Bitglass

In a world of cloud applications and mobile devices, IT must secure corporate data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are simply not suited to solving this task, since they were developed to secure the corporate network perimeter. The Bitglass Cloud Access Security Broker solution transcends the network perimeter to deliver total data protection for the enterprise—in the cloud, on mobile devices and anywhere on the Internet.

For more information, visit
**www.bitglass.com**

Phone: (408) 337-0190 | Email: info@bitglass.com