File sync & share apps in the age of BYOA:

Regaining control over corporate data

Part of the IT Management Research Series

LogMeIn

File sync & share apps in the age of BYOA:
Regaining control over corporate data

The rise of devices, data and apps represent a fundamental shift in consumer behavior that is fueling the “Consumerization” of IT. Consumers are now independent, universally-connected users of technology who no longer feel the need to ask permission to introduce new technologies into business environments. We first saw evidence of this with the sweeping trend of BYOD or “Bring Your Own Device.” Employees brought their personal smartphones or tablets into work for business use and IT had to adapt their infrastructure to accommodate this trend.

We are now seeing another wave of challenges for IT professionals in the form of BYOA or “Bring Your Own Application” This trend is particularly pronounced when it comes to file sync and share apps. Non-IT employees are now driving the introduction and adoption of file sync and share applications like Dropbox, often leaving IT out of the equation altogether. While these employee-introduced apps can have positive effects on organizations, there are many security risks that can arise. This is especially true as employees store personal and business files in one file sync and share applications.

It is essential for IT professionals who want to regain control over corporate data to understand how BYOA is changing the game. In this spirit, LogMeIn set out to understand how the trend is manifesting itself in the file sync and share space. This report, which is part of an overall series of IT Management Research Reports from LogMeIn, focuses on the growing trend of employees bringing their own file sync and share solutions into the workplace. It gives guidance on how IT professionals should address this new trend, and most importantly, how they can reclaim their strategic role managing their organization’s data.

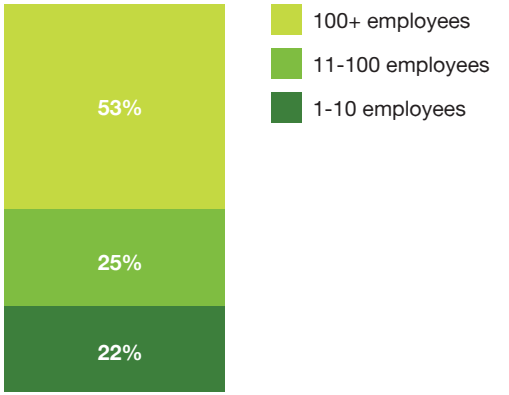
Methodology

This survey is part of a series of major research studies conducted by LogMeIn that focus on the state of IT management in today's world of independent, "BYO" consumers. The series focus on three key areas: managing applications, managing devices and managing data.

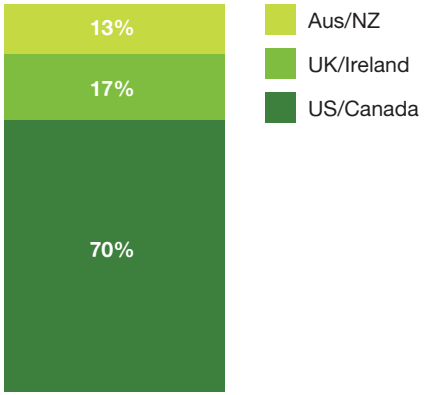
In this report, we explore the data side of BYOA and dig into usage and adoption of employee-introduced file sync and share applications within companies worldwide and how this has led to a loss of control for IT managers. We partnered with Edge Strategies to survey IT and non-IT professionals across the world in various-sized organizations.

Field Dates: November–December of 2013
Method: Online Survey
Segment Profile: Internal IT and Non-IT across the globe (863 total respondents)
Total Survey Base: 1,390, IIT, OIT and Non-IT respondents in six countries: US, Canada, UK, Ireland, Australia and New Zealand

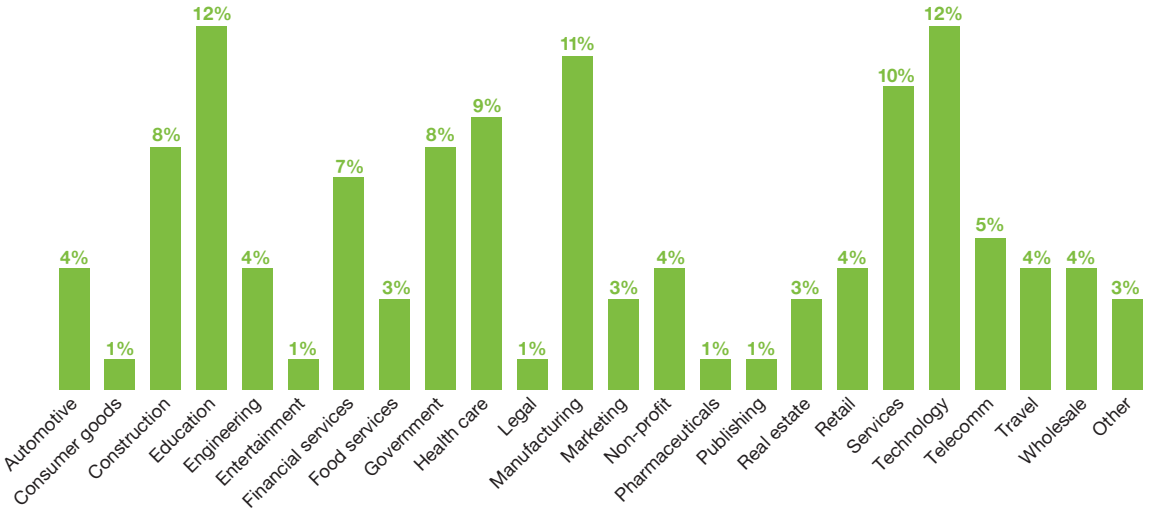
Client Size



Region



Industry



Summary

BYOA is here to stay.

70% of organizations have some presence of BYOA and it's a trend that is only going to increase.

File sync & share apps are particularly prone to BYOA.

File sync and share apps are introduced by employees 61% of the time—second only to social apps in terms of how often they're introduced by employees.

IT is out of the loop.

67% of IT professional believe less than 50% of their employees use file sync and share apps. This is in stark contrast to the 73% of non-IT respondents claiming to use file sync and share applications across their organizations.

Security risks are inconsistently managed—if at all.

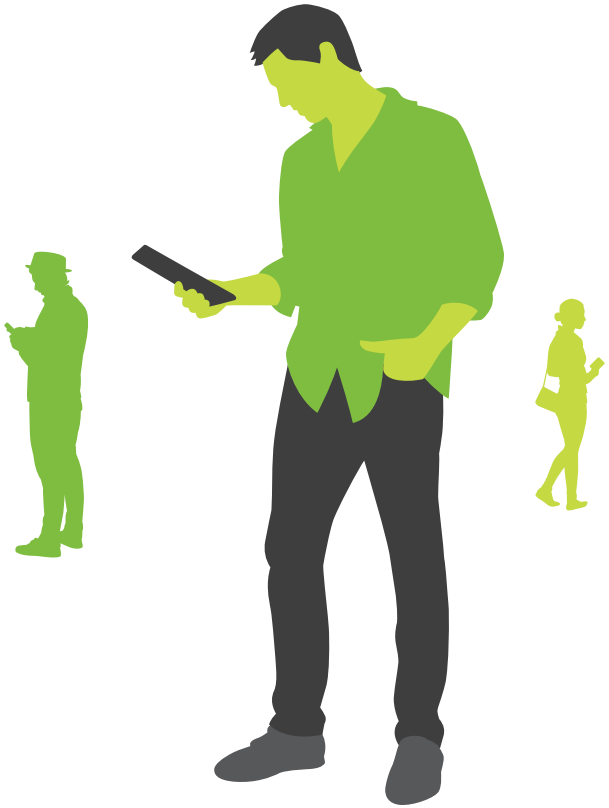
IT professionals acknowledge that BYOA poses huge security risks, and takes some of the control for technology out of their hands, but many are not actively working to address the problem; less than 1/3 of the file sync and share apps adopted by IT are centrally managed by IT.

Active employee engagement can help.

There are many positive things that can come from file sync and share applications if they are properly managed. Employees are looking for more user-friendly, mobile-friendly apps that make collaboration easy.

IT has the ability to choose its role.

IT professionals can decide what role they want to play. They can act as gatekeepers and restrict app adoption, act as passive observers and let the adoption happen without their involvement—or IT can act as strategic facilitators, managing and shaping the adoption and direction of the growing BYOA trend.




The realities
of BYOA

IT severely underestimates the impact of BYOA.

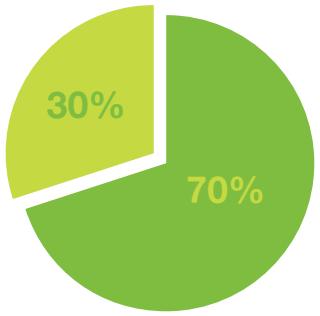
7X more apps coming into the workplace than IT estimates.

When asked about the presence of apps that were brought into their organization by users, 70% of IT professionals indicated there was a least one example of BYOA. But because IT is not always aware of BYOA, the number of organizations with some presence of employee-introduced apps is likely even higher—meaning it's basically everywhere now.

This trend is particularly pronounced in SMBs (11-100 employees)—81% said they have a BYOA presence. And it's not just an issue for the U.S. as organizations worldwide have indicated they're experiencing this trend too, with over 60% of organizations in UK/ Ireland and over 70% in Australia/New Zealand having some presence of BYOA.

One area we're seeing a huge hole is IT's lack of awareness to the sheer volume of apps being brought in. IT professionals in this study indicated that on average they estimate 2.8 apps per organization are brought in by employees. However, based on data LogMeIn has collected through app discovery with customers, this number is far closer to 21 apps—a staggering 7X more.

There is an enormous disconnect around the scale of BYOA



Percentage of organizations with presence of BYOA

Percentage of organizations without presence of BYOA

Average # of apps IT estimates to be brought in by end users

Actual # of apps non-IT users bring into organizations[1]

takeaway:

If you don't believe BYOA is happening at your organization, than you're either tragically unaware of what's really going on, or you're part of the very rare organization that's in the minority.

Base = IIT only, all applications
LogMeIn App Discovery usage data[1]

LogMeIn

It’s become a bit of the ‘wild west’ with regards to everyone using a different application, and application provider.

— IT manager, Construction, 501-1000 employees

Why IT needs to pay attention now.

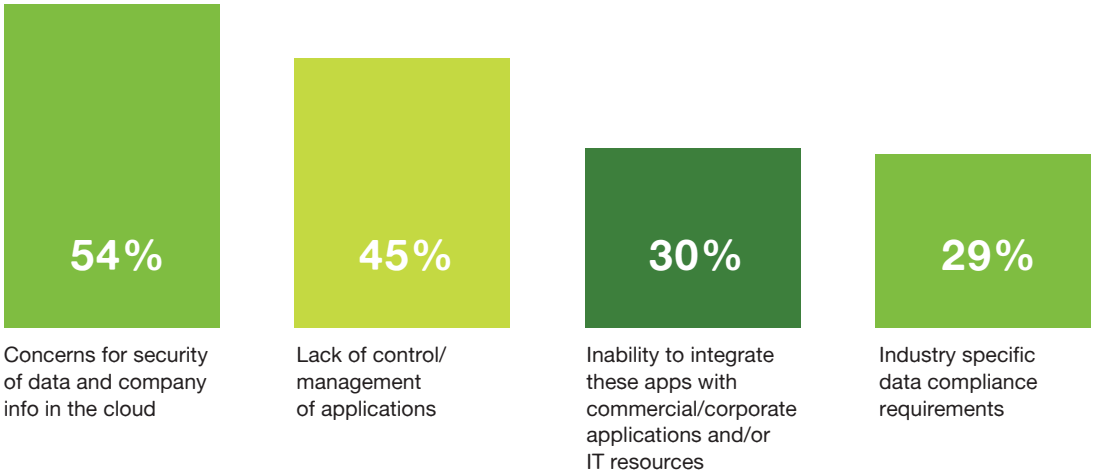
BYOA can pose huge security threats if not properly managed.

So why does it even matter if BYOA is so widespread? Because most IT professionals know that bringing apps into the workplace without consulting IT exponentially increases your security risks.

When asked which issues limit their company's adoption or support of BYOA, more than half (54%) point to concerns around data security, and 45% cite a lack of control/management of apps.

When IT loses management control of apps, they can no longer monitor which apps pose security threats, or appropriately integrate new apps with existing ones. Some IT professionals also point to data compliance requirements as a potential issue that can arise when BYOA goes unchecked.

Top issues limiting adoption and support of BYOA



takeaway:

IT pros who know about employee-introduced apps but don't take steps to manage them may face huge security and other threats that could ultimately damage their organization.

Which of the following (if any) limit your company's adoption of – or support for – employee-introduced applications?
Base = IIT only, all applications

Things are only going to get worse.

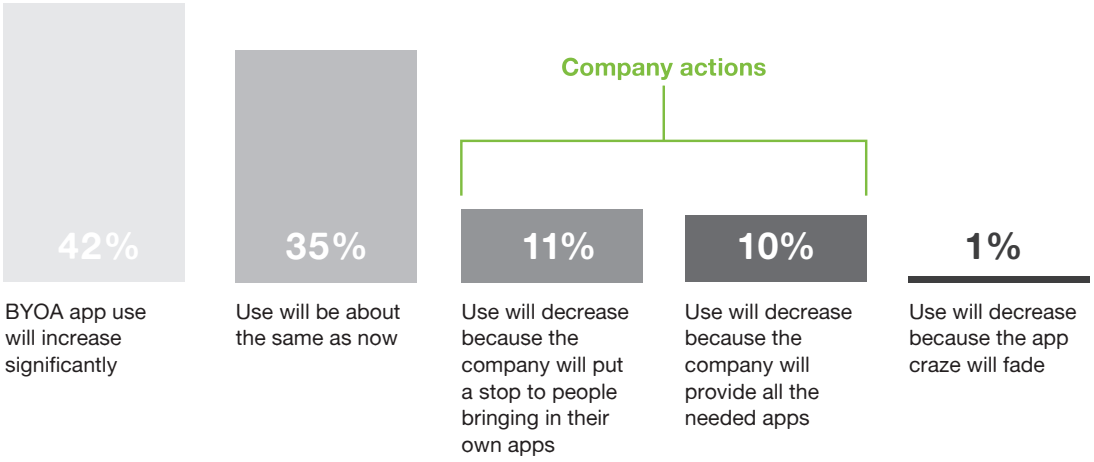
Over 40% say BYOA will significantly increase.

If we knew for sure that BYOA was going to wind down a year from now, it wouldn't be much cause for concern. But the fact is, IT professionals see this as a trend that will, at the bare minimum, stay the same (35%), but more likely significantly increase (42%).

On the flip side, those who feel the trend will go away only think that will happen based on a company's actions. 21% see BYOA decreasing because a company puts a stop to outside apps or provides all the apps needed. Just a small fraction (1%) see a decrease coming because the app craze fades away.

In short, no one sees anything stopping users from bringing in the apps they want to use other than companies taking major actions.

Changes in BYOA trend over next 5 years



takeaway:

Ignoring BYOA will not make it go away. IT pros need to make the shift now to the tools and processes that help manage this new way of doing business.

How do you believe that employee use of BYO apps will change over the next five years?
Base = IIT only, all applications

The trends for file sync & share apps

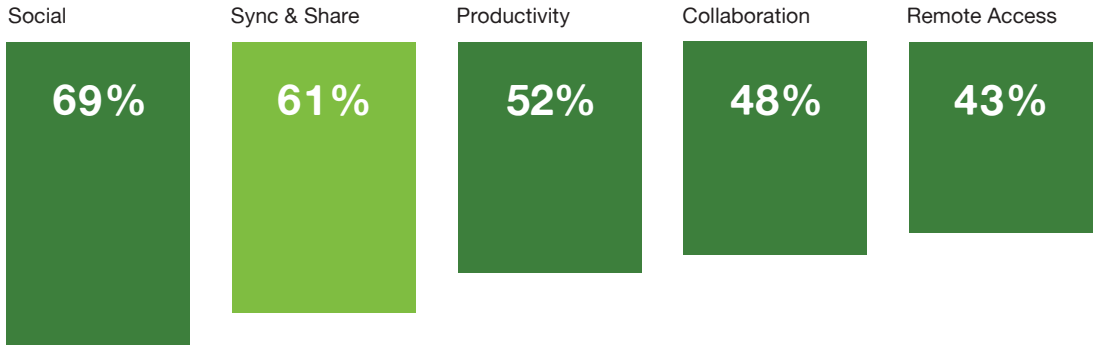
The “Dropbox” problem is spreading.

File sync & share apps lead the pack in employee-introduced apps.

This study found that for all of the major types of applications being used by employees, a high percentage were originally employee-introduced. This is particularly true for file sync and share apps which are introduced by employees 61% of the time.

We’ve all heard horror stories related to Dropbox usage in the workplace, but what’s most troubling is that the influx of sync and share apps isn’t shrinking. And with many employees using Dropbox for personal reasons on company-owned devices, the security risks are even greater.

Percentage of times applications were brought in by employees



takeaway:

IT can’t afford to sit idly by, and needs to pay serious attention to employee-introduced sync and share apps.

How were each of these applications brought into your company?
Base = IIT only Companies with employees using BYO application; DK answers excluded

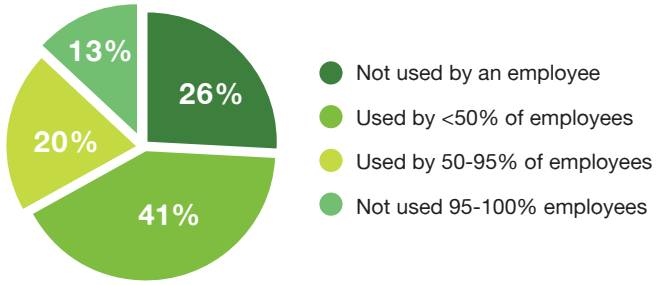
IT is in the dark about file sync & share apps.

67% think less than half of their employees use them—and they're wrong.

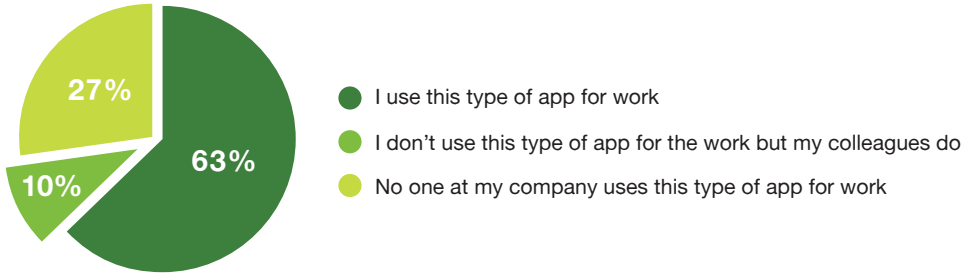
When asked about the presence of file sync and share apps that were used within their organization a staggering 67% of IT professionals indicated there is no use or that less than half their employees are using these apps.

In contrast, non-IT respondents surveyed indicated that a large majority (73%) are using file sync and share apps across their organization. That underscored the idea that IT professionals are out of touch with how their employees are sharing and storing company data.

IT view on file sync & share



Employee view on file sync & share



To the best of your knowledge, how many cloud sync & share applications are used by employees in your company?
Base = IIT only File Sync & Share Apps

takeaway:

The reality is employees are using file sync and share far more often than IT suspects. This can pose serious data leakage and security threats, and put organizations at risk if not addressed.

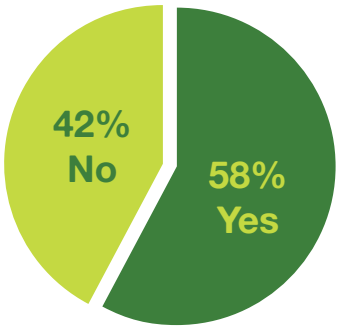
Drivers of file sync & share app adoption

IT admits to not being consulted on file sync & share.

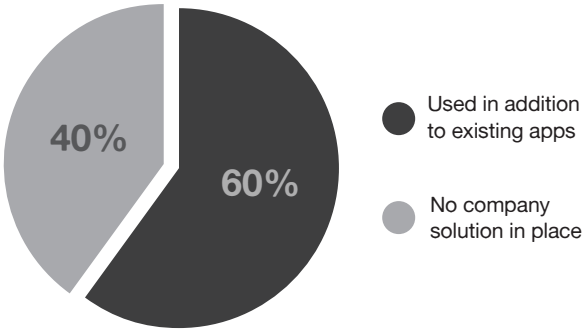
Most of the time employee-introduced apps duplicate existing solutions.

IT professionals concede that they're being consulted just over half the time (58%) when employees are bringing in file sync and share apps. This leaves IT out of some very important conversations about how corporate data will be managed.

On top of this, these apps are most often (60%) being brought in to be used in addition to existing applications that IT had already put in place.



Did the employees consult the IT department before deciding to use cloud storage/file sync & share apps in the workplace?



Are the BYOA apps filling a gap or being used in addition to existing tech/apps?

takeaway:

Today's empowered employees are bringing in their own sync and share apps, duplicating existing solutions and are not consulting IT whatsoever. IT needs to reign in their employees to prevent data loss and other security threats.

How were each of these applications brought into your company?
Base = IIT and Non-IT respondents, organizations with sync & share apps

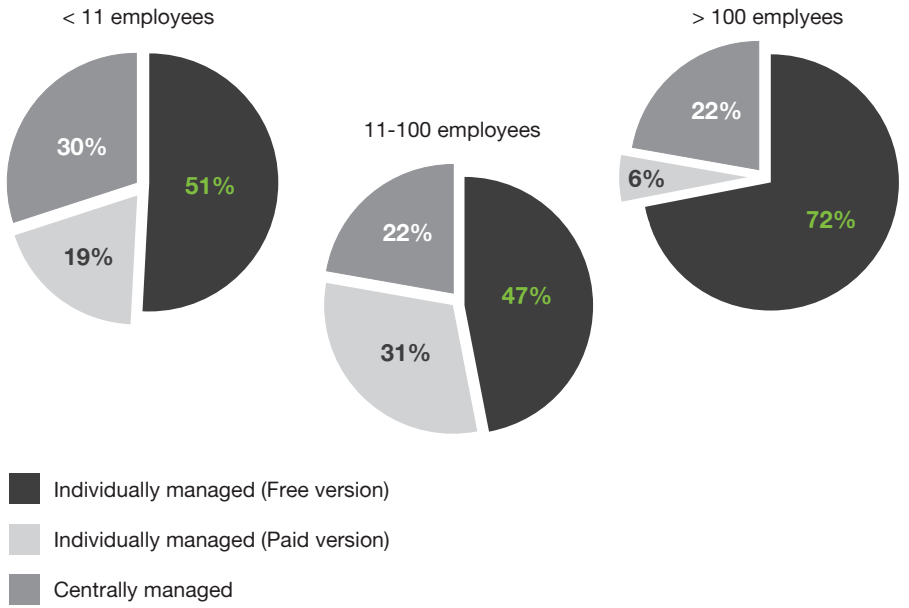
Even after adoption, IT isn't fully in control.

Less than 1/3 of file sync & share apps are being centrally managed.

Even after IT pros endorse employee-introduced sync and share apps, they're not always in complete control after they've been adopted. As shown here, only a very small percentage of apps brought into organizations become centrally managed. Across organizations of all sizes, less than 1/3 of file sync and share apps are centrally managed, with the rest being managed by individual employees, often as part of a free account.

At larger organizations, a vast majority are using free versions and putting corporate data at risk. For companies 11-100, nearly half are using free versions, and only 22% are being centrally managed by IT.

So what does this mean? Major management problems for IT. While free versions alleviate some of the cost, the flood of individual versions (both free and paid) prevent IT from managing these apps. That makes the previously mentioned "Dropbox problem" that much more problematic, and the potential for security risks to grow by leaps and bounds.



takeaway:

Individually managed free and paid apps can be great for employees but a nightmare for IT.

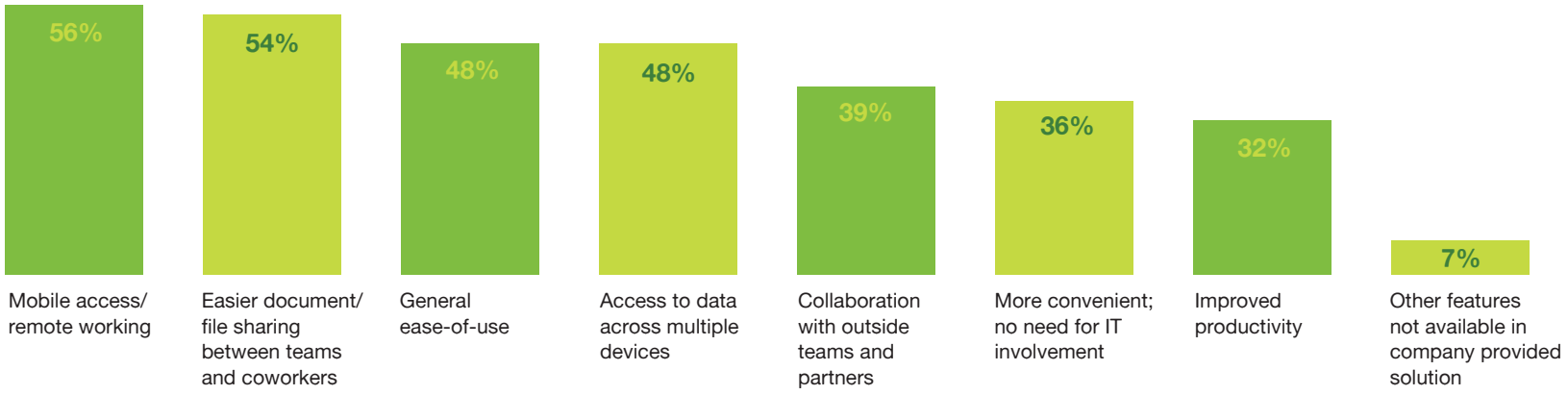
Since it is now endorsed by the company, are your employees primarily using the free, paid or business versions?
Base = IIT only Companies that have adopted Sync & Share; DK answers excluded

IT can see the positive side of file sync & share.

Helps employees work remotely and share data with teams.

Surprisingly, IT pros can point to many factors that drive employees to adopt file sync and share apps. Employees want the ability to work remotely and to be able to share documents and files with teams and coworkers using a simple solution across devices. The fact that these are major drivers of BYOA tells us that many IT departments aren't delivering easy-to-use solutions, or ones that are mobile-friendly for today's on-the-go employees.

Companies using BYO sync & share



takeaway:

File sync and share can help today's on-the-go employee be more productive and collaborative but IT needs to properly manage it to avoid negative impacts for the company.

Which of the following describes why employees have introduced cloud storage/file sync and share apps into the workplace?
Base = IIT only in companies with employees using BYO sync & share

The diminishing role of IT

The main factor against BYOA is the fragmentation and loss of company records. Main attractors seem to be the cool factor and desire to do it differently for the sake of it.

— IT manager, Government, 250-500 employees

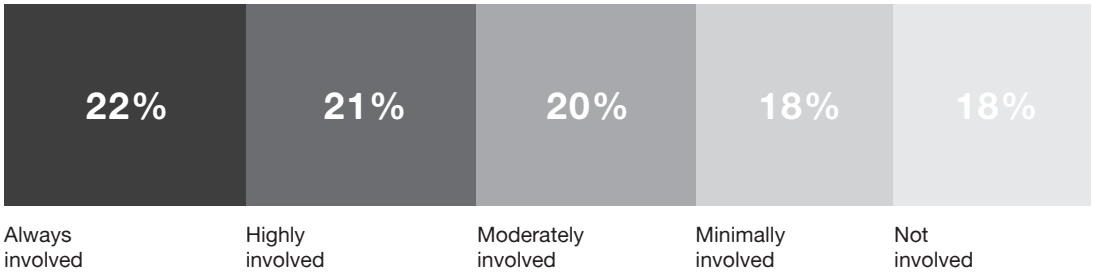
IT admits they are not focused on apps.

56% of the time they are moderately, minimally or not involved.

No IT professional wants to admit they're not controlling the technology decisions within their organization. But when asked how involved they are in certain IT activities, they often overstate their roles.

What's more surprising is how openly IT pros admit their lack of involvement in selecting apps. They claim to be involved only 43% of the time, not involved at all 18% of the time and minimally or moderately involved 38% of the time.

How involved are you or the others in your IT department in the selection of new cloud or SaaS apps today?



takeaway:

IT accepts the fact that employees are driving app decisions. But now they need to figure out how to manage those apps.

How involved are you or others in your IT department in the selection of new cloud or SaaS apps today?
Base = IIT pros only, all applications

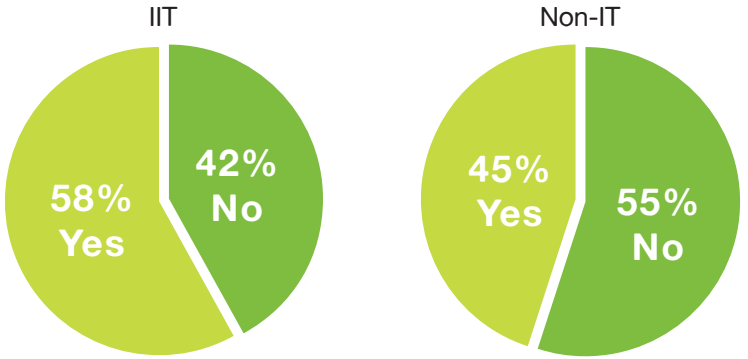
Non-IT employees are going rogue.

They only consult IT 45% of the time.

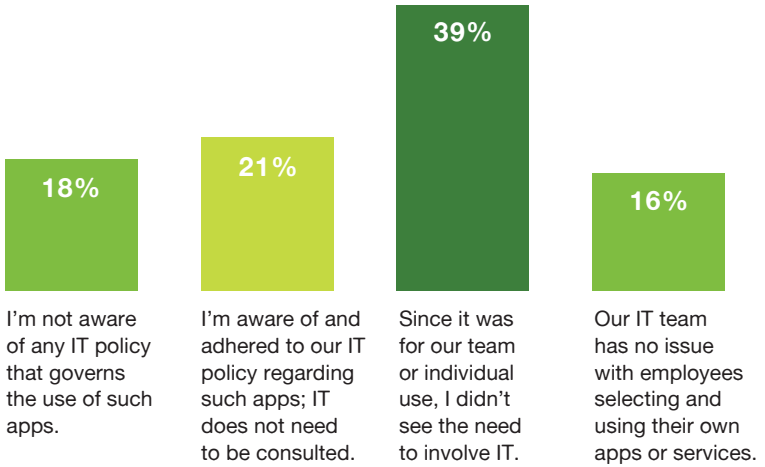
When asked if they're consulted on the decision to use file sync and share apps, IT admits they're only consulted 58% of the time. When you ask the actual people who would do the "consulting" (i.e.: non-IT professionals), the real number shows to be even smaller—just 45%. This shows a disconnect between the two groups, but more importantly, points out that no matter who you ask, IT is involved only roughly half of the time.

The number 1 reason they don't involve IT? 39% don't see a reason to consult IT if they're using an app for individual or team use.

Was IT consulted on the decision to use BYO sync & share apps?[1]



Which statement best describes why you did not involve IT in your desicion to use sync & share apps?[2]



takeaway:

It's impossible for IT to insert themselves into the entire process, but they can learn to manage the influx of apps brought in by non-IT employees.

[1]Base = Using BYO sync & store
[2]Base = Non-IT users that didn't consult IT before using BYO cloud sync & share

LogMeIn

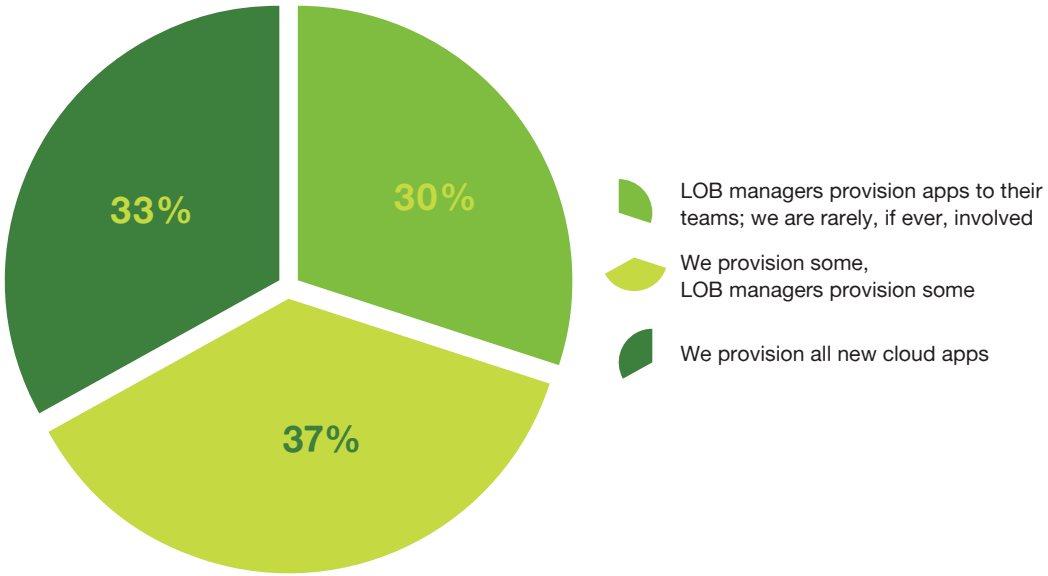
IT isn't even always involved with provisioning.

30% of the time LOB provisions on their own.

Even if IT was ok with employees bringing apps into an organization, you'd think they would want to be involved in provisioning the apps. That's not always the case. The bold truth is that line of business (LOB) managers are involved more often than IT managers in the process—67% of the time. What's more, 30% of the time LOB managers provision apps on their own, with zero involvement from IT.

The really scary part? While the IT department may know an app exists, they don't know who has the app or how they're using it. Which only worsens the major security risks and lack of control for IT.

What is IT's role in provisioning new cloud apps?



takeaway:

IT pros need to seek out tools that aid in the management and provisioning of apps so they're always in control.

Base = IIT pros only, DK excluded

Reclaiming IT control

We don’t currently have a policy. IT should make it a priority to sit down with company CEO, CFO and IT supervisors to create a policy.

— IT manger, Non-profit, 11-25 employees

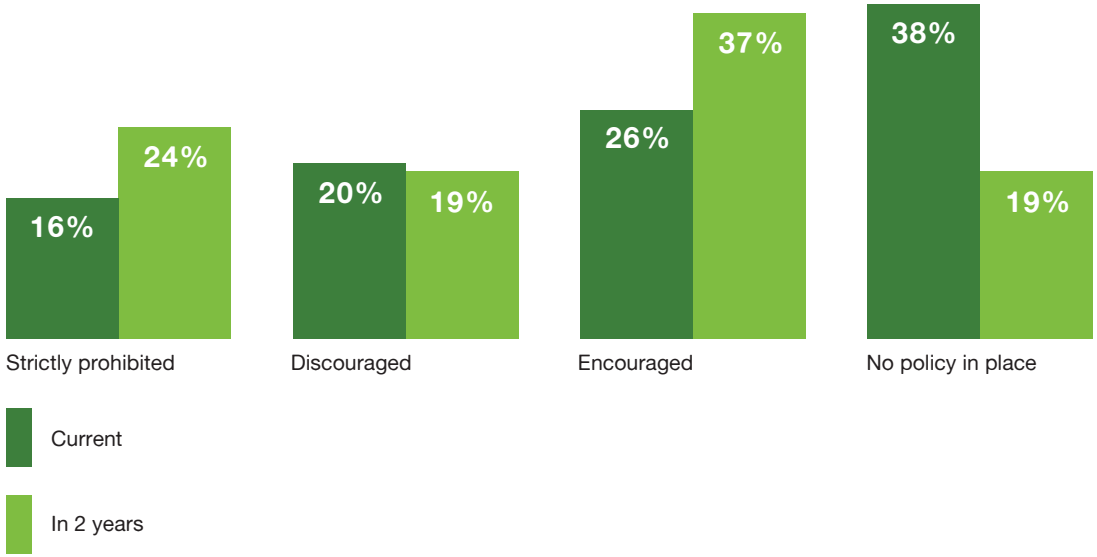
IT needs to focus on BYOA.

38% do not have policies in place now, 81% will within 2 years.

If you look at how IT professionals are dealing with the issue of BYOA, we see wildly disparate approaches, with many not even having a formal policy in place (38%).

More interesting is a closer look at the approach IT departments are making. Among those who have policies, we see a very even distribution of those who strictly prohibit (16%), those who discourage (20%), and those who encourage (26%). These are three very different approaches, and not one is the clear preferred choice.

What we do see is a general trend towards openness to BYOA coming in the future where the number who encourage it will grow from 26% to 37%.



takeaway:

IT pros are all over the map in how they're approaching the BYOA issue, with no clear consensus on the best path.

What is your current policy on the use of BYO apps for work purposes?
Base = IIT only, all applications

Strategic facilitators will be most successful.

Gatekeepers face an uphill battle, and observers will fall victim to perils of BYOA.

When asked how they're currently monitoring BYOA at their organization, IT pros again came back with three vastly different approaches.

The first was to act as a gatekeeper and restrict apps (34%). This is the role IT has traditionally taken—one of continually saying "no" to users and policing what they do.

Another way is to act as a passive observer, and let the BYOA trend wash over them without monitoring app usage. About 40% of IT professionals are currently employing this sit-back-and-take-it approach.

The third is to be more of a strategic facilitator by allowing apps to be brought in by employees, but actively monitoring and managing them. This promises to be the best suited as it embraces the BYOA trend as a reality, but doesn't try to stop it in its path with strict, gatekeeping policies.

Active gatekeeper:
Restrict BYOA by blocking apps

Strategic facilitator:
Manage BYOA through analyzing web traffic logs, packet sniffing, and/or monitoring devices

Passive observer:
Ignoring BYOA (not monitoring)

takeaway:
IT pros who act as gatekeepers will prevent app adoption at the expense of continuous improvement.

How are you monitoring the use of BYO apps?
Base = IIT only, all applications

The technology is advancing so rapidly IT departments have two choices: (1) Lock down all apps and control everything, hamstringing the productivity of 100% of their employees, or (2) Do their best to educate employees on security and trust them. I believe #2 is the only option. I have seen IT departments cost their companies hundreds of thousands of dollars because they are so rigid about the network security that it is nearly impossible to get things done

— Non-IT executive, Engineering firm, 10 employees

Conclusion: Regaining control over corporate data

The BYOA trend is accelerating, as more users are introducing their own file sync and share applications into the workplace, often without consulting IT. So, IT professionals have an important decision to make: are they going to sit back and let this trend wash over them, exposing their organization to huge security risks, or take back control over their corporate data?

Here are four ways that IT pros can use the findings from this study to help guide them down the right path.

1: Understand the scale and reality of BYOA.

70% of IT organizations recognize the BYOA trend exists, but they underestimate the scale. 67% of IT believe less than 50% of their employees use file sync & share apps—as opposed to 73% of non-IT respondents claiming to use file sync & share apps across their organizations.

2: Embrace the Consumerization of Apps as a positive that will make workers more productive.

IT recognizes the value of adopting employee-introduced applications so they shouldn't look at BYOA as a negative. Employees choose apps that allow better mobile access/remote working, easier document and file sharing, and easier access to data across devices.

3: Acknowledge that their peers are still figuring out the best route to take with BYOA.

Across the board there are disparate approaches to BYOA. Some (38%) do not have policies in place, others (40%) are not monitoring it at all—but 81% will have a BYOA plan in place within 2 years.

4: Seize the opportunity to define their strategic role within their organization.

IT can map out their path to facilitate continuous secure policies for their organizations now.

About LogMeIn

LogMeIn (Nasdaq:LOGM) transforms the way people work and live through secure connections to the computers, devices, data and people that make up their digital world. Serving over 90,000 customers, LogMeIn's solution portfolio of cloud services free millions of people to work from anywhere, empower IT professionals to securely embrace the modern cloud-centric workplace, give companies new ways to reach and support today's connected customer, and help businesses bring the next generation of connected products to market. Founded in 2003, LogMeIn is headquartered in Boston's Innovation District with offices in Australia, Hungary, India, Ireland and the UK.

IT management solutions:

LogMeIn's portfolio of intuitive IT management solutions enable organizations to effectively manage applications, data and devices in the cloud. Our solutions are purpose-built to help IT address the changing needs brought about by the Consumerization of IT, and the accelerating trends of BYOA and BYOD.

Manage applications:

AppGuru by LogMeIn

Learn more

Manage data:

cubby by LogMeIn

Learn more

Manage devices:

Central by LogMeIn

Learn more

Manage remote access:

Pro by LogMeIn

Learn more