

AppGuru by LogMeIn

BYOA: Embracing the Opportunity, Controlling the Risk

The challenges and rewards of effective
Bring-Your-Own-Application management



Of 440
IT pros
surveyed

70%

are supporting
two or more
devices¹

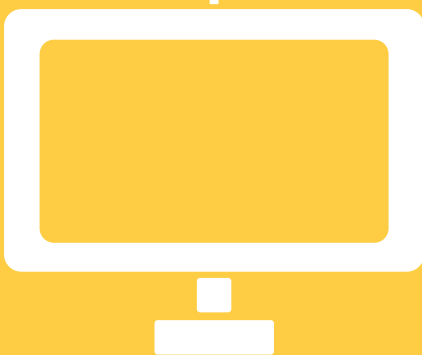
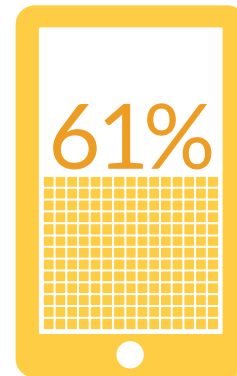
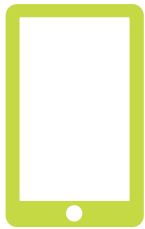
If You Can't Beat 'Em, Manage 'Em

As more and more organizations realize the economic and productivity benefits of BYOD (Bring Your Own Device), those that initially resisted the trend toward employees using their own laptops, tablets and smartphones at work have now largely accepted it and are even championing the practice. In fact, a recent Spiceworks survey of 440 IT pros revealed that almost 70% are supporting two or more devices per user (personal or company-owned), and 61% believe the number per employee will continue to grow over the next five years.¹

But with more devices come more applications – and many of the original concerns and misgivings about BYOD have now largely shifted to the related phenomenon of BYOA (Bring Your Own Application). The issue? When employees and contractors load devices with third-party, cloud-based applications, and then use those applications for business, they create the potential for risk, just as BYOD once did. As a result, IT departments that have come to terms with BYOD are now expressing concern over the risks involved with employees downloading miscellaneous applications on a variety of different devices – on the company network, for work purposes.²

61%

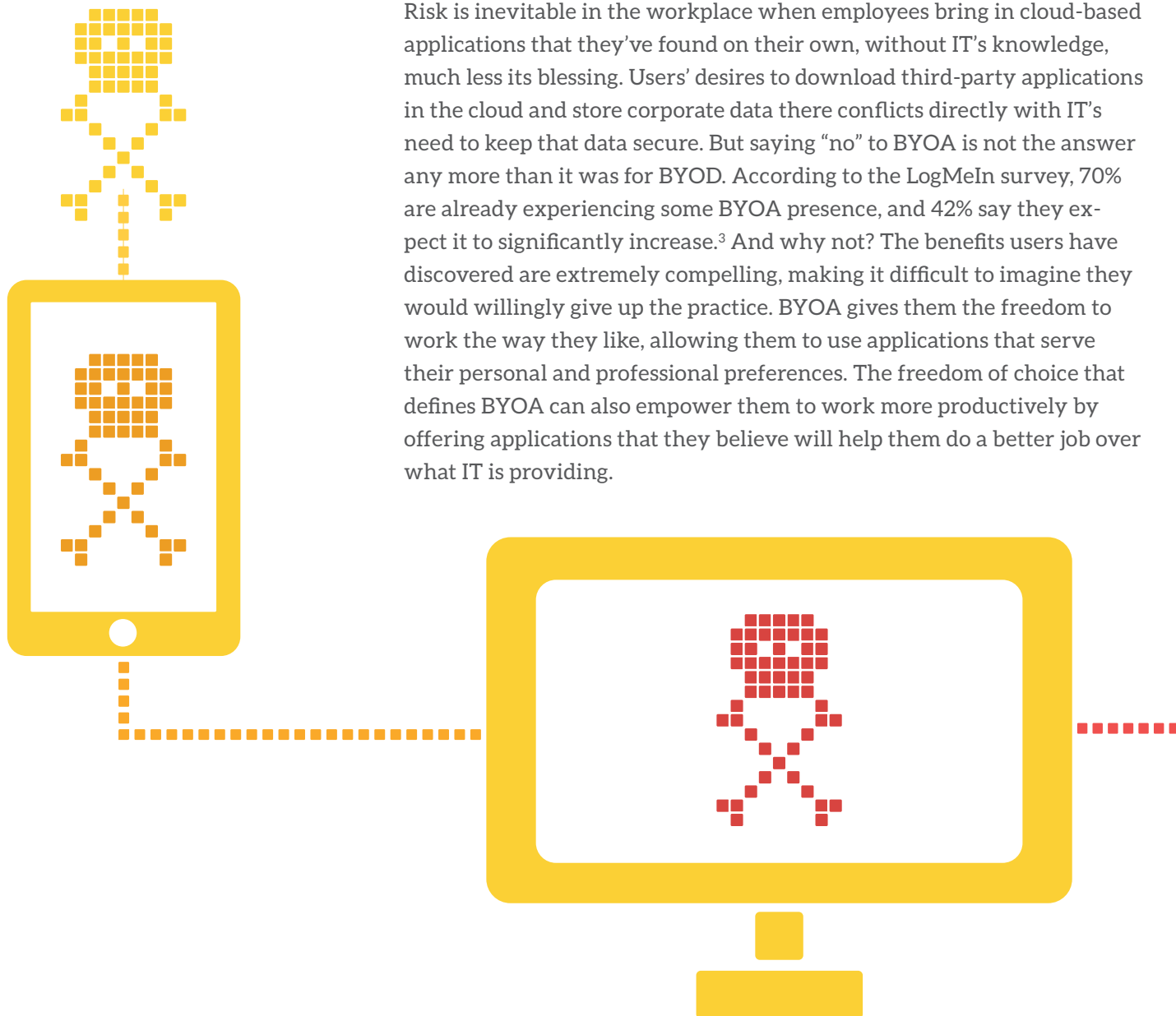
believe the number of
devices per employee
will grow¹



SPICEWORKS
USER QUOTE

“...sooner or later someone’s going to install a virus or use pirated software.”

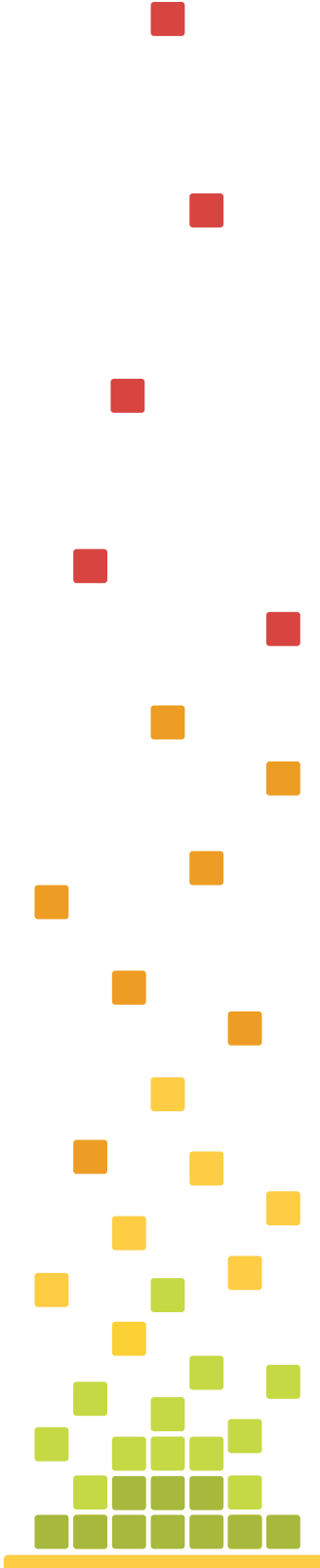
- Spiceworks Community user



A Spiceworks Community user confirms that security is a key IT concern with BYOA, pointing out that by allowing users to install their own software, “...sooner or later someone’s going to install a virus or use pirated software. Not only can this put the network and sensitive data at risk, but it can lead to liability issues for the organization.”

In fact, the question of security may be an even bigger issue than IT realizes. According to a global survey of organizations conducted by LogMeIn and Edge Strategies, IT professionals estimated that employees brought an average of 2.8 applications into the organization. LogMeIn data shows the actual average to be closer to 21 apps – more than seven times what IT estimates.³ The potential risk to security, along with the stress that comes with it, can only be expected to increase as BYOA continues to grow.

Risk is inevitable in the workplace when employees bring in cloud-based applications that they’ve found on their own, without IT’s knowledge, much less its blessing. Users’ desires to download third-party applications in the cloud and store corporate data there conflicts directly with IT’s need to keep that data secure. But saying “no” to BYOA is not the answer any more than it was for BYOD. According to the LogMeIn survey, 70% are already experiencing some BYOA presence, and 42% say they expect it to significantly increase.³ And why not? The benefits users have discovered are extremely compelling, making it difficult to imagine they would willingly give up the practice. BYOA gives them the freedom to work the way they like, allowing them to use applications that serve their personal and professional preferences. The freedom of choice that defines BYOA can also empower them to work more productively by offering applications that they believe will help them do a better job over what IT is providing.



A recent article in *Information Age* confirmed the intensity of users' commitment to BYOA, stating that, "So strong is the compulsion to use these apps that some [users] would even be prepared to pay for them personally. Indeed, a recent US survey found that 37% of employees who currently use apps for work would do just this. Even among those who don't currently use apps for work, one in five would be prepared to spend their own money."⁴ The question then becomes not what IT can do to stop BYOA, but what IT can do manage it. In the words of one Spiceworks Community user and IT administrator, "BYOA is here, and either you will control it; or it will control you."

If IT can find ways to be more involved in BYOA, and manage how it's adopted and used, organizations can reduce the risk associated with it and take advantage of its substantial benefits. These benefits include greater productivity that comes with freeing employees to work anywhere, using their own devices and applications, as well as lower technology expenditures that come with not having to procure or develop certain types of applications. They're similar to the benefits organizations found in BYOD. A similar strategy to what has worked for controlling risk in BYOD can work with BYOA, too. In BYOD, IT teams have found ways to use technology to gain visibility into, and manage the security of, business data on mobile devices. In BYOA, the right technology for discovering and managing cloud applications can enable IT to accomplish the same thing. As a result, IT can become a powerful force for helping empower employees to do their best work - without putting the business at risk. As noted by a Spiceworks Community IT pro, "The technology is here, and here to stay. You can't blindly jump into it, but you can't blindly avoid it either."

SPICEWORKS USER QUOTE

"The technology is here, and here to stay."

- Spiceworks Community user



Managing BYOA

As one Spiceworks Community user points out, a key benefit of BYOA is that employees can use applications they're more familiar with. But to limit the risk inherent with allowing employees to use their own cloud applications for work, IT must be able to manage how these applications are adopted and used. It is certainly worth it to bridge the gap between IT control and employee desire for BYOA, but this can be easier said than done.

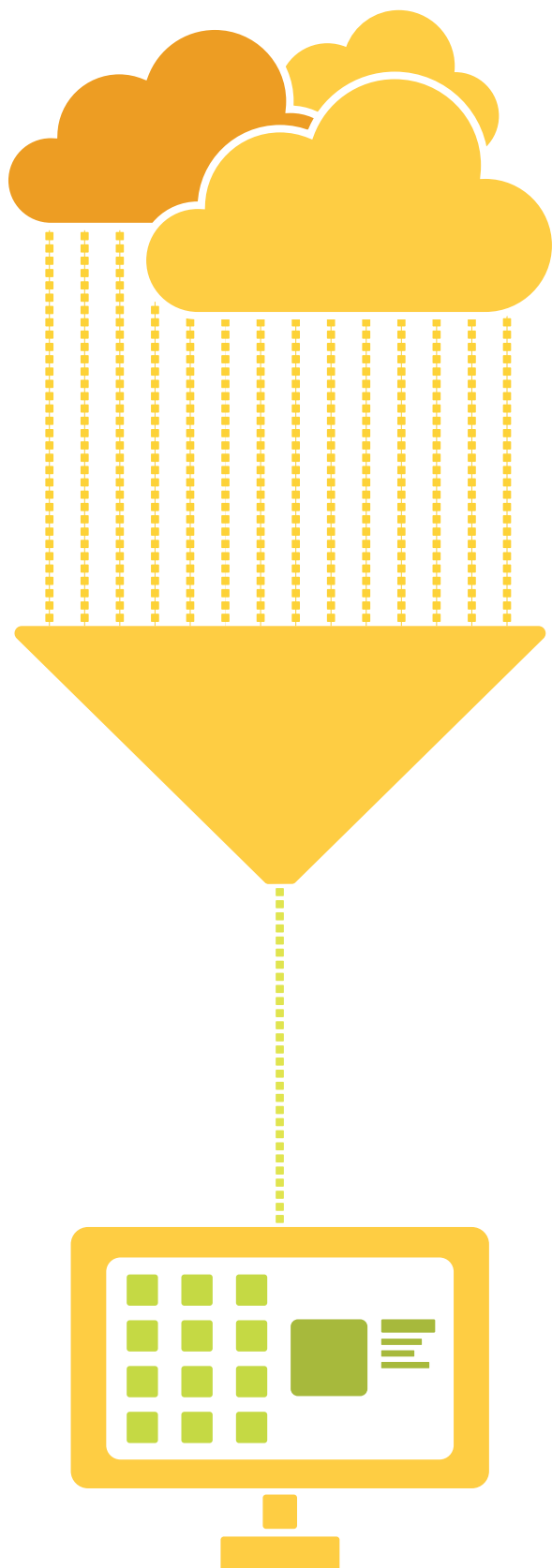
Assess the BYOA landscape

The principle is simple: You can't manage what you can't see. That's why the discovery of – and visibility into – what cloud applications are being used within the organization is perhaps the most fundamental capability IT needs to manage BYOA. But it's also one of the most challenging. Ideally, IT teams charged with securing corporate data need to be able to see:

- What cloud applications are being used on the corporate network, who is using them, and on which devices
- How much company data is going into the cloud, where users may unknowingly expose it to security threats
- When employees are unwittingly affecting organization financials by using software that the company has already paid to license and that is provisioned through IT
- Whether employees are adopting their own alternative cloud applications without IT's knowledge to accomplish the same work, creating unnecessary duplication of effort
- How much network bandwidth BYOA applications are commandeering, potentially compromising network performance across the organization

This type of information enables IT to assess the effects of BYOA and to find ways to manage and control what's happening with cloud applications on the corporate network.





Determine cloud application usage

Beyond discovery, IT needs to know how employee-introduced cloud applications are being used. To address possible risk, IT must determine whether users' applications are secure and whether users themselves are engaging in risky behavior. This information helps IT make decisions that ensure the most effective and efficient use of these applications. For example, if IT learns that several groups are using similar applications, they can look into consolidation for efficiency. Or, if IT can determine the degree to which employee applications are duplicating functionality available through applications the organization already owns, it can strive to eliminate duplication.

Seek central management and control

Using multiple consoles to onboard and offboard users for different applications presents a logistical challenge for any IT organization, and is even more of a challenge for managed service providers responsible for managing multiple applications for multiple organizations. Especially with so many cloud applications being introduced into organizations, centralized management can undoubtedly make it easier to bring applications under IT control - and for IT to ensure that they're being used securely.

Ideally, centralized management should also allow IT teams to perform a variety of tasks beyond onboarding and offboarding, to manage the organization's adoption of cloud applications. IT must be able to enforce security by:

- Standardizing application usage across the organization
- Monitoring usage in the context of security and compliance policies
- Controlling which features can be used based on their level of security risk

A centralized approach enables IT to consolidate access to all cloud applications in one place, for the benefit of both the organization and the application users. For example, unified authentication benefits users by enabling them to more easily manage passwords. Strong authentication also benefits the organization by bolstering application access security. With centralized visibility, IT can discover new applications that employees and contractors are using, and move toward formally adopting them within approved policies.

Embrace BYOA with AppGuru from LogMeIn

*With AppGuru, IT can **help**, not hinder users' efforts to work more productively through BYOA.*

AppGuru, LogMeIn's cloud application discovery and management solution, is designed to help IT teams and managed service providers gain visibility into the cloud applications employees and contractors are using, thus helping to ensure a strategic role for IT in BYOA. AppGuru provides the key capabilities discussed in this white paper, from delivering insights into applications being used on corporate networks, to monitoring usage to ensure security and compliance, to providing centralized provisioning to manage - instead of block - cloud applications used for business. With AppGuru, IT can help, not hinder users' efforts to work more productively through BYOA.

[Learn more >](#)



Sources

1. Spiceworks Voice of IT Report, “The Devices are Coming! How the ‘Internet of Things’ will affect IT... and why resistance is futile,” *Spiceworks*, May 2014. <http://www.spiceworks.com/voit/reports/the-devices-are-coming/>
2. Vijay Saradhi, “How to Tackle BYOA,” *CIO & Leader*, January 2, 2014. <http://www.cioandleader.com/cioleaders/features/19424/tackle-byoa>
3. LogMeIn IT Management Research Series, “Managing applications in the age of BYOA: Reclaiming IT’s strategic role,” *LogMeIn and Edge Strategies*, conducted November-December 2013. <http://solutions.logmein.com/channel-BYOA>
4. Ben Rossi, “BYOA: the next phase in the evolution of business technology,” *Information Age*, May 14, 2014. <http://www.information-age.com/technology/applications-and-development/123458007/byoa-next-phase-evolution-business-technology>