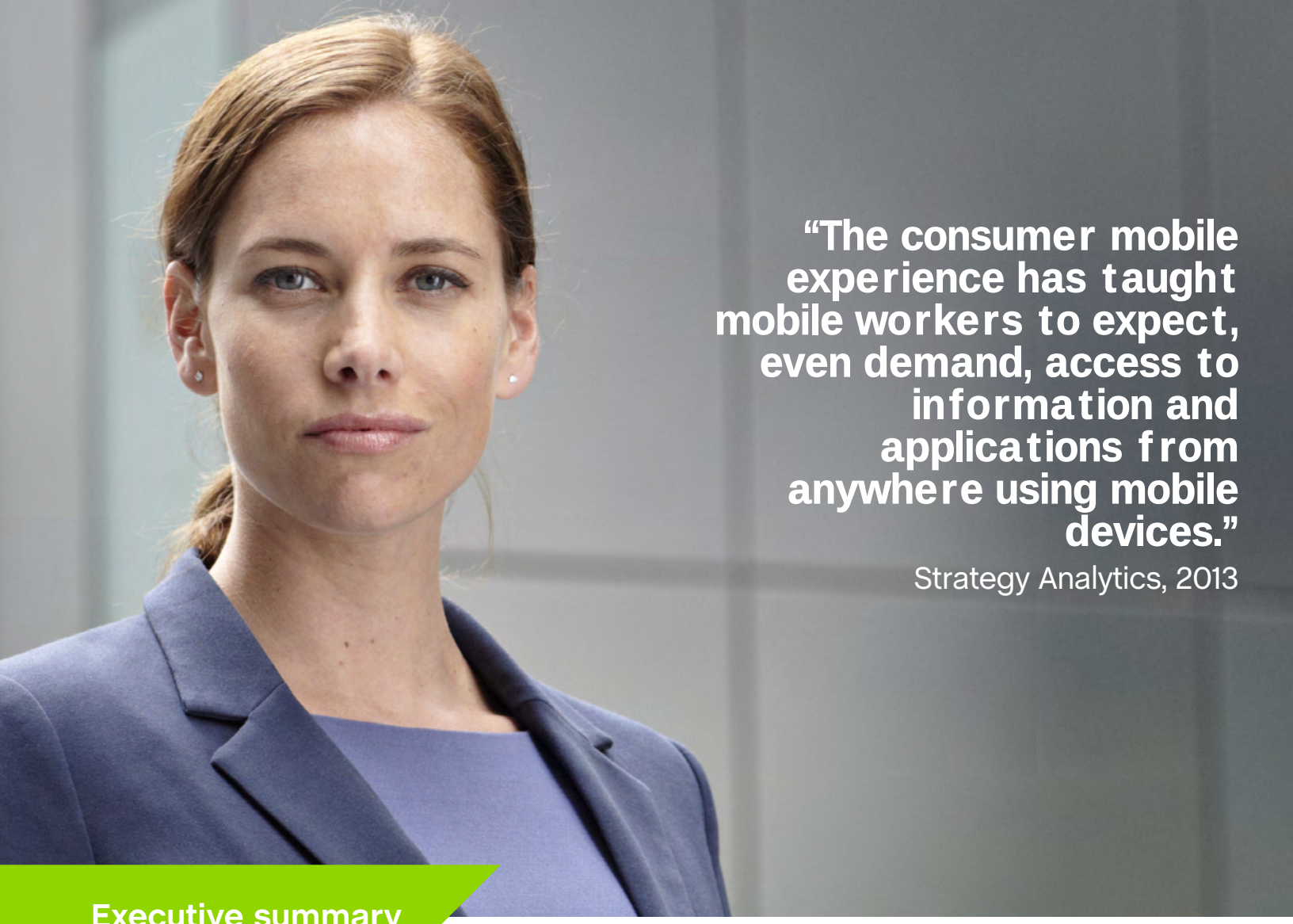
Is BYOD Dead?

Beyond BYOD: Securing Corporate Apps and Data in a Complex Mobile World

AppSense®

You are the technology



“The consumer mobile experience has taught mobile workers to expect, even demand, access to information and applications from anywhere using mobile devices.”

Strategy Analytics, 2013

Executive summary

In just a few years, the rapid proliferation of mobile devices has fundamentally changed enterprise IT management. This mobile phenomenon is often bundled into the term “BYOD”—the acronym for “bring your own device” to the workplace. First –generation solutions to the “BYOD problem”– Mobile Device Management (MDM) and others – have focused on locking down personal and corporate-owned devices.

This device-centric focus has left many IT experts unprepared for the explosion of mobile computing and the hundreds of thousands of apps that have come to market with it. Mobile apps and data are now fundamental drivers of productivity- making the device virtually irrelevant. A recent report from research firm Strategy Analytics estimates that more than 200 million workers are using apps for business. “Mobile workers have moved beyond just mobile email and messaging to include other collaboration apps such as conferencing, productivity apps such as content authoring, and business process apps such as CRM and even ERP,” the report states. “The consumer mobile experience has taught mobile workers to expect, even demand, access to information and applications from anywhere using mobile devices.”

Given the importance of mobile productivity, leading companies have begun to transition from a lock-down approach to focus on providing executives and end users the access to apps and data they demand and require—anytime and anywhere. We call this approach “BYOX”- providing security and control anywhere it is needed, regardless of device, without adversely affecting the user experience. By securing corporate apps and data, IT is truly ready for “bring your own anything” - helping ensure the competitiveness and success of their companies.

This document explores the transition from BYOD to BYOX, the opportunity for IT to become a champion of greater freedom and productivity, and nine big ideas that should drive the next generation of mobility management solutions.

“51% of secure IT networks experienced breaches from employees personal devices.”

Virgin Business Media, 2012

Overview: The rising wave

BYOD has exploded. In a 2012 survey of C-level executives, IT decision-makers and business unit heads conducted by technology consulting firm Avenade, 80% of respondents said they are using personal technology for business purposes. Whether personal or corporate-owned, employees are using multiple devices and a myriad of applications to do their jobs. A recent study cited that by the end of 2014, knowledge workers will use an average of 3.3 connected devices.

In the past, IT was the sole administrator of every device that was used to access corporate data. Today, end users are likely administrators of at least one of the 3.3 connected devices they use to do their jobs. It’s human nature- employees will do what they believe is necessary to do their jobs effectively.

Securing enterprise apps and data in a multi-device world once forced a tradeoff between benefits in productivity, flexibility, and satisfaction with risks of data leakage. First-generation MDM technology hasn’t made IT’s job any easier. By locking down the device, users are unable to access the apps they require and the user experience is severely compromised. One-size fits all security needs and risk profiles among users imposed the same controls across all users- from the C-suite to the frontline employee.

But IT needs the best of both worlds: a solution that allows employees the freedom to use their personal apps as they wish, in the way to which they are accustomed, while putting IT in full control of enterprise apps and data. IT must understand the challenge from the BYOX perspective – a comprehensive approach that encompasses devices, apps and data – and find a solution that reflects this broader view.

Fortunately, technology is emerging today that makes it much easier for enterprises to extend as much liberty to employees as they demand while giving IT control over apps and data as policies require.

“First-generation MDM technology has not made IT’s job any easier. It requires the locking down of devices and compromises the user experience.”

What’s Keeping You Up At Night?

BYOD is a user-generated phenomenon. Employees have embraced new mobile applications and devices to do their jobs more effectively, creating a number of potential nightmarish solutions for IT.

Picture users configuring their personal email clients to access their company email, then saving attachments to their Dropbox folders. Or an employee who inadvertently cuts and pastes text from a sensitive enterprise email attachment into a personal app. Are users backing up corporate data to Apple’s iCloud as a matter of routine? Clearly, the risk of data loss and exposure is enormous.

Then there is the inevitable challenge of workforce turnover. How can you ensure departing users aren’t taking proprietary data with them on their personal devices? Do you have a mechanism for removing company data – short of confiscating the myriad of potential devices and wiping them clean?

Network security breaches are also a stark reality. A recent survey of 500 British CIOs by Virgin Business Media found that 51% of the UK’s secure IT networks experienced breaches from employee’s personal devices in 2012.

It’s no wonder that IT managers are losing sleep over BYOD. The good news is that it’s now possible to liberate users while ensuring security that lets you sleep well at night. You too can create a BYOX organization.

9 BIG ideas for BYOX success

What would the optimal BYOX solution look like? These nine big ideas have emerged as drivers of successful enterprise mobility strategies- driving unprecedented user productivity while providing the security and compliance that IT requires. As you evaluate solutions, consider the extent to which they incorporate each of these ideas.

1 **Allow users to take advantage of the full functionality of their mobile devices.** Mobility gives your company a strategic advantage. Make the most of it by allowing employees to use the apps and functionality they choose. Only put controls where controls are needed. Avoid locking down devices from "personal" apps or requiring unwieldy 16-digit passwords. By investing in solutions that minimize any disruption of the employee's experience while keeping enterprise apps and data secure, you are also investing in employee satisfaction, loyalty and productivity.

2 **Enable employees to use the applications they need.** The right solution should be able to provide you with the same security, control and compliance layer over almost any business app you desire, not just a prescribed subset of apps. Let employees use apps they know and like, so they can collaborate more effectively and be more productive. The app of choice today can easily become the app forgotten tomorrow. Early efforts to manage applications meant either altering the underlying code, which changes the way the apps perform, or creating proprietary knockoffs that are no substitute for the original. Perhaps more importantly, modifying apps takes time and effort, which is not a scalable solution, especially in light of how fast new and improved apps are constantly coming to market. A truly modern BYOX solution must be able to secure apps WITHOUT having to modify the core application code. Look for a BYOX solution that is easy for third-party app vendors to adopt. Vendors will resist BYOX solutions that require them to rewrite or recompile their application code.

3 **Preserve the native experience.** Users shouldn't have to learn anything new just to launch and operate the apps they need for work – particularly email. Having to "rewrite" apps to layer on security in non-intuitive ways will lead to mass user dissatisfaction and eventual non-use of the very apps that are supposed to make them more productive.

4 **Don't build a program that depends on handling physical devices.** The most glaring weakness of conventional mobile security solutions is that they require the IT manager to physically take over the user's personal device. The right BYOX solution should make that completely unnecessary. Rather, it should empower you to manage employee devices, apps and data remotely, over the air – from onboarding and troubleshooting to taking preventive measures and retrieving enterprise apps and data.

5 **Acknowledge that the desktop and mobile worlds are different.** Mobile devices are not mere extensions of the desktop. With their fundamentally different form factors, limited screen real estate, and touch-screen controls, mobile devices are very different from their desktop counterparts. Trying to "mobilize" desktop apps through means such as virtual desktop infrastructure (VDI) is a disservice to the employee and to the enterprise. Mobile app usage statistics clearly show that the winning strategy is to optimize apps for the mobile form factor and to run in fully native mode.

6 **Ensure complete control and security of enterprise apps and data on employee devices.** While liberating users' personal apps and data, the optimal mobile management solution should allow you to manage every aspect of enterprise apps and data. This calls for fine-grained, application-level controls that allow you to implement, change and enforce policies in real time. Fine-grained controls also enable you to remove anything that belongs to the enterprise – apps, data, email and attachments – from employee devices when they decide to leave the organization, without ever touching their devices or disrupting their personal apps or data.

The choice isn't either/or between MDM and MAM – it's finding the right combination of the two in a single solution.

7 **Don't forget data storage.** Allowing employees to use public cloud-based storage compromises security, control and compliance. An effective enterprise data strategy gives users the freedom to work with data on personal devices using preferred apps, while maintaining a policy perimeter around data as it moves across devices and between applications. Your goal should be to deliver an experience that combines the simplicity of consumer cloud services with full IT control over where enterprise data is stored and how it is accessed.

Fill the gap between personal devices and the existing on-premise storage infrastructure, rather than forcing migration to a new storage layer. This leverages your existing investments in file servers and sharing, and avoids disruption of existing workflows that rely on current data access methods.

Your employees' devices have varying risk profiles. You need to be able to set policies for how data is managed at the individual device level. This includes the degree to which data is cached for offline use, as well as how often user authentication is required. In cases where data caching is allowed, you need a comprehensive remote data wipe strategy that includes the ability to remove data on demand or execute a time expiration-based wipe incase a device becomes unreachable.

8 **Email is the killer app- it will make or break your program.** The ability to use business email on personal devices was perhaps the biggest driver of BYOD, and email is likely to remain the most critical app in the BYOX environment for some time to come. Next-generation solutions should include:

- Advanced data loss prevention (DLP) capabilities for native e-mail. Users can use their native email client for business email, while IT can exercise controls to prevent unauthorized copy-and-paste, attachment forwarding and other potential breaches of confidentiality.
- Support for best-of-breed third-party email. Specific users who handle sensitive information should have the ability to install a third-party email client with tighter security controls than native email allows.

9 **Keep your IT footprint small with SaaS delivery.** A recent study by Aberdeen Group found that some 60% of enterprises using MDM have or plan to implement a self-managed, self-hosted deployment model. The same study, however, predicts that cloud-based delivery is likely to grow by 150% and ultimately become the dominant model. The enterprise trend is clearly toward moving as much technology infrastructure offsite as possible. There's no reason for a BYOX solution to require a hardware installation, software implementation or ongoing maintenance. SaaS deployment means that the solution delivers:

- Instant availability and rapid implementation.
- Automatic, instant upgrades as technology advances.
- Security with multiple safeguards against hacking, tampering and data theft.
- Optimal availability, reliability, scalability and performance.

About AppSense

AppSense, the people-centric computing company, is the leading global software provider of user virtualization solutions that transform organizations into productive mobile workforces securely governed by IT. AppSense MobileNow is the first solution to solve the complete BYOD problem for IT and end users- offering end-to-end security and encryption of corporate apps, data, and devices. The company is headquartered in New York, NY with offices around the world. For more information visit www.appsense.com/mobile or iwanttoknowmore@appsense.com

Conclusion

Fairly or unfairly, IT has largely been viewed as an enforcer rather than an enabler of the mobile workforce revolution. By adopting a BYOX approach, IT empowers employees with freedom to work the way they choose while maintaining the security, control, and compliance that company policies require. Technology exists today that gives both IT and the enterprise user base a better choice, allowing IT to become the champion and chief enabler of the mobile workforce.

USA
17 State Street
19th Floor
New York, NY 10004
USA
T +1 212 597 5500
us-sales@appsense.com

100 Mathilda Place
Suite 200
Sunnyvale
California 94086
USA
T +1 408 343 8181
us-sales@appsense.com

United Kingdom
AppSense Ltd
3300 Daresbury
Business Park
Daresbury
Warrington, WA4 4HS
United Kingdom
T 0845 223 2100
sales@appsense.com

France
AppSense France
17 Square Edouard VII, 75009 Paris
T + 33 01 53 43 5148
sales@appsense.com

Netherlands
Jansbuitensingel 20
6811 AD Arnhem
Netherlands
T +31 (0) 263 510 112
benelux-info@appsense.com

Germany
AppSense GmbH
Werner-von Siemens Ring 17
85630 Grasbrunn /
Munich
T +49 89 55 9997 0
de-info@appsense.com

Nordic region
AppSense AS
Tærudgata 1
2004 Lillestrøm
Norway
T +47 41 43 23 30
sales@appsense.com

Australia
St Kilda Road Towers
Suite 1027
1 Queen's Road
Melbourne
Victoria 3004
Australia
T +61 (0) 3 9863 7125
australia-info@appsense.com

AppSense®