SOPHOS
Security made simple.

3 Steps to Securing Your Mobile Workforce

Executive Summary

Today, every business is mobile. Across enterprises of all sizes, everyone from entrepreneurs to knowledge workers needs to stay connected to work with mobile devices, smart phones, laptops and tablets. Everyone from millennials to senior executives demands more and more autonomy and control of their device usage. Employees using their personal devices to access corporate applications and data can put their organizations at risk when passwords or devices are lost, compromised or misused. In addition, cybercriminals are capitalizing on these trends by building mobile malware to infiltrate networks and steal data. Mobile risk is on the rise.

For IT security teams this new reality creates a daunting challenge. They must manage this increased risk while at the same time empower users and respect their privacy. In order to meet this challenge you must have a clear set of priorities that allow you to provide flexibility, but also protect your networks and corporate data. This paper explores this challenge and lays out three key steps organizations must take to successfully secure their mobile workforce.

A Sophos Whitepaper March 2017

Everyone and Everything on the Move

Whether an organization allows users total freedom over personal device usage (so called "BYOD" or Bring Your Own Device), restricts personal devices to a well defined list ("CYOD" or Choose Your Own Device) or allows personal usage of corporate owned devices ("COPE" or "Corporate Owned – Personally Enabled), the trade-offs between control and privacy must be managed. In any of these cases, organizations must protect users and devices, the enterprise network and applications, and sensitive data.

This challenge is especially difficult in small and mid-size enterprises with widely distributed workforces, yet small and stretched IT administration and security teams. A September 2015 CompTIA study, Managing the Multi-Generational Workforce,showed that nearly half of small and mid-sized business have now fully adopted BYOD, as opposed to a little more than a quarter of large enterprises (46% vs. 28%)[1].

This challenge is especially difficult in small and mid-size enterprises

As the functionality of mobile devices have expanded together with their ability to access corporate data, usage and access policies alone are no longer sufficient to manage risk. If policies are overly restrictive sophisticated users will go around them to get work done and make their lives easier.

Millennials believe their personal devices are part of their life, and increasingly are demanding liberal mobile usage and BYOD policies as part of their job criteria. The CompTIA study referenced above shows that the rate of BYOD in millennials was over 53%, as opposed to 28% in boomers. Adding to this risk, the study shows that senior staffers were more than twice as likely to use personal devices than mid-level and lower staff members (65% vs. 32%).

Given these trends, organizations must find technology solutions to these problems that respect and empower users, protect the organization, and are easy to deploy, manage and scale.

[1]https://www.comptia.org/resources/managing-the-multigenerational-workforce

From Management to Security

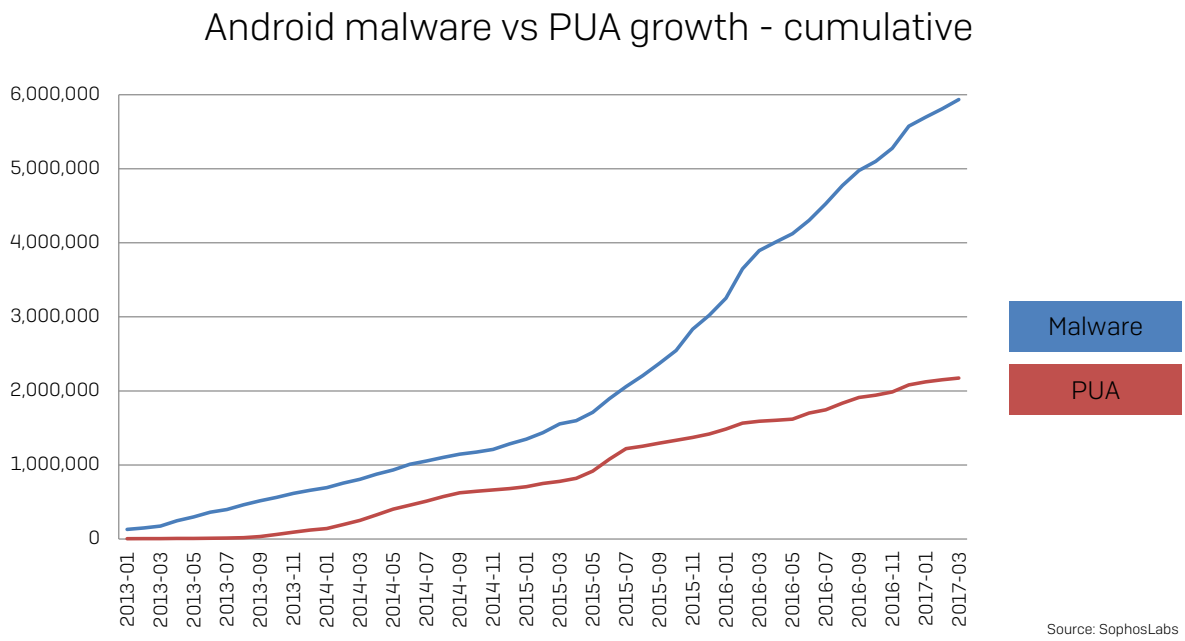
The ubiquity of mobile devices, and everyone's need to use them to be more productive, provides both benefits and risks to organizations. As mobile device usage grew, initially most businesses were concerned with basic device deployment and device loss and theft. Initially, Mobile Device Management, or MDM solutions came to market to help IT staff manage these two issues. However, employee access to corporate data through mobile devices created additional levels of risk. In addition, the number of apps that employees can download at will increases risk with each app.

Employees don't usually intend to put corporate data at risk

Employees don't usually intend to put corporate data at risk, but, they can do this unintentionally, as shown by the increasing number of potentially dangerous apps (PUAs) being identified by Sophos and others monitoring cybercriminal activity. Mobile malware and hacking is on the rise. Open eco-systems like Android are particularly vulnerable to attacks. In addition, recent news has shown that Apple iOS's "walled garden" becoming an increasingly vulnerable platform. The growth of Android malware and PUAs is shown graphically in a chart from SophosLabs[3].

[2]http://www.bbc.com/news/technology-35070853

[3]Sophos: Not Just for PCs Anymore: The Rise of Mobile Malware



Source: SophosLabs

An Alphabet Soup of Enterprise Mobility Management Options

Complex and expensive. Not integrated with data and network protections. Requires expertise to deploy and manage and scale. Intrusive to user productivity and privacy. How do we win in this environment? With an alphabet soup of acronyms like MDM, MAM, MEM and MCM we are faced with a confusing set of choices. It is difficult, if not impossible, to weigh the costs and benefits of each approach. Vendors and analysts offer a variety of frameworks and opinions.

An Alphabet Soup of Solutions

Acronym	Meaning	Focus
MDM	Mobile Device Management	Policy management to keep devices secure
MAM	Mobile Application Management	Ensure the safe usage of approved applications
MEM	Mobile Email Management	Secure access to corporate email
MCM	Mobile Content Management	Protect information being accessed by mobile devices
EMM	Enterprise Mobility Management	Umbrella term for comprehensivesolution, varies widely by vendor

In order to select the correct solution, we should first identify the top areas that mid-size enterprises must address in order to safely enable and take advantage of the mobile workforce.

Three Steps to Managing Today's Mobile Risk

The task of Enterprise Mobile security really boils down to three basic needs: Protecting the user and device; protecting the access to enterprise's network; and protecting an enterprise's data. And of course, most importantly, we need an easy to use solution that let's us accomplish our goals with available resources. Let's take a quick look at the key needs in each of these areas.

Step #1 - Protect users and devices

As we have seen, today's mobile user depends on their smartphone for organizing both their work and personal life. The division between work and personal identity is blurry. Therefore, organizations must step up and fill gaps where users and their constantly on, constantly on the move and ever more powerful devices leave the organization vulnerable. Protecting users and devices means:

- Implementing good password policy.
- Ensuring that users take advantage of native lost device and wipe device features.
- Providing Self Help tools for users to reset their own passwords and reduce the burden on IT.
- Assuring that effective and current anti-malware software is installed and active on all devices (especially Android).

Protecting users and their devices is the first key step to securing our mobile workforce.

Step #2 - Protect the Enterprise Network

Mobility and mobile devices go hand in hand with Wi-Fi access to both corporate and public networks. Managing these connections and the data that flows over them is critical to managing mobile security risk. This requires good network AND device security is in place. Protecting the network requires.

- Establishing and enforce Wi-Fi network access policy.
- Restricting access to the network to compliant users and devices.
- Restricting unwanted or risky applications from accessing the network.
- Securing access to frequently used and approved mobile applications and websites. through the use of a corporate browser solution.

Protecting the network provides a second layer of defense in our 3-step strategy.

Step #3 - Protect Corporate Data

Once we have protected our devices and networks, the next step is to protect critical corporate data. Data moving to and from mobile devices, as well as data on the devices themselves, creates risk that must be managed. A lot of valuable data passes through our mobile devices when we engage in email and other collaboration services such as file sharing and discussions. Many users also move confidential files to public file sharing sites like Box and Dropbox.

To protect business data we must:

- Ensure that email, file sharing and other collaboration and information exchanges take place in secure application "containers" and workspaces.
- Protect applications that support key business processes like order management, customer support, finance, sales and marketing, and product development.
- Enable encryption of important files when they are accessed and shared on cloud storage services like Box, Dropbox and Google Drive.

Protecting our data is the 3rd key step in our approach.

What Else is Needed? Comprehensive, Simple, End-User Ready!

By protecting users and devices, our network and our data, we complete the three key steps outlined here. However, if the solution or solutions we use are typical, they will be complex, piecemeal and not very user friendly. In order enable the safe path to mobile productivity, organizations need to not only take the 3 steps outlined above, but the solutions they adopt must be comprehensive, simple to deploy and manage and end-user ready. When selecting a solution to protect your users, networks and data, consider the following:

1) Is the solution comprehensive and integrated? Does it offer all of the critical protections outlined in this paper, or does it leave significant gaps in protection. If it is comprehensive, do all of the parts work as one, or is it a set of individual piece parts that require additional resources?

2) Is the solution simple for you? Is it easy to license, acquire, deploy and manage? Can you easily measure the effectiveness and compliance delivered by the solution? Does the solution have a single administrative, reporting and deployment capability? Are the management processes simple, straight-forward and easy to learn?

3) Is it end-user ready? Can you tailor the solution to meet the needs of your users? Does the solution respect user privacy while still meeting corporate objectives? Does the solution empower users to manage their own issues such as password reset and lost device location?

Mobile use and mobile risk is on the rise. Employees are no more likely to give up their smartphones and mobile devices and tether themselves back to their desktops than they are to give up streaming music and go back to LPs. Cybercriminals are well aware of these trends. Organizations cannot ignore mobile risk. They must protect their users, devices, networks and data. In order to do this effectively, they need comprehensive solutions that are simple to deploy and manage. And most importantly solutions that are end-user friendly. Only then can organizations reap the productivity benefits of using mobile devices while protecting themselves against the risk.

Sophos Mobile

Sophos Mobile is the EMM solution for businesses that want to spend less time and effort to manage and secure mobile devices. Manage mobile devices with the easy-to-use, web-based, unified Sophos Central admin interface alongside endpoint, network, or server security from Sophos. With its best-in-class data protection, comprehensive security, value-for-money, and flexible management options, Sophos Mobile is the best way to allow the use of mobile devices for work, keeping users productive, business data safe and personal data private.

Try it now for free

Try the online demo or download a free 30-day trial at sophos.com/mobile.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK
© Copyright 2017. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2017-03-17 WP-UK (MP)

SOPHOS