MOBILE SECURITY: 9 DISCUSSION POINTS TO MAKE THE SALE

By Michael Cobb

JULY 2016 | US$25

Channel Partners™

TABLE OF CONTENTS

Channel Partners™

ABOUT THE AUTHOR

@thehairyitdog

MICHAEL COBB, CISSP-ISSAP, is 20-year veteran of IT security with a passion for making industry best practices easier to understand and implement. As an adviser on security controls and information handling practices to companies and government agencies large and small, Cobb has helped numerous organizations achieve ISO 27001 certification and successfully migrate data and services to the cloud. Cobb has also worked with CESG, the Information Security arm of GCHQ, to promote security best practices in government. A renowned author and presenter, Cobb has written numerou technical articles and webcasts for leading IT publications as well as the book “IIS Security.” He has also been a Microsoft Certified Database Manager and registered consultant with the CESG Listed Ad visor Scheme (CLAS).

MOBILE SECURITY: 9 DISCUSSION POINTS TO MAKE THE SALE

By Michael Cobb

NO MATTER THE VERTICAL, SIZE OR GEOGRAPHY, THERE'S ONE THING ALMOST ALL CUSTOMERS HAVE IN COMMON: **Without mobility, employee productivity drops like a stone. Whether it's collaborating with coworkers in real-time, checking and responding to emails or capturing client requests, business is done on the move.**

Yet customers that are (at least mostly) comfortable with their desktop security solutions may still be struggling to find an effective combination of mobile security policies and controls. It's not easy to balance accessibility and security for networks and data. Poorly designed mobile security policies will leave both IT and business users frustrated and looking for ways around controls. Meanwhile, the product landscape is getting more crowded and confusing.

Mobility by the Numbers

53,309
Average number of mobile apps released on the Apple App Store each month in 2015

24.7%
Mobile apps that include at least one high-risk security flaw

74%
Organizations that allow, or plan to allow, employees to use their personal mobile devices for work

160
Unique IP addresses that the average device connects to every day

35%
Communications sent by mobile devices are unencrypted

Data: NowSecure

Let's face it, no one *wants* to spend money on new security products or services. But mobility is a whole new beast. Without a plan, data could be compromised.

As a trusted adviser, you know that sophisticated threats are targeting mobile apps and devices. Here's how to help customers craft a mobile security solution that balances access and safety with a smart mix of policies, services and technology.

Let's look at some questions customers might ask.

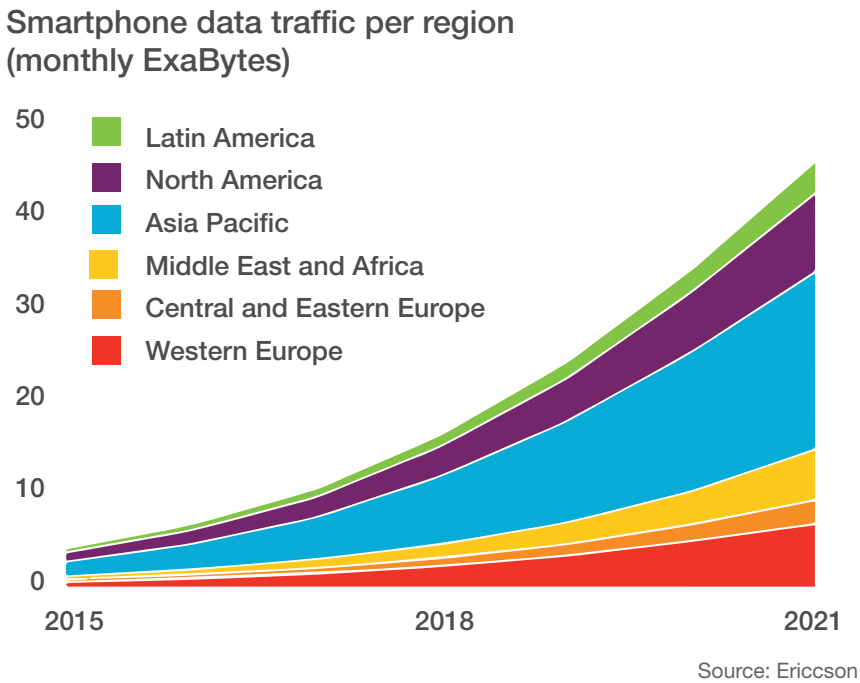
WHY CAN'T I JUST USE THE SAME SECURITY STRATEGY I ALREADY HAVE ON OUR PCS?

PC fleets tend to be homogenous and run a limited number of versions of Windows. They're company owned and, ideally, app installs and administration functions are controlled by IT or a services provider. Updates to the OS and applications are automated.

Mobile devices, on the other hand, exist in many flavors and forms. Fragmentation in the mobile market — and reliance on hardware manufacturers and carriers to test and push updates and patches through to users — mean that months can pass before a device is protected from newly discovered vulnerabilities.

End of the PC Era

Around 90 percent of mobile data traffic will be from smartphones by the end of 2021, according to Ericsson's November Mobility Report. Asia Pacific alone will generate 40 percent of total smartphone traffic by the end of 2021.



Source: Ericcson

For example, only about 10 percent of Android phones run the latest version of Android. That, according to security firm Zimperium, leaves millions of devices still vulnerable to the Stagefright attack, a vulnerability the firm discovered in July 2015.

Think about that — one year on, and close to 90 percent of devices are still at risk. This is one reason why third-party mobile security solutions are an essential component of an effective data security strategy.

WHY NOT JUST ISSUE EMPLOYEES LOCKED-DOWN DEVICES?

Some companies do issue smartphones and tablets, and maintain complete and rigid control. Mobile device management (MDM) tools support this approach and allow administrators to distribute applications, data and configuration settings to mobile devices to control their functionality and security. Such fully managed mobile devices are fine for company-specific tasks, such as tracking parcel deliveries and taking meter readings, and in situations where security is paramount. But for everyday use, employees want and often need more autonomy.

For example, a recent study by the Economist Intelligence Unit, sponsored by Aruba Networks, showed that companies whose employees rate organizational support for mobile technologies as "cutting edge" can see double-digit rises in productivity (16 percent), creativity (18 percent), loyalty (21 percent) and satisfaction (23 percent) compared with employers with poorly rated mobility strategies.

What Makes a 'Mobility Pioneer'?

In the Economist survey, practices and policies that highly rated companies are significantly more likely to adopt include:

- IT support for my own mobile devices if technical issues are affecting my ability to work
- Mobile communication apps such as WhatsApp for work
- All company applications can be easily used on mobile devices
- Cloud document hosting services like Dropbox for work documents
- Training on how to use mobile devices to collaborate more effectively

The survey included 1,865 full-time employees representing a range of ages, business departments and industries. Just 11 percent gave their employers the top rating of mobility "pioneer." Most, 42 percent, say their employers are "adequate."

Not exactly a recipe for attracting the best talent, but a great opportunity for partners.

OK, SO WHAT ARE OUR ALTERNATIVES?

Let's discuss the three most popular hybrid models: bring your own device (BYOD), choose your own device (CYOD), and corporate-owned, personally enabled (COPE).

With CYOD and COPE, policies provide some level of flexibility for employees while limiting them to those devices that the business feels are secure and compatible enough with existing access control, management and security tools. Typically,

employees can customize the device, to a point, but don't have administrative privileges, so they need to formally apply for any significant changes or software installations. This can leave employees feeling disgruntled from a lack of privacy and restricted by IT-imposed limitations, where applications are targeted to suit the mobile device rather than a user's needs.

Allowing people to work with their devices and applications of choice, the BYOD way, not only makes them more productive, it helps tackle the big problem of shadow IT, where users go rogue and bypass security measures to use the devices and services they prefer.

In BYOD environments, though, customer data resides on devices not owned or directly controlled by the organization itself. It's a conundrum that the industry is still trying to resolve. The main problem is data leakage. Once data —like a price quote or customer list — is saved to a device, employees can potentially paste it into other apps, forward it via email or save it to external storage.

BYOD Goes Big

Gartner says BYOD is most prevalent in midsize and large organizations — $500 million to $5 billion in revenue, with 2,500 to 5,000 employees. Companies in the United States are twice as likely to allow BYOD as those in Europe.

HOW CAN YOU HELP US ACHIEVE APPLICATION AND DATA SECURITY? WHAT TOOLS DO WE NEED?

As security, device and OS vendors gain a better understanding of the threats mobile data faces, they're continually adding features. For example, lost and stolen devices leave corporate data exposed, so remote-wipe functionality is pretty ubiquitous.

MDM tools introduce "secure containers" and "dual-personas"— different approaches for the same task, dividing smartphones into two partitions, one for personal use and the other for corporate use, with separate apps or modes for web browsing and accessing corporate data like email and documents, which are encrypted and processed inside the container. While suitable for some environments, the drawback with this approach is that it forces employees to access corporate data via a small selection of limited and often unfamiliar apps, or to switch back and forth between work and personal modes.

While not as bad as having to work with two entirely separate devices, a personal one and company issued one, it still can be an exasperating experience. And, while it enables better control of customer data, content is still at risk from user-installed apps.

Mobile application management (MAM) tools tackle this problem by controlling the applications in use on a device. Any data that travels to and from an employee's device using controlled applications can be tracked and monitored. It also helps in preventing employees from downloading and using applications that are not allowed by the customer's policy.

MAM offers more granular control than MDM but is pretty much limited to the security capabilities of a mobile device's underlying operating system. While vendors like Microsoft, Google and Apple continue to improve the security of their OSes, they can never be 100 percent, and poorly written apps can potentially enable attackers to exploit vulnerabilities.

NowSecure's 2016 Mobile Security Report found 24.7 percent of mobile apps include at least one high-risk security flaw, and business apps are three times more likely to leak login credentials than the average app. Problems such as insecure data storage, poor implementation of secure communication, and weaknesses in authentication and session management can lead to malicious as well as unintended data leakage.

The lines between different types of mobile security are blurring as vendors compete to offer the most flexible, yet most complete, solution. Partners may need to carry a selection of options on their line cards and have a methodology to align a customer's security and flexibility needs to the proper tool.

WHAT'S NEW IN MOBILE SECURITY SYSTEMS?

The latest suites focus on data encapsulation and application-level controls to protect corporate data from misuse and leakage while in transit, at rest and in use, without interfering with the native user experience.

Application-wrapping technologies attempt to do this by adding restrictions to app and device functionality by modifying mobile application binaries to give them more security and management features. It doesn't require any changes to the underlying application but enables an administrator or partner to set specific policy elements, such as whether data encryption is on by default, and whether data can be stored on the device or shared.

It's a very useful approach when devices lack sufficient device-level MAM features, or when managing devices using a MDM solution isn't practical, such as in BYOD environments where there are a lot of contractors or other third-party users. Unfortunately, wrapping changes the behavior of an app and often involves resigning and redistributing it, so it raises licensing issues that the industry as a whole is still undecided on.

Attacks against mobile users appear overnight, and cloud-based threat intelligence, optimized for mobile platforms, is becoming essential to ensure devices and users can be protected in real-time as they access the internet. This is an area that is developing quickly, with many firms forming alliances to offer improved threat intelligence and detection capabilities that can be integrated with various mobile security suites. Examples include Trustwave and CounterTack and Microsoft and Lookout.

Hidden BYOD Risk

What happens when an employee walks into a store and upgrades to the latest hot smartphone? How can your customer be sure sensitive data wasn't on the device? At minimum, set a policy that before any device is discarded, sold or traded in, it must be wiped. MDM software can be set to trigger an alert when someone attempts to register a new phone on the network.

These and other security controls need to be delivered via a lean client so neither the user experience nor the network is impacted. Large downloads of threat data or heavy signature updates impact device performance, whereas cloud-based protection is light and battery- and CPU-usage friendly.

Overall, security development has been piecemeal rather than holistic, making comprehensive mobile security difficult to achieve just with products. You also need policies.

WHAT SORT OF POLICIES DO WE NEED?

Partners need to help customers decide what type of mobile environment they are comfortable with and understand the associated risks. Gartner predicts that by 2017, half of employers will require employees to supply their own devices for work purposes. However, a study by HID Global found almost 60 percent of European SMEs and 33 percent of larger enterprises don't have security restrictions in place regarding company mobile phone use. The North American market may be a bit further ahead, but there's certainly room to improve.

Customers need tailored strategies for managing their mobile workforces to reduce the risks to an acceptable level. Smaller clients will certainly need help in assessing the risks of different device and carrier combinations and the security solution that's right for them. To maximize their ROI, they will also need support from planning and set up to operation.

Services should include:

A **risk assessment** to highlight the must-have mobile security solution features for their needs. For those moving toward some form of BYOD, tools will need to work at the content and application level, rather than at the device level. Support for self-service enrollment, customized over-the-air configuration and automated policy enforcement will make it easier to apply security across the board.

A **device audit** because, as mobile users have a huge variety of device types running different operating systems, it's essential that any solution provide protection for all the devices that are allowed on a network. For example, recommend a solution that supports at least iOS and Android if employees are using mobile phones to connect to the network.

A **management discussion** will reveal whether controls can be deployed and managed from a single console that, ideally, provides visibility into the status of user and device security as well integration with other back-office technologies, such as Active Directory and Citrix.

A **cloud versus on-premises discussion** is also critical. On-premises solutions need dedicated resources, both from a hardware and technical manpower perspective, so for many SMB customers, a cloud-based software-as-a-service (SaaS) solution will offer the easiest and quickest setup, and at a lower cost. Many solutions are offered in modular form, so you can help customers select just the security controls they need for their particular environment or user base.

Scalability and licensing also need to match the customer's business model and plans.

The **key security domains** that need to be addressed are system, configuration, apps, content and collaboration, and network communications. This means the features needed to provide an acceptable level of security — put enforcement behind policies — are:

- device configuration
- anti-malware
- anti-theft — locate, lock, or erase data remotely
- encryption
- secure connectivity
- application whitelisting
- data-loss prevention

Products will list far more features than these — commonly vulnerability shielding, anti-phishing, browser exploit prevention and ransomware protection. Many are marketing terms used to highlight differences in the way certain types of malware are detected or blocked. However, some features do add additional layers of security, so check with suppliers on what specific controls actually do and how they may enhance customer security. For example, ransomware is an epidemic, and application whitelisting, which allows only known-good applications to start, will stop malicious and unknown apps like ransomware from executing.

WHAT DO MY REGULATORY COMMITMENTS AND TRUSTED THIRD PARTIES MEAN TO A MOBILITY PROGRAM?

Mobility is hot in health care — 47 percent of physicians who have smartphones use them to show patients images and videos, according to a Manhattan Research study. Ask these customers what that means for HIPAA.

Fortunately, many vendors offer solutions tailored for particular customer verticals, such as health, finance and education, that must meet compliance standards like SOX, PCI-DSS and GLBA before sensitive or private data can be shared among authorized users. These solutions often include more robust data access controls, such as two-factor or one-time-password authentication, to limit access to authorized users only. Reporting features tend to be more comprehensive, too, in order to meet compliance rules.

Some clients may need a solution that has a particular type of certification or that has achieved a certain Common Criteria Evaluation Assurance Level grade.

As more partners, suppliers and contractors connect to a customer's network and data, being able to track user registration and device compliance is essential. Enterprise mobility management (EMM) suites offer greater control over business data and information on both unapproved and known devices connecting to internal resources. Devices are subjected to security checks each time they connect to ensure they're compliant with network security policy.

One aspect of mobile security that is often overlooked is log analysis. It's an important element in many compliance standards and when opening network access to third parties. Usage statistics, malware logs, quarantine, or firewall events can provide important insights into the overall security of a network and its clients

and users, so solutions that offer the ability to export this data for SIEM analysis should be a priority. Unusual user, application and network activity can then trigger automatic alerts to your or the customer's security team.

HOW DO WE COMMUNICATE ALL THIS TO OUR END USERS IN A WAY THAT DOESN'T CAUSE A REVOLT?

Whichever solution is deployed, it's vital that employees and contractors are fully aware of the mobile security policy and their roles in safeguarding corporate data.

Gartner's Managed Diversity Model for BYOD and CYOD to Manage and Safeguard Users, IT and the Business makes a key point when it comes to giving mobile users more choice and freedom. The Gartner model has three options, ranging from the traditional fully-managed device to the "user free-for-all" device. The analyst firm quite rightly emphasizes that users have to be more responsible if they may choose their own preference, and a clear delineation of responsibility, along with education, is critical. This is a valuable service to offer. Some areas to cover include use of device passcodes, knowing when an app is suspicious and VPN options for when they want to access public Wi-Fi.

Related Reports

- Case Study Challenge: Mobile Key to Vertical Success
- VPN Security: Trust, but Verify
- How to Sell Secure Mobile Connectivity
- Going Global, Selling Mobile
- Managed Wi-Fi: Your Next Services Moneymaker

The move away from the traditional, fully-managed device environment is inevitable, and while mobile technology does introduce security risks and management challenges, most companies can safely use mobile technology to further the business, if it's approached the right way, with the right tools and training.

The goal should be to secure mobile devices and apps without compromising productivity. After walking through these topics, the risks and demands of a customer's mobile users will be better understood, and partners can help match employee needs with security.