IBM Software

Thought Leadership White Paper

Accelerating the deployment of a secure mobile enterprise

Maturing the enterprise's mobile security posture to mitigate risk while in pursuit of business potential

Contents

Introduction

For more than two decades, organizations have struggled with the security challenges of the wireless workplace. Laptop computers first blurred the boundaries of traditional environments, and now smartphones and tablets are increasingly becoming the professional tools of choice. In 2011, smartphone sales exceeded PC sales for the first time—and analysts believe smartphone sales will exceed 1.5 billion units by 2016.[1] That same year, more than 350 million people are expected to use their smartphones for work.[2]

Organizations worldwide are taking full advantage of this trend, as the use of mobile devices—including the employees' personal devices used for work—can increase responsiveness, agility and productivity. But as more employees connect their mobile devices to the enterprise—introducing devices designed for the consumer market into business environments, adopting more informal behaviors typically used for personal communications and often placing business and personal data side by side on the same mobile platform—security across the entire enterprise IT environment becomes increasingly important and considerably more complex.

With layers of vulnerabilities now existing across the enterprise environment and a dramatic increase in sophisticated attacks, business leaders are demanding that IT take a proactive approach to protecting critical data and infrastructures. This white paper identifies key challenges and introduces strategies to reduce risk, and it examines ways organizations can become more secure in their use of mobile technologies.

What's different about mobile devices, applications, access—and threats

Mobile devices, applications and patterns of access are changing the way organizations interact with their customers, employees and partners. Across the globe, organizations are using growing mobile capabilities to capture new opportunities and transform business models while extending their existing capabilities for use anywhere, anytime. In the process, however, they face the need to implement new processes for managing mobile devices, applications and access—and for safeguarding their mobile organization against threats.

That's because mobility—whether on a secure corporate virtual private network (VPN) or a public wi-fi hotspot—involves behaviors, technologies and threats that are different from those encountered in an office environment. Some of these unique challenges include:

- **Mobile devices are used in more locations**. Mobile devices are most often used outside the corporate network, and users may employ a wide variety of networks to access their accounts. Authentication is important—the integrity of transactions or communication can easily be compromised—so access should be granted based on recognizable factors such as the context of the location, device characteristics, application information, time and network.

- **Mobile devices and the applications they support are diverse**. Users typically have more than one device, and the state of these devices is constantly changing. Different operating systems may support different security measures, and employees may install different applications on their devices. They also may store sensitive business information, making loss of a device and employee turnover as much of a threat as an attack. The organization needs full visibility into devices and applications to fully understand threats.
- **Mobile devices have become the primary interaction channel for many users**. Malicious targeting of mobile devices and their applications may lead to attacks on the enterprise network or infection of systems. The huge increase in the number of devices also can increase the cost and complexity of IT management—and protection.
- **Mobile devices are shared and have multiple personas**. Smartphones and tablets can be shared with family and coworkers, so the devices need to have different security profiles. An employee and his 5-year-old daughter should both be able to access personal photos, but only one of them should be able to view last quarter's earnings. Authenticating and authorizing only the user or only the device may not provide the controls and protection necessary.
- **Mobility prioritizes the user experience**. With users making device and application decisions based on their personal preferences, imposing security controls that are unsuited for mobility can lead to non-compliance or non-participation. Security measures that seamlessly blend into the user experience—for example, strong, but easy-to-manage passwords and controlled but simplified application installation—can increase compliance and enhance user productivity.

The core challenge, therefore, lies in finding ways to combat potential security threats without limiting the enthusiasm of employees for using mobile devices and applications. By employing a proactive, layered approach to securing the mobile enterprise, IT organizations can become business enablers—rather than being seen as the "security police" who discourage the use of new technologies. Organizations that deploy integrated security solutions and an adaptive security framework can empower their workforce to get more done anywhere, anytime.

Mobility can be a boon to users—but a headache for IT

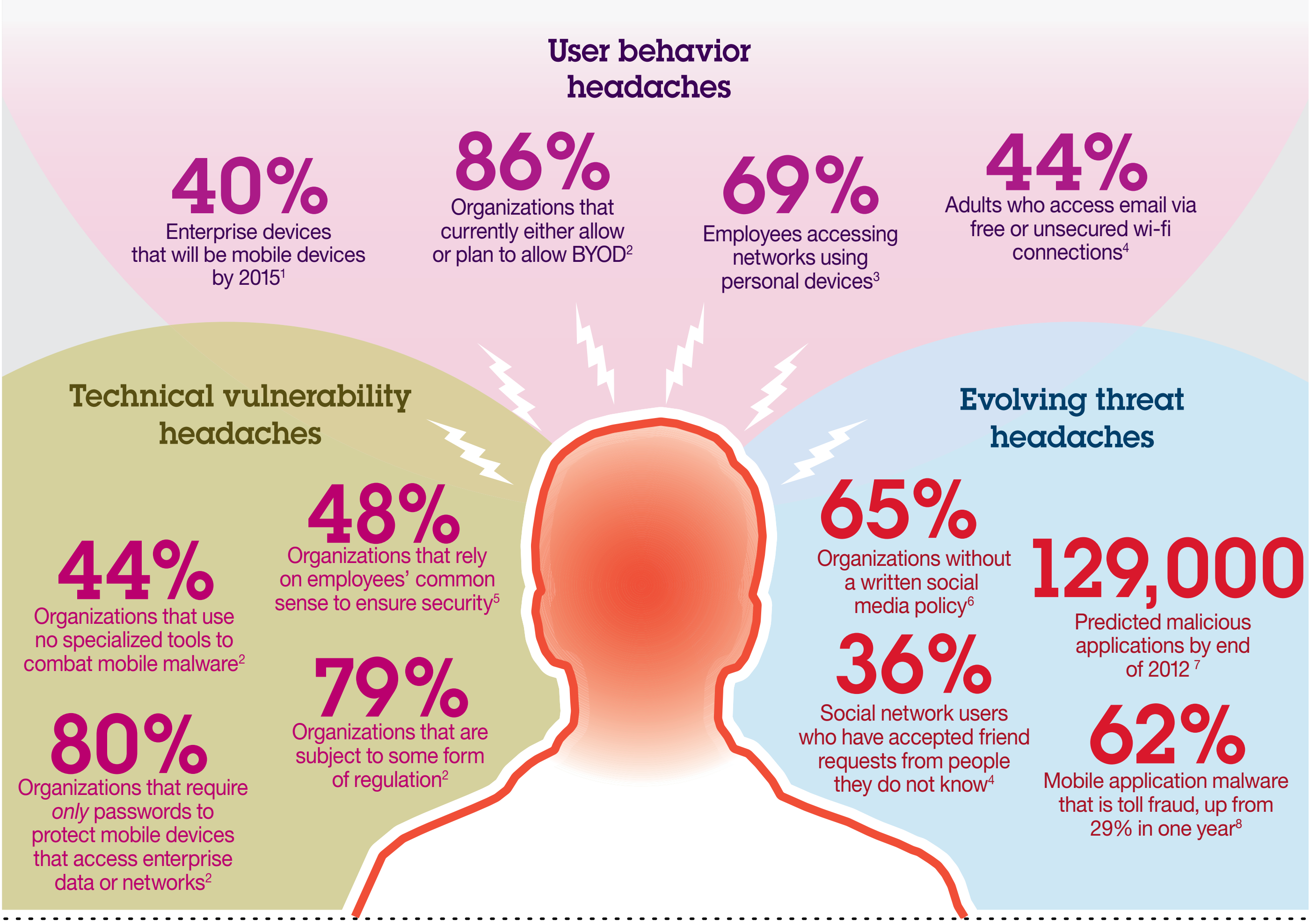
When IT operations encounter the unique characteristics of mobile devices, applications and access, specific challenges quickly appear. The headaches they cause for CIOs and IT administrators typically grow from three areas—user behavior, technical vulnerabilities and the evolving threat landscape.

User behavior

As smartphones and tablets are rapidly adopted for business use, they join the ranks of existing endpoints, such as laptops and desktops. Mobile additions may include iPhone, Android and Blackberry smartphones; iPad, Android-based and other tablets; voice/text-only cell phones (that is, phones without a data plan); netbooks or ultralight laptops; and other ruggedized, job-specific mobile devices.

But who owns these devices? Many businesses are instituting bring-your-own-device (BYOD) programs, under which employees can use their own mobile devices to access corporate email, data and applications. BYOD programs can help reduce IT operating and equipment costs, improve employee productivity and offer competitive differentiation—but the sheer volume and speed of new devices being introduced into the workplace can create significant management control headaches for IT, and the ways in which devices are used can create security headaches for those responsible for keeping corporate data safe and maintaining compliance to policies.

Mobile security headaches for the IT department



User behavior headaches

40% Enterprise devices that will be mobile devices by 2015[1]

86% Organizations that currently either allow or plan to allow BYOD[2]

69% Employees accessing networks using personal devices[3]

44% Adults who access email via free or unsecured wi-fi connections[4]

Technical vulnerability headaches

44% Organizations that use no specialized tools to combat mobile malware[2]

48% Organizations that rely on employees' common sense to ensure security[5]

80% Organizations that require *only* passwords to protect mobile devices that access enterprise data or networks[2]

79% Organizations that are subject to some form of regulation[2]

Evolving threat headaches

65% Organizations without a written social media policy[6]

129,000 Predicted malicious applications by end of 2012 [7]

36% Social network users who have accepted friend requests from people they do not know[4]

62% Mobile application malware that is toll fraud, up from 29% in one year[8]

[1] IBM projection.

[2] Michael Finneran, "2012 State of Mobile Security," *InformationWeek,* May 2012. http://reports.informationweek.com/abstract/21/8792/security/research-2012-state-of-mobile-security.html

[3] Information Security FS, "CISO - Chief Information Security Officer Role: From 'Digital Bouncer' to Strategist." http://www.wbresearch.com/InformationSecurityFS/ciso.aspx

[4] Symantec, "2012 North Cybercrime Report." http://www.slideshare.net/marianmerritt/2012-norton-cybercrime-report-14175700

[5] Jim Rapoza, "Buyer's Guide to Mobile Device Management," *InformationWeek*, November 2011. http://reports.informationweek.com/abstract/18/8546/Mobility-Wireless/buyer-s-guide-mdm.html

[6] IBM Corp., "IBM X-Force 2011 Trend and Risk Report," March 2012. http://www-935.ibm.com/services/us/iss/xforce/trendreports/

[7] Trend Micro, "Behind the Anroid Menace: Malicious Apps," Security Intelligence Blog, 2011. http://blog.trendmicro.com/trendlabs-security-intelligence/infographic-behind-the anroid-menace-malicious-apps/

[8] Lookout Mobile Security, "State of Mobile Security 2012," 2012. https://www.lookout.com/resources/reports/state-of-mobile-security-2012

Technical vulnerabilities

Today, everyone in the organization from IT to senior executives is paying more attention to device, application and access security than ever before. Many, in fact, place lost or stolen devices at the top of their list of mobile security concerns,[3] as the possibility for compromised or stolen data can cause serious damage to business reputation or competitive advantage.

Effective mobile security, however, goes beyond the device to require an end-to-end security posture. IT has to address mobile risks ranging from insecure data storage and weak server-side controls to insufficient transport layer protection, client-side injection, and poor authorization and authentication. To combat external threats, robust data security controls on mobile devices along with strong authentication measures to control network access can be essential for reducing risk.

The evolving threat landscape

IT organizations traditionally have operated in a reactive mode, responding to security risks only after a problem occurs. But given the speed with which mobile technologies change and mobile users' dependence on immediate access to do their job grows, reactive is no longer fast—or secure—enough. And since mobile technologies are still relatively new for most organizations, existing security measures often do not provide adequate protection.

Potential threats now target specific user behaviors or technical vulnerabilities enabled by mobile vulnerabilities using social engineering, identify theft, rogue applications, man-in-the-middle attacks or denial of service. In response, organizations need to more diligently manage areas such as their employees' use of social networking, where individuals may be too casual about sharing information. They need to monitor devices to make sure their operating systems are not jailbroken or rooted. They need to manage downloads of applications that may contain malicious code, expose sensitive corporate data and personal information, and cause damage to infrastructures.

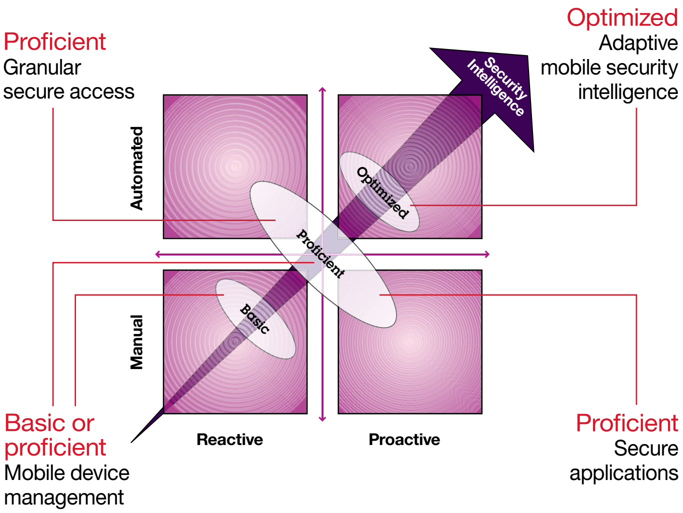
Four steps to a more secure mobile enterprise

The wide range of smartphones and tablets used in the enterprise together with growing threats to mobile device, application and access security mean IT organizations can face an uphill battle in defining comprehensive security standards and controls. But there are steps the organization can take.

Secure mobile devices: The foundation of a safe environment

Mobile device management is typically the cornerstone of any enterprise mobility strategy—and often the first investment made. That's because it is difficult to manage risk until you understand the scope of what you're trying to protect. A mobile device management solution allows IT to track and monitor the number of devices in use across the enterprise. Both employee-owned and corporate-owned devices can be managed using the same endpoint management solution.

Four steps to a more secure mobile enterprise



The security controls deployed by such technology should not limit the user experience—rather, they should enable safer working practices to protect the device and the sensitive data it stores and transmits. Ideally, a mobile device management solution should be an extension of an existing endpoint management solution, to give you a single-pane-of-glass view across all enterprise systems.

An effective mobile device management solution can prevent data loss with the ability to encrypt data for transmission and wipe data from lost or stolen devices. It can prevent access to devices with locking and can mitigate exposure to vulnerabilities using anti-malware, jailbreak detection, non-compliance detection and the ability to push security updates to devices.

Using mobile device management, organizations can set policies for approved connections. They can maintain records of "blacklisted" applications that are not authorized to access corporate resources. They can develop mobile security intelligence to support the constant vigilance that security requires. And they can grow and evolve their capabilities to meet the ever-increasing sophistication of threats and attacks.

Mobile device management can protect application access with user authentication and the ability to disable applications. In addition to meeting technical requirements, a mobile device management solution can help control IT costs and reduce management complexity as the number of endpoints that need management grows.

Protected mobile access: Bad guys out, good guys in

IT organizations need to ensure safe and secure access to resources by addressing the context-specific nature of mobile access. The location, the network, the specific user and many other attributes of a mobile interaction can influence the risk that comes with access to enterprise data and resources. The level of risk can influence the decision to grant or deny access, the choice of authentication scheme and the authorization of services enabled for the interaction.

Access control should authenticate both the user and the device, and the schemes employed should be selected based on their fit to mobile users—for example, biometrics or one-time passwords. Organizations also should keep in mind the need to employ an environment with strong session management capabilities in order to mitigate the risk of man-in-the-middle attacks that are prevalent in untrusted networks. An effective mobile access solution can provide secure access to enterprise systems with technologies such as VPNs, but due to multi-tasking nature of mobile users, it also should include the ability to maintain multiple secure connections. A robust mobile access management solution can prevent unauthorized access to enterprise systems, enforce consistent enterprise policies and assist in demonstrating compliance.

A standards-based mobile access manager enables seamless security for corporate data and applications without impacting user productivity. Different layers of secure access can be provided for mobile employees, customers and partners.

Safe mobile applications: Where policies and standards pay off

Beyond device- and access-related challenges, enterprises also can encounter serious security vulnerabilities in mobile applications. Malware can be hidden within applications downloaded from public application stores. Individual business teams, such as marketing or sales, may build ad-hoc applications to seize market opportunities or serve growing demand—but a lack of security understanding and structured development processes may introduce risks. The rapid adoption of new technologies may lead to gaps in the security of mobile applications. In addition, mobile applications often support multiple interaction points, increasing the threat surface area.

Increasingly, organizations are building, connecting and running mobile applications for their employees, customers and partners. But few if any enterprises can create all the mobile applications their users demand; they will turn, as a result, to third-party sources. In doing so, the organization must be vigilant in enforcing its security policies, as application creators may have lower security standards—or they may not have performed security testing at all. Enterprises can guard against traditional viruses targeting their mobile applications by validating that devices have not been jailbroken or rooted. To counter the emerging rogue application threat that results from malicious code or data being injected into vulnerable applications, enterprises must validate whether or not the application has been modified since the last interaction.

Enterprises, in other words, can take a proactive approach to mobile application security. It can be costly and time-consuming to apply patches and resolve vulnerabilities after applications are deployed—but the latest security products automate the application security testing and risk management process. The organization should select a mobile application platform based on its ability to provide support for developers to easily incorporate security features such as the encryption of local application data during the design and build processes. From development to testing, solutions can scan applications, identify vulnerabilities and generate reports of security gaps. And problems can be remediated before applications are deployed—designing security into the applications rather than applying it after the fact.

Mobile security intelligence: Awareness that leads to action

New user behavior and new threats will always precede security best practices. In the dynamic and inherently social and consumer-oriented mobile world, new device and application capabilities introduce new types of interaction that users might practice before IT is aware. As emerging threats uncover new vulnerabilities and target their attacks, security typically requires monitoring across various security solutions—so it, too, may lag.

Failure to develop security awareness and countermeasures, however, is not an option. Not only do security breaches carry monetary consequences under governmental regulations, but in an increasingly competitive world, they can result in the loss of business opportunities and trust relationships with customers, partners and employees.

It is imperative, as a result, to develop security intelligence based on the ability to aggregate security events from across all mobile security elements, analyze findings and develop actionable insights to support compliance, audit and business requirements.

As the workforce becomes increasingly mobile, security for their devices, access and applications will become an even higher priority for the enterprise. Hackers will continue to find and exploit vulnerabilities. The types of devices, platforms and applications will continue to escalate. But an adaptive approach to mobile security can help manage risks and destroy threats.

Conclusion

In today's mobile enterprise, security is a key business enabler, allowing employees to safely take advantage of the benefits that smart mobile devices offer. User behaviors, technical vulnerabilities and rapidly evolving threats pose challenges, but organizations can achieve protection and reliability by aligning security measures with their operational priorities. They can achieve an affordable and manageable solution with a phased approach that assimilates mobile security into existing technologies and the organizational culture.

The integrated and comprehensive IBM approach to security provides the core security structure that modern organizations require. Delivering a holistic approach to business-driven security, IBM solutions are designed to ensure that the correct people have access to the correct assets at the correct time, that critical data is protected in transit or at rest, that emerging threats are identified and that protection is provided across IT ecosystem.

For more information

To learn more about IBM mobile security solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/mobile-security

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

About the authors

Darren Argyle, *CISSP CISM*
IBM Global Security Solutions Leader
Email: darren.argyle@uk.ibm.com
twitter.com/D_Argyle

Vijay Dheap
IBM Global Product Manager for Mobile Security
IBM Master Inventor
Email: vdheap@us.ibm.com
twitter.com/dheap

[1] Alex Cocotas, "Smartphone Market Forecast: Sales Will Exceed 1.5 Billion Units a Year by 2016," *BI Intelligence*, February 2012. http://articles.businessinsider.com/2012-02-29/research/31109566_1_smartphones-pc-sales-mobile-phone-sales

[2] Forrester Research, "Mobile is the New Face of Engagement," February 2012. http://www-935.ibm.com/services/us/igs/secure-mobility-infographic.html

[3] Michael Finneran, "2012 State of Mobile Security," *InformationWeek*, May 2012. http://reports.informationweek.com/abstract/21/8792/security/research-2012-state-of-mobile-security.html

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2012

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

♻ Please Recycle