Securing the mobile enterprise with IBM Security solutions

Enable secure access to critical data and applications, while mitigating the risk of mobile malware

Highlights

- Unlock the potential of enterprise mobility by addressing the full spectrum of mobile risks
- Secure the device, protect critical content and applications, and enable safe mobile transactions
- Extend mobile security beyond just your employees to enable trusted transactions with your customers and partners
- Deliver confidence that the mobile environment is secure and data is safe with an intelligent, integrated and comprehensive approach to mobile security

When you have a smartphone or mobile device, the world is at your fingertips. Every day, there are new possibilities for mobile entertainment, shopping, banking, connecting socially and getting work done. But the speed at which mobile technology is changing has created dangerous gaps in security, and cybercriminals have taken notice.

At the same time, addressing the increasing number and sophistication of cyber threats is more challenging than ever. In today's mobile enterprise, the lines are blurred between personal and corporate assets, and IT organizations have to do much more than simply protect a corporate-owned device. In fact, the protection of personal data, ranging from electronic health information to financial records, is often mandated by evolving government regulations worldwide.

To meet these challenges, IBM has developed a comprehensive portfolio of mobile security solutions that address four key mobile security challenges: protecting devices, content, applications and transactions. The portfolio also includes a unique layer of security intelligence for advanced threat detection. IBM Security solutions emphasize an intelligent, integrated and innovative approach that can help your organization stay ahead of emerging threats, manage operational risks and lower the cost of maintaining a strong security posture.

Reducing mobile security risks

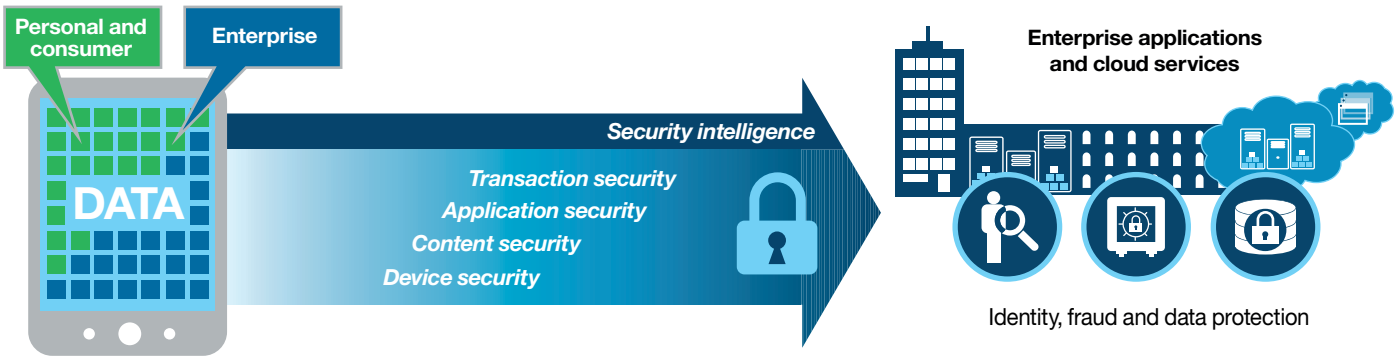
Around the world, the adoption of mobile products and services is growing exponentially. For example, nearly half of all smartphone owners have used mobile banking in the past year, according to a recent study conducted by the US Federal Reserve.[1] Plus, while bring-your-own-device (BYOD) programs are increasingly popular, organizations must also secure the mobile interactions of contract or temporary workers, business partners, and customers. An IBM Institute of Business Value study found that mobile devices are increasingly used for a wide range of work activities previously restricted to desktops. However, of the 81 percent of organizations that have personal devices accessing their networks, only 48 percent have a well-defined security strategy.[2]

The simple fact is that mobile technology has introduced significant risks, and the threats reach far beyond lost and stolen devices. Today's attackers take advantage of device jailbreaking, rooted devices, rogue applications, social engineering, mobile malware, mobile phishing and more. IBM Business Partner Arxan Technologies Inc. recently found that 78 percent of the top mobile applications have been hacked.[3] And with the explosive growth of both free and paid applications, hackers have a strong incentive to keep evolving their techniques and attack methods.

Taking an integrated approach to mobile security

IBM supports an intelligent, integrated and innovative approach to addressing the security challenges bombarding today's mobile enterprises. The comprehensive portfolio of IBM mobile security solutions can meet your needs for trusted, high-quality interactions at the device, content, application and transaction levels. In addition to helping manage *containerization* and *app wrapping*—that is, the separation of enterprise applications and data from personal applications and data—IBM solutions deliver a protective layer of security intelligence for correlating events across the enterprise and facilitating proactive responses. This way, organizations can help prevent identity theft, reduce the risk of fraud and protect all types of critical data.

IBM mobile security framework



Device security

Mobile devices go everywhere, making them more susceptible than traditional, stationary systems to attack, loss, infection or compromise. Enterprise mobile management, as a result, should range from the enrollment and provisioning of devices, to the monitoring of security policies and configuration compliance, to the ability to locate the device and remotely wipe corporate data from the device.

With MaaS360 by Fiberlink,[4] an IBM company, organizations can balance the enterprise security and employee privacy demands of BYOD programs. The solution offers dual-persona management for enterprise applications, secure email, web browsing and secure document sharing—helping separate work and personal data via containerization. Devices can be enrolled and secured in minutes with this on-demand, software-as-a-service solution. It also supports self-service enrollment, customized over-the-air configuration and automated policy enforcement.

Content security

With the increasing need for mobile productivity, organizations are faced with the challenges of securing file and document sharing across mobile devices. Mobile content management should give organizations a simple, scalable way to distribute, manage and secure documents on smartphones and tablets—without requiring management or control of the physical devices.

MaaS360 enables organizations to deploy a dual-persona experience from its Trusted WorkPlace container on mobile devices. It helps provide secure access to corporate content—including behind-the-firewall resources such as Microsoft SharePoint and cloud repositories such as Box—while also reducing the risks of data leakage. Individual users or documents can have their own security policies, creating a highly personalized and compliant experience. Security policies can restrict the copying, pasting and sharing of sensitive data inside the container. In addition, organizations can monitor the status and usage of specific documents, users and devices.

Application security

Poor coding practices and human error, combined with the relative ease with which hackers find and exploit these vulnerabilities, can make application security the Achilles' heel of enterprise security initiatives. What's more, compromised devices can increase the risk of fraud and create an insecure environment for business-critical applications and transactions. Today's enterprises must be able to verify the security of their own, in-house applications, while also enabling runtime risk detection, tamper resistance and enhanced control via "whitelisting" or "blacklisting" of applications.

IBM® Security AppScan® enables organizations to secure native and hybrid mobile applications. It helps IT staff identify and remediate mobile application security risks on mobile devices as well as the servers accessed by mobile applications. AppScan leverages extensive research of mobile operating systems—including Google Android and Apple iOS—to provide comprehensive security analysis. In fact, more than 40,000 mobile application programming interfaces have been added to the AppScan security knowledgebase. AppScan runs on popular mobile development platforms, such as Apple OS X, which helps developers to identify application security risks early in the software development lifecycle. This is one of the most efficient ways to develop secure code and protect mobile applications against data leakage.

In addition, IBM Worklight® offers organizations a secure platform for developing, testing and managing safe HTML5, hybrid and native mobile applications. The solution provides an integrated development environment (IDE) that helps

safeguard mobile security at the device, application and network layers. Organizations can use Worklight to protect sensitive personal data with an encrypted offline cache, for example. Plus, Worklight provides strong authentication mechanisms to help ensure that only authorized users have access to protected resources. Worklight also integrates with AppScan to make it easy to develop and secure applications within a single IDE.

Transaction security

As mobile devices become the preferred way to get things done, preventing unauthorized transactions by mobile users becomes a top requirement for all organizations. But with the latest attacks reaching across online and mobile channels, transaction security is more challenging than ever.

Trusteer[5] Mobile solutions dynamically detect the risk factors of the underlying device. This information is delivered to the native or web-based mobile application, as well as the application back-end services, to help secure transactions from devices to the back office. Application functions can be restricted based on mobile risk assessments, or organizations can require additional authentication if certain risk factors are detected. Furthermore, mobile transaction risk can be correlated with cross-channel risk factors to detect complex fraud schemes.

IBM Security Access Manager for Mobile helps organizations deliver secure access to mobile and web applications with authentication and authorization services, single sign-on and session management. It helps improve identity assurance with built-in support for flexible authentication schemes, such as the use of one-time passwords and RSA SecurID tokens. It also helps enforce context-aware access by integrating with Trusteer Mobile Software Development Kit (SDK) and Worklight runtime security features. Plus, it supports device finger printing, geographic location awareness and IP reputation techniques.

When deployed with IBM Security Access Manager for Web, organizations can also help shield mobile applications from many of the common web application security risks. These IBM solutions are available as either virtual or physical appliances to help simplify configuration and deployment.

Security intelligence

With attacks on devices, applications and transactions growing more numerous and more sophisticated by the day, it is more important than ever for organizations to have visibility into security events to help defeat advanced threats and spot malicious insiders. Security intelligence and event management (SIEM) solutions can help organizations identify trends across the millions—or even billions—of security events collected every day, so they can prioritize the events that require immediate action.

IBM Security QRadar® SIEM uses event correlation to help organizations quickly identify potential offenses and eliminate false-positive results. Unusual user, application and network activity can trigger automatic alerts to security teams, who can then investigate the potential offenses and proactively manage the remediation or mitigation. For example, when a device normally used in the US starts accessing the network from abroad, it could just mean an employee is travelling. However, when this event is correlated with the transfer of hundreds of confidential documents, the organization can quickly understand that a security breach has occurred and take action.

QRadar SIEM is part of IBM QRadar Security Intelligence Platform, a unified architecture for integrating real-time SIEM, log management, anomaly detection, and configuration and vulnerability management. As a result, organizations can take advantage of advanced threat detection, ease of use and lower cost of ownership.

Building security into the mobile application development lifecycle

While mobile security is often discussed in terms of IT management, application developers also must consider how to build security into their application designs. Mobile application development is faster and more iterative than traditional development; plus, developers have to deal with multiple device platforms and methodologies. They have to securely integrate into back-end enterprise services as well as cloud delivery platforms, and be ready to scale appropriately—even when demand occurs in less predictable patterns. What's more, there are often unique mobile requirements to manage, such as a user interface with significant restrictions in terms of real estate.

IBM mobile security solutions can help simplify each phase of the mobile application development lifecycle, enabling developers to:

- Design the optimal end-user experience across mobile devices and application types (web, native and hybrid)
- Instrument the application for analytics, risk detection, tamper proofing and management control
- Integrate with back-end data, systems and cloud services
- Test the application by using a vulnerability analysis tool to scan applications and identify risks automatically
- Distribute the application using a combination of internal and external app stores
- Manage authentication, enforced updates and versioning
- Apply risk-based analysis of business-critical transactions
- Analyze and improve the effectiveness of the application design by viewing detailed customer usage patterns

Why IBM?

IBM mobile security solutions are part of the IBM MobileFirst strategy of providing end-to-end solutions for the mobile enterprise. Based on nearly 6,000 customer engagements, more than 10 mobile-related acquisitions in the last four years, a team of thousands of mobile experts and 270 patents in wireless innovations, IBM MobileFirst combines the key elements of an application and data platform with the management, security and analytics capabilities needed for the enterprise.

For more information

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

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

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

[1] Deirdre Fernandes, "Banks struggle to keep up with mobile demand," *The Boston Globe*, July 14, 2013. https://www.bostonglobe.com/business/2013/07/13/mobile-apps-gain-popularity-banks-try-keep/qshfqhvKts7DlGZfAoF76K/story.html

[2] IBM Institute for Business Value and Oxford Economics, "The 'upwardly mobile' enterprise: Setting the strategic agenda," *IBM Corp.*, October 2013. http://www.oxfordeconomics.com/Media/Default/Thought%20Leadership/white%20papers/IBM%20upwardly%20mobile/2013_10_02_5650_Full_Report__The_upwardly_mo.pdf

[3] Arxan, "State of Security in the App Economy: 'Mobile Apps Under Attack," *Arxan Research Report*, Volume 2, 2013. https://www.arxan.com/assets/1/7/State_of_Security_in_the_App_Economy_Report_Vol._2.pdf

[4] Fiberlink Communications was acquired by IBM in December of 2013.

[5] Trusteer, Ltd. was acquired by IBM in September of 2013.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2014

WGS03019-USEN-00