Securing the mobile enterprise with IBM Security solutions

Gain visibility and control with proven security for mobile initiatives in the enterprise

Highlights

- Address the full spectrum of mobile risks with enterprise-class security
- Secure the device, protect access to enterprise resources and enable safe mobile applications
- Empower mobile employees, partners and customers with responsiveness and productivity
- Deliver confidence that the mobile environment is secure and data is safe with visibility and an adaptive approach to mobile security

Technology adoption traditionally has begun in the enterprise and then diffused into the consumer segment. But with mobile technologies, the pattern has been reversed. Enterprises of all types and sizes have adopted mobile computing for its potential not only to provide the communications that consumers enjoy, but also to improve productivity, responsiveness and innovation. By 2015, some 40 percent of enterprise devices are expected to be mobile.[1]

Mobile adoption, however, is not without its pitfalls, and a major concern for organizations today is how to manage and mitigate the risks associated with mobile interactions. Providing security for mobile devices, it turns out, is significantly different from providing security elsewhere in the enterprise. That's because mobile devices themselves are different—they are shared more often, used in more locations, fulfill more roles and are more technically diverse. Half of mobile applications transmit personal details or device information.[2] Threats from rogue applications and social engineering, as a result, are expected to double by 2013.[2]

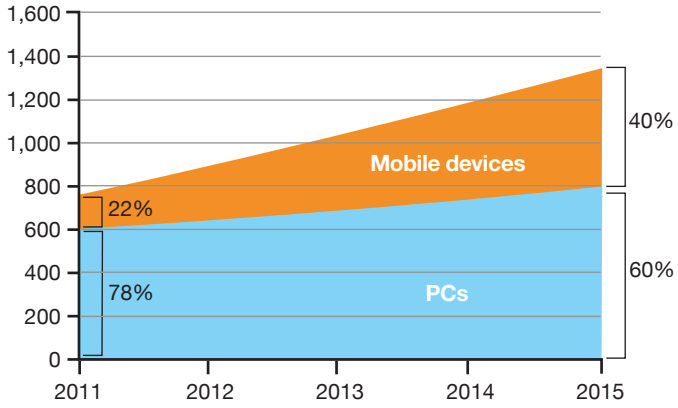
To meet this challenge, IBM has developed a portfolio of mobile security solutions spanning IT domains—people, data, applications and infrastructure. IBM capabilities emphasize an adaptive approach to security that can drive down costs, is secure and is just as dynamic as today's business climate. For organizations designing mobile services, deploying data and workloads to mobile devices, or consuming information

from mobile-based services, IBM solutions can meet critical requirements for managing operational risk and adhering to security priorities.

As mobile adoption grows, so do threats to mobile security

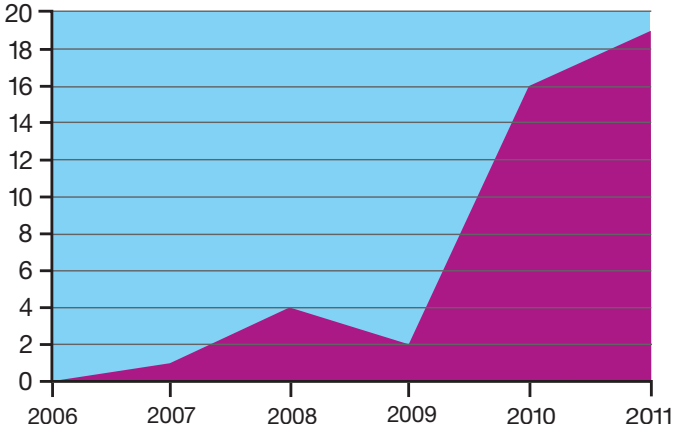
The projections tell a compelling tale: one billion enterprise smartphones and 1.2 billion mobile workers expected by 2014—with large enterprises tripling their smartphone user base by 2015.[2] The adoption of consumer-owned rather than enterprise-dedicated devices in 85 percent of large companies by 2014.[2] Half of organizations planning to deploy their own mobile applications within 12 months.[2] But with rapid adoption come mounting threats. The need to maintain business agility and to support changing employee behaviors not only will feed continued growth in the use of mobile devices, it will require organizations to find ways to mitigate the operational risks associated with mobility.

Growth in enterprise devices by type[1]



Mobile operating system exploits[3]

2006 - 2011



While enterprises have learned security lessons from the PC and Internet era, mobility brings both new challenges and the evolution of previous ones. At the top of the threat list are lost and stolen devices, but rogue applications, social engineering, malware, identity theft, stolen data, malicious websites and denial of service are becoming more sophisticated and are constantly on the increase.

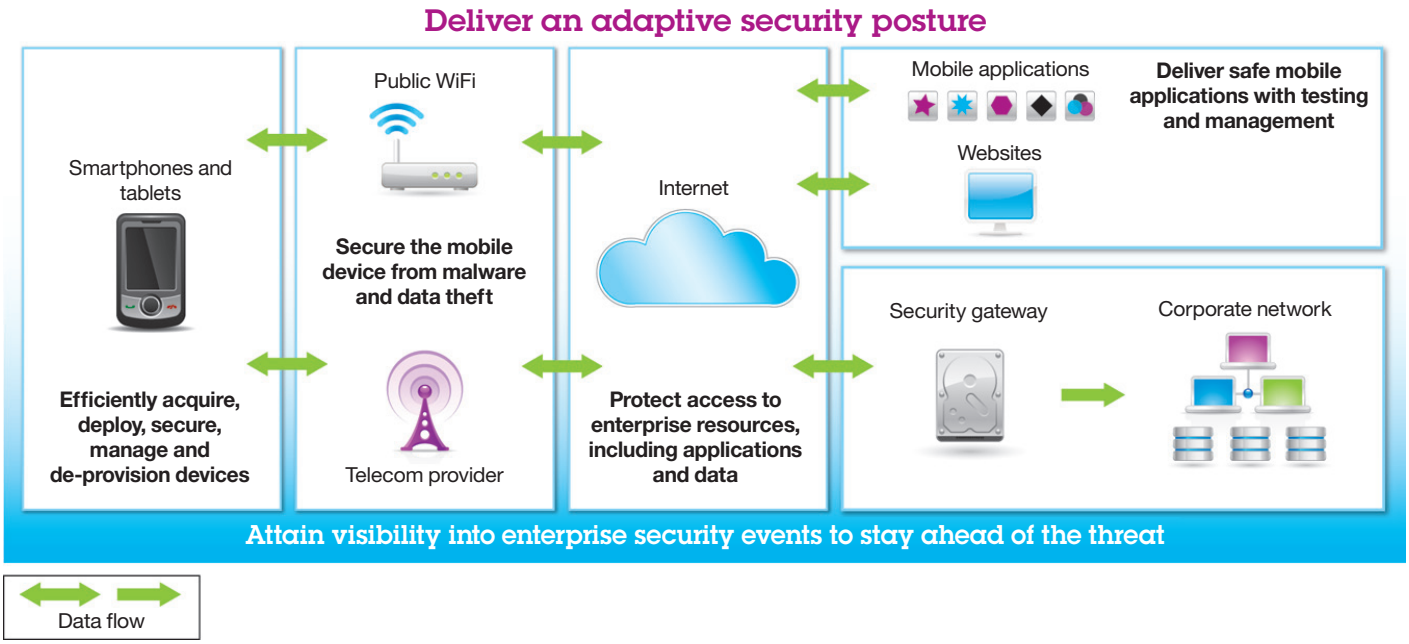
At the same time, the diversity of platforms and applications, general lack of enterprise visibility and control, and increased complexity in demonstrating regulatory compliance make it more difficult for IT to support mobile initiatives. Most mobile platforms are not natively designed to provide comprehensive security, and with the explosive growth in numbers of mobile devices, hackers have a strong incentive to develop new techniques or create attacks aimed specifically at these devices.

Organizations must therefore put into place tools and processes that enable them to meet threats designed to exploit mobility-related vulnerabilities, including:

- Credentials that enable access to business or personal accounts
- Sensitive data such as confidential business or personal information
- Device communication services
- The mobile device itself, which can be a jumping-off point to accessing other corporate resources

Follow the flow of data

Unprotected endpoint devices are like open doors into sensitive information. Organizations need to guard the data on those devices—whether the data is at rest or in motion over unsecured networks and infrastructure. Data protection must be the primary objective when developing an enterprise mobile strategy. Effective security for mobile environments should therefore be designed to follow the flow of data and to defend that data from unauthorized access. The design of an adaptive security posture should include policy management and security intelligence to guide the overall initiative as well as capabilities for protecting data throughout the mobile lifecycle.



With diverse devices in use throughout the enterprise—especially when the organization has adopted a "bring your own device" (BYOD) policy—it is first necessary to put into place comprehensive, cross-platform capabilities for managing and securing devices and applications. Secure access to enterprise assets should include secure connectivity with capabilities for managing identities, access and authorization. Conduct vulnerability testing of mobile applications to support the organization's trust relationships with customers, employees and business partners. Visibility into the full data flow is important for keeping the mobile security program ahead of constantly growing threats.

In the world of mobility, more so than in traditional IT environments, it is important that the security model adapt to the user rather than requiring the user to comply with mandates. Another reason for security to adapt to the user is that attacks tend to be more targeted at individuals, departments or organizations rather than being general, mass attacks. It is important to remember that user behavior is different when the issues are mobile devices and mobile access—more emphasis is placed on avoiding disruption of the user experience. The security model that adapts to a user's mobile context—for example, location, type of content accessed, time of day or risk profile—and that has minimal impact on user experience will help ensure compliance with security policies and ultimately assist in securing enterprise data.

The IBM portfolio ensures business-driven mobile security

IBM takes a holistic approach to mobile security requirements, using the well-established IBM Security Framework as a reference. IBM Mobile Security solutions help customers address challenges in mobile device management, access management, application security and security intelligence. Each not only delivers mobility-focused capabilities, but is designed to extend and complement existing IT security infrastructures, policies and procedures. Designed to help organizations transition from being reactive to taking the initiative in a constantly changing mobile security landscape, IBM solutions emphasize an integrated, end-to-end security model with visibility across the enterprise, as well as facilitate proactive responses.

People: Simplifying identity and access management

As mobile becomes the preferred screen for many users, preventing unauthorized access by mobile users becomes a top requirement for all organizations. But controlling mobile access, while sharing many of the same objectives with controlling traditional access infrastructures, presents very specific challenges.

IBM Security Access Manager for Mobile protects access to enterprise resources by authenticating and authorizing mobile users and their devices. This single infrastructure can be employed for all types of users, while also addressing some of the unique requirements of mobile access control. IBM Security Access Manager for Mobile provides solid session management capabilities to prevent man-in-the-middle attacks and affords the flexibility to employ multiple authentication and authorization schemes to validate both the user and the device. It also integrates with IBM Worklight to deliver seamless user and application security.

Ongoing development in IBM Security Access Manager for Mobile will deliver context-aware authentication and authorization. Organizations will be able to leverage the contextual information a mobile device provides to compute a risk profile and employ appropriate controls.

Data: Securing sensitive information

Safeguarding sensitive data and reducing the risk of unauthorized access is core to any mobile security initiative. IBM Endpoint Manager for Mobile delivers data security on the mobile device. It enforces the compliance of device configurations with enterprise security policies and employs platform facilities to enforce data encryption. This solution provides remote device lock and both full and selective data-wipe capabilities while providing the infrastructure to deliver anti-malware solutions. It can also require that virtual private networks be used to protect sensitive data communications.

IBM Worklight offers developers application-level data security by providing facilities with the tools needed to encrypt their applications' data.

In addition, subscription-based IBM Hosted Mobile Device Security Management is a turnkey software-as-a service (SaaS) solution that provides assurance of data security and policy compliance with anti-malware, anti-theft, lock and wipe features—all delivered from the cloud.

Applications: Fortifying mobile-deployed web applications

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. With the projected dramatic increase of enterprise mobile applications, security must keep pace.

The security features of IBM Worklight enable organizations to efficiently develop, deliver and run safe HTML5, hybrid and native mobile applications with direct updates and application validation. IBM Security AppScan® detects vulnerabilities in mobile web applications, in the web elements of hybrid mobile applications and in Android applications through static analysis during development. The IBM WebSphere® DataPower® message protection and XML firewall capabilities guarantee the integrity of message content and protect application programming interface calls.

Infrastructure: Protecting mobile endpoints and connections

Mobile endpoints go everywhere, making them more susceptible than traditional, stationary devices to attack, loss, infection or compromise. Mobile device management, as a result, should range from the acquisition and registration of devices to providing secure communications via virtual private networks, to password and configuration compliance.

IBM Lotus® Mobile Connect enables secure connectivity from mobile devices to backend systems, while IBM Endpoint Manager for Mobile Devices gathers and delivers detailed device information to assess compliance. IBM Endpoint Manager can also be used to identify compromised mobile devices—including "jailbroken" or "rooted" ones—and restrict their connections to the enterprise network.

Security intelligence: Visibility into activity and threats

With attacks on devices, applications and access growing more numerous and more sophisticated daily, it is more important than ever for organizations to have visibility into events and the environment. Comprehensive visibility can identify vulnerabilities before they can be exploited or attacks before they can take effect.

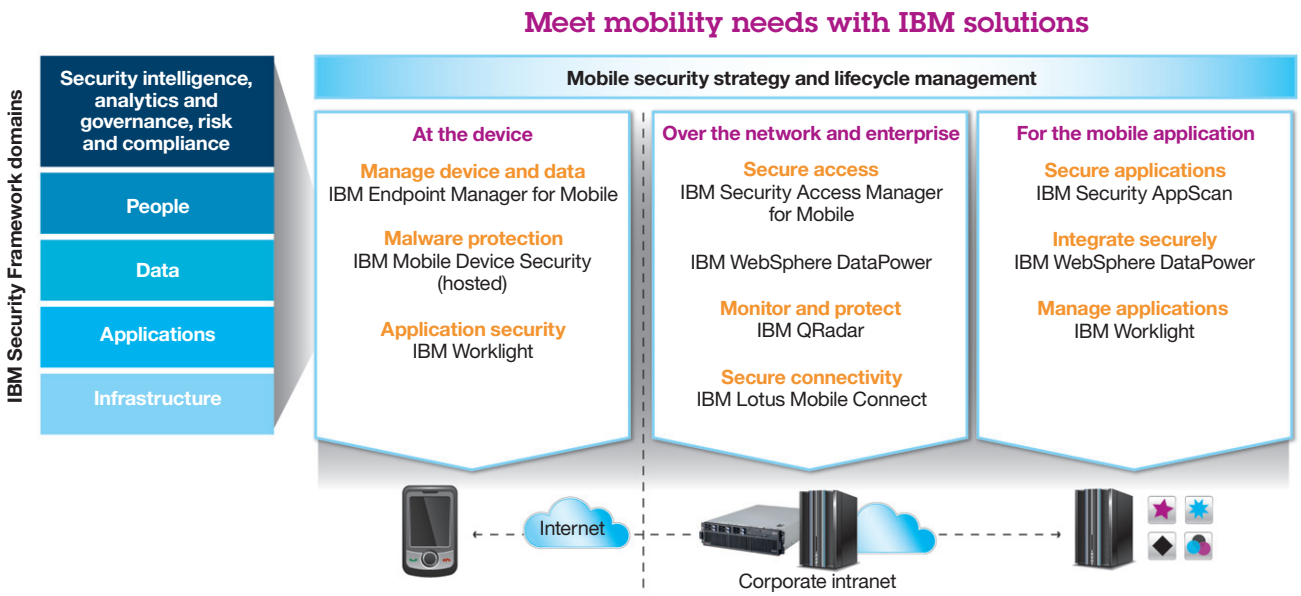
IBM QRadar offers a unified collection, aggregation and analysis architecture facilitating the consumption of security logs from IBM Worklight; security events from IBM Endpoint Manager for Mobile Devices and IBM Access Manager for Mobile; vulnerability data from IBM Security AppScan for Mobile; as well as configuration files and network flow telemetry. IBM QRadar also includes forensic capabilities to support security investigations and audits.

Mobile enterprise security roadmap

No matter how capable a mobile security solution is, its value is greatly diminished if it cannot be efficiently deployed or easily managed. The organization needs to carefully assess the overall risks to the enterprise and the effort required for initial roll-out and ongoing management of a solution. To help build an effective mobile enterprise strategy and roadmap, IBM can deliver a range of comprehensive professional security services, either directly or through local business partners.

Building on technology leadership and worldwide engagements with organizations across industries and of all sizes, IBM takes a risk-based approach to securing the mobile enterprise with the following steps:

- Securing the mobile device:
  - Capture detailed device information and identify non-compliant devices; detect "jailbroken" or "rooted" devices
  - Enforce security best practices and take corrective action including updates, denying or removing access, virtual private network configuration and delivery of anti-malware solutions
  - Remotely locate, lock and perform selective wipes when devices are lost, stolen or decommissioned
  - Leverage a single infrastructure to deliver controls for a broad set of enterprise endpoints including smartphones, tablets, desktops, laptops and servers
- Protecting access to enterprise resources:
  - Deploy context-aware authentication and authorization of mobile users and their devices
  - Support mobile-friendly open standards such as OAuth
  - Implement strong session management and protection
  - Extend the infrastructure employed for protecting access from any endpoint with the ability to address requirements unique to mobile computing
- Delivering safe mobile applications:
  - Support developers with security features including data encryption, direct updates and application validation
  - Perform vulnerability assessments during development, testing and runtime to mitigate the risk of deploying unsafe applications
  - Employ a secure channel through which to deliver mobile applications to enterprise mobile users
  - Offer a secure runtime environment for mobile applications that enables centralized management with application locking
- Attaining visibility and delivering an adaptive security posture:
  - Generate reports on compliance
  - Assess consistency of security policy enforcement
  - Be proactive in responding to emerging threats and adapt to changing user behaviors



IBM case study: European bank delivers secure mobile Internet banking

With dual goals of extending secure access to banking applications to mobile customers and enhancing the ability of employees to perform secure transactions via mobile devices, the bank is targeting popular Google Android and Apple iOS platforms, with future support for Microsoft Windows Mobile-based devices. Using IBM Security Access Manager for Mobile to authenticate requests and the IBM Worklight platform to support backend services, the bank safeguards its trust relationship with customers with data encryption and timely application updates.

Why IBM?

With IBM solutions, organizations can support mobile employees, enable mobile collaboration with partners and nurture customer relationships. They can realize new revenue channels as they reduce risk. They can ensure effective security for their mobile environments with capabilities for mobile device management, mobile identity and access management, network and data protection, and mobile application security.

The industry-leading IBM X-FORCE® research and development team provides the expertise for a solid, preemptive security approach. The team provides reports documenting all aspects of threats that affect Internet security, as well as maintaining a comprehensive threats and vulnerabilities database that powers the preemptive protection delivered by IBM products. In addition, the team distributes alerts and advisories that provide information about how IBM products and services can protect against the latest threats.

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

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
July 2012

[1] IBM projection.

[2] Blackstone, "IBM Enterprise Mobility," September 12, 2011.

[3] IBM X-FORCE, "IBM X-FORCE 2011 Trend and Risk Report," March 2012.

Please Recycle

WGS03003-USEN-00