Securely Adopting Mobile Technology Innovations for Your Enterprise Using IBM Security Solutions

Redguides
for Business Leaders

Arun Madan
Sridhar Muppidi
Nilesh Patel
Axel Buecker

■ Understand mobile computing business patterns and associated security risks

■ Secure and monitor mobile device, data, enterprise access, and applications

■ Realize mobile enterprise security strategy using IBM Security Solutions

Redbooks

Executive overview

Many organizations around the world are undergoing a mobile business transformation to achieve higher efficiencies, improve client relations, and increase business growth. There has been immense growth in mobile device and tablet sales. With easy-to-use interfaces, and the convenience to connect and collaborate with ever-increasing network bandwidth from almost anyplace, the *mobile revolution* has engulfed consumers and workers from all generations.

Organizations want to make use of these technology innovations for the workforce, and for reaching a larger number of clients and business partners. However, C-level executives, information security experts, and risk professionals are faced with the challenge of securing the organization's information and application data on a variety of mobile devices.

Security has emerged as the most important aspect of this mobile revolution, because the organization's information and data are distributed beyond their secure perimeter. Also, transactions are run on mobile devices, which can be shared and are often personally owned. Security compliance for those devices is usually not managed by the organization.

The purpose of this IBM® Redguide™ publication about creating and maintaining a secure operating environment for mobile devices is to provide detailed insight into the following topics:

► The growing importance of mobile devices
► Emerging mobile computing business patterns and associated security risks
► Mobile security threats, vulnerabilities, and risks
► Mobile security implementation patterns
► IBM solutions for mobile security

This publication can help organizations adopt mobile technology innovations for their workforce and clients alike. Clients can be addressed with new personalized capabilities that have to be delivered in a secure and compliant manner. In addition, employees can be supported to stay on top of their key work activities and actions to maintain productivity and, at the same time, protect organizational data with state of the art security capabilities.

1

The growing importance of mobile devices

Market abundance of powerful, feature-rich smartphones, tablets, and other mobile devices, coupled with the availability of high-speed network bandwidth at affordable costs, has made it irresistible for people to use mobile devices for work, infotainment, and games. Smartphones and mobile devices have become part of the lifestyle across generations, and people find it convenient and productive to use their mobile device for both personal and work situations.

Employees expect that they should be able to conduct all of their business on their mobile device, rather than on company-issued notebook computers for this purpose. Clients expect that all information and business transactions should be accessible from a mobile device. Mobile computing has become a way of life, and is part of the culture of the younger generation entering the workforce in coming years.

Organizations across the globe have risen to the cultural challenge of mobile computing, and have started to adopt mobile technology innovations to enhance client convenience and employee productivity. Organizations initially adopted mobile technology for senior executives, later followed that for employees, and now use mobile technology to transform their business, sales, and supply chain operations.

Organizations look at mobile computing as a way to *boost sales*, *improve agility*, and *reduce costs*. Organizations want to provide employees the option of using a personally-owned device as a way to reduce cost, and to allow them to work wherever or whenever they need to, but doing so requires diligence in protecting the organization's information.

Figure 1 shows that the growth in mobile devices for work, called *bring your own device* (BYOD), will be 40 percent by 2015 as per IBM projection. This is based on research by a number of different analysts.
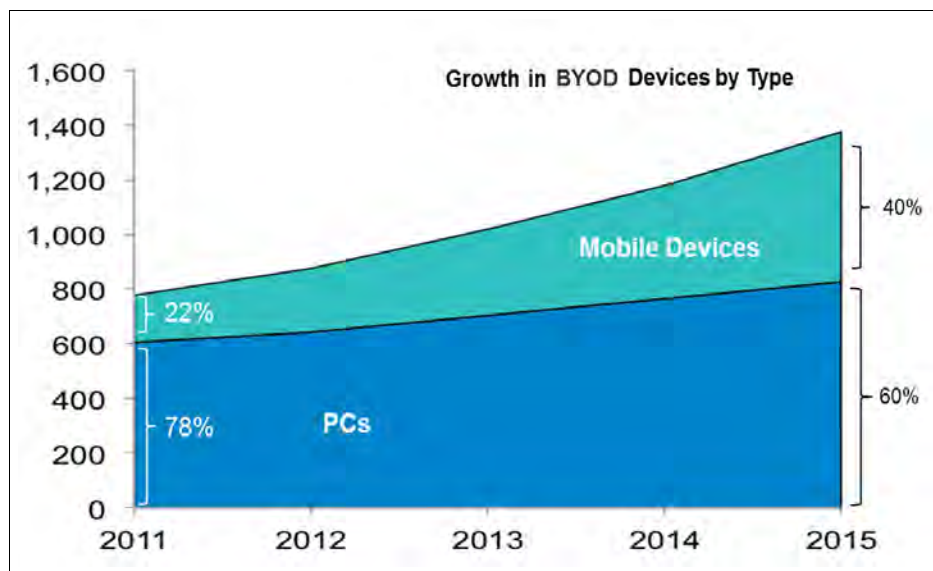

Figure 1   BYOD device growth (IBM projection)

A concise mobile computing policy for employees allows them to use their own mobile devices for business and personal activity. Organizations are tasked with supporting the new social, virtual, and mobile employee applications. Mobile threats are on the rise. Managing complex IT environments and security risks, maintaining policies, and helping organizations control costs are primary concerns for many Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and security and risk professionals.

Organizations have to ensure that *all risks to an organization's information* are mitigated through appropriate controls, because the cost to an organization that results from data or information loss can be enormous. These risks are likely to grow as mobile devices get more ubiquitous, smaller, and, unfortunately, easier to lose on a taxi, at the airport, or on a restaurant seat. Mobile security risks are bound to increase over time as more users bring their own mobile devices to work.

The challenge for executives is to accommodate requests for broad mobile access while protecting organizational information, delivering business value, and defining a mobile strategy that can be constantly adapted to changing technologies. A set of executive challenges related to mobility, including business-to-employee (B2E) and business-to-consumer (B2C), is depicted in Figure 2.
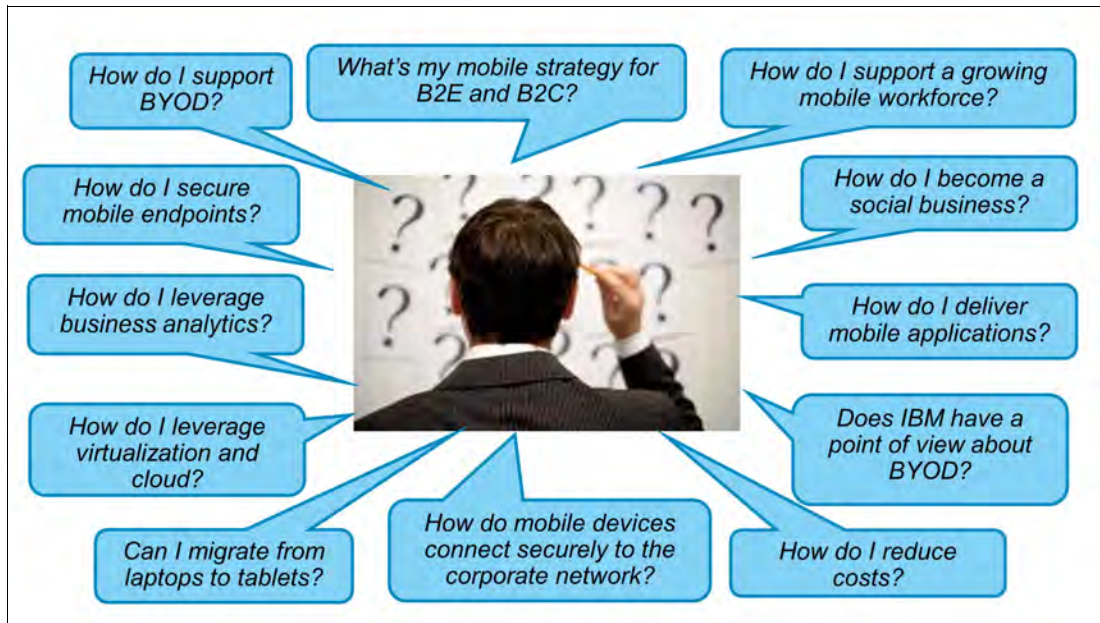

Figure 2   C-level executive challenges due to mobility

Emerging mobile computing business patterns and associated security risks

Mobile computing business patterns can be categorized based on mobile application ownership, its distribution, and its usage. Mobile devices can be used to carry out transactions and exchange information using a public cloud, a private cloud, the corporate network, or other devices (such as a notebook). Risks associated with the public cloud are considered highest, where other devices are rated medium. The lowest risks can be attributed to the private cloud and corporate network.

The level of risks, and the required security controls, vary according to the organization's use case patterns. The following sections more closely examine these patterns:

► For employees and business partners
► For clients or consumers
► For businesses

For employees and business partners

In this use case pattern, organizations publish applications for use by their employees and business partners (for example, applications delivering collaboration and communication solutions). The required security controls vary based on the application, the intended users, and the type of information used by the application.

The distinction between employees and business partners is important, because application use by business partners requires additional security considerations. Figure 3 on page 5 depicts risk and management complexity (on a scale of low, medium, high, and very high) for employees and business partners. The figure includes some use case examples:

► Collaboration

Collaboration applications (for example, email, instant messaging, or calendars), have a risk and management complexity level from *low to high*. They require minimal security controls (except for sensitive data, which needs to be handled in an encrypted manner).

► Productivity

Productivity applications (for example, Salesforce) have a *high* risk and management complexity level. They require adequate security controls, such as two-factor authentication, role-based access control, virtual private network and (VPN) communications.

► Efficiency

Efficiency applications (for example, Patient Monitoring) have a *very high* risk and management complexity level. In some countries, such as the US, these applications can be highly regulated, requiring stringent security controls, risk-based access control, audit logging, and monitoring.

For clients or consumers

Applications for clients or consumers are published by organizations to cover, for example, account self-care, client relations management, product catalogs, and sales. The level of attention to security usually depends on the type of application, and also on the culture of the organization. Use cases might include the following examples:

► Financial

Financial applications (for example, Mobile Banking handling money transactions) have a *very high* risk and management complexity level. These types of applications are often regulated, and require stringent audit logging and transactional integrity.

► E-commerce

E-commerce applications (for example, online sales) have a *high* risk and management complexity level, and require logging and transaction reversal in case of failure.

► Client interaction

Client interaction applications providing information (for example, flight schedules) have a *low to high* risk and management complexity level. These applications require minimal security controls, such as name and passenger name record (PNR) number for mobile check-ins.

Figure 3 on page 5 shows the risk management and complexity (on a scale of low, medium, and high) for clients or consumer applications.
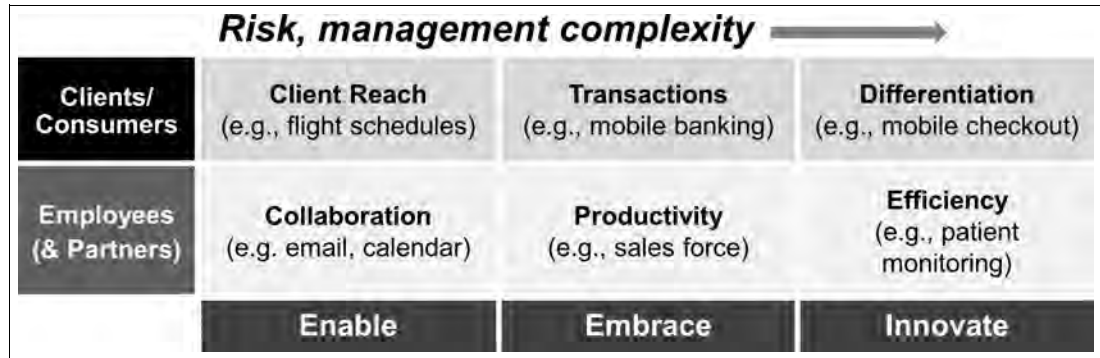
Figure 3   Risk and management complexity

For businesses

Mobile applications for use by other business organizations are published by managed service providers or independent software vendors (ISV), and are offered to other organizations. These applications are offered either as software or *software as a service* (SaaS). The applications also have to meet the highest level of security standards. They might be targeted towards clients, consumers, or employees of other businesses. There are different considerations for the service providing and consuming organizations:

► SaaS provider

  The service provider offering its applications to businesses needs to provide the highest level of security integration based on its client's business requirements.

► Service consumer

  Service consumer organizations (for example, the business that uses the SaaS application) require the ability to assess and mitigate risks to ensure an adequate level of security controls. The required security controls can vary from business to business based on their risk profile.

Mobile security threats, vulnerabilities, and risks

In this section, we take a closer look at the following security threats, vulnerabilities, and risks:

► Loss or theft of mobile devices
► Mobile device malware
► Mobile software vulnerabilities
► Mobile user behavior vulnerabilities
► Phishing
► Bluetooth and WiFi risks
► Spam
► Regulatory and compliance risks

Loss or theft of mobile devices

Loss and theft are some of the highest risks with mobile devices, because a majority of these devices can contain sensitive and confidential information. Suppose that a device contains intellectual property, regulated or sensitive data, or confidential information about the organization. If it gets into the wrong hands, it might result in loss of reputation, financial loss, or legal action.

Lost data can affect employee productivity for prolonged periods, because normally it is not backed up. Also, dependency on mobile devices constantly increases because they are so easy to use.

Lists of calls, text messages, and calendar entries can provide a lot of information to malicious hackers for potential misuse against the organization. Mobile identity theft is another serious consequence, because many applications and services link the digital identity to the mobile device.

Mobile device malware

Mobile device malware exists in various forms today:

► Viruses and worms

   Self-replication software that can quickly spread from device to device through application download, email, bluetooth, multi-media messaging services (MMS), and so on

► Trojan horse

   An application that appears to be a valid program but contains code to make unknown use of the device

► Spyware

   An application that hides itself to monitor the activities on the device, such as short message service (SMS), email, and phone calls

Malware can cause the loss of personal or confidential data, incur additional service charges (for example, some malware can send premium SMS text messages or make phone calls in the background), and, even worse, make the device unusable. More seriously, it can be used for gaining access to privileged information, stealing identities, carrying out financial transactions, gaining root access to devices, or installing spyware for tracking user activities.

Because most mobile devices now have Internet connections, common network-based threats that have previously attacked notebooks or desktops can now also apply to mobile devices. A device connected through WiFi or Bluetooth can even be at greater risk, because the WiFi source or the Bluetooth-enabled device might have been compromised.

When compromised, it can play a role in a *man-in-the-middle attack* (when a hacker configures a notebook, server, or mobile device to listen in on or modify legitimate communications) or other attack type.

When a device is not *jailbroken* or *rooted*, the threat to back-end application programming interfaces (APIs) is more dangerous than the threat to the device content alone.

Malware on mobile devices has been on a steep rise in the past few years, because most mobile platforms do not yet provide native mechanisms to detect malware. Hackers have recognized the opportunities to make financial gains by using malware to steal confidential data on the devices. No mobile platform available today is immune to malware.

Emerging mobile threats are getting more personalized, and are targeted to individuals or organizations. Using social engineering, rogue applications, malicious websites, and multiple means (for example, mobile borne denial-of-service (DOS) attacks, identity thefts, and man-in-the-middle attacks), hackers target mobile users to achieve financial gains.

There is little capability to perform code reviews for mobile applications that are available in the application stores from platform vendors. This provides hackers a haven to create and spread malware. To make it difficult to develop malware for mobile platforms, mobile operating

system vendors use an *application sandboxing technique* to limit application access to data and system resources outside the sandbox.

Traditionally, mobile platforms, such as Symbian and Windows Mobile, have been a proving ground for malware developers. Today, Android devices are experiencing the most malware development, primarily due to their increasing popularity and open software distribution model. Apple has been able to curb malware on its devices with a controlled application review process and distribution model through their application store. Microsoft is taking a similar approach for its mobile Windows platform.

Mobile software vulnerabilities

Because many mobile platforms are not natively designed to provide comprehensive security, hackers have a strong incentive to develop new techniques, or to create mobile-centric malware specifically for these devices. In a traditional information technology (IT) world, patching is the solution used to overcome operating system (OS) vulnerabilities.

In the mobile paradigm, however, patching is more complex. This is because it requires over-the-air (OTA) updates to multiple applications and operating systems, patch distribution, and patch-level sync up with multiple devices. Patching might require firmware or syncing up through a computer. It can involve the OS vendor, device vendor, and application vendor.

A recent IBM X-Force® security research report[1] shows that mobile operating system vulnerabilities have increased significantly (see Figure 4), and exploits of vulnerabilities are also on the rise (see Figure 5 on page 8).
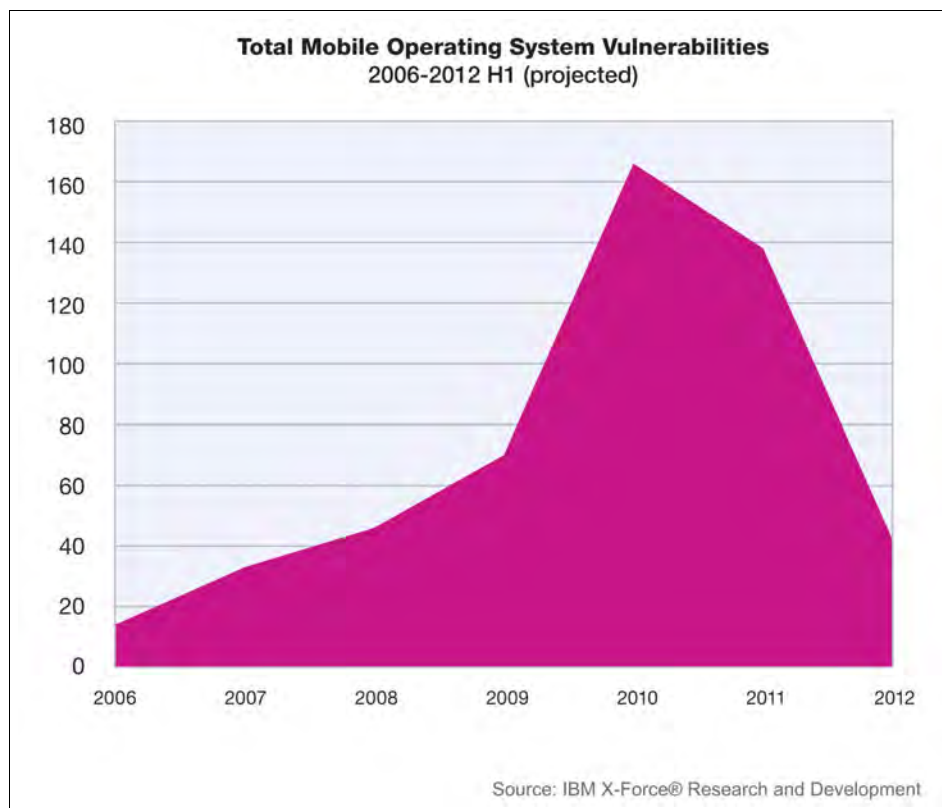

Figure 4   Mobile operating system vulnerabilities

---

[1] You can find the latest IBM X-Force trend reports at
   https://www.ibm.com/services/us/iss/xforce/trendreports/

Mobile Operating System Exploits
2006-2012 H1 (projected)
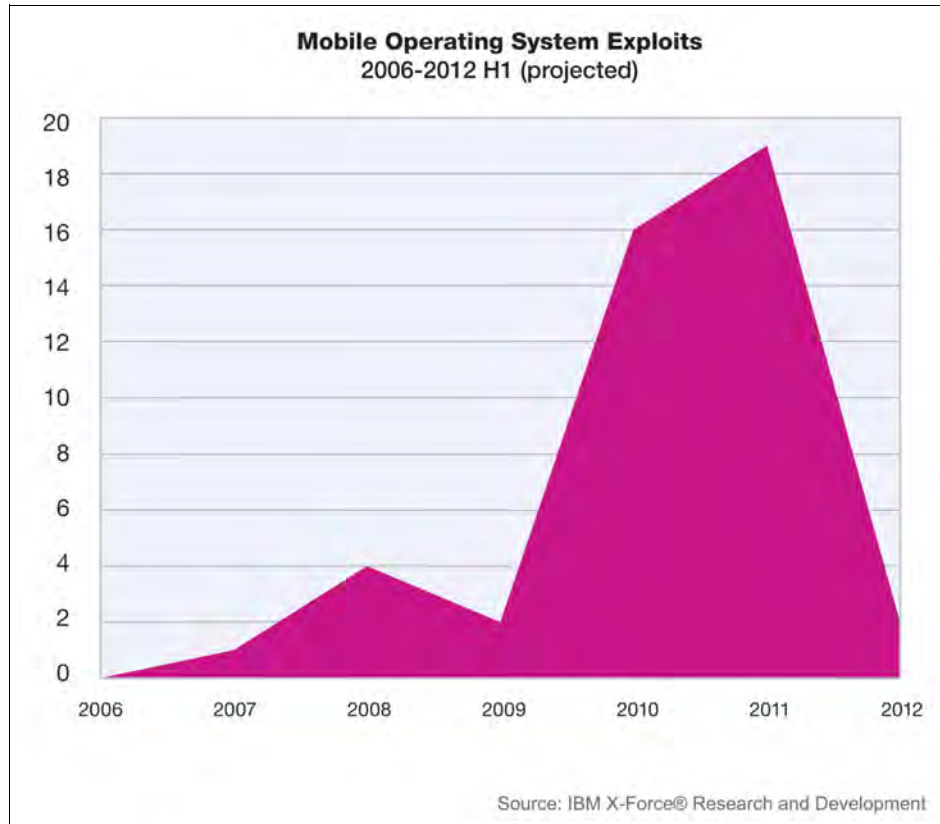
Source: IBM X-Force® Research and Development

Figure 5   Mobile operating system exploits

In the first half of 2012, reported mobile vulnerabilities and exploits are down to the lowest levels since 2008. The IBM X-Force team thinks there are several reasons for this:

► First, mobile operating system developers continue to invest in both in-house discoveries of vulnerabilities and enhancements to their security models to prevent vulnerabilities from being exploited.

► Second, as is typically the case with a relatively new area, such as mobile, we see a pattern. It begins with a spike in discoveries, with easier bugs found quickly, and then the ones that are more difficult to exploit are left. There is often a lag in time between researchers and attackers discovering techniques to overcome previously perceived limitations.

As mobile devices become a primary computing device for many (both in large organizations and the Internet at large), we might find that patching vulnerable devices becomes a primary security concern. This is because this area has had the least progress made in the past year or so.

When mobile devices are not patched in a timely manner, the situation leaves room for attack, especially when vulnerabilities are published and there is a time lag before patching. Organizations can use a mobile device management platform to overcome delays in deployment of patches on a large number of mobile devices and applications.

Mobile user behavior vulnerabilities

Organizations are at risk of exposing information because of intentional or unintentional mobile user behavior:

► Using private or public clouds to store enterprise data might result in the distribution of sensitive enterprise data to unknown storage accounts across the globe.

► Using public mail and messaging accounts to collaborate and communicate can put the organization at risk, because these public accounts mostly operate with far less stringent security parameters (such as encryption).

► Jailbreaking a device by the mobile user to install certain applications might result in the device getting exploited, sometimes without the user even knowing. The device might get jail broken by visiting a website.

Phishing

Phishing is an email or an SMS text message (dubbed *SMiShing*) that is sent to trick a user into accessing a fake website, sending a text message, or making a phone call to reveal personal information. For example, the user might reveal a Social Security Number in the United States, or credentials that would allow a hacker access to financial or business accounts. Phishing has already caused a tremendous amount of financial loss every year in the personal computer world, and will cause similar damage via the mobile channels.

Phishing through mobile browsers is more likely to succeed because the small screen size of mobile devices does not allow for some protection features used on the PC, such as web address bars or warning lights. In some cases, universal resource locators (URLs) might not show full domain names on mobile devices.

Although site authentication is recognized as an effective approach to thwart phishing, many commercial websites have not adopted it. Also, it still requires the users to get involved in verifying the authenticity of the website (as we know, user behaviors are not trustworthy in achieving security on the Internet).

Bluetooth and WiFi risks

Bluetooth and WiFi are not threats by themselves, but are effective communication channels and mechanisms to increase the connectivity of mobile devices within a certain range. They can be easily exploited to infect a mobile device with malware or compromise transmitted data.

A mobile device can be lured to accept a Bluetooth connection request from a malicious device. Hackers can use their notebook or desktop to pretend to be a valid *WiFi hotspot* so that a man-in-the-middle attack can be played to intercept and compromise all data sent to or from the connected devices.

Many users leave their mobile devices in a discoverable mode, allowing other Bluetooth-enabled devices to find them and initiate connections. A user often accepts a connection request without any trust relationship established with the other communicating device. It is also a risky operation to connect to a WiFi network available in a public area without any knowledge about its genuineness.

Spam

With the increased popularity of text messaging, spam (unsolicited communication sent to a mobile device from a known or unknown phone number) is also on the rise. Spam can take the forms of instant messages (IM), short message service (SMS), multimedia message service (MMS), email, or phone calls.

Spam is not only a concern for mobile service providers, because it wastes a significant amount of bandwidth, but it is also a growing security issue for mobile device users. According to a recent study, the majority of mobile spam attacks are for financial gain. For example, it could include fraudulent financial services, rather than the traditional advertising scenarios found in email spam.

Regulatory and compliance risks

There is increased pressure on organizations because of government regulations and compliance posture. The penalties for security breaches are not only monetarily expensive, but they could result in reputation loss, and damage trust relationships with clients, business partners, and employees.

Organizations need to build security intelligence by implementing tools for monitoring, logging, and controlling access to, or distribution of, sensitive organizational data. Of course, they must take care not to infringe on the privacy of the individual's personal data on the mobile device.

Mobile security implementation patterns

Organizations need to understand the risks to their information. They must consider the organization's culture and governance system, network and technology environment, types of mobile applications to be deployed, and country-specific regulatory requirements. To protect organizational data and intellectual capital, they need to create transparent, understandable, flexible, and executable mobile security policies to protect against risks related to the use of mobile devices.

The policy should be based on security controls involving people, processes, applications, and technology. The security controls should have the following characteristics:

► Enforceable on cross-platform mobile devices
► Centrally managed by the organization
► Simple to implement and support
► Flexible for administering users and devices
► Focused on preventing the loss or theft of organizational data
► Auditable in all of its parts
► Tested and verified in terms of disaster response
► Attentive to possible external threats

The first task of any organization that wants to support mobile collaboration is determining what type of overall policy to implement. BYOD is not correct for every organization. Some government agencies and certain financial institutions, for example, do not allow any BYOD mobile access to their networks. At the other end of the spectrum, there might be some organizations that fully embrace the mobile trend, allowing all of their employees mobile access to virtually all corporate applications and all data from any device and any place.

In these early stages of mobile collaboration, most organizations fall somewhere in the middle, providing some employees and devices access to some information and applications. This access model will most likely be staggered according to organizational roles.

Salespeople are granted access to certain corporate data and applications; the accounting staff is granted access to a different set. Guests to a corporate campus might only be able to use its wireless local area network (WLAN) for secure Internet access.

Therefore, before implementing a solution, business and IT leaders must understand user segments and their needs, determine their application and collaboration strategies, and formulate their overall employee device policies. To begin planning an effective mobile strategy, consider the following questions:

► What information and applications does each employee role need access to?

► Which of our employees travel, including travel from campus to campus?

► What are these employees' specific access needs?

► What type of access should be granted to campus guests, contractors, or business partners?

► What types of collaboration applications do we need to extend to mobile employees in order for those employees to work most effectively?

► Do we envision broadening our mobile policy as time passes, to allow more users, access, and devices?

With answers to these questions at hand, an organization is better prepared to begin building a technological roadmap for its network, taking into account how the network supports the other key elements of a mobile collaboration solution, devices, and applications. Also consider the following questions:

► Which type of mobile devices should we support?

► How do we plan to secure the network?

► How do we plan to manage and secure individual devices?

► What will we do to provide adequate bandwidth?

► How do we build the network and provision devices so that employees can move seamlessly from network to network?

Figure 6 depicts the visualization of mobile security for an organization.
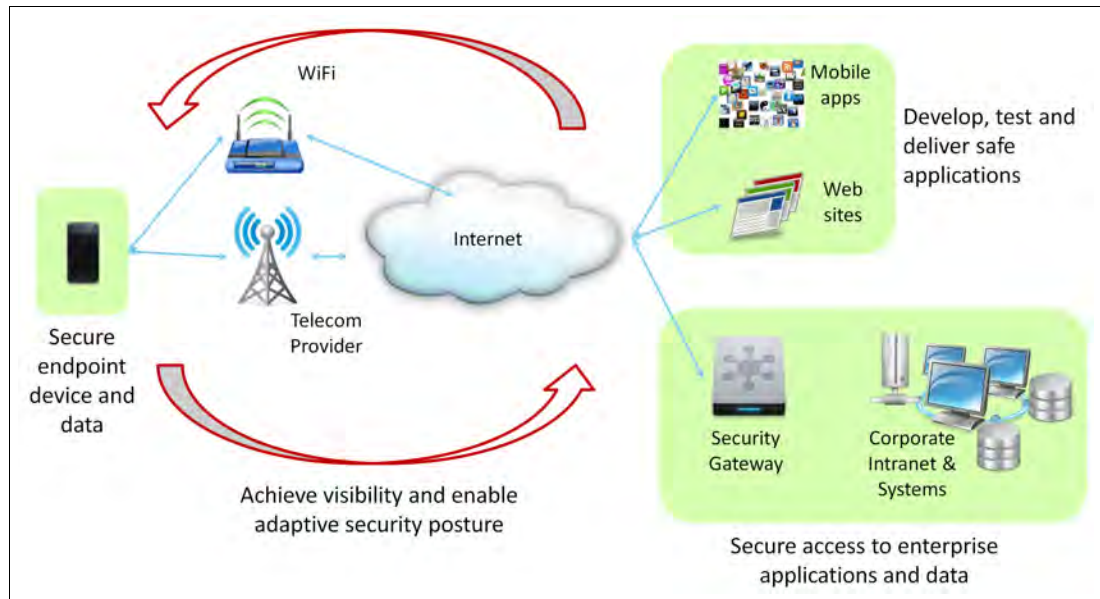

Figure 6   Visualizing mobile security

Let us now examine why mobile security implementation requires a strategy for securing three levels:

► The mobile device
► The network or channel
► The mobile application

Figure 7 depicts how risk mitigation controls for mobile security need to be deployed at all three levels.
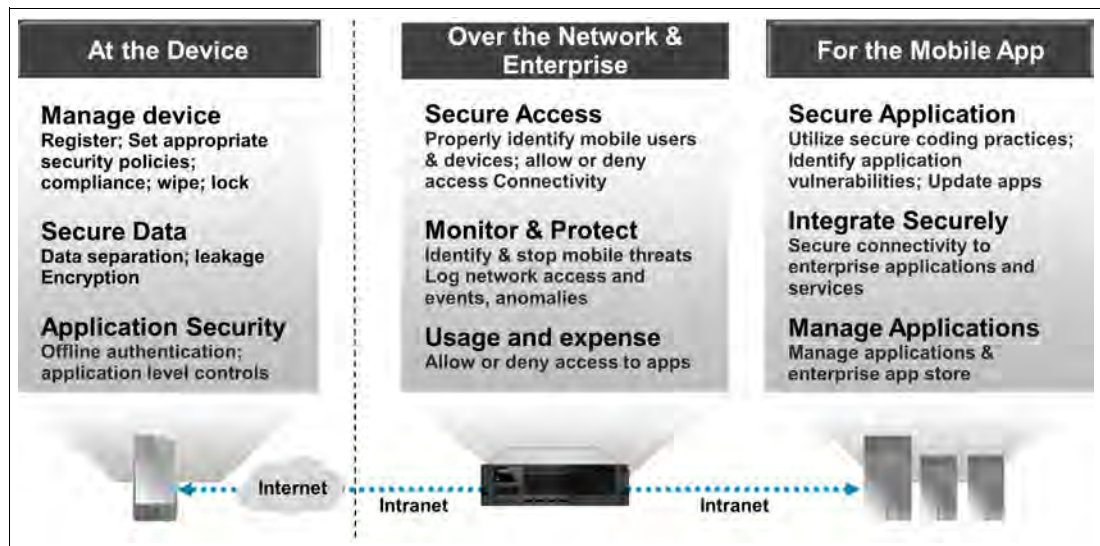

Figure 7   Mobile security implementation

Securing the mobile device

Most mobile devices are targeted toward the consumer market. The mobile platform vendors usually provide cool features convenient to users, with only rudimentary security capabilities built in as optional features.

For employees that want to participate in a BYOD scenario, organizations want to centrally manage the mobile devices used by those employees to conduct business. Although the degree of device management mandated definitely varies by organization based on their risk profile and the applications that have to be managed, the mobile device security management can involve delivering security notifications, proactive software updates, and anti-malware capabilities.

To manage devices and enforce corporate security policy, organizations use *mobile device management* (MDM) platforms. The MDM platform can also perform policy compliance assessments, device wipes, application management, and device lockdowns.

Organizations that want to manage mobile devices typically require their employees to install an agent or a mobile application embedded with a management agent. Each user then has to register and activate the device before it can be used for business. Given the management resources required, self-management capabilities can be offered to the employees to improve the responsiveness of the solution.

MDM solutions help organizations manage multivendor mobile devices through a central console, and help to enforce good practices:

► Password for user authentication

► Automatic locking if the device is idle for a certain period of time

► Anti-virus software and signature updates

► Auto wipe or erasing of data after a certain number of failed password attempts

► Self-service to remotely lock, locate, or wipe sensitive enterprise data on a device if stolen or lost

► Securing sensitive enterprise data by using, for example, encryption, containerization, or virtualization

► Configuration restrictions and patch level check

► Check on jailbreaking or rooting the device

► Application blacklisting or white listing with the capability to un-enroll devices in case a vulnerability is detected

► Monitoring, alerting, and tracking policy violations and access to certain applications

► Remote administration of several functions:

   – Device enrollment
   – Provisioning of users
   – Asset management
   – Patch management
   – Software distribution
   – Software upgrades
   – Audit and compliance reporting

An emerging trend when deploying a *mobile device management* solution is to segregate the personal profile and the business profile on the mobile device, and to manage only the business profile.

Another approach is to use a *secure container*, which separates and isolates the organizational data from personal data. In this case, however, the user is restricted to work only with applications and data within the container. This can result in limitations on the user experience, and on the applications within the container.

Virtualization is yet another approach, in which an application is published using a *virtual desktop infrastructure (VDI)*. In this case, enterprise data never leaves the corporate server, and it results in achieving high security at low cost. A disadvantage, however, is that it provides a restricted user experience, and there is no offline usage possible.

For an optimized user experience with good data security, web applications (using HTML5) and native web applications should be used. If enterprise data is required on a mobile device, it should be securely transferred and stored by using encryption technology.

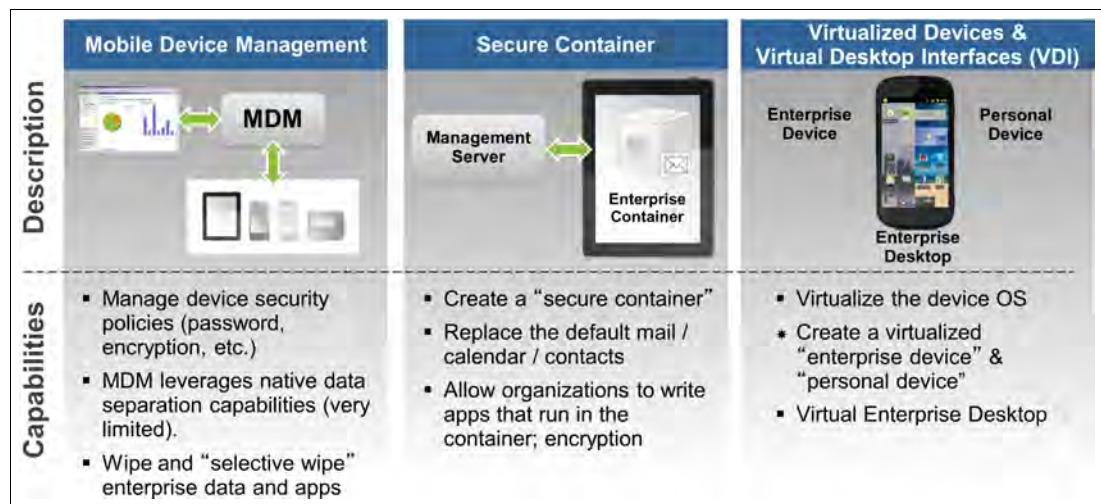Figure 8 depicts the three approaches used for mobile device data security.

Figure 8   Mobile device data security approaches

Users access mobile devices by entering a password or a PIN (when configured). The organization can enforce this by remotely using an MDM solution. Protecting access to enterprise applications and sensitive data on mobile devices requires strong authentication or two-factor authentication (2FA), and risk-based authentication (RBA).

Two-factor authentication often combines password authentication with a second factor, such as token- or certificate-based authentication, or a one-time password.

RBA is often used in banking and for highly secure and sensitive applications. It is more user-friendly, and can be employed in the background after the user has authenticated by using a basic user ID and password. RBA examines the risk level of the user access request and checks, for example, user ID, user location, device ID, analysis of user behavior, and usage patterns, to grant access to the transaction.

However, if indicators suggest an anomaly, or if the information requested is highly sensitive, the user is asked to provide additional authentication credentials. When RBA is used with single sign-on, it becomes highly convenient and productive for the users to access resources securely. RBA reuses the organization's existing single sign-on and identity management solution infrastructure.

There are other device feature-based methods, which can be deployed to authenticate a user:

- ► Near field communication (NFC) capabilities
- ► Touchscreens for capturing signatures
- ► Cameras for visual recognition
- ► Microphones for voice recognition

Securing mobile access to the network

The fundamental goal of any mobile collaboration or BYOD policy of an organization should be to provide employees with the best user experience possible. They should be able to easily and reliably access the information, applications, and mobile collaboration tools that they need to fulfill their jobs. Only by providing a consistent, high-quality user experience can the organization fulfill mobility's potential to bring value to the business by improving productivity and competitiveness.

The network has a critical role to play in meeting this goal. Networks need to deliver new levels of security while easing onboarding and access for legitimate users. They have to deliver a high level of performance. They need specialized tools to improve device manageability and control management costs. The best way to provide a quality user experience is by taking a comprehensive approach to modernizing the network, so that it can better support mobile devices and applications.

This approach entails assessing the current network, and then planning a network architecture and migration strategy that addresses new requirements for network security, device manageability, and service delivery. It is critically important for the network to determine what users and devices are accessing what information and applications, and from where.

This can be tricky, especially because users roam between corporate WLANs, cellular networks, and WiFi hotspots. Mobile device management tools can assist in this task, improving enforcement of access policies by granting employees access to only certain applications and data sets. However, proper network security is the first line of defense against these security risks.

Many organizations deploy automated network access control (NAC) tools to help secure mobile access to the network. These tools help IT place rules on mobile devices, determining who can access which enterprise data and applications, and from where. Automated NAC tools can also enable organizations to capture and push information to and from mobile devices.

For example, these tools can determine whether a device has up-to-date antivirus software before allowing the device access to the enterprise network, and send updates to the device if necessary. They can deny network access to non-compliant devices. If a device is lost or stolen, NAC tools can remotely lock it and, using the device's global satellite positioning system, find it.

When using enterprise applications, users have to create secure connections into the organization, and there must be adequate protection to keep the perimeter secure. A central location to manage and control access into the organization makes it easier to control and manage secure entry.

There are requirements for a mobile gateway into the enterprise that meet these needs:

► A VPN server that supports popular mobile device VPN protocols

► Advanced next-generation firewall capabilities to inspect traffic into and out of the enterprise for threats

► Access control to determine which users are granted access to which applications

VPNs are crucial to securing the organization's network, because they can provide an extra layer of protection beyond standard credentials when an employee is attempting to access corporate networks from cellular networks or WiFi hotspots. A VPN along with virtual desktop infrastructures can grant employees access to sensitive applications and data without having to store that data on the mobile device.

Alternatively, encryption technologies are available to protect data in transmission. A new trend is to migrate away from the device-level VPN and move toward an application-level VPN, because a device-level VPN allows malware to piggyback and hide inside the encrypted tunnel to eventually infect other application systems.

Every organization needs to perform a risk assessment to identify threats and vulnerabilities, log network access and event data, and monitor these logs to detect any anomalies. With personal and business data on a mobile device, organizations need to determine how much monitoring and control over data can be implemented without infringing on given privacy laws.

There might be a trade-off between managing the business risk and protecting the user's privacy. Monitoring and protection of enterprise data can be provided by a security intelligence and anomaly detection solution, which typically comes with a security information and event management (SIEM) platform at its core.

Of course, mobile devices will connect to many networks, not just a single *home* WLAN. Therefore, an enterprise network must be configured in such a way that employees can access corporate information and applications seamlessly as they transition from campus WLAN to campus WLAN, to cellular data networks, or to WiFi hotspots. Only in this way can mobility's promise of improved productivity be fulfilled.

However, it is too optimistic to believe that there will be enough bandwidth to support every user and every activity equally. That is why the need for bandwidth prioritization grows. Organizations have to consider how to provide the most bandwidth to those applications deemed most important to organizational goals. Put simply, organizations must decide, for example, if real-time collaboration applications should get more bandwidth than email.

Organizations need to be able to grant or deny access to applications based on usage or expense. Tools are available to automatically prioritize network flow, and assign users and devices to specific service classes. Similarly, these tools can prioritize applications, preventing secondary programs from using too much bandwidth.

Securing mobile applications

The real value of a mobile device in the workplace is in its capability to get work done, and that happens primarily through applications. Choosing between ready-to-use applications or custom development, application architecture, and security can be a daunting challenge. When selected, the mobile applications need to be installed on the users' devices, managed, tracked, secured, and monitored.

If users leave or move to new devices or platforms, applications need to be wiped or upgraded, often across broad geographies. Incorporating security into the development, delivery, and execution of mobile applications is important, because the application model is

the preferred user experience on mobile devices. Mobile applications must be considered just another kind of software: they are used to provide the business functions that a client is implementing.

Figure 9 depicts a typical mobile application development lifecycle.

Figure 9   Mobile application development lifecycle

There are two aspects to mobile application security. First, a *secure mobile application platform* that offers security services to all applications running on the platform. This can free application developers from implementing core security capabilities for each new application.

Second, *secure application development design* can consistently implement security policy into the development cycle for mobile applications. The secure application development design uses secure design considerations, code analysis or policy enforcement tools, and application testing, such as black box and white box testing. A proper development process should include certain characteristics:

► Secure design, including threat modeling
► Source code analysis of applications
► Mobile application security testing
► Vulnerability testing of web-based and hybrid applications
► Functional testing of web-based, native, and hybrid applications using device emulators

Attention to application security begins with the design stage of application development. Organizations must understand the following aspects of the operating environment for the mobile application:

► What information will be stored by the application within the mobile device?

► What information will be accessed by the application through the mobile device?

► What information will be transferred between the application on the mobile device and other remote applications or data stores?

Threat models should be used during the design to identify both the threats and expected mitigations for these threats.

It is important to note that, most likely, enterprise mobile applications have to integrate with existing applications and interfaces that are deployed across the organization. This aspect has to be taken into account during product planning, design, development, and test. A secure mobile gateway can help integrate the following functions into a single gateway to properly integrate mobile devices with existing enterprise applications:

► Mobile VPN
► Secure web gateway
► Mobile malware protection
► Data loss prevention (DLP)
► Wide area network (WAN) optimization
► Authentication
► Risk-based access control

Application security capabilities are required for all types of mobile applications (for example, web-based, native, and hybrid applications).

Native mobile applications are designed to run on a device's operating system and firmware. These applications are developed using native programming APIs provided by the mobile platform, which means that a customized version of the application needs to be developed for each platform. These applications can be distributed and installed on the devices through the respective application stores. Organizations can either set up their own application stores to control distribution, or they can use the device-dependent application stores.

Web applications use technologies, such as HTML5, client-side scripts, and JavaScript, and they generally work across multiple platforms and devices. Web applications can be wrapped in a native interface for easy download and installation from their application stores.

To ensure enterprise data security in mobile web, native, and hybrid applications, avoid using the native data store on the mobile device for storing application data. Rather, host the data on enterprise servers. Web applications with HTML5 can offer a rich user experience comparable to native applications, and still maintain data security, platform independence, and ease of distribution. Figure 10 depicts the different security measures required for the mobile application development lifecycle.
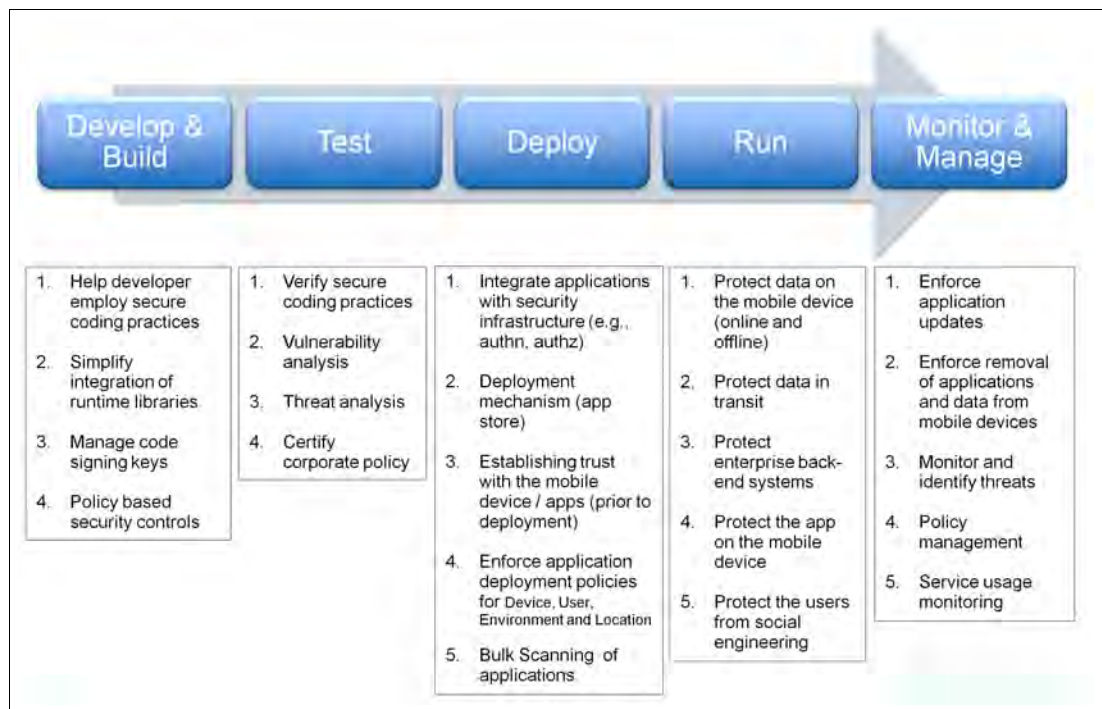

Figure 10   Mobile application security activities

IBM solutions for mobile security

IBM software offers solutions that provide mobile security and management capabilities:

► Build and connect enterprise assets
► Provide a mobile application development environment
► Improve enterprise systems to better manage and secure mobile devices and connections
► Extend and transform an organization's client relationships and internal processes

The following sections more closely examine mobile security:

- ► IBM MobileFirst solutions strategy
- ► IBM Mobile Security Reference Architecture
- ► IBM Mobile Security Framework
- ► IBM Mobile Security case study

IBM MobileFirst solutions strategy

The IBM MobileFirst[2] solutions strategy can help organizations transition from being reactive to taking the initiative proactively in a constantly changing mobile security landscape. IBM solutions emphasize an integrated, end-to-end security model with visibility across the enterprise, and they facilitate proactive responses.

IBM MobileFirst is the industry's most comprehensive mobile portfolio that, for the first time, links critical mobile software technologies, services, expertise, and an ecosystem of partners. Figure 11 depicts the IBM MobileFirst solutions strategy.

Figure 11   IBM MobileFirst solutions strategy

Mobile infrastructure strategy and planning

Mobile devices are at the heart of today's business, services, and operations, whether they are collecting global positioning data, supporting business transactions, or interfacing with the network to ensure optimal performance for technology functions. In a BYOD scenario, an organization can achieve significant cost savings because they are not purchasing hardware devices.

However, the resulting need to manage multiple operating systems and hardware platforms can cause additional expenses, and significant headaches for executives. Applications on

---

[2] To find more information about the IBM MobileFirst solutions strategy, visit
http://www.ibm.com/mobilefirst/us/en/

smartphones and tablets can move mobile business connectivity beyond voice and email, constantly increasing the need for more bandwidth and larger infrastructures.

Mobile application platform management

IBM software helps organizations strategize and build secure mobile applications, and then integrate these applications securely with back-end systems and storage. There are several key capabilities included in IBM solutions:

► Strategizing mobility
► Supporting diverse mobile devices
► Developing mobile applications
► Connecting applications with enterprise data, systems, and networks
► Optimizing bandwidth
► Managing the network and services

IBM solutions bring together key mobile foundation solution capabilities into a single integrated package that addresses a full array of challenges and opportunities. The *IBM Mobile Foundation* delivers a range of application development, connectivity, and management capabilities that supports a wide variety of mobile devices and mobile application types. The IBM Mobile Foundation includes the following solutions:

► IBM Worklight®

   An open mobile application platform for smartphones and tablets that can help organizations efficiently develop, run, and manage HTML5, hybrid, and native applications

► IBM Endpoint Manager

   A solution built on IBM BigFix® technology that addresses the issues of security, complexity, and BYOD policies that challenge support for an increasingly mobile workforce

► IBM WebSphere® Cast Iron® Hypervisor Edition

   An integration framework that enables organizations to rapidly connect their hybrid world of public clouds, private clouds, and on-premise applications

Managed mobility and mobile device security management

Managing and securing a mobile infrastructure represents a critical challenge. Because BYOD policies can potentially add large numbers of mobile users to the workforce, organizations need to secure transactions from virtually any device and any location.

At the same time, organizations must keep the network accessible, safe, and efficient, which includes enabling context-based security for cloud and mobile. Figure 12 on page 21 depicts the business need to manage and secure the mobile organization.
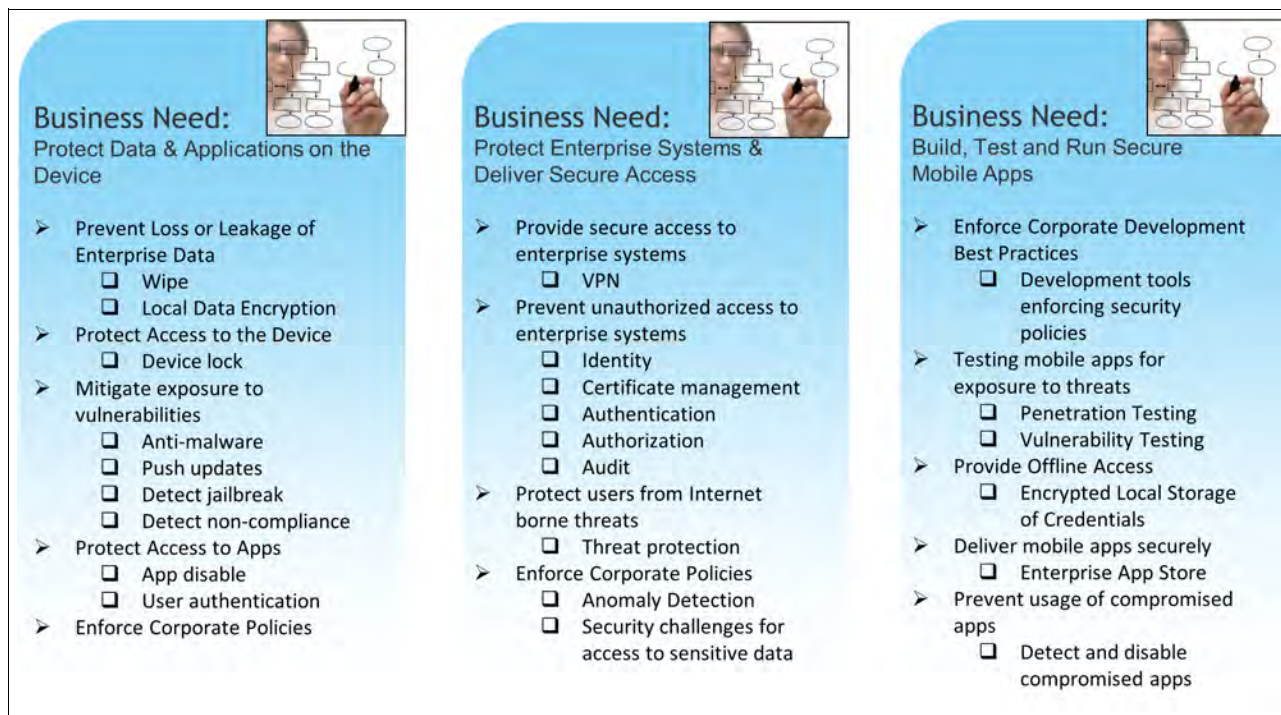
Figure 12   Business need to manage and secure the mobile organization

The IBM solutions that help manage and secure a mobile organization include infrastructure configuration and services that are required to manage and secure the mobile devices, applications, and data. The following section takes a closer look at these capabilities:

► Manage devices and applications

IBM provides a solution and services to help organizations gain real-time visibility into hardware, software, configuration, and location data, so that they can manage assets more efficiently. The solution allows an organization to oversee employee mobile devices as effectively as its own organizational assets, and it provides enhancements for business processes:

– Distribute and update mobile applications through an enterprise application store
– Unify the management of mobile devices, PCs, and servers
– Receive instant dashboard updates

► Secure data, applications, and devices

The IBM solution can help organizations defend against malware, provide security-enabled connectivity, and deliver security-conscious applications and application platforms. The IBM security solutions and services include several features:

– Mobile security risk assessments
– Mobile strategy and implementation
– Mobile application lifecycle management
– Device analytics and control
– Secure network and communications management

The key IBM security products include integrated dashboards and functionality to help secure any type of endpoint or network.

Mobility and wireless
IBM provides support for extending the existing business processes and business capabilities to mobile devices, and can help organizations with business transformation by creating new

opportunities. Key capabilities include mobile strategy, planning and implementation, and mobile-enabled solutions (including network optimization, analytics, commerce, social business, and mobile as a service).

IBM solutions help organizations to strengthen their business capabilities:

► Redefining the end-to-end mobile client experience
► Opening and expanding marketplaces
► Reaching consumers at the moment of decision by using location services
► Creating value through mobile capabilities that drive loyalty and satisfaction

IBM helps bring organizational employees and business partners the same benefits with efficient tools that ease the barriers to mobile collaboration, and help improve responses to emerging opportunities.

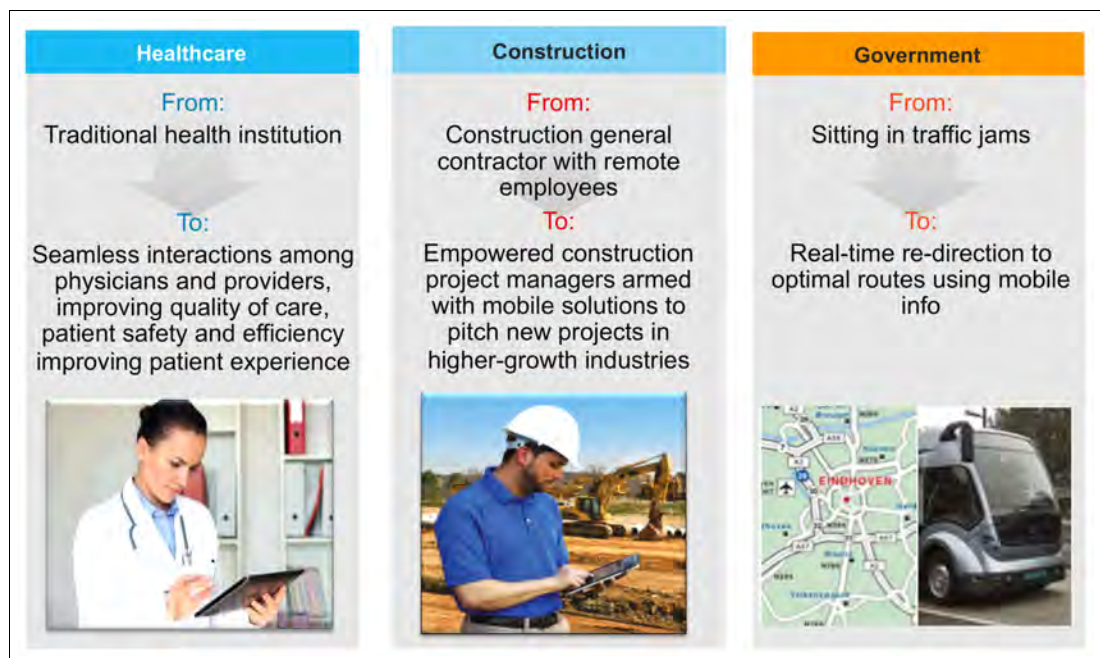Figure 13 depicts a variety of mobile-based business transformation examples.

Figure 13   Mobile-based business transformation examples

IBM Mobile Security Reference Architecture

The IBM Mobile Security Reference Architecture takes into consideration that mobile devices are computing platforms and communication devices. Therefore, mobile security is multi-faceted, driven by an organization's operational priorities.

For a comprehensive mobile security strategy, IBM factors in security capabilities in addition to the lifecycle of mobile devices and applications. The comprehensive IBM Mobile Security Reference Architecture extends vertically from the device platform all the way to back-end systems that are accessed by mobile devices.

As the device platforms offer more and more security capabilities to better address overall mobile security needs, these capabilities have been factored into the overall IBM Mobile Security Reference Architecture. In situations where the device platform security is not sufficient, solutions that extend the device platform are considered.

For example, a sandbox application environment or virtualization techniques can provide the ability to host multiple profiles on one device. These extensions can provide the ability to better enforce corporate polices at the enterprise container or profile level. This allows for more granular security controls (for example, encryption, application lifecycle management, data confidentiality, and data leakage prevention).

This approach works well in BYOD scenarios where some of the enterprise applications can potentially be engineered to work within the profile or the container.

The IBM Mobile Security Reference Architecture takes into consideration the security requirements of all types of mobile applications, which include web applications, native applications, and hybrid applications.

A mobile web application typically has minimal security on the device, and uses a server in the corporate data center for safeguarding a transaction. Alternatively, a native application can have comprehensive security capabilities within the application, and it can function or enforce the policies even in a disconnected mode. A hybrid application is a mix of both mobile and native, where the security capabilities depend on the specific requirements of the application.

Figure 14 depicts the IBM Mobile Security Reference Architecture along with IBM product-based solution names.
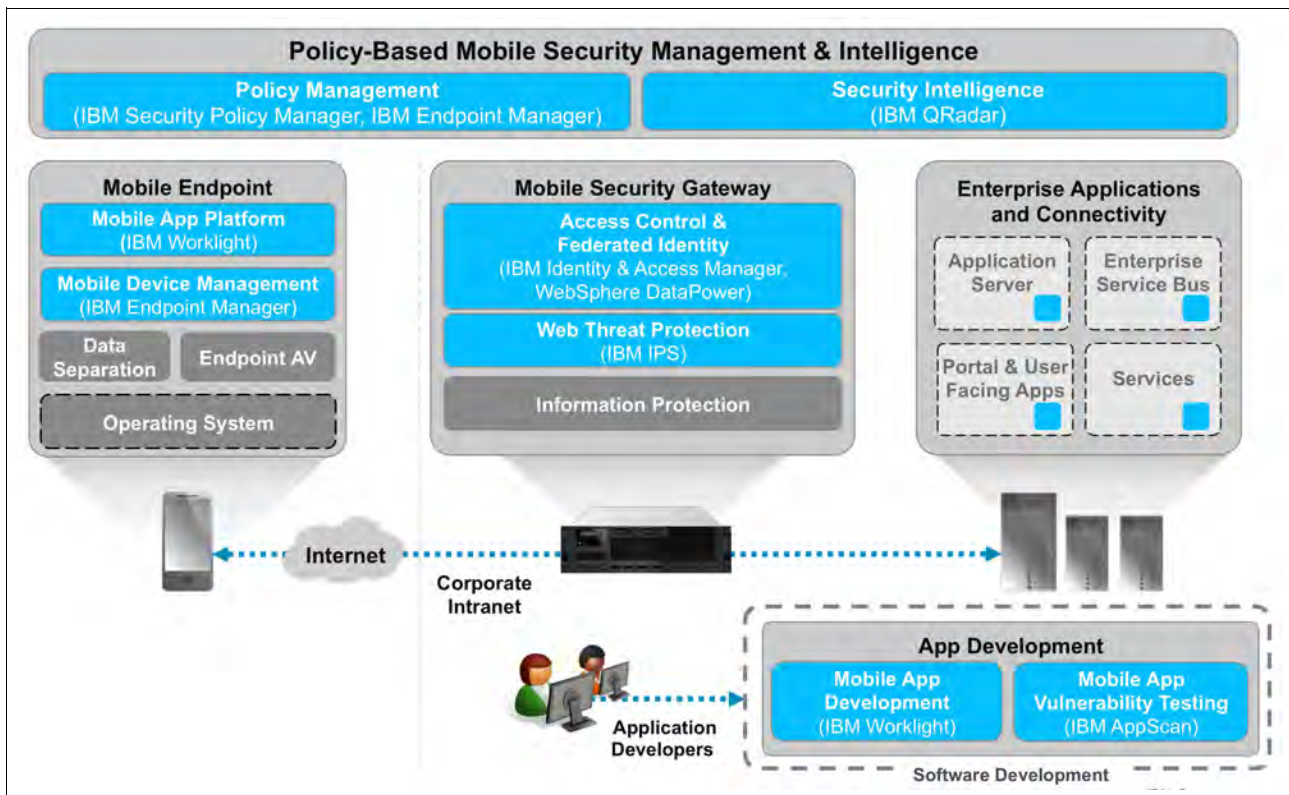

Figure 14   IBM Mobile Security Reference Architecture

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 capabilities:

► Secure the mobile device
► Protect access to enterprise resources

- ► Deliver safe mobile applications
- ► IBM Mobile Security Maturity Model

Secure the mobile device

To properly secure mobile devices, an organization needs to take the following steps:

- ► Capture detailed device information and identify noncompliant devices (for example, detect jailbroken or rooted devices).

- ► Enforce security best practices and take corrective action, including performing updates, denying or removing access, configuring a virtual private network, and delivering device security solutions:
  - – Anti-virus and anti-malware
  - – Personal firewall
  - – Anti-spam
  - – Loss or theft protection
  - – Device monitoring and control
  - – Secure access to corporate network via VPN

- ► Remotely locate, lock, and perform selective wipes when devices are lost, stolen, or decommissioned.

- ► Use a single infrastructure to deliver controls for a broad set of enterprise endpoints, including smartphones, tablets, desktops, laptops, and servers.

Figure 15 depicts the unified desktop, notebook, server, and MDM capabilities of the IBM Endpoint Manager for Mobile solution.
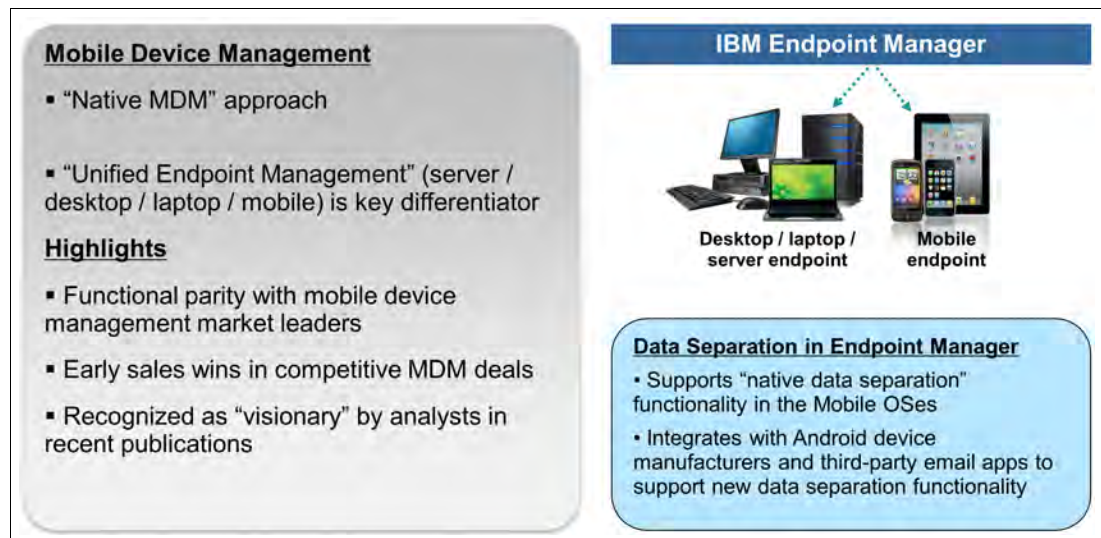

Figure 15   Mobile device management

Protect access to enterprise resources

To properly protect access to enterprise resources, an organization needs to perform the following actions:

- ► 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

Figure 16 depicts the IBM Mobile Security Gateway solution.

Figure 16   IBM Mobile Security Gateway

Deliver safe mobile applications

To properly deliver safe mobile applications, an organization needs to follow these practices:

- ▶ Support developers with security features, including data encryption, direct updates, and application validation
- ▶ Perform vulnerability assessments during development, testing, and run time 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
- ▶ Attain visibility and deliver an adaptive security posture
- ▶ Generate reports on compliance
- ▶ Assess consistency of security policy enforcement
- ▶ Be proactive in responding to emerging threats
- ▶ Adapt to changing user behaviors

IBM Mobile Security Maturity Model

The previously-mentioned IBM Mobile Security Reference Architecture combines industry-leading mobile security technologies with IBM products, solutions, and deeper security knowledge. With the IBM Mobile Security Maturity Model as a reference, an organization can benefit from improved operational, compliance, financial, and strategic efficiencies across the organization.

Perhaps most importantly, organizations can enhance their overall security posture to increase their business competitiveness. Figure 17 on page 26 depicts the IBM Mobile Security Maturity Model, which can help organizations better position themselves, and enhance their security posture from basic to proficient, leading to optimized security intelligence.
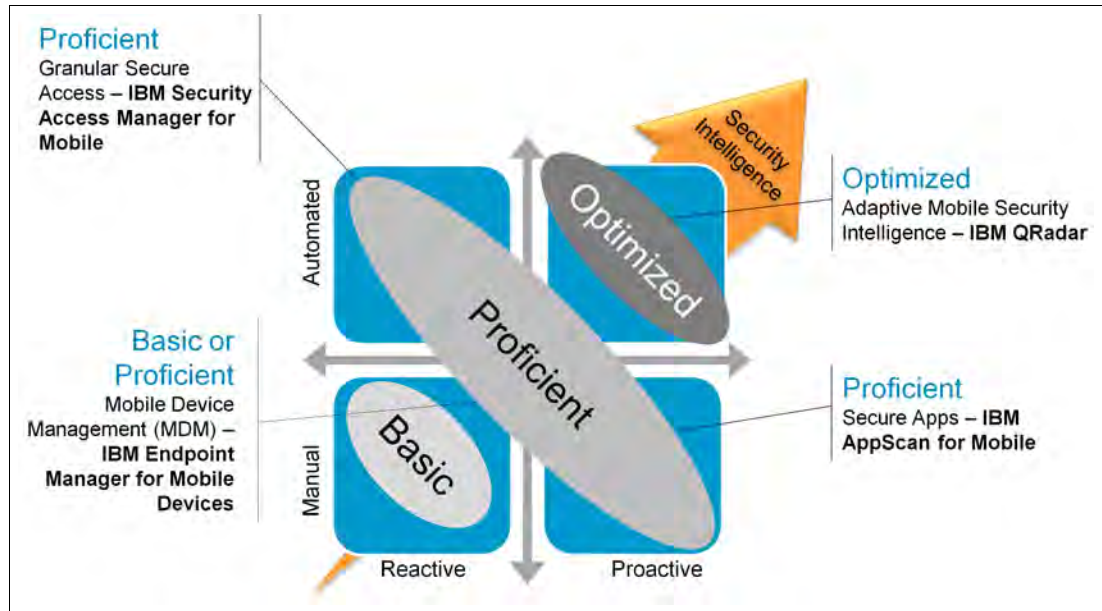
Figure 17   IBM Mobile Security Maturity Model

IBM Mobile Security Framework

IBM Mobile Security Framework solutions can help organizations properly address challenges in mobile device management, access management, application security, and security intelligence. IBM not only delivers mobility-focused capabilities, but solutions are designed to extend and complement existing IT security infrastructures, policies, and procedures. IBM takes a holistic approach to address security requirements in general, using the well-established IBM Mobile Security Framework.

Figure 18 on page 27 depicts the IBM Mobile Security Framework, which uses a security "magnifying glass" to examine the mobile device, network, and mobile applications aligned with the IBM Mobile Security Framework domains for People, Data, Applications, Infrastructure, and Security Intelligence, Analytics, and Governance, Risk, and Compliance (GRC).
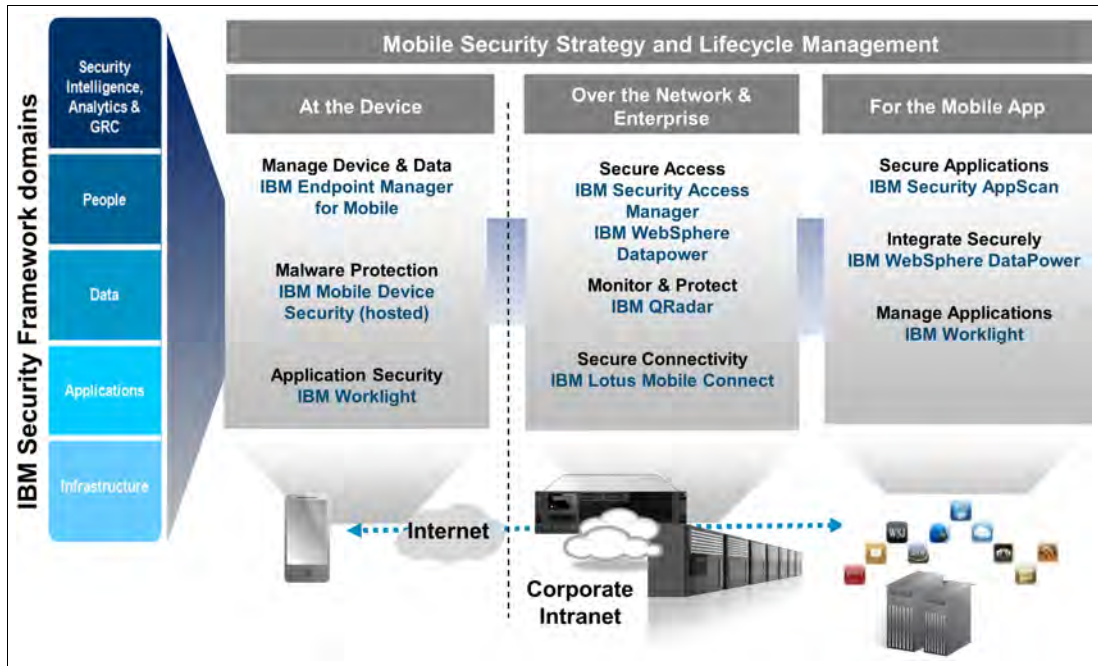
Figure 18   IBM Mobile Security Framework

People: Simplifying identity and access management

As the mobile device becomes the preferred tool for many users, preventing unauthorized access by mobile users becomes a top requirement for organizations. However, controlling mobile access, while sharing many of the same security objectives with controlling traditional access infrastructures, presents specific challenges. Figure 19 depicts how the IBM Security Access Manager for Mobile can be used as a mobile security gateway.
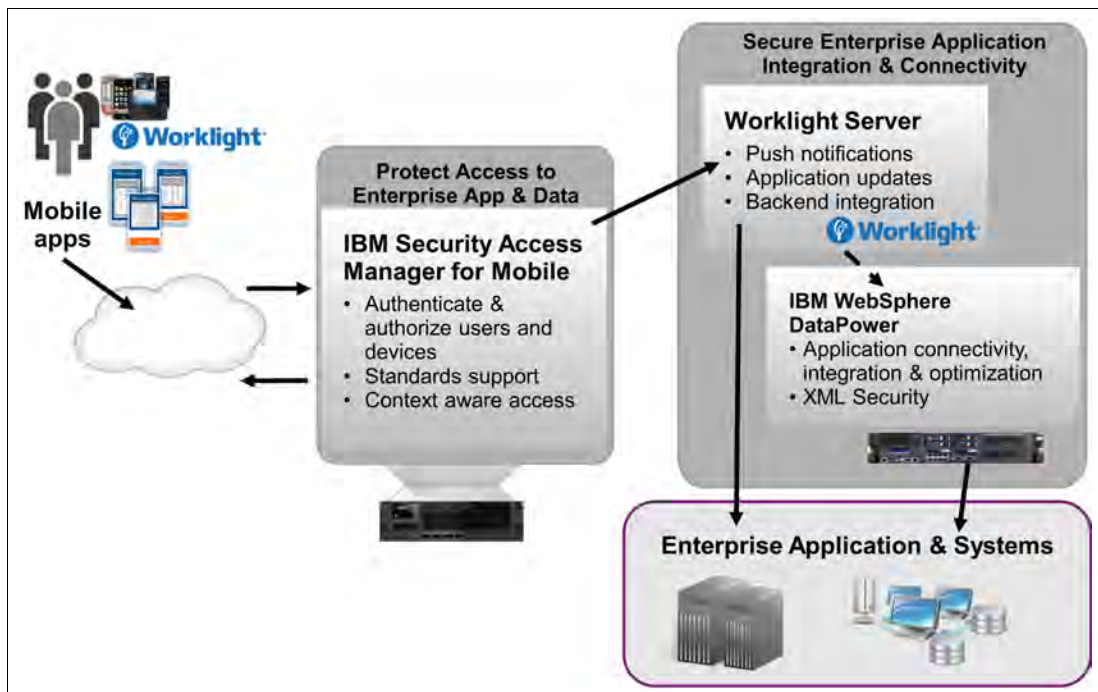

Figure 19   IBM Security Access Manager for Mobile solution

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 deployed and shared for all types of users while addressing some of the unique requirements of mobile access control.

IBM Security Access Manager for Mobile provides 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 the IBM Worklight solution to deliver seamless user and application security.

IBM Security Access Manager for Mobile provides context-aware authentication and authorization. Organizations can use the contextual information that 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 are core to any mobile security initiative. IBM Endpoint Manager for Mobile Devices delivers data security on the mobile device. It can enforce the compliance of device configurations with enterprise security policies, and uses platform facilities to enforce data encryption.

This solution provides remote device lock and both full and selective data-wipe capabilities, and also provides the infrastructure to deliver anti-malware solutions. VPNs are used to protect sensitive data communications. Figure 20 depicts the IBM Endpoint Manager for Mobile Devices, a highly-scalable, unified solution that delivers device management and security across a variety of device types and operating systems for visibility and control.
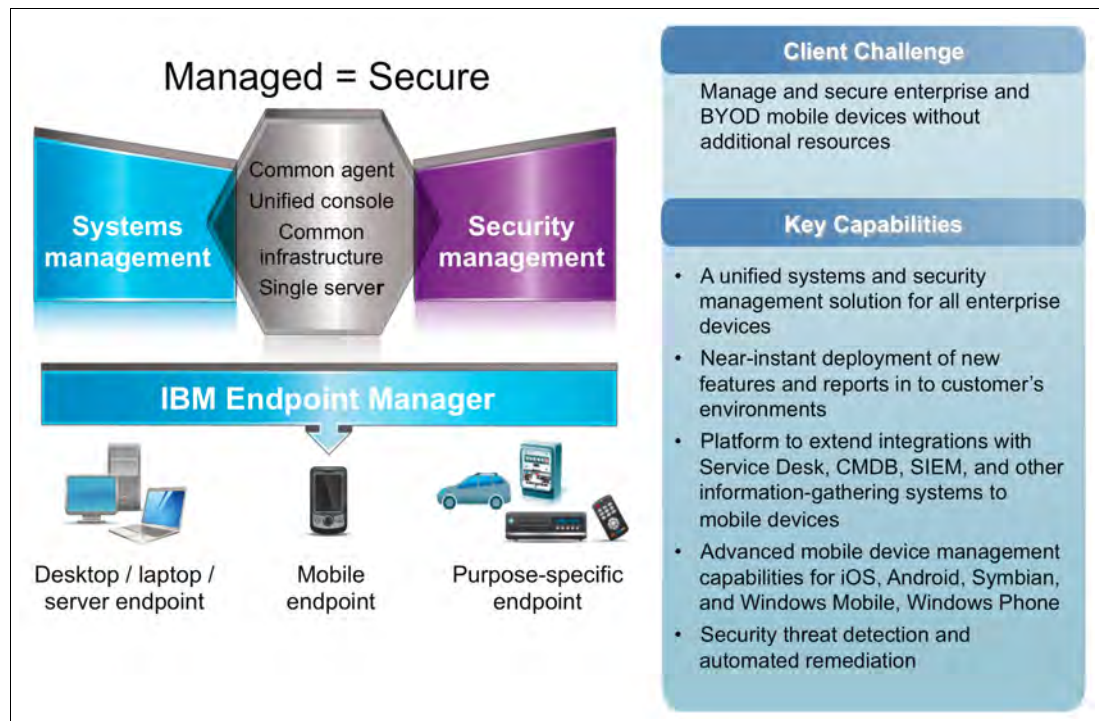

Figure 20   IBM Endpoint Manager for Mobile Devices solution

The IBM Worklight solution offers developers application-level data security by providing facilities and the tools needed to encrypt their applications and data. In addition, subscription-based IBM Hosted Mobile Device Security Management is a turnkey SaaS solution that can provide assurance of data security and policy compliance with anti-malware, anti-theft, and 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. The security risks that organizations face when deploying mobile applications include data disclosure, malicious data injection, tampered application logic, and broken cryptography, among others.

An enterprise application can encounter attacks of this sort from malware on the mobile device, or by malicious users who have either stolen or hijacked the mobile device. With the large projected increase of enterprise mobile applications, security must keep pace. Figure 21 depicts the IBM Worklight solution to develop, deliver, and deploy security-rich mobile applications to streamline business activities while also delivering a rich user experience.

Figure 21 IBM Worklight solution

The security features of the IBM Worklight solution enable organizations to efficiently develop, deliver, and run safe HTML5, hybrid, and native mobile applications with direct updates and application validation. The question becomes: How can organizations be more proactive in delivering safe mobile applications to mitigate the risk to trust relationships that these organizations have forged with their employees, clients, and business partners?

The IBM WebSphere DataPower® message protection and XML firewall capabilities can improve the integrity of message content, and protect application programming interface calls.

Instead of focusing on the inbound attacks and trying to counter them one at a time, imagine if we could remove vulnerabilities within the mobile applications themselves that malware and exploits capitalize on. Enumerating potential vulnerabilities for a mobile application requires research. When armed with this understanding, however, it becomes much easier to identify these vulnerabilities, and to cost-effectively patch them during development and test phases.

Research into vulnerabilities assesses the platform on which the application will run, the frameworks that the application uses, and the technologies that the application is built with. This ongoing research has been encapsulated into the IBM Security AppScan® vulnerability testing platform.

IBM Security AppScan can detect vulnerabilities in mobile web applications, the web elements of hybrid mobile applications, iOS applications, and Android applications through static analysis during development. Figure 22 depicts the use of the IBM Security Appscan solution for application security testing and risk management.
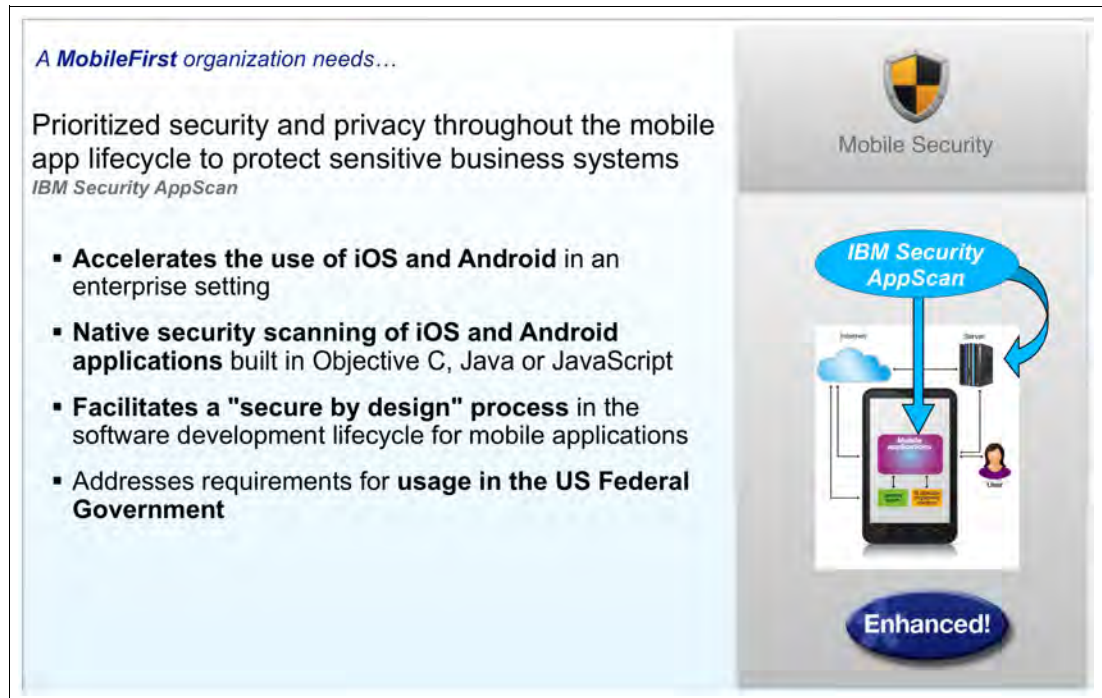

Figure 22   IBM Security AppScan solution

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, ranges from the acquisition and registration of devices to providing secure communications using virtual private networks, to password and configuration compliance.

IBM Lotus® Mobile Connect enables secure connectivity from mobile devices to back-end systems. IBM Endpoint Manager for Mobile Devices gathers and delivers detailed device information to assess compliance. IBM Endpoint Manager for Mobile Devices can also be used to identify compromised mobile devices (including jailbroken or rooted ones), and restrict their connections to the enterprise network. Figure 23 on page 31 shows how IBM Lotus Mobile Connect can help deliver a security-rich connection to enterprise resources from mobile devices.
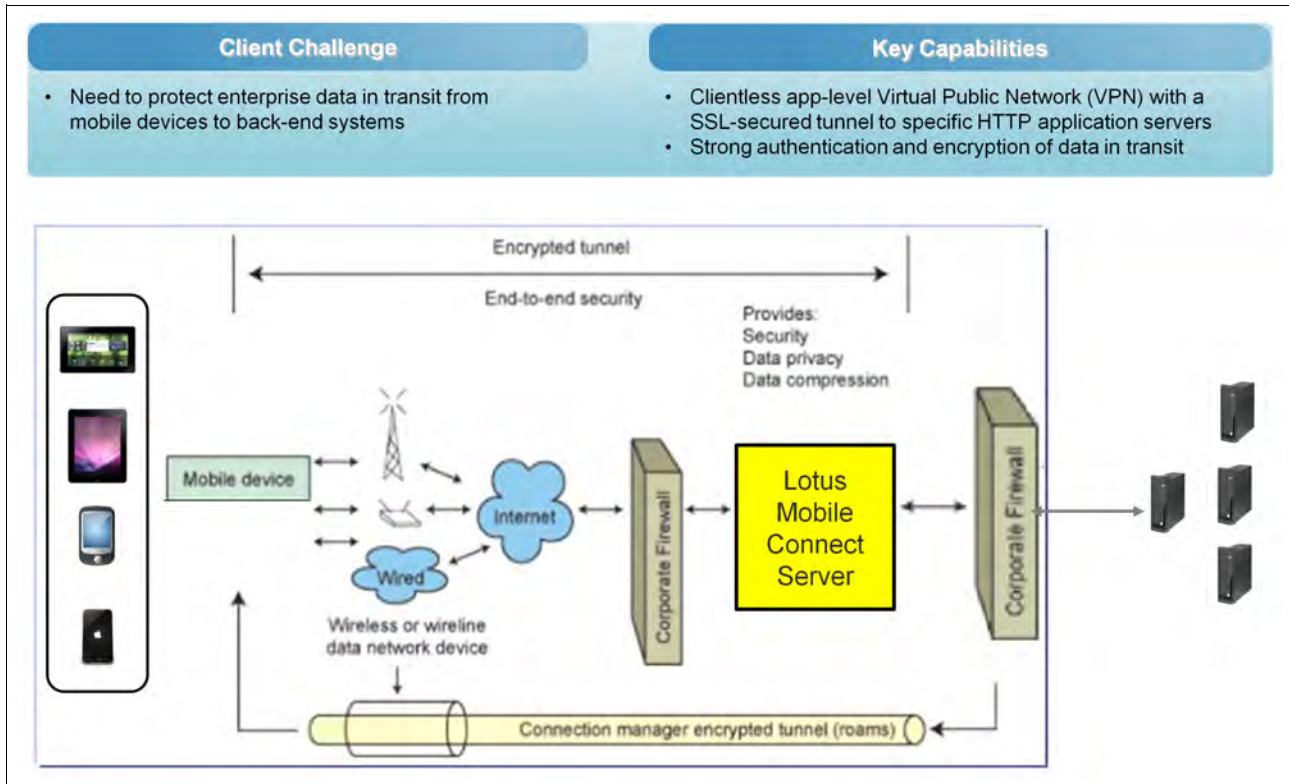
Figure 23   IBM Lotus Mobile Connect for secure VPN to mobile device

Security intelligence: Visibility into activity and threats

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

The IBM QRadar® solution offers a unified collection, aggregation, and analysis architecture facilitating the use of the following data:

► 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

► Configuration files

► Network flow telemetry

IBM QRadar also includes forensic capabilities to support security investigations and audits.

Figure 24 on page 32 depicts IBM QRadar delivering mobile security intelligence by monitoring data collected from other mobile security solutions. It also provides visibility, reporting, and threat detection.
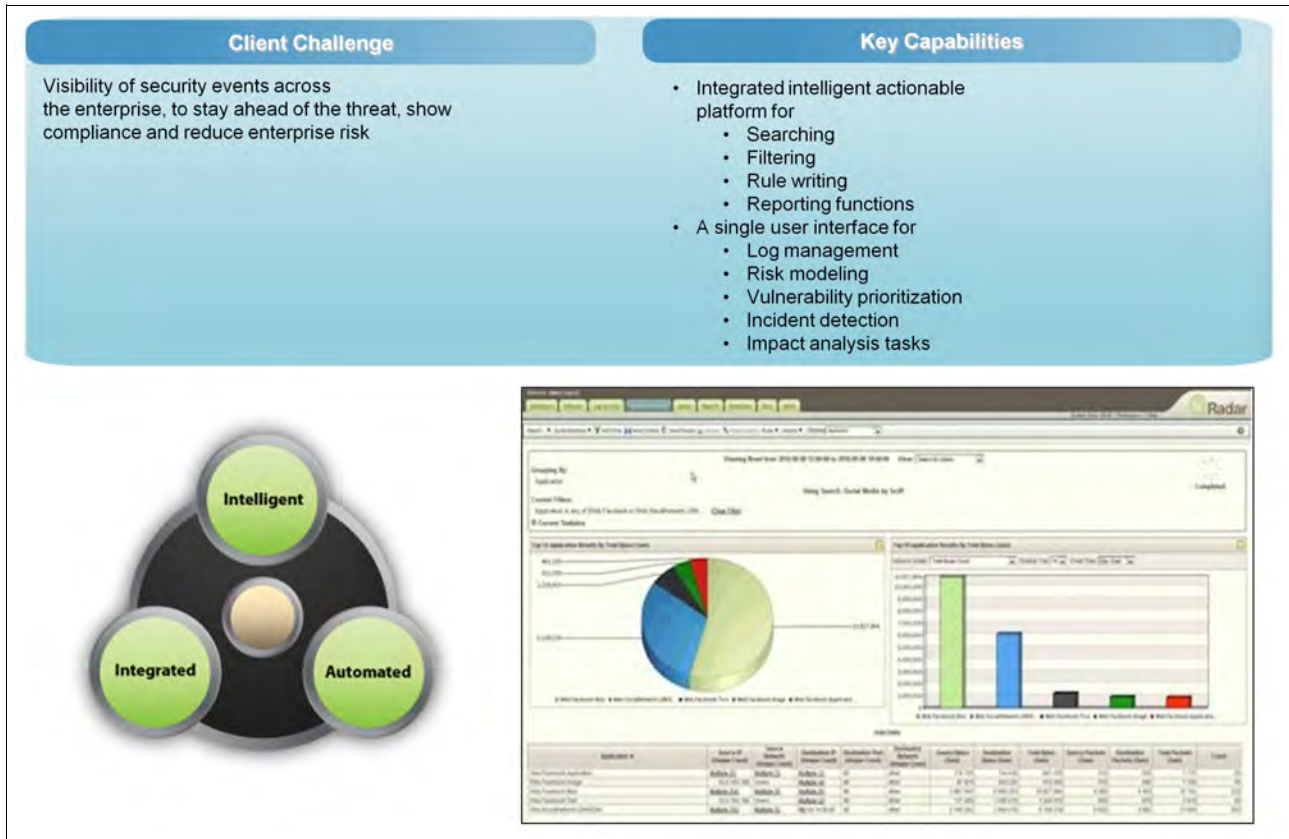
Figure 24   IBM QRadar mobile security intelligence solution

Mobile organizational security roadmap

To help build an effective mobile enterprise strategy and roadmap, IBM delivers a range of comprehensive professional security services. IBM provides an enterprise-specific security strategy and roadmap after identifying the business requirements and carrying out a threats, vulnerabilities, and risk assessment. IBM can provide the products and solutions to implement the security recommendations, and can also provide hosted managed security services for the device security management.

The IBM Mobile Security strategy and roadmap takes into consideration mitigation controls required for all aspects of the IBM Mobile Security Framework to provide a phased implementation approach:

► People
► Data
► Applications
► Infrastructure
► Security intelligence and analytics

Figure 25 on page 33 depicts the IBM Mobile Security Framework solution components.
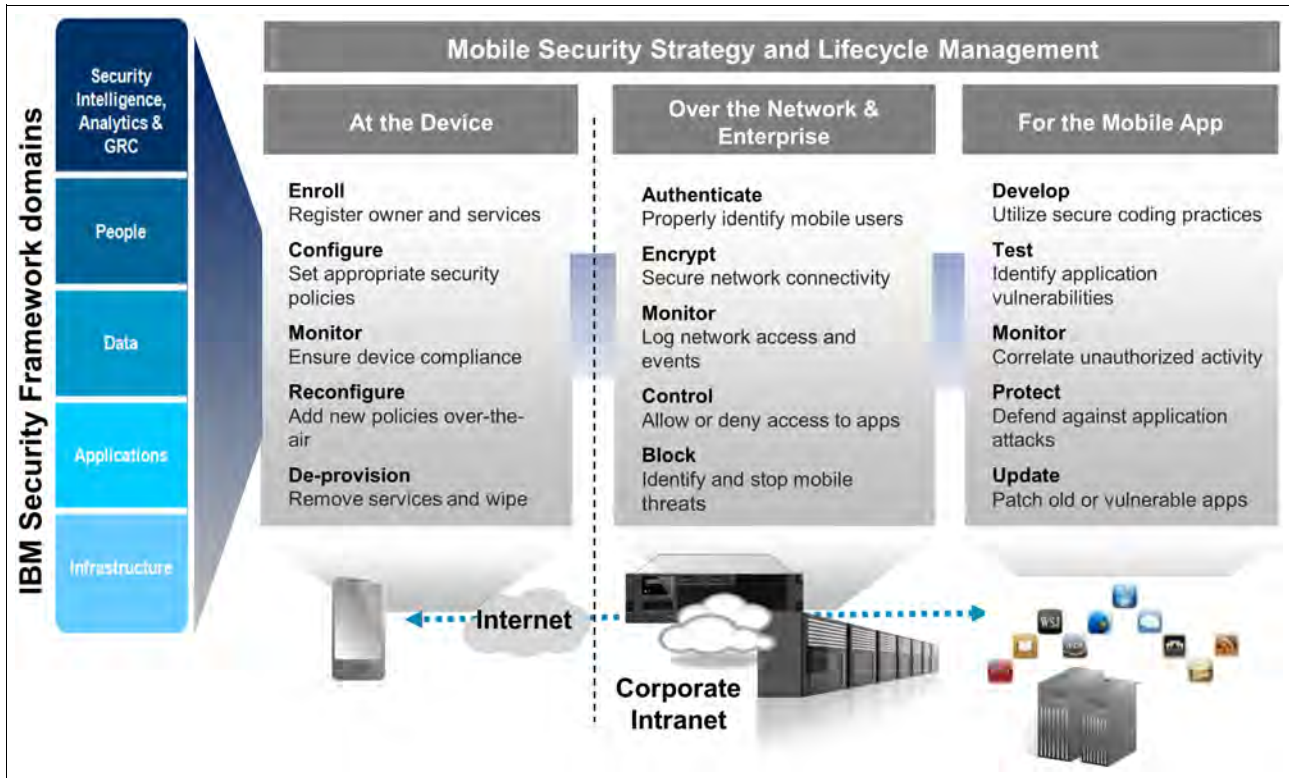
Figure 25   IBM Mobile Security Framework solution

IBM Mobile Security case study

In this section, we look at a fictitious financial institution and how to deliver on their secure mobile strategy.

The financial institution has two goals:

► Extending secure access to banking applications to mobile clients

► Enhancing the abilities of employees to perform secure transactions via mobile devices by allowing them to bring their own devices into the workplace

With these dual goals in mind, the financial institution targets a staged approach by first supporting Google Android and Apple iOS platforms, with future support planned for Microsoft Windows Mobile-based devices. Figure 26 on page 34 depicts the business requirements of the financial institution.

Figure 26   Business requirements for the financial institution

The financial institution wants to centrally manage the mobile devices that will be used for business purposes by their employees. IBM helped the client develop a formal mobile security strategy and develop the corresponding policies. Figure 27 depicts the IBM mobile security delivery strategy for the financial institution.

Figure 27   IBM mobile security delivery strategy

The MDM infrastructure performs policy compliance assessments, device wipe, application management, and device lockdown. Given the management overhead, self-service capabilities are offered to the employees to improve the overall responsiveness of the solution.

Because the employees bring their own mobile devices and use them in dual-purpose mode, for both personal and business reasons, the IBM team had to segregate the personal profile and the business profile on the mobile device. The solution only manages the business profile.

Using IBM Security Access Manager for Mobile to authenticate requests and the IBM Worklight platform to support back-end services, the financial institution safeguards its trust relationship with their clients using data encryption and timely application updates. Figure 28 depicts the IBM mobile security solution deployment for the financial institution.

Figure 28   IBM mobile security solution deployment

Summary

The explosive growth and application diversity of mobile devices are helping organizations to reach their clients in innovative ways. Embracing mobile technology in the enterprise can also help increase employee productivity. Organizations want to provide employees the option of using a personally-owned device as a way to reduce costs, and allow them to work wherever or whenever they need to, but doing so requires diligence in protecting corporate data.

In this era of BYOD, with employees using their own mobile devices for business and personal activity, organizations are now tasked with supporting the new social, virtual, and mobile employee, and the applications that they access.

With mobile threats on the rise, increasingly complex IT environments, and advanced security risks, the need to maintain enterprise policies is more important than ever. Helping organizations adopt mobile technologies to enhance efficiencies and control costs is a major concern for C-level executives, and for security and risk professionals.

No matter how capable a mobile security solution is, its value is greatly diminished if it cannot be efficiently deployed or easily managed. Every organization needs to carefully assess the overall risks for them, and the effort required for initial rollout and ongoing management of a mobile solution. Security involves ongoing monitoring and periodic assessments.

Although installed software and solutions have been the traditional delivery model, increasingly clients are looking for cloud-based delivery models. Another growing trend is the appeal of the appliance form factor for on-premises deployments.

IBM Security Systems and IBM Security Services can provide a holistic mobile security solution and a comprehensive range of mobile security services. This helps an organization keep pace with mobile technology innovations. IBM is using its research and technology knowledge base to continuously enhance the security solutions and services landscape on an ongoing basis.

Other resources for more information

- ► The latest IBM X-Force trend reports:

  https://www.ibm.com/services/us/iss/xforce/trendreports/
- ► The IBM Mobile Enterprise:

  http://www.ibm.com/mobile-enterprise/us/en/
- ► IBM mobile development resources:

  http://www.ibm.com/developerworks/mobile/
- ► Smarter Security and Resilience:

  http://www.ibm.com/smarterplanet/us/en/business_resilience_management/nextsteps/index.html
- ► IBM Security Access Manager for Cloud and Mobile product information:

  http://www.ibm.com/software/security/products/samcm/
- ► IBM Endpoint Manager for Mobile Devices product information:

  http://www.ibm.com/software/products/us/en/ibmendpmanaformobidevi/
- ► IBM Worklight product information:

  http://www.ibm.com/software/mobile-solutions/worklight/
- ► IBM Security AppScan product information:

  http://www.ibm.com/software/awdtools/appscan/
- ► IBM Application Security:

  http://www.ibm.com/software/products/us/en/subcategory/SWI10

Authors

This guide was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO).

Arun Madan is a Senior Technical Staff Member (STSM), Certified Information Systems Auditor (CISA), Associate Director, and Chief Architect at IBM Global Technology Services®: Strategic Outsourcing, IBM India/South Asia. Arun is also an author at the International Technical Support Organization, Austin Center.

Arun has worked with IBM for the past six years, and he has over 30 years of experience in the information technology industry. He has designed and led implementations of organization-wide security frameworks, published, and presented papers at various security forums.

Sridhar Muppidi is a Senior Security Architect at IBM Software Group. As a Senior Technical Staff Member, he drives security architecture and design activities across IBM security products. He is responsible for service-oriented architecture (SOA) and SOA security solutions. He is a lead architect for the IBM Security Policy Management solution. His responsibilities also include providing secure solutions to enterprises, working on new product development, and representing IBM in standards activities. Sridhar holds a Ph.D. degree in computer science and has published extensively.

Nilesh Patel is a senior identity and access management and security intelligence professional in the IBM Security System division. Nilesh is an IBM International Technical Support Organization-accredited Master Author. He is a Solution Advisor for IBM security and compliance management solutions. He has extensive experience in the design and implementation of identity and access management solutions, along with security intelligence and compliance solutions.

Nilesh has published many technical papers within the IBM developer domain, and has customized integration modules on the IBM Open Process Automation Library for identity and access management and security intelligence products. He has delivered many technical webcasts to educate clients about new features for, and integration of, IBM Security products. Nilesh has authored and contributed to several IBM Redbooks® publications.

Axel Buecker is a Certified Consulting Software IT Specialist at the ITSO, Austin Center. He writes extensively and teaches IBM classes worldwide about areas of software security architecture and network computing technologies. He has a degree in Computer Science from the University of Bremen, Germany.

He has 26 years of experience in a variety of areas related to workstation and systems management, network computing, and e-business solutions. Before joining the ITSO team in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

Thanks to the following people for their contributions to this project:

Vijay Dheap
IBM

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and client satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Obtain more information about the residency program, browse the residency index, and apply online at:

http://**ibm.com**/redbooks/residencies.html

Stay connected to IBM Redbooks

- ► Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- ► Follow us on Twitter:

  http://twitter.com/ibmredbooks

- ► Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- ► Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- ► Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-4957-00, was created or updated on July 10, 2013.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at
http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AppScan®	Global Technology Services®	Redguide™
BigFix®	IBM®	Redbooks (logo) ®
Cast Iron®	Lotus®	WebSphere®
DataPower®	Redbooks®	X-Force®

The following terms are trademarks of other companies:

QRadar, and the Q1 logo are trademarks or registered trademarks of Q1 Labs, an IBM Company.

Worklight is trademark or registered trademark of Worklight, an IBM Company.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.