Mobile Security: How to Determine Which Path Your Mobile Security Strategy Takes

SUMMARY

Industry
All industries

Product
Mobile devices including computers, tablets and smartphones

Region
All regions

Typical Applications
Mobile Security Strategy and Planning

Customer Benefits
Safeguard your company's mobile devices, apps and content

Protect your corporate networks from cyberattacks

Like it or not, there are people out there with malicious intent and employees who can be inadvertently careless. Just as you can't safeguard your company's devices without proper security planning, you also need a plan for protecting apps and content. Taking a three-pronged approach is the key to successful mobile security management. But before you consider the software solutions, policy settings and other tactical elements that make up your mobile security package, you need to identify how your company and your employees use their devices and how far you need to go on the security trajectory. Here's a sampling of areas to consider.

Regulatory rigmarole

Every company has its own standards for security, but some industries require companies to jump through more hoops than others. The world of mobility puts companies at greater risk of being out of compliance with regulations. Businesses that process credit cards are subject to the Payment Card Industry Data Security Standard (PCI DSS), healthcare organizations need to make sure that they stay compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and publicly held companies must adhere to the Sarbanes-Oxley Act of 2002 (SOX). These are the biggies, but there are other, lesser-known regulations to be aware of. Make sure that you know your industry requirements as they pertain to mobile devices, apps and content.

Even if your company is not subject to stringent industry regulations, it is still a best practice to set security policies as though it were. After all, regulations are meant to help companies determine which information is considered sensitive, who should have access to it and under which circumstances, and how to respond if that information is compromised.

Stay flexible

Security can be a double-edged sword. If you completely control your mobile devices, apps and content, you'll limit your employees' productivity. But if you give employees too much freedom, you're more likely to experience security breaches. It's best to determine where to draw that magic line for your company, your employees and your data. Also, because things change so quickly in the mobile world, it's smart to implement security policies that won't prevent your business from adapting down the road.

Take inventory

Many of the platforms, devices and apps in your mobile environment already have security features that provide protection while others may not. Find out the details about all the components that make up your current environment, and determine which ones have adequate native protection.

Honeywell

Evaluate BYOD

By now, you probably understand the benefits of bring-your-own-device (BYOD) programs. Unfortunately, BYOD programs do present their own security concerns. One of the challenges of BYOD is that security responsibilities can be distributed between the company and its employees. Some companies alleviate the problem by taking on the responsibility for mobile security. They use company-managed gateways to maintain consistent control over data access and storage at the policy level. Even without those gateways, companies need to have baseline security requirements for BYOD that include enhanced password controls, data encryption, the ability to lock devices after a certain number of unsuccessful password attempts, and remote lock and/or wipe features.

Privacy is another consideration when it comes to BYOD programs. In a survey of enterprise workers, most were concerned that BYOD would "transform IT from helpful business partner into an Orwellian Big Brother keeping round-the-clock tabs on all device activity." Lots of companies use tracking software to help with mobile device security, but the majority of workers feel that tracking – either their devices or the websites they visit – invades their privacy. You'll need to establish concrete policies and clearly communicate with employees so that everyone knows to what extent your company monitors devices.

Hands-on or hands-off?

There's a lot that goes into properly securing any infrastructure, let alone one that includes devices that can be taken anywhere. Although IT departments have plenty of options to choose from for mobile security software, many are overwhelmed by the rise in mobility. As mobile technologies evolve, the process of securing devices, apps and content becomes more complex.

Some IT departments take on the challenge of protecting their mobile infrastructure, while others choose to rely on partners who offer mobile security expertise. If you opt to work with a partner to secure your mobile environment, find one that has experience in securing multiple platforms and in addressing the entire mobile lifecycle so that you don't run into roadblocks later.

Did you know?

In a global survey of mobile device users and IT decision makers, 89% of people who use their personal devices for business purposes say they use them to access critical work information.

Better than a security blanket: Which combination of software solutions is right for you?

The first wave of mobile security software focused on the devices themselves. Now the focus has expanded to include mobile apps and content. Combining mobile device management (MDM) software with mobile application management (MAM) and mobile content management (MCM) software is most effective. The trick is to find the right balance among the three software types so that your mobile environment continues to run effectively.

MDM: Keep devices secure

MDM software focuses on centralized lifecycle management, but many features that fall under the device management category are also relevant in the security realm. For example, if you can use your MDM solution to update applications, you can use that same update capability as a way to reduce the vulnerability of your devices. MDM solutions help you enforce security policies and manage noncompliant devices by applying security measures, like blocking access to data or removing data from the devices. You can use MDM software to apply acceptable-use policies to devices, ensure that devices have the mandatory security settings in place, and issue devices with certificates for access. You can also enforce whitelisting and blacklisting of apps, disable unauthorized native apps, and audit device settings to detect risky or potentially malicious activity – all good steps toward maintaining a secure mobile environment.

MAM: Protect apps

As mobile apps become more relevant in the enterprise, MAM software is gaining popularity. And for good reason. MAM software helps ensure that mobile apps are free of malware and viruses, and it protects mobile environments by controlling access – only certain users can access particular applications on particular devices. These software packages can transparently install missing whitelisted apps, such as spam filters or firewalls, which means that you don't have to wait for employees to install and configure security apps.

You can use MAM software to track app downloads and usage. You can also use it to push updates for enterprise apps and remind your employees to install updates on non-corporate apps, thus keeping devices compliant with your security policies. When combined with the right MDM solution, MAM software can play a valuable role in securing mobile apps.

MCM: Safeguard data

MCM deals with the data that's in use on mobile devices. By using

MCM capabilities, your employees can securely share, collaborate on and send documents, presentations, videos and more. MCM strategies help establish a secure container around sensitive data, encrypting it and allowing only approved applications to access and distribute that data. Although still evolving, MCM solutions are expected to become more useful as integration improvements and the development of industry standards make it easier for devices and apps to recognize the protections placed on data.

But that's not all

In addition to the "big three" in mobile security solutions, consider these other areas of opportunity:

Secure access. If your employees only use their devices for email, the security features (like Exchange ActiveSync) associated with your email systems are probably just fine. However, you probably need greater levels of authentication, so check that you have strong authentication to the network, encrypted tunneling capabilities and a host-integrity-checking capability that restricts access based on a user's security state.

Threat protection. As more people rely on their mobile devices, antimalware protection for mobile platforms has become increasingly important. Look for a robust grouping of web security capabilities that examines content from every possible angle to detect new threats.

Data protection. Embedded data loss prevention (DLP) capabilities in your email and web security gateways will control the data that can get to mobile devices in the first place. Mobile DLP functionality helps keep data from being exposed, whether accidentally or maliciously.

Mobile application reputation services. You can take advantage of several services that integrate with the major MDM vendors to provide risk assessments of applications. You can use the information from these services to perform quarantines, update for compliance and receive alerts if they detect vulnerabilities.

Did you know?

In a survey of CIOs and IT Managers, of those who were planning to increase their investment in mobile devices, only 7% said that they planned on readdressing security policies and looking into management solutions such as MDM.

The nitty-gritty: Consider these security elements, measures and processes

Aside from the planning that goes into your mobile security strategy and the software solutions that play a role in protecting your environment, the following mobile security methods and considerations may also work for your company.

Dual personas. The idea behind dual-persona devices is that two separate sets of usage controls exist within a single mobile device, which keeps personal and business information in separate buckets. This applies especially in BYOD scenarios. Not all devices are able to offer this dual-persona model, so look for that sort of mobile unified communication as you assess devices and providers.

Secure single sign-on. Secure single sign-on is fairly common in the desktop environment, and it is slowly becoming the standard in the world of mobility, too. By making it possible for users to gain access to all their apps and content through secure single sign-on, companies avoid the need for employees to remember multiple URLs, user names and passwords – yet apps and data remain protected. Users are authenticated once and then have one-click access to authorized apps, which keeps them productive and saves time for your help-desk staff because users need less assistance with routine access-related issues.

Containerization. Your employees might be cautious, responsible users, but they could still accidentally put company content and systems at risk by downloading unsafe applications or tapping into unprotected personal content. Containerization separates business and personal content and makes it possible for IT staff to control business content without affecting personal information. App containerization technology provides each managed app – and its data – with its own secure "container."

Did you know?

Of enterprise users surveyed, 85% have a passcode automatically enforced on their smartphones or tablets, but 93% of those users employ very basic passcode types.

Honeywell

Mobile operating system security. Different mobile operating systems have different security capabilities. It can be helpful to compare access control options, such as file system encryption availability, type of SD card encryption and security patch flow. Knowing how these mobile operating systems differ may have an impact on your purchasing priorities.

Security analytics and predictive intelligence. Addressing big data is one of the current technology trends, and that big data can help you shore up your mobile defenses, too. If you apply business intelligence to your mobile environment, you can sniff out abnormal behavior and administer real-time security compliance protocols for devices that access sensitive corporate data.

Wi-Fi risks. One often-overlooked area of mobile security involves Wi-Fi access. Most mobile device platforms make it easy to connect to a previously used Wi-Fi access point, but it's simple to impersonate those connection points and attack connected devices. Deploy configuration profiles with corporate Wi-Fi settings, with the highest validation enforced, and encourage employees to use private, rather than public, certificates.

Keep it current

Mobile security isn't a set-it-and-forget-it deal. Once you have a plan in place, you have to keep it current or you'll put your company in jeopardy as security threats and employee needs change. Take time on a quarterly basis to assess new risk factors and indicators that may cause you to adjust your policies, device settings and other aspects of your mobile environment.

Need more assistance working through the challenges that mobile security presents? Take a look at our **MDM white paper** and **BYOD Policy Template**.

Sources

- www.honeywell.com/enterprisemobility
- BYOD Beware
- Trusted Mobility Index
- Companies Focus on Mobile Device Rollout While Overlooking Security, IFS Study Reveals
- Soft Passcodes Still Prevail on Enterprise Mobile Devices

For more information:
www.honeywell.com/enterprisemobility

Honeywell Sensing and Productivity Solutions
9680 Old Bailes Road
Fort Mill, SC 29707
800-582-4263
www.honeywell.com

Mobile Security AB Rev B 03/16

Honeywell