Trustwave®
Smart security on demand

ENTERPRISE MOBILITY ASSESSMENT

OVERCOME MOBILE SECURITY CHALLENGES

Trustwave's Enterprise Mobility Assessment is designed to help your organization create an enterprise wide mobile program using a pragmatic balance of productivity and security.

THE BYOD/MOBILE CHALLENGE

The rise of the smart phone and tablets has led to an unprecedented growth in mobile productivity tools. Ask any employee in an organization, and they'll likely tell you that they can't do their jobs without the support of such devices.

If you ask a CISO the same question you will get a very different response. "Bring Your Own Device" means something different to everyone. For some, it's productivity and ubiquity of access—but for the CISO, it's unchecked risk—such as lost/misused data and an entry point for malware to enter the organization. These devices bring unprecedented growth in risk of data theft, and the pressure to provide the much in-demand functionality of access from anywhere often far exceeds an organizations' ability to effectively secure the underlying data.

THE TRUSTWAVE DIFFERENCE

The Trustwave Enterprise Mobility Assessment is designed to provide a pragmatic balance of productivity and security. This assessment utilizes a suite of fully customizable professional services to help your organization implement the appropriate program for your business. No matter where you are in the process of adopting an mobile/BYOD strategy—just starting out or fully mature—the Trustwave Enterprise Mobility Assessment will help ensure your data is secure and your protection is in line with your mobile access and overall strategy.

The Enterprise Mobility Assessment helps ensure the integrity of your mobile data, and is right for any business faced with the challenges of a workforce supported by mobile and BYOD technology.

The Enterprise Mobility Assessment will take your organization through these steps:

- BYOD Strategy Development & Risk Assessment
- Mobile Device Policy & Procedure Development
- Management Architecture & Technology Review
- Mobile Application and Device Testing
- Security Awareness Education

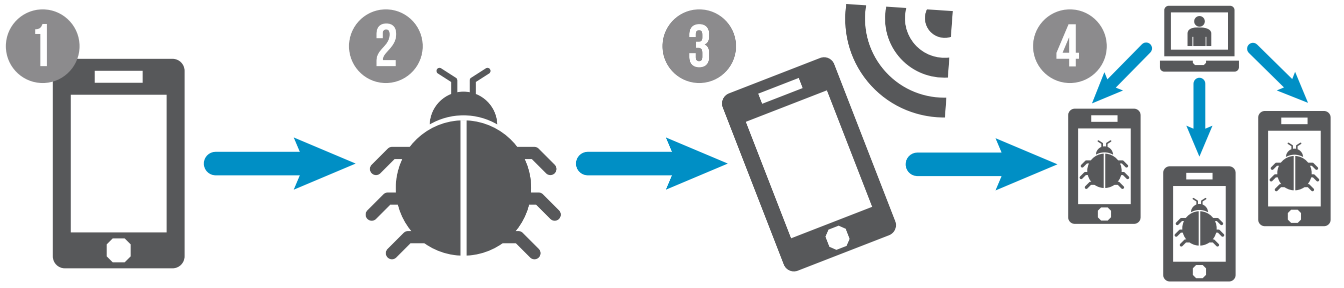
TOP 10 MOBILE VULNERABILITIES

RANK*	Finding	Percentage of Mobile Applications Containing Vulnerability
1	Insufficient Cache Controls	21%
2	Replay Attack on Sensitive Transactions	21%
3	XSS and Code/Content Injection	8%
4	MDM/Platform Security Bypass	8%
5	Sensitive Information in a Server Response	17%
6	Insecure Password Policy	8%
7	Username Enumeration	8%
8	Sensitive Data in Application Cache	8%
9	Secure Cookie Options Not Used	8%
10	Verbose Error Messages	8%

Attacks perpetrated against mobile applications are not very different from those launched against the Web. Attacks can vary depending on platform and application purpose. Web-based applications, client applications and the server endpoints are the usual targets.

Source: 2013 Trustwave Global Security Report

COMMON MOBILE MALWARE SCENARIO



USER DOWNLOADS GAME

GAME INSTALLS MALWARE

PHONE RECEIVES HIDDEN SMS

MALWARE REACTS & PHONE BECOMES PART OF BOTNET

BYOD STRATEGY DEVELOPMENT & RISK ASSESSMENT

Like any other line of business, the first step is an examination of both the required mobile functionality and the potential risks associated with it. From there, identify the data that needs to be secured to support the mobile plan and assess potential financial impact of its loss.

A Trustwave consultant will review the proposed BYOD/mobile business plan, determine all known threat vectors and provide best practice advice on how to plan with security at the core.

MOBILE DEVICE POLICY & PROCEDURE DEVELOPMENT

Policies and procedures are the foundation of all business processes and are the most important living document on which to build any new service—navigating the paperwork, responsibility for security controls and cross-border data laws is complex. Corporate policy must account for personal privacy laws that change across regions and geographies.

> “The first step is an examination of both the required mobile functionality and the potential risk associated with it.”

Trustwave has guided countless organizations in the creation of effective and sustainable policies in support of their specific environments. Your BYOD-specific policies will cover areas such as acceptable use, browsing, employee responsibility, and incident response and set the tone for how your program will be run and managed.

MANAGEMENT ARCHITECTURE & TECHNOLOGY REVIEW

The choice of mobile and BYOD technologies and the systems to manage them should be done with not only the desired functionality and security in mind but also with consideration of cost, scalability, management, and sustainability. Trustwave will assist in the determination of which device management and security features are optimal, while staying vendor agnostic.

The choice of mobile and BYOD technologies and the systems to manage them should be done with not only the desired functionality and security in mind, but also with consideration of cost, scalability, management, and sustainability.

MOBILE APPLICATION & DEVICE TESTING

A process is needed to review the security exposure of mobile devices on an ongoing basis. Application Penetration Testing services will help you assure that your BYOD/Mobile program has the right level of security, without undue impact to productivity. Trustwave also performs mobile device specific tests to ensure your organization has the optimal security levels for devices and applications.

SECURITY AWARENESS EDUCATION

Your Enterprise Mobility Assessment is wrapped in Trustwave’s Mobile Security Awareness Education modules. This education helps build employee awareness and knowledge about mobile/BYOD risks and acceptable uses and promotes adherence to policies across your organization.

Need a comprehensive approach to your mobile needs? Learn more about Trustwave’s offers by visiting here: https://www.trustwave.com/mobile-security.

Trustwave®
Smart security on demand

For more information: www.trustwave.com