IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

Comprehensive Protection from Advanced Threats Requires Mobile Threat Assessment

March 2016

Adapted from *The Evolving Mobile Threat Landscape* by Robert Westervelt, IDC #258443

Sponsored by Check Point Software Technologies

Existing enterprise mobility solutions that validate the use of device encryption and PIN code access and that wipe lost or stolen devices remotely can't provide protection from modern mobile threats. This Technology Spotlight explores why a comprehensive security approach is required to keep mobile devices and data safe and how some of the latest mobile threat prevention solutions use the cloud to reduce complexity and increase visibility and control. The paper also discusses the role Check Point plays in helping organizations prevent advanced attacks on smartphones and tablets. These mobile security solutions integrate with existing security investments to support incident response and provide continuous protection regardless of where employees are located.

Comprehensive Protection Supports Business Enablement

Security consistently remains at the forefront of all enterprise mobility stakeholder concerns. As smartphones and tablets become more powerful, the risk of data loss will be a constant battle. These devices are also often being used to authenticate into SaaS-based services and company resources, raising the specter of an attacker targeting an employee to steal account credentials or eavesdrop on critical communications.

In fact, security researchers are observing financially motivated cybercriminals now using tactics commonly associated with cyberespionage to develop custom malware for multistaged mobile attacks. High-profile attacks and vulnerabilities such as Brain Test, Certifi-gate, Hacking Team, and Xsser, along with newly discovered critical vulnerabilities, underscore the need to add security beyond platforms that simply enforce basic device hygiene.

Savvy cybercriminals are leveraging vulnerabilities in modern operating systems (OSs) and their components to gain nearly complete control of mobile devices, including access to the sensitive data stored on them. Furthermore, hardware limitations (e.g., processor, memory, and storage) restrict the scope and visibility of standard mobile antivirus applications.

IDC's 2015 *Mobile Enterprise Software Survey* reached 508 enterprise mobility decision makers in the United States and found that 57.5% of enterprise IT organizations encounter security and compliance issues during mobile deployment efforts. The study also found that many of these organizations have made investments to address mobile security and bring-your-own-device (BYOD) issues by enforcing basic hygiene policies. More than 91% of enterprise organizations use Exchange ActiveSync, a combination of Exchange ActiveSync and other mobile device management tools, or other tools only.

These solutions control the potential damage inflicted by lost or stolen devices, but they address risks only on the surface. Arguably, some organizations have implemented specialized point solutions, which creates a hodgepodge of siloed security solutions that offer incremental and often rudimentary

enhancements. Comprehensive mobile security should be a system of components that work together cohesively to identify threats and to protect data while addressing employee privacy concerns.

IDC believes organizations require a multilayered security infrastructure that provides comprehensive protection and is also tracking the growing adoption of mobile security solutions that address a wide variety of security functions. These products address device and application vulnerabilities, leverage devices to control identity and access management, and protect against advanced threats using antimalware, intrusion prevention, and firewalls for mobile devices.

Significant Mobile Threats

Most of the known attacks target Android devices, but enterprise chief information security officers (CISOs) are quickly learning that iOS devices are not immune. Attackers have found ways to target iOS devices, in many cases leveraging stolen Apple application distribution certificates given to developers and enterprises to enable the side loading of their malicious applications. Other issues include mobile remote access trojans (mRATs), which are designed to bypass security restrictions, enabling remote control and surveillance capabilities. WireLurker used an enterprise certificate to enable users to reportedly side load hundreds of potentially malicious applications outside of the official Apple App Store in 2014 without the need to jailbreak their iOS devices. Some of the latest threats reflect rising sophistication are as follows:

- Brain Test, a malicious mobile application, appeared on the official Google Play Store and was downloaded by hundreds of thousands of users before Check Point warned Google and the application was pulled down five days later. Brain Test establishes a rootkit on the device, giving attackers the ability to execute malicious code on the device such as adware messages or malware that can steal account credentials and other data.
- Certifi-gate, a serious vulnerability in the underlying architecture of many Android remote support tools used to provide technical support, exposed millions of devices to data theft. Attackers could exploit weaknesses to the certificate authorization process that validates remote support applications to gain unrestricted access to devices.
- The Hacking Team data breach in 2015 exposed new zero-day vulnerabilities in Windows and Adobe Flash, impacting mobile devices. Based in Italy, Hacking Team is a security services organization that provides penetration tools, including a mobile malware suite, to law enforcement and national security organizations, enabling them to gain access to targeted networks and devices.
- Xsser, an mRAT used in targeted surveillance, works against iOS and Android users. It spreads through phishing attacks and is designed to eavesdrop on victims, steal data, and give attackers the ability to upload additional malware remotely.

The mobile threat landscape changes rapidly. Attack campaigns associated with a malicious or phony app provide a quick win for criminals but eventually decline once news of the issue spreads. Many of the overarching tactics remain the same. Aggressive adware associated with legitimate applications often harvests an overabundance of device data that can be easily stolen and exploited in the wrong hands. Employees are also at risk of being exposed to WiFi man-in-the-middle attacks designed to eavesdrop on their activity.

Employees who use third-party app repositories or mobile app distribution sites are vulnerable to fake installers, which can deliver a wide variety of attacks, including SMS trojans, one of the most common threats. SMS trojans give attackers quick cash by using the victim's device to text premium-rate numbers. Ransomware, a long-standing threat, has also started appearing on mobile platforms.

Patching challenges to laptops and PCs also extend to Android devices. Manufacturers and network service providers may have to issue their own version of patches when vulnerabilities are detected in the device firmware, causing a slow rollout of system updates. In some cases, mobile device users disregard updates. For example, Google issued a patch shortly after the critical Stagefright vulnerability had surfaced, but months later, the patch still had not been applied to tens of thousands of devices.

Protection Requires Employee Awareness, Respects Privacy

Employees want to use their own devices and expect a consumer-like experience regardless of whether they're messaging with a friend or emailing the latest corporate revenue forecast to a colleague. Employees believe these devices are as secure as computers. Rising privacy concerns and the need to free up device resources prompt some users to disable critical security controls. Others are unwilling to have solutions on their devices that can collect personal data or give corporate access to personal device resources, such as location.

Allowing employees to access enterprise content across multiple devices also increases complexity for the business. Each operating system is tied to myriad device models, each with unique upgrade cycles, resulting in a management nightmare for IT. Further complicating security is unauthorized use of cloud services (file sharing, storage, etc.), which can expose unsecured enterprise content to tremendous risk.

All of these challenges exacerbate the risk of falling victim to cyberattacks. Organizations must employ solutions that don't impact performance or device battery life because end users won't sacrifice either. In addition, they need solutions that manage security confidently and cost effectively on a vast array of device makes and models.

Check Point Mobile Threat Prevention

Check Point Mobile Threat Prevention is designed to provide complete protection from threats by extending visibility over the device (OS), mobile apps, and the network. It uses malicious app detection to find known and unknown threats by applying threat emulation, advanced code flow analysis, app reputation, and machine learning.

The solution analyzes apps to detect known and unknown threats and assess device-level (OS) vulnerabilities to reduce the attack surface. It can be integrated with existing mobile device management or enterprise mobility management solutions and can monitor network activity to identify suspicious behavior.

Check Point Mobile Threat Prevention is designed to integrate with mobile device management or enterprise mobility management solutions to provide comprehensive protection and simplify deployment. It can also provide threat intelligence support to an organization's existing security information event management system and tie to the rest of the existing security infrastructure to create cohesiveness from multiple attack vectors. Check Point is also well aware of balancing the need to apply protection while respecting end-user privacy.

The solution can protect sensitive business data at rest, in use, and in transit on iOS and Android mobile devices. Customers can view device states and take action when an issue is detected through a Web-based management console. The data can be fed into existing security information event management systems, supporting the ability to gain full situational awareness over the quantity and types of mobile threats that can impact the business.

Check Point Mobile Threat Prevention is bolstered by a proprietary, cloud-based Behavioral Risk Engine (BRE) that detects and mitigates mobile threats without performance impacts or battery drain. The BRE identifies suspicious patterns and behaviors over time by sandboxing apps in an emulator to understand exactly how they interact with specific device types and the risks these interactions may pose.

The BRE enables Check Point to detect threats at the device, app, and network levels, and to do so in a way that is highly reliable. The analysis can identify exploitation of mobile device vulnerabilities, including phony certificates, unusual configuration profiles, and network setting changes. It can be configured to alert incident responders or quarantine a problematic device by blocking all network connections until the threat has been removed.

Check Point also offers Capsule Cloud, a lightweight SaaS-based version of Capsule that may appeal to a broad range of enterprises. Capsule Cloud tunnels mobile devices and laptops through its inspection service to conduct URL inspection, antivirus, antibot, threat emulation, intrusion prevention, and HTTPS inspection capabilities. Capsule Cloud supports Windows clients, and Check Point has plans to extend support to Android and iOS devices. Check Point also offers a Mobile Access Blade for remote access through an SSL VPN.

Check Point Challenges

Check Point's mobile security offerings appeal to its customer base. To get the most comprehensive protection from advanced threats, organizations would derive more value from combining the solution with other products in Check Point's portfolio, such as specialized threat analysis and protection products for advanced threat detection.

Conclusion and Guidance

Early adopters of mobility management solutions have quickly learned that external factors — the adoption of SaaS-based services for secure collaboration, data storage, and backup and file sharing among business partners — have created the need to bolster existing controls that simply validate end-user adherence to basic security policies. Customers should consider the following guidance when evaluating additional mobile security protection:

- Review existing mobile security and data protection policies to determine if they need updating. Consider how effectively they have been communicated to employees and if existing security controls are capable of enforcing them.
- Identify solutions that can detect static (known) threats and provide behavioral analysis of anonymized user data to identify risk indicators that signal a new or advanced threat.
- Assess where gaps exist and identify solutions that integrate with existing investments to complete the mobile security stack. Security solutions should accommodate business needs by extending corporate policies wherever employees are located and on whatever devices are used to access information.
- Examine the mobile security solution's ability to integrate with a variety of mobile solutions and network infrastructure. A mobile security solution that integrates with endpoint security, identity management, network security, network access, data security, and security management will result in the most comprehensive protection.

IDC believes Check Point Mobile Threat Prevention is a strong solution for any organization attempting to create a cohesive security architecture that extends comprehensive protection to mobile devices. It increases visibility over threats and has demonstrated that it can protect sensitive corporate data from eavesdropping and targeted attacks. The solution also goes a step further by respecting employee privacy while applying behavioral analysis to the anonymized data it collects to identify emerging mobile threats. It can be configured to alert incident responders or to quarantine a problematic device by blocking all network connections until any threats have been removed.

Mobile device management or enterprise mobility solutions were a great first-generation approach to mitigating mobile risks, but they require additional support against a rising tide of sophisticated attacks on mobile devices. Modern mobile protection must be different. It can't simply be a mobile antivirus app that scans applications and performs antiquated antivirus-like scans because modern device firmware limits the visibility and control those mobile security apps can provide. Any solution your organization evaluates must provide protection from network-based attacks used by criminals to eavesdrop on victims. It should be able to identify mobile firmware vulnerabilities and block attempts to exploit those weaknesses. And it must address the threats posed by malicious applications, custom malware, and application vulnerabilities that cause data leakage.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com