ılıılı cısco

Cisco AppHQ Enterprise Application Center: Deploy Mobile Business Apps with Confidence

The Enterprise Exposed

The post-PC era is here, thanks to next-generation mobile devices and applications. And although mobile applications are helping to transform the workspace (Figure 1), these applications expose the enterprise to new threats, creating new security challenges for IT organizations that must find:

- A rapid and reliable security vetting process for mobile apps
- · A central repository for secure distribution and management of apps
- A means of ensuring apps remain secure in a dynamic threat environment

The Cisco AppHQ[™] enterprise application center addresses these needs, delivering Cisco controlled mobile application vetting, publishing, distribution, and management to IT while offering end users a friendly app center experience.

Figure 1. In 2011, Tablet and Smartphone Purchases Exceeded PC Purchases¹



The Mobile Majority

New research from Forrester indicates that half of U.S. information workers spend less time working out of their offices and more time working from home and other remote locations.² Work is no longer a location people go to. Rather, it is what people do wherever they may be. The increasing trend toward mobility also represents a changing workforce with new behaviors and expectations.

¹ Deloitte, Smartphones and tablets: More than half of all computers aren't computers anymore.

² Forrester, Q2 2011 US Workforce Technology and Engagement Online Survey

Cisco's second annual Connected World Technology Report, which surveyed nearly 3000 college students and professionals under 30, notes that 66 percent of students and 58 percent of young professionals consider a mobile device their most important technology, and two out of three workers around the world now believe they do not need to be in the office to be productive. These new attitudes, expectations, and demands are creating new challenges for companies, as they strive to balance current and future employee and business needs amid expanding mobile capabilities and security risks (Figure 2).



Figure 2. Employees Have New Attitudes about Technology that Create New Risks for the Enterprise³

The New Threat Landscape

Next-generation mobile devices and the apps that enable people to collaborate in new ways will fuel the next wave of business productivity, growth, and innovation. At the same time, the shift toward mobility can expose the enterprise to risks that require changes in their security policies. These risks include:

- Attackers are adjusting their focus from the desktop to mobile devices: According to the Cisco 2010 Annual Security Report, "PC vendors are building better security into their products" and it is "increasingly timeconsuming and resource-intensive to find ways to exploit PC platforms. As a result, cybercriminals are shifting their focus to mobile platforms."
- Developers have not factored mobility into their programming practices: App developers are used to relying
 on the enterprise to secure desktop applications within organizational boundaries. However, as
 applications and corporate data move outside of traditional boundaries, developer practices such as
 hardcoding passwords and allowing access to protected files or contact lists within mobile applications can
 result in serious data breaches.
- The line between consumer and business apps is blurring: With more consideration being given to employees bringing their own devices into the workplace (that is, bring your own device [BYOD]), consumer apps are also making their way into the enterprise. This situation represents a new threat. According to

³ Cisco Connected World Report, 2011

digital forensics company viaForensics, 83 percent of the consumer apps it evaluated either warranted a security warning or failed basic security tests⁴ (Figure 3).



Figure 3. Consumer Apps Can Compromise Security Because Many Fail Basic Security Tests

Source: viaForensics, appWatchdog Findings, July 2011

It takes only one app with malware code on one mobile device for a hacker to gain access to your enterprise. The cost to deal with this type of attack has grown substantially. In its second annual Cost of Cyber Crime Study published in 2011, the Ponemon Institute found that the median annual cost of cyber crime for the 50 organizations it surveyed was \$5.9 million per year, representing an increase in median cost of 56 percent from its first cyber cost study published in 2010.⁵

"The median cost of cyber crime is \$5.9 million per year." – Ponemon Institute, 2011 Cost of Cyber Crime Study

All of these factors necessitate a shift in security practices, according to research firm Ovum, which says, "It is no longer enough to secure mobile devices." Ovum sees the new challenge for chief information officers (CIOs) as a move from managing desktops to applications.

"The CIO is now going to be dealing with managing public and private mobile applications."

- Mike Sapien, Principal Analyst, Enterprise Practice, Ovum

The Mobile App Security Dilemma

In October 2011, IDG Research conducted a survey of 115 IT security professionals. Survey results indicated that 94 percent of respondents believe there is inherent risk in supporting a mobile workforce. Risks include unauthorized data sharing, data loss, and the introduction of viruses or malware to the corporate LAN. And although enterprises recognize the need to implement strong security measures for mobile apps, they are struggling with how best to do it.

"59 percent of respondents reported that they are somewhat or not at all effective at minimizing mobile security and compliance risks." – IDG Research, October 2011

⁴ viaForensics, appWatchdog Findings, July 2011

⁵ http://www.arcsight.com/collateral/whitepapers/2011 Cost of Cyber Crime Study August.pdf

Companies could, of course, decide to secure mobile apps on their own. However, most IT organizations today are overworked and underfunded, making it difficult, if not impossible, to thoroughly vet all mobile applications and remediate every security vulnerability. Companies that decide to secure mobile apps themselves typically end up having to prioritize remediations, leaving them still vulnerable.

Of greater concern, companies do not have the technical competence to monitor sites that could breed malware, nor do they have the capability to maintain heuristic algorithms that could catch them. And although many organizations have dedicated security teams, the expertise of these teams is almost assuredly based on securing the network and the devices connected to it versus securing the applications that run on those devices.

Acquiring the application security expertise and the myriad of mobile app security tools needed to provide enterprise-grade protection can be a lengthy and costly process. As a result, there is a growing reliance on consumer marketplaces to police and secure these apps. But a recent CSO article indicates that "poor vetting and unregulated third-party markets means there are few guarantees when downloading apps."⁶ Enter the Cisco AppHQ enterprise application center (Figure 4).



Figure 4. The Cisco AppHQ Enterprise Application Center Lets You Deploy Mobile Apps with Confidence

The Cisco AppHQ Enterprise Application Center: Mobile App Validation for Mission-Critical Security

In its report on cybersecurity for a mobile world, Accenture states, "Organizations need to be able to evaluate an app's strength and ability to process and handle sensitive information throughout its development lifecycle." According to ZDNet, a corporate app center is a viable way for businesses to safely acquire mobile software.

"(Enterprise) app stores are not only viable, but an increasingly preeminent way in which software is acquired." - ZDNet, Enterprise App Stores Arrive, May 21, 2011

⁶ <u>http://www.csoonline.com/article/686128/android-app-vetting-is-still-weak-says-security-developer</u>

Every application published to the <u>Cisco AppHQ</u> enterprise application center - whether developed by Cisco or by members of the Cisco[®] Developer Network Marketplace - undergoes an extensive multistep validation process that goes beyond basic malware protection to include:

- Mobile threat management
- Risk intelligence
- Vulnerability tracking

Vet Apps Using Enterprise-Grade Security Policies and Business Rules

This unified approach is far more than a red light/green light approach to mobile app security. Before apps are published to the Cisco AppHQ enterprise application center, they are thoroughly evaluated using custom security policies and business rules defined by Cisco, an industry leader in securing the enterprise. Business rules are applied during static and dynamic analysis. This enterprise-grade vetting process delivers a level of proactive protection and application visibility that can be rigorous enough to help meet the security needs of enterprises in every industry, including those in financial industries, military, and defense.

Uncover Malicious Intent with Unique Static Analysis Detection Technology

Mobile business apps are very complex and require very stringent vetting. Unlike other static analysis scanning engines that repurpose desktop security tools to simply scan lines of code, the Cisco AppHQ solution uses a bestin-class heuristics engine that accounts for the complexity of mobile applications. Its innovative detection technology is built for mobile app security. As a result, it can help:

- · Discover malicious code and enterprise policy violations within apps
- · Detect previously unknown threats as well as new malware variants
- · Identify apps that contain potentially unwanted behavior but are not classified as malware

A context-directed engine goes beyond analyzing code. It uses Artificial Intelligence (AI) to ferret out malicious behavior in apps. The system also learns with every app scanned, sends learned behavior to the back-end threatmanagement system, and applies risk intelligence to the entire system (Figure 5). And at any time throughout the life of an application, the system can quarantine the app, effectively preventing it from being downloaded until it has once again been deemed safe.



Figure 5. Cisco AppHQ Analyzes Suspicious Limbs for Malicious Code and Tracks Them Down to the Roots

Because the Cisco AppHQ enterprise application center also checks for valid version codes and signatures⁷, it can protect mobile business apps from being hijacked by verifying the original author and validating all future application updates and releases. Without these checks in place, an attacker could modify or inject malicious code into trusted apps.

Prioritize Threats with Dynamic Analysis

Prior to publication, the system also performs dynamic software execution analysis. Business apps are run through a wide variety of scenarios designed to uncover malicious intent. This analysis extends to the framework level, allowing Cisco to sandbox an application and monitor its interactions. With its advanced, rules-based engine, the Cisco AppHQ solution:

- Makes informed decisions, based on historical data, about the intent and risk factors associated with each app
- Prioritizes threats and instantly bans applications, whether they are globally malicious or simply because they are not compliant with Cisco security policies and business rules
- Prevents zero-day assaults⁸ with a series of security checkpoints that help ensure high-risk code quickly bubbles to the top of the threat management queue

This rigorous analysis provides a deeper understanding of apps and facilitates a higher level of risk management with control that goes beyond labeling apps as simply "good" or "bad". Apps within the Cisco AppHQ enterprise application center are scored not just on **security**, but also on **privacy**. In addition to app behaviors, manifests⁹ and permissions are also analyzed. For example, if an app:

 Requests to "read calendar", the system raises a red flag for a potential privacy issue, because calendars contain meeting IDs, contacts, meeting times, etc.

⁷ Signatures are mathematic schemes for demonstrating the authenticity of a digital message or document.

⁸ Zero-day assaults: Attacks that take advantage of vulnerabilities in software that are unknown to the developer (and other users) before the attack happens.

⁹ Manifests: Android apps require a manifest file. Manifests are XML files that explicitly present essential information about the app to the Android system. The Android system must know the manifest information before it can run any of the app code.

 Contains unsecured content providers or is debuggable¹⁰, the system alerts Cisco to these permission leaks

Scan report information for a given mobile app can be made available to IT administrators, upon request.

When published, ongoing scanning helps ensure that apps remain secure throughout the life of the software. Ongoing scanning occurs automatically, independent of security event triggers. In addition, apps are automatically rescanned if:

- Business rules change
- A new malware signature, behavior, or footprint is discovered
- · New knowledge is acquired by the system

When red flags are raised during static or dynamic analysis to indicate noncompliance with business rules or vulnerabilities, Cisco engages with the application developers. The developers can then address the concerns identified and resubmit applications for validation testing and publication. When informed about security or privacy issues, the vast majority of developers revise their code to meet Cisco standards. This process can help developers create better and safer apps, and make the mobile workplace safer for everyone.

Take Advantage of Terabytes of Knowledge with a Market-Leading Infrastructure

The Cisco AppHQ enterprise application center uses a market-leading cloud computing infrastructure that is far superior to device-based scanners, because it takes advantage of terabytes of knowledge based on every app ever analyzed by the system. It acquires app code knowledge through:

- · Research and academic communities
- Corporate partners
- Consumer end users
- · Third-party app stores
- Various websites and forums
- Honeypots¹¹

Rapid scalability, real-time queries across the knowledge system, and automatic integration of autonomous knowledge creation make it possible to:

- Analyze large sets of applications
- · Deliver a risk assessment within seconds and without human intervention
- Discover newly developed malware and instantly assess risk, so Cisco can quickly determine whether to publish, ban, quarantine, or remove apps

A Long History of Protecting the Enterprise

Cisco is by far the largest vendor of security solutions in the world, with a long history of delivering innovative solutions to address the security concerns of the enterprise. One of these innovations includes Cisco Security Intelligence Operations (SIO), the largest threat telemetry service in the world.

¹⁰ Debuggable: Developers can set or flag an app as debuggable to help them solve problems and run analytics while writing the app. If the debuggable flag is left when the app is published, any user can attach to the app using Java Debug Wire Protocol (JDWP) to extract vital app information and even execute code on behalf of the debuggable app.

¹¹ Honeypots are a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems http://en.wikipedia.org/wiki/Honeypot_(computing), 2012.

The Cisco AppHQ enterprise application center is yet another example of how Cisco puts the power of the network to work for you with an innovative solution that is designed to help IT organizations secure mobile business apps by uncovering malicious intent, prioritizing threats based on business rules, and by using terabytes of knowledge to help keep your corporate network and your intellectual capital safe.

For More Information

For more information, please visit:

Cisco AppHQ solution: <u>http://www.cisco.com/go/apphq</u>



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA