Tackling the Mobile Device Challenge with Tenable

White Paper

Introduction

For all intents and purposes, the underlying business drivers and technology trends are pretty much irrelevant. It's not the rise of user mobility and expectation of increased productivity, the proliferation of mobile device types, or the consumerization of IT that really matters. All that really matters is that highly capable mobile devices – be they PDAs, smartphones, or tablets – are now an unavoidable part of the enterprise computing landscape. Even more to the point is this ever evolving and steadily growing population of devices is accompanied by a number of security and management challenges that are not only relatively unique, but also potentially quite damaging to organizations that fail to get a handle on them.

Just a handful of the more notable mobile device issues, concerns, and derivative implications that now confront organizations of all types and sizes worldwide include the following:

- **Mobile devices are not "active scanner friendly."** For the most part, the major mobile operating systems have been designed from the outset to be inherently more secure than their traditional desktop brethren. Without getting into a lot of detail, the resulting locked-down approach taken by the developers of these platforms essentially precludes the use of network-based active scanners to conduct vulnerability and configuration assessments. This not only means that mobile devices fall outside the scope of the traditional vulnerability and security management systems employed by most enterprises, but also implies the need for an alternative way to detect mobile device vulnerabilities.
- **Mobile devices are inherently transient.** By their very nature, mobile devices routinely come and go from the enterprise network. The initial point of connection to the network is also subject to frequent change. Because they are not fixed assets, like ordinary desktops, it will be necessary to cast a wider net when trying to detect their presence and the activities in which they are engaged. Network-based monitoring alone is unlikely to be sufficient.
- **Mobile devices are often not owned or managed by IT.** Coupled with the likelihood they will be used for a combination of both personal and business purposes, this condition introduces greater variability – and therefore uncertainty – with regard to the configuration details and state of vulnerability for mobile devices on your network. To be clear, the same concerns still apply for devices that are owned and managed by IT; it's just that they're not as great due to the additional insight and control IT has at its disposal. The implication, however, remains the same: IT must do whatever it can to boost its visibility and control, particularly when it comes to mobile devices.
- **Mobile devices are harder to control/protect.** Because they often operate beyond the boundaries of the corporate network, mobile devices are more frequently and directly exposed to malware and other types of threats. In addition, relatively few mature countermeasures are available (and in some cases allowed – think Apple with iOS) to run on these platforms. Complicating matters further is the growing diversity of mobile device types and platforms. This reinforces the point that organizations must bolster their defenses for mobile devices in any way they can, but also highlights the need for solutions with broad applicability.
- **Mobile devices introduce new risks.** The combination of small portable devices, with significant potential for loss or theft, and those device's ability to store vast amounts of potentially sensitive or protected data opens yet another attack vector. This risk exacerbates these other concerns, and brings more urgency to the task of monitoring, tracking, and managing such devices.

How Tenable can help

The components that make up the Tenable solution for mobile devices are ones many organizations already have in place to help with their broader vulnerability, security event, and compliance management objectives. They include:

SecurityCenter – A central management console, SecurityCenter facilitates and unifies essential security processes for discovering network assets, conducting configuration and compliance audits, detecting vulnerabilities and data leaks, and managing corresponding events. Among its many functions, it serves as the primary interface for administrators to view, analyze, process, and report on the mobile device asset, vulnerability, and activity data gathered by other Tenable components.

Passive Vulnerability Scanner (PVS) – A software-based network discovery and vulnerability analysis solution, PVS delivers real-time network monitoring and profiling for continuous assessment of an organization's security posture in a non-intrusive manner. PVS monitors network traffic at the packet level to determine topology, provide visibility into both server and client-side vulnerabilities, and identify the flow of sensitive data and the use of common protocols and services (e.g., HTTP, SQL, file sharing). Unlike an active scanner, which takes a snapshot of the network in time, PVS takes a completely different approach by behaving like a security motion detector that continuously observes everything crossing its path, including network activity from mobile devices.

Log Correlation Engine (LCE) – LCE is a software module that aggregates, normalizes, correlates and analyzes event log data from the myriad of devices within your infrastructure. LCE can be used to gather, compress and search logs from any application, network device, system log or other sources. This not only makes it an excellent tool for forensic log analysis, IT troubleshooting and compliance monitoring, but also provides an ideal means to "cast a wider net" and obtain additional pieces of the mobile device puzzle – pieces that are often essential to establish details such as user and device identity.

Along with Nessus – the world-leading leading vulnerability scanner – these components form the backbone of Unified Security Monitoring, a Tenable solution that unifies real-time vulnerability, event, and compliance monitoring into a single, role-based interface for administrators, auditors, and risk managers to evaluate, communicate, and report information necessary for effective decision making and systems management.]

Some of the specific ways the Tenable solution helps today's organizations with the mobile device challenge include enabling them to:

- Identify rogue (i.e., unknown and/or unwanted) mobile devices
- Identify and classify mobile device vulnerabilities
- Identify mobile user/device activities, such as applications and services being used
- Identify policy violations, as well as drains on user productivity
- Identify the overall level of risk attributable to mobile devices
- Bring mobile devices back into the fold of a centralized, enterprise-class management system

How the Tenable solution works

Mobile devices and their users typically interact with the enterprise network in a handful of different ways. Common options include:

- Local connection via wireless access point, with potentially broad access to internal resources;
- Remote synchronization for email and calendaring via Exchange ActiveSync®;
- Remote connection directly to web-enabled, DMZ-based applications;
- Mobile device resident apps and,
- Remote connection via an access gateway, such as an SSL VPN, which supports either limited, proxy-based access and/or full-network level access.

The good news is the Tenable solution addresses all of these scenarios, and more, with the same set of capabilities. In particular, not only can network administrators detect the presence of mobile devices, classify them by manufacturer and platform, and identify associated vulnerabilities, but also monitor ongoing activity, correlate other data sources to reveal further details, and respond to any findings that require further attention.

Mobile device detection and vulnerability assessment. A major strength of the Tenable solution is that it can detect mobile devices simply from the network traffic they generate. There's no need to perform an active scan and the detection capability, by design, is always on. Related PVS plug-ins identify the manufacturer, operating system, and version for each mobile device in real-time. A combination of additional plug-ins and platform-specific intelligence subsequently enable identification and classification of applicable vulnerabilities by severity level (i.e., high, medium, and low).

Using SecurityCenter, administrators can view and create associated dashboards, drill-down to obtain further detailed information about specific vulnerabilities and devices (e.g., IP address, MAC address, and point of access), and even elect to accept or re-classify the associated risk – for example, based on enterprise-specific preferences or first-hand knowledge of mitigating conditions. IT can easily track important trends, including the total number of mobile devices detected over a period of time, the total number of devices with high severity vulnerabilities, or the total number of vulnerabilities period. Taking advantage of SecurityCenter's flexibility and extensive customization capabilities, administrators can even create a dashboard to identify unapproved (or unmanaged) mobile devices based on excluding all those that fit a specified "corporate" profile.

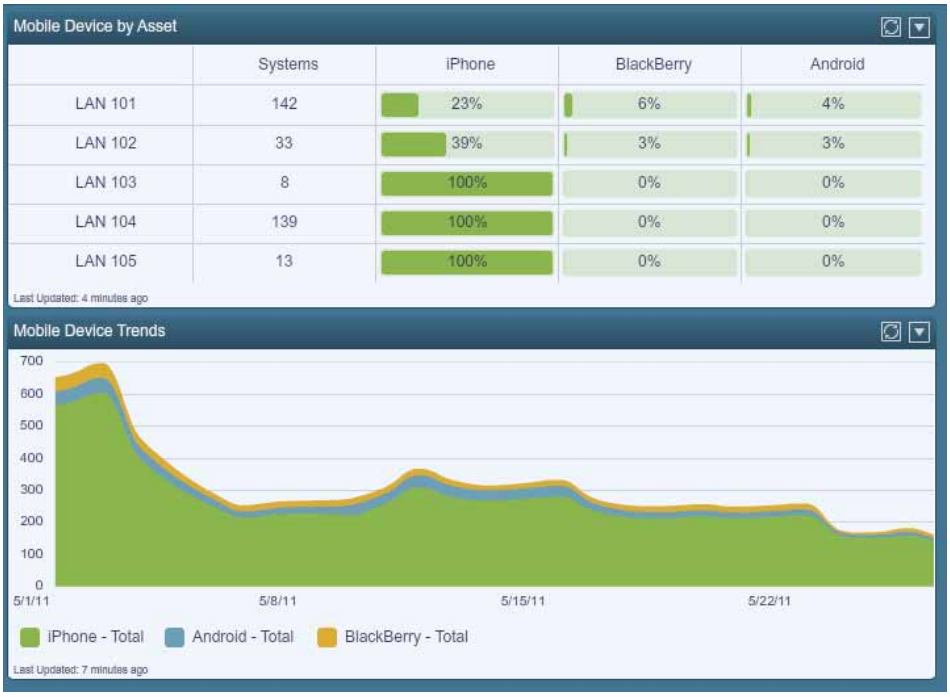

Figure 1 SecurityCenter, from Tenable, provides up-to-the-minute insights into the type, location, and number of mobile devices on your network.

Mobile device monitoring. Besides detecting mobile devices in the first place, the Tenable solution can also monitor what they are doing on your network. Web client enumeration, web query lookups, and DNS query lookups are just a few of the mechanisms that supplement traditional port and destination address information to establish the applications and resources being accessed by a given user/device. The output in this case can be used by administrators to identify policy violations, the frequency and volume of unproductive user activity, and the type/sensitivity of information that is accessible – an important detail that might point to the need to invest in additional mobile device security solutions.

Mobile device correlation. Bringing Tenable LCE into the mix unlocks further capabilities while expanding the scope and precision of mobile device monitoring. For example, an extensive set of ActiveSync normalization rules not only supports detection of all related activity, but also reveals the user identity associated with each mobile device. Administrators can then apply IP tracking functionality across all collected logs both to supplement the mobile device activity already detected by Tenable PVS and to associate a specific user with each detected event or activity. Depending on the environment, other sources for linking user identities to devices may be available as well (e.g., a mobile-aware SSL VPN).

The net result is that with LCE organizations obtain a wealth of additional information that can be analyzed (a) to provide further insight into the extent and nature of mobile device activity on the corporate network, and (b) to facilitate and/or justify taking the next step – such as finding and remediating vulnerable devices, modifying policies, adjusting access rules for specific resources, or implementing additional countermeasures.

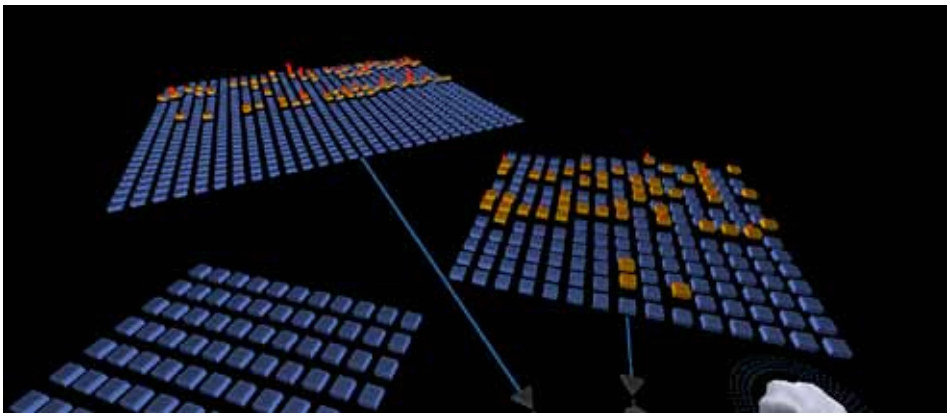

Figure 2 Complex relationships among mobile devices are revealed using Tenable's 3D Tool, a component of Security Center. Mobile devices are highlighted on the graphical display, while vulnerabilities are flagged with color-coded markings.

Mobile device response and mitigation. In support of "taking the next step," the Tenable solution includes numerous options for informing IT personnel of the need for action. In addition to ordinary logging mechanisms, extensive alerting logic can be configured to trigger emails, trouble tickets, and in-system notifications. Pre-defined and customized reports can also be created, saved, scheduled, and distributed to keep line-of-business managers and executives fully informed of the mobile device situation for their domain of interest. By arming them in this way with detailed information on mobile device counts, vulnerability profiles, activity levels, and associated trends, Tenable empowers IT and business managers to make well-informed, risk-guided decisions when it comes to the continued use of mobile devices on their organization's networks.

Figure 3 In addition to high level overviews of trends and activities, SecurityCenter provides users with drill-down displays of specific issues associated with mobile devices.

Figure 4 Tenable supports discovery and assessment of virtually all commercially popular mobile device types and operating systems.

Benefits of the Tenable solution

Companies that select Tenable to help address the rapidly mounting challenges associated with mobile devices stand to gain in a number of important ways. To begin with, significant technical benefits include the ability to:

- Simplify infrastructure and operations. The same integrated set of Tenable solutions can be used to unify vulnerability, event, and compliance management for all of an organization's systems, not just mobile devices.
- Facilitate and streamline operations. The load on over-burdened network administrators is relieved, in general, by having greater visibility of mobile devices/users and, more precisely, by related troubleshooting, analysis, trending, and forensic capabilities, plus the ability to prioritize remediation efforts on a risk-aligned basis.
- Help establish the need for supplemental countermeasures. Mobile device findings can be used to quantify the need for other capabilities and tools, particularly relative to protecting sensitive data that is accessed (e.g., file/disk encryption, device-level DLP, and remote lock/wipe).

Equally compelling are the business-oriented benefits of using Tenable. These include the ability to:

- Reduce risk. Insight into mobile device vulnerabilities and activities, such as access to sensitive applications and data, is an essential starting point for taking corrective action.
- Reduce TCO. Tenable eliminates the need for separate security, event, and compliance management solutions for both mobile and non-mobile devices.
- Demonstrate compliance. Administrators can fulfill and document adherence to policies, regulations, and requirements for vulnerability management and activity monitoring of mobile devices and their users.
- Improve user productivity and business process efficiency. The Tenable solution eliminates security and compliance obstacles that might otherwise preclude widespread adoption of mobile devices and the opportunities they enable.

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit www.tenable.com.

TENABLE Network Security®

Corporate Headquarters: 7063 Columbia Gateway Drive, Suite 100, Columbia, Maryland 21046
Contact Us: Please visit www.tenable.com or call us at 410.872.0555