tenable
network security

VERISTOR

Brought to you by Veristor

veristor.com | contact@veristor.com

Tackling the Mobile Device Challenge with Tenable

June 17, 2015

(Revision 2)

Table of Contents

Introduction

For all intents and purposes, the underlying business drivers and technology trends surrounding the use of mobile devices in the workplace 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 thatmobile 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 alsohighlights the need for solutions with broad applicability.

- **Mobile devices introduce new risks.** The combination of small portable devices, with significant potential for loss ortheft, and those devices' 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 placeto help with their broader vulnerability, security event, risk assessment, and compliance management objectives. They include:

SecurityCenter Continuous View – Tenable's SecurityCenter Continuous View™ (SecurityCenter CV™) is the only continuous network monitoring™ solution, which provides the most comprehensive and integrated view of enterprise health.

- Broadest coverage of networks, devices, systems, virtual, mobile, and cloud services
- In-depth detection of vulnerabilities, misconfigurations, malware, and real-time threats
- Advanced analytics with actionable information and trending to prioritize events/alerts
- Highly customizable dashboards, reports, and workflows for rapid response
- Continuous assurance using Assurance Report Cards (ARCs) that communicate the effectiveness of security investments

SecurityCenter Continuous View is comprised of the following components:

Nessus – Tenable's Nessus® is the world's most widely-deployed vulnerability, configuration, and compliance assessment product. Nessus prevents network attacks by reducing your attack surface – identifying the vulnerabilities and configuration issues that hackers could use to penetrate your network, whether your network is on-premises, in the cloud, or hybrid.

Passive Vulnerability Scanner – Tenable's Passive Vulnerability Scanner™ (PVS™) continuously monitors network traffic to identify risks and vulnerabilities as they occur in real time. PVS helps you:

- Eliminate blind spots by identifying and analyzing transient mobile, virtual, and cloud assets
- Identify unpatched and compromised applications
- Detect unauthorized and malicious network activity
- Identify vulnerabilities 24/7 to accelerate remediation

Log Correlation Engine – Tenable's Log Correlation Engine ™ (LCE™) collects and aggregates data from firewalls, intrusion detection and prevention systems, and data loss prevention solutions, as well as raw network traffic, application logs, and user activity. LCE helps you:

- Normalize, correlate, and analyze event data from a single console
- Store, compress, and perform full-text search for rapid attack analysis
- Detect the presence of malware running in your environment
- Demonstrate compliance with internal and external mandates efficiently
- Continually assess your security and compliance posture through flexible reporting and consistent metrics

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., critical, high, medium, and low). Security administrators and compliance auditors can use the Tenable's solution and its built-in integration with Apple® Profile Manager, Microsoft® Exchange via Active Directory®, MobileIron MDM, AirWatch®, and Good Technology™ Good for Enterprise to:

- Enumerate iOS, Android-based, and Windows Phone devices accessing the corporate network;
- Provide detailed mobile device information, including serial number, model, version, timestamp of last connection, and user;
- Detect known mobile vulnerabilities, including out-of-date versions of Apple iOS; and,
- Discover jailbroken iOS devices

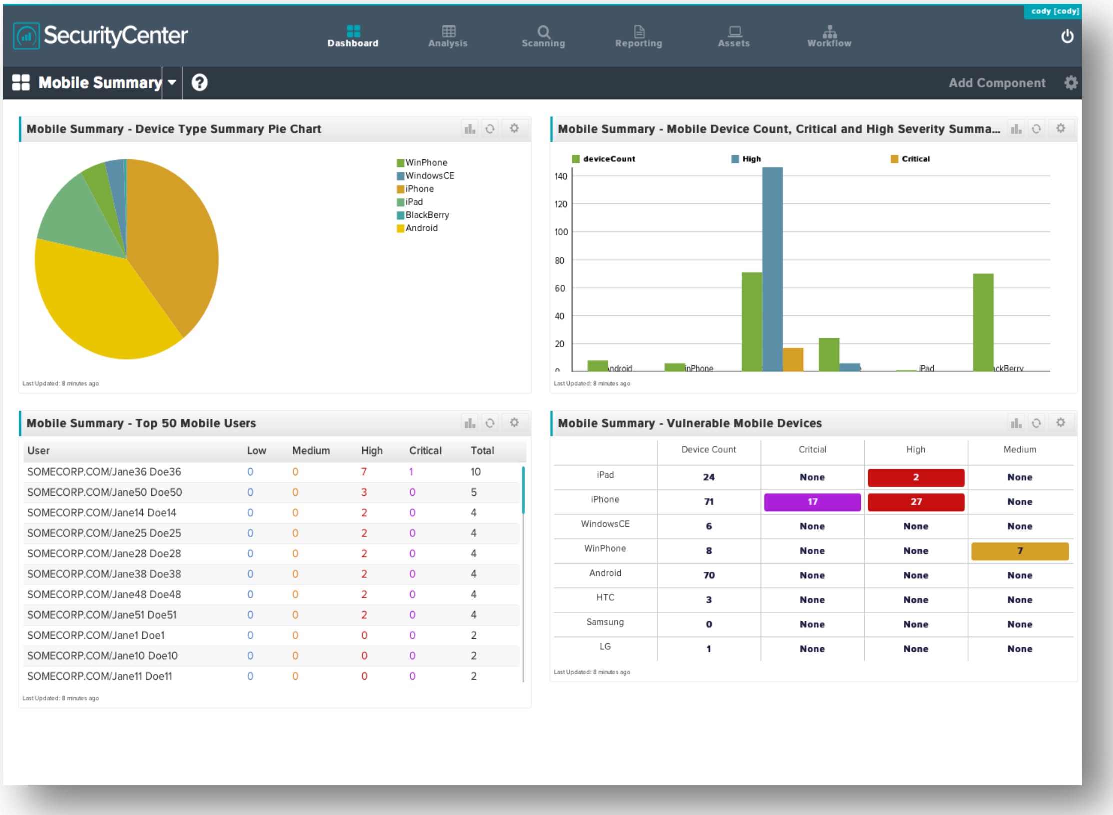
With more than one million users worldwide, Nessus is the global standard in detecting and assessing network data. Nessus solutions scale from the most comprehensive vulnerability assessment toolset on the market to a highly integrated vulnerability management solution that supports security teams. With both on-premises and cloud-hosted solutions, it offers complete flexibility in how and where you deploy vulnerability management.

With the introduction of Nessus 6.4, deeper integration is provided for MobileIron and AirWatch MDM systems. Nessus 6.4 provides more in-depth MDM data so organizations can better protect mobile assets. New metrics available include identifying apps installed on mobile devices (and being able to whitelist and blacklist specifics apps), and identifying new mobile devices connecting to the network as well as mobile devices that haven't connected in a designated time period. A single Nessus audit file provides all this information, making it very efficient to identify and report on mobile vulnerabilities. Finally, CIS audit files for iOS version 6, 7, and 8 and Android version 2.3, and 4 are now available for Nessus and SecurityCenter Continuous View mobile device assessments.

Using SecurityCenter Continuous View, 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 critical or high severity vulnerabilities, or the total number of vulnerabilities, period.

Taking advantage of SecurityCenter Continuous View'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.

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 Summary - Top 50 Mobile Users

User	Low	Medium	High	Critical	Total
SOMECORP.COM/Jane36 Doe36	0	0	7	1	10
SOMECORP.COM/Jane50 Doe50	0	0	3	0	5
SOMECORP.COM/Jane14 Doe14	0	0	2	0	4
SOMECORP.COM/Jane25 Doe25	0	0	2	0	4
SOMECORP.COM/Jane28 Doe28	0	0	2	0	4
SOMECORP.COM/Jane38 Doe38	0	0	2	0	4
SOMECORP.COM/Jane48 Doe48	0	0	2	0	4
SOMECORP.COM/Jane51 Doe51	0	0	2	0	4
SOMECORP.COM/Jane1 Doe1	0	0	0	0	2
SOMECORP.COM/Jane10 Doe10	0	0	0	0	2
SOMECORP.COM/Jane11 Doe11	0	0	0	0	2

Last Updated: 8 minutes ago

Mobile Summary - Vulnerable Mobile Devices

	Device Count	Criticial	High	Medium
iPad	24	None	2	None
iPhone	71	17	27	None
WindowsCE	6	None	None	None
WinPhone	8	None	None	7
Android	70	None	None	None
HTC	3	None	None	None
Samsung	0	None	None	None
LG	1	None	None	None

Last Updated: 8 minutes ago

Figure 1: SecurityCenter Continuous View, from Tenable provides up-to-the-minute insights into the type, location, andnumber of mobile devices on your network.

Mobile device correlation. Bringing SecurityCenter Continuous View's LCE component 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 address tracking functionality across all collected logs both to supplement the mobile device activity already detected by Tenable's 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 SecurityCenter Continuous View, 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.

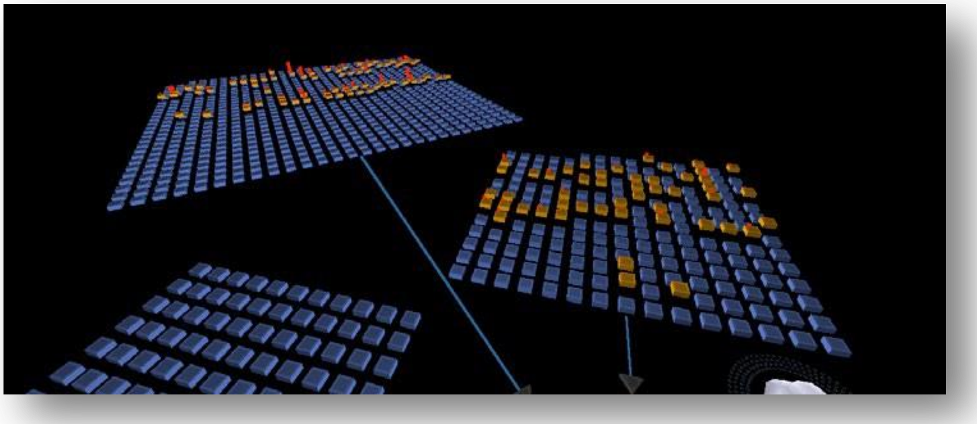
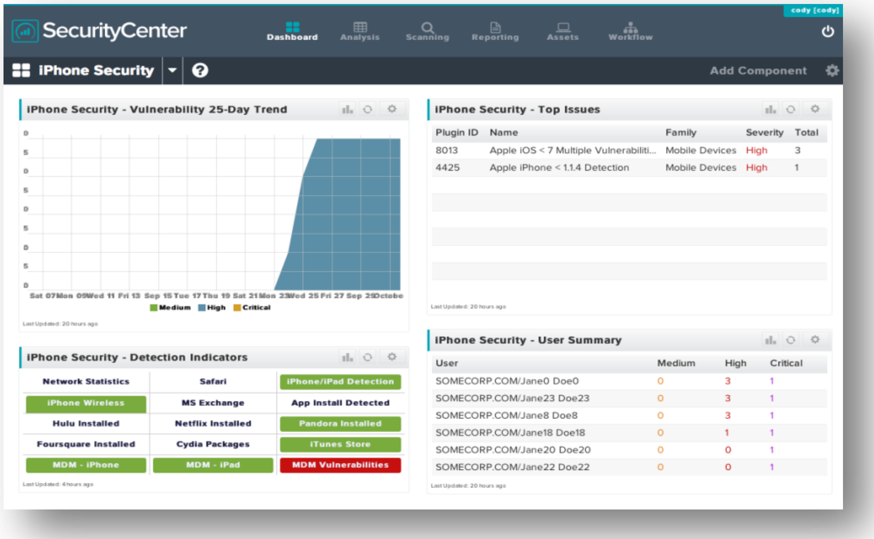


Figure 2: Complex relationships among mobile devices are revealed using Tenable's 3D Tool, a component of SecurityCenter. Mobile devices are highlighted on the graphical display, while vulnerabilities are flagged with color-coded markings.

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.


SecurityCenter
Dashboard
Analysis
Scanning
Reporting
Assets
Workflow
cody [cody]
iPhone Security
Add Component
iPhone Security - Vulnerability 25-Day Trend
0
5
0
5
0
5
0
5
0
Sat 07 Mon 09 Wed 11 Fri 13 Sep 15 Tue 17 Thu 19 Sat 21 Mon 23 Wed 25 Fri 27 Sep 29 Octobe
Medium
High
Critical
Last Updated: 20 hours ago

iPhone Security - Top Issues

Plugin ID	Name	Family	Severity	Total
8013	Apple iOS < 7 Multiple Vulnerabiliti...	Mobile Devices	High	3
4425	Apple iPhone < 1.1.4 Detection	Mobile Devices	High	1

Last Updated: 20 hours ago

iPhone Security - Detection Indicators

Network Statistics	Safari	iPhone/iPad Detection
iPhone Wireless	MS Exchange	App Install Detected
Hulu Installed	Netflix Installed	Pandora Installed
Foursquare Installed	Cydia Packages	iTunes Store
MDM - iPhone	MDM - iPad	MDM Vulnerabilities

Last Updated: 4 hours ago

iPhone Security - User Summary

User	Medium	High	Critical
SOMECORP.COM/Jane0 Doe0	0	3	1
SOMECORP.COM/Jane23 Doe23	0	3	1
SOMECORP.COM/Jane8 Doe8	0	3	1
SOMECORP.COM/Jane18 Doe18	0	1	1
SOMECORP.COM/Jane20 Doe20	0	0	1
SOMECORP.COM/Jane22 Doe22	0	0	1

Last Updated: 20 hours ago

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.

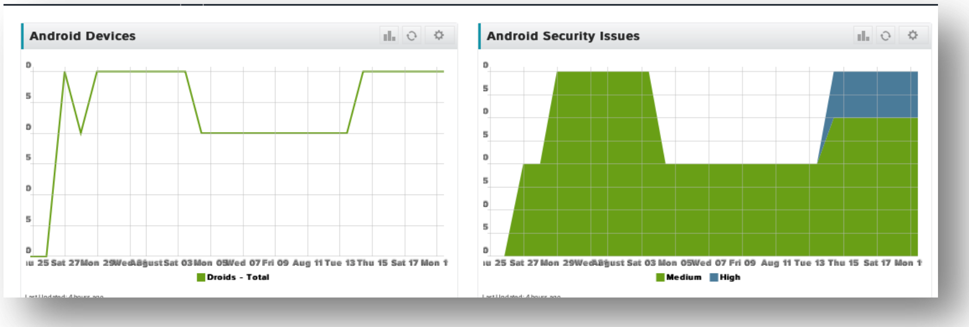


Figure 4: Tenable supports discovery and assessment of virtually all commercially popular mobile device types and operating systems.

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, risk, 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, risk, 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 provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.