Issue 2

Vulnerability Management for Mobility

Identify Mobility Risk through Mobile Device Visibility and Vulnerability Assessment

Vulnerability Management for Mobility

The modern enterprise is highly dependent on mobile devices to keep pace with business demands and to maintain a competitive edge. However, mobile devices remain a key challenge in the security risk they pose. Why?

- The deployment and management of mobile devices lies in the network operations team, and security teams may not be involved in the decision process. As a result, the business drivers for mobile devices may outweigh security concerns.
- Mobile devices connect and disconnect from the corporate network ad-hoc. Because of this, they may not be visible to traditional vulnerability scans.
- With Bring Your Own Device (BYOD) deployments any operating system or application may be running on the mobile device, adding another layer of complexity.

The proliferation of mobile devices has increased the volume of threats and vulnerabilities that target these devices. Organizations must consider a holistic approach to bring together mobile device visibility and vulnerability assessment.

To address these concerns, enterprises should include mobile device assessment (MDM) as part of their vulnerability management offering. However, there is no single template for mobile device vulnerability assessment since organizations have various types of mobile devices, various ways of managing these devices, and the mobile devices themselves are sensitive to security software installed. As a result, choosing a vulnerability assessment solution that addresses these needs and that works with existing IT investments is critical to provide the maximum flexibility and fullest visibility of mobile risk.

The following research outlines how vulnerability management solutions are capturing the risk from mobility, what technologies are used to assess mobile devices, and which vulnerability management vendors offer the broadest coverage.

Featuring research from Gartner

Of the vendors evaluated, Tenable Network Security offers one of the broadest mobile device assessment coverage that includes:

- Enterprise Mobility Management Integration including Apple Profile Manager, AirWatch, Good for Enterprise, and MobileIron
- ActiveSync Integration with Microsoft Exchange ActiveSync
- Passive Vulnerability Scanning

Together these technologies allow Tenable Network Security to:

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

Read this Gartner research to understand more about the benefits of integrating mobile device assessment into your vulnerability assessment program, and the capabilities provided by Tenable Network Security.

Source: Tenable Network Security

From the Gartner Files:

Four Ways to Close the Gap Between Enterprise Mobility and Vulnerability Management

Mobile device coverage in vulnerability assessment solutions has not kept pace with mobile device adoption in the enterprise. This has resulted in a growing gap in oversight for security organizations. Here are four options for closing that gap.

Key Challenges

- Mobile and bring your own device adoption in the enterprise continue to increase, but security organizations are not yet including them in vulnerability management programs.
- Traditional vulnerability assessment solutions and methods provide only minimal support for mobile device assessment, complicating the process of including them in the vulnerability assessment workflow.
- Without including mobile devices, security organizations are failing in maintaining responsibility and oversight.
- Security organizations must address the organizational issue that IT and mobile systems are typically managed by distinct organizations.

Recommendations

IT security managers:

- Expand the scope of vulnerability management programs to include mobile devices in addition to traditional devices.
- Assess, select and implement the most suitable best practice for your organization from the ones presented in this research for integrating mobile devices into the vulnerability management workflow.
- Make mobile device assessment capabilities a core requirement for vulnerability assessment product selection.

Strategic Planning Assumptions

By 2019, 80% of vulnerability assessment (VA) vendors will offer enterprise mobility management (EMM) integration capabilities to assess mobile devices, up from 20% today.

By 2017, 40% of enterprises will deploy or extend their VA solution to cover smartphones and tablets, up from 5% today.

Introduction

The adoption of mobile devices in the enterprise has increased year for year,[1] in the case of bring your own device (BYOD) with 62% of employees already using theirs for work purposes.[2] While the usage of EMM (see Note 1) and MDM solutions has grown, these rarely include a focus on vulnerability management in terms of functionality, as EMMs are usually bought and operated by nonsecurity actors, such as IT operations. Integration of VA and management solutions has not kept up pace with the fast growth of enterprise mobility, and VA vendors are behind this curve, leaving organizations to fend for themselves.

The consequence is that smartphones, tablets and other mobile devices are not being included in VA and management programs. This has created a gap in the ability of IT security organizations to gain a centralized, environmentwide view of the true risk and security posture. This hole can only grow wider as mobility becomes a fundamental component of an enterprise.

The purpose of this research is to provide four possible alternative approaches and best practices to plug this gap and consolidate VA and management for mobile and traditional devices.

Analysis

Vulnerability management has grown and evolved over the past decade, with standardized workflows, a shared terminology and a number of

vendor-independent standards, such as Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), and Common Vulnerability Reporting Framework (CVRF). VA solutions have both adopted and helped formalize these further, and provide the technological framework for most vulnerability management programs. In addition, other technologies from the security ecosystem have adapted to the same standards and offer interoperability with these (e.g., security information and event management [SIEM]) solutions.

Traditional vulnerability scanning methods rely on network-based assessments that can connect to a given target via an IP address, interrogate open ports and services, and authenticate remotely. Alternatively, some solutions utilize an installed local agent. In the case of mobile devices, both of these methods pose challenges. Caution is advised when vendor offerings claim to support mobile devices such as smartphones and tablets based on IP-scanning, as it is neither a reliable nor an effective means of assessment. Mobile devices are not designed to provide remote authentication via the network, nor do they as a general rule offer network services to remotely assess. Installing agents requires an entirely different infrastructure and approach than traditional computer systems.

EMM systems, with a shorter history and experience in commercial environments, have rapidly entered the enterprise space. Unlike traditional endpoint protection platforms, EMM tools have focused on managing and securing enterprise mobile devices by enabling them, rather than locking them down. As the buying center for EMM tools is usually closer to IT operations than IT security, VA support has not been the focus of EMM tools so far.

VA vendors have slowly begun adding capabilities to bridge this gap, with ActiveSync and EMM integration the most widely encountered features, and a few maverick vendors providing direct assessment methods. By integrating mobile device management (MDM) technology with vulnerability management, the security organization regains visibility and oversight back over the rapidly growing population of mobile-based assets. This allows mobile devices to be included in risk metrics and reporting, as well as enabling the assessment and management of mobile device vulnerabilities by the IT security organization.

Option No. 1: Direct Mobile Vulnerability Assessment

In direct mobile VA, the VA solution gathers security information locally from the mobile endpoint, usually via an agent in app form. A common approach is to publish the agent app via an official app store (i.e., Google Play Store), allowing end users to install the application themselves. The agent app can then be configured with connection and authentication credentials for a centralized management platform, usually cloud-based, to couple it with the VA solution. This particular method is also suited to a BYOD self-service model.

A native agent app can provide bidirectional communication for direct management by the security organization, for example to schedule scans and audits as required, and to execute scans based on custom profiles. The local system access that an agent app provides also permits deeper security audits, including on application permissions and configuration settings.

Benefits

- A locally installed app directly gathers security-relevant information, instead of relying on operational data and inference.
- Deep security assessments are possible due to direct system access.
- Detailed vulnerability findings and asset inventory data are directly integrated into enterprise vulnerability and risk metrics and reporting.
- Bidirectional integration occurs — the app can be directly managed by the security organization.

Challenges

- It requires the installation and management of a local agent application, and this challenge is compounded as the number and variety of mobile devices increases.
- It's Android only; iOS's security model severely limits the necessary functionality.
- Mobile devices must be able to connect back to the VA management interface, necessitating either an external service to be exposed on the

perimeter, or a cloud-based model providing a centralized public management point.

- It requires access to mobile endpoints by involvement of both the mobile management and VM teams.
- There is currently only a limited selection of available solutions offering this capability.

Sample vendors

BeyondTrust: Retina CS for Mobile is a native mobile VA solution that offers Android device VA via an agent available from Google Play Store. The solution fully integrates with Retina CS for consolidated VA.

Secunia: Secunia offers the free PSI for Android client on the Google Play Store. The PSI can scan for missing patches and vulnerable applications, and provides alerting and app update features. The PSI agent can be configured to integrate with the latest release of Secunia's cloud-based vulnerability and patch management offering, Secunia CSI 7.

Option No. 2: EMM Integration

A small number of VA and management solutions provide the ability to integrate and communicate with third-party EMM solutions. By authenticating to the EMM and utilizing APIs, they are able to access, for example, device and application inventory data, such as the manufacturer, OS and installed application versions.

Coverage is not mature, with VA solutions commonly only supporting a small subset of available third-party offerings, with varying depths of integration. For example, some EMMs apply reputational intelligence to installed apps and maintain other vulnerability and patch information, but not necessarily in a format useful or exportable to a VA solution. In addition, EMM vendors are currently trying to rapidly enrich their suites with enablement features, making integration with VA a secondary item in their road maps.

Benefits

- It reuses already existing agent infrastructure from EMM.
- It permits at least a partial view into security-relevant mobile device data, without the need to gain access to every mobile endpoint.
- Vulnerability findings and asset inventory data are directly integrated into vulnerability and risk metrics and reporting.

Challenges

- VA solutions only support a subset of EMMs. APIs and asset data formats are not standardized, so that unique integration APIs have to be created for every EMM vendor to be coupled. This restricts choice if integration is a stringent requirement.
- The depth and scope of data that is exportable is limited in comparison to native assessment. Very basic implementations will only populate device type (i.e., Android, iOS) and the firmware version, allowing only a superficial assessment.
- Integrations not based on strategic technological vendor partnerships may not be further developed and matured in the future in both the VA and the EMM solution. Vendors must be carefully vetted for future plans in this regard.
- Most implementations are unidirectional and can only fetch device information from the EMM and not initiate assessments or change audit policies.

Sample Vendors

Tenable Network Security: Tenable's Nessus and SecurityCenter can integrate with Good for Enterprise and Apple Profile Manager to gather such information as OS version, model, serial number and similar device data.

McAfee: McAfee Enterprise Vulnerability Manager can be integrated with McAfee Enterprise Mobility Management via McAfee ePO.

BeyondTrust: Retina CS integrates with BlackBerry BES to gather device data.

Option No. 3: ActiveSync (EAS) Integration

Certain mobile solutions are installed on the Exchange Client Access Server and perform VA by comparing device information with vulnerability databases. These solutions leverage the Microsoft Exchange ActiveSync (EAS) protocol that provides synchronization of data such as emails and contacts between the Exchange server and mobile devices, as well as mobile device policy enforcement. EAS has the advantage of being ubiquitous, as it is inbuilt in most modern mobile devices. However, it lacks structure and granularity as the number of policies is limited (e.g., jailbreak detection is missing) and each mobile device supports a different subset of those policies. EAS-based solutions are a lightweight option for organizations that either do not yet have an EMM in place, or have not worked with the department deploying the EMM to cover VA functionality, and need a quick fix to this.

Benefits

- It integrates with existing Windows/exchange infrastructure.
- It does not require additional external services to be exposed.
- It's the most commonly supported method across VA solutions and mobile OSs, as it leverages the broad third-party device coverage that EAS provides.

Challenges

- ActiveSync does not yet provide full-fledged EMM capabilities, and these same limitations limit the data available to VA solutions.
- Security-relevant information is only partially available.
- VA vendor EAS integration implementations must be continuously developed to maintain lockstep with new EAS releases and leverage new features, so vendors must be assessed for their ongoing commitment.
- Support for cloud-based (e.g., Office 365) and third-party EAS implementations (e.g., Lotus) varies.

Sample vendors

BeyondTrust Retina CS and Tenable Network Security offer this capability.

Option No. 4: Passive Vulnerability Scanning

Passive vulnerability scanning (PVS) inspects network traffic on the wire to identify vulnerabilities based on heuristics, such as banner, session, and protocol information. An example is identifying a Web browser's version by inspecting the browser agent string sent when viewing a Web page.

The technology can be used to identify device types, such as iOS or Android devices, OS versions and some applications. The distinct advantage of PVS is that it is nonintrusive and requires no installation or configuration on the end devices.

PVS can only provide limited visibility, as it relies solely on what is available in network traffic to infer pertinent information, such as the application name and version, and associated vulnerabilities. Practically, this means that it can only detect network-enabled applications that send and receive data, and only when they actively do so. Encryption, for example, can severely limit the effectiveness.

PVS for mobile devices is useful as stopgap measure before implementing a more direct method for managed devices, or as an augmentation to more direct access to mobile devices. In the case of unmanaged or even rogue devices, it is the only method. It can either be implemented at the perimeter, or at the border between different network zones, to identify client vulnerabilities via their traffic. This requires mobile traffic to be routed to a network chokepoint on the network that will allow the inspection of all mobile traffic in one place (e.g., via a SPAN port). A good example would be between an organization's wireless LAN (WLAN) and the Internet. Mitigation can then take the form of either informing the device owner that he has to take remediation steps, or by actively blocking access to the network or specific resources for that device.

Benefits

- It's noninvasive; inspects traffic on the wire.
- It allows coverage of noncentrally managed devices requiring access to internal resources.
- It's a suitable stopgap measure when no other option is available.
- It adds additional features, such as activity monitoring and malware activity.

Challenges

- Only vulnerabilities affecting applications that generate network traffic can be detected.
- It can only assess assets that traverse the company network infrastructure.
- It requires network chokepoints to centralize mobile traffic for inspection.
- Network encryption can greatly reduce the effectiveness.

Sample vendor

Tenable Network Security: Tenable offers the Nessus Passive Vulnerability Scanner (PVS).

A Look Forward

Two trends, the general growing proliferation of mobile devices such as smartphones and smartpads, as well as the increasing acceptance and adoption of BYOD policies within enterprises, will increasingly mandate that security organizations regain and maintain oversight over these. As the overall percentage of mobile devices in the enterprise asset population increases, so will the risks.

VA vendors will strengthen and extend their capabilities with tighter partner ecosystems and integrations between VA and EMM technologies, especially for on-premises and remote scanning solutions, where roaming agent support and the associated infrastructure are not feasible. Relying on the EMM capabilities will make any improvement in functionality dependent on parallel improvements in the EMM.

As for many mobile implementations, cloud-based deployments for VA solutions intended to also assess mobile devices have a true advantage with respect to alternatives. We have seen this with secure Web gateways as well as with data loss prevention (DLP) tools. However, as with secure Web gateways (SWGs) or DLP, efficient cloud-based implementations are still far away from being a reality. Cloud and SaaS offerings will be in the vanguard of fully native, direct mobile VA, and will increasingly add functionality that will directly compete with EMM offerings.

EMM vendors will also align more closely with common vulnerability and risk management standards and practices, adding more security capabilities and features themselves. The ability to leverage their already existing agent infrastructure provides an ideal foundation for this. This will also simplify tighter integrations with VA solutions. We are already seeing this trend, with vendors such as Lacoon and Skycure offering pure-play mobile security products that bridge this gap.

As enterprise mobility keeps maturing and network performance will keep improving, these issues will be increasingly easier to solve and bring mobile VA to the mainstream.

Additional research contribution and review were provided by Anton Chuvakin.

Appendix

Table 1. Vendor Options

Vendor	Native Mobile Assessment	EMM Integration	EAS/ ActiveSync	PVS
BeyondTrust Retina CS	X[1]	X[2]	X	
McAfee Enterprise Vulnerability Manager		X[3]		
Rapid7 Nexpose			*	**
Tenable Nessus/ SecurityCenter		X[4]	X	X
Secunia CSI/PSI	X[1]			
Qualys				**

* Rapid7 offers a SaaS mobile security solution called Mobilisafe. There are plans to integrate Mobilisafe with Nexpose
** Via integration with Cisco Sourcefire
[1] Android agent
[2] BlackBerry BES; MobileIron is being planned
[3] McAfee EVM integrates with McAfee Enterprise Mobility Management via McAfee ePO
[4] Good for Enterprise

Source: Gartner (April 2014)

Acronym Key and Glossary Terms

BYOD Bring your own device

EAS Exchange ActiceSync

EMM Enterprise mobility management

MDM Mobile device management

PVS Passive vulnerability scanner/scanning

VA Vulnerability assessment

VM Vulnerability management

Evidence

[1] "Forecast Analysis: Devices, Worldwide, 4Q13 Update"

[2] "User Survey Analysis: Is Bring Your Own Device Job Essential or a Personal Preference?"

Note 1. MDM/EMM

This note refers to mobile device management solutions as enterprise mobility management throughout the document.

Gartner Research Note G00260857, Oliver Rochford Dionisio Zumerle, 30 April 2014

About Tenable Network Security

Founded in 2002, Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk and ensure compliance. Relied upon by more than 24,000 organizations around the world, Tenable's key clients include Fortune Global 500 companies across industries as well as the entire U.S. Department of Defense and many of the world's leading governments.

Our family of products includes SecurityCenter Continuous View™ and Nessus®. SecurityCenter Continuous View allows for the most comprehensive and integrated view of network health. Nessus is the global standard in detecting and assessing network data. With the largest install base and best expertise in our industry, Tenable gives customers the ability to identify their biggest threats and respond quickly.

In 2014 Tenable was selected as a Red Herring Top 100 North America award winner. The company was also named Best Vulnerability Management Solution at the SC Magazine Europe awards. Tenable has been selected as a Deloitte Technology Fast 500 Company every year since 2009.

Our Mission

Tenable founders Ron Gula, Renaud Deraison, and Jack Huffard build technology that secures and protects any device from threats on the Internet – malicious software, hackers, viruses, and more. Tenable wants its customers and every company to have access to the latest and best technology that will ensure they stay connected, online, and in business.

For more information, contact Tenable.