Technical Evaluation Best Practices Guide

How to test enterprise mobile security deployment, device monitoring, threat detection, and support

TABLE OF CONTENTS

Why a test plan is critical

Before selecting an enterprise mobile security provider, it is essential to conduct a thorough evaluation of the technology and its usability to answer four important questions:

1. How will we deploy the endpoint security app to our global employees?
2. How will we monitor the security status of those devices?
3. Will the solution we're testing detect all the different mobile threats our business is facing?
4. Will this vendor's support meet our needs, whether through a knowledge portal, email, or phone?

The answers to these questions will ensure that the enterprise mobile security solution you ultimately select will do what it was designed to do: detect, analyze, and respond to mobile threats.

Lookout

STEP 1: Testing app deployment

How quickly and easily can enterprise mobile security apps be installed throughout my organization?

The first step to evaluating an enterprise mobile security solution is deploying to a test segment of your end-users. This segment can be as small as just your IT team. The most important criteria for defining the segment of users to test is that you want to include both managed and unmanaged devices.

If you haven't already created an inventory of your mobile devices, use this simple Mobile Inventory Spreadsheet to document your devices and environment.

TABLE 1: DEPLOYING MOBILE SECURITY ENDPOINT APPS

STAGE	OBJECTIVE	DESCRIPTION
ADMINISTRATIVE SETUP	Get access to the admin. console for the IT and security team members that will be doing the technical evaluation	This is an easy first step that works best with guidance from a vendor account or support representative
MDM INTEGRATION	Use existing MDM software to distribute the endpoint app to users of managed devices	This requires setup of the Microsoft Intune, VMware AirWatch, MobileIron connector, followed by configuration of tags/labels, application provisioning groups, and iOS configuration profiles
CLIENT PROVISIONING	Configuring apps, emails, or other distribution channels for enrolling end-users	For unmanaged devices (often found in BYOD environments), it's common to distribute the endpoint mobile security app via email
EMPLOYEE ENROLLMENT	Manually or automatically enrolling users' primary and secondary devices	Managed devices will have automatic enrollment, and unmanaged devices will likely require the end-user to open the app and enter an enrollment code

STEP 2: Testing security monitoring

How customizable and easy to manage are the security incident functions?

The second step is to actually experience monitoring the security of mobile devices that have access to your corporate data. This is when you'll input custom policies for your organization based on the level of risk from different types of malware, sideloaded apps, and man-in-the-middle attacks. This is also when you'll set up risk syncing with your MDM, if applicable.

This stage also should include the first use of EICAR samples provided by the vendor to show how the solution detects and responds to potential threats.

TABLE 2: THE SECURITY MONITORING USER EXPERIENCE

STAGE	OBJECTIVE	DESCRIPTION
POLICY DEVELOPMENT	Set the risk level for the full range of covered threats.	Input the level of risk for your organization for different classifications of malware, and when you would like to receive notifications by email.
MDM INTEGRATION	Configure MDM to automatically enforce policies and label at-risk devices.	Each MDM will have a slightly different configuration process.
ALERT CONFIGURATION	Install a malware sample and view the threat detection alert that end-users will receive.	Install the EICAR test virus from Google Play or via sideloading on iOS to see the solution detect the threat and alert administrators.
USER EXPERIENCE	Deep dive into a detection to understand what was discovered, why it was flagged as a risk to the organization, and track its history.	Continue to explore the device list to view your entire mobile fleet to see which devices have encountered mobile threats.

STEP 3: Testing threat protection

How effectively does the mobile security platform detect critical threats?

The third step of testing an enterprise mobile security solution is to evaluate its ability to identify malware, vulnerability exploits, man-in-the-middle attacks, device compromise, and sideloaded apps. In addition, comprehensive testing should include detection abilities on both Android and iOS and the solution's ability to remediate threats through the MDM integration, if present. This stage also includes use of EICAR and other samples provided by the vendor to show how the solution detects and responds to potential threats.

TABLE 3: THE SECURITY MONITORING USER EXPERIENCE

STAGE	OBJECTIVE	DESCRIPTION
CONFIGURE REMEDIATION ACTIONS	Configure remediation actions for each threat level in the console of your MDM solution, if applicable.	As an administrator of a mobile security solution that integrates with an MDM, you're able to configure that MDM's corporate policy rules to take effect for devices with different risk-level tags.
THREAT DETECTION - MALWARE	Test the mobile security solution's ability to detect malware, riskware, and file-based threats.	Confirm that each type of malware is detected and that the remediation actions you configured in the previous step are applied.
THREAT DETECTION – VULNERABILITIES	Test the mobile security solution's ability to detect vulnerability exploits.	Confirm that the mobile security solution detects the vulnerability exploit test file and reports the threat in the console.
THREAT DETECTION – DEVICE COMPROMISE	Test the mobile security solution's ability to detect rooted or jailbroken devices.	Use a rooted Android device and/or a jailbroken iOS device to confirm that the mobile security solution detects these device states.
THREAT DETECTION – SIDELOAD DETECTION	Test the mobile security solution's ability to detect sideloaded applications from both trusted and untrusted developers.	Confirm that the solution takes the configured remediation action, or in the case of an app that has been sideloaded from a trusted location, that the solution detects the app, but no action is taken.
THREAT DETECTION – NETWORK ATTACK DETECTION	Test the mobile security solution's ability to detect a man-in-the-middle attack.	The solution you are testing should not generate man-in-the-middle alerts when connected to your corporate, home, or the Wi-Fi network at a nearby cafe or hotel that uses a captive portal. If any of those connections trigger an alert, chances are it is a false positive. To test the detection of man-in-the-middle, configure an HTTPS proxy on your mobile device to mimic an attack and ensure the solution detects it.

STEP 4: Testing enterprise support

How available and useful is this vendor's support?

SELF-SERVICE

Does the vendor's knowledge base enable you to answer key questions about the solution's functionality without assistance?

PHONE & EMAIL SUPPORT

How responsive and effective is this vendor?

Are they meeting or exceeding the SLA?

Do their support hours match your needs?

MALWARE ADVISORY SUPPORT

Is this vendor able to deliver more information on the impact of a mobile malware detection in your environment?

About Lookout

Lookout is a cybersecurity company that makes it possible for individuals and enterprises to be both mobile and secure. With 100 million mobile sensors fueling a dataset of virtually all the mobile code in the world, the Lookout Security Cloud can identify connections that would otherwise go unseen - predicting and stopping mobile attacks before they do harm. The world's leading mobile network operators, including AT&T, Deutsche Telekom, EE, KDDI, Orange, Sprint, T-Mobile and Telstra, have selected Lookout as its preferred mobile security solution. Lookout is also partnered with such enterprise leaders as Microsoft AirWatch, Ingram Micro and MobileIron. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.