Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2020-118 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /  
JAMES L. SIDORAN  
Work Unit Manager

/ S /  
JAMES S. PERRETTA  
Deputy Chief, Information Exploitation & Operations Division  
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government’s approval or disapproval of its ideas or findings.
CONTINUOUS VALIDATION AND THREAT PROTECTION FOR MOBILE APPLICATIONS

DAEMON MORRELL

LOOKOUT, INC.
275 BATTERY STREET, SUITE 200
SAN FRANCISCO, CA 94111

Air Force Research Laboratory/RIGA
525 Brooks Road
Rome NY 13441-4505

Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

The developed platform uses a predictive security model, based on over 12 years of mobile threat data collection and research using advanced machine learning, that enables threat detection even in cases where no prior signatures exist and before threats exhibit malicious behavior. Mobile Endpoint Security (MES) protects mobile endpoints and infrastructures from Web and Content based-threats (e.g. phishing attacks), Application-based threats and device risks, network-based threats, and also enables deep threat investigation providing administrators unparalleled visibility into the multitude of potential threats and risks within their mobile environment.

Mobile Threat Protection, Mobile Endpoint Security
Table of Contents

List of Figures ............................................................................................................................................... ii
List of Tables ................................................................................................................................................ iv
1.0 SUMMARY ............................................................................................................................................... 1
2.0 Introduction ................................................................................................................................................ 2
  DEPLOYMENTS AND PROOF OF CONCEPT TESTING ........................................................................... 3
3.0 Methods, Assumptions & Procedures .................................................................................................... 4
4.0 Results and Discussion ............................................................................................................................ 5
4.1.1 RISKY APPLICATION VISIBILITY ................................................................................................... 5
  4.1.1.1.a - Insecure use of Data ..................................................................................................................... 6
  4.1.1.1.b.1 - Use of SDKs from social networking clouds such as Twitter and Facebook ...................... 7
  4.1.1.1.c.1 - Actual sending of data to cloud services ................................................................................ 7
  4.1.1.d.1 - Understand what URLs are being accessed by the app and whether these are of low reputation ........................................................................................................................................ 8
  4.1.1.f - Geoview of URLs ........................................................................................................................................... 10
  4.1.1.g – Use of private APIs (iOS) ................................................................................................................ 10
  4.1.1.2a - Custom Policies Allowing Admins to Set Rules Based on App Behaviors ............................. 11
  4.1.1.2b - Blacklisting of Unwanted Applications ..................................................................................... 12
  4.1.1.2c - End-User notification for non-compliant/risky apps ................................................................. 13
  4.1.1.2d - MDM Notification for Non-compliant/Risky Apps ................................................................. 14
4.1.2 ADVANCED THIRD PARTY APPLICATION INVESTIGATION AND “OLD AGE” APP DETECTION ................................................... 16
  4.1.2.1.a - Detection of Apps Removed from App Store ........................................................................... 16
  4.1.2.1.b. - Policy to notify end-users and admins of removed apps ...................................................... 17
  4.1.2.2 – Third Party App Store Deliverables .............................................................................................. 18
4.1.3 MAN IN THE MIDDLE DETECTION ................................................................................................. 20
  4.1.3.1 Content Modification Detection and Alerting ................................................................................ 23
4.1.4 MOBILE VULNERABILITY DETECTION AND MANAGEMENT ............................................................................ 24
  4.1.4.1- Detection of OS vulnerabilities matching databases such as NVD and CVE ............................ 24
  4.1.4.2 - Detection of application vulnerabilities ...................................................................................... 26
  4.1.4.3.a. - Actionable options when vulnerabilities are detected ........................................................... 27
  4.1.4.3.b. - Actionable options when vulnerabilities are detected ........................................................... 28
4.1.5 CONTINUOUS CONDITIONAL ACCESS ......................................................................................... 29
  4.1.5.1 – Device Identification and Lookout Enforcement ........................................................................ 30
  4.1.5.2 - Conditional Access Support for Office 365 using AAD for IDP ............................................... 33
  4.1.5.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

4.1.5.3.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in ........................................................................................................................................ 33

5.0 CONCLUSION ....................................................................................................................................... 34
6.0 LIST OF ACRONYMS ............................................................................................................................. 35
LIST OF FIGURES

Figure 1. Screenshot showing insecure data in motion for an application on an Android device. (Deliverable 4.1.1.1.a.2) .................................................................................................................. 6
Figure 2. Screenshot showing insecure data in motion and at rest for an iOS device, based on Apple ATS (Deliverable 4.1.1.1.a.1 & 4.1.1.1.a.2) ................................................................................................................. 6
Figure 3. Screenshot showing configuration of policy to match use of Social networks (Deliverable 4.1.1.1.b.1) ................................................................................................................................................................. 7
Figure 4. Screenshot showing data from an app that shows access to Cloud services (deliverable 4.1.1.1.b.1) ................................................................................................................................................................. 7
Figure 5. Screenshot of sensitive data (IMEI) being sent to a third-party ........................................................................................................................................................................................................... 7
Figure 6. Dashboard control to enable Phishing and Content Protection (PCP) ........................................................................................................................................................................................................... 8
Figure 7. Device showing that Safe Browsing (Client PCP) is active on the device ........................................................................................................................................................................................................... 8
Figures 8 & 9. Screenshot warnings to end user about malicious URLs that they attempted to access ................................................................................................................................................................................................................................. 9
Figure 10. Screenshot of low reputation and malicious URLs being identified and blocked ................................................................................................................................................................................................................................. 9
Figure 11. Screenshot showing the Geo-location of IPs/URLs within an application ................................................................................................................................................................................................................................. 10
Figure 12. Screenshot showing an application that accesses Private APIs ................................................................................................................................................................................................................................. 10
Figure 13. Screenshot showing the ability for administrators to configure policy violations for application based behaviors. (Deliverable 4.1.1.2.a) ................................................................................................................................................................................................................................. 11
Figure 14. – Screenshot showing the ability for administrators to configure policy violations for application based behaviors. (Deliverable 4.1.1.2.a) ................................................................................................................................................................................................................................. 11
Figure 15. Screenshot showing numerous configuration policies for application based behaviors. (Deliverable 4.1.1.2.a) ................................................................................................................................................................................................................................. 12
Figure 16. Screenshot showing an application that violates the custom policy for applications that access the camera. (Deliverable 4.1.1.2.a). Note that the application is available for Blacklisting because of the violation (Deliverable 4.1.1.2.b) ................................................................................................................................................................................................................................. 12
Figure 17. Screenshot showing that the application violating policy has been blacklisted. (Deliverable 4.1.1.2.b) ................................................................................................................................................................................................................................. 13
Figure 18. Screenshot showing the ability to Blacklist an Android application. (Deliverable 4.1.1.2.b) ................................................................................................................................................................................................................................. 13
Figure 19. Screenshots showing the end user notification that the app they have installed is violating policy and has been blacklisted. (Deliverable 4.1.1.2.c) ................................................................................................................................................................................................................................. 13
Figure 20. Screenshot showing applications that have been Blacklisted can be configured to notify an MDM at a certain threat level. (Deliverable 4.1.1.2.d) ................................................................................................................................................................................................................................. 14
Figure 21. Screenshot from MDM showing that a mobile device has a Blacklisted application (Deliverable 4.1.1.2.d) ................................................................................................................................................................................................................................. 14
Figure 22. Dashboard view of applications that Access Bluetooth, NFC and Accept incoming traffic ................................................................................................................................................................................................................................. 15
Figure 23. Application details that show connectivity for NFC/Bluetooth and accept incoming traffic ................................................................................................................................................................................................................................. 15
Figure 24. Screenshot showing filter for App Store Apps ................................................................................................................................................................................................................................. 16
Figure 25. Screenshot showing an App that came from the Apple App Store ................................................................................................................................................................................................................................. 17
Figure 26. Screenshot showing an App that did NOT come from the Apple App Store ................................................................................................................................................................................................................................. 17
Figure 27. Screenshot showing the configuration options to flag Android Sideloaded Applications and Whitelist/Blacklist specific sources and App stores ................................................................................................................................................................................................................................. 18
Figure 28. Screenshot showing an Administrators notice of an Android Sideloaded Application on a user device............................................................................................................................. 18
Figure 29. Screenshots showing an end user notice of an Android Sideloaded Application detected on their device ................................................................................................................ 19
Figure 30. Screenshot showing the configuration option to Whitelist Android applications. Blacklisting of Android applications was also covered under deliverable 4.1.1.2.b and 4.1.1.2.c ....................................................................................................................................................... 19
Figure 31. Screenshot showing an administrators ability to block a device connected to a Rogue Wifi or a detected MITM attack (Deliverable 4.1.3.1) ........................................................................................................ 20
Figure 32. Admin notification of a MITM threat on a user’s device (Deliverable 4.1.3.1) ....... 21
Figures 33 & 34. End user notification and remediation actions for MITM threat on mobile device. (Deliverable 4.1.3.1) ......................................................................................................... 21
Figures 35 & 36. Screenshots showing the option to whitelist certificates for legitimate proxy of traffic (deliverable 4.1.3.2) ........................................................................................................ 22
Figure 37. Certificate details of a MITM threat (Deliverable 4.1.3.2) ........................................ 23
Figure 38. Screenshot showing a content modification detection (Deliverable 4.1.3.3) ............ 23
Figure 39. Screenshot showing an iOS with out of date OS and the number of unpatched CVEs associated with that release. (Deliverable 4.1.4.1) ......................................................................................... 24
Figure 40. Screenshot showing an iOS release and the details of the associated unpatched CVEs (Deliverable 4.1.4.1) ....................................................................................................................................................... 25
Figure 41. Screenshot showing an Android device with out of date ASPL and the number of unpatched CVEs associated with that release. (Deliverable 4.1.4.1) ................................................... 25
Figure 42. Screenshot showing number of unpatched CVEs associated with a specific ASPL. (Deliverable 4.1.4.1) ....................................................................................................................................................... 26
Figure 43. Screenshot showing Data Handling vulnerabilities for an application (Deliverable 4.1.4.2) ....................................................................................................................................................... 26
Figure 44. Screenshot showing OWASP violations (Deliverable 4.1.4.2) .................................. 26
Figure 45. Screenshot showing an application with a detected vulnerability (Deliverable 4.1.4.2) ....................................................................................................................................................... 27
Figure 46. Screenshot showing device software distributions and associated vulnerabilities.... 27
Figure 47. Device configuration information for Android devices (Deliverables 4.1.4.1, 4.1.4.3) ....................................................................................................................................................... 27
Figure 48. Device configuration information for iOS devices (Deliverables 4.1.4.1, 4.1.4.3).... 28
Figure 49. Screenshot showing the option to Blacklist an application if the identified vulnerabilities are too risky to ignore ........................................................................................................... 28
Figure 50. Overview of how Continuous Conditional Access work ........................................... 30
Figures 51 & 52. Screenshots showing an end user device (iOS and Android) requiring that Lookout needs to be installed on the device before they can access Outlook ....................................... 32
Figure 53. Screenshot showing that a mobile device cannot access Outlook because Lookout has detected threats on their device, enforcing Real Time Access ......................................................... 33
LIST OF TABLES

Table 1. Federal Agencies that have deployed Lookout or testing proof of concepts .................... 3
Table 2. Risky Application Visibility deliverables and completion date ....................................... 5
Table 3. Advanced Third Party Application deliverables and completion dates .......................... 16
Table 4. Main in the Middle Detection deliverables and completion dates .................................. 20
Table 5. Mobile Vulnerability Detection deliverables and completion dates .............................. 24
Table 6. Continuous Conditional Access deliverables and completion dates ................................. 31
1.0 SUMMARY

Lookout is pleased to provide our Final report for the DHS BAA Agreement No. FA8750-17-2-0236. The deliverables in this proposal were developed for the Lookout Mobile Endpoint Security (MES) product, which is already deployed in numerous Federal agencies and is being tested with multiple others. All of the completed deliverables in this report have been enabled for Federal customer tenants for testing or production deployment to begin taking advantage of the enhanced mobile security provided by DHS and Lookout.
2.0 INTRODUCTION

Lookout has been providing mobile security since 2007 and the Lookout Mobile Endpoint Security (MES) solution is the most comprehensive solution available to mobile device administrators. MES is a cloud-based platform that detects and stops both mainstream and advanced mobile threats. The platform uses a predictive security model, based on over 12 years of mobile threat data collection and research using our advanced machine learning, that enables threat detection even in cases where no prior signatures exist and before threats exhibit malicious behavior. MES protects mobile endpoints and infrastructures from Web and Content based-threats (e.g. phishing attacks), Application-based threats and device risks, network-based threats, and also enables deep threat investigation providing administrators unparalleled visibility into the multitude of potential threats and risks within their mobile environment.
# Deployments and Proof of Concept Testing

Table 1. Federal Agencies that have deployed Lookout or testing proof of concepts

<table>
<thead>
<tr>
<th>Production Deployments</th>
<th>Testing/Engagement</th>
</tr>
</thead>
<tbody>
<tr>
<td>House of Representatives</td>
<td></td>
</tr>
<tr>
<td>US Marshals</td>
<td>FEMA</td>
</tr>
<tr>
<td>Customs and Border Protection</td>
<td>DoJ</td>
</tr>
<tr>
<td>Department of Veterans Affairs</td>
<td>USCIS</td>
</tr>
<tr>
<td>Peace Corps</td>
<td>HUD</td>
</tr>
<tr>
<td>Northcom</td>
<td>Treasury (OCC)</td>
</tr>
<tr>
<td>DISA</td>
<td>Dept of Transportation</td>
</tr>
<tr>
<td>Depart of Commerce NTIS</td>
<td>State Department</td>
</tr>
<tr>
<td>Dept of Commerce OIG</td>
<td>USDA</td>
</tr>
<tr>
<td>Dept of Commerce BEA</td>
<td>HHS</td>
</tr>
<tr>
<td>CTTSO</td>
<td>CDC</td>
</tr>
<tr>
<td>US Senate</td>
<td>US Courts</td>
</tr>
<tr>
<td>Federal Judicial Center</td>
<td></td>
</tr>
<tr>
<td>US Marshals TOG</td>
<td></td>
</tr>
<tr>
<td>FirstNet</td>
<td></td>
</tr>
<tr>
<td>Transportation Security Administration</td>
<td></td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td></td>
</tr>
</tbody>
</table>
3.0 METHODS, ASSUMPTIONS & PROCEDURES

Lookout practices the Agile software development methodology. In order to ensure integrity of its systems and software during the development and production deployment processes, Lookout utilizes a software development lifecycle with embedded review and security controls. All software changes are peer reviewed before testing. All code is tested by appropriate parties and signed off before release. Security testing includes the use of both static and dynamic analysis tools. Lookout adheres to a policy with separation of duties to ensure that developers do not push their own code into production systems. Test accounts, credentials, and data are not promoted to production systems. Lookout systems are regularly scanned and verified with an industry-leading vulnerability scanner. Lookout corporate and production networks have in-line intrusion detection systems monitored by the infrastructure security team. Lookout maintains a robust change management system for all changes and software releases. Changes are made at the same time across regions in AWS, so production and contingency environments remain synchronized.
4.0 RESULTS AND DISCUSSION

Lookout has completed the development of all the deliverables detailed in DHS BAA Agreement No. FA8750-17-2-0236. Each deliverable is either already deployed in Federal Agencies or available for Proof of Concepts. Details of the deliverables and examples of how they function are described in the following sections.

4.1.1 Risky Application Visibility

Table 2. Risky Application Visibility deliverables and completion date

<table>
<thead>
<tr>
<th></th>
<th>Deliverable</th>
<th>Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1.1.a.1</td>
<td>Insecure use of data at rest</td>
<td>Complete Nov 2017</td>
</tr>
<tr>
<td>4.1.1.1.a.2</td>
<td>Insecure use of data in motion</td>
<td>Complete Nov 2017</td>
</tr>
<tr>
<td>4.1.1.1.b.1</td>
<td>Use of SDKs from social networking clouds such as Twitter and Facebook</td>
<td>Complete Aug 2017</td>
</tr>
<tr>
<td>4.1.1.1.c.1</td>
<td>Actual sending of data to cloud services</td>
<td>Complete Dec 2019</td>
</tr>
<tr>
<td>4.1.1.1.d.1</td>
<td>Understand what URLs are being accessed by the app and whether these are of low reputation.</td>
<td>Complete Feb 2019</td>
</tr>
<tr>
<td>4.1.1.1.e</td>
<td>Dynamic code loading - These are indications of apps that can dynamically load code and hence might evade traditional vetting strategies</td>
<td>Complete Dec 2019</td>
</tr>
<tr>
<td>4.1.1.1.f</td>
<td>Geoview of URLs</td>
<td>Complete Sep 2018</td>
</tr>
<tr>
<td>4.1.1.1.g</td>
<td>Uses private APIs (iOS)</td>
<td>Complete Dec 2019</td>
</tr>
<tr>
<td>4.1.1.2.a</td>
<td>Custom policies allowing admins to sets rules based on app behaviors</td>
<td>Complete Nov 2017</td>
</tr>
<tr>
<td>4.1.1.2.b</td>
<td>Blacklisting of unwanted applications</td>
<td>Complete Nov 2017</td>
</tr>
<tr>
<td>4.1.1.2.c</td>
<td>End-user notification for non-compliant/risky apps</td>
<td>Complete for iOS Aug 2017. Complete for Android Oct 2018</td>
</tr>
<tr>
<td>4.1.1.2.d</td>
<td>MDM notification for non-compliant/risky apps</td>
<td>Complete Nov 2017</td>
</tr>
<tr>
<td>Additional</td>
<td>Identify applications that listen on sockets to receive data</td>
<td>Complete Jan 2018</td>
</tr>
<tr>
<td>Additional</td>
<td>Identify applications that make use of Bluetooth and/or NFC</td>
<td>Complete Jan 2018</td>
</tr>
</tbody>
</table>
4.1.1.1.a - Insecure use of Data

4.1.1.1.a.1 - Insecure use of Data at Rest
4.1.1.1.a.2 - Insecure use of Data in Motion

Applications can store data locally on a mobile device or transmit it to numerous domains and the end user does not always have visibility into how their data is protected. Lookout has now added the capability for administrators to review whether or not an application is following best practices for securing and transmitting data.

![Network Traffic]

**Figure 1.** Screenshot showing insecure data in motion for an application on an Android device. (Deliverable 4.1.1.1.a.2)

![Data Handling Security]

**Figure 2.** Screenshot showing insecure data in motion and at rest for an iOS device, based on Apple ATS (Deliverable 4.1.1.1.a.1 & 4.1.1.1.a.2)
4.1.1.1.b.1 - Use of SDKs from social networking clouds such as Twitter and Facebook

Figure 3. Screenshot showing configuration of policy to match use of Social networks (Deliverable 4.1.1.1.b.1)

Figure 4. Screenshot showing data from an app that shows access to Cloud services (deliverable 4.1.1.1.b.1)

4.1.1.1.c.1 - Actual sending of data to cloud services

Figure 5. Screenshot of sensitive data (IMEI) being sent to a third-party
4.1.1.d.1 - Understand what URLs are being accessed by the app and whether these are of low reputation.


Functionality to detect and mitigate phishing both during its occurrence and device susceptibility will be developed. The functions to be developed will analyze all mobile traffic including browsing and app traffic from any source (e.g., email, SMS, Facebook, messaging apps) and of any protocol type (e.g., HTTP and HTTPS). It will detect phishing and malicious content and alert end-users before the URL is accessed, for example, to prevent risky content from being loaded. For admins, the capability to set configurations in Lookout's MES to either Block or Warn users of risky content. This will give admins visibility into whether or not devices in their fleet have enabled Phishing & Content Protection, and device details such as a count of URLs blocked.

![Figure 6. Dashboard control to enable Phishing and Content Protection (PCP)](image)

![Figure 7. Device showing that Safe Browsing (Client PCP) is active on the device](image)
Figures 8 & 9. Screenshot warnings to end user about malicious URLs that they attempted to access

Figure 10. Screenshot of low reputation and malicious URLs being identified and blocked
4.1.1.1.f - Geoview of URLs

![Figure 11. Screenshot showing the Geo-location of IPs/URLs within an application](image)

### 4.1.1.1.g – Use of private APIs (iOS)

![Figure 12. Screenshot showing an application that accesses Private APIs](image)
4.1.1.2.a - Custom Policies Allowing Admins to Set Rules Based on App Behaviors

A typical customer environment can have thousands of applications across their mobile device fleet. Many of these applications have permissions and capabilities that, while not intentionally malicious, may be considered risky based on IT policies. Lookout now allows customers to sort Android and iOS applications in their environment based on a wide variety of parameters to identify applications that may require a more detailed review.

Figure 13. Screenshot showing the ability for administrators to configure policy violations for application based behaviors. (Deliverable 4.1.1.2.a)

Figure 14. – Screenshot showing the ability for administrators to configure policy violations for application based behaviors. (Deliverable 4.1.1.2.a)
4.1.1.2b - Blacklisting of Unwanted Applications

After identifying applications that are considered too risky for a mobile environment, administrators can take an action to Blacklist that application. Users are notified that their device has the risky application installed and require its removal.

Figure 16. Screenshot showing an application that violates the custom policy for applications that access the camera. (Deliverable 4.1.1.2.a). Note that the application is available for Blacklisting because of the violation (Deliverable 4.1.1.2.b)
4.1.1.2c – End-User notification for non-compliant/risky apps

Figure 17. Screenshot showing that the application violating policy has been blacklisted. (Deliverable 4.1.1.2.b)

Figure 18. Screenshot showing the ability to Blacklist an Android application. (Deliverable 4.1.1.2.b)

Figure 19. Screenshots showing the end user notification that the app they have installed is violating policy and has been blacklisted. (Deliverable 4.1.1.2.c)
4.1.1.2d - MDM Notification for Non-compliant/Risky Apps

For applications that have been Blacklisted, an action can be taken to set the risk level and notify an MDM which devices are out of compliance because they contain Blacklisted applications. If desired, the MDM can take a remediation action (e.g. block email) on those devices until the Blacklisted applications are removed.

Figure 20. Screenshot showing applications that have been Blacklisted can be configured to notify an MDM at a certain threat level. (Deliverable 4.1.1.2.d)

Figure 21. Screenshot from MDM showing that a mobile device has a Blacklisted application (Deliverable 4.1.1.2.d)
Additional Delivered Features

1) Identify applications that listen on sockets to receive data
2) Additional Delivered Feature - Identify applications that make use of Bluetooth and/or NFC

Figure 22. Dashboard view of applications that Access Bluetooth, NFC and Accept incoming traffic

Figure 23. Application details that show connectivity for NFC/Bluetooth and accept incoming traffic
4.1.2 - Advanced Third Party Application Investigation and “Old Age” App Detection

Table 3. Advanced Third Party Application deliverables and completion dates.

<table>
<thead>
<tr>
<th>4.1.2.1</th>
<th>Detection of Apps Removed from App Store</th>
<th>Complete April 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Policy to notify end-users and admins of removed apps</td>
<td>Complete April 2019</td>
</tr>
<tr>
<td>4.1.2.2</td>
<td>Android Side Loaded App Detection (Flag apps not from Google Play)</td>
<td>Complete Jan 2020</td>
</tr>
<tr>
<td></td>
<td>Notify end-users and admins of non-Google Play apps</td>
<td>Complete Jan 2020</td>
</tr>
<tr>
<td></td>
<td>Blacklist and Whitelist for Android apps</td>
<td>Complete Jan 2020</td>
</tr>
<tr>
<td></td>
<td>Whitelist specific Third Party app stores (e.g. Amazon)</td>
<td>Complete Jan 2020</td>
</tr>
<tr>
<td></td>
<td>Blacklist a third party app store</td>
<td>Complete Jan 2020</td>
</tr>
</tbody>
</table>

4.1.2.1.a. - Detection of Apps Removed from App Store

Filters have been added that will now allow admins to identify apps that are not in Apple App Store. Any apps that did not come from the App store and are NOT approved can be blacklisted and end-users will be notified that the app is no longer approved for use on their device.

![Figure 24. Screenshot showing filter for App Store Apps](image)
4.1.2.1.b. - Policy to notify end-users and admins of removed apps

Figure 25. Screenshot showing an App that came from the Apple App Store

Figure 26. Screenshot showing an App that did NOT come from the Apple App Store
4.1.2.2 – Third Party App Store Deliverables

4.1.2.2 – Android Side Loaded App Detection (Flag Apps not from Google Play)
4.1.2.2 - Whitelist specific Third Party App stores
4.1.2.2 - Blacklist a third party App store

Figure 27. Screenshot showing the configuration options to flag Android Sideloaded Applications and Whitelist/Blacklist specific sources and App stores

4.1.2.2 – Notify end-users and admins of non-Google Play apps

Figure 28. Screenshot showing an Administrators notice of an Android Sideloaded Application on a user device
Figure 29. Screenshots showing an end user notice of an Android Sideloaded Application detected on their device

4.1.2.2 – Blacklist and Whitelist for Android Apps

Figure 30. Screenshot showing the configuration option to Whitelist Android applications. Blacklisting of Android applications was also covered under deliverable 4.1.1.2.b and 4.1.1.2.c
4.1.3 Man in The Middle Detection

Table 4. Main in the Middle Detection deliverables and completion dates

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time on-device detection of network based threats</td>
<td>Complete Aug 2017</td>
</tr>
<tr>
<td>Automatic disconnect option from malicious networks (configurable by admin)</td>
<td>Complete Feb 2019</td>
</tr>
<tr>
<td>Notify admins, end-users and MDMs of the detected threat</td>
<td>Complete Aug 2017</td>
</tr>
<tr>
<td>Certificate whitelisting for legitimate proxy of traffic</td>
<td>Complete April 2019</td>
</tr>
<tr>
<td>View certificate details of a detected attack</td>
<td>Complete Aug 2017</td>
</tr>
<tr>
<td>Content Modification Detection and Alerting</td>
<td>Complete Nov 2019</td>
</tr>
<tr>
<td>Rogue-Wifi detection</td>
<td>Complete Dec 2018</td>
</tr>
</tbody>
</table>

4.1.3.1 - Real-time on-device detection of network based threats
4.1.3.1 - Automatic disconnect option from malicious networks (configurable by admin)
4.1.3.1 - Notify admins, end-users and MDMs of the detected threat

In the event that a Man-In-The-Middle attack is detected or the user connects to a Rogue Access Point, the admins have the ability to enforce a quarantine on the device and alert the user.

Figure 31. Screenshot showing an administrators ability to block a device connected to a Rogue Wifi or a detected MITM attack (Deliverable 4.1.3.1)
Figure 32. Admin notification of a MITM threat on a user’s device (Deliverable 4.1.3.1)

Figures 33 & 34. End user notification and remediation actions for MITM threat on mobile device. (Deliverable 4.1.3.1)
4.1.3.2 - Certificate whitelisting for legitimate proxy of traffic

4.1.3.2 - View certificate details of a detected attack

Figures 35 & 36. Screenshots showing the option to whitelist certificates for legitimate proxy of traffic (deliverable 4.1.3.2)
4.1.3.3 Content Modification Detection and Alerting

Figure 37. Certificate details of a MITM threat (Deliverable 4.1.3.2)

Figure 38. Screenshot showing a content modification detection (Deliverable 4.1.3.3)
4.1.4 Mobile Vulnerability Detection and Management

Table 5. Mobile Vulnerability Detection deliverables and completion dates

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.4.1 Operating System Analysis Stack</td>
<td></td>
</tr>
<tr>
<td>Out of date OS notification</td>
<td>Complete Aug 2017</td>
</tr>
<tr>
<td>Detection of OS vulnerabilities matching databases such as NVD and CVE</td>
<td>Complete Nov 2017</td>
</tr>
<tr>
<td>4.1.4.2 Application Analysis Stack</td>
<td></td>
</tr>
<tr>
<td>Detection of application vulnerabilities</td>
<td>Complete Jan 2019</td>
</tr>
<tr>
<td>4.1.4.3 Lookout Management Console Enhancements</td>
<td></td>
</tr>
<tr>
<td>MES Console reporting on device vulnerabilities</td>
<td>Complete Aug 2017</td>
</tr>
<tr>
<td>Actionable options when vulnerabilities are detected</td>
<td>Complete Jan 2019</td>
</tr>
</tbody>
</table>

4.1.4.1 - Detection of OS vulnerabilities matching databases such as NVD and CVE

Mobile device OS and firmware need to be regularly updated to protect against vulnerabilities that are identified and patched. With this new feature, Lookout can provide visibility into what software a mobile device is currently running and what vulnerabilities are associated with that particular release.

![Figure 39. Screenshot showing an iOS with out of date OS and the number of unpatched CVEs associated with that release. (Deliverable 4.1.4.1)](image-url)
Figure 40. Screenshot showing an iOS release and the details of the associated unpatched CVEs (Deliverable 4.1.4.1)

Figure 41. Screenshot showing an Android device with out of date ASPL and the number of unpatched CVEs associated with that release. (Deliverable 4.1.4.1)
Figure 42. Screenshot showing number of unpatched CVEs associated with a specific ASPL. (Deliverable 4.1.4.1)

4.1.4.2 - Detection of application vulnerabilities

![Data Handling Security]

Figure 43. Screenshot showing Data Handling vulnerabilities for an application (Deliverable 4.1.4.2)

![OWASP Mobile Top 10]

Figure 44. Screenshot showing OWASP violations (Deliverable 4.1.4.2)
4.1.4.3a - MES Console reporting on device vulnerabilities

Figure 45. Screenshot showing an application with a detected vulnerability (Deliverable 4.1.4.2)

Figure 46. Screenshot showing device software distributions and associated vulnerabilities

Figure 47. Device configuration information for Android devices (Deliverables 4.1.4.1, 4.1.4.3)
4.1.4.3b - Actionable options when vulnerabilities are detected

Figure 48.  Device configuration information for iOS devices (Deliverables 4.1.4.1, 4.1.4.3)

Figure 49.  Screenshot showing the option to Blacklist an application if the identified vulnerabilities are too risky to ignore
4.1.5 Continuous Conditional Access

RE: DHS BAA Agreement No. FA8750-17-2-0236.

In the existing agreement Lookout had proposed developing a Certificate Authority Reputation System (CARS) as defined in section 4.1.5

“Repository for cataloging and analyzing certificates to find, measure and characterize relationships between CAs, relying parties, the certificates they have issued, known malware, and maliciously configured services on the Internet.”

After researching the proposed system and gathering customer feedback, it has been determined that a CARS solution does not currently lend itself to a tangible product that would provide significant improvements in today’s mobile security environments. Rather than continue to fund research and development of a solution that has limited deployment prospects, Lookout proposes that we replace the CARS deliverable in Section 4.1.5 with a new capability, Continuous Conditional Access (CCA). CCA is solution that will combine Policy based threats and Identity & Access Management to determine a device’s current Health and Risk before resources are accessed. This solution is a more tangible product that can be widely deployed in the Federal space and provide immediate enhancements to securing mobile devices. The solution applies to GFE and BYOD devices and has broad interest among customers.
Updated Statement of Work – Section 4.1.5 (Replace CARS with CCA)

4.1.5 Continuous Conditional Access (CCA) – Access to corporate resources will be protected by granting access to users or devices based on endpoint risk. Lookout will develop functionality that, prior to accessing corporate data, ensures devices have Lookout installed and the health of the device is within accordance to defined policies in the Lookout MES console. Devices that are out of compliance will be prevented from accessing corporate networks and data.

How Continuous Conditional Access Works

1. Employee accesses corporate resource
2. Auth request to Lookout ID Broker
3. App installed if not present
4. Device health check
5. Any device health issues remediated
6. Auth sent to SSO
7. Employee presented SSO auth challenge
8. Access granted to corporate resource

Figure 50. Overview of how Continuous Conditional Access work
Table 6. Continuous Conditional Access deliverables and completion dates.

<table>
<thead>
<tr>
<th>4.1.5</th>
<th>Continuous Conditional Access</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.5.1</td>
<td>Device Identification on iOS &amp; Android - Check if Lookout app is installed on a device &amp; enforce app installation if the Lookout App is not installed.</td>
<td>Complete Nov 2019</td>
</tr>
<tr>
<td>4.1.5.2</td>
<td>Conditional Access Support for Office 365 using AAD for IDP</td>
<td>Complete Nov 2019</td>
</tr>
<tr>
<td>4.1.5.3</td>
<td>Real Time Access – Enforce conditional access based on Device Health Check before logging in.</td>
<td>Complete Nov 2019</td>
</tr>
</tbody>
</table>

Lookout will develop functionality that, prior to accessing agency data, ensures devices have Lookout installed and the health of the device is within accordance to defined polices in the Lookout MES console. Devices that are out of compliance will be prevented from accessing agency networks and data. This functionality enhances protection for agencies that want to enable a BYOD and/or Container program for protecting mobile devices.
4.1.5.1 – Device Identification and Lookout Enforcement

4.1.5.1 - Device Identification on iOS & Android
4.1.5.1 - Check if Lookout app is installed on a device & enforce app installation if the Lookout App is not installed

Figures 51 & 52. Screenshots showing an end user device (iOS and Android) requiring that Lookout needs to be installed on the device before they can access Outlook.
4.1.5.2 – Conditional Access Support for Office 365 using AAD for IDP

When a user launches one of the supported Microsoft Office 365 applications, their device will test to make sure that Lookout is installed and no threats are detected before they can access data.

4.1.5.3 - Real Time Access – Enforce conditional access based on Device Health Check before logging in

Figure 53. Screenshot showing that a mobile device cannot access Outlook because Lookout has detected threats on their device, enforcing Real Time Access
5.0 CONCLUSION

The features developed for DHS BAA Agreement No. FA8750-17-2-0236 expand the capabilities and functionality of Lookout’s MES solution to provide more comprehensive protection of mobile devices and visibility into the types of applications capabilities and permissions that are being deployed in customer environments.
# 6.0 List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAD</td>
<td>Azure Active Directory</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ASPL</td>
<td>Android Security Patch Level</td>
</tr>
<tr>
<td>ATS</td>
<td>App Transport Security</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>CARS</td>
<td>Certificate Authority Reputation System</td>
</tr>
<tr>
<td>CCA</td>
<td>Continuous Conditional Access</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures</td>
</tr>
<tr>
<td>IDP</td>
<td>integrated data processing</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identity</td>
</tr>
<tr>
<td>MDM</td>
<td>Mobile Device Management</td>
</tr>
<tr>
<td>MES</td>
<td>Mobile Endpoint Security</td>
</tr>
<tr>
<td>MITM</td>
<td>Man in The Middle</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>NVD</td>
<td>National Vulnerability Database</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>PCP</td>
<td>Phishing and Content Protection</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Developer Kit</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Location</td>
</tr>
</tbody>
</table>