AFRL-RI-RS-TR-2020-118

CONTINUOUS VALIDATION AND THREAT PROTECTION FOR MOBILE APPLICATIONS

LOOKOUT, INC.

JULY 2020

FINAL TECHNICAL REPORT

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

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.

REPORT DOCUMENTATION PAGE	*Form Approved* **OMB No. 0704-0188**

1. REPORT DATE *(DD-MM-YYYY)* JULY 2020	**2. REPORT TYPE** FINAL TECHNICAL REPORT	**3. DATES COVERED** *(From - To)* JUL 2017 – JAN 2020

4. TITLE AND SUBTITLE CONTINUOUS VALIDATION AND THREAT PROTECTION FOR MOBILE APPLICATIONS	**5a. CONTRACT NUMBER** FA8750-17-2-0236
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER 69220K
6. AUTHOR(S) DAEMON MORRELL	**5d. PROJECT NUMBER** DHS7
	5e. TASK NUMBER LO
	5f. WORK UNIT NUMBER OK
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) LOOKOUT, INC. 275 BATTERY STREET, SUITE 200 SAN FRANCISCO, CA 94111	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/RIGA 525 Brooks Road Rome NY 13441-4505	**10. SPONSOR/MONITOR'S ACRONYM(S)** AFRL/RI
	11. SPONSOR/MONITOR'S REPORT NUMBER AFRL-RI-RS-TR-2020-118

12. DISTRIBUTION AVAILABILITY STATEMENT
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.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

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.

15. SUBJECT TERMS

Mobile Threat Protection, Mobile Endpoint Security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** **JAMES S. SIDORAN**
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	42	**19b. TELEPHONE NUMBER (*Include area code)*** **N/A**

Table of Contents

LIST OF FIGURES

LIST OF TABLES

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

Production Deployments	Testing/Engagement
House of Representatives	
US Marshals	FEMA
Customs and Border Protection	DoJ
Department of Veterans Affairs	USCIS
Peace Corps	HUD
Northcom	Treasury (OCC)
DISA	Dept of Transportation
Depart of Commerce NTIS	State Department
Dept of Commerce OIG	USDA
Dept of Commerce BEA	HHS
CTTSO	CDC
US Senate	US Courts
Federal Judicial Center	
US Marshals TOG	
FirstNet	
Transportation Security Administration	
Department of Homeland Security	

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

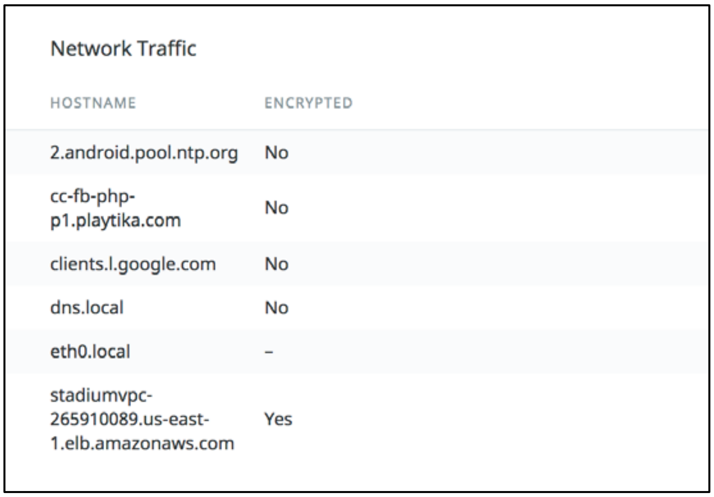
Table 2. Risky Application Visibility deliverables and completion date

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

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

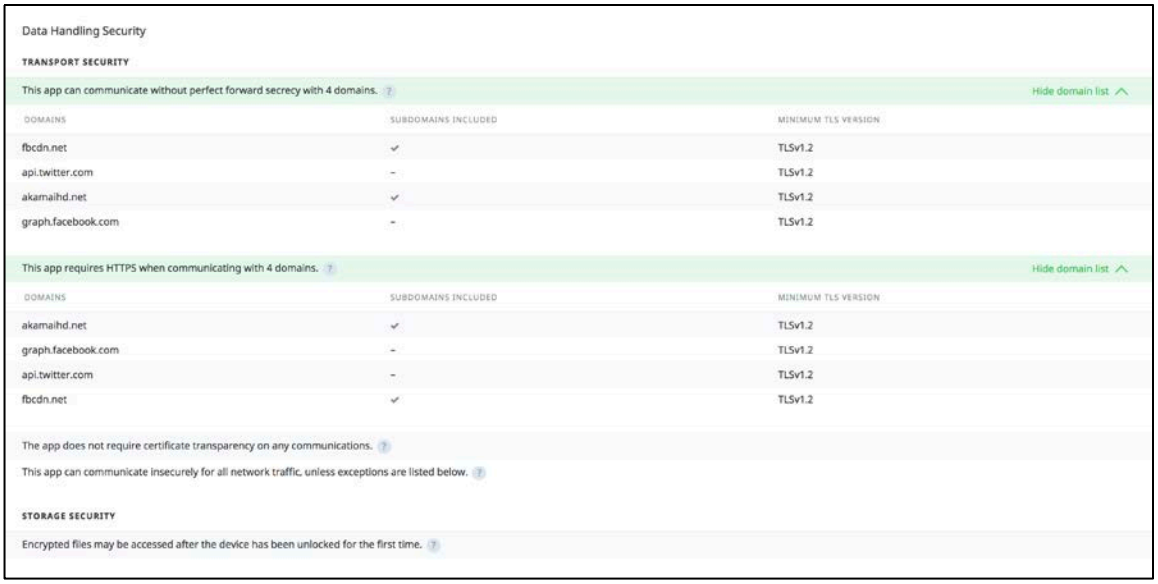
Applications can store data locally on a mobile device or transmit it to numerous domains and the end user does not always have visibility into how their data is protected. Lookout has now added the capability for administrators to review whether or not an application is following best practices for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



Network Traffic

HOSTNAME	ENCRYPTED
2.android.pool.ntp.org	No
cc-fb-php-p1.playtika.com	No
clients.l.google.com	No
dns.local	No
eth0.local	–
stadiumvpc-265910089.us-east-1.elb.amazonaws.com	Yes

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

TRANSPORT SECURITY

This app can communicate without perfect forward secrecy with 4 domains. ?

DOMAINS	SUBDOMAINS INCLUDED	MINIMUM TLS VERSION
fbcdn.net	✓	TLSv1.2
api.twitter.com	-	TLSv1.2
akamaihd.net	✓	TLSv1.2
graph.facebook.com	-	TLSv1.2

This app requires HTTPS when communicating with 4 domains. ?

DOMAINS	SUBDOMAINS INCLUDED	MINIMUM TLS VERSION
akamaihd.net	✓	TLSv1.2
graph.facebook.com	-	TLSv1.2
api.twitter.com	-	TLSv1.2
fbcdn.net	✓	TLSv1.2

The app does not require certificate transparency on any communications. ?

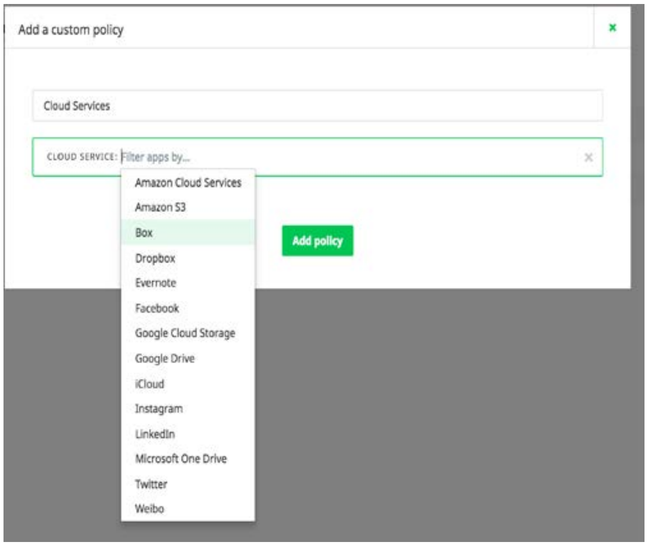
This app can communicate insecurely for all network traffic, unless exceptions are listed below. ?

STORAGE SECURITY

Encrypted files may be accessed after the device has been unlocked for the first time. ?

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

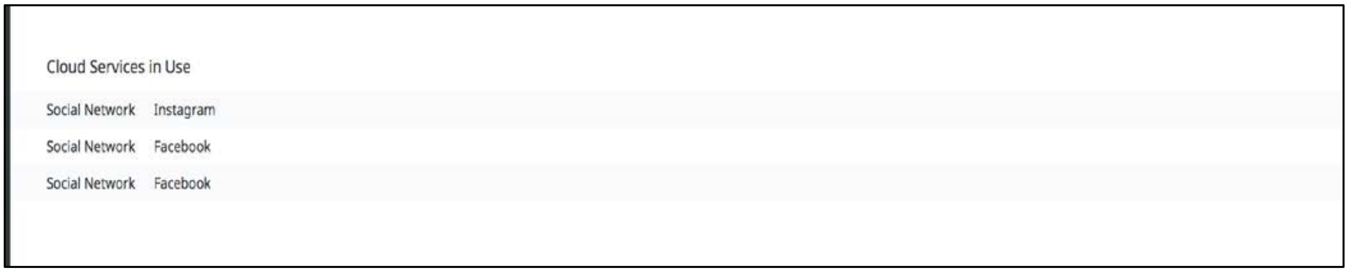


Add a custom policy

Cloud Services

CLOUD SERVICE: Filter apps by...

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

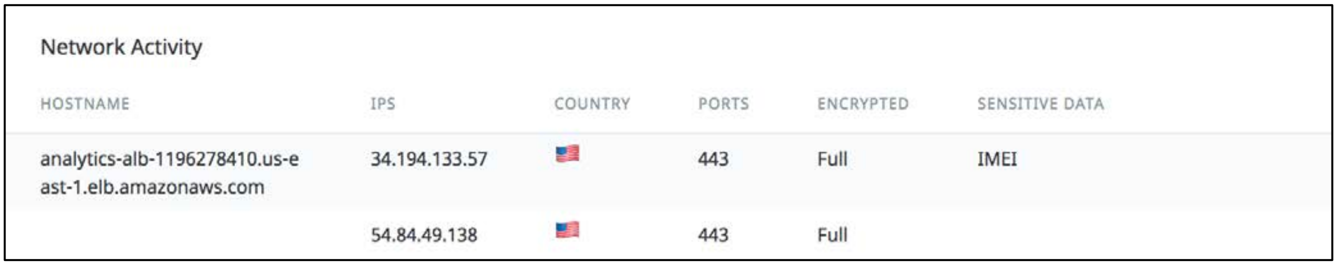


Cloud Services in Use

Social Network	Instagram
Social Network	Facebook
Social Network	Facebook

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



Network Activity

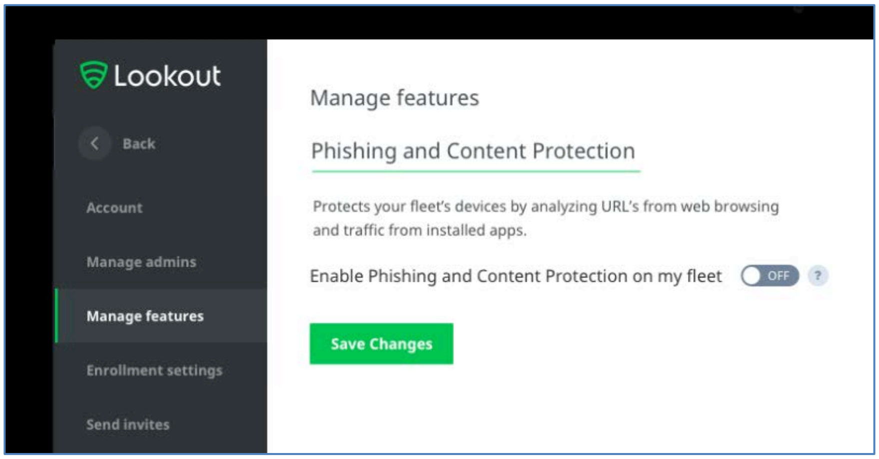
HOSTNAME	IPS	COUNTRY	PORTS	ENCRYPTED	SENSITIVE DATA
analytics-alb-1196278410.us-east-1.elb.amazonaws.com	34.194.133.57	🇺🇸	443	Full	IMEI
	54.84.49.138	🇺🇸	443	Full	

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.

4.1.1.1.d.1 - Released as Phishing & Content Protection and updated in SOW - Lookout Mobile Security Proposed Statement of Work for FA8750-17-2-0236, dated April 2, 2018.

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.



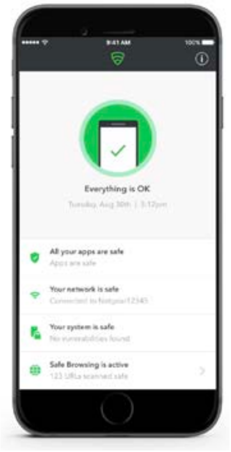
Manage features

Phishing and Content Protection

Protects your fleet's devices by analyzing URL's from web browsing and traffic from installed apps.

Enable Phishing and Content Protection on my fleet OFF ?

Figure 6. Dashboard control to enable Phishing and Content Protection (PCP)



Everything is OK

Tuesday, Aug 30th | 3:12pm

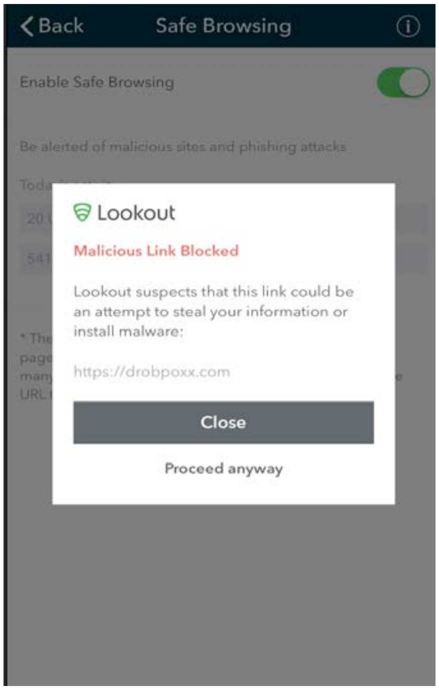
All your apps are safe
Apps are safe

Your network is safe
Connected to Netgear12345

Your system is safe
No vulnerabilities found

Safe Browsing is active
123 URLs scanned safe

Figure 7. Device showing that Safe Browsing (Client PCP) is active on the device



Enable Safe Browsing

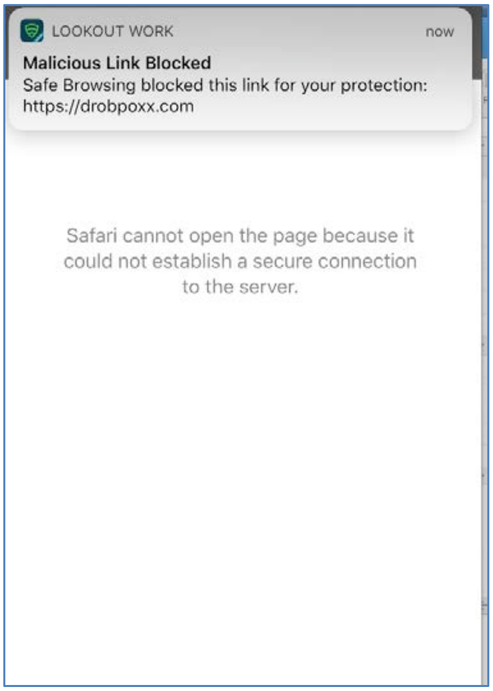
Be alerted of malicious sites and phishing attacks

Lookout

Malicious Link Blocked

Lookout suspects that this link could be an attempt to steal your information or install malware:

https://drobpoxx.com

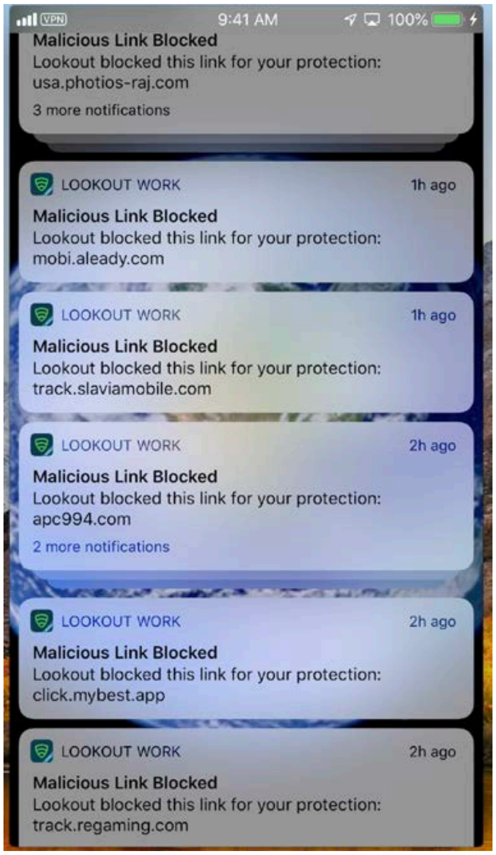


LOOKOUT WORK now

Malicious Link Blocked
Safe Browsing blocked this link for your protection:
https://drobpoxx.com

Safari cannot open the page because it could not establish a secure connection to the server.

Figures 8 & 9. Screenshot warnings to end user about malicious URLs that they attempted to access



VPN 9:41 AM 100%

Malicious Link Blocked
Lookout blocked this link for your protection:
usa.photios-raj.com
3 more notifications

LOOKOUT WORK 1h ago
Malicious Link Blocked
Lookout blocked this link for your protection:
mobi.aleady.com

LOOKOUT WORK 1h ago
Malicious Link Blocked
Lookout blocked this link for your protection:
track.slaviamobile.com

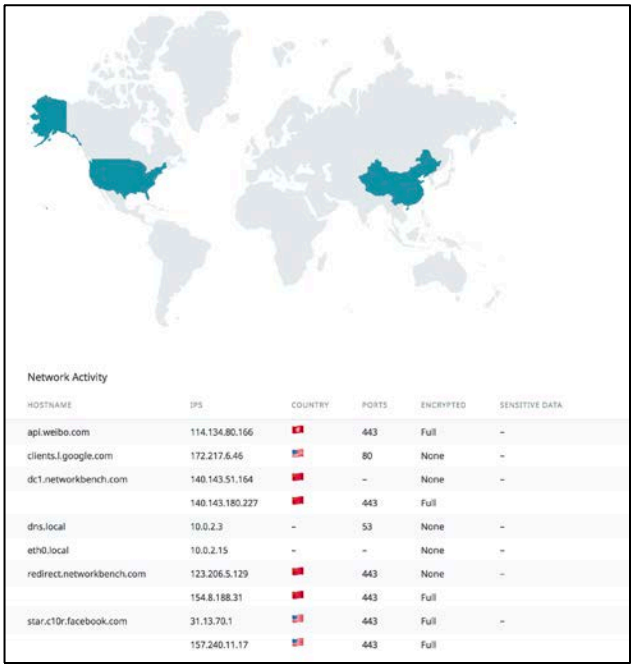
LOOKOUT WORK 2h ago
Malicious Link Blocked
Lookout blocked this link for your protection:
apc994.com
2 more notifications

LOOKOUT WORK 2h ago
Malicious Link Blocked
Lookout blocked this link for your protection:
click.mybest.app

LOOKOUT WORK 2h ago
Malicious Link Blocked
Lookout blocked this link for your protection:
track.regaming.com

Figure 10. Screenshot of low reputation and malicious URLs being identified and blocked

4.1.1.1.f - Geoview of URLs

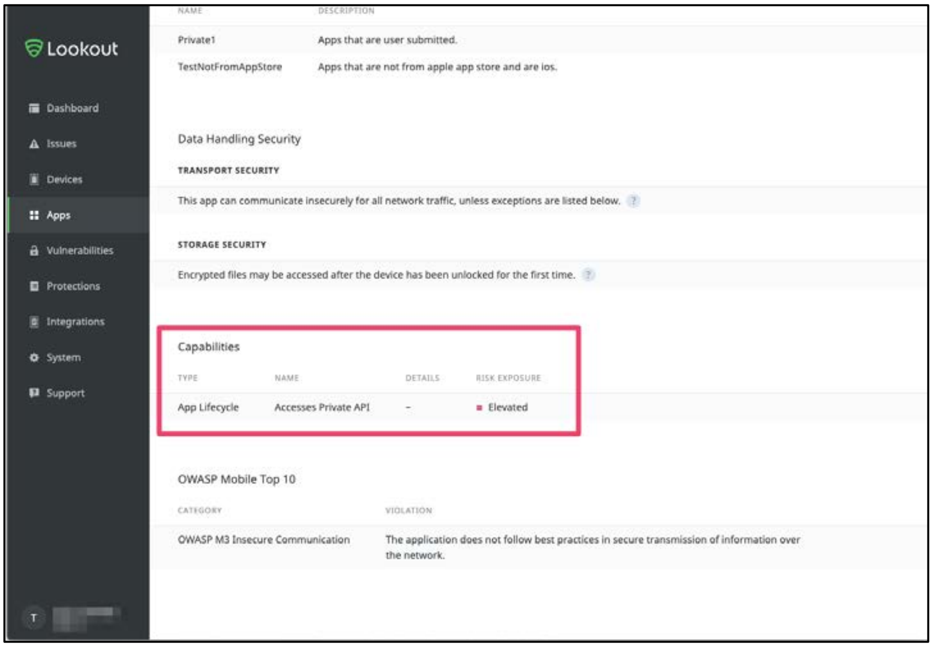


Network Activity

HOSTNAME	IPS	COUNTRY	PORTS	ENCRYPTED	SENSITIVE DATA
api.weibo.com	114.134.80.166	🇭🇰	443	Full	-
clients.l.google.com	172.217.6.46	🇺🇸	80	None	-
dc1.networkbench.com	140.143.51.164	🇨🇳	-	None	-
	140.143.180.227	🇨🇳	443	Full	
dns.local	10.0.2.3	-	53	None	-
eth0.local	10.0.2.15	-	-	None	-
redirect.networkbench.com	123.206.5.129	🇨🇳	443	None	-
	154.8.188.31	🇨🇳	443	Full	
star.c10r.facebook.com	31.13.70.1	🇺🇸	443	Full	-
	157.240.11.17	🇺🇸	443	Full	

Figure 11. Screenshot showing the Geo-location of IPs/URLs within an application

4.1.1.1.g – Use of private APIs (iOS)



[redacted]

NAME	DESCRIPTION
Private1	Apps that are user submitted.
TestNotFromAppStore	Apps that are not from apple app store and are ios.

Data Handling Security

TRANSPORT SECURITY

This app can communicate insecurely for all network traffic, unless exceptions are listed below. ?

STORAGE SECURITY

Encrypted files may be accessed after the device has been unlocked for the first time. ?

Capabilities

TYPE	NAME	DETAILS	RISK EXPOSURE
App Lifecycle	Accesses Private API	-	■ Elevated

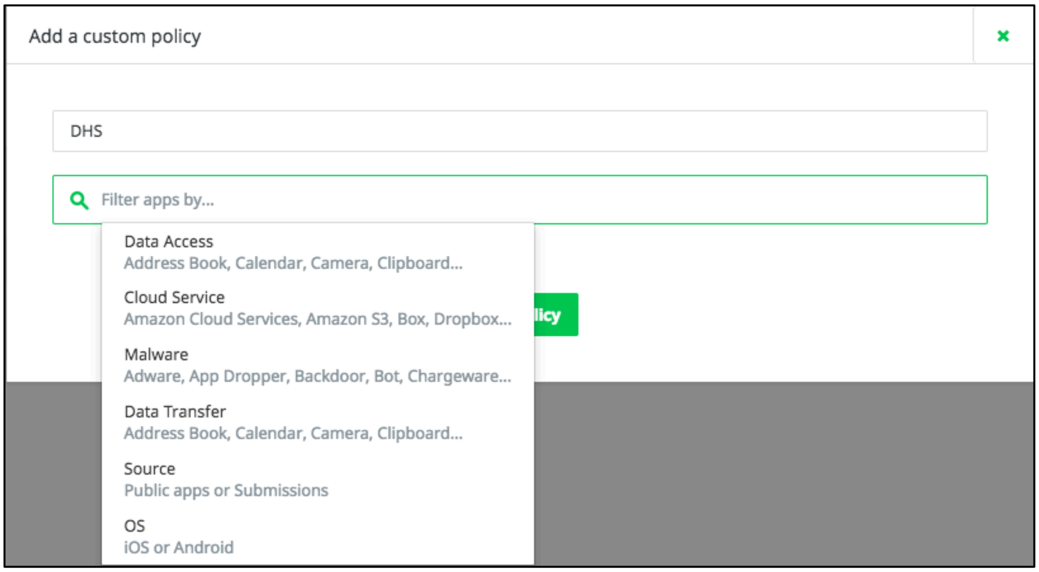
OWASP Mobile Top 10

CATEGORY	VIOLATION
OWASP M3 Insecure Communication	The application does not follow best practices in secure transmission of information over the network.

Figure 12. Screenshot showing an application that accesses Private APIs

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.

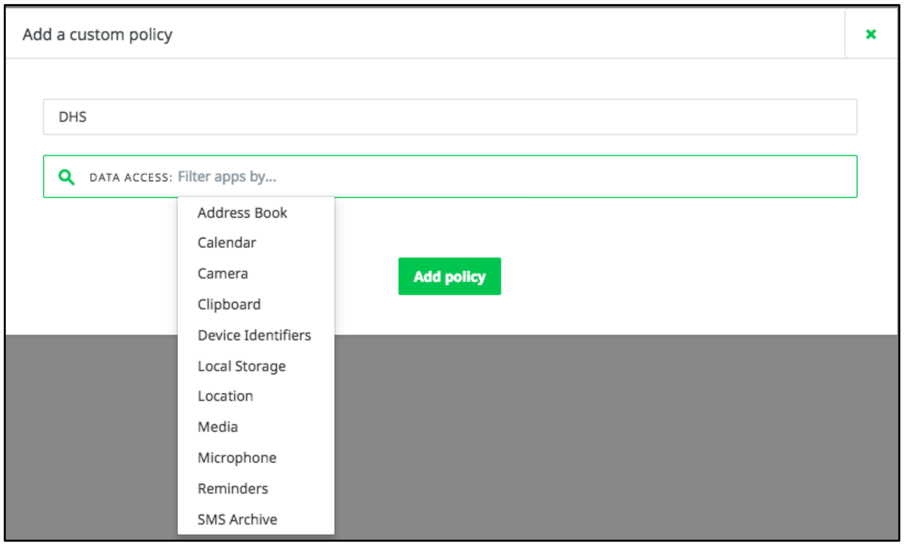


Add a custom policy

DHS

×
Filter apps by...
Data Access
Address Book, Calendar, Camera, Clipboard...
Cloud Service
Amazon Cloud Services, Amazon S3, Box, Dropbox...
Malware
Adware, App Dropper, Backdoor, Bot, Chargeware...
Data Transfer
Address Book, Calendar, Camera, Clipboard...
Source
Public apps or Submissions
OS
iOS or Android
licy

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

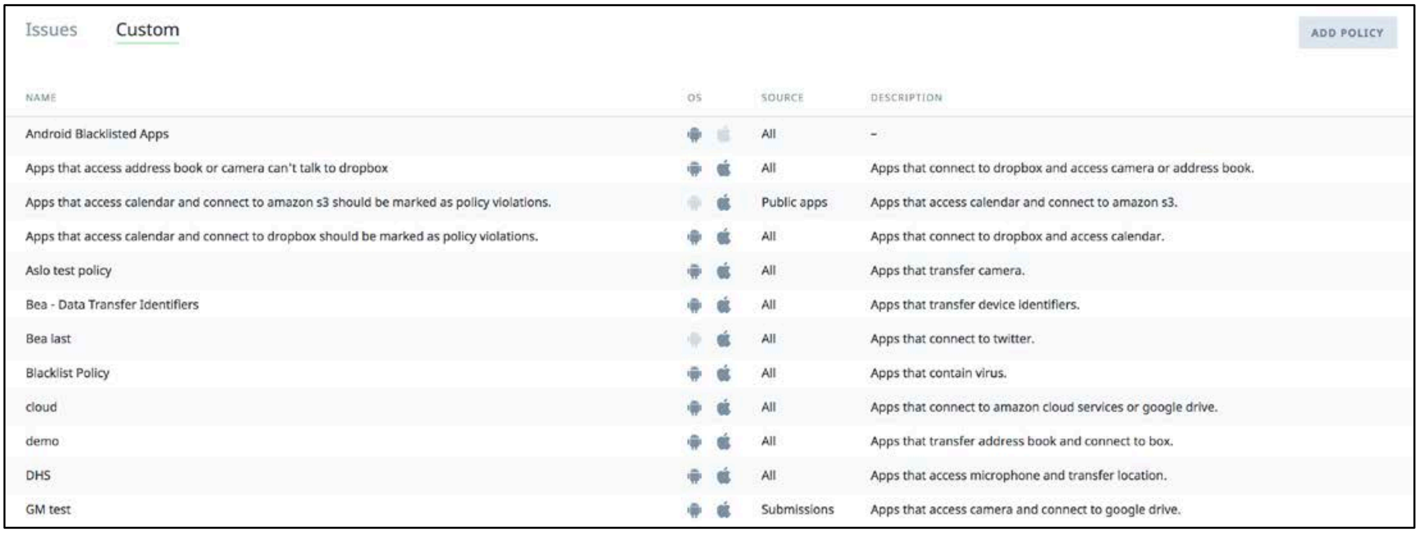


Add a custom policy

DHS

DATA ACCESS: Filter apps by...

Figure 14. – Screenshot showing the ability for administrators to configure policy violations for application based behaviors. (Deliverable 4.1.1.2.a)

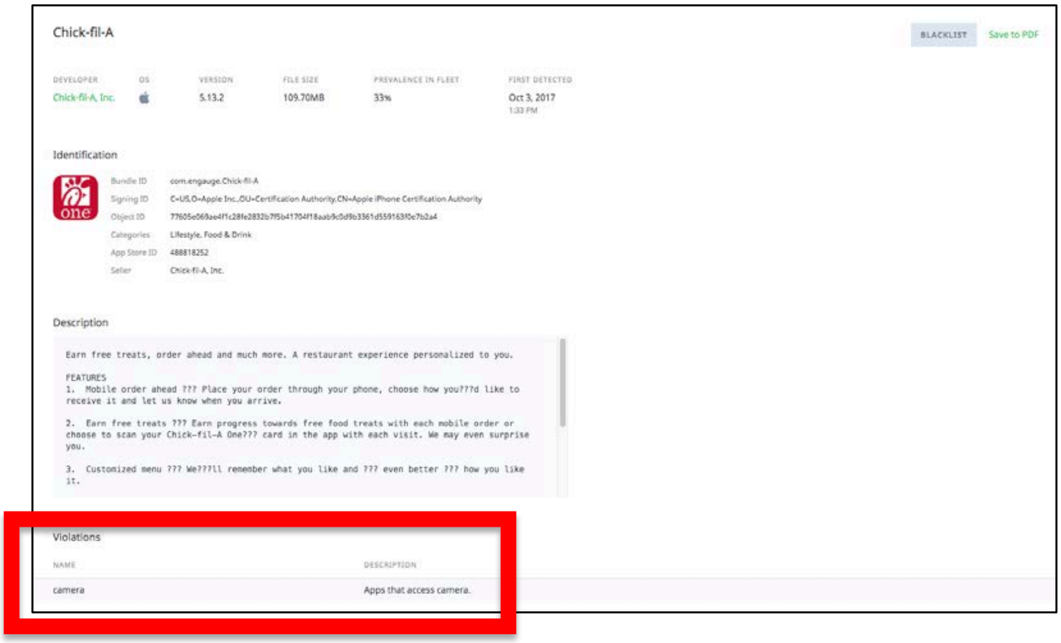


NAME	OS	SOURCE	DESCRIPTION
Android Blacklisted Apps	🤖	All	-
Apps that access address book or camera can't talk to dropbox	🤖 🍎	All	Apps that connect to dropbox and access camera or address book.
Apps that access calendar and connect to amazon s3 should be marked as policy violations.	🍎	Public apps	Apps that access calendar and connect to amazon s3.
Apps that access calendar and connect to dropbox should be marked as policy violations.	🤖 🍎	All	Apps that connect to dropbox and access calendar.
Aslo test policy	🤖 🍎	All	Apps that transfer camera.
Bea - Data Transfer Identifiers	🤖 🍎	All	Apps that transfer device identifiers.
Bea last	🍎	All	Apps that connect to twitter.
Blacklist Policy	🤖 🍎	All	Apps that contain virus.
cloud	🤖 🍎	All	Apps that connect to amazon cloud services or google drive.
demo	🤖 🍎	All	Apps that transfer address book and connect to box.
DHS	🤖 🍎	All	Apps that access microphone and transfer location.
GM test	🤖 🍎	Submissions	Apps that access camera and connect to google drive.

Figure 15. Screenshot showing numerous configuration policies 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.



Chick-fil-A

DEVELOPER	OS	VERSION	FILE SIZE	PREVALENCE IN FLEET	FIRST DETECTED
Chick-fil-A, Inc.	🍎	5.13.2	109.70MB	33%	Oct 3, 2017 1:33 PM

Identification

Bundle ID	com.engauge.Chick-fil-A
Signing ID	C=US,O=Apple Inc.,OU=Certification Authority,CN=Apple iPhone Certification Authority
Object ID	77605e069ae4f1c28fe2832b7f5b41704f18aab9c0d9b3361d559163f0e7b2a4
Categories	Lifestyle, Food & Drink
App Store ID	488818252
Seller	Chick-fil-A, Inc.

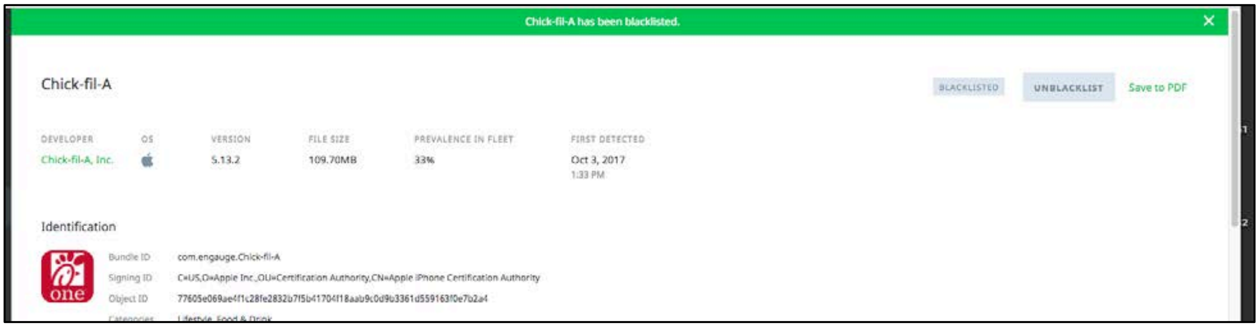
Description

```
Earn free treats, order ahead and much more. A restaurant experience personalized to you.

FEATURES
1.  Mobile order ahead ??? Place your order through your phone, choose how you???d like to
receive it and let us know when you arrive.

2.  Earn free treats ??? Earn progress towards free food treats with each mobile order or
choose to scan your Chick-fil-A One??? card in the app with each visit. We may even surprise
you.

3.  Customized menu ??? We???ll remember what you like and ??? even better ??? how you like
it.
```

Violations

NAME	DESCRIPTION
camera	Apps that access camera.

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)



Chick-fil-A has been blacklisted.

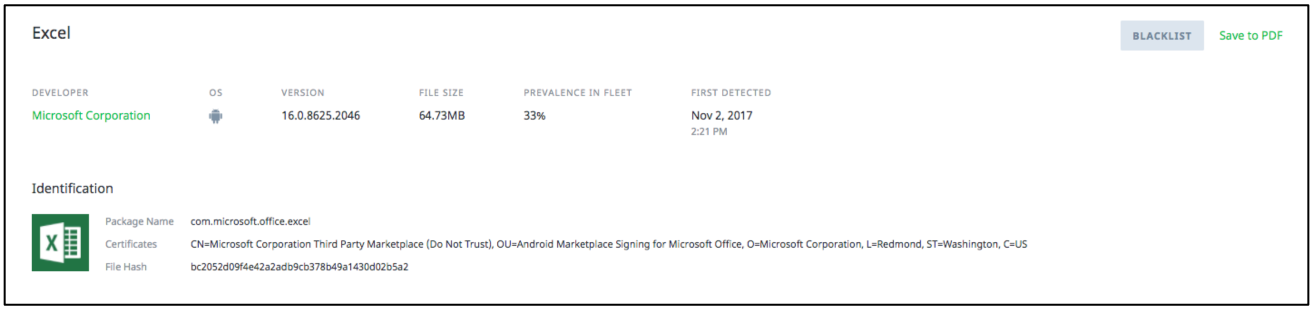
Chick-fil-A

DEVELOPER	OS	VERSION	FILE SIZE	PREVALENCE IN FLEET	FIRST DETECTED
Chick-fil-A, Inc.		5.13.2	109.70MB	33%	Oct 3, 2017 1:33 PM

Identification

Bundle ID	com.engauge.Chick-fil-A
Signing ID	C=US,O=Apple Inc.,OU=Certification Authority,CN=Apple iPhone Certification Authority
Object ID	77605e069ae4f1c28fe2832b7f5b41704f18aab9c0d9b3361d559163f0e7b2a4
Categories	Lifestyle, Food & Drink

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



Excel

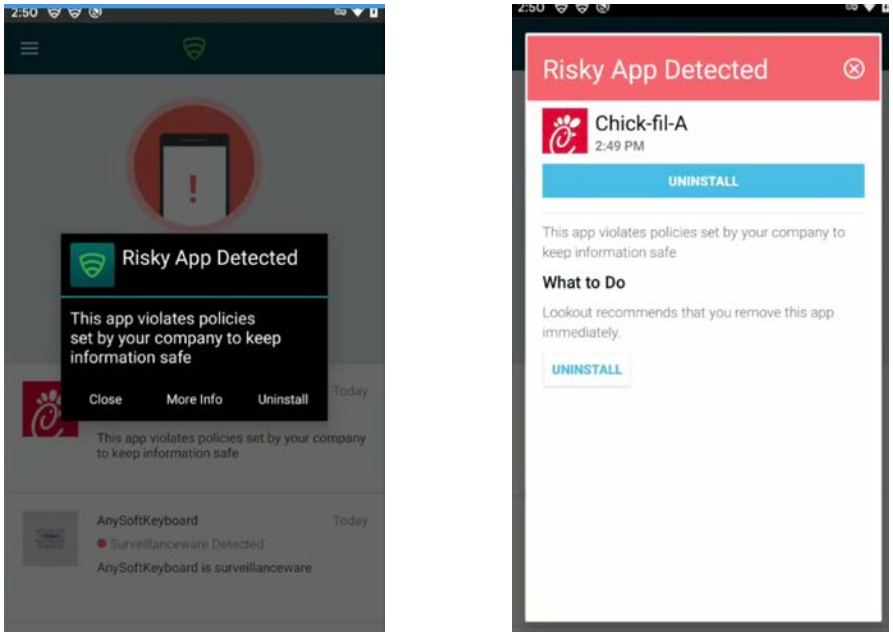
DEVELOPER	OS	VERSION	FILE SIZE	PREVALENCE IN FLEET	FIRST DETECTED
Microsoft Corporation		16.0.8625.2046	64.73MB	33%	Nov 2, 2017 2:21 PM

Identification

Package Name	com.microsoft.office.excel
Certificates	CN=Microsoft Corporation Third Party Marketplace (Do Not Trust), OU=Android Marketplace Signing for Microsoft Office, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US
File Hash	bc2052d09f4e42a2adb9cb378b49a1430d02b5a2

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

4.1.1.2c – End-User notification for non-compliant/risky apps



Risky App Detected

This app violates policies set by your company to keep information safe

This app violates policies set by your company to keep information safe

AnySoftKeyboard

● Surveillanceware Detected

AnySoftKeyboard is surveillanceware

Risky App Detected

Chick-fil-A
2:49 PM

This app violates policies set by your company to keep information safe

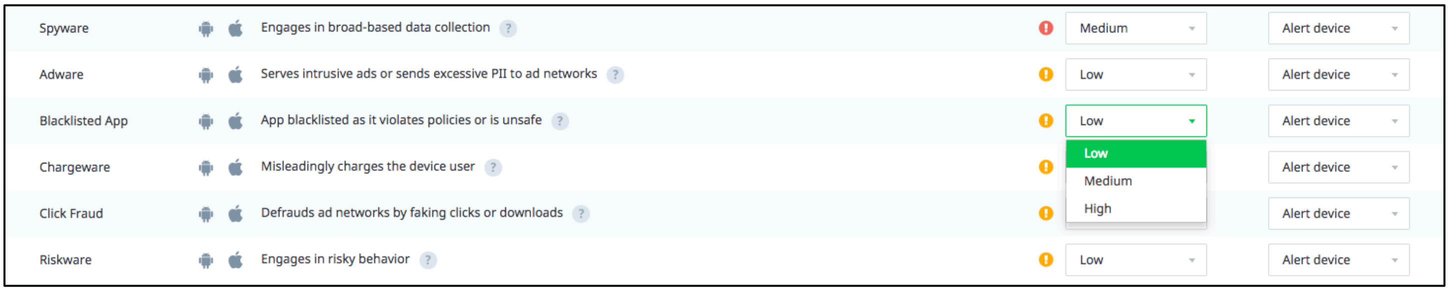
What to Do

Lookout recommends that you remove this app immediately.

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)

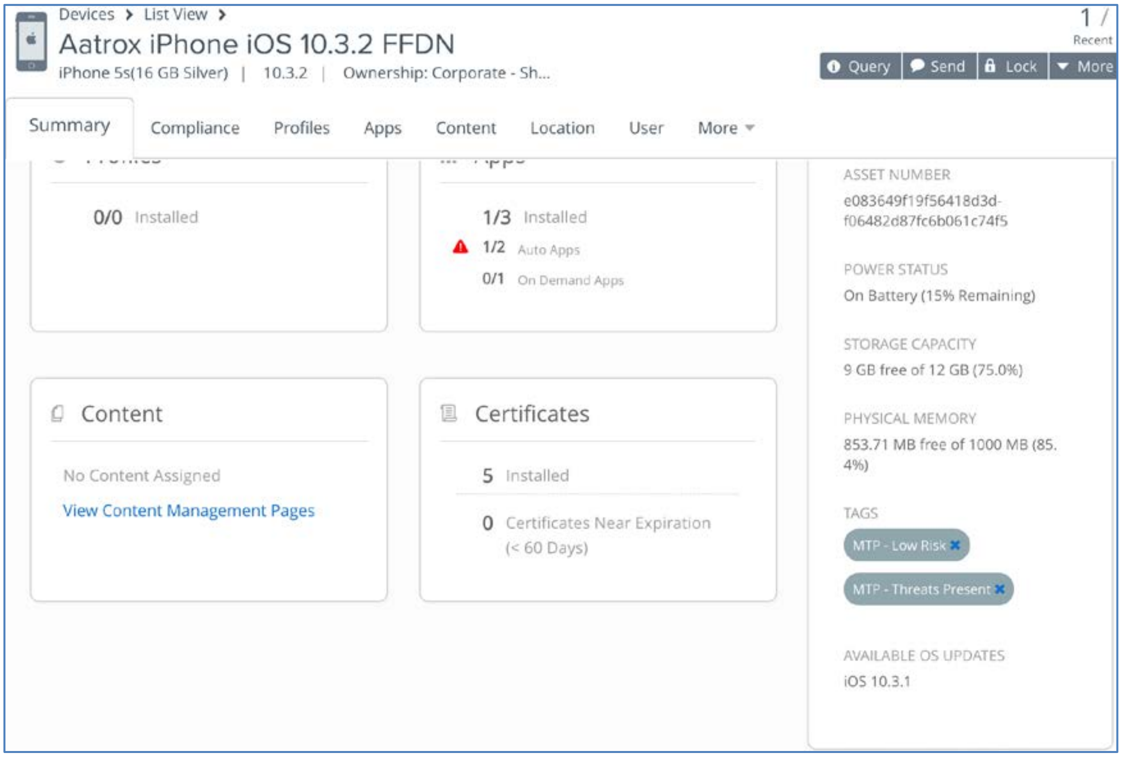
4.1.1.2d - MDM Notification for Non-compliant/Risky Apps

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.



Spyware	Engages in broad-based data collection ?	Medium	Alert device
Adware	Serves intrusive ads or sends excessive PII to ad networks ?	Low	Alert device
Blacklisted App	App blacklisted as it violates policies or is unsafe ?	Low	Alert device
Chargeware	Misleadingly charges the device user ?		Alert device
Click Fraud	Defrauds ad networks by faking clicks or downloads ?		Alert device
Riskware	Engages in risky behavior ?	Low	Alert device

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)



Aatrox iPhone iOS 10.3.2 FFDN

iPhone 5s(16 GB Silver) | 10.3.2 | Ownership: Corporate - Sh...

0/0 Installed

1/3 Installed

1/2 Auto Apps

0/1 On Demand Apps

Content

No Content Assigned

View Content Management Pages

Certificates

5 Installed

0 Certificates Near Expiration (< 60 Days)

ASSET NUMBER
e083649f19f56418d3d-f06482d87fc6b061c74f5

POWER STATUS
On Battery (15% Remaining)

STORAGE CAPACITY
9 GB free of 12 GB (75.0%)

PHYSICAL MEMORY
853.71 MB free of 1000 MB (85.4%)

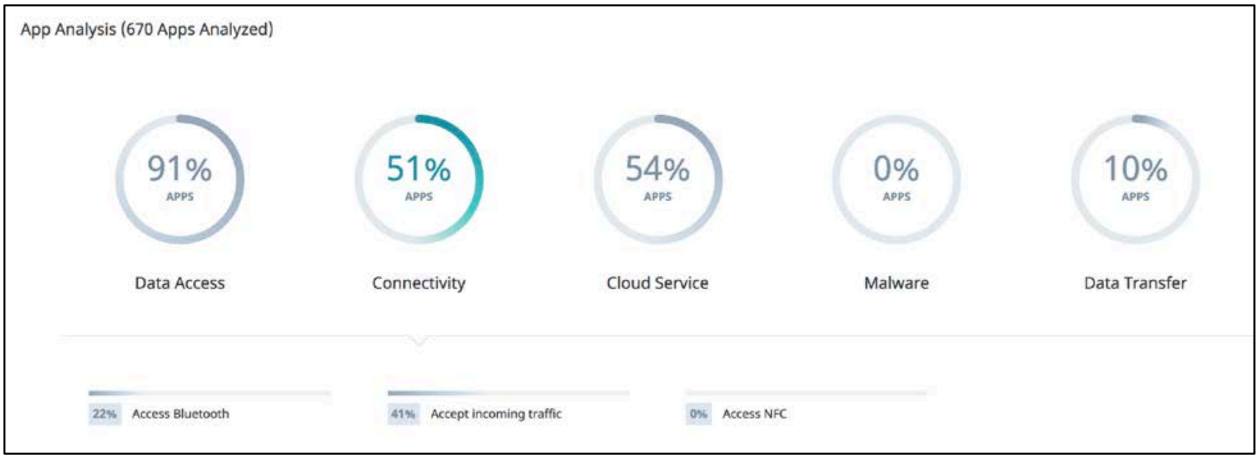
TAGS
MTP - Low Risk
MTP - Threats Present

AVAILABLE OS UPDATES
iOS 10.3.1

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



App Analysis (670 Apps Analyzed)

91% APPS Data Access

51% APPS Connectivity

54% APPS Cloud Service

0% APPS Malware

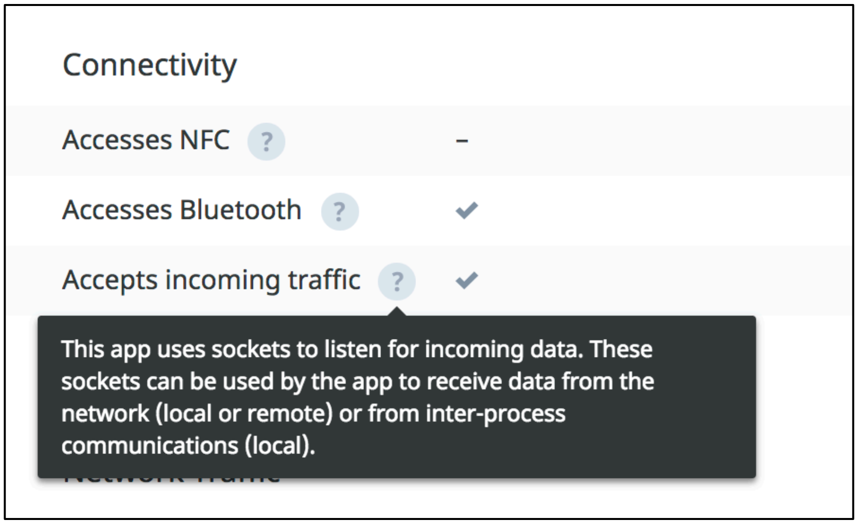
10% APPS Data Transfer

22% Access Bluetooth

41% Accept incoming traffic

0% Access NFC

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



Connectivity

Accesses NFC ?	–
Accesses Bluetooth ?	✓
Accepts incoming traffic ?	✓

This app uses sockets to listen for incoming data. These sockets can be used by the app to receive data from the network (local or remote) or from inter-process communications (local).

Figure 23. Application details that show connectivity for NFC/Bluetooth and accept incoming traffic

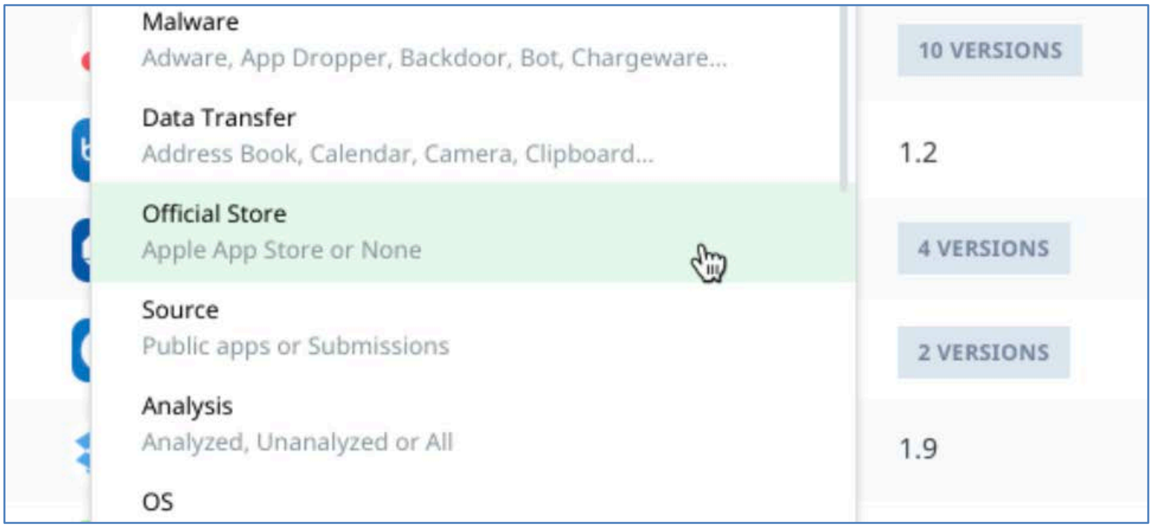
4.1.2 - Advanced Third Party Application Investigation and "Old Age" App Detection

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

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

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.



Malware
Adware, App Dropper, Backdoor, Bot, Chargeware...

Data Transfer
Address Book, Calendar, Camera, Clipboard...

Official Store
Apple App Store or None

Source
Public apps or Submissions

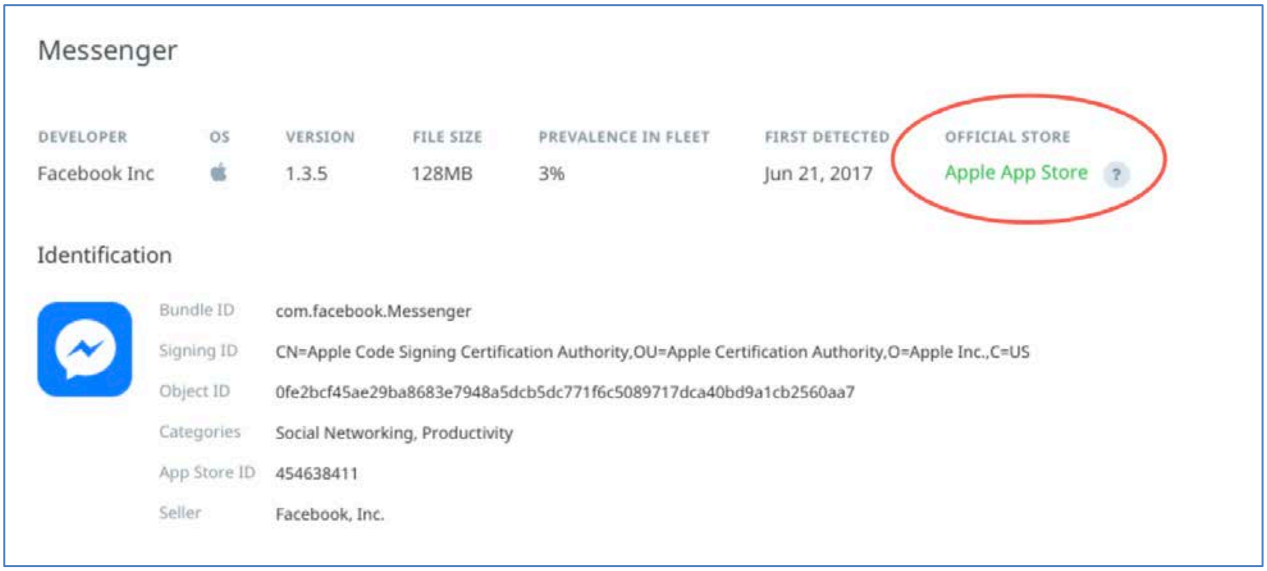
Analysis
Analyzed, Unanalyzed or All

OS

10 VERSIONS
1.2
4 VERSIONS
2 VERSIONS
1.9

Figure 24. Screenshot showing filter for App Store Apps

4.1.2.1.b. - Policy to notify end-users and admins of removed apps



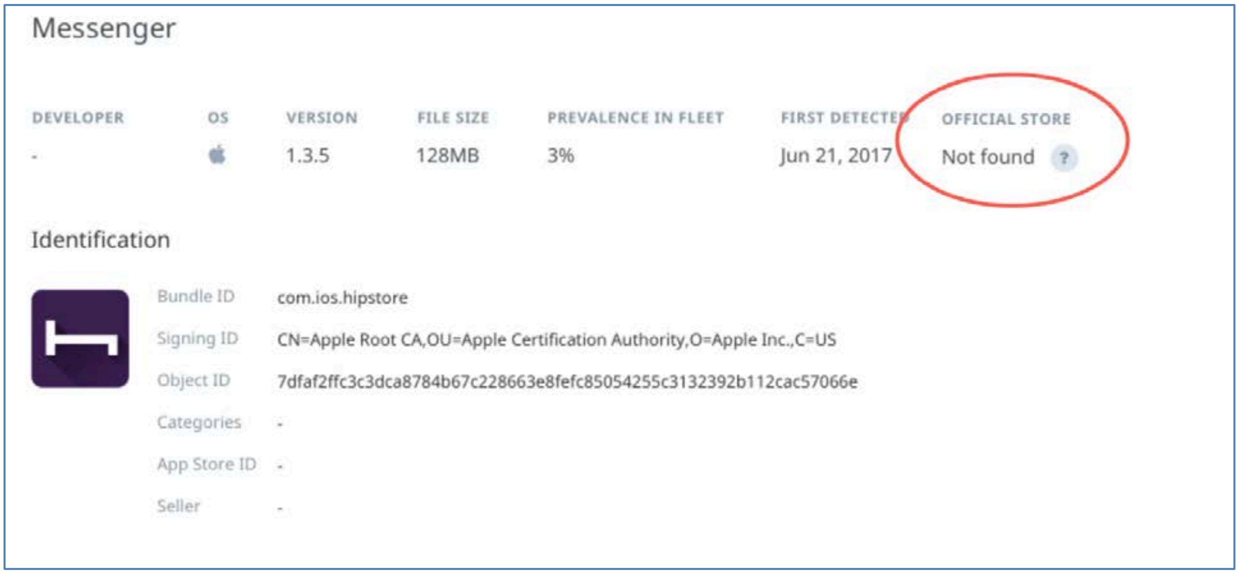
Messenger

DEVELOPER	OS	VERSION	FILE SIZE	PREVALENCE IN FLEET	FIRST DETECTED	OFFICIAL STORE
Facebook Inc		1.3.5	128MB	3%	Jun 21, 2017	Apple App Store ?

Identification

Bundle ID	com.facebook.Messenger
Signing ID	CN=Apple Code Signing Certification Authority,OU=Apple Certification Authority,O=Apple Inc.,C=US
Object ID	0fe2bcf45ae29ba8683e7948a5dcb5dc771f6c5089717dca40bd9a1cb2560aa7
Categories	Social Networking, Productivity
App Store ID	454638411
Seller	Facebook, Inc.

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



Messenger

DEVELOPER	OS	VERSION	FILE SIZE	PREVALENCE IN FLEET	FIRST DETECTED	OFFICIAL STORE
-		1.3.5	128MB	3%	Jun 21, 2017	Not found ?

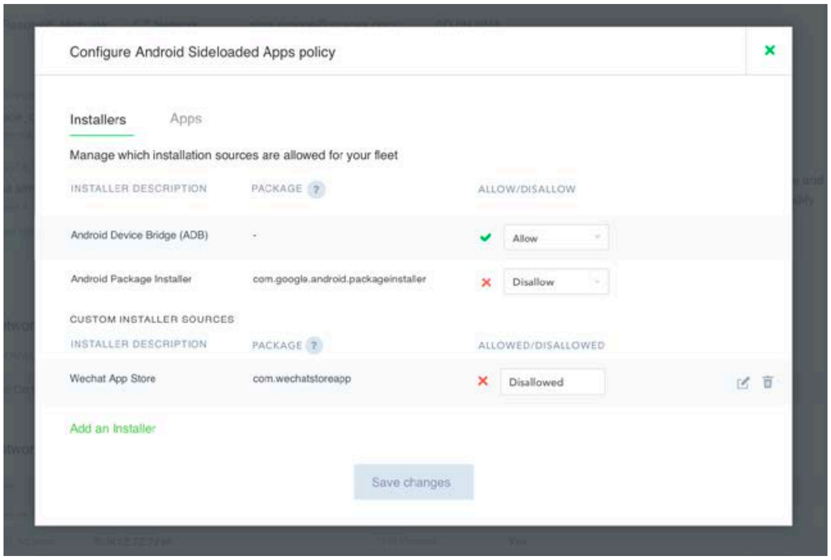
Identification

Bundle ID	com.ios.hipstore
Signing ID	CN=Apple Root CA,OU=Apple Certification Authority,O=Apple Inc.,C=US
Object ID	7dfaf2ffc3c3dca8784b67c228663e8fefc85054255c3132392b112cac57066e
Categories	-
App Store ID	-
Seller	-

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



Configure Android Sideloaded Apps policy

Manage which installation sources are allowed for your fleet

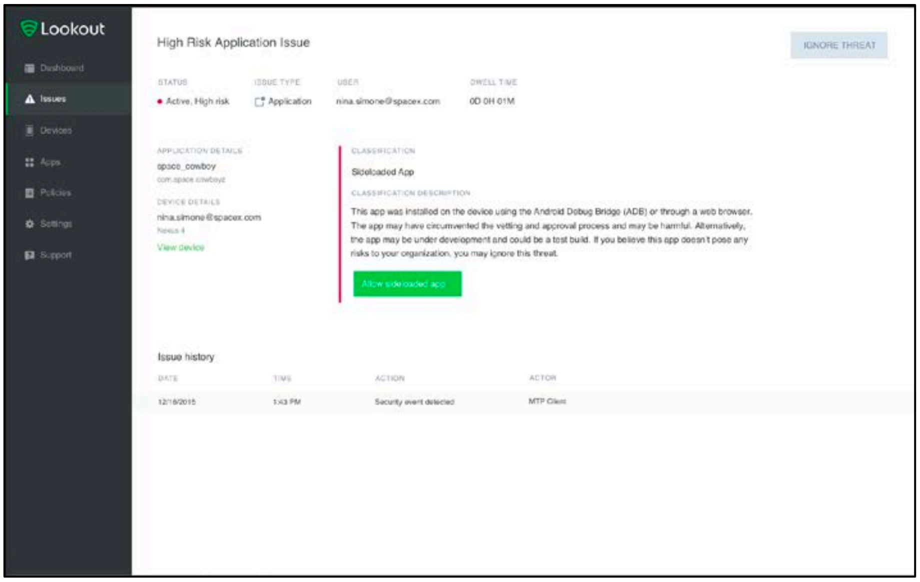
INSTALLER DESCRIPTION	PACKAGE ?	ALLOW/DISALLOW
Android Device Bridge (ADB)	-	✓ Allow
Android Package Installer	com.google.android.packageinstaller	✗ Disallow

CUSTOM INSTALLER SOURCES

INSTALLER DESCRIPTION	PACKAGE ?	ALLOWED/DISALLOWED
Wechat App Store	com.wechatstoreapp	✗ Disallowed

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



High Risk Application Issue

STATUS	ISSUE TYPE	USER	DWELL TIME
● Active, High risk	Application	nina.simone@spacex.com	0D 0H 01M

APPLICATION DETAILS
space_cowboy
com.space.cowboyz

DEVICE DETAILS
nina.simone@spacex.com
Nexus 4

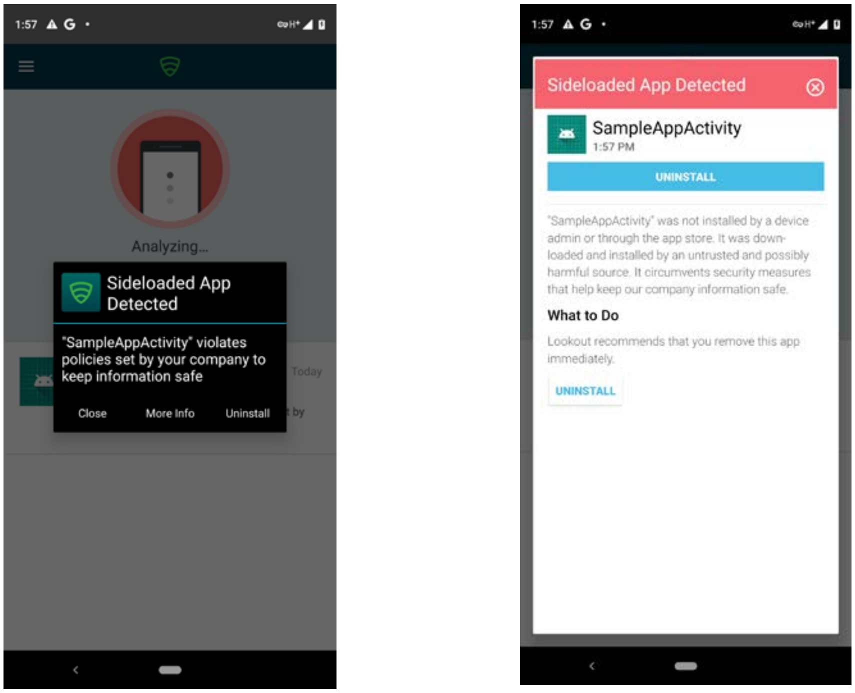
CLASSIFICATION
Sideloaded App

CLASSIFICATION DESCRIPTION
This app was installed on the device using the Android Debug Bridge (ADB) or through a web browser. The app may have circumvented the vetting and approval process and may be harmful. Alternatively, the app may be under development and could be a test build. If you believe this app doesn't pose any risks to your organization, you may ignore this threat.

Issue history

DATE	TIME	ACTION	ACTOR
12/18/2015	1:43 PM	Security event detected	MTP Client

Figure 28. Screenshot showing an Administrators notice of an Android Sideloaded Application on a user device



Sideloaded App Detected

"SampleAppActivity" violates policies set by your company to keep information safe

Sideloaded App Detected

SampleAppActivity
1:57 PM

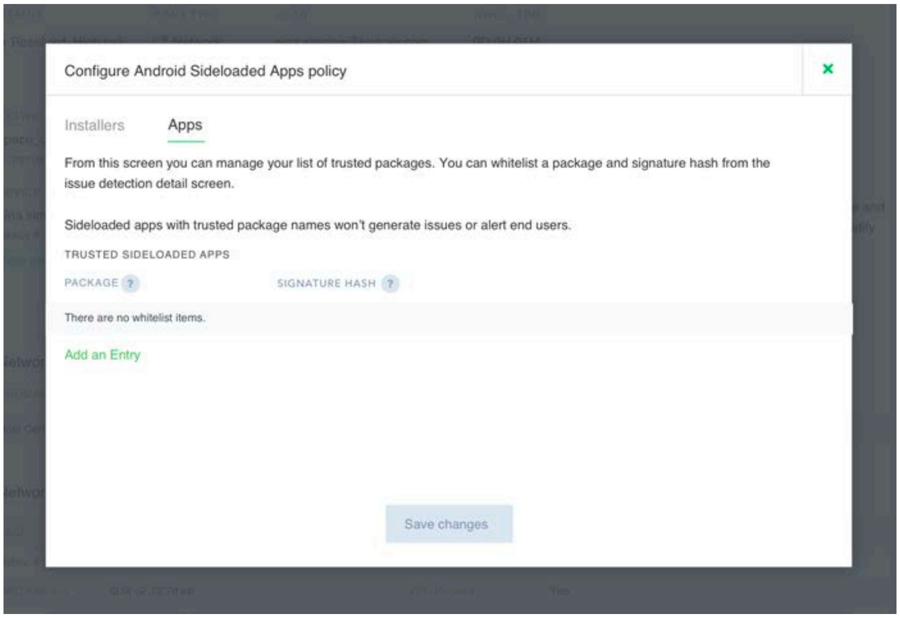
"SampleAppActivity" was not installed by a device admin or through the app store. It was downloaded and installed by an untrusted and possibly harmful source. It circumvents security measures that help keep our company information safe.

What to Do

Lookout recommends that you remove this app immediately.

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



Configure Android Sideloaded Apps policy

From this screen you can manage your list of trusted packages. You can whitelist a package and signature hash from the issue detection detail screen.

Sideloaded apps with trusted package names won't generate issues or alert end users.

TRUSTED SIDELOADED APPS

There are no whitelist items.

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

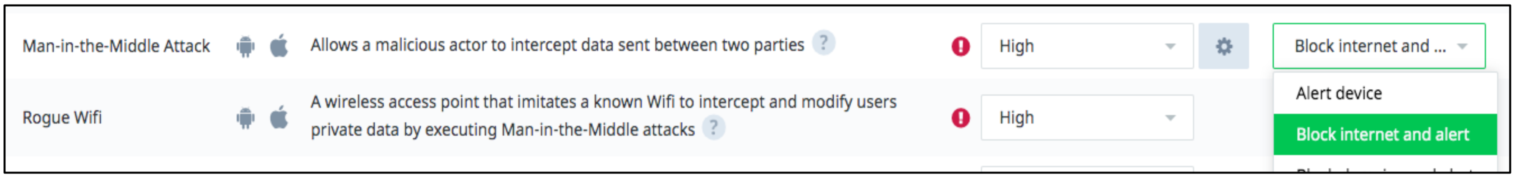
4.1.3 Man in The Middle Detection

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

4.1.3.1	Real-time on-device detection of network based threats	Complete Aug 2017
	Automatic disconnect option from malicious networks (configurable by admin)	Complete Feb 2019
	Notify admins, end-users and MDMs of the detected threat	Complete Aug 2017
4.1.3.2	Certificate whitelisting for legitimate proxy of traffic	Complete April 2019
	View certificate details of a detected attack	Complete Aug 2017
4.1.3.3	Content Modification Detection and Alerting	Complete Nov 2019
Additional	Rogue-Wifi detection	Complete Dec 2018

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

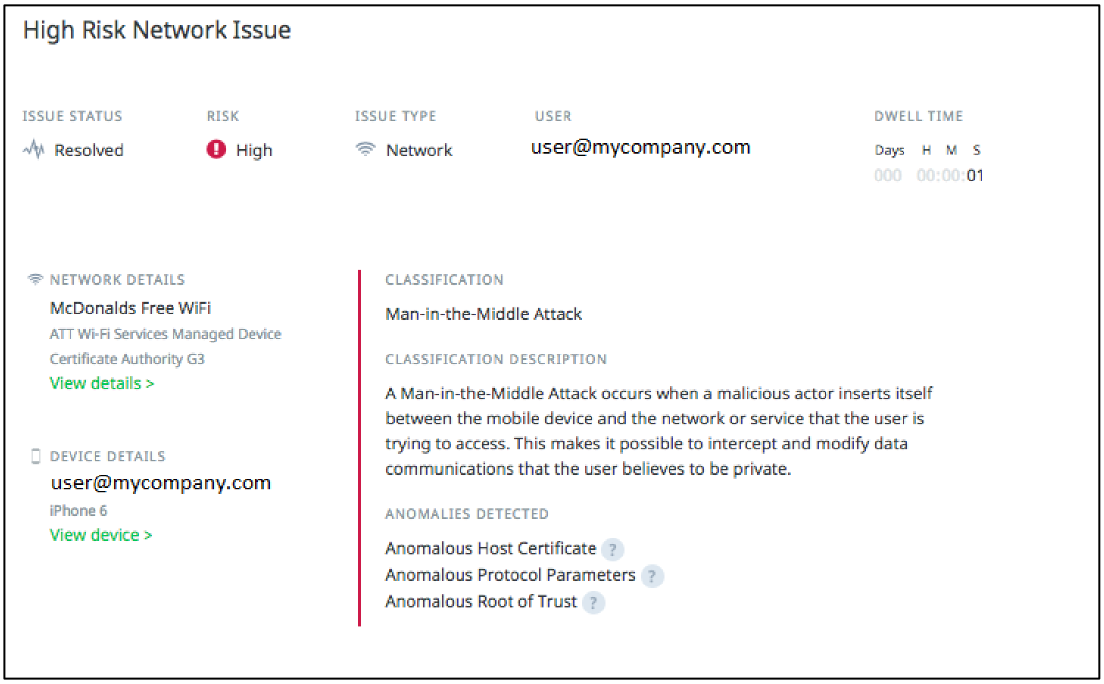
In the event that a Man-In-The-Middle attack is detected or the user connects to a Rogue Access Point, the admins have the ability to enforce a quarantine on the device and alert the user.



Man-in-the-Middle Attack — Allows a malicious actor to intercept data sent between two parties ? — High — Block internet and ...

Rogue Wifi — A wireless access point that imitates a known Wifi to intercept and modify users private data by executing Man-in-the-Middle attacks ? — High

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)



High Risk Network Issue

ISSUE STATUS	RISK	ISSUE TYPE	USER	DWELL TIME
Resolved	High	Network	user@mycompany.com	Days H M S 000 00:00:01

NETWORK DETAILS

McDonalds Free WiFi

ATT Wi-Fi Services Managed Device

Certificate Authority G3

View details >

DEVICE DETAILS

user@mycompany.com

iPhone 6

View device >

CLASSIFICATION

Man-in-the-Middle Attack

CLASSIFICATION DESCRIPTION

A Man-in-the-Middle Attack occurs when a malicious actor inserts itself between the mobile device and the network or service that the user is trying to access. This makes it possible to intercept and modify data communications that the user believes to be private.

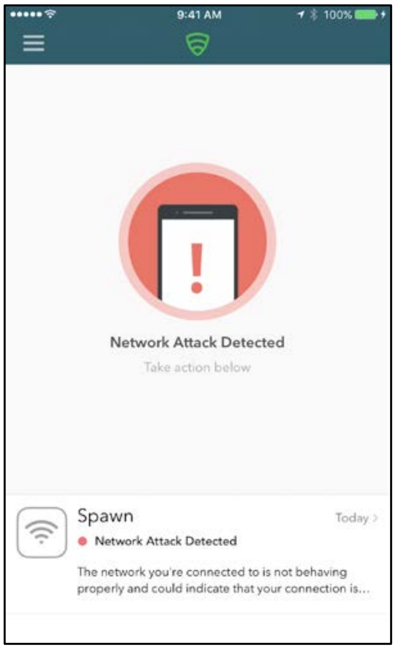
ANOMALIES DETECTED

Anomalous Host Certificate ?

Anomalous Protocol Parameters ?

Anomalous Root of Trust ?

Figure 32. Admin notification of a MITM threat on a user's device (Deliverable 4.1.3.1)



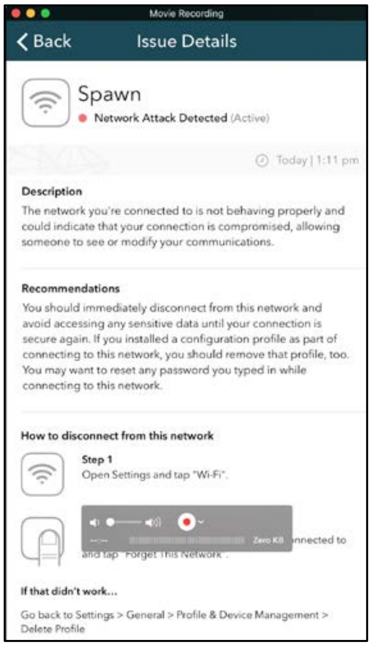
Network Attack Detected

Take action below

Spawn Today >

● Network Attack Detected

The network you're connected to is not behaving properly and could indicate that your connection is...



Issue Details

Spawn

● Network Attack Detected (Active)

Today | 1:11 pm

Description

The network you're connected to is not behaving properly and could indicate that your connection is compromised, allowing someone to see or modify your communications.

Recommendations

You should immediately disconnect from this network and avoid accessing any sensitive data until your connection is secure again. If you installed a configuration profile as part of connecting to this network, you should remove that profile, too. You may want to reset any password you typed in while connecting to this network.

How to disconnect from this network

Step 1
Open Settings and tap "Wi-Fi".

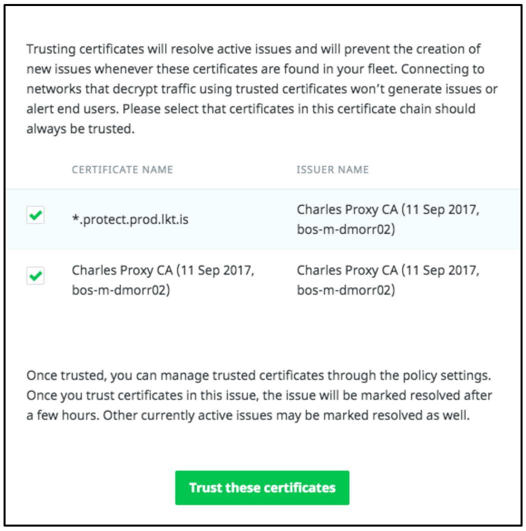
nnected to and tap "Forget This Network".

If that didn't work...

Go back to Settings > General > Profile & Device Management > Delete Profile

Figures 33 & 34. End user notification and remediation actions for MITM threat on mobile device. (Deliverable 4.1.3.1)

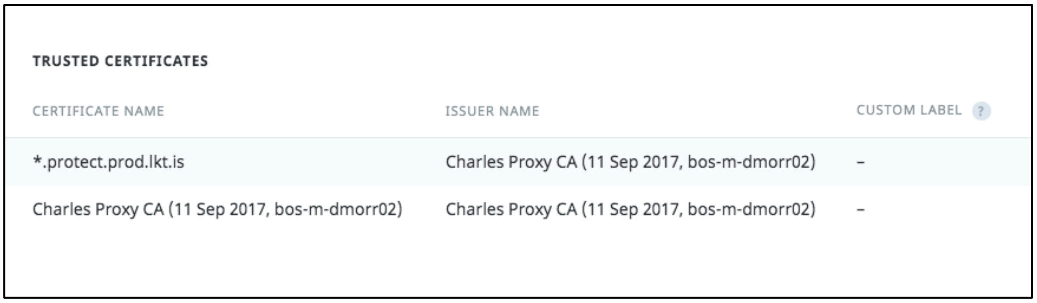
4.1.3.2 - Certificate whitelisting for legitimate proxy of traffic
4.1.3.2 - View certificate details of a detected attack



Trusting certificates will resolve active issues and will prevent the creation of new issues whenever these certificates are found in your fleet. Connecting to networks that decrypt traffic using trusted certificates won't generate issues or alert end users. Please select that certificates in this certificate chain should always be trusted.

	CERTIFICATE NAME	ISSUER NAME
☑	*.protect.prod.lkt.is	Charles Proxy CA (11 Sep 2017, bos-m-dmorr02)
☑	Charles Proxy CA (11 Sep 2017, bos-m-dmorr02)	Charles Proxy CA (11 Sep 2017, bos-m-dmorr02)

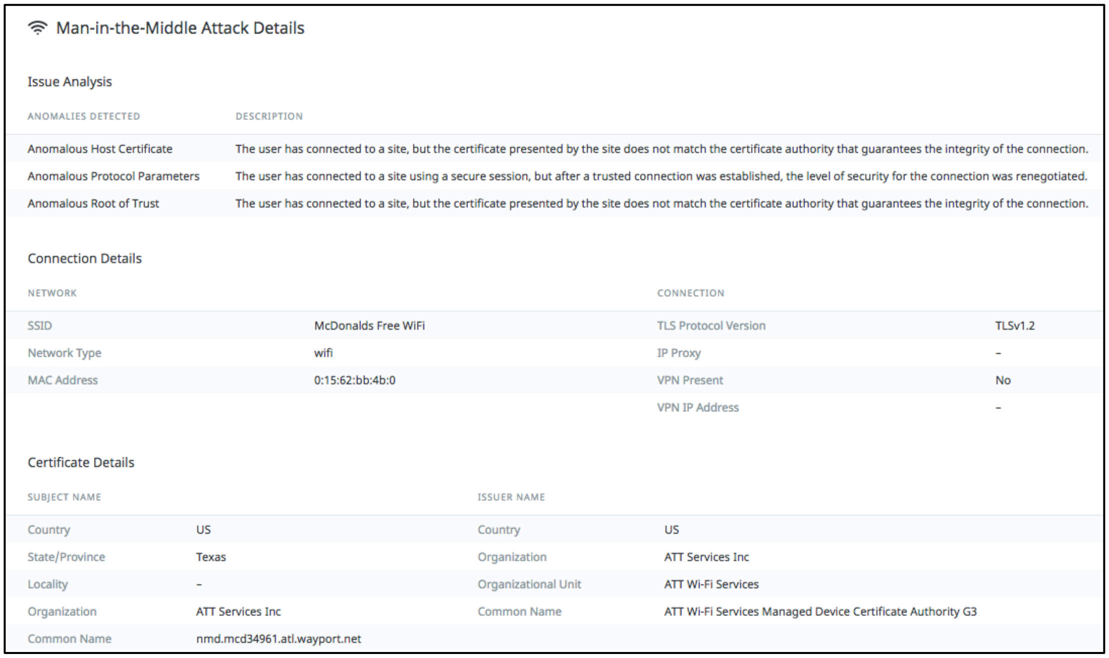
Once trusted, you can manage trusted certificates through the policy settings. Once you trust certificates in this issue, the issue will be marked resolved after a few hours. Other currently active issues may be marked resolved as well.



TRUSTED CERTIFICATES

CERTIFICATE NAME	ISSUER NAME	CUSTOM LABEL ?
*.protect.prod.lkt.is	Charles Proxy CA (11 Sep 2017, bos-m-dmorr02)	–
Charles Proxy CA (11 Sep 2017, bos-m-dmorr02)	Charles Proxy CA (11 Sep 2017, bos-m-dmorr02)	–

Figures 35 & 36. Screenshots showing the option to whitelist certificates for legitimate proxy of traffic (deliverable 4.1.3.2)



Man-in-the-Middle Attack Details

Issue Analysis

ANOMALIES DETECTED	DESCRIPTION
Anomalous Host Certificate	The user has connected to a site, but the certificate presented by the site does not match the certificate authority that guarantees the integrity of the connection.
Anomalous Protocol Parameters	The user has connected to a site using a secure session, but after a trusted connection was established, the level of security for the connection was renegotiated.
Anomalous Root of Trust	The user has connected to a site, but the certificate presented by the site does not match the certificate authority that guarantees the integrity of the connection.

Connection Details

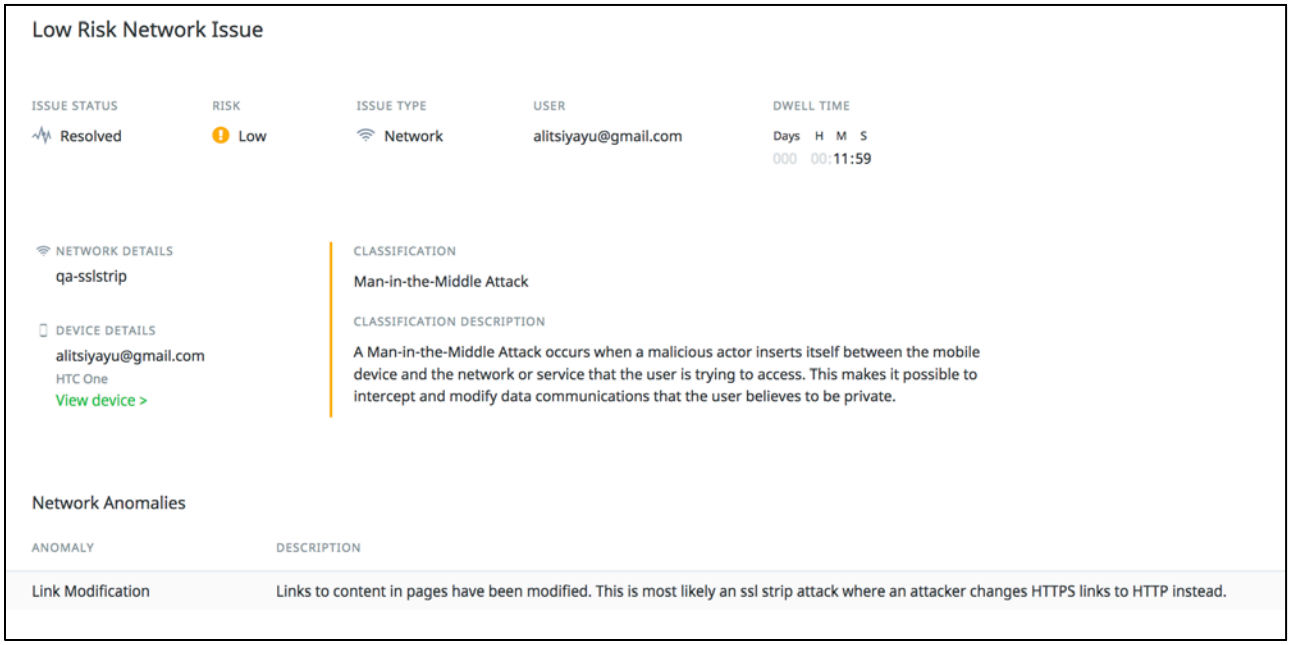
NETWORK		CONNECTION	
SSID	McDonalds Free WiFi	TLS Protocol Version	TLSv1.2
Network Type	wifi	IP Proxy	–
MAC Address	0:15:62:bb:4b:0	VPN Present	No
		VPN IP Address	–

Certificate Details

SUBJECT NAME		ISSUER NAME	
Country	US	Country	US
State/Province	Texas	Organization	ATT Services Inc
Locality	–	Organizational Unit	ATT Wi-Fi Services
Organization	ATT Services Inc	Common Name	ATT Wi-Fi Services Managed Device Certificate Authority G3
Common Name	nmd.mcd34961.atl.wayport.net		

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

4.1.3.3 Content Modification Detection and Alerting



Low Risk Network Issue

ISSUE STATUS	RISK	ISSUE TYPE	USER	DWELL TIME
Resolved	Low	Network	alitsiyayu@gmail.com	Days H M S 000 00:11:59

NETWORK DETAILS
qa-sslstrip

DEVICE DETAILS
alitsiyayu@gmail.com
HTC One
View device >

CLASSIFICATION
Man-in-the-Middle Attack

CLASSIFICATION DESCRIPTION
A Man-in-the-Middle Attack occurs when a malicious actor inserts itself between the mobile device and the network or service that the user is trying to access. This makes it possible to intercept and modify data communications that the user believes to be private.

Network Anomalies

ANOMALY	DESCRIPTION
Link Modification	Links to content in pages have been modified. This is most likely an ssl strip attack where an attacker changes HTTPS links to HTTP instead.

Figure 38. Screenshot showing a content modification detection (Deliverable 4.1.3.3)

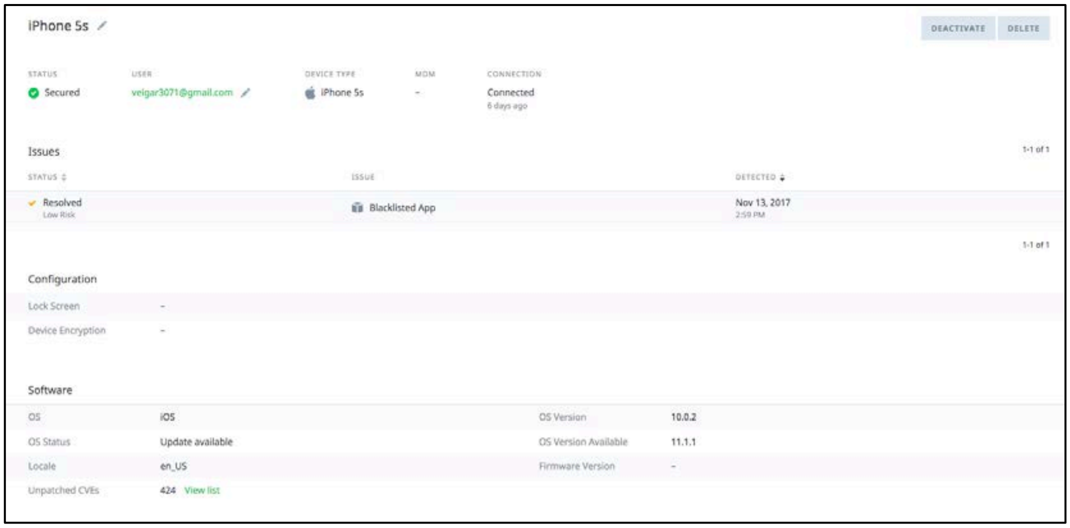
4.1.4 Mobile Vulnerability Detection and Management

Table 5. Mobile Vulnerability Detection deliverables and completion dates

4.1.4.1	Operating System Analysis Stack	
	Out of date OS notification	Complete Aug 2017
	Detection of OS vulnerabilities matching databases such as NVD and CVE	Complete Nov 2017
4.1.4.2	Application Analysis Stack	
	Detection of application vulnerabilities	Complete Jan 2019
4.1.4.3	Lookout Management Console Enhancements	
	MES Console reporting on device vulnerabilities	Complete Aug 2017
	Actionable options when vulnerabilities are detected	Complete Jan 2019

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 that particular release.



iPhone 5s

STATUS	USER	DEVICE TYPE	MDM	CONNECTION
Secured	veigar3071@gmail.com	iPhone 5s	-	Connected 6 days ago

Issues

1-1 of 1

STATUS	ISSUE	DETECTED
Resolved Low Risk	Blacklisted App	Nov 13, 2017 2:59 PM

1-1 of 1

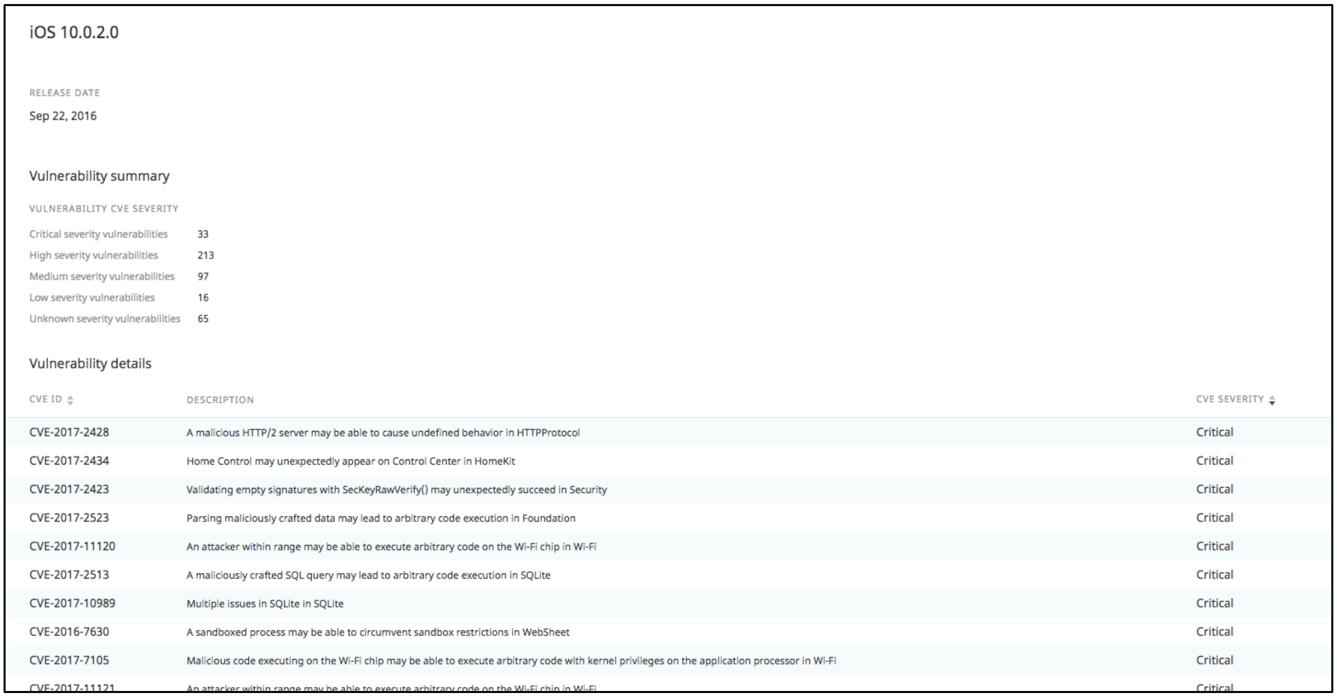
Configuration

Lock Screen	-
Device Encryption	-

Software

OS	iOS	OS Version	10.0.2
OS Status	Update available	OS Version Available	11.1.1
Locale	en_US	Firmware Version	-
Unpatched CVEs	424 View list		

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)



iOS 10.0.2.0

RELEASE DATE

Sep 22, 2016

Vulnerability summary

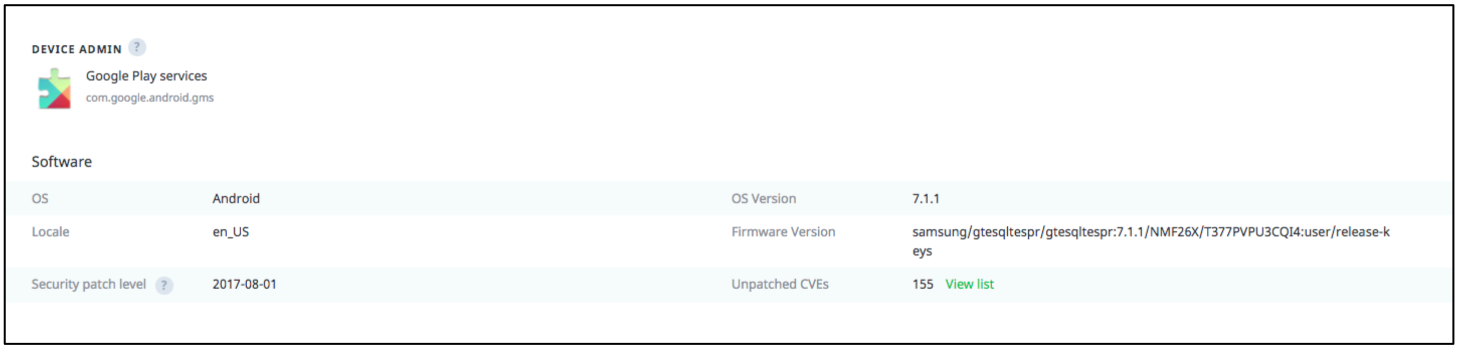
VULNERABILITY CVE SEVERITY

Critical severity vulnerabilities	33
High severity vulnerabilities	213
Medium severity vulnerabilities	97
Low severity vulnerabilities	16
Unknown severity vulnerabilities	65

Vulnerability details

CVE ID	DESCRIPTION	CVE SEVERITY
CVE-2017-2428	A malicious HTTP/2 server may be able to cause undefined behavior in HTTPProtocol	Critical
CVE-2017-2434	Home Control may unexpectedly appear on Control Center in HomeKit	Critical
CVE-2017-2423	Validating empty signatures with SecKeyRawVerify() may unexpectedly succeed in Security	Critical
CVE-2017-2523	Parsing maliciously crafted data may lead to arbitrary code execution in Foundation	Critical
CVE-2017-11120	An attacker within range may be able to execute arbitrary code on the Wi-Fi chip in Wi-Fi	Critical
CVE-2017-2513	A maliciously crafted SQL query may lead to arbitrary code execution in SQLite	Critical
CVE-2017-10989	Multiple issues in SQLite in SQLite	Critical
CVE-2016-7630	A sandboxed process may be able to circumvent sandbox restrictions in WebSheet	Critical
CVE-2017-7105	Malicious code executing on the Wi-Fi chip may be able to execute arbitrary code with kernel privileges on the application processor in Wi-Fi	Critical
CVE-2017-11121	An attacker within range may be able to execute arbitrary code on the Wi-Fi chip in Wi-Fi	Critical

Figure 40. Screenshot showing an iOS release and the details of the associated unpatched CVEs (Deliverable 4.1.4.1)



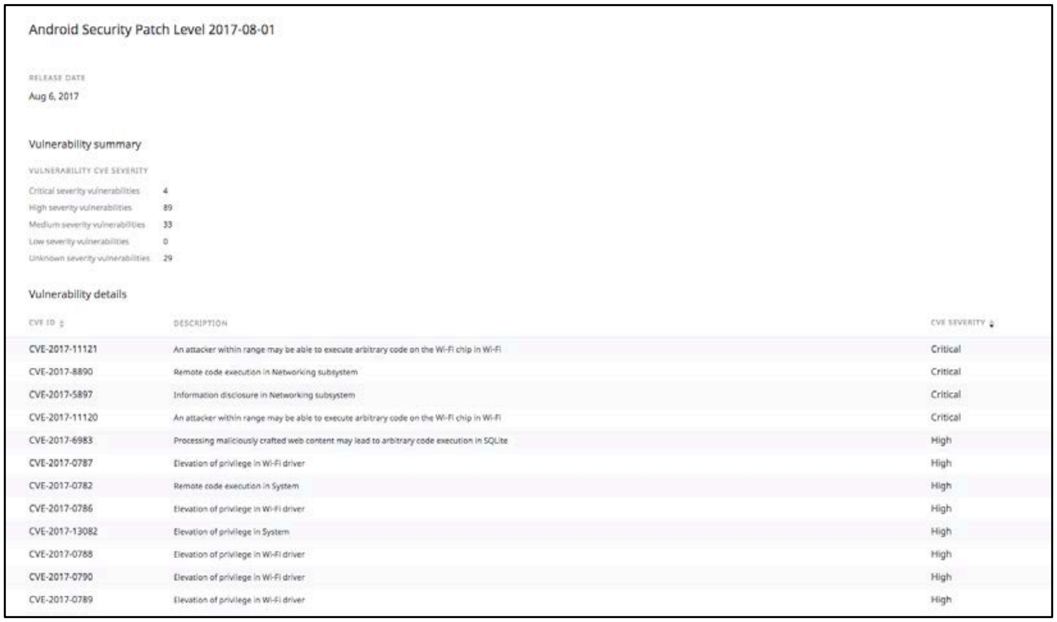
DEVICE ADMIN ?

Google Play services
com.google.android.gms

Software

OS	Android	OS Version	7.1.1
Locale	en_US	Firmware Version	samsung/gtesqltespr/gtesqltespr:7.1.1/NMF26X/T377PVPU3CQI4:user/release-keys
Security patch level ?	2017-08-01	Unpatched CVEs	155 View list

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)



Android Security Patch Level 2017-08-01

RELEASE DATE

Aug 6, 2017

Vulnerability summary

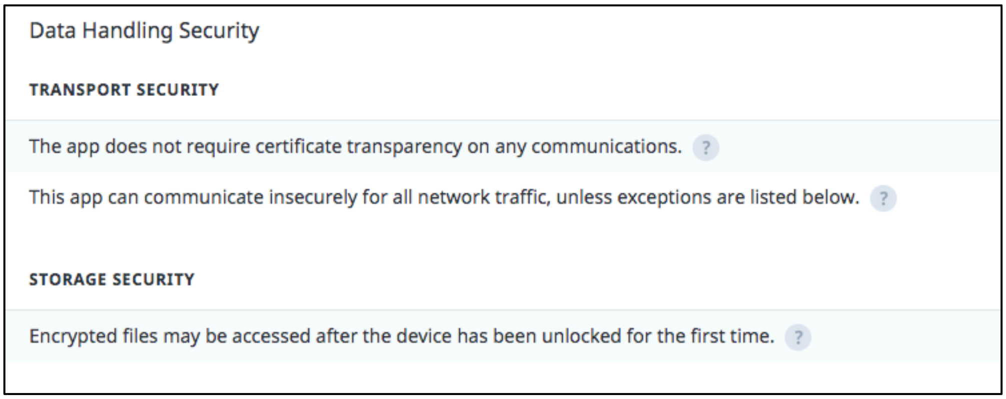
VULNERABILITY CVE SEVERITY	
Critical severity vulnerabilities	4
High severity vulnerabilities	89
Medium severity vulnerabilities	33
Low severity vulnerabilities	0
Unknown severity vulnerabilities	29

Vulnerability details

CVE ID	DESCRIPTION	CVE SEVERITY
CVE-2017-11121	An attacker within range may be able to execute arbitrary code on the Wi-Fi chip in Wi-Fi	Critical
CVE-2017-8890	Remote code execution in Networking subsystem	Critical
CVE-2017-5897	Information disclosure in Networking subsystem	Critical
CVE-2017-11120	An attacker within range may be able to execute arbitrary code on the Wi-Fi chip in Wi-Fi	Critical
CVE-2017-6983	Processing maliciously crafted web content may lead to arbitrary code execution in SQLite	High
CVE-2017-0787	Elevation of privilege in Wi-Fi driver	High
CVE-2017-0782	Remote code execution in System	High
CVE-2017-0786	Elevation of privilege in Wi-Fi driver	High
CVE-2017-13082	Elevation of privilege in System	High
CVE-2017-0788	Elevation of privilege in Wi-Fi driver	High
CVE-2017-0790	Elevation of privilege in Wi-Fi driver	High
CVE-2017-0789	Elevation of privilege in Wi-Fi driver	High

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

TRANSPORT SECURITY

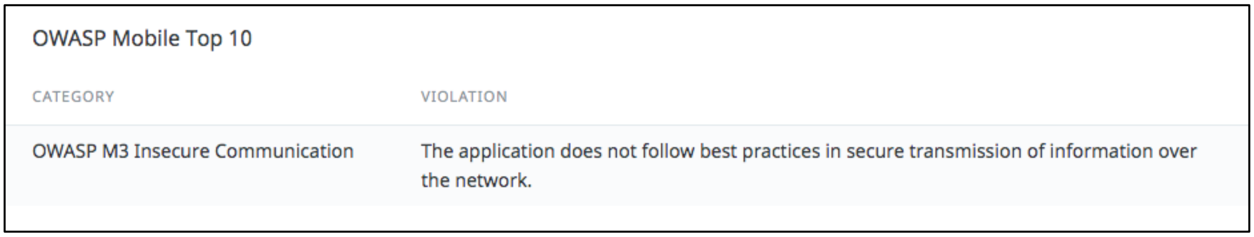
The app does not require certificate transparency on any communications. ?

This app can communicate insecurely for all network traffic, unless exceptions are listed below. ?

STORAGE SECURITY

Encrypted files may be accessed after the device has been unlocked for the first time. ?

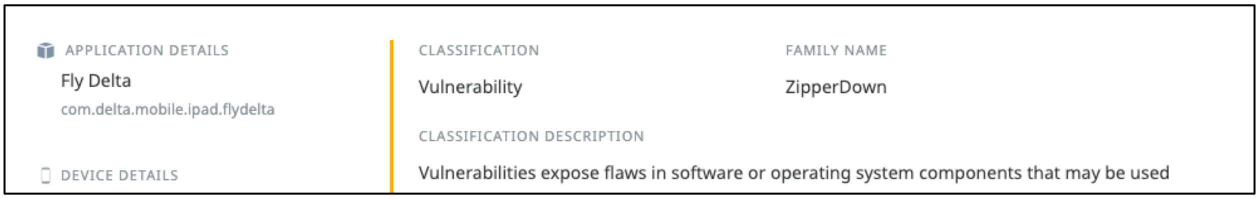
Figure 43. Screenshot showing Data Handling vulnerabilities for an application (Deliverable 4.1.4.2)



OWASP Mobile Top 10

CATEGORY	VIOLATION
OWASP M3 Insecure Communication	The application does not follow best practices in secure transmission of information over the network.

Figure 44. Screenshot showing OWASP violations (Deliverable 4.1.4.2)



APPLICATION DETAILS

Fly Delta

com.delta.mobile.ipad.flydelta

DEVICE DETAILS

CLASSIFICATION: Vulnerability

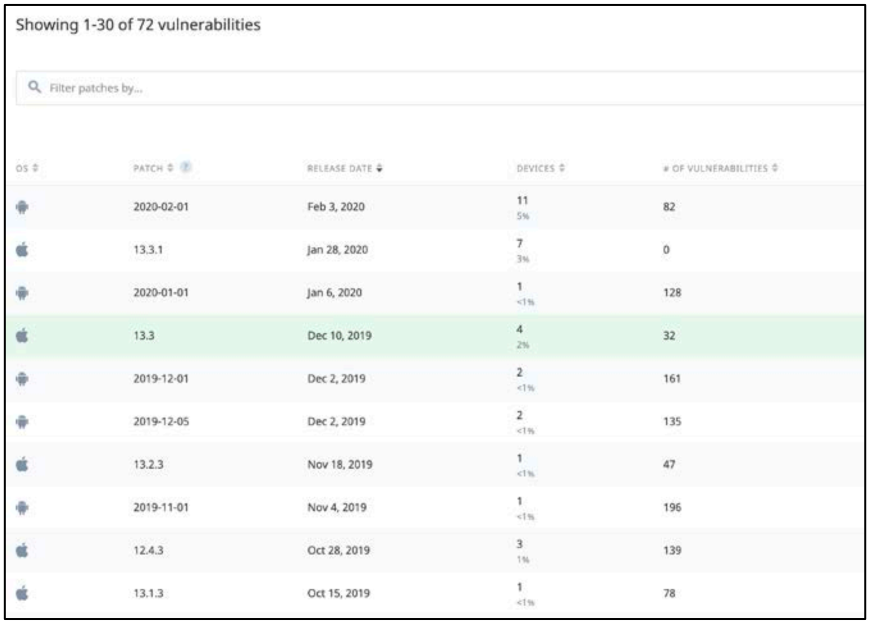
FAMILY NAME: ZipperDown

CLASSIFICATION DESCRIPTION

Vulnerabilities expose flaws in software or operating system components that may be used

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

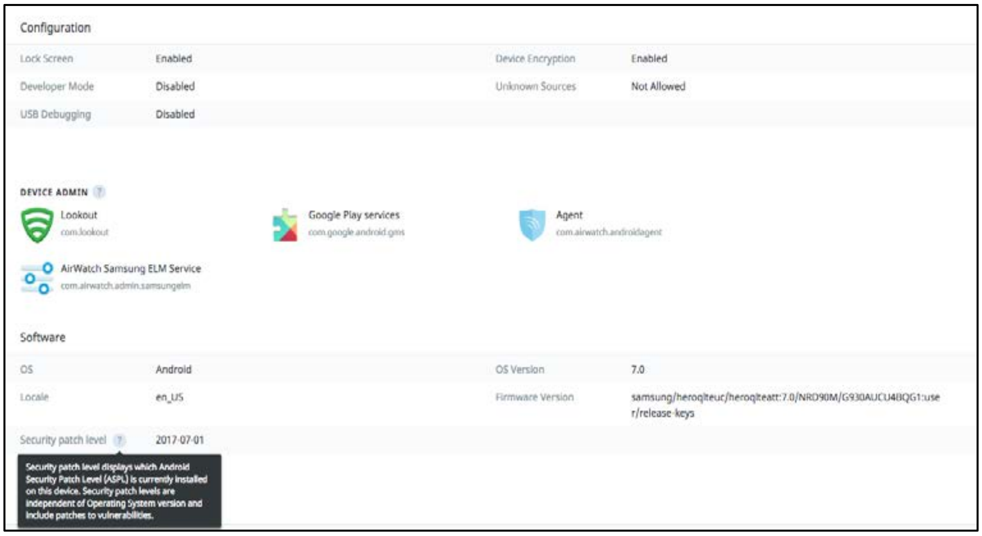
4.1.4.3a - MES Console reporting on device vulnerabilities



Showing 1-30 of 72 vulnerabilities

OS	PATCH	RELEASE DATE	DEVICES	# OF VULNERABILITIES
🤖	2020-02-01	Feb 3, 2020	11 5%	82
🍎	13.3.1	Jan 28, 2020	7 3%	0
🤖	2020-01-01	Jan 6, 2020	1 <1%	128
🍎	13.3	Dec 10, 2019	4 2%	32
🤖	2019-12-01	Dec 2, 2019	2 <1%	161
🤖	2019-12-05	Dec 2, 2019	2 <1%	135
🍎	13.2.3	Nov 18, 2019	1 <1%	47
🤖	2019-11-01	Nov 4, 2019	1 <1%	196
🍎	12.4.3	Oct 28, 2019	3 1%	139
🍎	13.1.3	Oct 15, 2019	1 <1%	78

Figure 46. Screenshot showing device software distributions and associated vulnerabilities



Configuration

Lock Screen	Enabled	Device Encryption	Enabled
Developer Mode	Disabled	Unknown Sources	Not Allowed
USB Debugging	Disabled		

DEVICE ADMIN

Lookout
com.lookout

Google Play services
com.google.android.gms

Agent
com.airwatch.androidagent

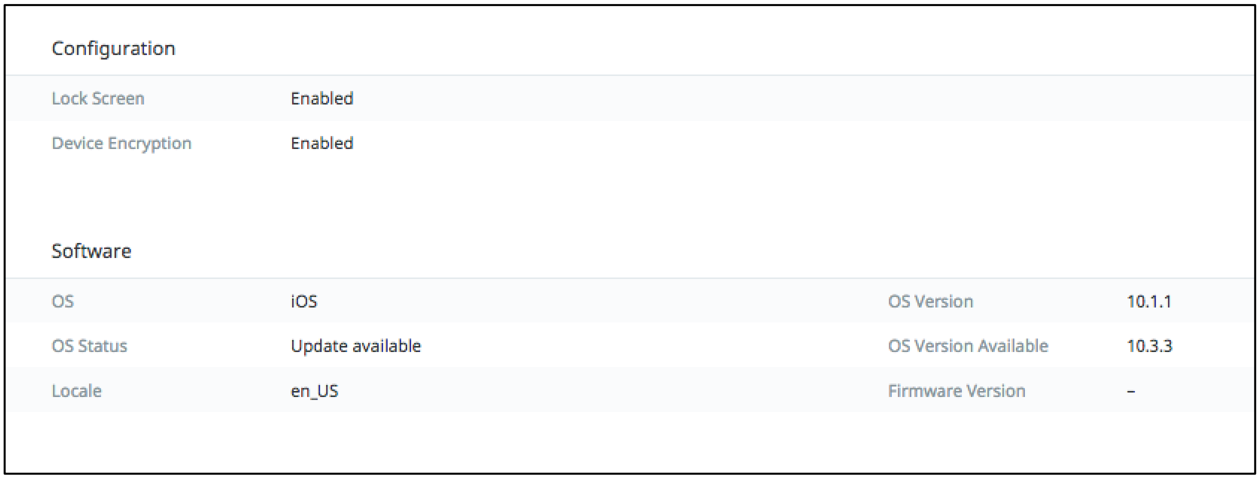
AirWatch Samsung ELM Service
com.airwatch.admin.samsungelm

Software

OS	Android	OS Version	7.0
Locale	en_US	Firmware Version	samsung/heroqlteuc/heroqlteatt:7.0/NRD90M/G930AUCU4BQG1:user/release-keys
Security patch level	2017-07-01		

Security patch level displays which Android Security Patch Level (ASPL) is currently installed on this device. Security patch levels are independent of Operating System version and include patches to vulnerabilities.

Figure 47. Device configuration information for Android devices (Deliverables 4.1.4.1, 4.1.4.3)



Configuration

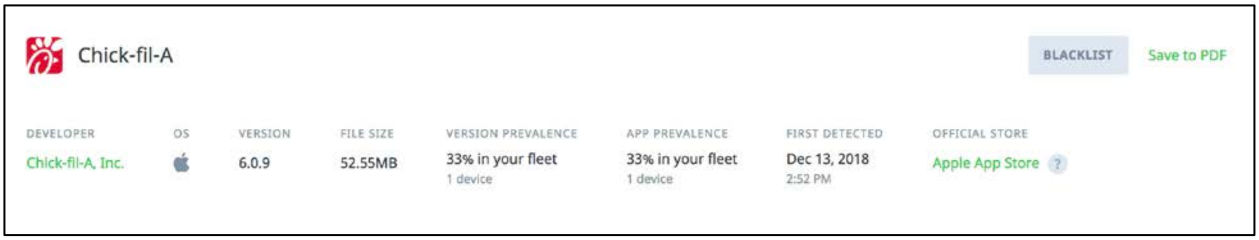
Lock Screen	Enabled
Device Encryption	Enabled

Software

OS	iOS	OS Version	10.1.1
OS Status	Update available	OS Version Available	10.3.3
Locale	en_US	Firmware Version	–

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

4.1.4.3b - Actionable options when vulnerabilities are detected



Chick-fil-A

DEVELOPER	OS	VERSION	FILE SIZE	VERSION PREVALENCE	APP PREVALENCE	FIRST DETECTED	OFFICIAL STORE
Chick-fil-A, Inc.		6.0.9	52.55MB	33% in your fleet 1 device	33% in your fleet 1 device	Dec 13, 2018 2:52 PM	Apple App Store ?

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 polices in the Lookout MES console. Devices that are out of compliance will be prevented from accessing corporate networks and data.

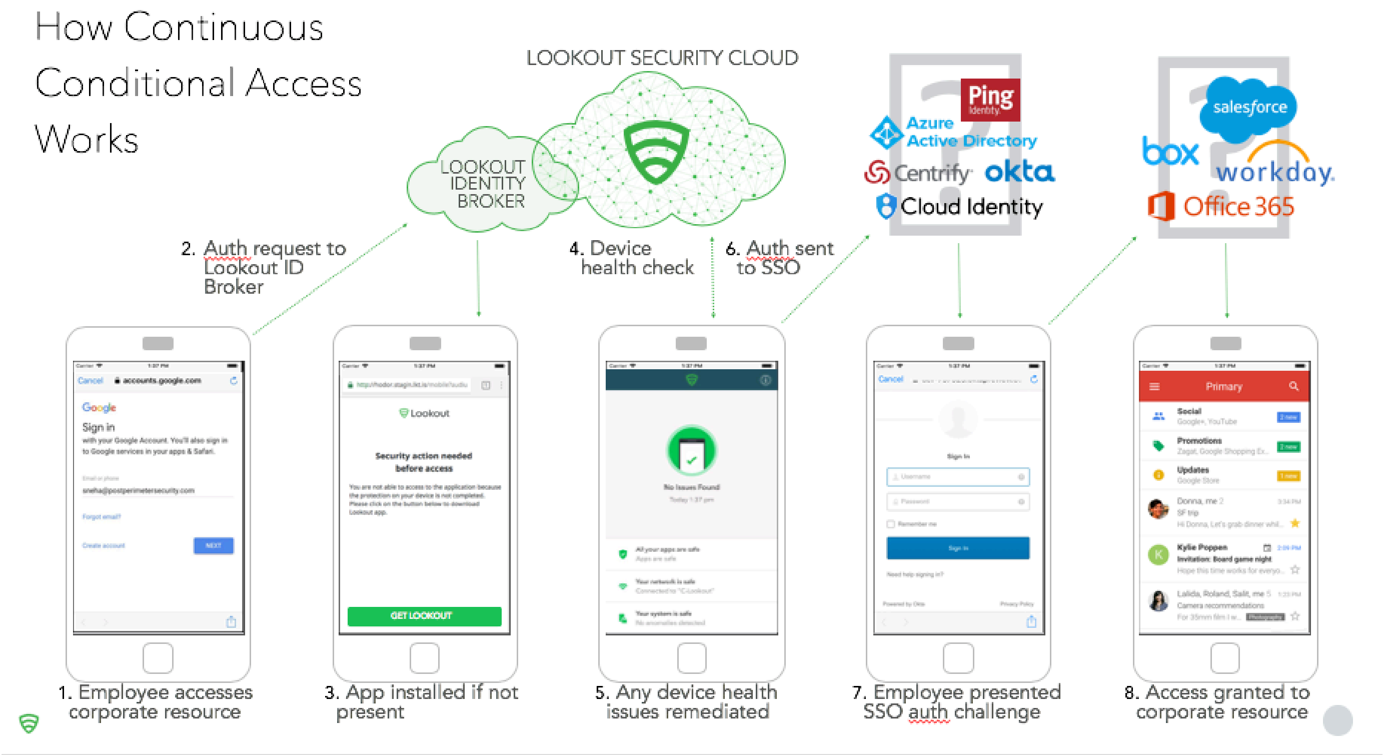

How Continuous Conditional Access Works
LOOKOUT SECURITY CLOUD
LOOKOUT IDENTITY BROKER
Ping Identity
Azure Active Directory
Centrify
okta
Cloud Identity
salesforce
box
workday.
Office 365
2. Auth request to Lookout ID Broker
4. Device health check
6. Auth sent to SSO
1. Employee accesses corporate resource
3. App installed if not present
5. Any device health issues remediated
7. Employee presented SSO auth challenge
8. Access granted to corporate resource
Google
Sign in
Lookout
Security action needed before access
GET LOOKOUT
No Issues Found
Sign in
Primary
Social
Promotions
Updates

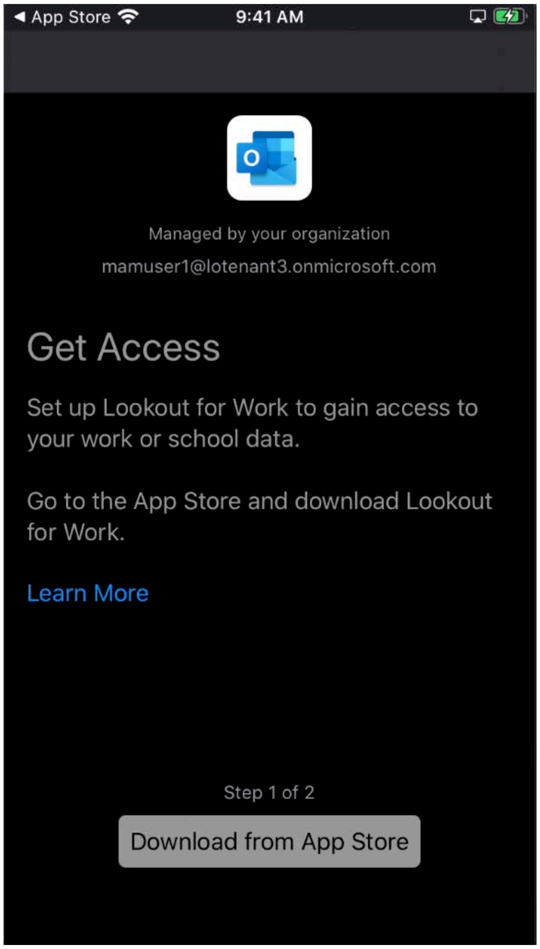
Figure 50. Overview of how Continuous Conditional Access work

Table 6. Continuous Conditional Access deliverables and completion dates.

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

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



Managed by your organization

mamuser1@lotenant3.onmicrosoft.com

Get Access

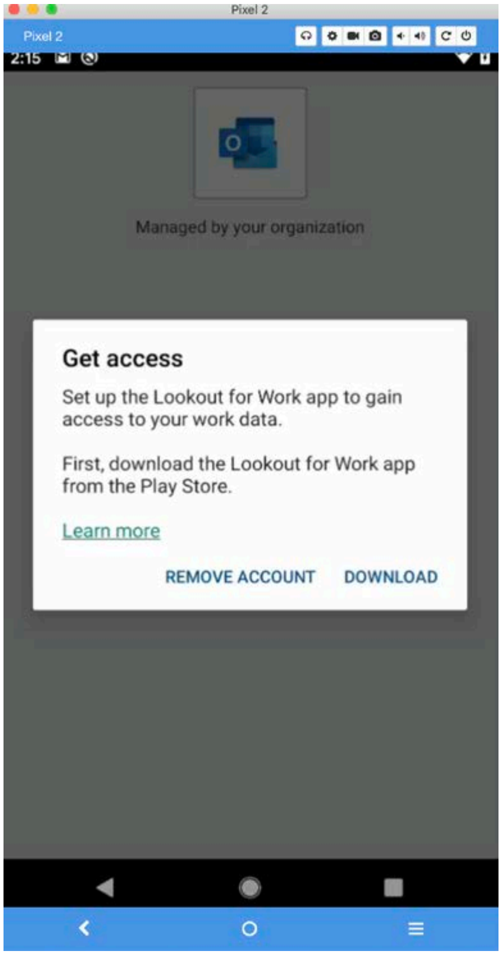
Set up Lookout for Work to gain access to your work or school data.

Go to the App Store and download Lookout for Work.

Learn More

Step 1 of 2

Download from App Store



Managed by your organization

Get access

Set up the Lookout for Work app to gain access to your work data.

First, download the Lookout for Work app from the Play Store.

Learn more

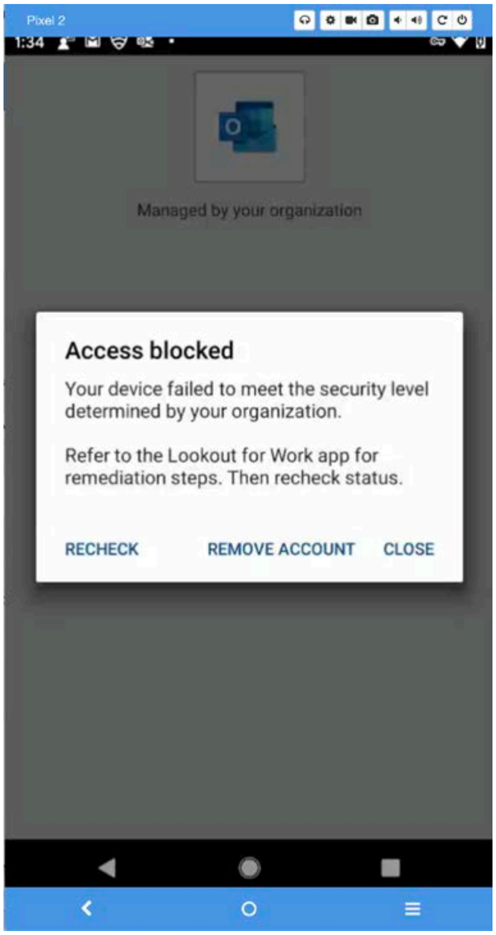
REMOVE ACCOUNT   DOWNLOAD

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



Access blocked

Your device failed to meet the security level determined by your organization.

Refer to the Lookout for Work app for remediation steps. Then recheck status.

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

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