WHITE PAPER

Lookout

LOOKOUT MOBILE ENDPOINT SECURITY HEALTHCARE SECURITY ARCHITECTURE AND TECHNOLOGY WHITE PAPER

ERIC WALKER | QSA(P2PE), PA-QSA, CISSP, GWAPT
NICK TRENC | QSA, PA-QSA, CISSP, CISA

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

INTRODUCTION

Lookout Inc. (Lookout) engaged Coalfire, a leading provider of industry-specific cyber risk management and compliance services, to conduct an independent technical assessment of the Lookout Mobile Endpoint Security platform and determine the platform's suitability and compliance for meeting the anti-virus, anti-malware, application security risks, and protection of electronic protected health information (ePHI) requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and HITRUST CSF™, in addition to the "Anti-Virus Checklist" from the "Top 10 Tips for Cybersecurity in Health Care" as published by the U.S. Department of Health and Human Services (HHS). Lookout Mobil Endpoint Security platform was tested with the use of an optional Mobile Device Management (MDM) solution for policy enforcement of anti-virus, anti-malware, application security risks, and EPHI protection. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance validation.

In this white paper, Coalfire describes how the Lookout Mobile Endpoint Security platform is able to meet the anti-virus and anti-malware, application security risks, and EPHI transmission protection requirements of the HIPAA Security Rule and HITRUST CSF™, in addition to the "Anti-Virus Checklist" from (HHS), based on the sample testing and evidence gathered during this assessment.

The paper also briefly describes the origin of HIPAA, presents the features of the software that can be leveraged for suitability and compliance, and provides a mapping of available features in the platform specific to HIPAA and HITRUST CSF™.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA is a 1996 United States legislation that provides data privacy and security provisions for safeguarding patient medical information. The HIPAA Security Rule provides requirements on the safeguarding of ePHI, which sets the standards for patient data security.

HIPAA SECURITY RULE

The HIPAA Security Rule specifically focuses on the protection of ePHI through the implementation of administrative, physical, and technical safeguards. Compliance is mandated to all organizations defined by HIPAA as a Covered Entity, Business Associate, or Subcontractor. Organizations such as these are required to:

- Ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the HIPAA Privacy Rule; and
- Ensure compliance by its workforce.

The requirements of the HIPAA Security Rule are organized according to safeguards, standards, and implementation specifications. The major sections include:

- Administrative Safeguards;
- Physical Safeguards; and
- Technical Safeguards.

HITRUST CSF™

HITRUST™ was founded in 2007 on the principles of establishing a common framework of information security controls, supported by a common assessment and reporting methodology, for the healthcare industry, including Business Associates of Covered Entities that service more than just healthcare. In addition, HITRUST normalizes and harmonizes requirements from ISO, NIST, PCI, HIPAA, and numerous other frameworks, standards, and regulations. The objective of the HITRUST CSF™ is to safeguard protected data during all phases of activity, such as transmission, storage, and data at rest.

ABOUT LOOKOUT MOBILE ENDPOINT SECURITY

Lookout Mobile Endpoint Security is a mobile protection platform that provides comprehensive risk management across iOS and Android devices to secure against threats, vulnerabilities, risky behavior, and configuration issues for mobile device applications, devices, and network connections.

With integration to a MDM solution, Lookout Mobile Endpoint Security will allow organizations to adopt secure mobility across personal and corporate owned devices.

Lookout Mobile Endpoint Security relies on three (3) main components:

- **Lookout for Work Application**: An Apple iOS or Android agent for corporate-owned and Bring-Your-Own Devices (BYOD) that provides connectivity to the Lookout Security Cloud, monitors the device attack surface, and executes policy-defined protection response.
- **Lookout Security Cloud**: The Lookout Security Cloud uses cloud correlative analysis to identify threats on devices. It is built on a foundation of mobile threat insights, application data, and malware analysis, including a corpus of more than 50 million mobile applications that are executed, assessed, compared, and analyzed on an on-going basis. The Lookout Security Cloud is also backed by crowd-sourced telemetry data collected from over 150 million mobile devices, with tens of millions of devices contributing new security telemetry every month from 150 countries.
- **Lookout Enterprise Dashboard**: The management console is a central location where administrators can facilitate device enrollment, receive data on threats and high-risk applications in their network, set security policy, and configure their optional MDM integration.

LOOKOUT MOBILE ENDPOINT SECURITY SUPPORT FOR HIPAA SAFEGUARDS, HITRUST CSF™, & HHS CHECKLIST REQUIREMENTS

Lookout Mobile Endpoint Security will allow organizations to meet requirements for HIPAA, HITRUST CSF™, and HHS Anti-Virus Checklist. The specific requirements that Lookout Mobile Endpoint Security can be utilized to meet are identified in the sections below:

HIPAA SAFEGUARDS

§164.308 Administrative Safeguards

§ 164.308(a)(5)(ii)(B) – (Addressable)

Protection from Malicious Software - Procedures for guarding against, detecting, and reporting malicious software.

§ 164.308(a)(6)(ii) – (Required)

Response and Reporting - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

For more information, visit:

https://www.gpo.gov/fdsys/pkg/CFR-2009-title45-vol1/pdf/CFR-2009-title45-vol1-sec164-308.pdf

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

§164.312 Technical Safeguards

§164.312(a)(2)(iv) – (Addressable)

Encryption and decryption - Implement a mechanism to encrypt and decrypt electronic protected health information.

§164.312(e)(1) – (Addressable)

Transmission Security - Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network

§164.312(e)(2)(ii) – (Addressable)

Encryption - Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

For more information, visit:

https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-312.pdf

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

HITRUST CSF™

09.04 Protection Against Malicious & Mobile Code

Ensure that integrity of information and software is protected from malicious or unauthorized code.

09.j Controls Against Malicious Code

Detection, prevention, and recovery controls shall be implemented to protect against malicious code, and appropriate user awareness procedures on malicious code shall be provided.

Protection against malicious code shall be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.

Protection against malicious code shall be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.

Bring your own device (BYOD) users are required to use anti-malware software

09.k Controls Against Mobile Code

Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.

Automated controls (e.g., browser settings) shall be in place to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations).

09.08 Exchange of Information

Ensure the exchange of information within an organization and with any external entity is secured and protected, and carried out in compliance with relevant legislation and exchange agreements.

09.s Information Exchange Policies & Procedures

Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication mediums.

When using electronic communication applications or systems for information exchange, the following items shall be addressed:

1. policies or guidelines shall be defined outlining acceptable use of electronic communication applications or systems;
2. the use of anti-malware for the detection of and protection against malicious code that may be transmitted through the use of electronic communications;
3. procedures shall be implemented for the use of wireless communications including an appropriate level of encryption (see 09.m);
4. employee, contractor and any other user's responsibilities shall be defined to not compromise the organization (e.g., through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.);
5. the required use of cryptographic techniques to protect the confidentiality, integrity and authenticity of covered information;
6. the retention and disposal guidelines shall be defined for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations; and
7. controls and restrictions shall be implemented associated with the forwarding of communications (e.g., automatic forwarding of electronic mail to external mail addresses). through the use of all types of communication mediums.

09.v Electronic Messaging

Information involved in electronic messaging shall be appropriately protected.

The electronic messages shall be protected throughout the duration of its end-to-end transport path. Cryptographic mechanisms shall be employed to protect message integrity and confidentiality unless protected by alternative measures, e.g., physical controls.

For more information, visit: https://hitrustalliance.net/hitrust-csf/

DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS)

Anti-Virus Checklist

- ☐ Policies are in place requiring use of anti-virus software.
- ☐ All staff understand and agree that they shall not hinder the operation of anti-virus software.
- ☐ All staff know how to recognize possible symptoms of viruses or malware on their computers.
- ☐ All staff know what to do to avoid virus/malware infections.
- ☐ Anti-virus software is installed and operating effectively on each computer in compliance with manufacturer recommendations.
- ☐ Anti-virus software is set up to allow automatic updates from the manufacturer.
- ☐ Anti-virus software is fully up-to-date according to the manufacturer's standards.
- ☐ Handheld or mobile devices that support anti-virus software have it installed and operating.

For more information, visit: https://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf

LOOKOUT MOBILE ENDPOINT SECURITY SUMMARY FINDINGS

Lookout Mobile Endpoint Security has many capabilities for addressing the requirements for HIPAA, HITRUST™ and the HHS Anti-Virus Checklist, the section below describes the highlights about the identified capabilities:

Lookout Mobile Endpoint Security centralized management is an online portal that includes device information, active issues, and application analysis.

The following findings are relevant highlights from this assessment:

- The Lookout Mobile Endpoint Security platform was able to detect and alert all supplied examples of viruses, Trojans, spyware, and other known malware.
- Automatic updates are no longer necessary as the software checks devices in real time against Lookout's proprietary virus repository.
- Application identification for Data Handling Security covering Transport Security and Storage Security, Data Access and Transfer, Network Traffic, and Cloud Services in Use for all applications in use on mobile devices. Applications can be blacklisted on devices and will alert users on installation and access to applications.
- The Lookout Mobile Endpoint Security platform was able to detect kernel-level exploits to gain root/jailbreak access to mobile devices.

- The Lookout Mobile Endpoint Security platform was able to detect man-in-the-middle (MiTM) threats from connected wireless networks.
- Lookout Mobile Endpoint Security centralized management allows administrators to send out links or push out from a MDM solution to deploy agents to iOS and Android devices.
- Lookout Mobile Endpoint Security centralized management shows the status of all device deployments, deployment risks, active issues, app analysis, issue trends, and issue detections breakdown.
- Lookout Mobile Endpoint Security can also provide additional policies for device restrictions, layout, settings access, and notifications and allow for policies to be assigned based on OS or ownership type (BYOD or corporate-owned) through the use of an external MDM solution.

LOOKOUT MOBILE ENDPOINT SECURITY DATA COLLECTION:

At a high level, Lookout Mobile Endpoint Security collects four (4) classes of data from enrolled devices:

- **Application Data:** Identify application-based security threats.
- **Firmware/OS Data:** Identify compromised firmware or operating systems.
- **Configuration Data:** Identify risky or malicious configurations.
- **Device Identifier Data:** Identify and remediate devices that pose a security risk to organization and communicate with device users in the event of a security issue.

Lookout does not collect any personally identifiable information (PII) or data generated by employees using applications, such as images, audio, video, or text content.

Lookout Mobile Endpoint Security administrators can define and enforce corporate policies by creating monitoring rules based on capabilities and behaviors to stay in compliance with the following risks:

- **Access to Sensitive Data:** Applications that access sensitive corporate or employee data (PII).
- **Data Exfiltration:** Applications that upload sensitive data to external servers and create risk for companies in regulated industries.
- **Data Sovereignty:** Applications that violate data sovereignty regulations or send data to risky geographies.
- **Use of Cloud Services:** Applications that access cloud storage providers, social networking services, or peer-to-peer networks.
- **Insecure Data Handling:** Applications that do not use proper encryption when storing or sending data.
- **Vulnerabilities:** Applications with known vulnerabilities and are the weakest link for attackers to exploit.

Lookout Mobile Endpoint Security data security of collected data in transit:

- Data in transit
  - Transport Layer Security (TLS) v1.2 with Forward Secrecy (FS)
  - Certificate Pinning

Additionally, Lookout Mobile Endpoint Security customers may choose to limit the personal data that Lookout collects from end users to comply with their organization's security policies. Lookout relies on a security cloud to power its analysis and threat detection, but through their integration with MDM solutions

and privacy controls capability, they can avoid collection and storage of PII from users while still providing full security capabilities.

ASSESSOR COMMENTS

The assessment scope put a significant focus on validating the use of Lookout Mobile Endpoint Security in a healthcare environment. Lookout Mobile Endpoint Security, when properly implemented following guidance from Lookout, can be utilized to meet technical requirements for:

- HIPAA: §164.308(a)(5)(ii)(B), §164.308(a)(6)(ii), §164.312(a)(2)(iv), §164.312(e)(1) and §164.312(e)(2)(ii)
- HITRUST CSF™: 09.j Controls Against Malicious Code, 09.k Controls Against Mobile Code, 09.s Information Exchange Policies & Procedures, and 09.v Electronic Messaging requirements.

However, as most computing environments and configurations differ drastically, it is important to note that use of this product does not guarantee security and even the most robust endpoint protection application can fail when improperly implemented or without ongoing maintenance. A defense-in-depth strategy that provides multiple layers of protection should be followed as a best practice. Please consult with Lookout for configuration questions and best practices.

It should also not be construed that the use of Lookout Mobile Endpoint Security guarantees full compliance with HIPAA or HITRUST™. Disregarding these requirements and security best practice controls for systems and networks inside or outside of the scope of the electronic health records environment can introduce many other security or business continuity risks to the healthcare organization. Security and business risk mitigation should be any healthcare organization's goal and focus for selecting security controls.

APPENDIX A: ABOUT THE TECHNICAL ASSESSMENT

AUDIENCE

This assessment white paper has three target audiences:

1. **Internal Audit Community:** This audience may be evaluating Lookout Mobile Endpoint Security to assess a healthcare organization, business associate, or service provider environment.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating Lookout Mobile Endpoint Security for use within their organization for compliance requirements and an addition to their MDM solution.
3. **Healthcare Organizations, Business Associate, and Service Providers:** This audience may be evaluating Lookout Mobile Endpoint Security for deployment in their environment and the benefits that could be achieved from using this solution with their MDM solution.

ASSESSMENT METHODOLOGY

Coalfire completed a multi-faceted technical assessment using the below industry and audit best practices. Coalfire conducted technical lab testing in its Colorado lab from October 16, 2017 to October 26, 2017.

The assessment used the following methods to assess the potential coverage of the solution:

1. Analysis of the architecture and configuration of the solution in accordance with vendor guidelines.
2. Deployment of the Lookout for Work application to test devices from both Google Play Store and Apple Store as well as from an email link sent directly from the Lookout Mobile Endpoint Security web portal.
3. Execution of known malware samples (to include virus, ransomware, Trojans, rootkits, adware, and worms) deliberately propagated to test devices.
4. Deployment of rogue access points and MiTM attacks in the environment to allow for wireless network-based threat detection.
5. Enablement of root on an Android phone for allowing privilege access to the OS functions. iOS jailbreak was not tested as older iOS versions have been blacklisted and are unable to be installed on current versions of Apple devices. As of writing this white paper, iOS versions 11.0.3 to 10.0.2 do not currently have a jailbreak available.
6. Review of management portal for verification of detection, and recommendations on removal of all test samples. Also, evaluation of the Lookout for Work application for verification that it is communicating to backend system, up-to-date, and protecting against real-time threats.
7. Review of policy enforcement with the use of an MDM solution for protecting mobile devices that are impacted by identified security threats from Lookout Mobile Endpoint Security.

LOOKOUT MOBILE ENDPOINT SECURITY COMPONENTS

Lookout Mobile Endpoint Security is a mobile protection solution comprised of:

1. **Lookout for Work Application** – Device application that connects to the Lookout Security Cloud for monitoring the device for threats and execution of policy-defined protection responses.
2. **Lookout Security Cloud** – Collective of systems that uses cloud correlative analysis to identify threats on devices.

3. **Lookout Enterprise Dashboard** – Central management web platform for administrators to facilitate device enrollment, review active issues, issue trends, issue detection breakdown, and gain an overall picture of device applications, potential threats, and optional integration with an MDM solution.
4. **Optional MDM Solution Integration** – Integration to an MDM solution allows management of mobile devices to include whitelisting/blacklisting applications and enforcement of policies before connecting to corporate assets. It should be noted that Lookout Mobile Endpoint Security works with multiple MDM solutions through a connection broker, MDM solutions are not directly part of the Lookout Mobile Endpoint Security solution.

ASSESSMENT ENVIRONMENT

The Lookout for Work application was installed on the following devices:

- Apple iPhone 6 (Hardware Version: MG5X2LL/A) with a fresh install of iOS 11.0.3
- Huawei Nexus 6P (Hardware Version: ANGLER-VN2) with a fresh install of Android 8.0.0 (Patch 10/5/2017 and Build OPR5.170623.007)

AirWatch MDM platform was used for testing policy enforcement with Lookout Mobile Endpoint Security

- AirWatch 9.2.0.411 running in an external hosted environment.

TOOLS AND TECHNIQUES

Standard tools Coalfire utilized for this technical assessment included:

TOOL NAME	DESCRIPTION
Malware Samples	Sample binaries of known malware for both Apple iOS and Android • Sample Apple iOS malware obtained from DeepEnd Research Dropbox https://www.dropbox.com/s/3wbonx0f9bjn9dh/Trojan_iPhoneOS_YiSpecter.zip?dl=0 • Sample Apple iOS malware obtained from Ricardo J. Rodr´ıguez Assistant Professor in Zaragoza, Spain http://webdiis.unizar.es/~ricardo/files/papers/supplementary_material/iOS-malware-samples.7z • Sample Android malware obtained from Ashish Bhatia GitHub Page https://github.com/ashishb/android-malware • Android Test EICAR malware obtained from Google Play Store at https://play.google.com/store/apps • Test EICAR file from WICAR.org http://www.wicar.org/ *Note – Visiting and downloading from the above sample malware may lead to infection. It is highly recommended to not download actual malware samples.
mitmproxy	Man-in-the-Middle Proxy (mitmproxy) is an interactive MiTM proxy for HTTP and HTTPS with a console interface. • Software can be obtained from https://mitmproxy.org/
hostapd	Host Access Point Daemon (hostapd) is a software access point capable of turning a device into a Wi-Fi access point. • Software can be obtained through various channels depending on Operating System https://packages.debian.org/jessie/hostapd *Note: hostapd was used in conjunction with various custom scripts and applications to act as a rogue access point and to allow for MiTM attacks.
AirWatch Mobile Device Management	VMWare AirWatch Mobile Device Management is a software platform for businesses to address the challenges associated with mobile devices, allowing for viewing and managing all devices from a central admin console.

	Software can be obtained from https://www.air-watch.com

REFERENCES

Lookout Website:

- https://lookout.com

HITRUST:

- HITRUST CSF™
  - https://hitrustalliance.net/hitrust-csf/
- Healthcare Sector Cybersecurity Framework Implementation Guide
  - https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf

U.S. Department of Health & Human Services:

- Code of Federal Regulations 2009 Title 45 Vol1 Sec 164-308:
  - https://www.gpo.gov/fdsys/pkg/CFR-2009-title45-vol1/pdf/CFR-2009-title45-vol1-sec164-308.pdf
- Health Insurance Portability and Accountability Act of 1996:
  - https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996
- Security Standards: Administrative Safeguards:
  - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
- Top 10 Tips for Cybersecurity in Health Care:
  - https://www.healthit.gov/playbook/pdf/top-10-tips-for-cybersecurity.pdf
- Anti-Virus Checklist:
  - https://www.healthit.gov/sites/default/files/Anti-Virus_Checklist.pdf
- 10 Best Practices For The Small Healthcare Environment:
  - https://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf
- Security Standards: Administrative Safeguards
  - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
- Security Standards: Technical Safeguards
  - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

AirWatch Website:

- https://air-watch.com

APPENDIX B: EXECUTED TEST PLAN

PROTECTING MOBILE DEVICES	TEST VALIDATION PLAN	CURRENT LOOKOUT MOBILE ENDPOINT SECURITY STATUS
Validate deployment of application on mobile devices	For a sample of devices, verify that the application is able to be deployed.	**1. Manual installation of application** All devices were able to install the application without any issues. Android and iOS versions had a specific version from their respected application store.
		2. Automated installation of application Automated deployment was conducted using the AirWatch MDM solution. Other MDM solutions were not tested during this assessment, but should function in a similar manner to AirWatch for automated deployment.
Detect and identifying known types of malicious software on mobile devices.	Review vendor documentation and examine configurations to verify that the application: • Detects all known types of malicious software; • Alerts for all known types of malicious software; and • Is able to protect against all known types of malicious software. This requires the use of an MDM solution. Examples of types of malicious software include: • viruses • Trojans • worms • spyware • adware • rootkits.	**1. Detect known types of malware:** Listings from virus repository or any other malware feed provided this type of data assurance.
		2. Alert on all known types of malware: Demonstrated that the Lookout for Work application alerted users of detected malware and gave specific details on how to remove the malware. Lookout Mobile Endpoint Security administrators received an email alerting to the malware on the device. Additionally, the Lookout Enterprise Dashboard showed the device that was affected, the time it took to remediate the alert, or if the alert was still ongoing.
		3. Protect against all known types of malware: Lookout Mobile Endpoint Security was able to detect common malware on the tested devices and, with the use of the AirWatch MDM solution, allowed for removing access to email and file shares until the devices were no longer affected by the detected malware.

PROTECTING MOBILE DEVICES	TEST VALIDATION PLAN	CURRENT LOOKOUT MOBILE ENDPOINT SECURITY STATUS
		Other MDM solutions were not tested during this assessment, but should function in a similar manner to AirWatch for automated protection.
Network-based Threat Detection on mobile devices.	Review vendor documentation and examine configurations to verify that the application: • Detects network-based attacks; • Alerts for network-based attacks; and • Is able to protect against all network-based attacks. This requires the use of an MDM solution. Examples of network-based attacks include: • MiTM • Rogue Access Point • TLS Protocol Downgrade	**1. Detect network-based attacks:** Demonstrated how the Lookout Mobile Endpoint Security application was able to detect MiTM attacks, Rouge access points, and TLS Downgrade attacks.
		2. Alert on network-based attacks: Alerts for both attacks were displayed on the mobile device with remediation steps. Lookout Mobile Endpoint Security administrators received an email alerting to the network-based threat on the device. Additionally, the Lookout Enterprise Dashboard showed the device that was affected, the time it took to remediate the alert or if the alert was still ongoing.
		3. Protect against network-based attacks: Lookout Mobile Endpoint Security was able to detect network based attacks, such as MiTM and rogue wireless networks. With the use of the AirWatch MDM solution devices had their wireless network disabled and access to email removed. Other MDM solutions were not tested during this assessment, but should function in a similar manner to AirWatch for automated protection.
Detect Root or Jailbreak on mobile devices	Review vendor documentation and examine configurations to verify that application: • Detects device-based attacks • Alerts for device-based attacks • Is able to protect against device-based attacks. This requires the use of an MDM solution.	**1. Detect on device-based threat detection:** Demonstrated how the Lookout Mobile Endpoint Security application was able to detect root (on Android) mobile operating systems. iOS jailbreak was not tested as access to an older version of iOS was not available to be installed. Versions 11.0.3 to 10.0.2 did not have a jailbreak available during the testing period. Older versions have been

PROTECTING MOBILE DEVICES	TEST VALIDATION PLAN	CURRENT LOOKOUT MOBILE ENDPOINT SECURITY STATUS
		blacklisted and are not able to be installed on current versions of Apple devices.
		2. Alert on device-based threat detection: Alerts for root (Android) were displayed on the mobile device with remediation steps. Lookout Mobile Endpoint Security administrators received an email alerting to the device-based threat on the device. Additionally, the Lookout Enterprise Dashboard showed the device that was affected, the time it took to remediate the alert, or if the alert was still ongoing.
		3. Protect against device-based threat detection: Lookout Mobile Endpoint Security was able to detect root enabler applications and if the device had been rooted. With the use of the AirWatch MDM solution device access to email and test applications were removed. Other MDM solutions were not tested during this assessment, but should function in a similar manner to AirWatch for automated deployment. iOS jailbreak was not tested as older iOS versions have been blacklisted and are not able to be installed on current versions of Apple devices. As of writing this white paper iOS versions 11.0.3 to 10.0.2 did not have a jailbreak exploit available during the testing period.
Application Risks	Review vendor documentation and examine configurations to verify that the application: • Detects application configuration, behavior, application data transmission and storage; • Alerts for risky application configuration, behavior,	**1. Detect on application-based threat detection:** Lookout Mobile Endpoint Security was able to detect the Access and Transfer of Address Book, Calendar, Camera, Clipboard, Device Identifiers, Local Storage, Location, Media, Microphone, Reminders, and SMS Archive on mobile devices for all applications installed.

PROTECTING MOBILE DEVICES	TEST VALIDATION PLAN	CURRENT LOOKOUT MOBILE ENDPOINT SECURITY STATUS
	application data transmission and storage; and • Is able to protect against risky application configuration, behavior, application data transmission and storage. This requires the use of an MDM solution	**2. Alert on application-based threat detection:** Lookout Mobile Endpoint Security was able to alert users on applications that were blacklisted and are currently installed on the mobile device.
		3. Protect against application-based threat detection: Lookout Mobile Endpoint Security was able to detect blacklisted applications and notify the end-user of the noncompliance. With the use of an MDM solution the applications could be removed or specific access to email or other applications could be removed.
Validate connectivity of application to cloud service	Review connectivity of the application to Lookout services • Validate TLS connection • Validate TLS version • Validate Certificate Pinning	**1. Validation of communication of Lookout for Work Application** Review of packet captures for initial connections from the application validated that TLS v1.2 with a minimum of AES-128 Cipher was used for all connections to Lookout services Detailed Cipher Suite Information: (TLS_ECDHE_RSA_WITH_ AES_128_GCM_SHA256)

ABOUT THE AUTHORS

Eric Walker | Senior Security Consultant

Eric Walker (eric.walker@coalfire.com) is an Senior Security Consultant in the Payment Solutions Team with Coalfire. Eric has several years of experience working as a QSA(P2PE) and PA-QSA helping clients develop systems and software for use in PCI DSS environments and has authored and spoken on multiple security topics including application security, social-engineering, penetration testing, software development lifecycle, and PCI compliance. He holds the CISSP, QSA(P2PE), PA-QSA, GWAPT and ISO/IEC 27001:2013 Lead Auditor certifications.

Nick Trenc | Practice Director

Nick Trenc (ntrenc@coalfire.com) is a Practice Director and Application Security Specialist with Coalfire. Nick has several years of experience working as a QSA and PA-QSA helping clients develop systems and software for use in PCI DSS environments and has authored and spoken on multiple security topics including mobile security, application security, virtualization, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance. He holds the CISSP, CISA, QSA, and PA-QSA certifications.

Published November 2017.

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com