Lookout

Lookout Proof of Concept Overview

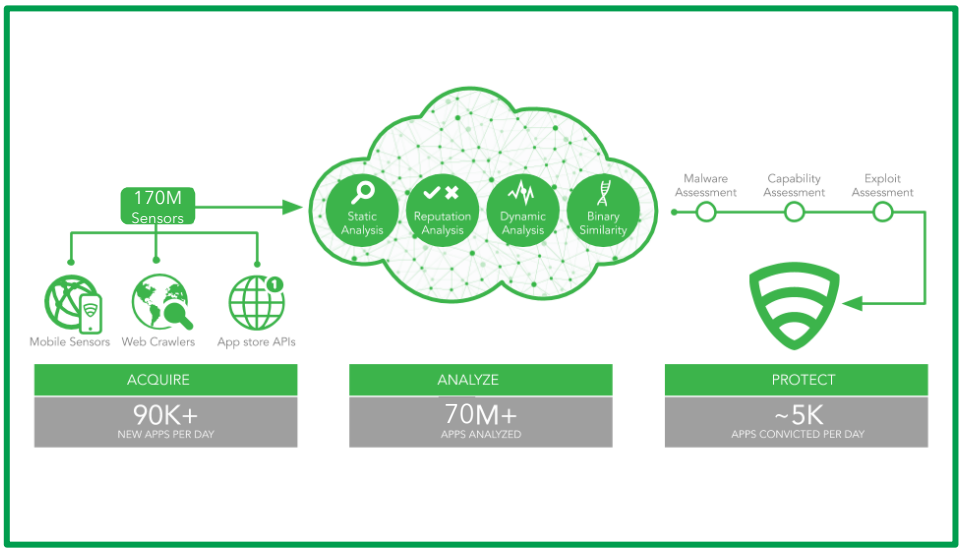
I. About Lookout
II. Products and Services
III. Technical Insights
IV. Industry Recognition
V. Privacy

About Lookout

Lookout is a cybersecurity company for the post-perimeter, cloud-first, mobile-first world. Powered by the largest dataset of mobile code in existence with over 170M devices and 70M apps, the Lookout Security Cloud provides visibility into the entire spectrum of mobile risk.

Since 2007, Lookout has focused solely on mobile security, creating solutions that are effective, respectful of privacy and offer an intuitive and enjoyable user experience. Lookout recognizes that the security challenges associated with mobile devices are always changing and that a new approach to security is required. This approach should be holistic and pre-emptive, while still supporting the freedom that mobile users require to be productive

Lookout is trusted by hundreds of millions of individual users, enterprises, and government agencies as well as partners such as AT&T, Verizon, Vodafone, Microsoft, Apple and others. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.



Notable Lookout Discoveries

Lookout's security research team and AI-powered security cloud are constantly discovering new threats.

Below are select examples:

Monokle: July 14th, 2019

- Monokle is a new and sophisticated set of Android surveillanceware tools developed by Russian-based company Special Technology Centre, Ltd. (STC). STC was sanctioned by the U.S. Government in connection with interference in the 2016 U.S. presidential elections.

DNC Phishing Attack: August 22nd, 2018

- Lookout's PhishingAI discovered and alerted on this site as a custom phishing site hosted on DigitalOcean's infrastructure. The site replicated a login page for NGP VAN, which is used by Democrats, their campaigns, and associated non-profits.

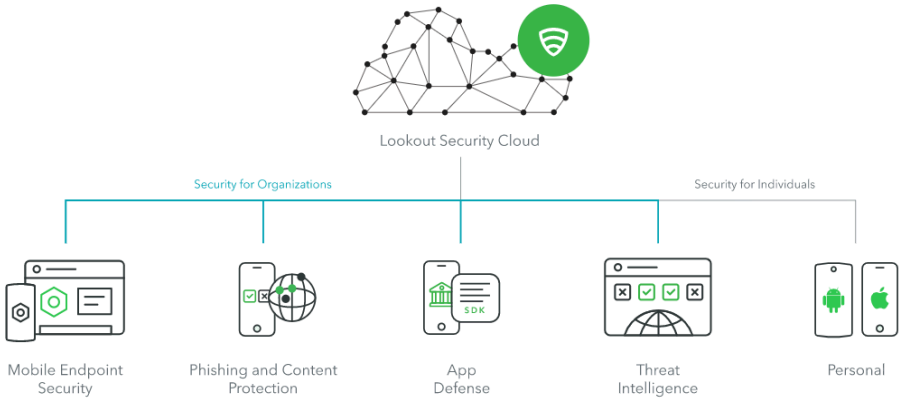
ViperRAT: February 16th, 2017

- Nation-state sponsored attack targeting Israeli Defense Force (IDF) soldiers through aggressive social engineering. With the goal of getting the soldiers to download trojanized apps that gave the actor control of the device and its data

Pegasus: August 25th, 2016

- Pegasus allowed an adversary to silently jailbreak the device and listen in on conversations, spy through the camera, steal messages and contact lists, log passwords, and center GPS location.

Products & Services Overview



Mobile Endpoint Security (MES)

As more organizations embrace the use of smartphones and tablets as a means of enabling mobility amongst their employees, more sensitive data is going mobile beyond the reach of traditional perimeter-based security tools. Lookout Mobile Endpoint Security is powered by data from over 170M mobile devices and 70M apps to grant visibility into the entire spectrum of mobile risk across app, network, and device-based threats, apply policies across the mobile fleet to measurably reduce risk, and integrate into existing security and mobility management solutions to ensure full coverage.

Lookout MES relies on 3 main components:

1. **Lookout for Work app**: The iOS and Android app for corporate-owned and BYO devices that provides connectivity to the Lookout Security Cloud, monitors the device risk surface, and executes policy-defined protective responses.
2. **Lookout Security Cloud**: The Lookout Security Cloud uses correlation and analysis to identify threats on the device. Built on a foundation of mobile threat insights, application data, and malware analysis, it leverages Lookout's industry-leading data corpus to analyze apps and devices on an ongoing basis.
3. **Management Console:** The management console is the central location where administrators can facilitate device enrollment, gain clear visibility into threat data and risky apps in their fleet, set custom remediation and access policies, and configure their MDM integration.

Phishing and Content Protection

Phishing is the primary means for attackers to gain access to your organization's network and corporate data. It is relatively easy to fool an end user into clicking on a link, especially on mobile. Many organizations have already invested in email security protections and spam filters, supplemented by additional perimeter provisions such as firewalls and secure web gateways. However, these measures alone have become inadequate as employees move outside the perimeter and use other apps, both personal and corporate, for data access and communications.

The Lookout artificial intelligence detection engine proactively determines the reputation of sites on the Internet. With an always-on approach, Lookout Phishing AI detects phishing kits as they are being built, before any user is targeted and an attack is executed. We share select findings with the world on Twitter via @PhishingAI.

App Defense SDK

Smartphone apps have become an integral part of everyday life and now represent 60% of all time spent online. While mobile apps bring new conveniences to customers, such as mobile banking, they also introduce new risks. Mobile security threats such as trojans and jailbroken/rooted devices can steal both customer and employee login credentials and leave your entire organization and customer base vulnerable to data compromise. Lookout App Defense SDK helps reduce the risk of fraud and data compromise, comply with standards such as GDPR and PSD2, and protect unaware consumers by identifying issues on their device when using the app itself.

Lookout for Small Business

Lookout for Small Business makes it easy for your customers to secure their mobile devices with predefined protection settings, a simple three click deployment process, and on-device remediation guidance for users. Lookout has visibility into over 170 million mobile devices worldwide. This unparalleled visibility into apps, devices, networks, and OS firmware allows Lookout to continuously adapt its machine learning technologies to detect emerging threats with high fidelity. With Lookout for Small Business, mobile operators can deliver this unrivaled visibility and insight to organizations that lack dedicated IT or security staff, with a simple, actionable mobile security offering

Lookout Personal

Lookout Personal is the only solution that provides mobile security, identity protection and theft prevention in a single app. Tens of millions of individuals who use their phones for everything and are concerned about the security and privacy of their personal information have turned to Lookout for a simple and straightforward way to help protect their devices and their personal data. Get Lookout Personal today for all-in-one mobile security and identity theft protection

Mobile Intelligence Center (MIC)

Lookout's Mobile Intelligence Center enables governments, carriers, and large enterprises to tap into the power of a vast mobile app database through an intuitive, web-based interface. The Mobile Intelligence Center offers access to an invaluable platform, providing data-driven insights that can accelerate app investigations and response times, while protecting mobile infrastructures, organizations, and individuals.

Threat Advisory Services

Lookout Threat Advisory provides cutting-edge mobile threat intelligence from Lookout's global sensor network of millions of mobile devices and insights from Lookout's top mobile security researchers. Customers get access to monthly threat reports and analyst inquiry calls, quarterly webcasts, and also get early access to novel Lookout threat research

Technical Insights

App-based Threat Detection

Lookout MES automatically assesses malicious apps on both iOS and Android devices. Examples of app-based threats include **trojans** that exfiltrate data, **spyware** that monitors device sensors and usage, and **sideloaded apps** that bypass app store review. Lookout classifies these app threats across 19 categories based on their type and the level of potential damage they could cause the device.

How does Lookout detect new threats that get introduced in the wild? Using the massive data corpus, Lookout can assess code similarities between a new app and the 70M+ unique apps already analyzed. This binary similarity technology reveals where that app's code (or its relatives) appears in the world by analyzing approximate similarity between individual code classes and then computes an aggregate similarity score. This scalable detection also enables new threat detection without needing a prior or existing signature by aligning similarities.

Device-based Threat Detection

Like traditional desktop endpoints, iOS and Android devices contain exploitable vulnerabilities in their OS. Taking advantage of a device at this level can lead to a **rooted** or **jailbroken** device, which gives the attacker full control and allows them access to all apps and corporate data stored or accessed on that device.

How does Lookout detect compromised operating systems? Lookout collects device security telemetry to form a digital firmware fingerprint of each device. This includes OS file metadata such as file size and OS configuration data such as build properties. Lookout can then take that fingerprint and assess it against the dataset to identify when a device is vulnerable or has been compromised by a jailbreak or root.

Network-based Threat Detection

Network attacks are executed by getting access to network traffic and decrypting the sensitive information being transferred, despite strong encryption used by many enterprise solutions, such as email. On mobile devices, these attacks aim to get in the middle of data transferred over cellular and Wi-Fi networks. Lookout network protection provides automatic on-device analysis of network connections to defend against man-in-the-middle attacks and ensure information is being securely transmitted in real time.

How does Lookout detect network attacks? Whenever a device connects to a new network, the Lookout app probes reference servers with known certificate properties and a known TLS configuration. This allows us to compare *expected* network configuration properties with the *established* network properties we see. By analyzing whether these established connections meet expected properties, we can determine whether connections are being tampered with by utilizing any of the methods described above.

Phishing and Content Protection

Attackers have discovered that email is the lowest cost method to execute a phishing attack. Many organizations have already invested in solutions that protect desktops within the traditional perimeter from phishing attacks. However, as employees access more corporate data from mobile devices, those traditional tools can't keep up with protecting against phishing attempts from SMS,

messaging platforms, and risk vectors that don't exist on a desktop. It's also much more difficult to spot a phishing link on mobile, as the end user oftentimes can't see the full URL that they're clicking on or visiting.

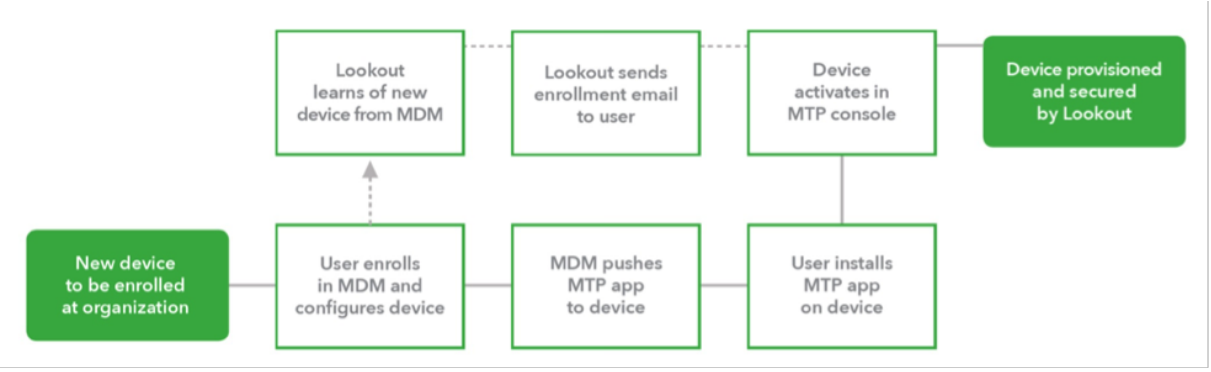
How does Lookout detect phishing attacks? Lookout inspects all outbound connections made by the mobile device and installed apps at the network level at the time a user attempts to connect. With this approach, Lookout it doesn't rely on inspecting message content, and therefore does not violate end user privacy. Lookout correlates the URL being accessed against malicious URLs identified by the Lookout Security Cloud and alerts the end user if it is malicious prior to the connection being completed. This real-time alert prevents exposure to risky content such as malicious apps or websites with known vulnerabilities.

MDM Integration

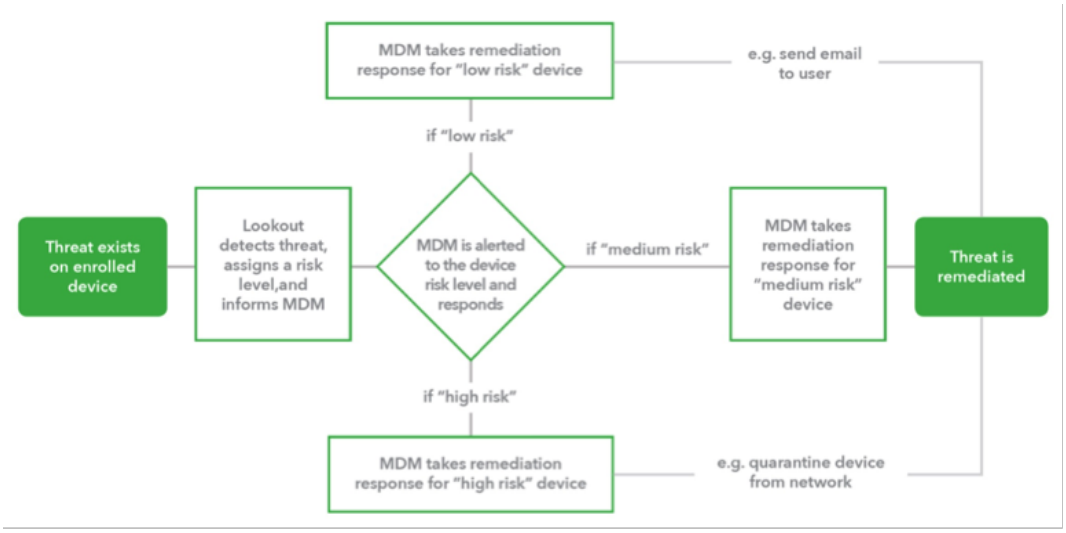
Lookout integrates with many leading MDM platforms, allowing organizations to enhance their existing tools and benefit from highly efficient security workflows. This integration allows administrators to deploy Lookout across their entire fleet and gain real-time visibility into all devices and their security state. Supported MDM platforms include:

Intune, airwatch by vmware, IBM MaaS360, MobileIron, BlackBerry UEM

The integration simplifies **device provisioning**, as well. The MDM can be used to easily distribute the Lookout app to your mobile devices, allowing for rapid and scalable device provisioning. The device provisioning process follows these basic flows:



To help with **threat remediation**, the MDM can leverage Lookout to quarantine risky devices in real-time by using custom remediation policies. When Lookout detects a threat on a device, it is categorized as high, medium, or low risk. With that information the administrator can set up policies that quarantine the device from accessing corporate apps, corporate data, or just wipe the device completely.



Mobile Risk API

Lookout MES supports a RESTful API endpoint for mobile device threat events. The API is used to support **Lookout's SIEM and syslog connector** application and can also be used to create connectivity with other web services. The Mobile Risk API includes a rich set of information and metadata pertaining to threat encounters on a Lookout-protected device. Data includes, but is not limited to, threat type (with associated metadata for that type), threat name, threat classification, threat risk level, device identification, User identification, timestamp, and threat state (*encountered*, *resolved, ignored*).

Enterprise App Analysis

Lookout Mobile Endpoint Security for App Risk allows you to verify that your in-house apps are built according to security best practices, do not include any malicious code and are compliant with data policies in place. With Enterprise App Analysis, you'll be able to get visibility on you own apps, directly from the Lookout Console, without the need to use a separate solution or option. You can upload your IPA or APK files directly and the analysis report will be generated and available in the App Risk section for review.

Self-Remediation for End Users

Lookout Mobile Endpoint Security has an extremely low false positive rate and avoids generic threat categorizations. As such, if a threat is encountered, the user is presented with a clear description and instructions on how to remediate. In our experience, users will self-remediate 95% of the time without involving IT. In addition, administrators will have the ability to enforce restriction via MDM while a threat remains active.

Industry Recognition

Lookout is the highest-rated mobile threat defense solution by customers in Gartner Peer Insights

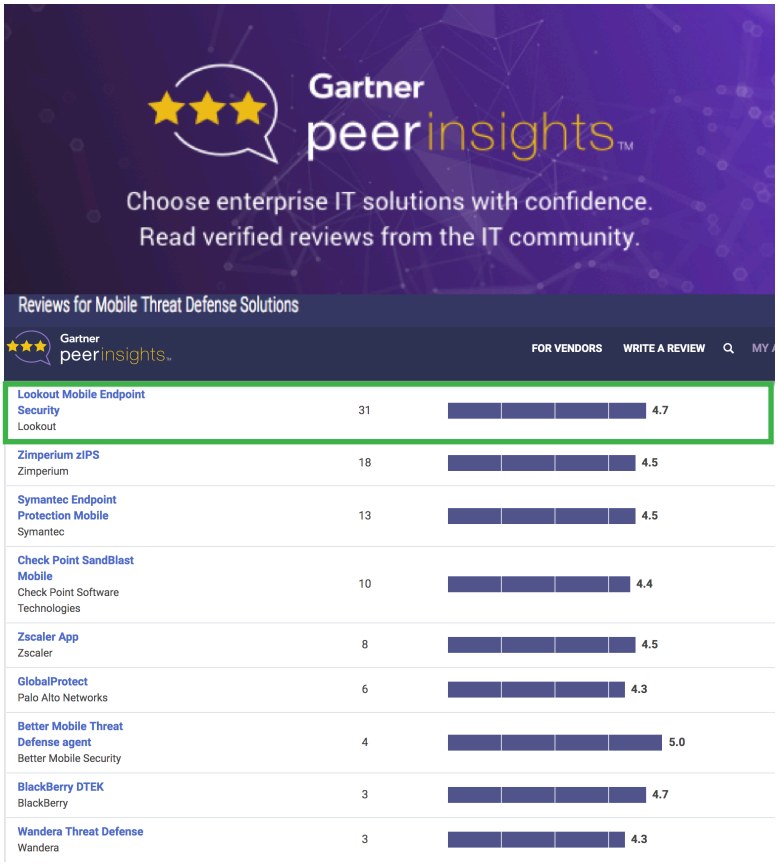
Gartner Peer Insights Reviews for Mobile Threat Defense Solutions

"The Mobile Risk API…can trigger "A leader in its field. The application was very easy to deploy and in the short time it was implemented it already paid for itself by alerting us of potential cyber security risks which might have otherwise gone undetected. From users' perspective it works silently in the background with no interference and very low battery usage."
Senior Program Manager, Digital, in the Government Industry $1B-3B

"This was one of the easiest deployments I have ever done. Further, their integration with [Microsoft's] O365 security stack complements perfectly and aligns with some of our other cybersecurity enhancements."
Chief Information Security Officer in the Services Industry, Security & Risk Management, <50M

"Lookout was easy to implement & integrate with our Airwatch solution. Lookout has a friendly user interface and admin portal. Installation to our end users via Airwatch was very straight forward and we encountered no major issues. Users really like the Lookout VPN feature that protects them while browsing."
Server Architecture Supervisor, Manufacturing, $500M-1B

"Lookout has provided excellent support and answered all possible questions almost immediately. The product is simple and efficient, requiring little effort on our part to maintain it. The client app remains mostly invisible to the user unless action is required. The user experience is above most other mobility apps, as even the less tech-savvy users don't often require help with it. "
Systems Analyst in the Finance Industry $1B-3B



"Best tool which covers all the security issues addressed for the mobile devices.. overall experience is good. The best part is protection against Phishing, content filtering, and VPN"
Lead mobile and devices in the Manufacturing Industry, Infrastructure & Operations, $10B-30B

Lookout is the Leader in the IDC MarketScape for Mobile Threat Management

IDC MarketScape Worldwide Mobile Threat Management Software

Continuous Conditional Access *"The Mobile Risk API…can trigger actions from partner EMM platforms, identity access providers, and other infrastructure such as Network Access Control (NAC) and secure web gateways (SWGs). These scenarios can involve detection of risks that are beyond the reach of perimeter-based security tools"*[1]

Breadth of coverage: *"In addition to discovering over a thousand malicious apps on public app stores, and thousands per day from other sources, Lookout researchers and AI have discovered vulnerabilities in watchOS, tvOS, MacOS, Safari/Mobile Safari, WebKit, Google Glass, and Bluetooth stacks."*[1]

Global partnerships and integrations: *"Lookout has very strong go-to-market partnership with over 15 carriers…it also integrates with more than a dozen SIEM and EMM products, which are increasingly critical enterprise platforms for mobile security and enablement"*[1]

Source: IDC, 2018

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.
Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs.
Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years.

IDC's Summary of Lookout MTM:

"Lookout also uses artificial intelligence tools to analyze data in its cloud, allowing it to analyze and detect new and unknown threat such as malware/malicious app variants, phishing attacks, and other sophisticated network-based attacks. All of these techniques combine for a strong mix of on-device/cloud-enabled MTM functions that can cover most mobile threat scenarios around app, device, and network-level attacks"[1]

1 IDC MarketScape: Worldwide Mobile Threat Management Software 2018–2019 Vendor Assessment" Doc #US45521018, December 2018

Lookout

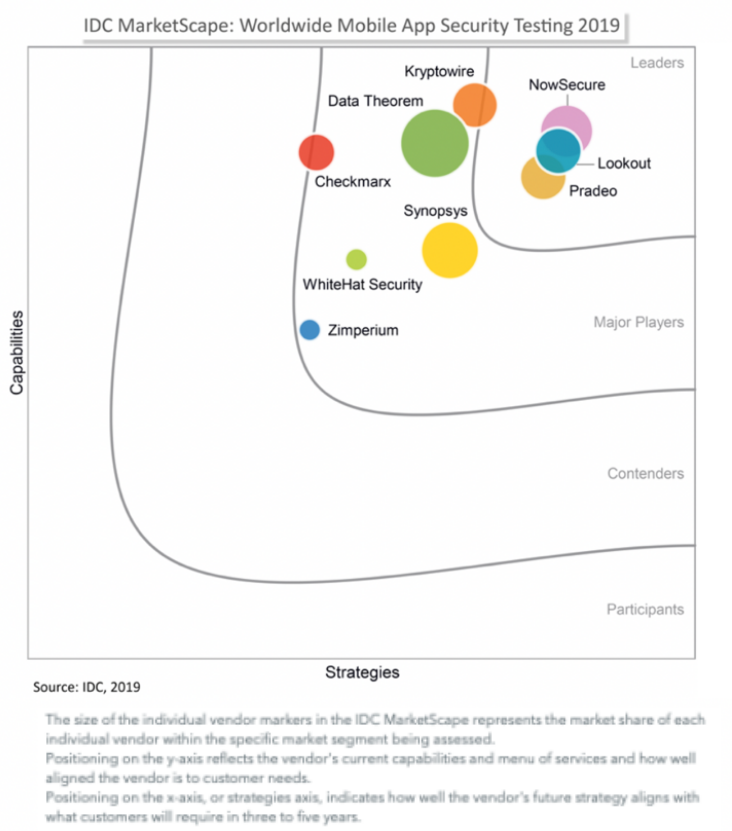
Lookout is a top Leader in the IDC MarketScape for Mobile App Security Testing (MAST)

IDC MarketScape Worldwide Mobile App Security Testing

The massive dataset feeding/informing our AI engine: *"Lookout's use of telemetry to inform the AI engine of ongoing mobile security risks brings a unique level of app risk knowledge to the company's MAST and other Mobile Endpoint Security Capabilities"*[2]

Partnerships: *"Lookout's distribution partnerships with many of the world's largest mobile network operators...contribute(s) to the vendor's growing base of Android and iOS mobile devices and app security knowledge"*[2]

MDM integration: *"Lookout's console and administrative functionality complements the vendor's MDM integrations, making it possible for Android-using organizations with and without EMM software and iOS-using organizations with MDM software to implement mitigations to mobile app security risks"*[2]



IDC Recommends Organizations Consider Lookout for MAST When:

"Organizations should consider Lookout when they are looking for a MAST vendor that brings an extensive knowledge set and AI to identifying security risks of mobile apps in use in the employee base…Organizations that also plan to deploy Mobile Threat Management tools should consider Lookout as a single integrated offering providing threat detection capabilities and application security testing"[2]

2 IDC, Inc. "IDC MarketScape: Worldwide Mobile App Security Testing 2019 Vendor Assessment – InfoSec Emphasis", Doc #US45459219, September 2019

Lookout

Privacy

Lookout firmly believes that your privacy is as important as your security, so we are completely transparent about the data we collect to safeguard your devices and the security of your employee. The Lookout Privacy Policy can be found here: https://www.lookout.com/legal/privacy-policy/mobile-endpoint-security-privacy-statement

Data Collection

In order to secure mobile devices, Lookout Mobile Endpoint Security collects and analyzes certain data to identify and mitigate risk.

Lookout Mobile Endpoint Security collects 4 classes of data from enrolled devices:

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

Lookout does not collect any personal information or data generated by employees using apps, such as images, audio, video or text content.

Data Collection

Lookout secures device data collected in transit and at rest using:

- Data in transit
  - Transport Layer Security (TLS) with Forward Secrecy (FS)
  - Certificate Pinning
- Data at Rest (PII only)
  - Authenticated encryption using AES-256 with HMAC-SHA256
  - Searchable device data forward hashed with SHA-256

GDPR

Lookout is committed to helping our customers meet the data handling requirements mandated by the General Data Protection Regulation in 2018. To demonstrate our commitment and compliance to privacy protection, Lookout is ISO27018 certified as of December 2017.

Privacy Controls

Customers can choose to limit the personal data that Lookout Mobile Endpoint Security collects from end users in order to comply with their organization's security policies.