Lookout

MOBILE VULNERABILITY & PATCH MANAGEMENT

REDUCE RISK BY PATCHING MOBILE VULNERABILITIES

Hope is not a vulnerability patch strategy

With tablets and smartphones now being used in nearly every business process, there is too much inherent risk in hoping that employees will keep their operating system and apps up to date. This was less of a risk when these devices were only being used to read email, but now that they have the same access to data as every laptop and desktop.

Mobile devices are the key to productivity, so cybercriminals have been increasingly exploiting mobile vulnerabilities on outdated apps and OS versions to initiate their attack. Amplifying this risk, a single out-of-date app can expose the entire device to exploitation. Patching mobile vulnerabilities has become a priority.

The Financial Times reported on a WhatsApp vulnerability that was able to deliver spyware onto iOS and Android devices without any user interaction at all. Just by receiving and not answering a WhatsApp VoIP call from an attacker, your device could become compromised.[1]

BENEFITS

- Gain visibility into all mobile operating system versions
- Access the most comprehensive mobile vulnerability database
- Obtain insights into Common Vulnerabilities and Exposures (CVE) in unpatched apps
- Enforce patch management policies through data access limitations
- Manage risk exposure with custom remediation policies

1. Srivastava, Mehul, Financial Times, 'WhatsApp voice calls used to inject Israeli spyware on phones', May 13, 2019

APP VULNERABILITY KILL CHAIN

INFILTRATE

- Phishing
- Incoming message
- Incoming call

GAIN ACCESS

- Exploit app vulnerability
- Execute malicious code

ELEVATE PRIVILEGE

- Exploit additional vulnerabilities
- Install payload

PERFORM ESPIONAGE

- Exfiltrate personal data
- Steal corporate credentials

Patching requires the right combination of OS and apps versions

Traditional vulnerability and patch management focuses on servers, rather than endpoints. This is because desktops and laptops are managed, use a common image and are regularly patched. Therefore, the primary vulnerability risk has been the unpatched server.

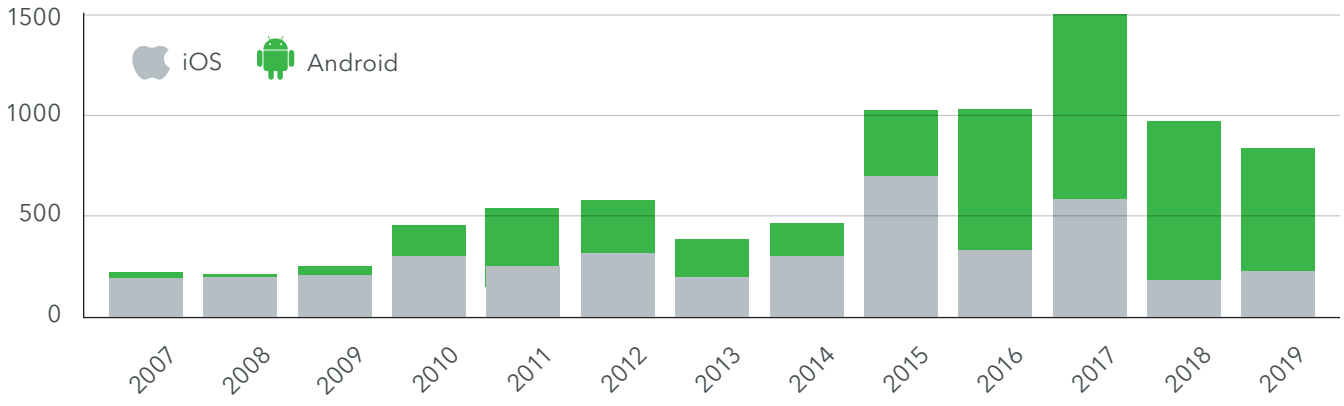
Today, it is only possible to ensure managed mobile devices run a minimum version of the operating system with mobile device management (MDM). But as organizations increasingly introduce Bring Your Own Device (BYOD) for work, MDM cannot provide complete coverage. Traditional vulnerability management can't fill this gap since it relies on devices attaching to the office network rather than home Wi-Fi or cellular networks.

Vulnerabilities across your mobile fleet continue to increase

OS vulnerabilities continue to increase across iOS and Android. The pace at which cybercriminals develop exploits is keeping pace with security enhancements. This is the same game of leap frog that exists on desktop operating systems.

The chart below maps the vulnerabilities across iOS and Android over the past two decades.

NUMBER OF iOS AND ANDROID VULNERABILITIES BY YEAR

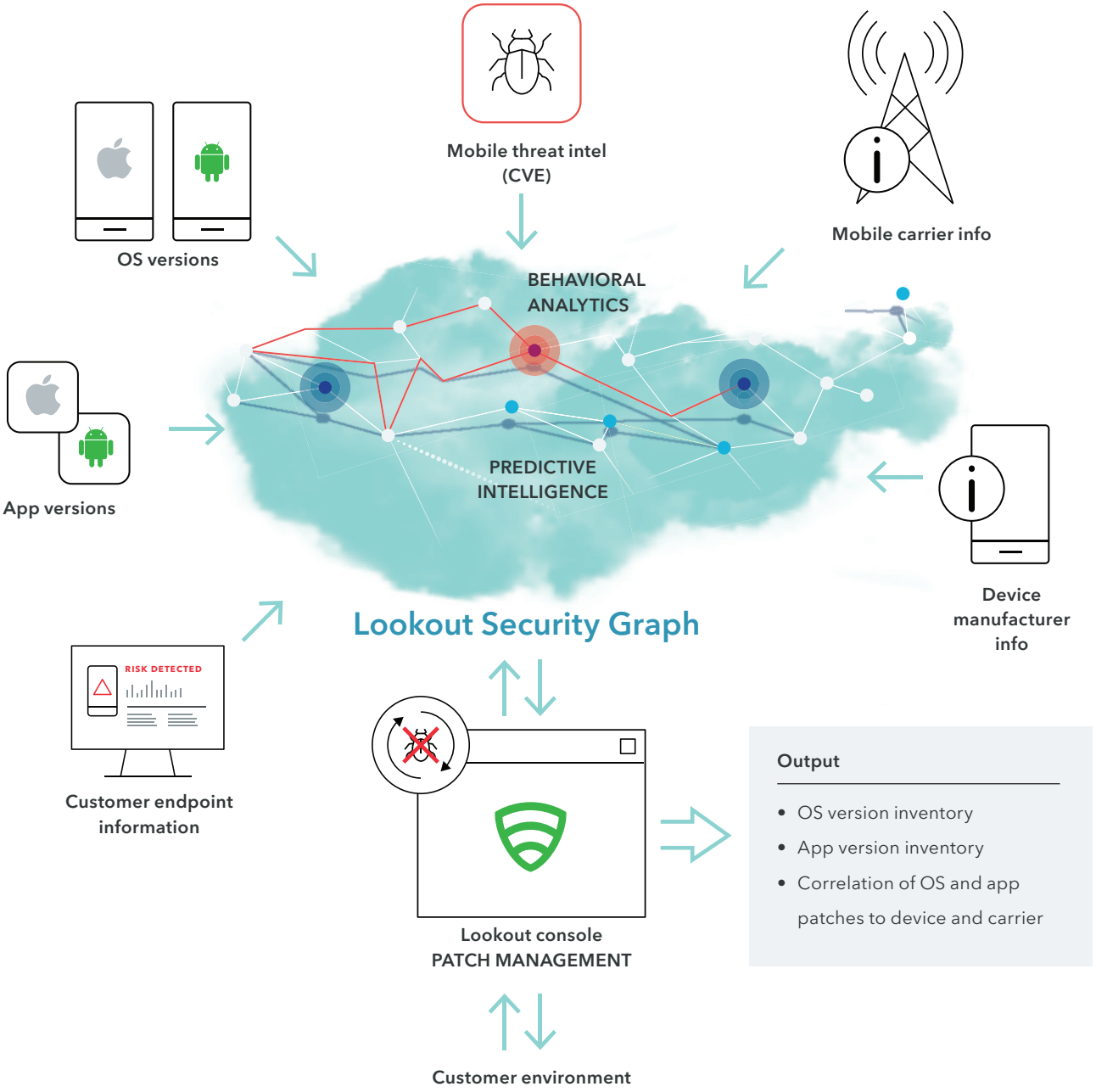


Patch with confidence using curated vulnerability data

Lookout Mobile Vulnerability and Patch Management enables you to know every version of an operating system and mobile app in your organization. We provide visibility into device risk independent of whether it is company- or employee-owned, as well as managed or unmanaged.

Lookout crowdsources the most comprehensive vulnerability and patch management database from analysis of nearly 200 million mobile devices and over 120 million apps. It correlates the app and operating system versions needed to patch vulnerabilities. In addition, the database specifies the version of operating system that is specific to a carrier and device manufacturer for the patch.

To prevent vulnerabilities on mobile apps, operating systems and devices from putting your data at risk, Lookout restricts access to corporate infrastructure until the device is patched. In addition, we send remediation instructions to the user so they can regain access once they eliminate the risk.



Just by having a different device manufacturer and mobile carrier, a security patch can be delayed by months. In the example below, Lookout indicates the release of a security patch for LG Pixel 2 on the Orange network being released after the patch for a similar LG device on the Verizon network.

This variability across your mobile fleet means it is not possible to apply a blanket policy to specify a minimum patch level. A policy that fully covers devices in your mobile fleet would need to evaluate each device individually to apply the available updates that are compatible with the firmware of the device.

The vulnerability risk due to the variability in OS and security updates is even more pronounced for unmanaged personal devices that are used for work. Employees do not always apply OS updates and security patches right away. This creates a vulnerability window that can be exploited by an app threat such as the What'sApp vulnerability (CVE-2019-3568). Fortunately, Lookout detects app vulnerabilities such as the "WhatsApp" example and automatically alerts the end user to remediate the threat.

Current device information				Latest available		Update action		
Make, model & carrier	OS Version	Security Patch	WhatsApp Version	OS Version	Security Patch	OS Version	Security Patch	WhatsApp
LG Pixel 2 (Verizon)	Android 8.1.0	2018-07-05	2.18.30.6	Android 10.0.0	2019-10-06	Update	Update	Update
LG Pixel 2 (Orange)	Android 8.1.0	2019-02-05	2.17.70	Android 10.0.0	2019-02-05	Update	Not available	Update

About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust.

For more information visit **lookout.com**

Request a demo at **lookout.com/request-a-demo**

A platform built for mobile from the ground up

Explore the Lookout Platform at **lookout.com/platform**

Lookout®