



LOOKOUT MODERN ENDPOINT PROTECTION

SECURITY THAT GOES EVERYWHERE YOU GO

Traditional endpoint protection does not protect all of your endpoints, leaving you blind to security threats targeting iOS, Android, and Chrome OS. These devices have access to the same cloud data as desktops and laptops, but need modern endpoint protection to reduce risks from the latest cybersecurity threats.

Protecting modern endpoints requires a different approach that does not require heavy agents dependent on kernel access. Agents will cause the device to perform slowly and drain the battery quickly. Modern endpoint protection must detect threats in apps, the device and network connections. It must protect the user, the device and the organization while respecting user privacy. It must work equally well for employee-owned and company-owned devices.

Organizations are embracing the use of smartphones and tablets to increase productivity inside and outside the workplace. As a result, more than half of the devices used to access your organization's data run iOS, Android and Chrome OS. The problem is only a fraction of these devices have endpoint security, creating a significant gap in your security architecture.

Mobile devices are a primary target for cyberattackers because they have a treasure trove of data. Threat actors

BENEFITS

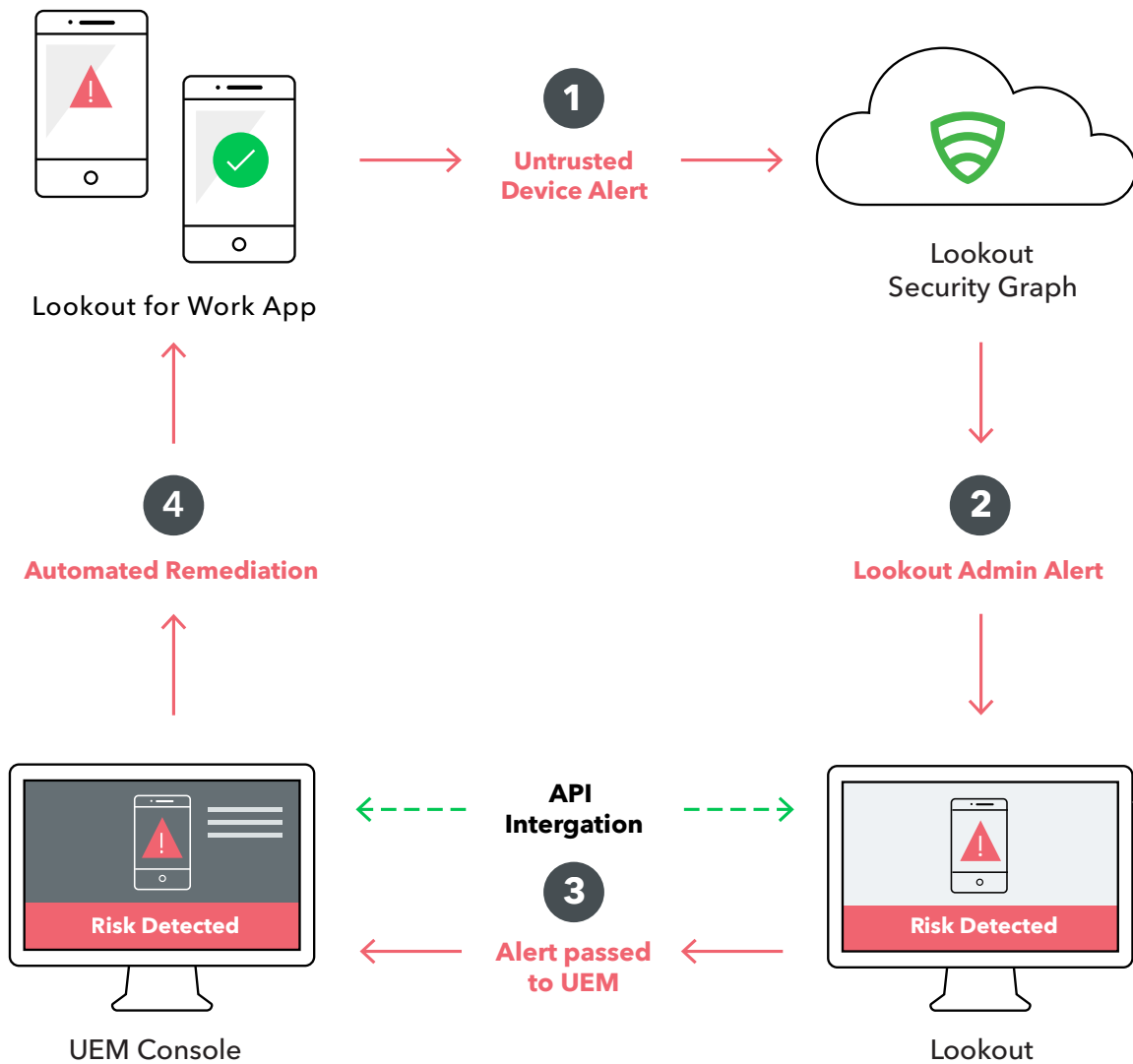
- Continuous monitoring of mobile devices for risks
- Close security gaps by gaining visibility into all iOS, Android, and ChromeOS devices
- Enable secure BYOD to increase employee productivity
- Real-time visibility into incidents enabling self remediation
- Protect organizational and employee data with built-in privacy controls
- Integrate with SIEMs, including Splunk, Windows Defender ATP, Micro Focus, ArcSight, IBM Security and QRadar
- Support for any UEM including VMware Workspace ONE® UEM, Microsoft Intune, BlackBerry® UEM, IBM MaaS360®, and MobileIron

hope to gain access into your organization's infrastructure by introducing mobile malware such as spyware and banking trojans that undermine the native security of the mobile device.

Lookout Modern Endpoint Protection

Lookout® Modern Endpoint Protection is a cloud-delivered module on the Lookout Security Platform. It leverages a lightweight endpoint app on each employee's device and is managed through a cloud-based admin console.

The console delivers real-time visibility into mobile risk and customizable reporting. The console simplifies enrollment and enforcement policies through integration with Unified Endpoint Management (UEM) solutions.



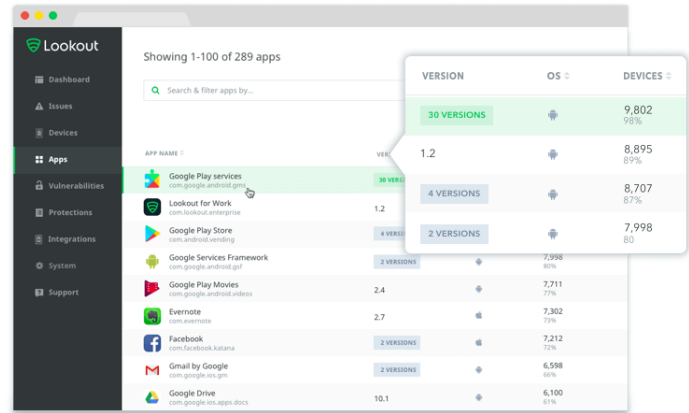
Protection against the latest mobile threats

As more sensitive data is accessed by mobile devices, they are increasingly becoming a primary target for threat actors. Lookout Modern Endpoint Security identifies mobile threats targeting three attack vectors: app threats, device threats, and network threats.

Protection from app-based risks

Apps are the predominant way that sensitive data is accessed on mobile devices, with risks spanning across both iOS and Android. The Lookout app analysis technology is powered by intelligence from over 120 million iOS and Android apps, giving you visibility into app-based risks such as:

- Trojans and spyware that can exfiltrate data from the device
- Vulnerabilities in app data transfer and storage
- Risky app behaviors that pose a compliance risk
- Sideloaded apps that bypass official app stores

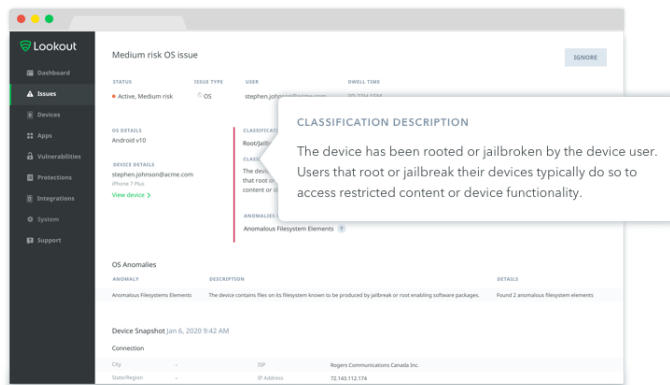


APP NAME	VERSION	OS	DEVICES
Google Play services	30 VERSIONS		9,802 (98%)
Lookout for Work	1.2		8,895 (87%)
Google Play Store	4 VERSIONS		8,707 (80)
Google Services Framework	2 VERSIONS		7,998 (80%)
Google Play Movies	2.4		7,711 (77%)
Evernote	2.7		7,302 (70%)
Facebook	2 VERSIONS		7,212 (70%)
Gmail by Google	2 VERSIONS		6,598 (66%)
Google Drive	10.1		6,100 (61%)

Protection from device-based risks

If the device is compromised with software vulnerabilities, the built-in security of the operating system can be bypassed. Lookout creates a fingerprint of each mobile device and compares it against nearly 200 million devices in our security platform to identify anomalies and risks, such as:

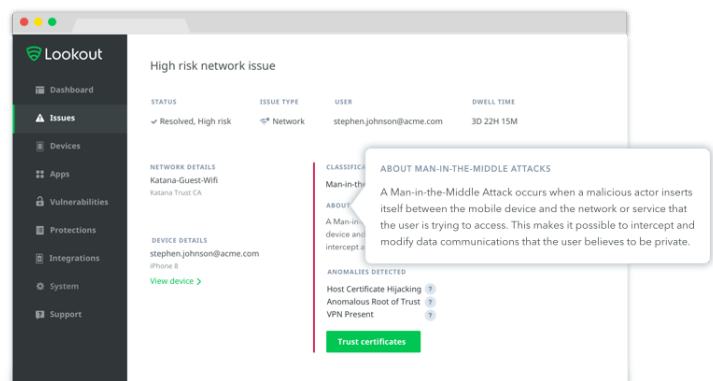
- Behavioral anomalies
- Advanced root or jailbreak
- Out-of-date operating systems
- Device configuration risks



Protection from network-based risks

Often taking the form of a man-in-the-middle attack, these network threats are typically executed by spoofing a Wi-Fi hotspot to intercept network traffic and decrypt sensitive data. By analyzing network connections from our global sensor network, we effectively mitigate false positives while detecting high impact threats, including:

- Man-in-the-middle attacks
- Host certificate hijacking
- SSLStrip attacks
- TLS protocol downgrades



Delivering Mobile Zero Trust with Continuous Conditional Access

Access to corporate data should be granted based on an assumption of zero trust and the continuous monitoring of an endpoint's risk level. Lookout Continuous Conditional Access works behind the scenes, dynamically assessing the risk level of the endpoint while the user is connected to the enterprise. Lookout permits only devices that have an acceptable risk level to connect to enterprise infrastructure and data, for both managed and unmanaged deployments.

Lookout Continuous Conditional Access blocks access to corporate data when detecting:

- Lack of compliance with customizable policies set by Lookout administrator
- Apps, device, and network threats identified as risky by Lookout Security Graph
- Industry-specific threats from apps accessing and sharing regulated content

Machine learning that powers modern protection

Detecting and analyzing the latest threats across 200 million devices is beyond human capabilities. Instead the Lookout global sensor network feeds machine learning engines that deliver continuously updated endpoint security delivered from the cloud to the app on your device. This enables our platform to be predictive by using machine intelligence to identify complex patterns of mobile risk.

Lookout has analyzed more than 120 million apps, driven by the daily analysis of more than 100 thousand apps. We have visibility into nearly every version of every mobile app in existence. Our machine learning engines auto convict up to 10,000 malicious apps every day.

We protect your smartphones, tablets and Chromebooks because they are at the intersection of the personal you and the professional you. Our mission is to secure and empower the digital future in a privacy-focused world where these devices are essential for work and play.

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

© 2020 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT®, and PROTECTED BY LOOKOUT®, are registered trademarks of Lookout, Inc. in the United States; and POST PERIMETER SECURITY ALLIANCE™ is a trademark of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders. 20201013-Lookout-USv1.0