Lookout Mobile Intelligence APIs

Gain visibility into your mobile security blind spot

Mobile devices have evolved into the cornerstone of employee productivity, communication and identity. However, they remain a blind spot for security teams and are a natural target for any threat actor aiming to compromise an organization.

Key Challenges

Challenge: Traditional EDR is limited on Mobile
Security teams have understandably turned to next-gen SIEM and XDR solutions to see everything in one place. However, these tools grant little to no visibility into mobile devices. Security teams cannot analyze their exposure, understand what data is at risk, or detect how attackers could exploit employee mobile devices.

How Lookout helps: Lookout Mobile Intelligence APIs bring utility to the critical security data that exists in the mobile ecosystem by moving it from the peripheral edge of the network into the same views and solutions that security teams are already using. This enables the identification of coordinated attacks across platforms, trends, and potential risks.

Challenge: Mobile is in the Crosshairs
Threat actors have identified the mobile edge as a weak point due to those devices historically being dismissed by security teams.

How Lookout helps: To protect against this imminent threat on the devices their employees use the most, Lookout Mobile Intelligence APIs inform security teams of what's going on with their mobile fleet to protect against account compromise due to social engineering, data leaks due to vulnerable apps, and device takeovers due to out of date operating systems.

Challenge: Streamlining Web Security
Organizations struggle to manage web security across multiple devices while ensuring consistent protection and integrating with traditional tools. Without a streamlined approach, gaps in threat intelligence and policy alignment can lead to missed threats, inconsistent protection, and operational inefficiencies.

How Lookout helps: Lookout Mobile Intelligence APIs enable administrators and security analysts to integrate third-party threat intelligence feeds, allowing them to extend their existing web content deny lists to mobile. Alignment ensures consistent protection across devices and helps prevent threats before they materialize. This reduces the management burden on administrators while allowing them to adjust content availability in line with business needs.

Why Lookout

Mobile environments are significantly different from conventional endpoint environments and, therefore, must be protected by a purpose-built solution for their unique aspects and challenges. As part of Lookout Mobile Endpoint Security (MES), the Mobile Intelligence APIs deliver invaluable data about an organization's mobile infrastructure — providing detailed streaming of security events, device and user audits, and threats as they occur.

Security teams can now review the state of their mobile fleet in the same views as their other endpoints — unifying their organization's entire risk and security management strategy to create uniformity across all devices, users, and networks. Now, they will be able to get previously unseen context around how mobile plays a key part in risk management, incident response, and threat detection.

To see how it works, contact us for a demo.

© 2024 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design® and the Lookout multi-color/multi-shaded Wingspan Design® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, and the 4 Bar Shield Design.