Lookout For CrowdStrike: Multi-layered Endpoint Security

Combine the power of Lookout and CrowdStrike to strengthen your endpoint security

Challenges

In today's world, mobile has become a primary target for cyber criminals. The reason is simple: We all use these devices and that makes them vulnerable, high-reward entry points into organizations.

Even with the high stakes, many organizations still use legacy endpoint detection and response (EDR) point products that have minimal visibility into mobile-related risks. Without EDR for mobile devices, they're left exposed to phishing, spyware, ransomware, operating system vulnerabilities, and zero-day attacks.

Solution

Lookout layered on CrowdStrike provides comprehensive real-time protection against mobile threats across iOS, Android, and ChromeOS devices. With this protection, security teams are empowered to stop phishing attacks and protect against malicious applications, device exploits, and man-in-the-middle attacks, all while keeping users informed about the threats their devices have encountered and the actions they can take to stay safe.

Lookout for CrowdStrike makes it easy to detect and remediate mobile threats. The Lookout Mobile Endpoint Security lightweight mobile app and admin console are connected to Lookout telemetry security graph, which features data collected from more than 220 million devices and 300 million mobile apps. Powered by artificial intelligence, the security graph enables robust protection against the most-sophisticated mobile threats. Lookout's algorithms search the internet, including the dark web, for sites purpose-built for phishing and malicious apps that execute malicious code. Whether you download apps with new malware or you're the target of the latest ransomware or phishing scam, Lookout layered with the CrowdStrike Falcon platform protects you automatically.

Key Benefits

- Proactively detect and respond to mobile threats across both managed and unmanaged devices.
- Reduce risk of credential theft and social engineering with phishing protection across SMS, messaging apps, and email.
- Comply with regulations that ban the use of specific mobile apps based on their behavior.
- Ensure threat intelligence teams see the full picture by extending access to Lookout mobile threat intel.

Use Case / Challenge	Solution	Benefits
Prevent credential theft from mobile use	Protection from phishing and malicious content in emails, SMS, and web apps	Employees can safely browse the internet and communicate via email, SMS, and messaging apps
Reduce risk of ransomware entering through mobile device exploits	Protection from threats like mobile malware and zero-day attacks	Organizations are less likely to experience a ransomware attack or data breach
Reduce the risk of malicious and non-compliant apps	Risk analysis based on app reputation, permissions, and capabilities	Your team can see all apps currently in use and set policies to prevent access to data if a risk is present
Easily deploy mobile security to employees	Deployment of the Lookout app at scale without user interaction	You save time and deployment resources while ensuring uniform protection across entire employee base
Hunt and analyze threats originating from mobile devices	Use of Lookout admin console to set policies and analyze mobile threat data	You can conduct comprehensive investigations by including mobile exploits as part of the forensics process

Mobile is now an indispensable attack vector adopted by Advanced Persistent Threat (APT) groups[1] and a primary entry point into an organization. Whether it is via surveillanceware, an SMS phishing attack, or a device-level exploit, mobile threats present a blind spot for most organizations.

Unlike traditional endpoints, mobile devices do not allow access to the underlying system kernel, which gives them an inherent level of protection. However, cybercriminals have altered their tactics to exploit these devices, most often seeking to steal user credentials for use in broader attacks.

You can use the Lookout console to tap directly into a large database of mobile threat intelligence. This gives you deeper insight into each step of the mobile kill chain. Use it to get details on everything from phishing attacks, IOCs, and app behaviors to web services in use and the relationships between apps and app families. For example, the app vetting functionality shows you the permissions and capabilities of apps that have poor reputations and those that seem to have clean bills of health.

By offering insight into the underlying app composition it allows you to assess the threat risk of each app and enforce appropriate security policies. This not only greatly reduces the risk introduced by mobile apps but also helps your organization meet compliance requirements.

The console also shows you all of the OS versions and security patch levels of devices accessing your network. This ensures only updated devices, which are free of vulnerabilities, can access your data.

By continuously monitoring for threats targeting mobile devices, Lookout provides the visibility you need to protect this highly distributed endpoint ecosystem, which often remains in the dark when using legacy solutions.

[1] Automatically Attributing Mobile Threat Actors by Vectorized ATT&CK Matrix and Paired Indicator

> "Lookout gave us the visibility we needed to better understand the security actions we had to take: when to communicate and when to quarantine or deactivate. It's been a very effective solution in the mobile security landscape."
>
> – Alan Zaccardelle, Cybersecurity Officer at Airbus

Technical Solution

Lookout for CrowdStrike consists of a lightweight mobile app on the endpoint, an administrator console, and the security graph. The mobile app continuously monitors the mobile device for threats and communicates directly with the Lookout security graph for real-time threat information. When a threat is detected, the end user is notified within the app and provided guidance on how to resolve the threat.

For example, if a malicious app is detected on a device, the end user is guided to delete the app. Threat detections are also sent to the admin console and appropriately escalated for resolution if advanced remediation is required. Meanwhile, to protect user privacy, no user information is logged and shared with the administrator.

With the combined power of Lookout and the Falcon platform, you get multi-layered endpoint security to strengthen your organization's security posture and defend against modern threats.

Key Capabilities of Lookout

Stop phishing attacks.

Improve visibility of your attack surface and leverage automated response actions to proactively detect and block phishing attacks.

Reduce compliance risk.

Set policies that look at the permissions and capabilities of the mobile apps your employees use to ensure compliance with both internal corporate mandates as well as industry regulations such as GDPR, HIPAA, and GLBA.

Manage vulnerabilities.

Ensure your mobile devices are running the latest operating systems and security software to reduce exploitable OS vulnerabilities.

Enhance your threat intel.

Incorporate mobile threat intelligence from Lookout into threat hunting and forensic investigations to ensure you have the full picture into the evolving threat landscape and modern kill chain.

Buy Lookout on the CrowdStrike Marketplace →

About Lookout

Lookout, Inc. is the data-centric cloud security company that uses a defense in-depth strategy to address the different stages of a cybersecurity attack. Data is at the core of every organization, and our approach to cybersecurity is designed to protect that data in the modern threat landscape. With a focus on people and their behavior, the Lookout Cloud Security Platform ensures real-time threat visibility, and quickly halts breaches from initial phishing attempts to data extraction. To learn more, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and X.

For more information visit
lookout.com

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

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/
Follow us: Blog | X | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

© 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.

© 2024 CrowdStrike, Inc. All rights reserved.