Lookout

Lookout For CrowdStrike: EDR For Mobile Devices

Maximize EDR for mobile and unleash the potential of your hybrid workforce

Challenges

Mobile is increasingly becoming the primary attack vector for cybercriminals. It provides a silent, highly distributed entry point into organizations. The challenge for most organizations is their existing endpoint detection and response solutions cannot protect against the full spectrum of risks related to mobile devices. Without EDR for mobile devices, organizations are exposed to mobile cyberthreats such as phishing, spyware, ransomware, operating system vulnerabilities, and zero-day attacks.

Solution

Lookout for CrowdStrike provides comprehensive real-time protection against mobile threats across iOS, Android, and Chrome OS devices. We stop phishing attacks, protect against malicious apps, device exploits, and man in the middle attacks. We do this while keeping users informed about the threats they have encountered and actions they can take to stay safe.

We detect and remediate mobile threats with a lightweight mobile app and admin console that are connected to our telemetry security graph made up of data collected from over 200 million devices and 175 million mobile apps. Powered by artificial intelligence, the security graph enables robust protection against the most sophisticated mobile threats. Our algorithms search the internet and the dark web daily to find sites purpose-built for phishing and malicious apps designed to execute malicious code. Whether you download apps with new malware or are the target of the latest ransomware or phishing scam, you are protected automatically.

CROWDSTRIKE

Key Benefits

- Extended attack surface visibility to proactively detect and respond to mobile threats.
- Reduced risk of credential theft and ransomware with phishing protection across SMS, messaging apps, and email.
- Compliance with regulations that ban the use of specific mobile apps based on their behavior.

Use Case/Challenge	Solution	Benefits
Prevent credential theft from mobile use	Protection from phishing and malicious content in emails, SMS, 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 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	App risk analysis based on reputation, permission and capabilities of apps in use	See all apps in use across your fleet and set policies to prevent access to company data if an app risk is present
Easily deploy mobile security to employees	Scale deployment of the Lookout app without user interaction	Save time and deployment resources while ensuring uniform protection across your entire employee base
Hunt and analyze threats originating from mobile	Use admin console to set policies and analyze mobile threat data	Conduct comprehensive investigation by including mobile exploits as part of the forensics process

Security is different on mobile devices. Unlike traditional endpoints, mobile devices do not allow access to the underlying system kernel, which gives them an inherent level of protection. Cybercriminals have evolved their tactics to exploit these devices as a primary entry way into an organization. Whether it is surveillanceware, an SMS phishing attack, or a device-level exploit, mobile threats present a blindspot for most organizations.

Administrators can use the Lookout console to tap directly into the industry's largest database of mobile threat intelligence. By querying the database, they can gain deeper insight into each step of the mobile kill chain. Information such as source details on phishing attacks, IOCs, app behaviors, web services in use, and relationships between various apps and app families is available. This depth of information provides a holistic view of a mobile security incident.

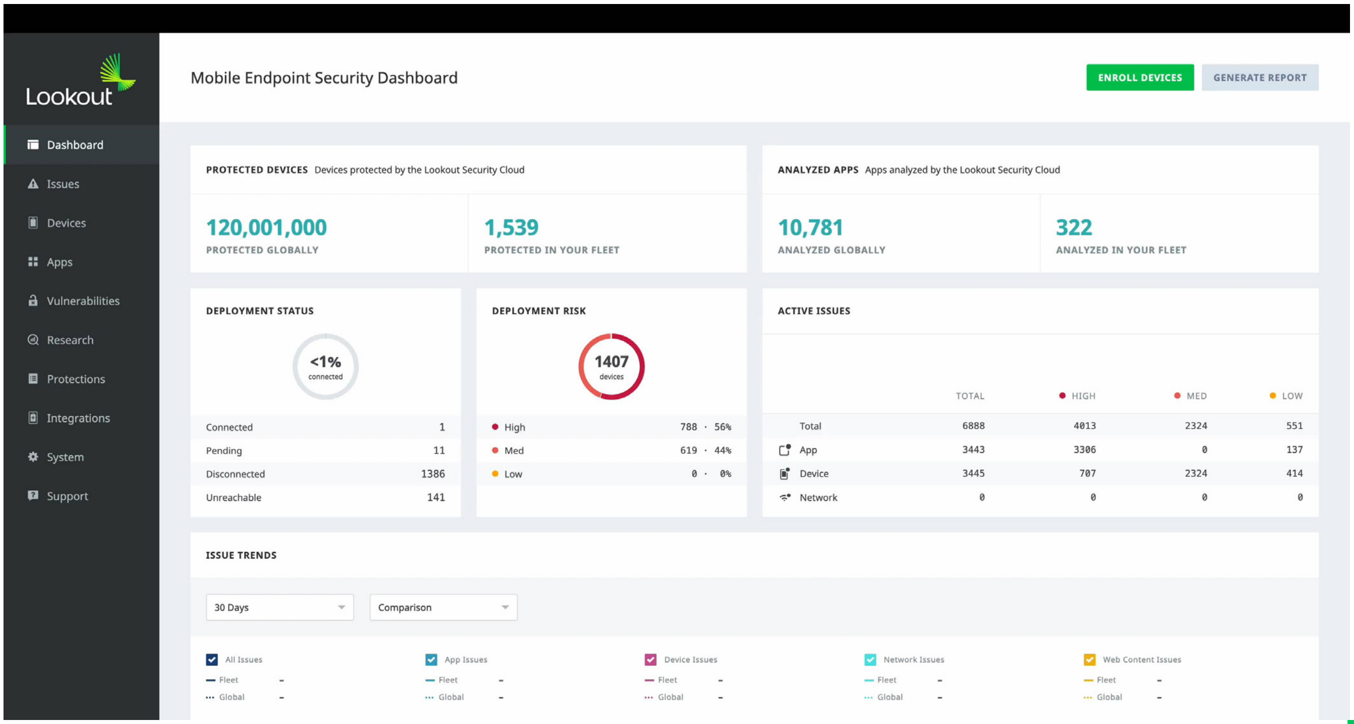
For example, our app vetting functionality looks at the permissions and capabilities of apps with known poor reputations as well as apps that may seem to have a clean bill of health. It is only by understanding the underlying app composition that the true risk of that app can be assessed and meaningful security policies enforced. This not only greatly reduces the risk introduced by mobile apps but also helps organizations meet compliance requirements.

We also provide full visibility into outdated device OS versions and security patch levels to ensure only updated devices that are free of vulnerabilities are allowed to access your data. By continuously monitoring for threats targeting mobile devices, we provide you with visibility into this highly distributed endpoint ecosystem, which otherwise would remain in the dark.

> “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**, cyber security 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 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.



Mobile Endpoint Security Dashboard

PROTECTED DEVICES Devices protected by the Lookout Security Cloud

120,001,000 PROTECTED GLOBALLY

1,539 PROTECTED IN YOUR FLEET

ANALYZED APPS Apps analyzed by the Lookout Security Cloud

10,781 ANALYZED GLOBALLY

322 ANALYZED IN YOUR FLEET

DEPLOYMENT STATUS

Connected	1
Pending	11
Disconnected	1386
Unreachable	141

DEPLOYMENT RISK

● High	788 · 56%
● Med	619 · 44%
● Low	0 · 0%

ACTIVE ISSUES

	TOTAL	● HIGH	● MED	● LOW
Total	6888	4013	2324	551
App	3443	3306	0	137
Device	3445	707	2324	414
Network	0	0	0	0

ISSUE TRENDS

30 Days

Comparison

☑ All Issues		☑ App Issues		☑ Device Issues		☑ Network Issues		☑ Web Content Issues	
Fleet	–	Fleet	–	Fleet	–	Fleet	–	Fleet	–
Global	–	Global	–	Global	–	Global	–	Global	–

Key Capabilities

Stop phishing attacks

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

Reduce compliance risk

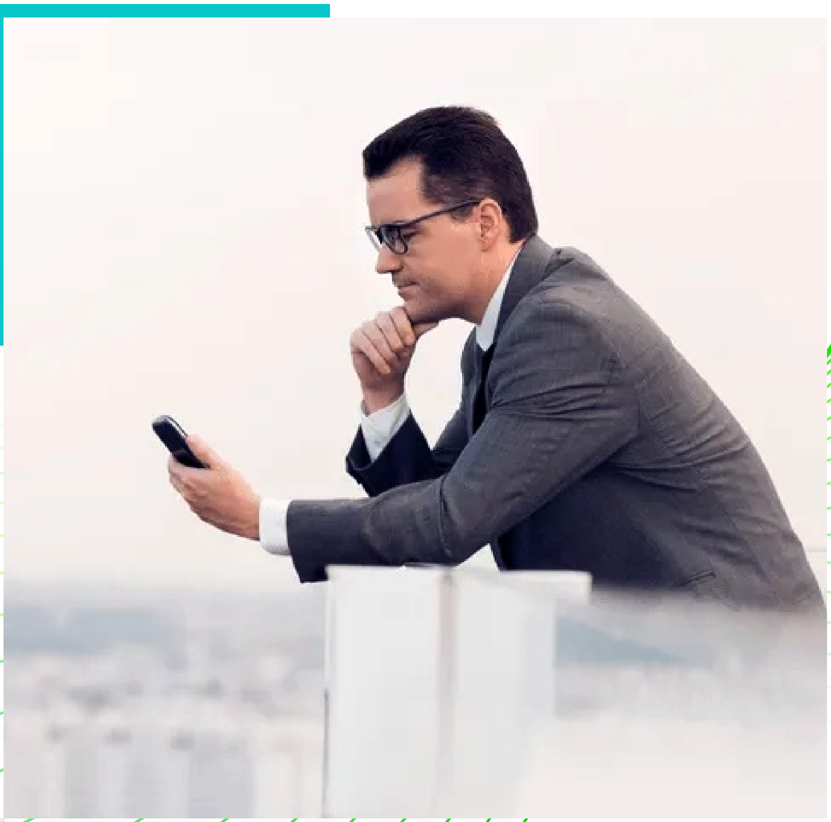
Set policies that look at the permissions and capabilities of the mobile apps your employees use to ensure compliance with both internal corporate mandates as well as industry regulations such as GDPR, HIPAA, and GLBA.

Manage vulnerabilities

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

Harden your defenses

Combine powerful Lookout and CrowdStrike protection capabilities to unify deep visibility across endpoints and mobile devices.



About Lookout

Lookout, Inc. is the data-centric cloud security company that delivers zero trust security by reducing risk and protecting data wherever it goes, without boundaries or limits. Our unified, cloud-native platform safeguards digital information across devices, apps, networks and clouds and is as fluid and flexible as the modern digital world. Lookout is trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to work and connect freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit lookout.com

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

About CrowdStrike

CrowdStrike Holdings, Inc. (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 | Twitter | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

https://go.crowdstrike.com/try-falcon-prevent.html