FIRSTNET APP CATALOG

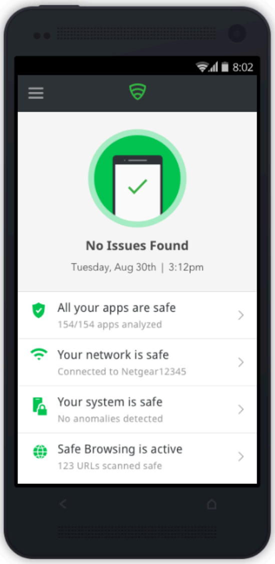
DATASHEET

Lookout Mobile Endpoint Security

Protecting your enterprise mobile fleet from mobile cyberattacks

What is Lookout Mobile Endpoint Security?

Lookout MES is a mobile threat defense (MTD) solution that protects your enterprise data from cybersecurity attacks targeting mobile devices. Cyber threats like phishing and malicious applications seek to exploit users as they operate beyond the traditional security perimeter with their smart phone and tablets. With robust protection for iOS and Android devices, Lookout leverages the massive data set of the Lookout Security Cloud - 170 Million devices and 70 million applications - to provide protection against the spectrum of mobile risk.



8:02

No Issues Found

Tuesday, Aug 30th | 3:12pm

All your apps are safe
154/154 apps analyzed

Your network is safe
Connected to Netgear12345

Your system is safe
No anomalies detected

Safe Browsing is active
123 URLs scanned safe

Benefits

- **Measurable reduction of risk** with Lookout analysis and reporting features
- **Real-time visibility** into incidents on mobile devices enables rapid response
- **Securely enable mobility** to embrace more flexible mobility programs such as BYOD
- **Privacy by design** approach to ensure data sovereignty, employee privacy, and regulatory compliance
- **Seamless interoperability** with leading EMM, SIEM, and, IAM solutions

About Lookout

Lookout is a cybersecurity company for the post-perimeter, cloud-first, mobile-first world. Powered by the largest dataset of mobile code in existence, the Lookout Security Cloud provides visibility into the entire spectrum of mobile risk. Lookout is trusted by hundreds of millions of individual users, enterprises and government agencies and partners such as AT&T, Microsoft, Apple and others. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.

Lookout Capabilities

MES Comprehensive

App-based threat protection
Malware, Rootkits, Spyware, Ransomware

Network-based threat protection
Man-in-the-Middle attacks, SSL attacks

Device-based threat protection
Advanced jailbreak/root detection, Operating system vulnerabilities, Risky device configurations

Custom threat policies

Threat dashboard

Data leakage control from apps that:

- Access sensitive data, such as contacts
- Send sensitive data (PII) externally
- Communicate with cloud services
- Have insecure data storage/transfer

Risky apps dashboard

Custom policies for risky apps

App blacklisting

Enterprise app review

Phishing and Content Protection

Web and Content-based threat protection
Phishing attacks from email, SMS, social, apps
Malicious URLs to risky websites

Management and Support

EMM Integration (VMware Workspace ONE UEM, IBM MaaS360, Microsoft Intune, Blackberry UEM, and MobileIron)

IAM Integration (Azure Active Directory, Okta, Google Cloud Identity, Ping Identity, and Centrify)

SIEM Integration via Mobile Risk API (Splunk, Windows Defender ATP_, Micro Focus, ArcSight, IBM Security and QRadar)