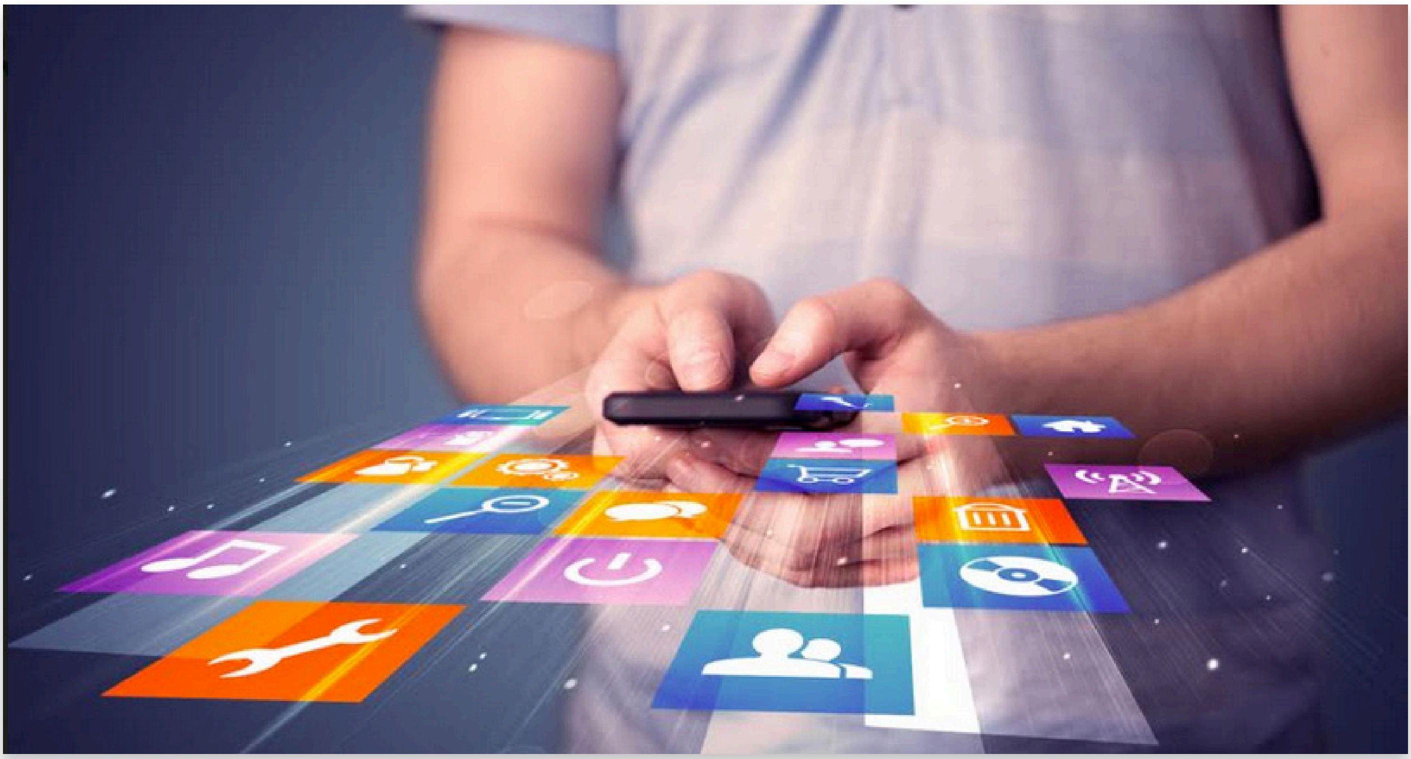
mobile mentor

Mobile Threat Management Service

Do you know which mobile apps are saving your data overseas, calling Dropbox APIs, passing your credentials in clear text and have a reputation score less than 5 out of 10?



If you manage a corporate mobile environment with a unique portfolio of apps on each device, then you have a unique risk profile for every user.

- Where is the user's app data being stored?
- Are users downloading apps with known vulnerabilities?
- What permissions have been granted to app developers?

If you are unable to answer these questions, you may like to consider a mobile threat management service from Mobile Mentor.

Mobile Threat Surface

The mobile threat surface is growing rapidly and enterprises are faced with increased risks from millions of available apps that may be on devices in their mobile environment. These seemingly innocuous apps expose enterprise users to data leakage, credential theft, the exfiltration of private information that can be used to target specific employees in advanced attacks and in cases malware that is capable of traversing folders and directories over the shared network.

There are three serious and highly variable risks associated with an exposed security posture of an enterprise mobile fleet:

1. New iOS and Android apps available through public apps stores;

2. Updates and patches to existing apps with elevated permissions;

3. Inability of current toolsets to detect and prevent mobile malware;

The purpose of Mobile Threat Management service is to identify risks in the business, determine their magnitude, likelihood and potential impact, proactively address them and then report monthly findings.

a) Provision of an industry leading app reputation scanning platform;

b) Proactive vulnerability scans to identifying the unknown;

c) Threat identification and assessment with severity scores;

d) Software patching, app updates, policy changes and system settings;

e) Report on device security posture, risk scores and system health;

f) Remediation of high risk apps by blocking, removing and escalating;

Mobile Mentor creates a process flow which includes extraction of app details from managed devices to cross-reference the millions of free and paid iOS and Android apps. Each app is scored against over 1,000 potentially malicious and privacy-leaking behaviours to determine its risk. Significant risk scores are subject to the mobile policy and have a unique course of action applied though people, process and technology.

Communications and recommendation of upgrades to OS and EMM platform are applied through regular interactions with the output being comprehensive protection and visibility against malicious and privacy-leaking iOS and Android apps.

Our People

Mobile Mentor is 100% focused on enterprise mobility. Our people are passionate about all things mobile and they provide our clients with depth and experience.

Our Experience

Mobile Mentor has 13 years experience on the frontline of enterprise mobility and we have empowered 1 million people.

Our Partners

Mobile Mentor has partnered with two global leaders for mobile threat protection: Lookout and ProofPoint. Their technology integrates with the leading EMM platforms.

Customers

Mobile Mentor is trusted by the largest healthcare, transport, forestry and government agencies.

Our clients rely on us for app development, security **solutions and mobility management.**