proofpoint

PROOFPOINT MOBILE DEFENSE

ADVANCED PROTECTION AGAINST APPS AND WI-FI NETWORKS THAT STEAL YOUR DATA

Enterprises face growing threats from malicious Wi-Fi hotspots and millions of apps on employee-owned devices. These apps can include malware and "riskware" – apps that might not be overtly malicious but exhibit behavior that puts enterprise data at risk. Together, these threats expose enterprise users to data leakage, credential theft, and the exfiltration of private information that can be used to target specific employees in advanced attacks.

"Through 2017, 75% of all mobile security breaches will be through apps, not through deep technical attacks on the OS,"

Gartner

Enterprise users casually access Wi-Fi hotspots and give these riskware apps sweeping permissions, not realizing that their personal and corporate data may be sent to remote servers and advertising networks all over the world, where it can be mined by cyber criminals and hostile governments seeking access to corporate networks.

APP THREAT INTELLIGENCE AND DEFENSE FOR THE ENTERPRISE

Proofpoint Mobile Defense provides enterprises with comprehensive protection and visibility against malicious and privacy-leaking iOS and Android apps. These apps frequently lead to advanced persistent threats (APTs), spear phishing attacks on employees, and leaked corporate data.

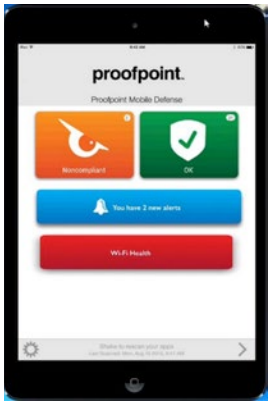
The Mobile Defense service works with mobile device management (MDM), enterprise mobility management (EMM), and mobile security management (MSM) solutions including AirWatch, MobileIron, and Mass360.

Our app analysis engine powers Mobile Defense. Our team of analysts, cryptographers and cyber crime specialists have analyzed over 23 million free and paid iOS and Android apps from more than 1 million publishers. Each app is scored against more than 1,000 potentially malicious and privacy-leaking behaviors to determine whether it is risky or safe.

ENTERPRISE CONTROLS

- Administrative console offers a dashboard view of app risk throughout the enterprise
- Set new thresholds for risky app behavior, and restrict specific behaviors
- Whitelist and blacklist specific apps
- Users and admins receive alerts when apps exceed risk thresholds
- Quarantine devices or deny access to enterprise services and data until risky apps are removed

Mobile Defense's easily configurable administrative console uses a dashboard to show the overall state of app security in your mobile deployment.



Smart mobile client dashboard alerts users to malicious Wi-Fi networks, non-compliant apps and enterprise notifications.

THE MOBILE DEFENSE CLIENT

Mobile Defense includes an optional mobile client app that works with leading MDM and EMM platforms to inform employees in corporate BYOD environments about the potential risks associated with the apps on their devices.

- Users can see whether an app is dangerous or safe at a glance.
- An app data location feature maps where apps send data.
- New apps loaded onto the device are scanned within minutes.
- Alerts instruct the user to delete an app if it is risky or dangerous.
- Automatic malicious Wi-Fi detection (including man-in-the-middle and SSL stripping attempts).

See which apps are dangerous and what they're doing behind the scenes.

AUTOMATED WORKFLOW

Workflows automate your defense with Mobile Defense:

1. Mobile Defense identifies a dangerous app on the employee's device
2. The employee receives an alert that a dangerous app on their device must be removed
3. If the employee fails to remove the dangerous app in time, Mobile Defense quarantines the device
4. Once the app is deleted, corporate services are reinstated

Mobile Defense shows you where in the world an app is sending your personal data.

EMPLOYEE PRIVACY

To assure that businesses comply with a wide range of employee privacy laws and regulations, Mobile Defense offers several levels of control. Mobile Defense may be configured to:

- Report all apps and specifically correlate apps to a user's device
- Report apps anonymously, without correlating to a specific user
- Total privacy, where no app information is reported to the enterprise, only whether there is a dangerous app on an employee's device

WHY MOBILE DEFENSE?

By combining rich mobile app analysis data with an automated workflow, Mobile Defense provides network and security administrators with the information and visibility needed to manage mobile app risk in the enterprise. Mobile Defense helps you:

- Control apps that leak corporate data
- Dynamically assess threats and where data is sent
- Control for dangerous apps
- Safeguard your BYOD program for iOS and Android
- Protects users from malicious Wi-Fi and the apps that steal data

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.