proofpoint

Targeted Attack Protection Mobile Defense

Protects against apps that steal corporate data

Enterprises face a far greater threat from the millions of generally available apps on their employees' devices than from mobile malware. Called 'riskware,' these seemingly innocuous apps 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.

Enterprise users casually 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 cybercriminals and hostile governments seeking access to corporate networks.

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

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

App threat intelligence and defense for the enterprise

Targeted Attack Protection (TAP) 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 TAP Mobile Defense service works in conjunction with enterprise Mobile Device Management (MDM), Enterprise Mobility Management (EMM), and Mobile Security Management (MSM) solutions to provide dynamic app threat detection and protection.

Proofpoint's app analysis engine powers TAP Mobile Defense. Proofpoint's team of analysts, cryptographers and cybercrime specialists have analyzed more than 2 million free and paid iOS and Android apps from more than 500,000 publishers. Each app is scored against more than 1,000 potentially malicious and privacy-leaking behaviors to determine whether it is risky or safe.

See whether you've downloaded dangerous apps with the TAP Mobile Defense optional personal client.

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
- White list and black list 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

The TAP Mobile Defense client

TAP 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.

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

Automated workflow

Workflows automate your defense with TAP Mobile Defense:

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

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

Employee privacy

To assure that businesses comply with a wide range of employee privacy laws and regulations, TAP Mobile Defense offers several levels of control. TAP 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 TAP Mobile Defense?

TAP Mobile Defense is the market leading solution for app threat intelligence and defense. By combining rich mobile app analysis data with an automated workflow, TAP Mobile Defense provides network and security administrators with the information and visibility needed to properly manage mobile app risk in the enterprise.

- Controls apps that leak corporate data
- Dynamically assesses threats and where data is sent
- Provides automatic controls for dangerous apps
- Assures safety of your rollout of BYOD program for iOS and Android

About Proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

©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.

892 Ross Drive
Sunnyvale, CA 94089

1.408.517.4710
www.proofpoint.com