

FIREEYE MOBILE THREAT PREVENTION

IDENTIFY, ANALYZE AND BLOCK MOBILE THREAT ATTACKS

OVERVIEW

Mobile malware can access a trove of invaluable user information to perform attacks via the Web and email. FireEye Mobile Threat Prevention (MTP) identifies threats in an application and stops them from interfering with mobile devices. Rather than relying on signatures — which are powerless against today's constantly changing threats — FireEye MTP executes apps within FireEye's threat intelligence engine to determine an application's well-being in order to protect mobile devices against compromised applications.

Whether utilizing the cloud or appliance version of FireEye MTP, customers get real-time visibility into application threats on mobile devices, obtaining play-by-play analysis of any suspicious apps, including an index of pre-analyzed apps. Additionally, FireEye MTP can generate the same type of threat assessments for custom applications. FireEye MTP leverages the FireEye Dynamic Threat Intelligence™ (DTI) cloud, which is backed by FireEye global research, to deliver robust on-device mobile threat detection.

FireEye threat intelligence engine detects unknown threats

FireEye MTP utilizes FireEye's powerful threat intelligence engine. Rather than relying on binary signatures, the engine can detonate an application within instrumented virtual Android and iOS mobile environments. Its dynamic analysis capability can examine various malware parameters and use contextual correlation to connect disparate actions to assemble a full picture of the app's intent, quickly flagging any suspicious behavior. This approach makes FireEye MTP resilient to obfuscation, code manipulation, evasion techniques, jailbreak detection, device misconfiguration, unpatched devices and even the installation of apps from unauthorized sites, ensuring it addresses threats — both known and unknown — that other defenses simply miss.

HIGHLIGHTS

- Identifies and blocks mobile threats against Android and iOS devices
- Conducts contextual correlation, connecting seemingly disparate actions to uncover malicious or unwanted application behavior
- Analyzes data to detect compromises in mobile devices and provides enforcement options for threat response
- Uses APIs to integrate with key MDM and other enterprise systems

FireEye MTP Analysis enables on-demand app threat assessments

FireEye MTP LiveAnalysis™ uses a combination of semantic, dynamic and behavioral analysis to develop comprehensive on-demand threat assessments. This gives organizations visibility into an app’s operation to see precisely what the app did to trigger an alert and determine whether the app should be allowed to run. This feature enables organizations to understand threat ratings and gain actionable intelligence to block apps and enforce security policies.

FireEye MTP Analysis offers access to a continuously updated database of more than 9 million iOS and Android apps from multiple app stores, providing detailed threat analysis and scores that enable real-time remediation.

FireEye MTP Management provides enterprise-wide visibility of mobile threats

FireEye MTP Management provides real-time visibility into threats on mobile devices. FireEye MTP Management enables security administrators to gain an enterprise-wide view into mobile device compromise while offering a customizable enforcement option. FireEye MTP Management is a cloud, on-premise or hybrid solution (details below). It works in conjunction with the FireEye MTP App to assimilate and disperse threat information

to mobile endpoints, and offers integration with MDM solutions for a true detect-to-fix solution.

The FireEye MTP App is a lightweight mobile app that can be downloaded to mobile devices. It communicates with FireEye MTP Management to display app threat scores, detail malicious or unwanted behavior within each app and examine factors associated with endpoint device compromise.

On-device detection includes SMS- and network-based threats, jail break, phishing and OS vulnerabilities.

Global mobile threat intelligence

Cyber criminals often orchestrate attacks across multiple threat vectors such as Web, email and mobile. FireEye MTP draws intelligence from the FireEye Dynamic Threat Intelligence cloud, which weaves together anonymized data shared by a range of FireEye platforms deployed around the globe. By leveraging the cloud, the FireEye MTP platform more efficiently detects both known and unknown malware, zero-day exploits and highly targeted attacks used for cyber crime, cyber espionage and cyber reconnaissance.

Deployment flexibility

FireEye MTP is an open platform that provides API access for customer flexibility in integrating MTP with their existing tools, such as SIEM or an enterprise workflow or ticketing system.

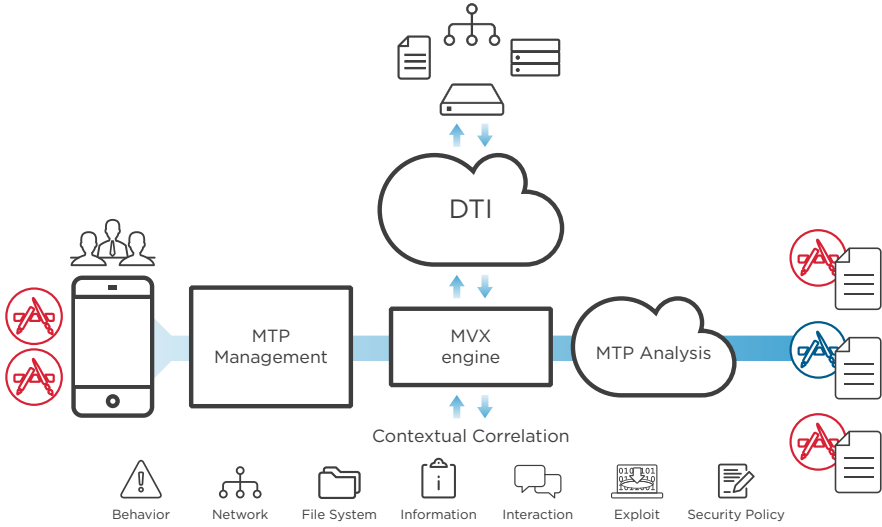
USE CASES

- **Mobile Deployments** — offers proactive protection for unsecured bring-your-own-device (BYOD) and corporate deployments
- **Mobile Forensics** — provides deep inspection capabilities for mobile threats and vulnerability management
- **App Development** — enables security auditing for in-house or outsourced app development
- **Multiple Enterprise App Stores** — identifies secure apps for employee use across multiple apps stores

MTP FEATURES	MTP MANAGEMENT	MTP ANALYSIS
Android and iOS Application Dynamic Analysis	•	•
FireEye NX and DTI Integration	•	•
Callback Records	•	•
APIs	•	•
App Policy Management	•	
Device Threat Assessment	•	
Phishing Detection	•	
Messaging/SMS Security	•	
App Behavioral Analytics with LiveAnalysis Mode		•

SYSTEM SPECIFICATIONS		
COMPONENT	MX 900	MX 8400
Users Supported	10,000	100,000
FIPS 140-2 Compliant	Yes	Yes
Form Factor	1U Rack-Mount	2U Rack-Mount
Weight	17 lbs (7.7kg)	42 lbs (19 kg)
Dimensions (W x D x H)	16.8 x 14.0 x 1.7 inches (42.6 x 35.6x 4.3cm)	17.2 x 28.0 x 3.4 inches (43.7 x 71.1 x 8.6 cm)
Enclosure	Fits 19-inch Rack	2 RU, Fits 19-inch Rack
Management Interfaces	(1) 10/100/1000BASE T Ports	(2) 10/100/1000BASE T Ports

FireEye Mobile Threat Prevention



For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
 1440 McCarthy Blvd. Milpitas, CA 95035
 408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

© 2016 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. DS.MTP.EN-US.042016

