DATASHEET

FireEye Mobile Threat Prevention

Identify, Analyze, and Block Mobile Attacks Within Your Organization

HIGHLIGHTS

- Identifies and blocks attacks against Android and iOS devices
- Uses the FireEye® Multi-Vector Virtual Execution™ (MVX) engine to perform contextual correlation—connecting disparate actions for a full picture of the app's intent—to uncover malicious and unwanted behaviors
- Provides granular visibility into mobile device compromise as well as enforcement options for security administrators
- Presents detailed behavioral analytics including a live-analysis mode where organizations can visually see the impact of malicious and unwanted behavior specific to the industries you care about

TARGET APPLICATIONS

- **BYOD Deployments**—offers proactive protection for unsecured BYOD deployments
- **Mobile Forensics**—provides deep inspection capabilities for mobile threat and vulnerability management
- **App Development**—enables security auditing for offshored app development
- **Enterprise App Stores**—identifies secure apps for employee use

Overview

Malicious apps can access a trove of invaluable user information that can be used to perform attacks via the Web and email threat vector. FireEye Mobile Threat Prevention identifies and stops mobile threats. Rather than relying on signatures—which are powerless against today's constantly changing threats—FireEye Mobile Threat Prevention executes apps within the FireEye MVX engine to protect mobile devices against compromise.

FireEye Mobile Threat Prevention (MTP) offers real-time visibility of threats on mobile devices, displays play-by-play analysis of suspicious apps, provides an index of pre-analyzed apps, and generates threat assessments for custom apps. FireEye Mobile Threat Prevention also leverages the broad FireEye ecosystem by exchanging threat intelligence through the FireEye Dynamic Threat Intelligence™ (DTI) cloud.

FireEye Mobile MVX engine detects unknown threats

FireEye Mobile Threat Prevention (MTP) is powered by the MVX engine. Rather than relying on binary signatures, the MVX engine detonates apps within instrumented virtual Android and iOS mobile environments. With this dynamic analysis, the MVX engine examines various malware parameters. And using contextual correlation—connecting disparate actions for a full picture of the app's intent— it flags suspicious behaviors. This approach makes FireEye Mobile Threat Prevention resilient to obfuscation, code manipulation, evasion techniques, and ensures it identifies known and unknown threats that other defenses miss.

FireEye MTP Analysis enables on-demand app threat assessments

FireEye MTP Analysis uses a combination of semantic, dynamic, and behavioral analysis to give comprehensive on-demand threat assessments. Live analysis gives organizations more visibility into the app detonation and the dynamic analysis process. Security professionals can see precisely what the app did to trigger each alert. 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 FireEye app threat database of more than 3M iOS & Android apps with detailed threat analysis and scores for real-time remediation.

FireEye MTP Management provides enterprise-wide visibility of mobile threats

FireEye MTP Management is a hybrid cloud offering that 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. MTP Management is offered as an on-premise MX900 appliance and works in conjunction with the FireEye MTP App to assimilate and disperse threat information from the MVX engine 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 on mobile devices. It communicates with FireEye MTP Management to display threat scores of apps on mobile devices, detail malicious or unwanted behavior within each app, and examine factors associated with endpoint device compromise. The FireEye MTP App alerts mobile uses to threats before a malicious app is executed on their device.

Global mobile threat intelligence

Cybercriminals often orchestrate attacks across multiple threat vectors such as Web, email, and mobile. FireEye Mobile Threat Prevention draws intelligence from the FireEye DTI cloud. The DTI cloud weaves together anonymized data shared by participating FireEye platforms deployed around the globe. By leveraging the DTI cloud, the FireEye Mobile Threat Prevention platform more efficiently detects both known and unknown malware, zero-day exploits, and highly targeted attacks used for cybercrime, cyber espionage, and cyber reconnaissance.

Mobile Threat Prevention Features	Availability
Android and iOS Application	🟠
App Policy Management	🟠
Device Threat Assessment	🟠
FireEye DTI	🟠 ●
App Threat Assessment	🟠 ●
App Behavioral Analytics	●
Live-Analysis Mode	●
Callback Records	●

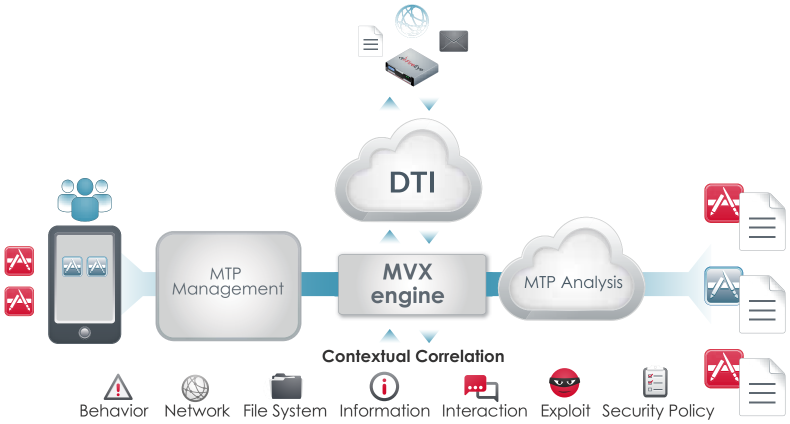
🟠 MTP Management ● MTP Analysis

System Specifications

The table below provides the technical specifications of the FireEye MX 900.

Component	MX 900
Form Factor	1U Rack-Mount
Weight	17 lbs (7.7kg)
Dimensions (W x D x H)	16.8 x 14.0 x 1.7 inches (42.6x35.6x4.3cm)
Enclosure	Fits 19-inch Rack
Management Interfaces	(1) 10/100/1000BASE-T Ports
AC Input Voltage	Auto-switching 100 ~ 240 VAC Full Range
AC Input Current	4.8 - 2.0 A
Power Supply / RAID	Single 200W / No
Power Consumption (Max)	528 BTU/hr
Frequency	50 - 60 Hz
Operating Temp	10° C to 35° C

FireEye Mobile Threat Prevention


DTI
MTP Management
MVX engine
MTP Analysis
Contextual Correlation
Behavior
Network
File System
Information
Interaction
Exploit
Security Policy