FireEye

Datasheet

FireEye Mobile Threat Prevention

Cloud-based platform that identifies, analyzes, and blocks mobile attacks

Highlights

- Uses contextual correlation—connecting disparate actions for a full picture of the app's intent—to uncover the hidden malicious and unwanted behaviors embedded deep within an app
- Provides a live-analysis mode where organizations can visually see the impact of malicious and unwanted behavior
- On-demand threat assessments for both custom apps and apps available in public or enterprise app stores
- Integrates with the FireEye DTI cloud to use and share information gleaned from other FireEye deployments
- Offers APIs to integrate with mobile management and endpoint solutions

Target Applications

- **Mobile Forensics**—provides deep inspection capabilities for mobile threat and vulnerability management
- **App Development**—enables security auditing for offshored app development ensuring secure enterprise apps
- **Enterprise App Stores**—identifies secure apps for employee use
- **BYOD Deployments**—offers proactive protection for unsecured BYOD deployments that have no insight on security lapses

FireEye® Mobile Threat Prevention identifies and stops mobile threats. Rather than relying on malware signatures—which are powerless against today's fast-moving, constantly changing threats—FireEye Mobile Threat Prevention executes apps within the FireEye Multi-Vector Execution™ (MVX) Engine to provide comprehensive mobile threat assessments.

The cloud-based platform offers play-by-play analysis of suspicious apps, an index of pre-analyzed apps, and 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. It integrates with mobile management and endpoint vendors to secure your enterprise mobile deployment.

The mobile threat

Mobile malware is exploding. According to one estimate, the number of malware apps targeting Android alone will reach 1 million by the end of 2013.[1] These apps can access a trove of invaluable information: user messages, emails, calendar, contacts, and a host of other information. This stolen information can be used for other attacks that use the Web and Email threat vectors.

The few "mobile virus scanners" sold today have the same problem that traditional desktop anti-virus software has: malware can easily evade them through code changes and other obfuscation techniques. These scanners may warn users of some known malware. But they cannot spot new threats, and they do not flag unwanted app behavior.

Organizations must deploy a defense that understands mobile app behavior. Knowing what an app does with the information it controls is critical to keeping networks safe and intellectual property secure.

Mobile MVX detects unknown threats

FireEye Mobile Threat Prevention is powered by the Mobile Multi-Vector Virtual Execution engine. Rather than relying on binary signatures, the MVX engine detonates apps within instrumented virtual Android

1 FOXBusiness. "Cyber Hackers on Course for One Million Malware Apps." August 2013.

environments. With this dynamic analysis, the Mobile 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 changing, and evasion techniques. It can identify known and unknown threats that other defenses miss.

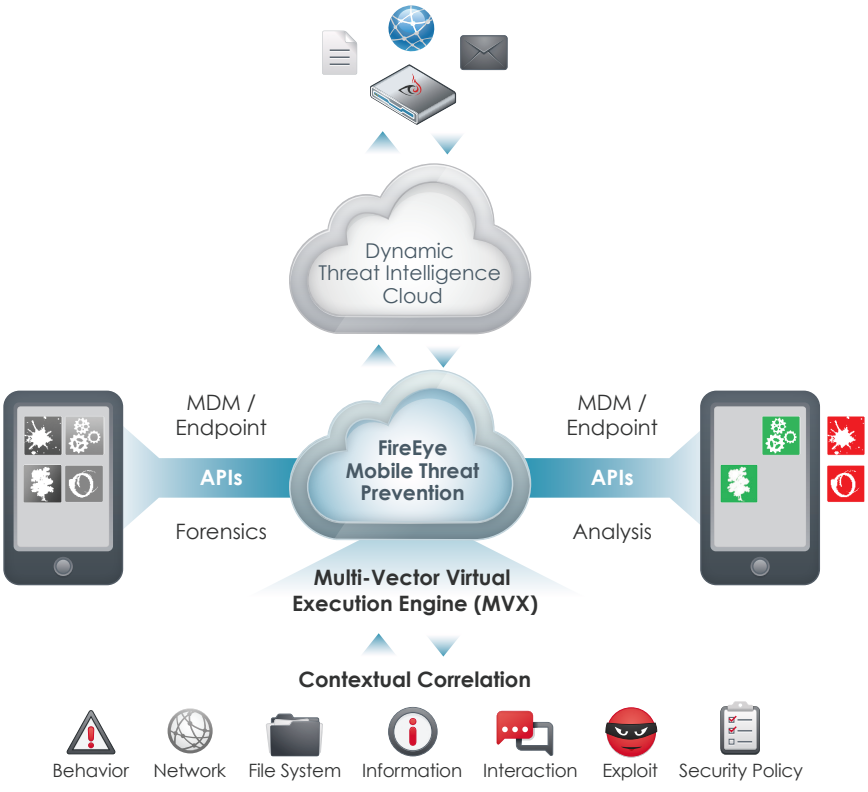
Live-analysis mode enables real-time threat intelligence

Live-analysis mode gives organizations more visibility into the app detonation and the dynamic analysis process. Second-by-second video playback shows the app's actions and on-screen display; 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 Mobile Threat Prevention maintains an app threat database of over a million Android apps, with detailed threat analysis and scores for real-time remediation. New and updated apps can also be analyzed within minutes in the Mobile MVX engine.

Easy-to-integrate cloud-based solution

FireEye Mobile Threat Prevention is a cloud service. It provides unmatched visibility into app behavior to help security professionals make informed decisions about mobile app security policies. Users can search for and analyze custom-built apps and those from both public and enterprise app stores. And they can specify which version of Android to use for detonating apps. With the FireEye Mobile Threat Prevention solution, customers can submit apps through Web dashboard for analysis. Organizations can also automate analysis using FireEye Mobile Threat Prevention APIs and our ecosystem of mobile device management (MDM) and endpoint partners. Using FireEye threat scores, organizations can specify and enforce mobile security policies through the endpoint or MDM solution.



FireEye™

Datasheet

Global mobile threat intelligence

The mobile threat vector does not work in isolation. Cybercriminals often orchestrate attacks across multiple threat vectors such as Web and email. FireEye Mobile Threat Prevention draws from the broad FireEye ecosystem through the FireEye DTI cloud. The DTI cloud weaves together anonymized data shared by participating FireEye platforms deployed around the globe. The DIT cloud acts as a global distribution hub to share threat intelligence such as callback channels, malware profiles, vulnerability exploits, and obfuscation tactics. It even incorporates new threat findings from the FireEye Labs and verified third-party security feeds. By leveraging the DTI cloud, the FireEye platform more efficiently detects known malware and zero-day, highly targeted attacks used for cybercrime, cyber espionage, and cyber reconnaissance. Using threat information gathered from the DTI cloud, FireEye Mobile Threat Prevention identifies threats that use multi-vector tactics.

Features	Mobile Threat Prevention for Android	Mobile Threat Prevention with MDM	Mobile Threat Prevention with Endpoint
Application Dashboard	•	•	•
FireEye Threat Score	•	•	•
App Threat Database	•	•	•
Admin Initiated App Analysis	•	•	•
Custom Apps	•	•	•
Detailed Threat Assessment	•	•	•
FireEye DTI	•	•	•
Live-Analysis Mode	•	•	•
Mobile Endpoint Analysis	Available with API integration	•	•
Mobile Endpoint Policy Enforcement	Available with API integration	•	•

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