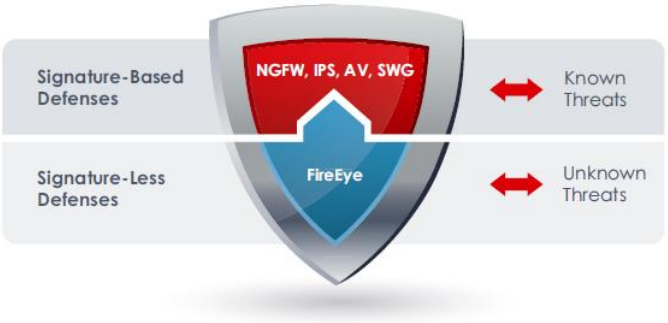
FireEye Threat Prevention Platform

The FireEye Threat Prevention Systems are the industry's first threat prevention solution to the advanced malware infection life cycle, stopping targeted and zero-day attacks along the web, file server, and email vectors.



FireEye technologies fill the security hole left by traditional defenses

- **FireEye Web Security** Protects the user against web-borne threats. FireEye Web Security (FireEye **NX** Series) uses its multi-phase detection mechanism and callback analysis to detect advanced malware.

- **FireEye Malware Analyses** (FireEye **AX** Series) Performs detailed, customized forensic analysis of advanced malware, zero-day, and targeted APT attacks embedded in common file formats, email attachments, URLs, binaries, and web objects.

- **FireEye Email Security** (FireEye **EX** Series) Provides protection against spear-phishing attacks by detecting and preventing advanced malware from infecting the end user via attachments and URLs embedded in email intended to extract sensitive organizational data.

- **FireEye Content Security** (FireEye **FX** Series) Provides proactive threat management for enterprise intranet file shares. File MPS performs recursive, scheduled, remote scanning of accessible networked file shares to detect and quarantine resting malware without impact to corporate productivity.

- **FireEye CM** (FireEye **CM** Series) The threat prevention central management and integration system for FireEye appliances and services.

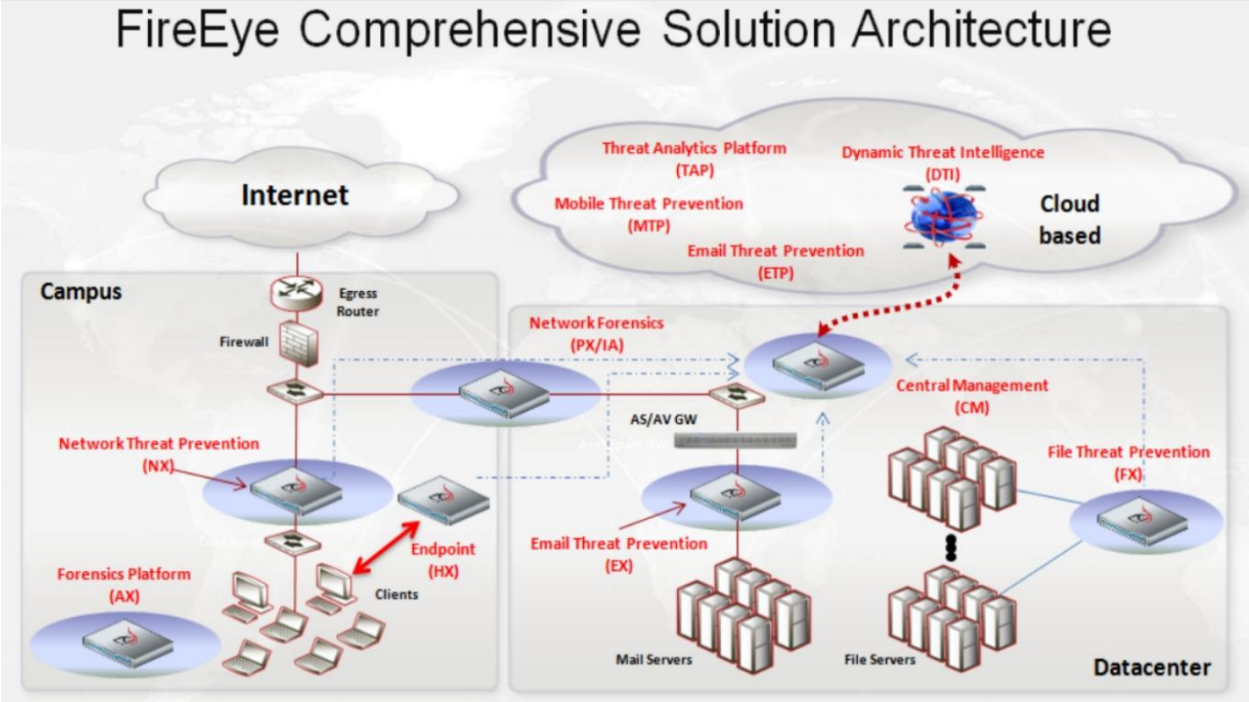
- **FireEye Mobile Threat Prevention (MTP)** identifies and stops mobile threats. Rather than relying on malware signatures—which are powerless against today's fast-moving, constantly changing threats—FireEye **Mobile Threat Prevention** executes apps within the FireEye Multi-Vector Execution (MVX) engine and provides an automated mobile threat assessment that enables organizations to enforce security policies in the mobile environment.

- **FireEye Email Threat Prevention (ETP)** is a cloud-based platform that protects against today's advanced email attacks. With no hardware or software to install, the cloud-based **Email Threat Prevention** platform is a particularly good fit for organizations already moving their overall infrastructure into the cloud. To start protecting against malicious emails, organizations simply route messages to the Email Threat Prevention platform. The cloud then uses the signature-less FireEye Multi-Vector Virtual Execution (MVX) engine to analyze every attachment and URL to detect threats and stop APT attacks in real time.

- **Threat Analytics Platform (TAP)** is a cloud-based solution that enables security teams to identify and effectively respond to cyber threats by layering enterprise generated event data with real-time threat intelligence from FireEye.

- **FireEye HX Threat Prevention (MSO)** is an Endpoint Threat Prevention Platform that detects, analyzes, and resolves security Incidents on the endpoint in a fraction of the time it takes using conventional approaches.

- **PX\IA** Technologies (known as nPulse) is the performance leader in network forensics and Packet capture for security focused organizations who looking to significantly reduce incidence response time by having network traffic recording at 20Gbps.

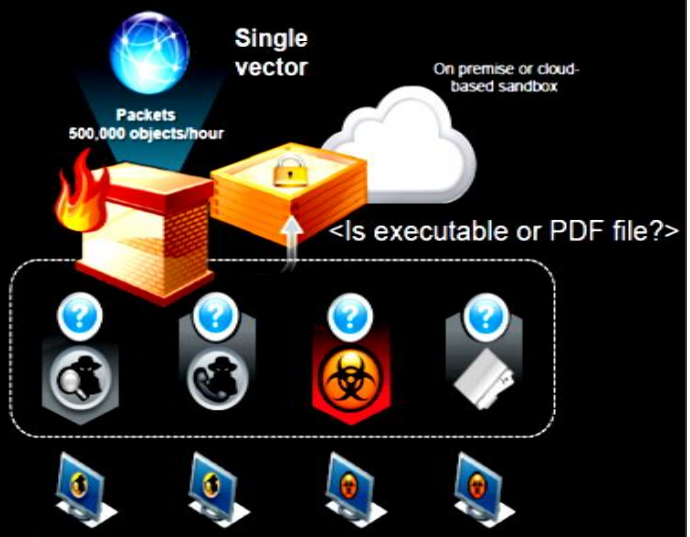


FireEye

Why FW + Sandbox Solutions Miss APT Attacks

Limitations of Sandbox approach

- No hardened hypervisor
- No multi-vector protection
- No multi-flow analysis
- In-the-clear executable files only
- Incoming file rate of 3-5/hour
- No cross-matrix of vulnerable SW
- No web exploit detection!



This is NOT an APT prevention solution!

Multi-Flow Structure of APT Attacks (e.g. Operation Aurora, Operation Beebus, CFR…)

1. Exploit injects code in Web browser
2. Exploit code downloads encrypted malware (not SSL!)
3. Exploit code decrypts malware
4. Target end point connects to C&C server