

# The Evolution of Cyber Attacks and Next Generation Threat Protection

Ashar Aziz

Founder, Vice-Chairman and CTO  
FireEye, Inc.

Security in  
knowledge

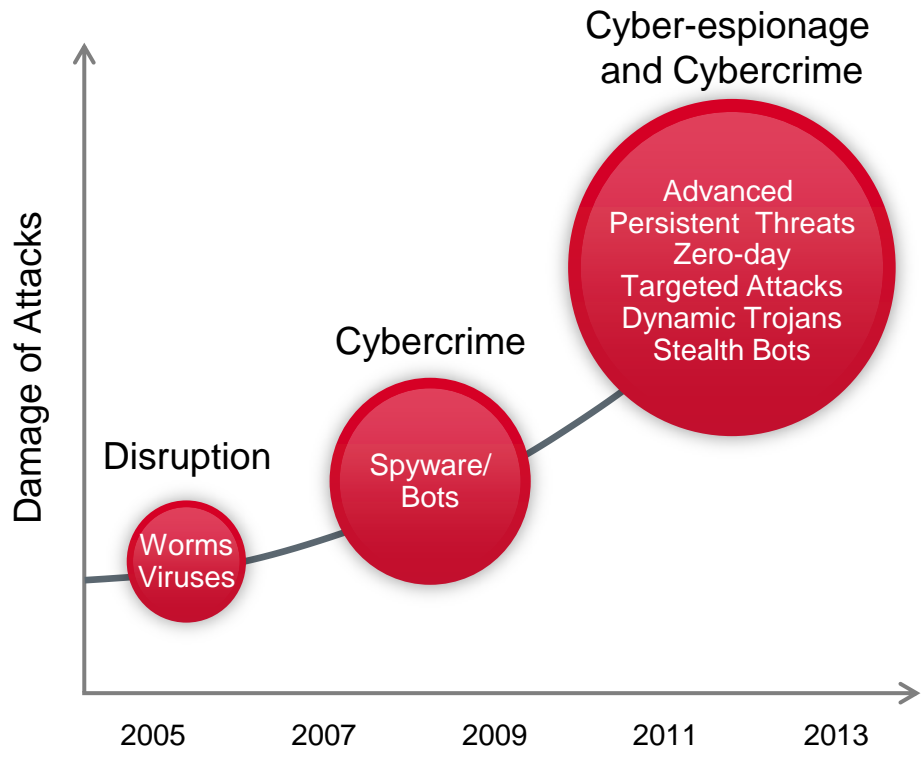


# — Agenda

- ▶ The New Threat Landscape
- ▶ Deep Dive on Advanced Attacks
- ▶ Principles of Next Generation Protection

# The New Breed of Attacks

- ▶ Nature of threats changing
- ▶ Today's attacks sophisticated and successful



“Organizations face an evolving threat scenario that they are ill-prepared to deal with....threats that have bypassed their traditional security protection techniques and reside undetected on their systems.”

Gartner, 2012

# What's Changed?



Coordinated Persistent Threat Actors



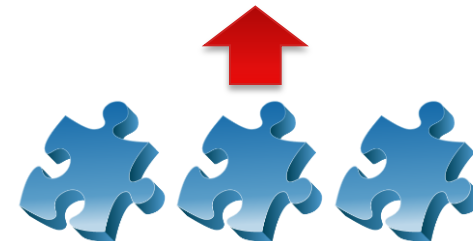
Dynamic,  
Polymorphic Malware



## NEW THREAT LANDSCAPE



Multi-Vector Attacks



Multi-Stage Attacks

# Multiple Vectors - Targeting An Organization's Valuable Assets



Spear Phishing



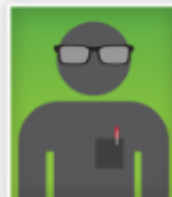
CFO



Financial Information



Web-Based Attack



Director of Engineering



Intellectual Property



File-Based Attack

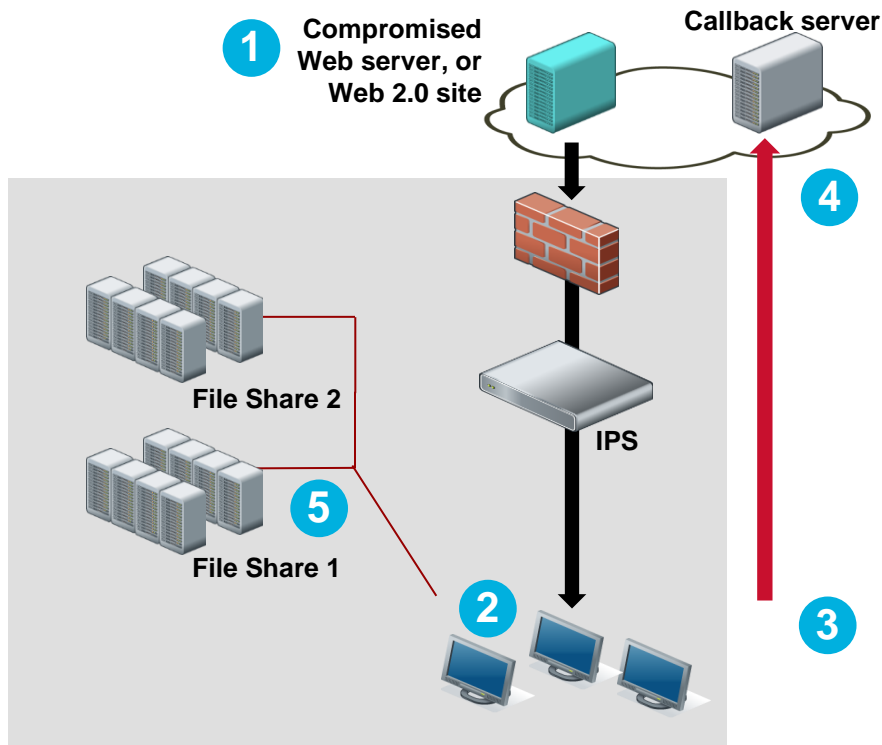


Government Employee



National Security Info

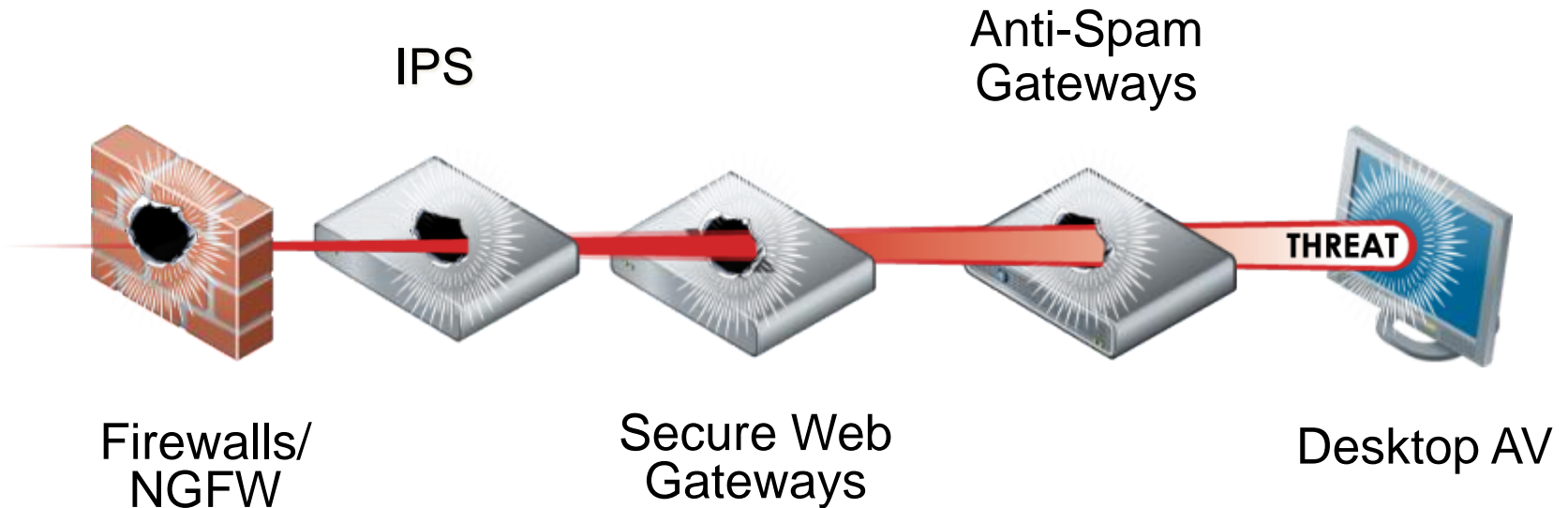
# Multiple Stages: The New Attack Life Cycle



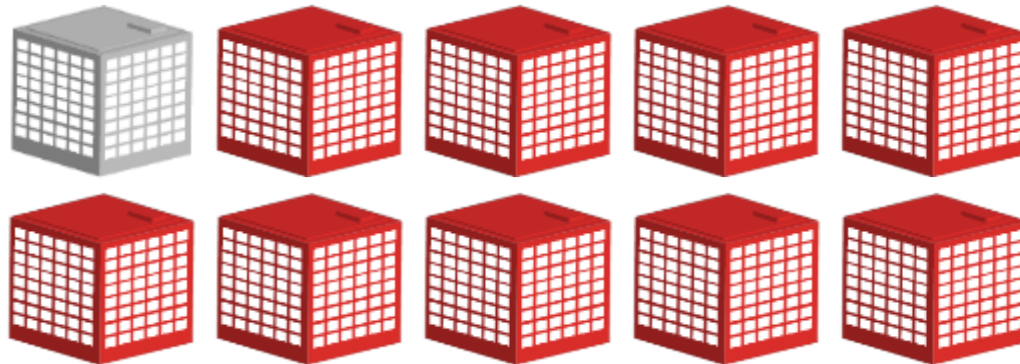
- 1 Exploitation of system
- 2 First Callback for malware download
- 3 Malware executable download
- 4 Data exfiltration
- 5 Malware spreads laterally

# Traditional Defenses Don't Work

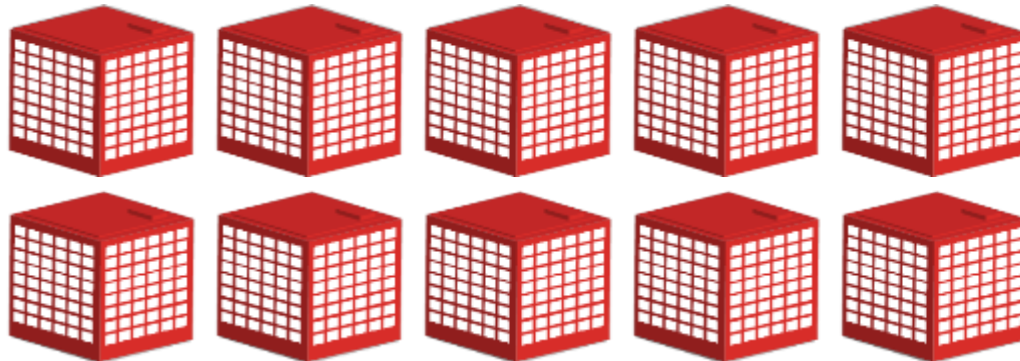
The new breed of attacks evade signature-based defenses



# The Security Gap is Broad



**95% of Companies are Compromised**



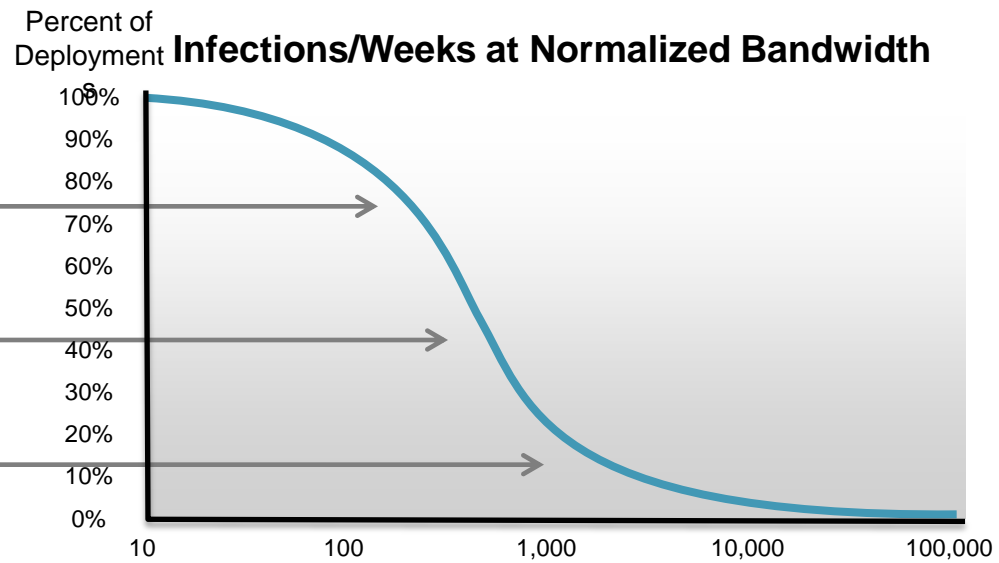


# The Degree of Compromise is Significant

**98.5%** of deployments see at least 10 incidents/week

Median is about **643** incidents/week

**20%** of deployments have thousands of incidents/week



Source: FireEye Advanced Threat Report, Feb. 2012

## 643 Median Net New Infections Per Week!

# Spectrum of Frequent Advanced Attacks



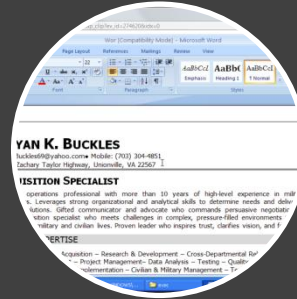
## Mass Website Compromises

- Exploit toolkits
- Zero-day exploits (rare)
- Sophisticated crimeware



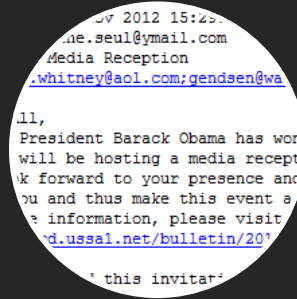
## Watering Hole Attacks

- Compromised site specific to industry vertical
- Zero-day exploits more common
- Frequently nation-state driven



## Weaponized Email Attachments

- Common file formats
- Legit work product presented (decoy)
- Preferred by nation-states



## Malicious URLs in Email (Spear phish)

- Exploits specific to target environment
- Only exploit if visited from target network(s)
- Use existing trust relationships

**1000+ Victims**

**(Easiest to Detect)**

**~1-2 Victims**

**(Hardest to Detect)**



# 1) Offense: Watering Hole Methods

- ▶ Growing in popularity among nation-state threat actors
- ▶ Useful when precise targeting intel is unknown
- ▶ Compromise website likely visited by target
- ▶ Start campaign when target is distracted (e.g. holidays)
- ▶ Once victim compromised, clean up site
- ▶ Or, leave exploit for opportunistic attacks



# 1) Offense: Watering Hole Methods

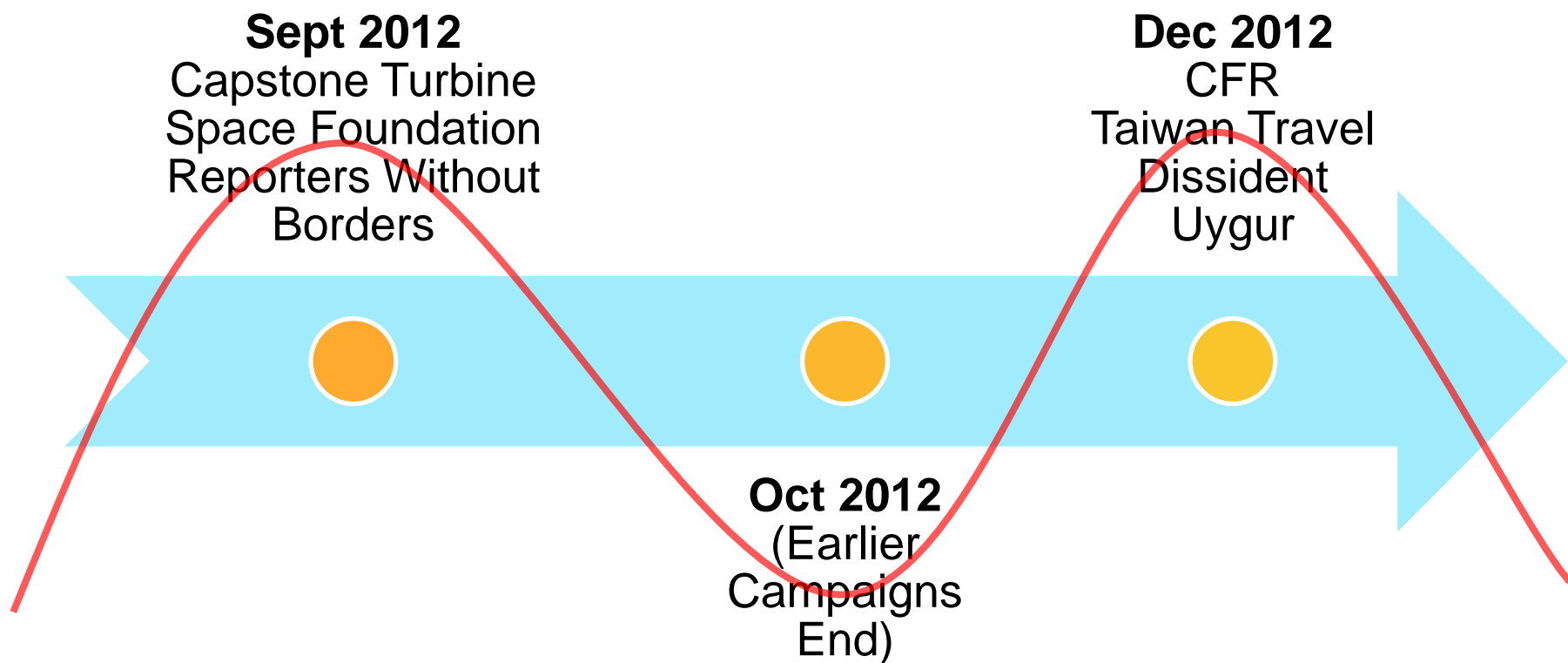
## Ex: Council on Foreign Relations (CFR)

- ▶ On Dec 21, 2012, FireEye detected attacks from cfr.org to 4 major customers
  - ▶ Victims: large scale ISP, large US financial, US media outlet, and local government
  - ▶ Only worked from US, JP, KO, and CN systems
  - ▶ Exploit triggers only one time (cookie tracking)
  - ▶ First reported IE 8 zero-day exploit (CVE-2012-4792)
  - ▶ Obfuscated JS + Heapspray via Flash + IE 8 exploit
  - ▶ Fetches xsainfo.jpg as XOR encoded backdoor
  - ▶ Loads backdoor as “shiape.exe”
  - ▶ Callbacks to dynamic DNS C2 provider as normal HTTP POST traffic
  - ▶ More at: <http://blog.fireeye.com>

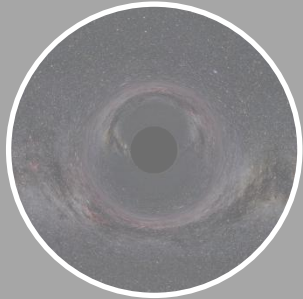


# 1) Offense: Watering Hole Methods

**CFR is not the first...nor the last...**



# Email Attacks



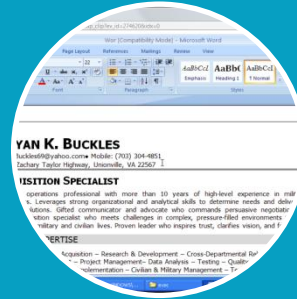
## Mass Website Compromises

- Exploit toolkits
- Zero-day exploits (rare)
- Sophisticated crimeware



## Watering Hole Attacks

- Compromised site specific to industry vertical
- Zero-day exploits more common
- Frequently nation-state driven



## Weaponized Email Attachments

- Common file formats
- Legit work product presented (decoy)
- Preferred by nation-states



## Malicious URLs in Email (Spear phish)

- Exploits specific to target environment
- Only exploit if visited from target network(s)
- Use existing trust relationships

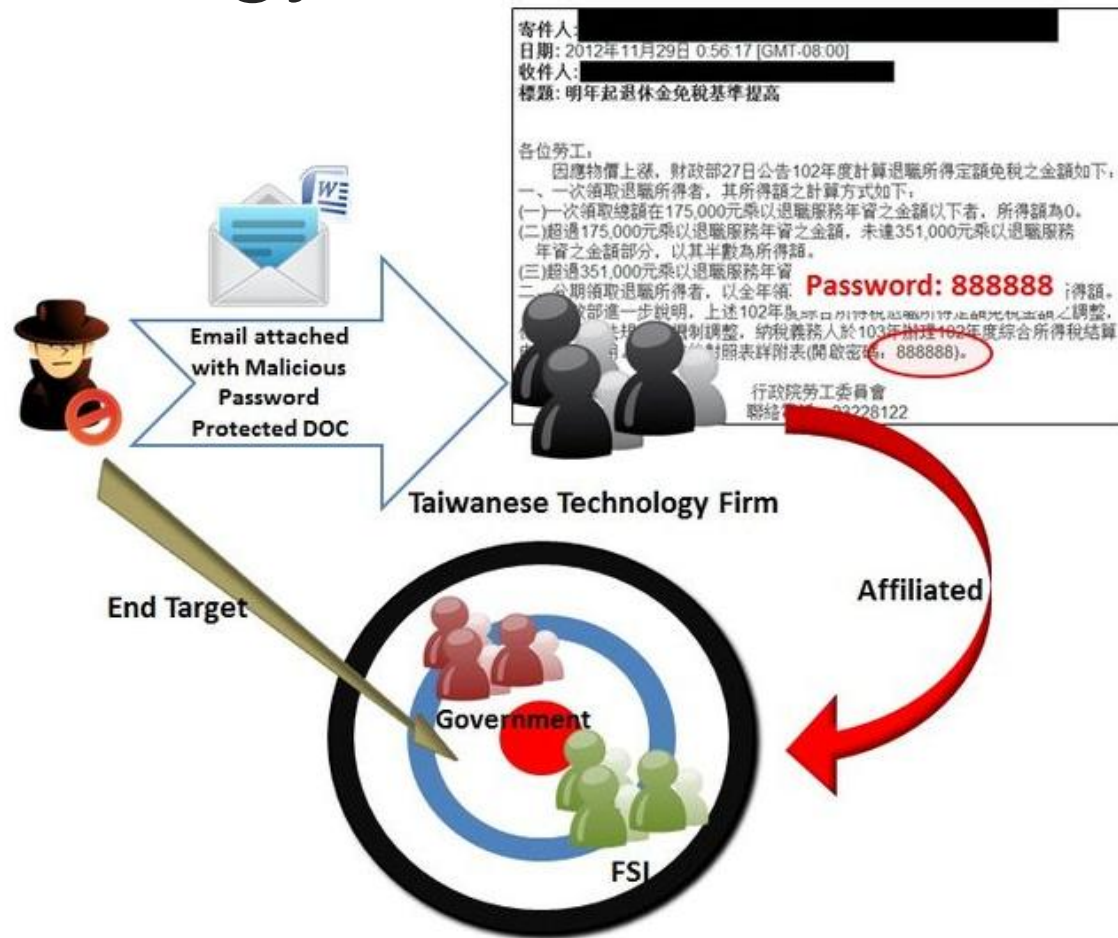
1000+ Victims

(Easiest to Detect)

~1-2 Victims

(Hardest to Detect)

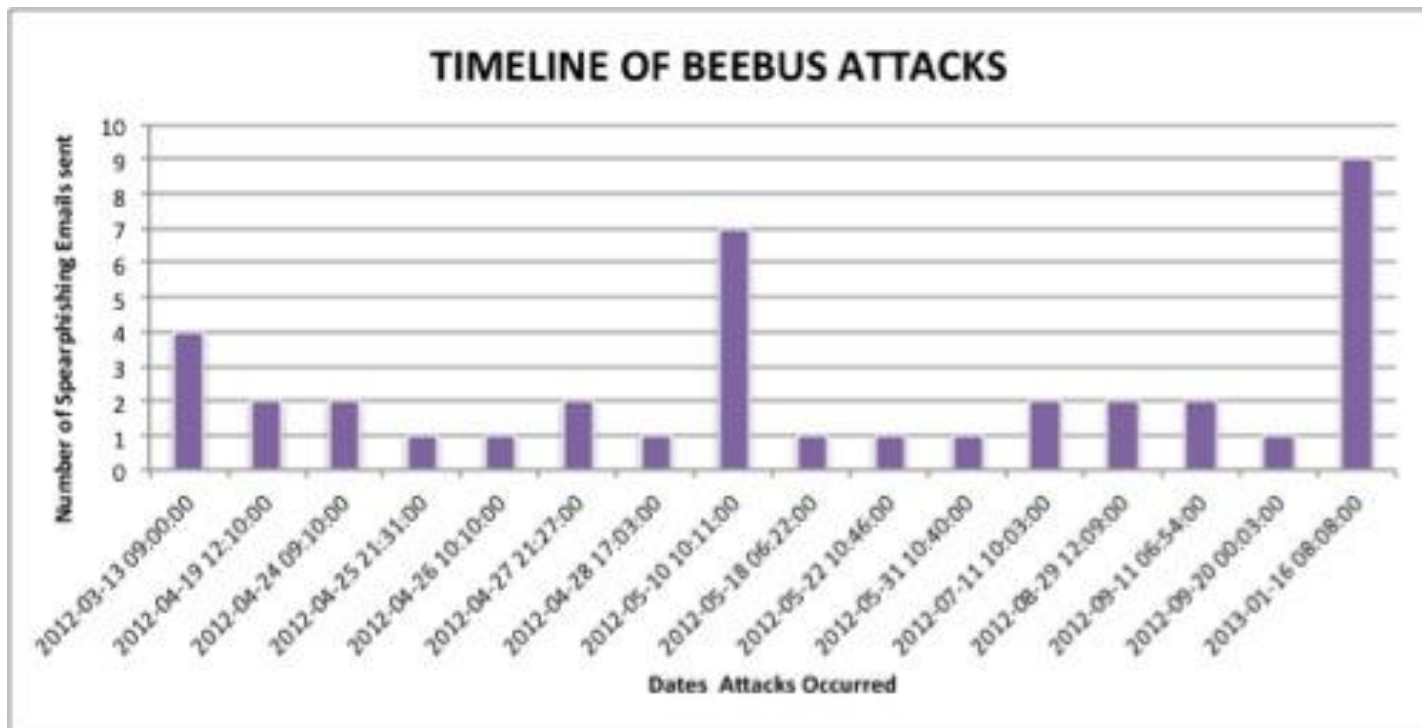
# Targeting a Large Taiwanese Technology Firm





# Attack Campaigns: Operation BeeBus

- ▶ Coordinated and sustained attacks on Aerospace and Defense contractors



# A New Model is Required

## Legacy Pattern-Matching Detection Model

**MATCH**

```
101011010101101000101110001
101010101011001101111100101
011001001001001000
100100111001010101010110
110100101101011010101000
```

- Signature-based
- Reactive
- Only known threats
- False positives

## New Virtual Execution Model



- Signature-less
- Dynamic, real-time
- Known/unknown threats
- Minimal false positives
- Dynamic Threat Indicator creations

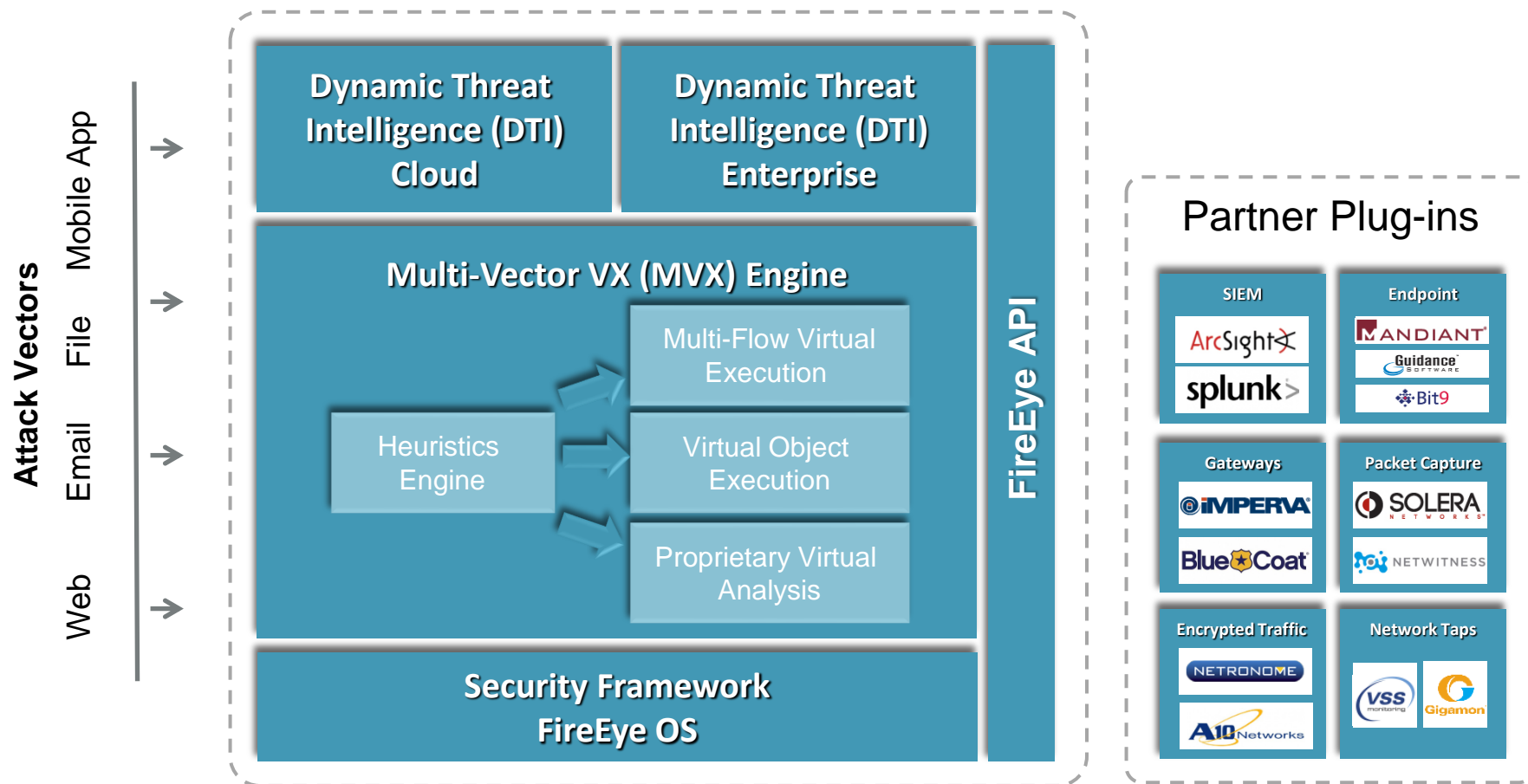
# With Dynamic Cloud Threat Intelligence



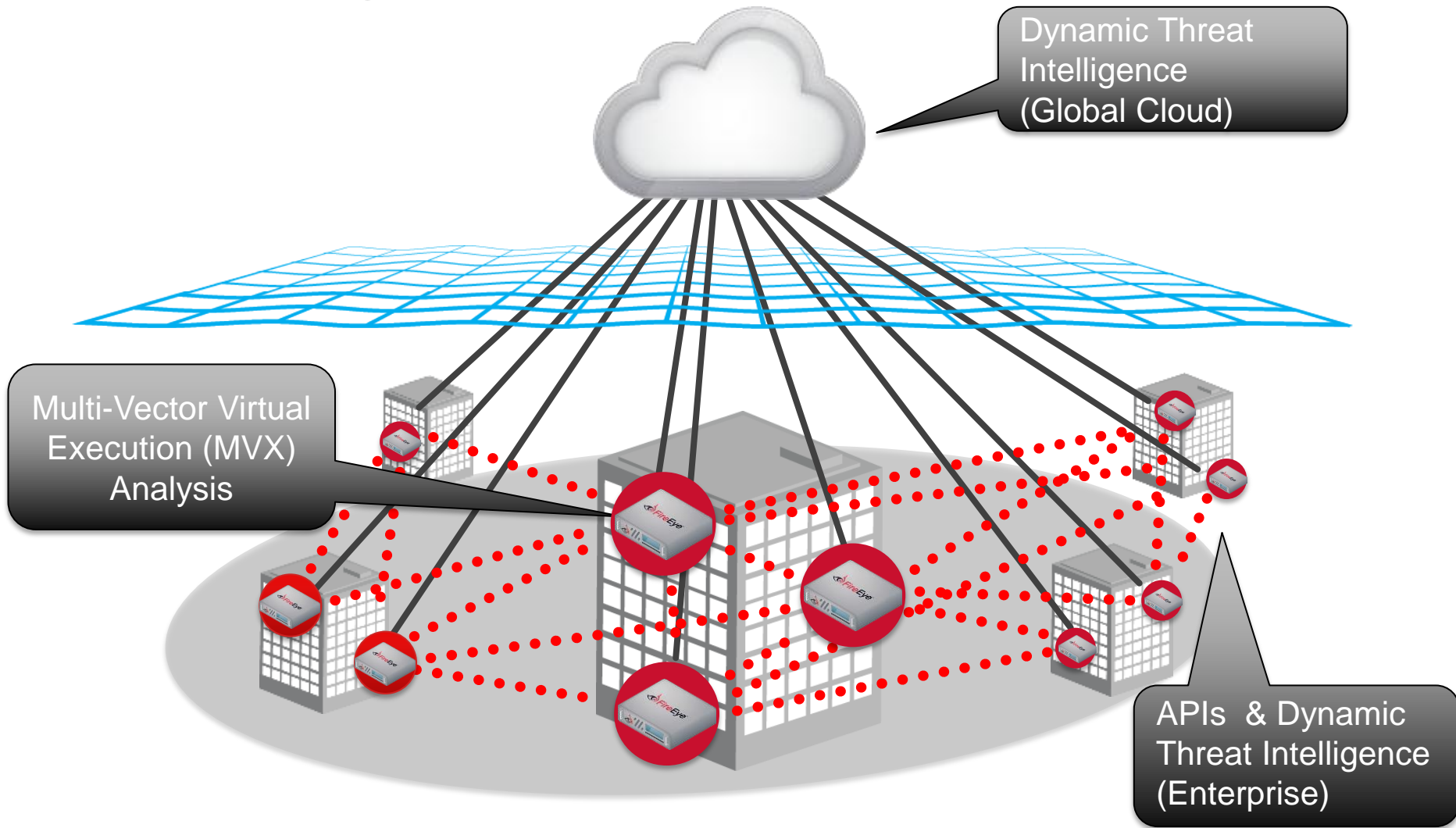
# 5 Design Principles of Next-Generation Threat Protection

- ▶ Signature-less detection engine
- ▶ Multi-vector coverage of attacks
- ▶ Multi-stage protection architecture
- ▶ Dynamic Threat intelligence for global sharing
- ▶ Dynamic Threat Intelligence for enterprise internal sharing with API's for validation/interdiction/remediation

# FireEye's DynamicThreat Protection Platform

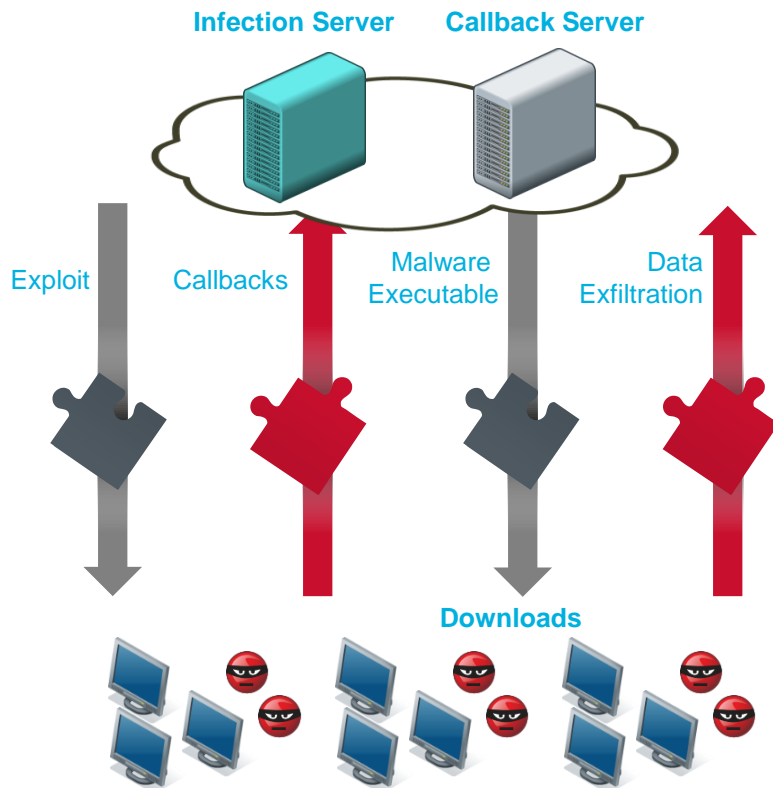


# Building Blocks of Our Fabric



# Advanced Analysis Techniques

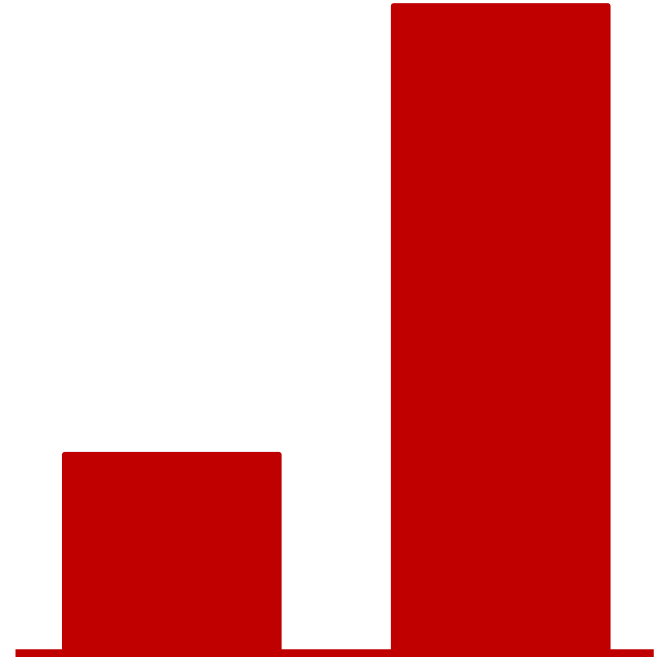
## Multi-flow Virtual Execution



- ▶ FireEye uses multi-flow virtual execution analysis to capture the full context of today's new breed of cyber attacks
- ▶ Stateful attack analysis enables customers to see full attack life cycle
- ▶ Point products only focus on a single attack object (e.g., malware executable), thereby missing the attack and full life cycle view

# The Rising Tide of Mobile Malware

- ▶ Diverse app markets with millions of apps, billions of app downloads
- ▶ Mobile an attractive target for malware
  - ▶ 50% of Android phones have unpatched vulnerabilities [2]
  - ▶ Mobile malware increased from 14,000 to 40,000 from July '11 to May '12 [3]



Sources:

[1] Managing cybersecurity risks: mobile and cloud open doors to opportunities and threats, Aug 2012

[2] Duo Security, X-Ray tool report, Sep 2012

[3] Cybersecurity Policy Report, Sep 2012



# Current Solutions

## ▶ Anti-virus tools

- ▶ Signature-based for known malware
- ▶ Easy to evade: code morphing, obfuscation



## ▶ MDM tools

- ▶ Little to no knowledge about app behaviors
- ▶ Can not reason about high-level security properties



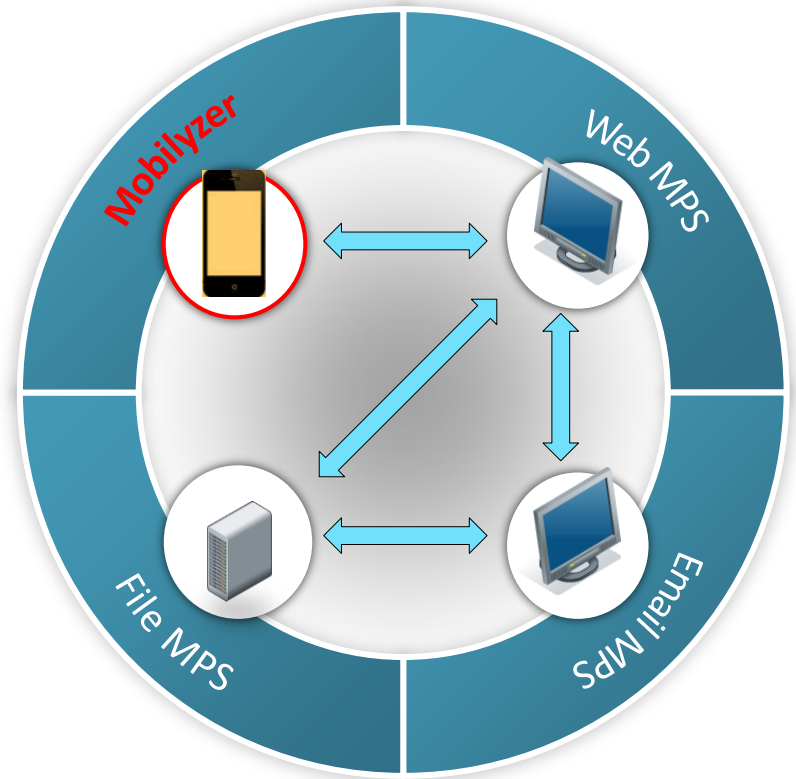
# Mobile Malware Malicious Behaviors

- ▶ Privacy violation
- ▶ Data theft
- ▶ Location tracking
- ▶ A/V recording

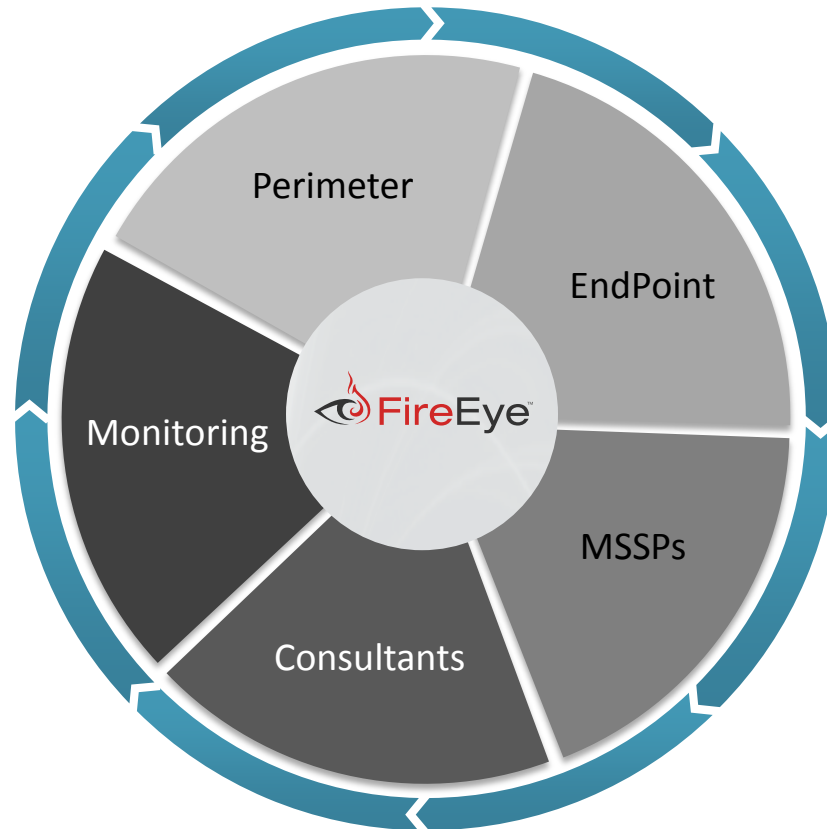


# FireEye Mobile Solution

- Mobile is now the latest vector supported by FireEye
- Flexible and extensible MVX engine to analyze app behaviors



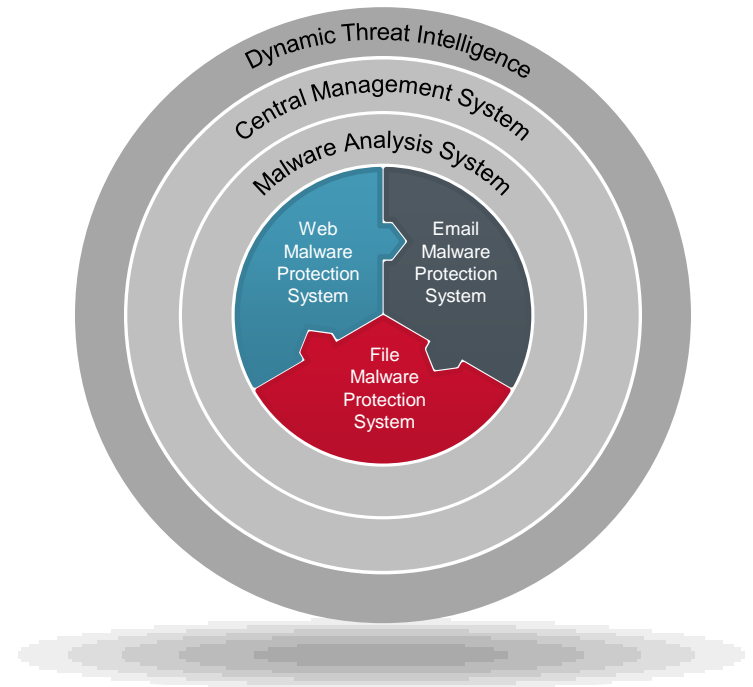
# FireEye Platform Partners



# Next-Generation Threat Protection Portfolio

- ▶ Protects across all major threat vectors, Web, email, file and mobile
- ▶ Protects against the lateral movement of malware within the enterprise
- ▶ Most comprehensive portfolio to stop the infiltration mechanisms of today's cyber attacks and its persistence

Complete Protection Against Next-Generation Threats



# Summary

- ▶ The new breed of attacks are more advanced and sophisticated, affecting all verticals and all segments
- ▶ Traditional defenses (NGFW, IPS, AV, and gateways) can't stop these attacks
- ▶ Real-time, integrated signature-less solution is required across Web, email, mobile, and file attack vectors

## Complete Protection Against Next-Generation Threats

