FireEye™

Security Reimagined

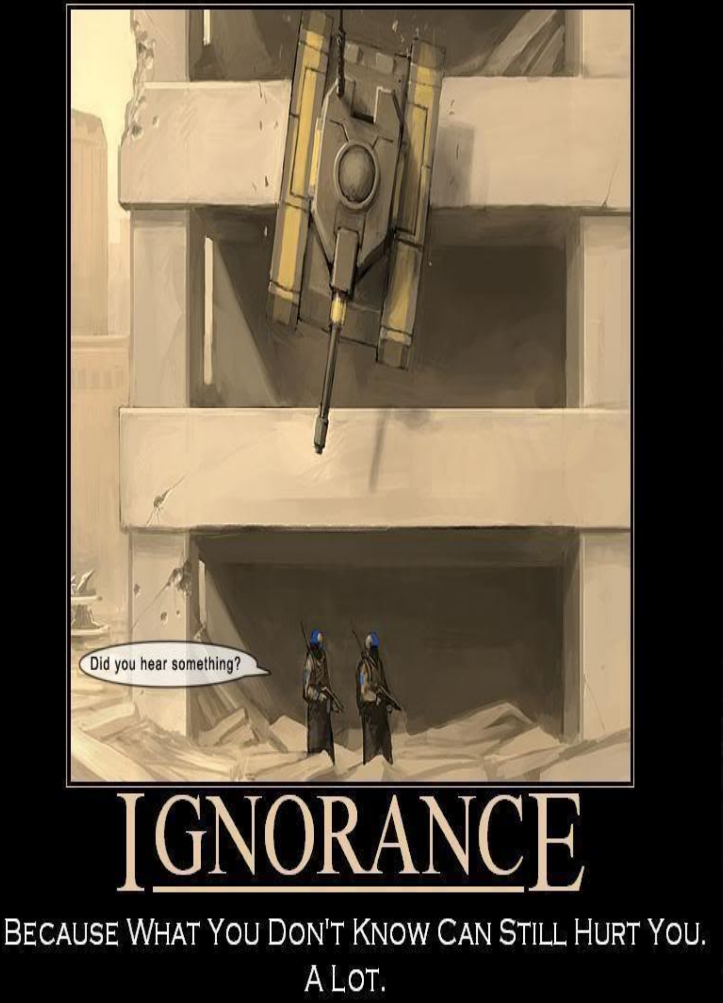
FireEye Continuous Threat Protection

Paolo Cecchi, Territory Manager Italy, FireEye

Paolo.cecchi@FireEye.com

May 2014

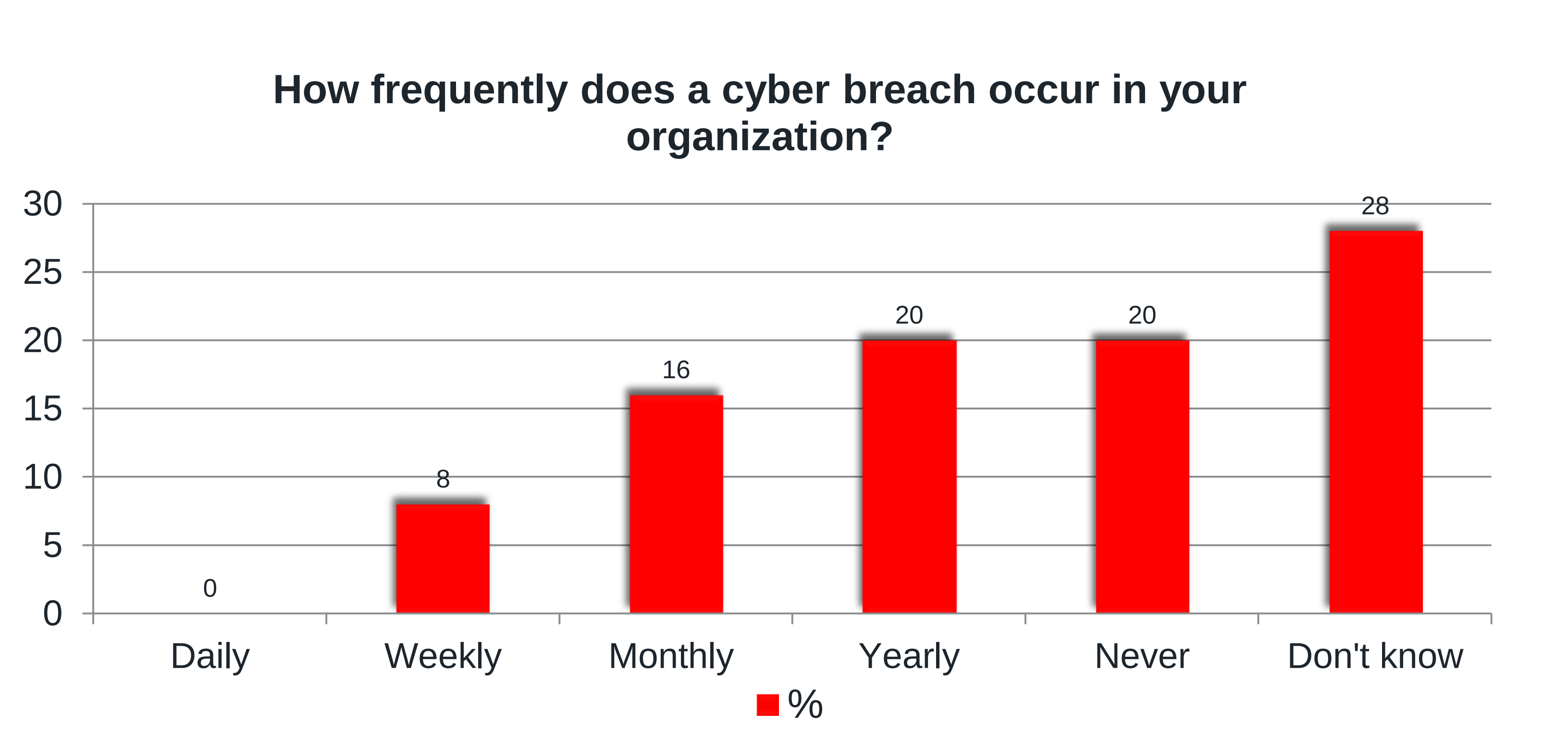
Cyber Defense or Resilience?



- 71.5% thought their security was between good to excellent

- 51% either “unsure” or said “NO” when asked if the technology they use would block a modern day attack

Ponemon Research: UK data 2103
Cyber Security in the Trenches


How frequently does a cyber breach occur in your organization?

Industry: Government (Federal)

31

FireEye PoV

100%

Customers Compromised

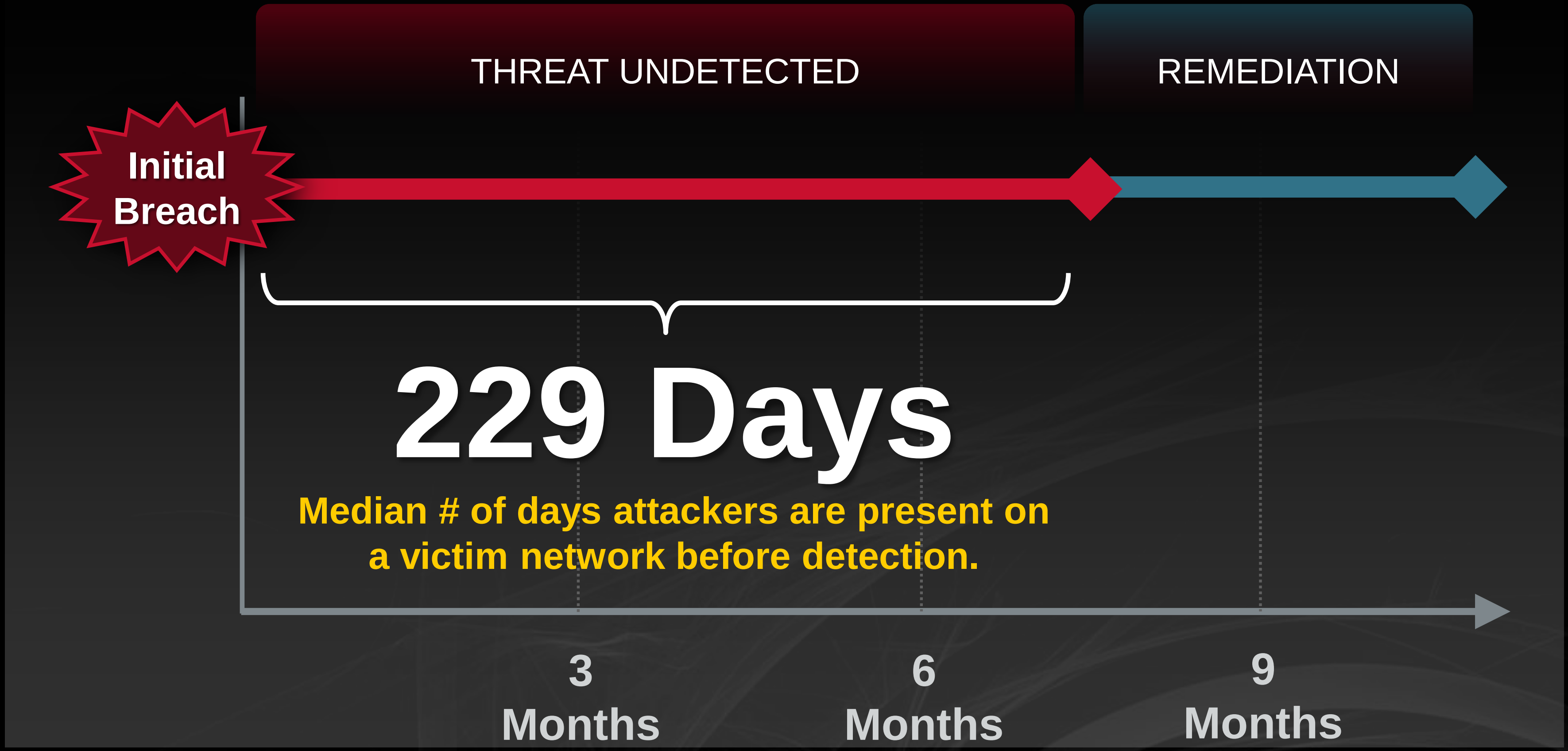
39%

Had APT

(Per Week)	Average	Max
Web Exploit	▼ 0.39	2.63
Malware Download	▼ 164.75	4939
Unique Malware	▼ 13.95	303.06
Unique Callback	▼ 350.44	11046.3
Impacted Hosts	▼ 352.55	11058.1

Top APT	Business Impact
Backdoor.APT. Houdini(25%)	Loss of sensitive information. Houdini is believed to be the developer's name of VBS-based RAT known to target international energy industry and take part in spammed email campaign.
Top Crimeware	**Business Impact**
Malware.Archive (68%)	Malware is discovered inside archive file (ZIP, RAR)
Malware.Binary (52%)	Loss of sensitive financial information, e.g. credit card, banking login

The High Cost of Being Unprepared



229 Days

Median # of days attackers are present on a victim network before detection.

67%

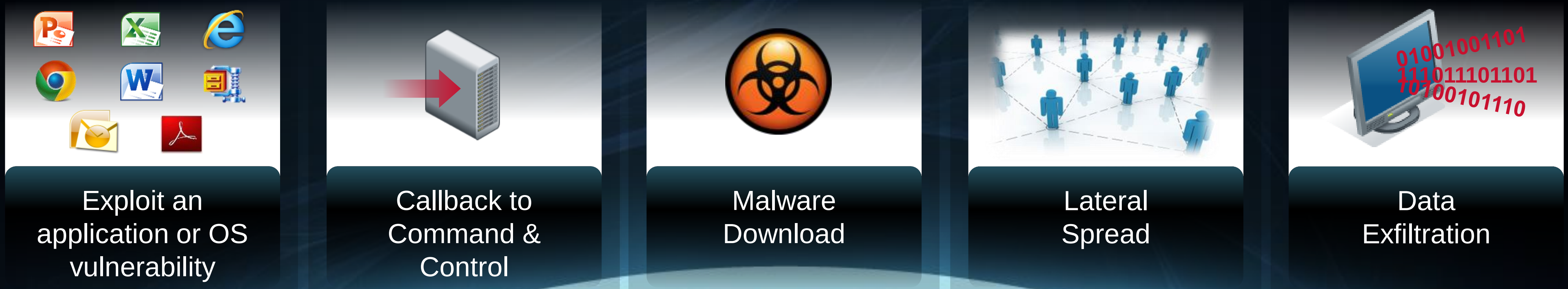
of Companies Learned They Were Breached from an External Entity

100%

of Victims Had Up-To-Date Anti-Virus Signatures

Source: M-Trends Report

Know The Adversary



Exploit an application or OS vulnerability

Callback to Command & Control

Malware Download

Lateral Spread

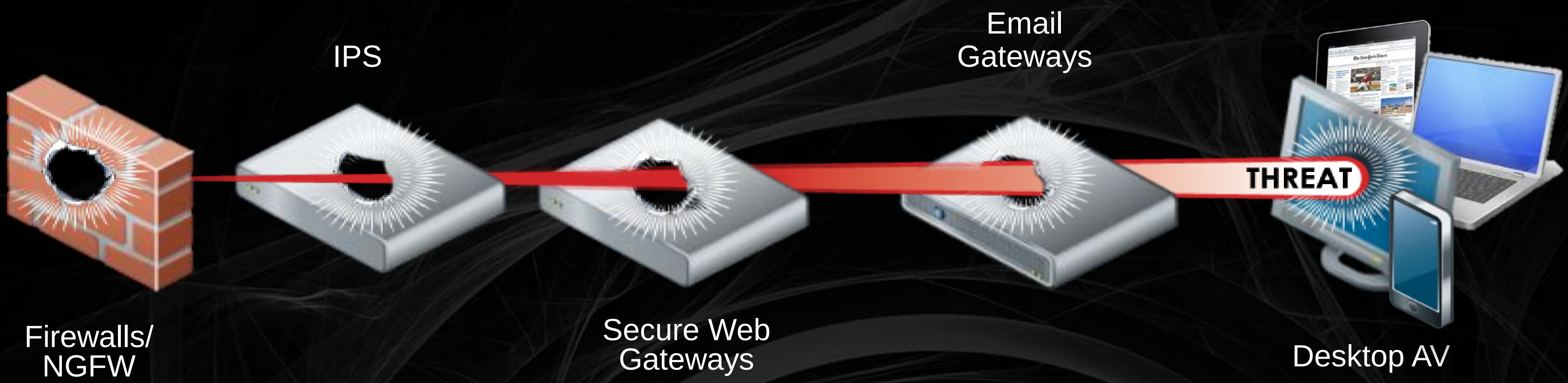
Data Exfiltration

Exploit detection critical

Every stage after the exploit can be hidden or obfuscated

“Defense-in-Depth” is Failing

The New Breed of Attacks Evade Signature-Based Defenses



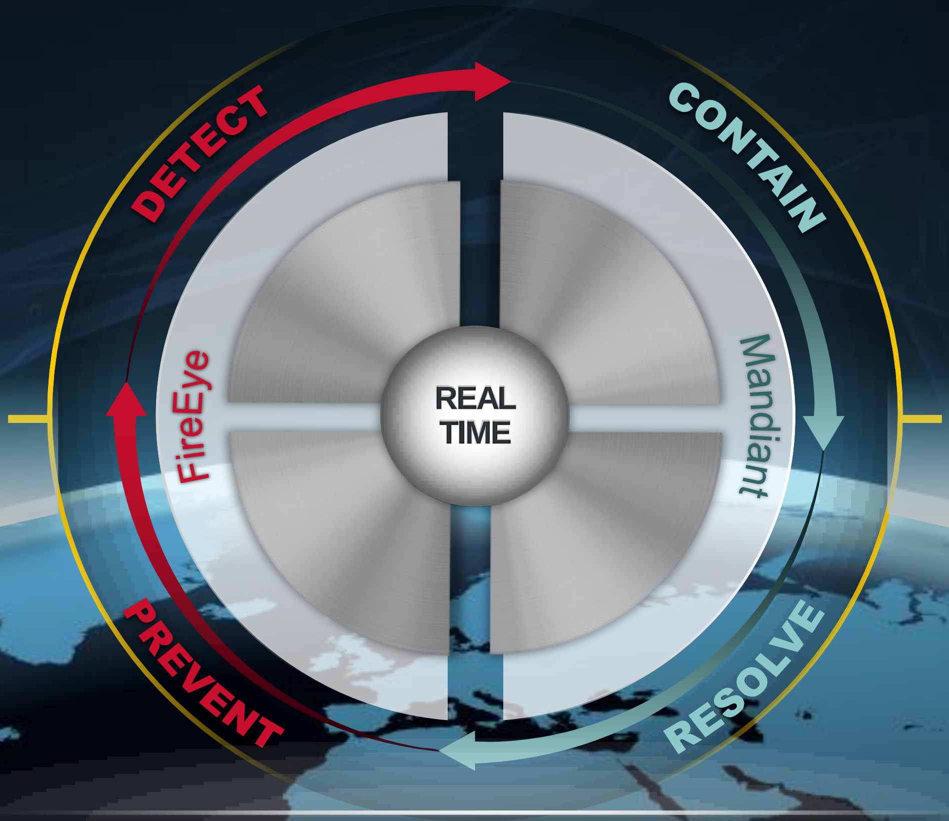
>95% organizations compromised*

* *Based on data from customer evaluations conducted by FireEye*

The Objective: “Continuous Threat Protection”

Time to Detect

Time to Fix



Prevent

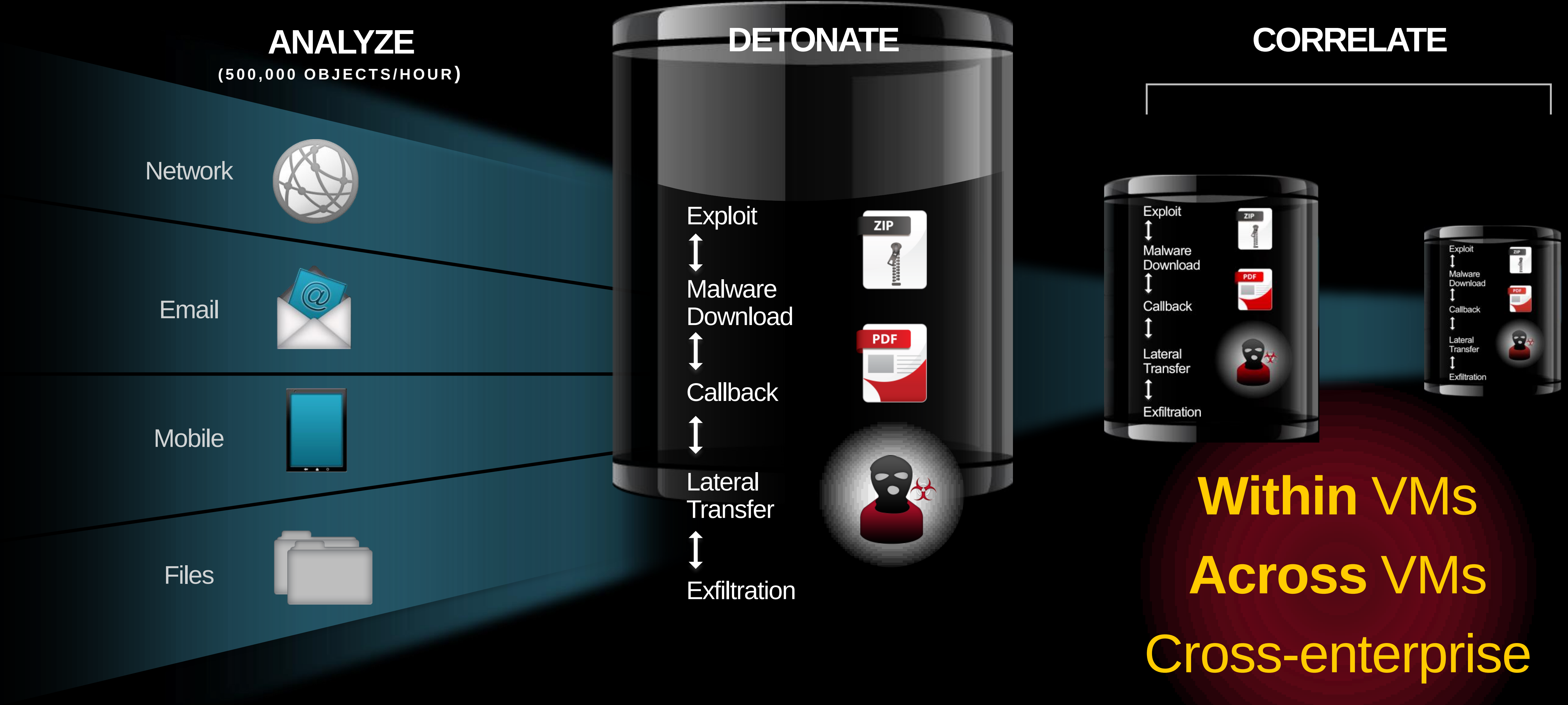
THEFT OF ASSETS & IP

COST OF RESPONSE

DISRUPTION TO BUSINESS

REPUTATION RISK

FireEye’s Technology: **State of the Art Detection**



ANALYZE

(500,000 OBJECTS/HOUR)

Network

Email

Mobile

Files

DETONATE

Exploit
↕
Malware Download
↕
Callback
↕
Lateral Transfer
↕
Exfiltration

CORRELATE

Within VMs

Across VMs

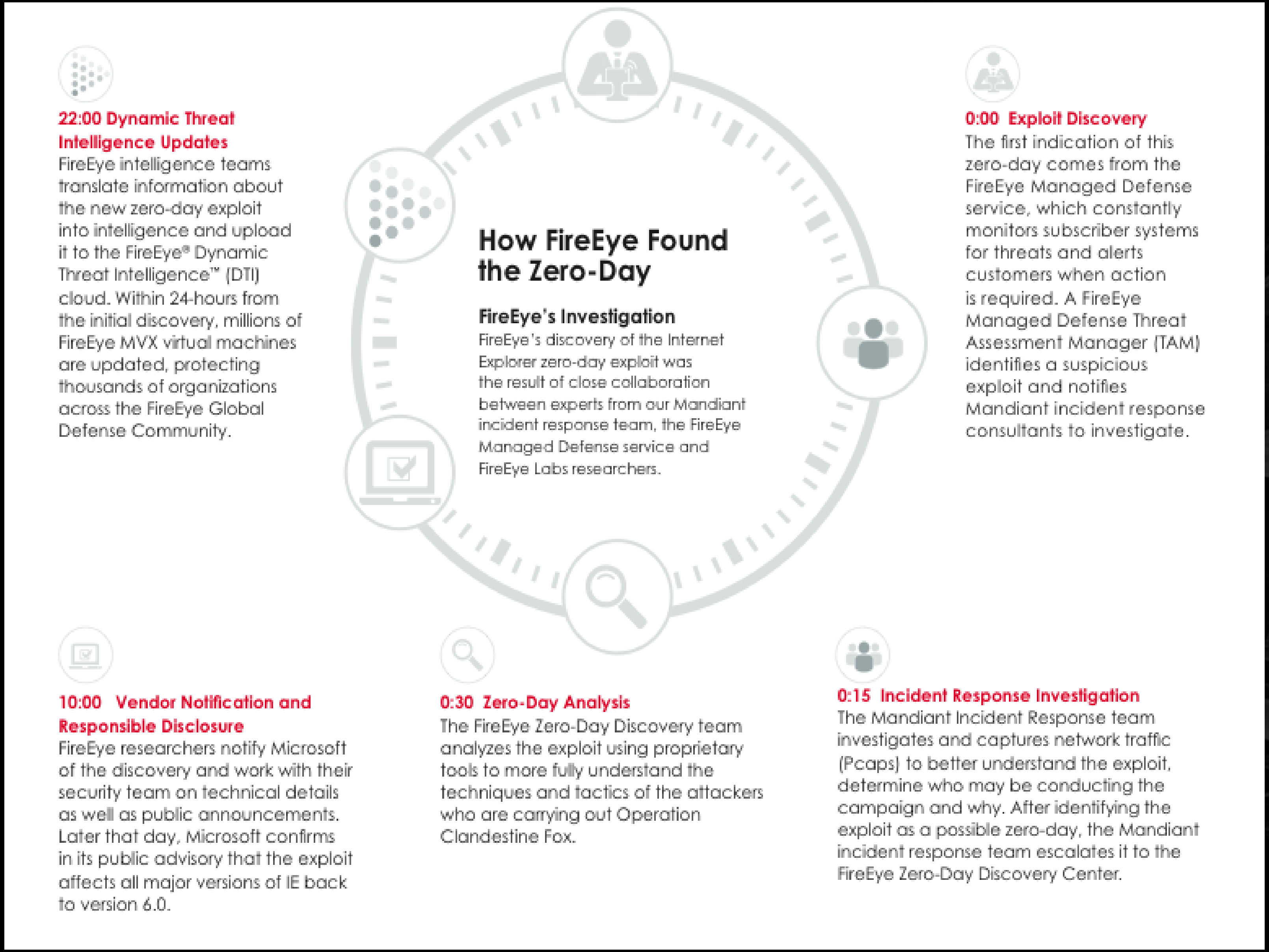
Cross-enterprise

Why Trust FireEye?

11 of 13
Zero Days
from 2013
discovered by FireEye

First to detect malware
Over 80%
of the times
(compared to traditional
AV engines)

The Operation Clandestine Fox Zero-Day



How FireEye Found the Zero-Day

FireEye's Investigation

FireEye's discovery of the Internet Explorer zero-day exploit was the result of close collaboration between experts from our Mandiant incident response team, the FireEye Managed Defense service and FireEye Labs researchers.

0:00 Exploit Discovery

The first indication of this zero-day comes from the FireEye Managed Defense service, which constantly monitors subscriber systems for threats and alerts customers when action is required. A FireEye Managed Defense Threat Assessment Manager (TAM) identifies a suspicious exploit and notifies Mandiant incident response consultants to investigate.

0:15 Incident Response Investigation

The Mandiant Incident Response team investigates and captures network traffic (Pcaps) to better understand the exploit, determine who may be conducting the campaign and why. After identifying the exploit as a possible zero-day, the Mandiant incident response team escalates it to the FireEye Zero-Day Discovery Center.

0:30 Zero-Day Analysis

The FireEye Zero-Day Discovery team analyzes the exploit using proprietary tools to more fully understand the techniques and tactics of the attackers who are carrying out Operation Clandestine Fox.

10:00 Vendor Notification and Responsible Disclosure

FireEye researchers notify Microsoft of the discovery and work with their security team on technical details as well as public announcements. Later that day, Microsoft confirms in its public advisory that the exploit affects all major versions of IE back to version 6.0.

22:00 Dynamic Threat Intelligence Updates

FireEye intelligence teams translate information about the new zero-day exploit into intelligence and upload it to the FireEye® Dynamic Threat Intelligence™ (DTI) cloud. Within 24-hours from the initial discovery, millions of FireEye MVX virtual machines are updated, protecting thousands of organizations across the FireEye Global Defense Community.

On April 26th FireEye discovered a zero-day exploit affecting approximately 25% of the web browsers used on the Internet.

The zero-day exploits a vulnerability in Internet Explorer. While attackers targeted versions IE9 through IE11, the vulnerability affects IE6 through IE11.

Microsoft has assigned CVE-2014-1776 to the vulnerability.

The Italian National Plan for Cyberspace Protection

OG1 - STRENGTHENING OF INTELLIGENCE, POLICE, CIVIL AND MILITARY DEFENSE CAPABILITIES

1.2 Strengthening of the capability to collect, process, and disseminate the information (cyber intelligence)

a) Strengthen cyber intelligence capabilities
b) Develop capabilities and procedures to monitor volumes of traffic and to correlate events with the goal of enhancing the capability to promptly detect anomalies associated with cyber threats and attacks
c) Implement early warning procedures

1.3 Development of capabilities to contrast cyber threats

a) Improve the capability to attribute a cyber attack
b) *Cyber Situational Awareness*
c) Facilitate agreements aimed at promoting info-sharing between the relevant public Administrations and the private sector, along the lines of already existing norms
d) Strengthen the capability to respond to cyber incidents and to contrast cyber crime

1.5 Development of digital forensics analysis capabilities

a) Strengthen and disseminate the capability to acquire data through digital forensics techniques
b) Increase “live digital forensics” capabilities
c) Strengthen data analysis capabilities
d) Develop “post mortem” digital analysis

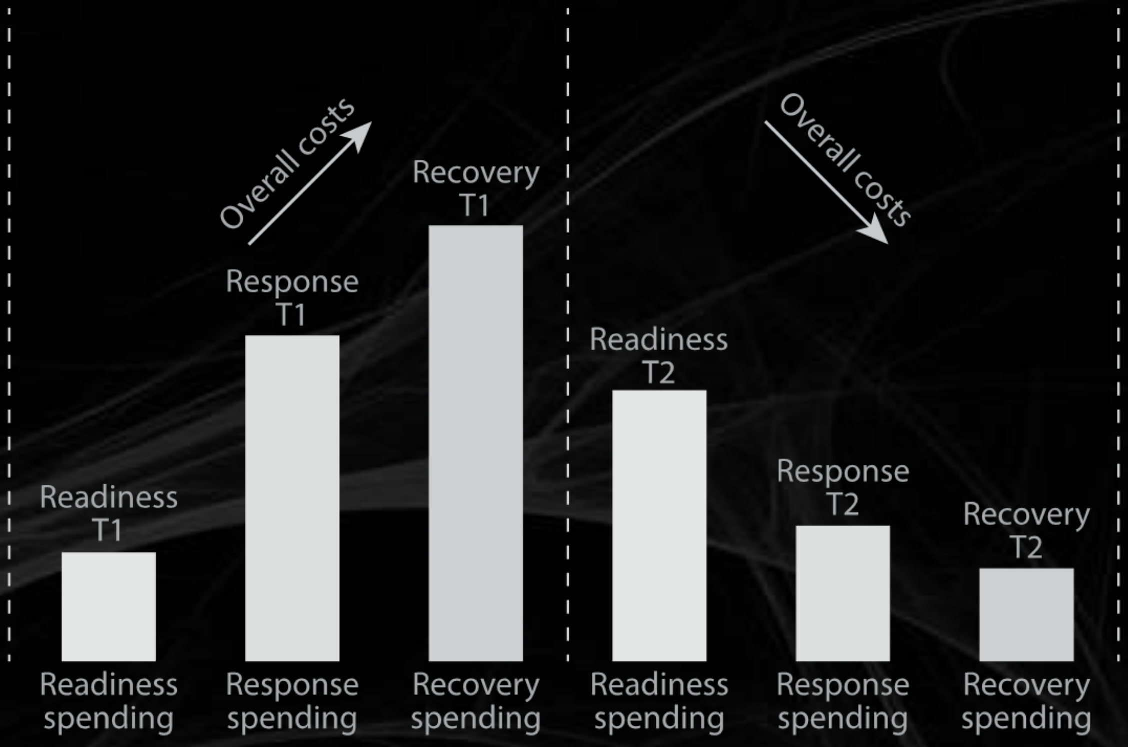
Improved readiness reduces response and recovery costs

Readiness includes all preparation designed to protect against breach events. Investments here are designed to prepare your organization against attacks and potential breaches. This includes activities such as, but not limited to, system patching, data loss prevention, secure network architecture, risk assessments, and security awareness campaigns.

Response describes immediate efforts to reduce the impact during a breach. Efforts in this category are for defense of the organization in an actual security event. This includes spending for activities such as system quarantine and firewall or DNS reconfiguration.

Recovery investments are penalties and expenditures required to rebuild value after an event. Recovery spending is for activities directly related to the cleanup from an event. This includes system replacement, data cleansing, data restoration, disciplinary action, post-event reviews, and budget allocated to pay legal costs and fines.

Figure 2 Changes In Readiness Spending Impact Overall Security Spending



Note: Assume non-zero-day event(s)

103881

Source: Forrester Research, Inc.

Forrester: Measure information Security effectiveness — information Security economics 103 – Sept 2013

FireEye™

Thank You

Security Reimagined