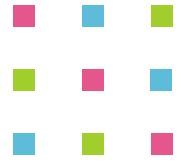
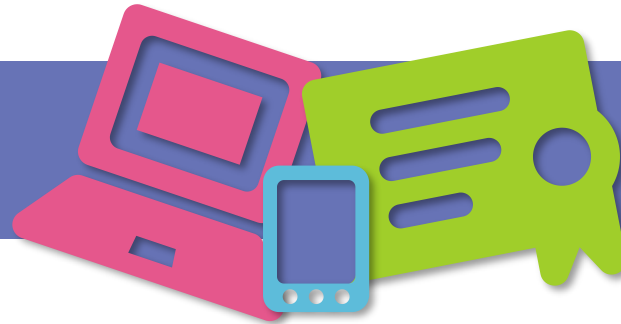


# SECURITY 2015



23. ročník konference o bezpečnosti v ICT



## **Designing an Adaptive Defense Security Architecture**

George Chiorescu

FireEye



# Designing an Adaptive Security Architecture

## ■ Key Challenges

- Existing blocking and prevention capabilities are insufficient to protect against motivated, advanced attackers.
- Most organizations continue to overly invest in prevention-only strategies.
- Limited visibility in advanced attacks.
- Because enterprise systems are under continuous attack and are continuously compromised, an ad hoc approach to "incident response" is the wrong mindset.

**Source: Gartner's Report, Designing an Adaptive Security Architecture.**

Available at [https://www2.fireeye.com/GTM\\_ADV\\_RPT\\_Gartner-Designing-an-Adaptive-Security-Architecture.html](https://www2.fireeye.com/GTM_ADV_RPT_Gartner-Designing-an-Adaptive-Security-Architecture.html)



# Designing an Adaptive Security Architecture

## ■ Recommendations

- Shift from „Incident response“ to „Continuous response“.
- Adopt an adaptive security architecture.
- Spend less on prevention; invest in detection, response and predictive capabilities.
- Develop a security operations center that supports continuous monitoring.

**Source: Gartner's Report, Designing an Adaptive Security Architecture.**

Available at [https://www2.fireeye.com/GTM\\_ADV\\_RPT\\_Gartner-Designing-an-Adaptive-Security-Architecture.html](https://www2.fireeye.com/GTM_ADV_RPT_Gartner-Designing-an-Adaptive-Security-Architecture.html)

# UNRESTANDING THE ATTACK

ATTACKERS UTILIZE MULTIPLE VECTORS  
AND MULTIPLE FLOWS TO COMPLETE THEIR MISSION



DETECTING THE EXPLOIT IS KEY SINCE EVERY PHASE AFTER THAT CAN BE ENCRYPTED BY THE ATTACKER



# ABOUT THE ADVERSARY

IT'S A "WHO,"  
NOT A "WHAT"



THERE'S A HUMAN AT A  
KEYBOARD

HIGHLY TAILORED AND  
CUSTOMIZED ATTACKS

TARGETED SPECIFICALLY AT  
YOU

THEY ARE  
PROFESSIONAL,  
ORGANIZED AND  
WELL FUNDED



NATION-STATE SPONSORED

ESCALATE SOPHISTICATION OF  
TACTICS AS NEEDED

RELENTLESSLY FOCUSED ON  
THEIR OBJECTIVE

IF YOU KICK  
THEM OUT THEY  
WILL RETURN



THEY HAVE SPECIFIC OBJECTIVES

THEIR GOAL IS LONG-TERM  
OCCUPATION

PERSISTENCE TOOLS ENSURE  
ONGOING ACCESS





# THE IMPACT OF THE TRADITIONAL MODEL

## 229 DAYS

MEDIAN NUMBER OF DAYS BEFORE DETECTION

## 32

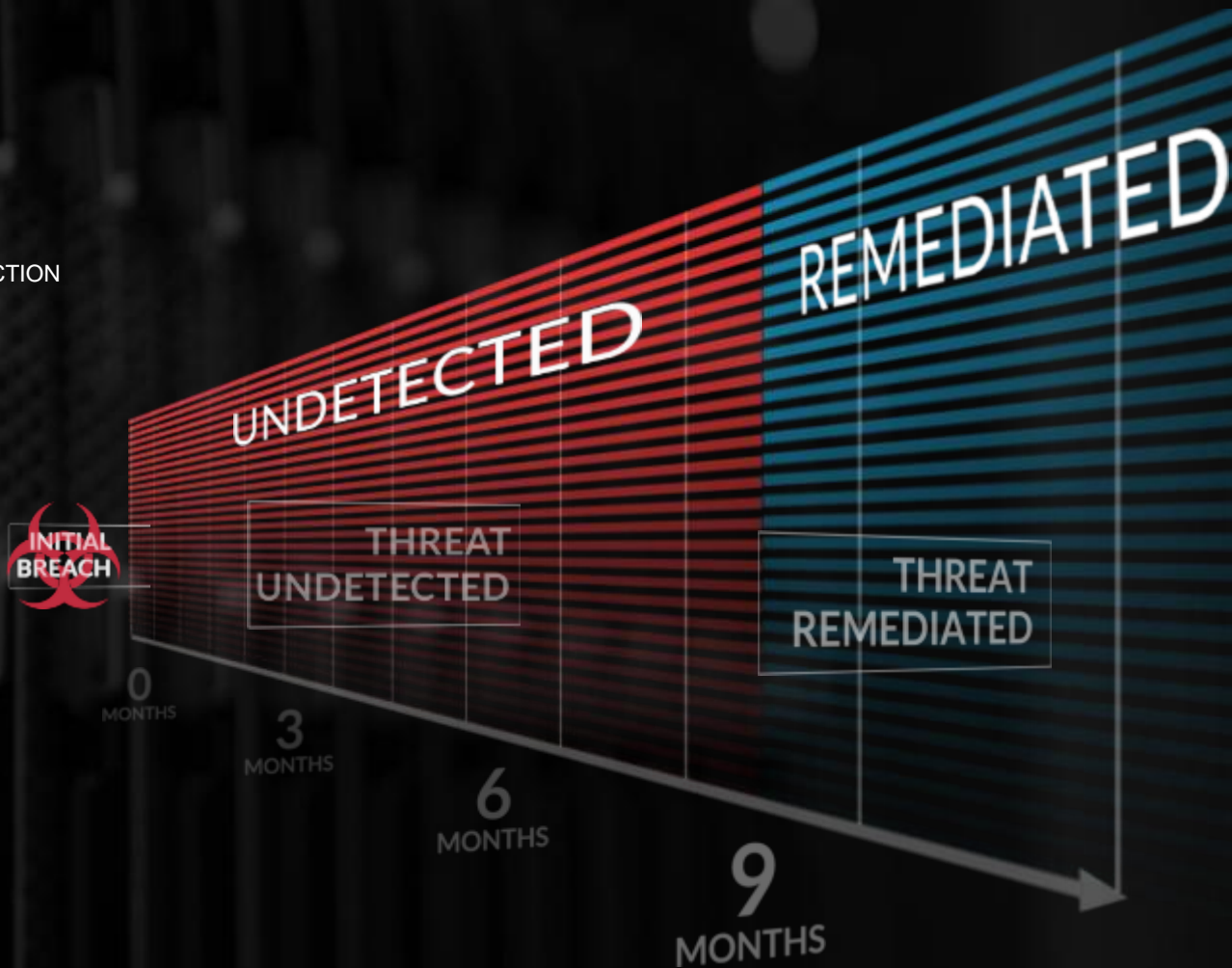
DAYS TO RESPOND TO A BREACH

## 67%

OF COMPANIES LEARNED THEY WERE BREACHED FROM AN EXTERNAL ENTITY

## 100%

OF VICTIMS HAD FIREWALLS OR UP-TO-DATE ANTI-VIRUS SIGNATURES



SOURCE: MANDIANT M-TRENDS REPORT, PONEMON COST OF DATA BREACH STUDY



# THE IMPACT OF THE TRADITIONAL MODEL



**1216**

PoV  
Customers



**63**

Countries



**20+**

Industries



**97%**

Customers  
Compromised



**27%**

Had APT



# THE IMPACT OF THE TRADITIONAL MODEL



Financial  
**18%**



Government  
**16%**



Chemical &  
Manufacturing  
**7%**



High-Tech  
**7%**



Consulting  
**7%**



Energy  
**6%**



Retail  
**5%**



Healthcare  
**4%**



Others  
(12+)

Others  
**30%**





# THE IMPACT OF THE TRADITIONAL MODEL



Exploit



Malware  
Download



Command  
and Control

97%

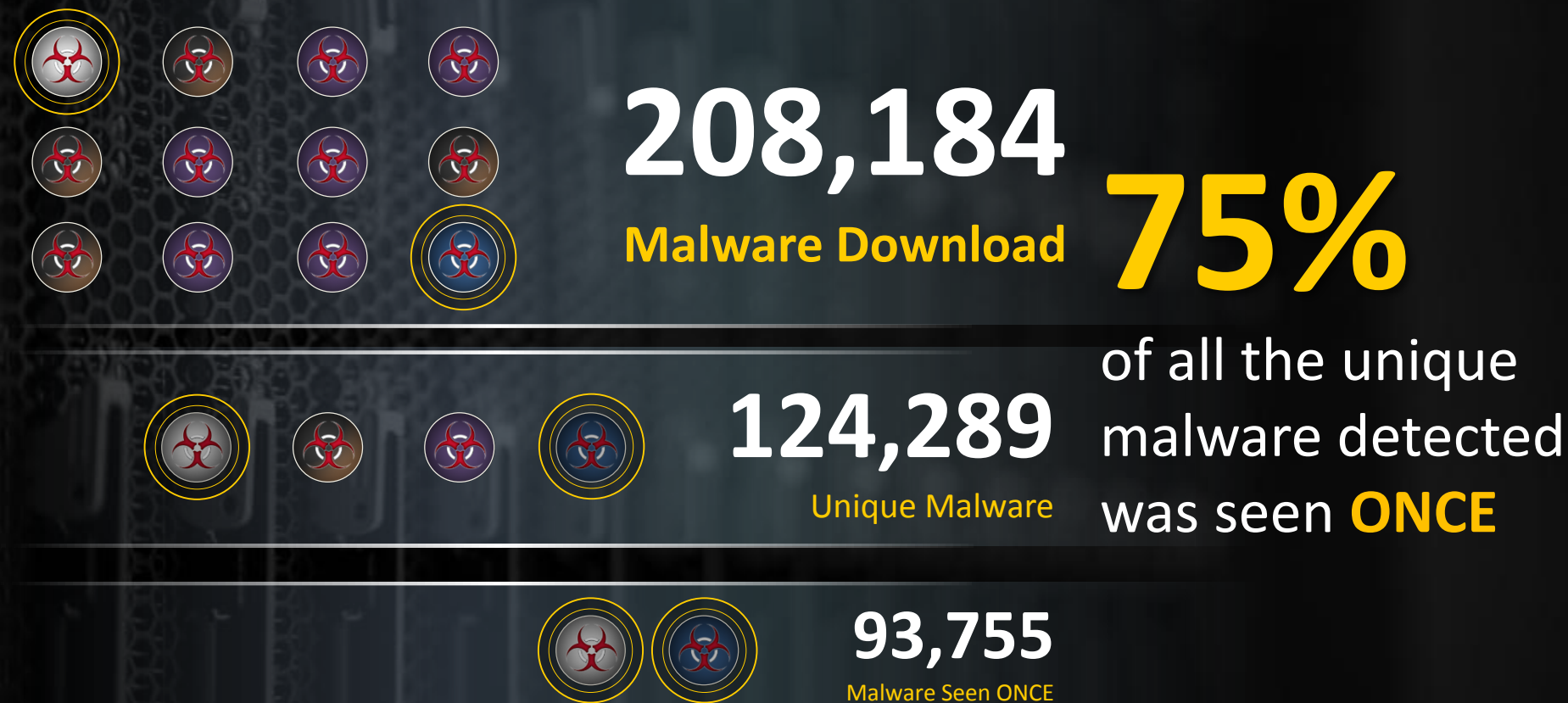
of PoV customers were compromised  
(attacks went through customers' defense)

75%

of PoV customers had  
CnC communication



# Today's Malware is Highly Targeted





# The Adaptive Defense Security Model

## DETECT

SIGNATURE-LESS AND MULTI FLOW  
VIRTUAL MACHINE BASED APPROACH  
THAT LEVERAGES SUPERIOR THREAT  
INTELLIGENCE

## PREVENT

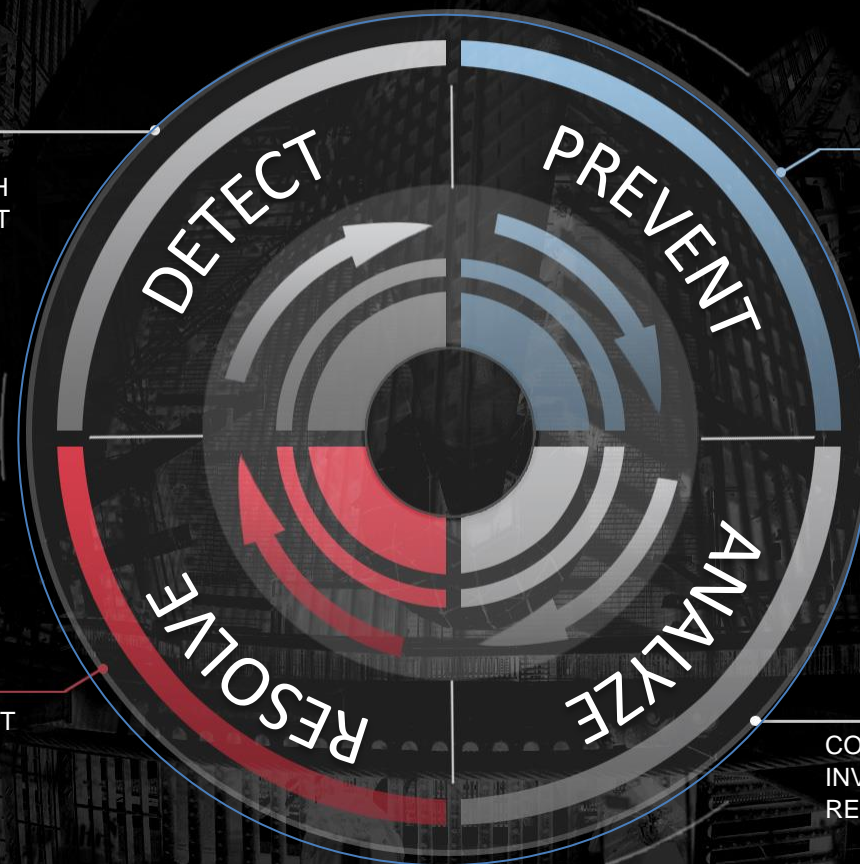
MULTI-VECTOR INLINE KNOWN AND  
UNKNOWN THREAT PREVENTION

## RESOLVE

REMEDIATION SUPPORT AND THREAT  
INTELLIGENCE TO RECOVER AND  
IMPROVE RISK POSTURE

## ANALYZE

CONTAINMENT, FORENSICS  
INVESTIGATION AND KILL CHAIN  
RECONSTRUCTION





# The Adaptive Defense Security Model

## DETECTION AND PREVENTION – TECHNOLOGY



PURPOSE-BUILT FOR SECURITY

HARDENED HYPERVISOR

SIGNATURE-LESS

EXPLOIT BASED DETECTION, NOT JUST FILE

FINDS KNOWN AND UNKNOWN THREATS

MULTI-VECTOR

PERFORMANCE

EFFICACY



# The Adaptive Defense Security Model

## DETECTION AND PREVENTION – TECHNOLOGY







# The Adaptive Defense Security Model

ENDPOINT SECURITY ARCHITECTURE MUST BE AGILE, FLEXIBLE, AND DEEPLY INTEGRATED.

## ADAPTIVE DEFENSE



### DETECT AND PREVENT

- Advanced Threat Detection (Signature-Less, Tamper resistant)
- Threat Prevention Across All Endpoints



### ANALYZE AND RESPOND

- Threat Intel (Network, Cloud)
- Endpoint Live Response (Validate, Contain, Search, Sweep)

## NEXT GENERATION ENDPOINT SOLUTION REQUIREMENTS

- DETECTION TO RESPONSE: detection, validation, containment, and remediation
- PROACTIVE AND ADAPTIVE: searching, sweeping, and advanced detection of unknown threats
- COMPREHENSIVE ENDPOINTS: on premise, remote and Mobile endpoints
- REAL-TIME INTELLIGENCE: real-time intelligence feeds from cloud and network alerts



# The Adaptive Defense Security Model

DETECTION AND PREVENTION – INTELLIGENCE & EXPERTISE

**50B+**

VM ANALYSIS PER DAY

**400K**

**UNIQUE**

MALWARE SAMPLES  
REVIEWED AND  
PROCESSED EACH DAY

**100K+**

HOURS OF HIGH  
PROFILE INCIDENT  
RESPONSE PER YEAR

**10 YEARS**

OF BEING THE INDUSTRY  
LEADING INCIDENT  
RESPONSE PROVIDER

**1B+**

EVENTS PER DAY  
ANALYTICS TO IDENTIFY  
NON-MALWARE BASED  
MALICIOUS ACTIVITY



# The Adaptive Defense Security Model

## INTELLIGENCE

DISCOVERED 16 OF THE LAST 25 ZERO-DAYS  
“FRONT LINE” INTEL FROM INCIDENT  
RESPONSE  
MILLIONS OF NETWORK & ENDPOINT SENSORS  
HUNDREDS OF INTEL AND MALWARE EXPERTS  
HUNDREDS OF THREAT ACTOR PROFILES

## TECHNOLOGY

IDENTIFIES KNOWN, UNKNOWN, AND NON  
MALWARE BASED THREATS

INTEGRATED TO PROTECT ACROSS ALL MAJOR  
ATTACK VECTORS

PATENTED VIRTUAL MACHINE TECHNOLOGY

## EXPERTISE

“GO-TO” RESPONDERS FOR SECURITY  
INCIDENTS

HUNDREDS OF CONSULTANTS AND ANALYSTS  
UNMATCHED EXPERIENCE WITH ADVANCED  
ATTACKERS



# SECURITY 2015



23. ročník konference o bezpečnosti v ICT

## Děkujeme za pozornost.

George Chiorescu

FireEye

George.Chiorescu@FireEye.com

