



# The Importance of Threat-Centric Security

Nikos Mourtzinos, CCIE #9763  
Security Product Specialist  
Global Security Sales Organization

April 2015

# Changing Business Models

## Any Device to Any Cloud



salesforce.com  
Success On Demand™

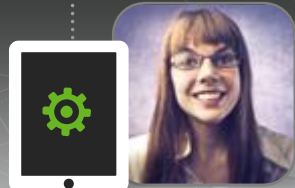
box



Google™



SkyDrive





## 2015 Annual Security Report

# Cisco 2015 Annual Security Report

Now available:

[cisco.com/go/asr2015](http://cisco.com/go/asr2015)

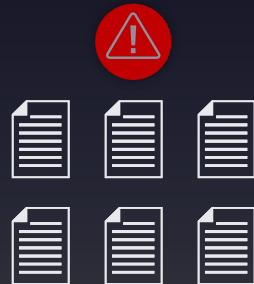
# Impact of a Breach

Breach occurs



START

**60%** data in breaches is stolen in **hours**



HOURS

**54%** of breaches remain undiscovered for **months**



MONTHS

Information of up to **750 million** individuals on the black market over last three **years**



YEARS

Source: Verizon Data Breach Report 2014

# Global Cybercrime Market



## WELCOME TO THE HACKERS' ECONOMY

# The Security Problem



Changing  
Business Models



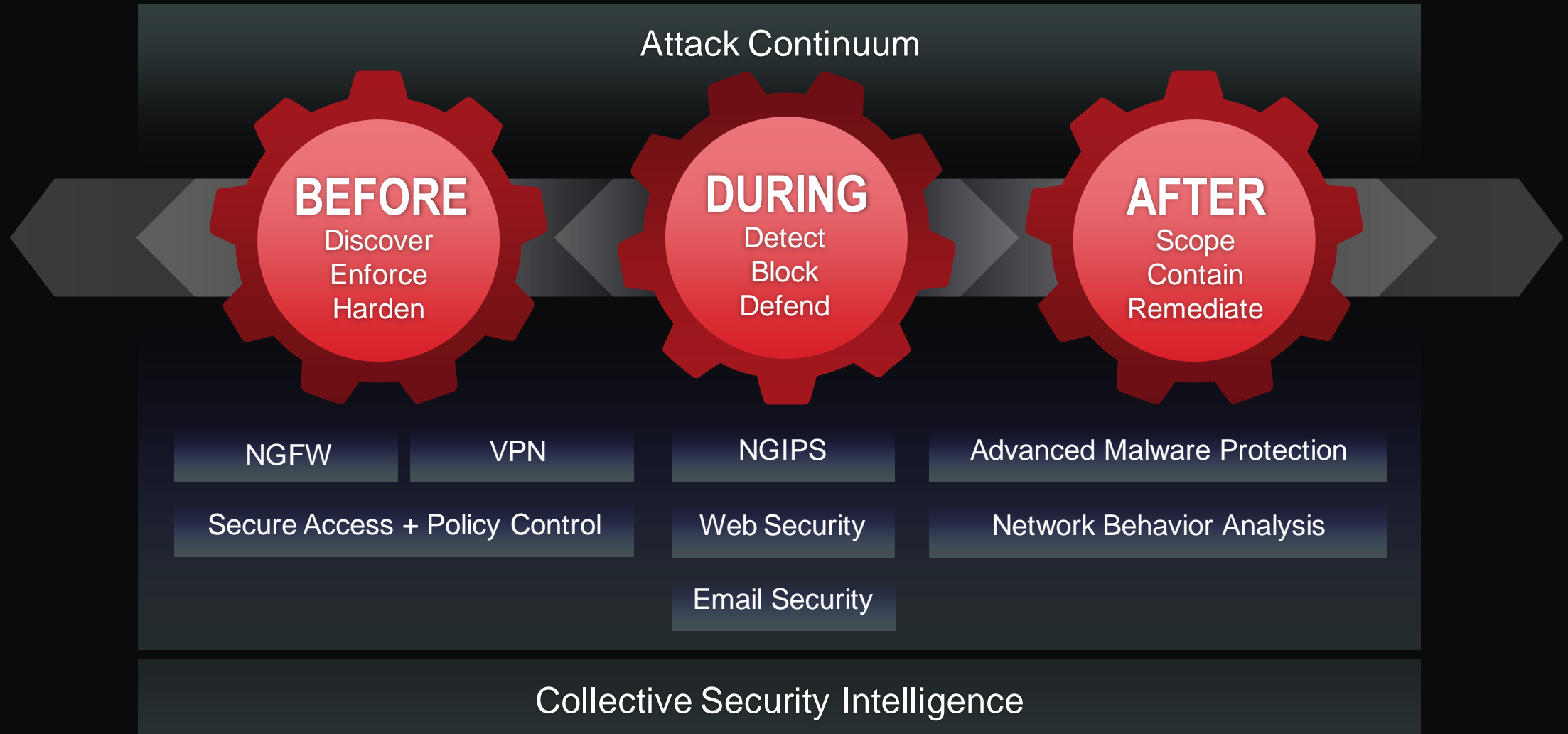
Dynamic  
Threat Landscape



Complexity  
and Fragmentation



# The Threat-Centric Security Model



# Enhanced Security & Simplifies Operations & Cost Savings

## Superior Network Visibility



Servers, hosts, Mobiles  
Applications, OS, Vulnerabilities,

## Automated Tuning



Adjust IPS policies automatically  
based on network changes

## Impact Assessment & Correlation



Threat correlation reduces  
actionable events by up to 99%

## Advanced Malware Protection



Analyses files to block malware

## Remediation



Continuous Analysis,  
Trajectory

## Indications of Compromise



Warning indicator to more rapidly  
remediate threats



# Superior Network Visibility

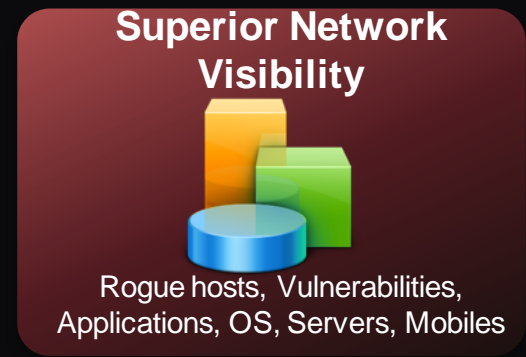
## Categories

Hosts  
Network Servers  
Routers & Switches  
Mobile Devices  
Printers  
VoIP Phones  
Virtual Machines  
Operating Systems  
Applications (Web , Client etc)  
Users  
File Transfers  
Command & Control Servers  
Threats  
Vulnerabilities



*You can't protect  
what you can't see*

Real-time notifications of  
changes



# Automated Tuning

## Automated Tuning



Adjust IPS policies automatically based on network changes

- Automated Recommended Rules based on Customer's Infrastructure
- Automated IPS Policies based on Changes
- Simplifies Operations & Reduces Costs

### NSS IPS Test Key Findings:

Protection varied widely between **31%** and **98%**.  
**Tuning is required**, and is **most important** for remote attacks against servers and their applications.


**Organizations that do not tune could be missing numerous "catchable" attacks.**

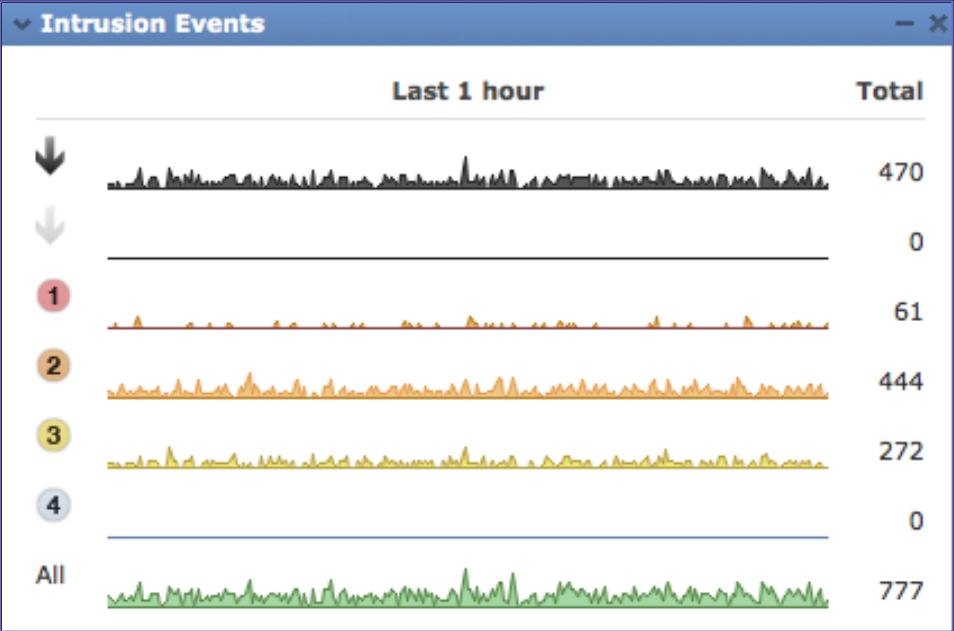


# Impact Assessment & Correlation

Automatically Correlates  
all intrusion events

Impact Assessment & Correlation





**Impact Assessment**  
Threat correlation reduces actionable events

IMPACT FLAG	ADMINISTRATOR ACTION	WHY
 1	Act Immediately; Vulnerable	Event corresponds with vulnerability mapped to host
 2	Investigate; Potentially Vulnerable	Relevant port open or protocol in use, but no vulnerability mapped
 3	Good to Know; Currently Not Vulnerable	Relevant port not open or protocol not in use
 4	Good to Know; Unknown Target	Monitored network, but unknown host
 0	Good to Know; Unknown Network	Unmonitored network

# Advanced Malware Protection

## Advanced Malware Protection



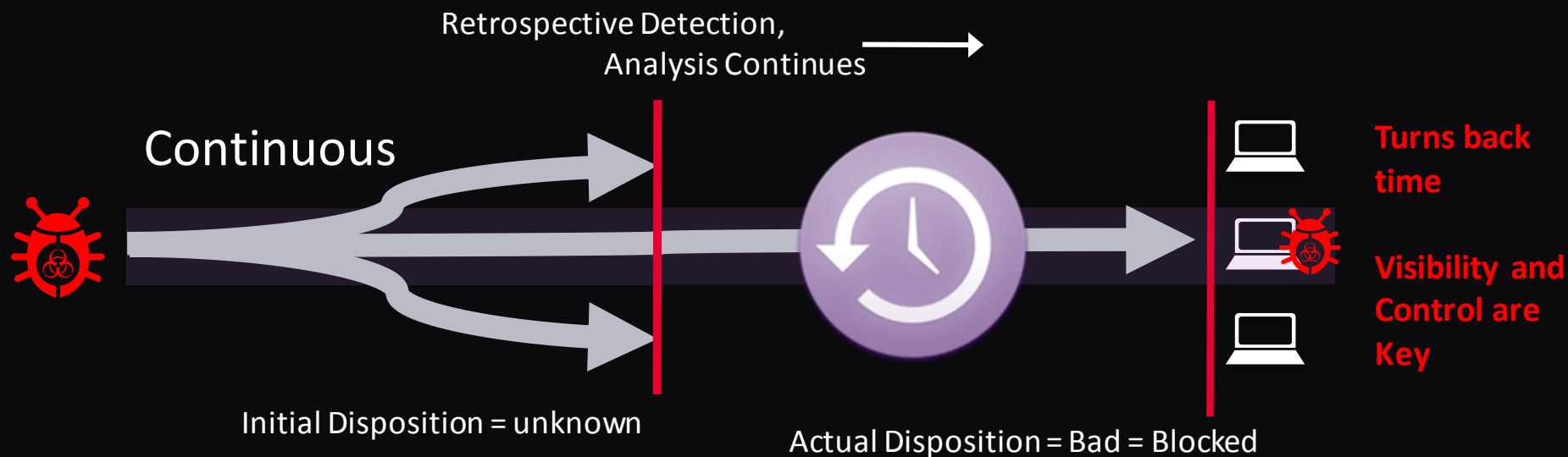
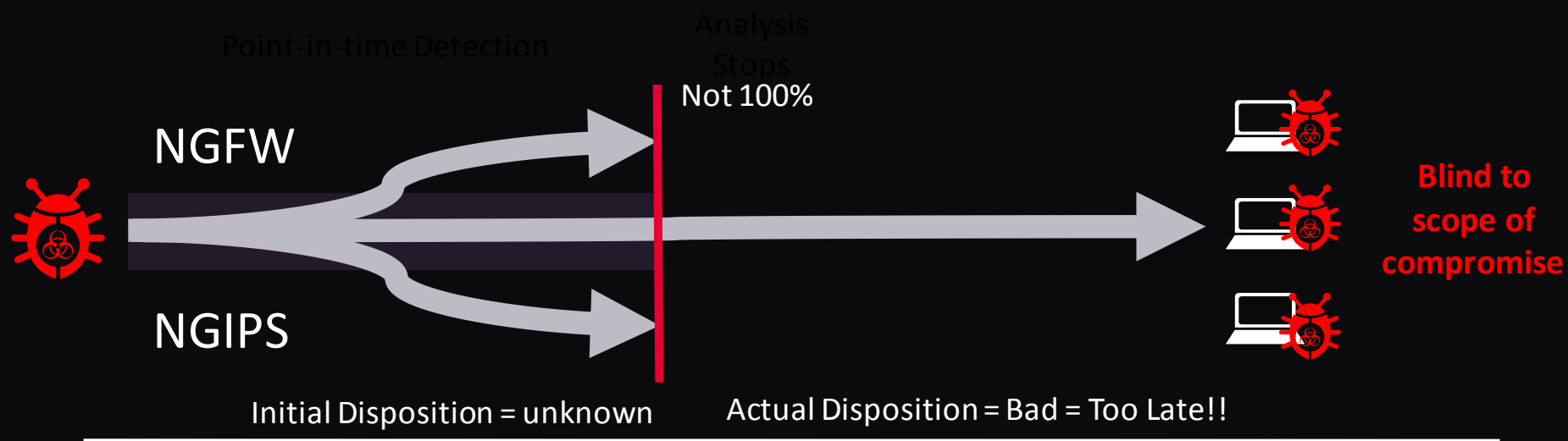
Analyses files to block malware

Analyses files to detect and block malware

- File Reputation
- Big data analytics
- Continuous analysis
- Multi AV engines
- Dynamic Analysis with Sandboxing
- State-of-the-art Algorithms for continuous malware targeting



# Remediation



## Remediation



Continuous Analysis,  
Trajectory

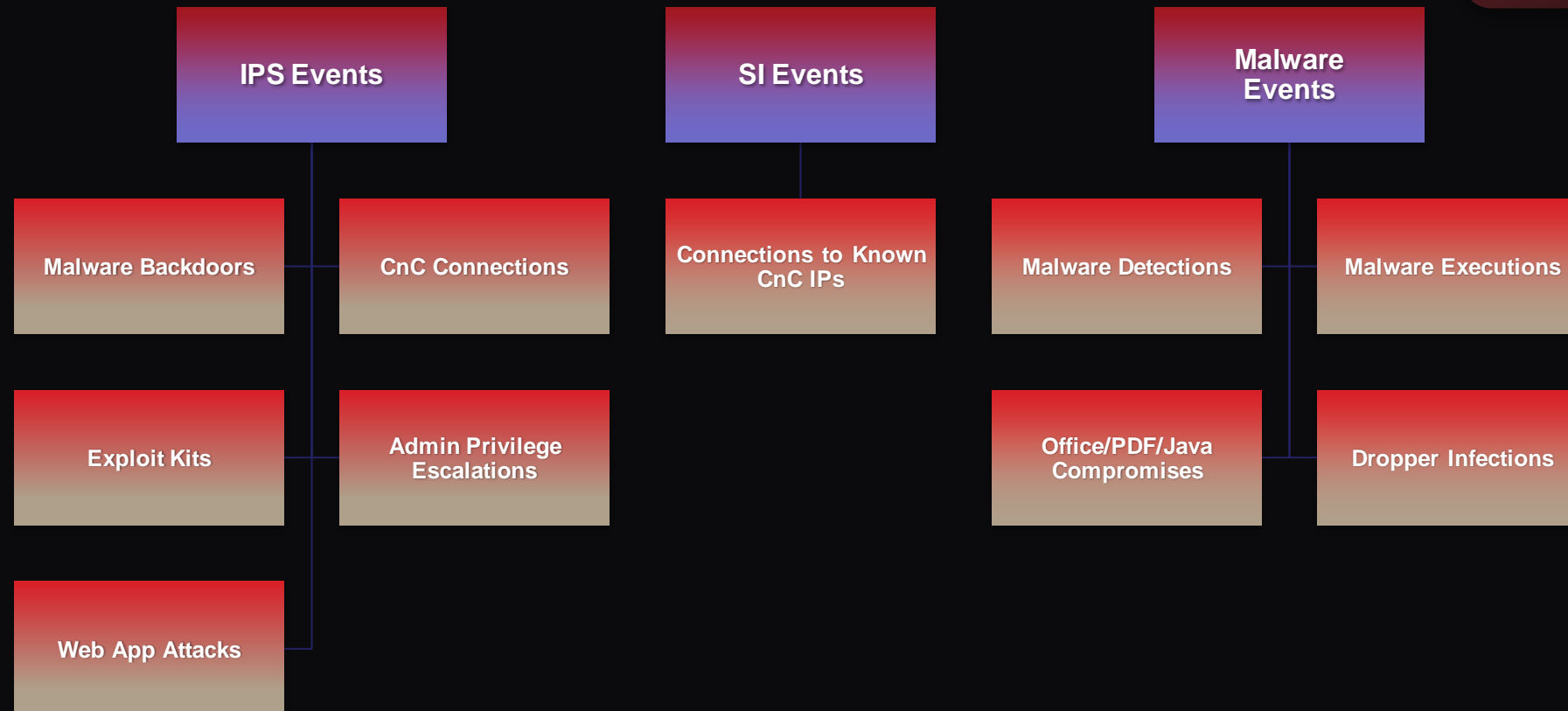
# Indications of Compromise (IoCs)

Early warning indicator to more rapidly remediate threats before they spread

## Indications of Compromise



Warning indicator to more rapidly remediate threats



# Cisco ASA Firepower Workshop

**13:45-15:00**

**Αίθουσα ΒΕΡΓΙΝΑ BE-03**

**Advanced Malware Protection και Indications of Compromise Workshop**

**Jean-Paul Kerouanton,  
Cisco Consulting System Engineer**

Με τη συμμετοχή σας στο workshop μπαίνεται στην κλήρωση για μια κάμερα Go Pro HERO 4!





# Industry Leading Threat Detection

Industry Leading  
Threat Detection



*The NGFW Security Value Map shows the placement of Cisco ASA with FirePOWER Services as compared to other vendors.*

*Cisco achieved 99.2 percent in security effectiveness and now all can be confident that they will receive the best protections possible*



**Cisco  
Best Protection Value**

99.2%  
Security  
Effectiveness



*“Cisco is disrupting the advanced threat defense industry.”*

**Gartner**

2014 Vendor Rating  
for Security: Positive



*“The AMP products will provide deeper capability to Cisco's role in providing secure services for the Internet of Everything (IoE).”*



*“Based on our (Breach Detection Systems) reports, Advanced Malware Protection from Cisco should be on everyone's short list.”*

Source: NSS Labs 2014



Cisco ASA with  
FirePower Services

Thank You



**Αίθουσα ΒΕΡΓΙΝΑ**

**BE-03 13:45-15:00**

**Advanced Malware Protection και Indications of Compromise**