



**Stop looking for  
the silver bullet,  
Start Think like a Bad Guy**

**: HP 사이버 킬체인 시큐리티 프레임워크**

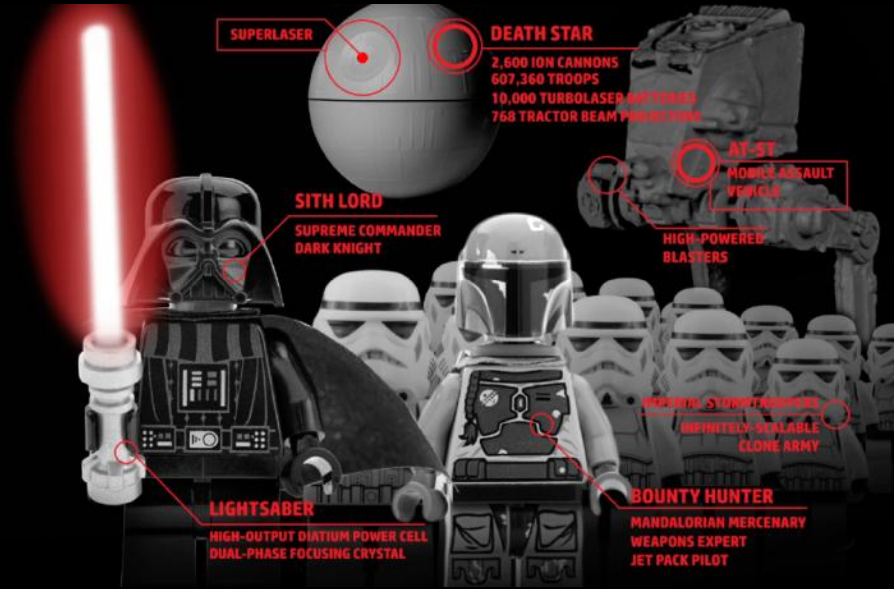
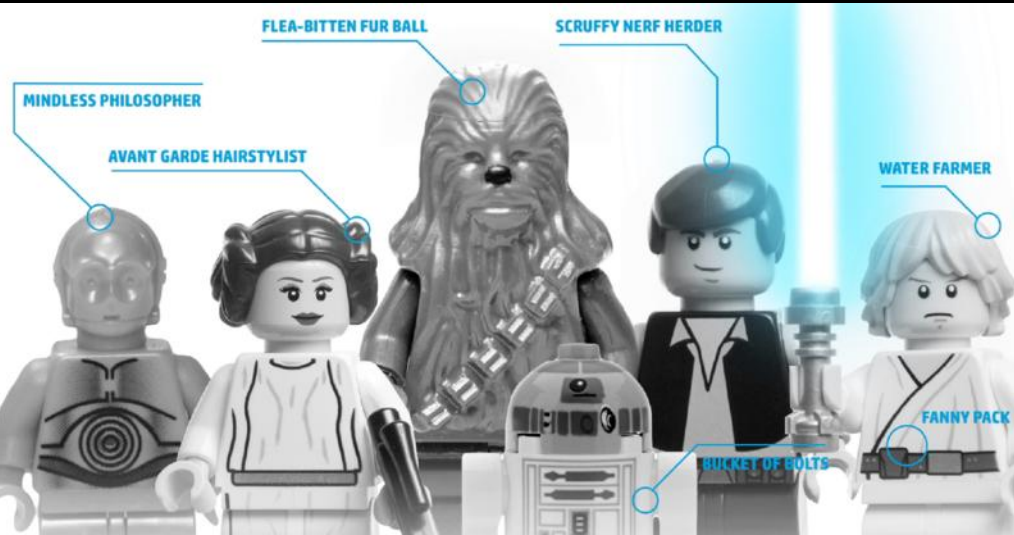
April 2014

박진성 이사 | 보안사업부장



보안사업부(ESP) | 한국HP





©iStock.com/LeventKonuk

# HACKTIVIST



**ORGANIZE**  
**SPECIALIZE**  
**MONETIZE**



**\$46 BILLION**

Global Spend on Cyber Security



**20%**

increase in  
**NUMBER OF  
BREACHES**

**30%**

increase in cost  
of a single  
**BREACH**



They only need to be right

**ONE TIME**

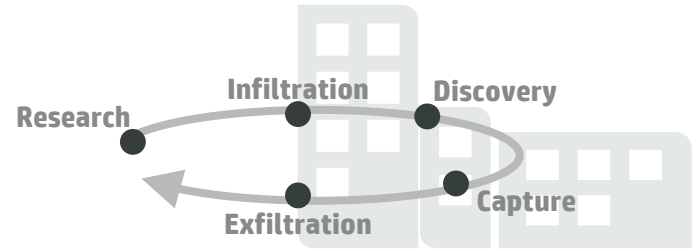


We need to be right  
**EVERY TIME**



# Challenges you are facing

**1 Nature and motivation of attacks**  
(Fame to fortune, market adversary)



**2 Transformation of enterprise IT**  
**(Delivery and consumption changes)**

## Delivery



## Consumption



**3 Regulatory pressures**  
**(Increasing cost and complexity)**



# What's so significant about these numbers?

63, 84, 68, 243

Mandiant, "M-Trend 2013: Attack the Security Gap"



**ADVERSARY**



**RESEARCH**



**INFILTRATION**

**DISCOVERY**



**EXFILTRATION**



**CAPTURE**



**MARKETPLACE**

ADVERSARY



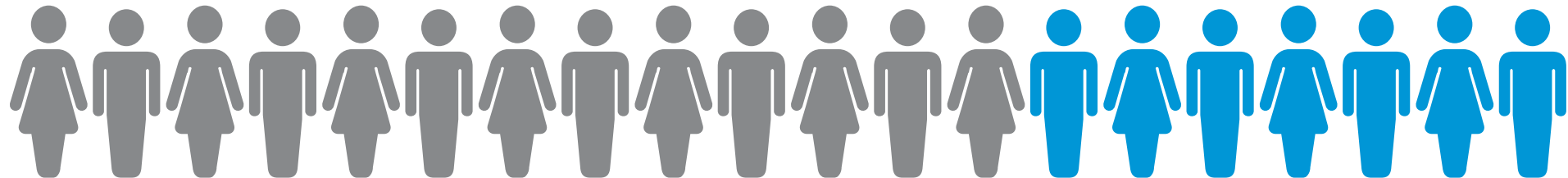
RESEARCH



# 63%

자사에 보안침해사고가 있었다는 것을  
“외부”에서 알려줌

: 보안침해사고를 자체 인지하는  
프로세스의 부재



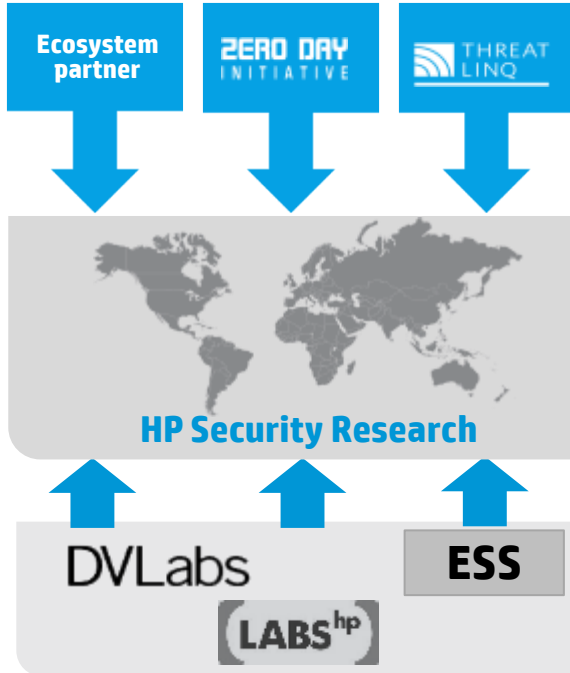
# 보안침해사고 선제대응을 위한 클라우드소싱 연구조직 운영

전문적인 자체 보안 연구인력 및  
글로벌 보안연구조직과의 협업을 통한  
선제적인 보안 인텔리전스 확보/관리



# HP Security Research

## Innovative research



SANS, CERT, NIST, OSVDB, software, and reputation vendors

- ~3,000 researchers
- 2,000+ customers sharing data
- 7,000+ managed networks globally



## Actionable security intelligence

- Automatically integrated into HP products
- HP finds more vulnerabilities than the rest of the market combined
- Top security vulnerability research organization for the past three years - Frost & Sullivan

## Thought leadership



# HP Threat Central

## Crowd-source actionable threat intelligence



### Companies must collaborate to mitigate threats

- Companies today spend time combatting the same threat
- The adversary is collaborating in an effective eco-system



### Current information sharing models are ineffective

- Manual and slow
- Limited participation
- Intel is not actionable



### Government alone can't fix the problem

- Can't hire the right resources fast enough
- Limited visibility: Need intelligence/data from industry



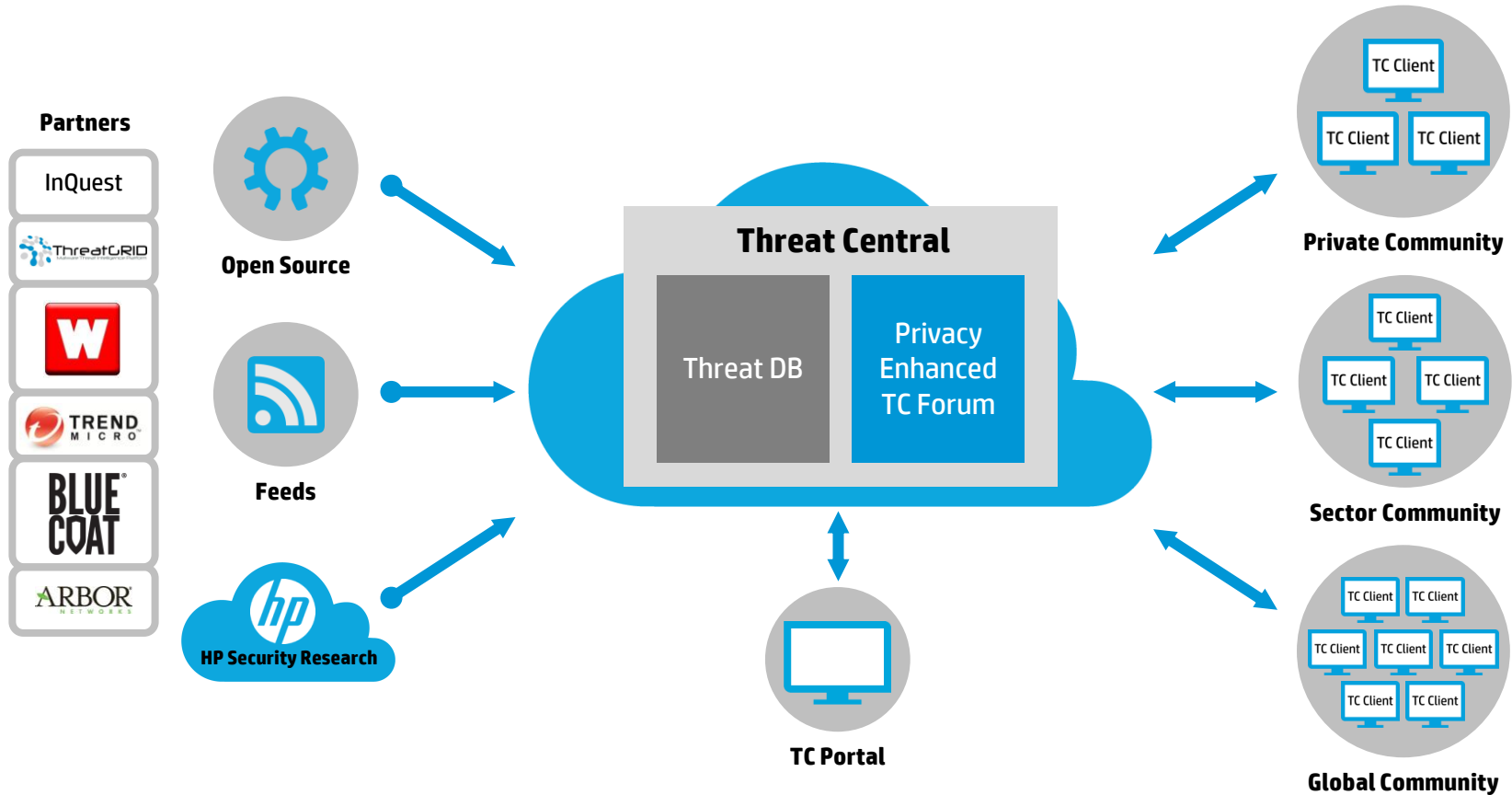
### Threat Central enables

- **Bi-directional** collaboration
- **Context** for **actionable** data in **automated** manner
- **Established community** with existing ArcSight customer base
- **Integrated** directly with mitigation engine (IPS)

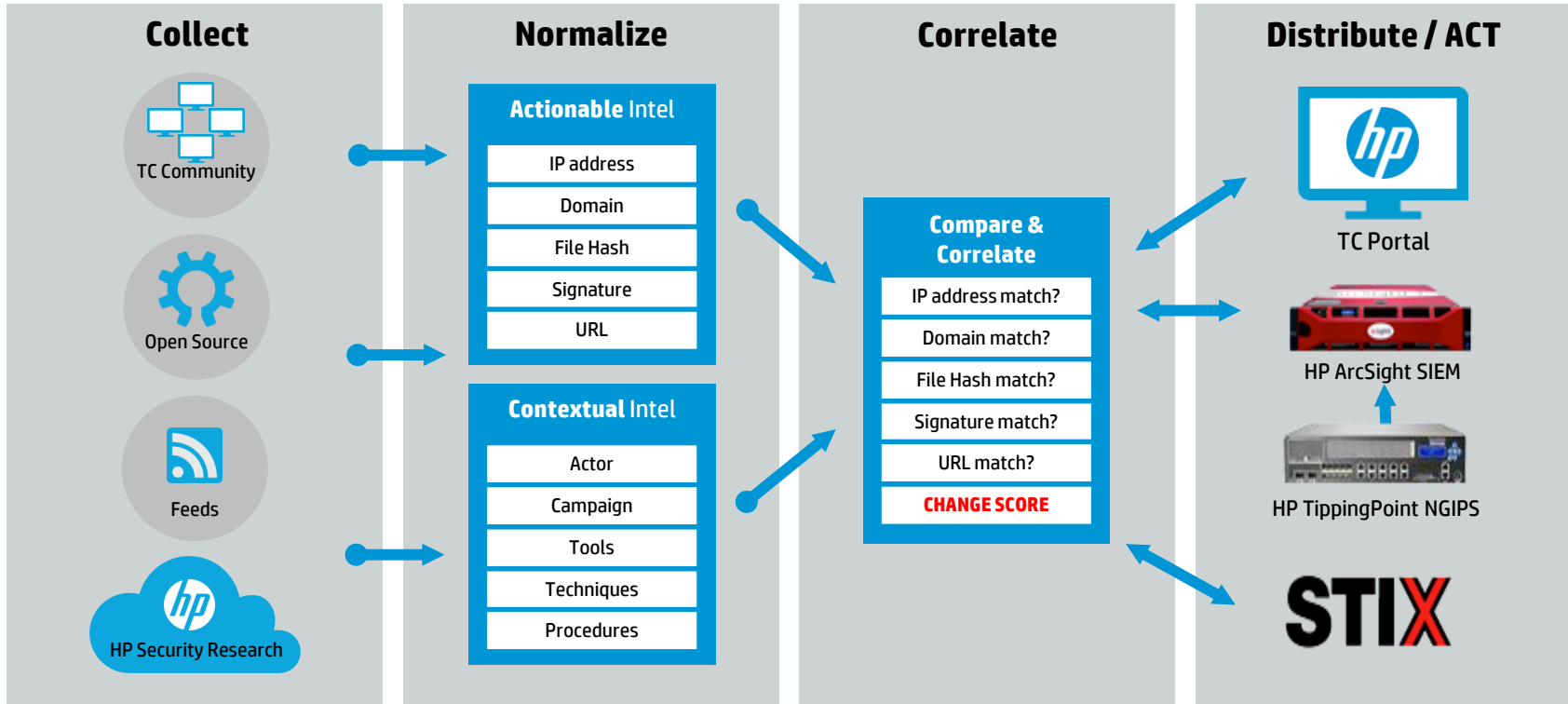




# Threat Central



# Automated Action Influenced by Context





84%

의 공격이

**Application Layer**

에서 발생하고 있음

그 중에서도 특히

**Mobile App**에 대한

취약점 발견율이

68%

이상 증가하고 있음



# 애플리케이션/소스코드 취약점 - 사이버공격의 근원

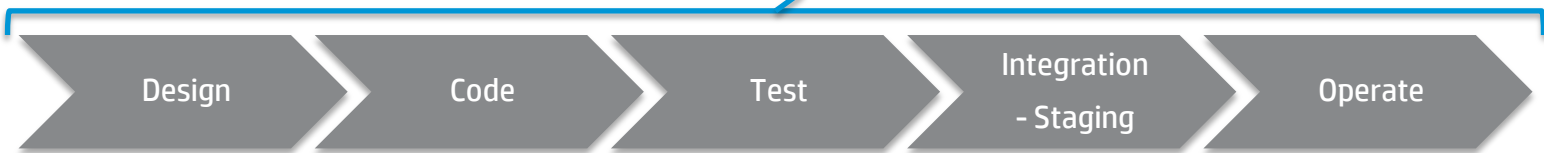
소프트웨어/애플리케이션의 보안약점을  
코딩단계에서부터 원천 제거하여 공격의  
루트가 되는 **Security Hole**을 사전 차단



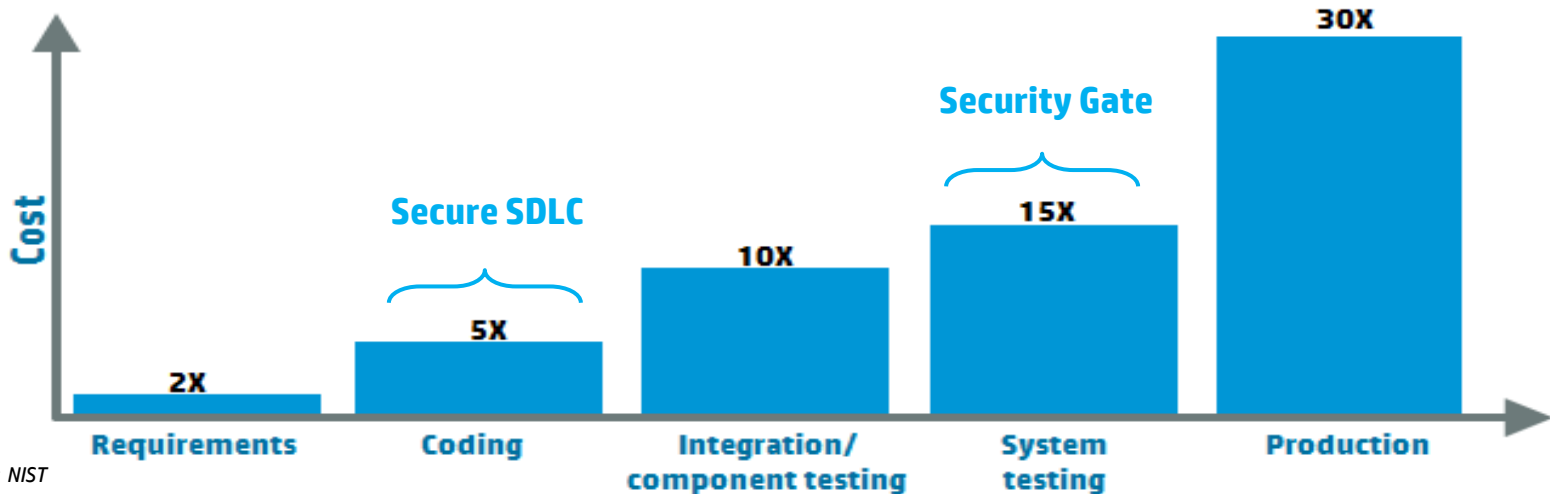
# 소프트웨어 보안 품질 보증

SDLC 애플리케이션 보안 소요비용

소프트웨어 보안



애플리케이션이 실제 운영환경에 설치된 후 보안문제 해결비용은 SDLC상에서 초기에 보안성을 탑재했을 때 대비 **최대 30배 이상** 소요!



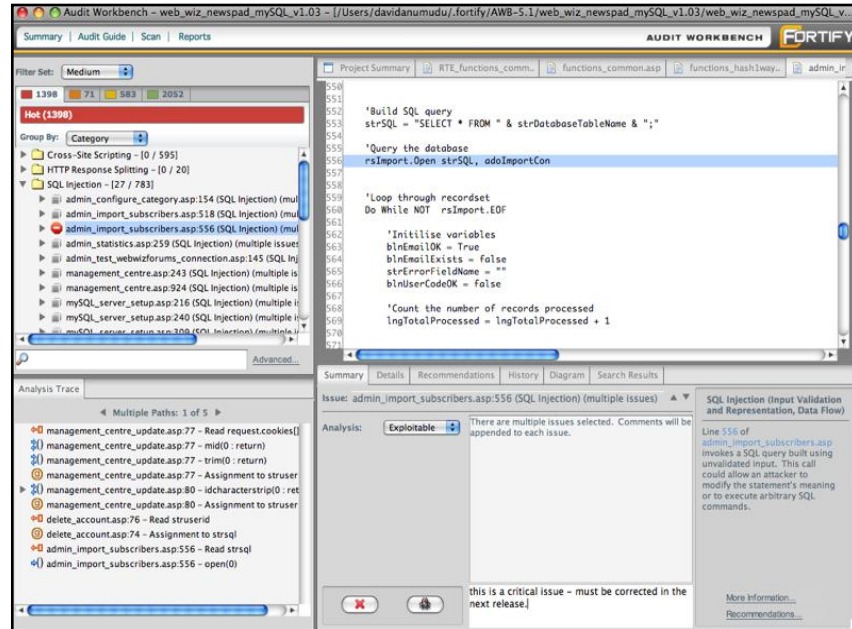
Source: NIST



# 정적분석을 통한 소스코드 보안취약점 발견 및 조치

## - HP Fortify Static Code Analyzer (SCA)

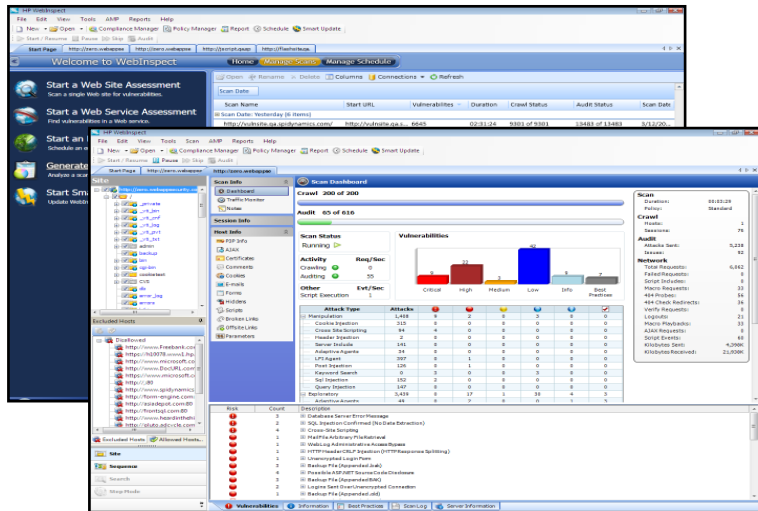
- 소스코드 정적보안취약점 분석 **De facto standard** 제품
- **500개 이상** 보안카테고리 및 업계최다인 **21개의** 개발 언어 대상 코드레벨 정적 보안 취약점 분석지원(**Java7, HTML5 포함**)
- 업계 유일 **Mobile app** 개발 언어 분석지원 (**Apple Objective-C/Xcode, Android Java** 모두 지원)



# 동적분석을 통한 웹 보안취약점 발견 및 조치

## - HP WebInspect

- 네트워크를 통한 웹서버 대상 보안 스캐닝을 통해 짧은 시간안에 고위험도 웹애플리케이션 보안취약점 탐지 및 조치 가이드
- 개발 프로젝트 진행, “보안검수시점과 운영 중 웹보안품질 측정”통해 보안취약점에 대한 상시 점검
- **1Hybrid 분석 기술 채용을 통해 소스코드분석결과와 동적분석결과 연계, 보안취약점에 대한 우선순위기반 보안취약점관리방안 제공(WebInspect Agent)**



**1Hybrid 분석 기술:** 정적분석기법인 소스코드 분석(Static code analysis)과 런타임 분석 기법인 프로그램 실행분석(WebInspect Agent), 동적분석기법인 웹 보안취약점 스캐너인 WebInspect를 상호 연동, 애플리케이션 보안취약점에 대해 통합분석함으로써, 동적분석의 한계인 분석 범위를 확장하고 정적분석결과를 실제 공격이 가능한순으로 분류하여 분석결과를 제공하므로 위험도와 실행 가능성이 높은 보안취약점을 빠르게 식별 및 우선적으로 수정할 수 있도록하여 전체 개발비용과 소요시간을 급격히 절감할 수 있는 **신기술**



**ADVERSARY**



**RESEARCH**



**INFILTRATION**





# Advanced Threats, Advanced Protect

차원이 다른 새로운 보안 인텔리전스 기반  
침입방지시스템

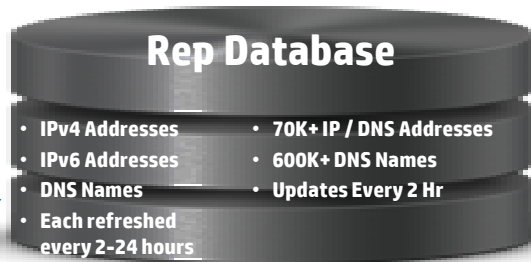


# 新 보안 인텔리전스를 통한 보안위협 선제 대응

## 레putation 활용을 통한 보안위협 식별 및 방어결정능력 향상

- 보안 전반에 걸친 알려진 “Bad” 트래픽 Reputation Database 기반 탐지 제공, \*별도의 패키지로 제공\*
- 글로벌 #1 Security Research Team(DVLabs)에 의한 평판 분석 및 악성보안 지수화(오탐율 최소화, APT 대응)

### ✓ 취약점 연구소(DVLabs)



### TippingPoint NG IPS & NG Firewall



## 약 110만개 Reputation DV 2시간 단위 업데이트

: 외부 기관과의 공조(Malware Domain List, EmergingThreats, IPTrust.com, Sunbelt, Esoft, SANS..) 를 통한 레putation 데이터 추가 확보 및 이를 ThreatLinQ를 통해 고객에게 전달

### Reputation Data Source

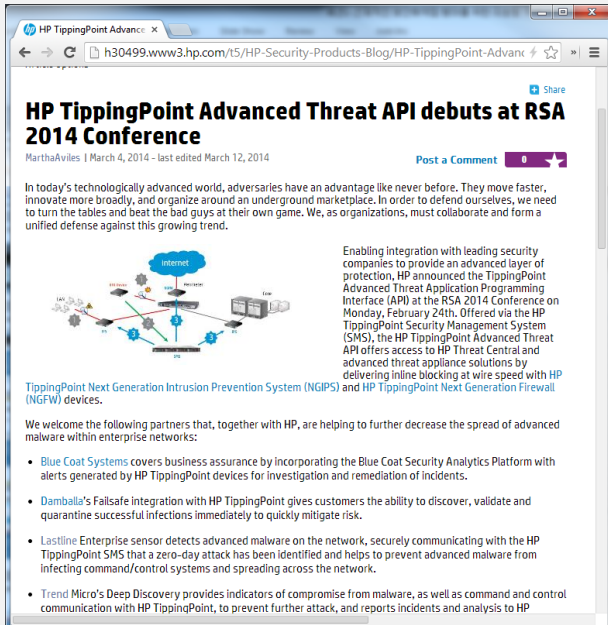
- HP Tipping-Point light-house attack sensors
- World-wide HP TippingPoint IPS installations
- Third-party Malware, Web, and E-Mail Research, Open Source Community ( eSoft, SANS, Malware Domain List, Sunbelt Border Patrol List, EmergingThreats, IPTrust.com,... )

Botnet C&C  
Scanner  
Spam  
Malware  
P2P  
Phishing  
Spyware



# HP TippingPoint ATA - Advanced Threat API Alliance

멀웨어 탐지 솔루션과의 연동 프로그램 가동



HP TippingPoint Advanced Threat API debuts at RSA 2014 Conference

MarthaAviles | March 4, 2014 - last edited March 12, 2014

In today's technologically advanced world, adversaries have an advantage like never before. They move faster, innovate more broadly, and organize around an underground marketplace. In order to defend ourselves, we need to turn the tables and beat the bad guys at their own game. We, as organizations, must collaborate and form a unified defense against this growing trend.

Enabling integration with leading security companies to provide an advanced layer of protection, HP announced the TippingPoint Advanced Threat Application Programming Interface (API) at the RSA 2014 Conference on Monday, February 24th. Offered via the HP TippingPoint Security Management System (SMS), the HP TippingPoint Advanced Threat API offers access to HP Threat Central and advanced threat appliance solutions by delivering inline blocking at wire speed with HP TippingPoint Next Generation Intrusion Prevention System (NGIPS) and HP TippingPoint Next Generation Firewall (NGFW) devices.

We welcome the following partners that, together with HP, are helping to further decrease the spread of advanced malware within enterprise networks:

- Blue Coat Systems covers business assurance by incorporating the Blue Coat Security Analytics Platform with alerts generated by HP TippingPoint devices for investigation and remediation of incidents.
- Damballa's Failsafe integration with HP TippingPoint gives customers the ability to discover, validate and quarantine successful infections immediately to quickly mitigate risk.
- Lastline Enterprise sensor detects advanced malware on the network, securely communicating with the HP TippingPoint SMS that a zero-day attack has been identified and helps to prevent advanced malware from infecting command/control systems and spreading across the network.
- Trend Micro's Deep Discovery provides indicators of compromise from malware, as well as command and control communication with HP TippingPoint, to prevent further attack, and reports incidents and analysis to HP

- 멀웨어 탐지 솔루션과의 상호 연동을 통한 보안 에코 시스템 파트너십 프로그램
- 협력 파트너: **TrendMicro, Damballa, Lastline, BlueCoat**

**Blue Coat**



**lastline**



- 탐지: 멀웨어탐지 솔루션
- 제어: **HP TippingPoint IPS**, 멀웨어 확산 방지를 위해 네트워크 상에서 방어

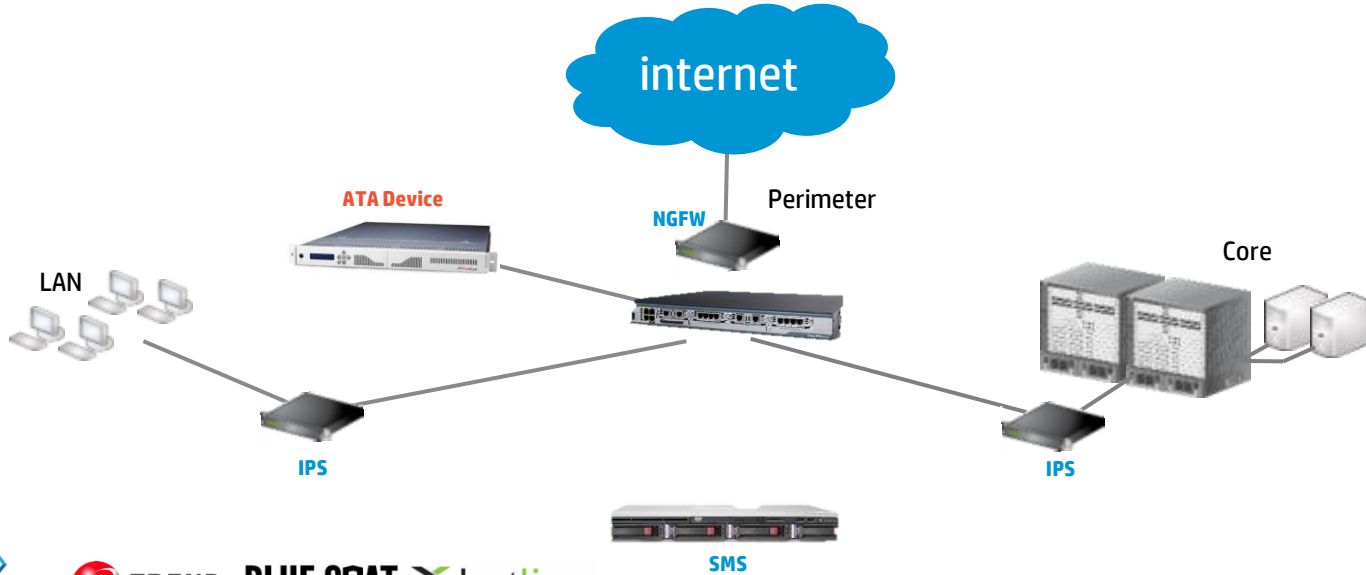
Source : [http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/HP-TippingPoint-Advanced-Threat-API-debuts-at-RSA-2014/ba-p/6385091#.Uy7y2fl\\_t84](http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/HP-TippingPoint-Advanced-Threat-API-debuts-at-RSA-2014/ba-p/6385091#.Uy7y2fl_t84)



# Advanced Threat API: Deployment Example

ATA Dev off SPAN port at perimeter, TippingPoint NGFW at Perimeter, IPS at Core, LAN

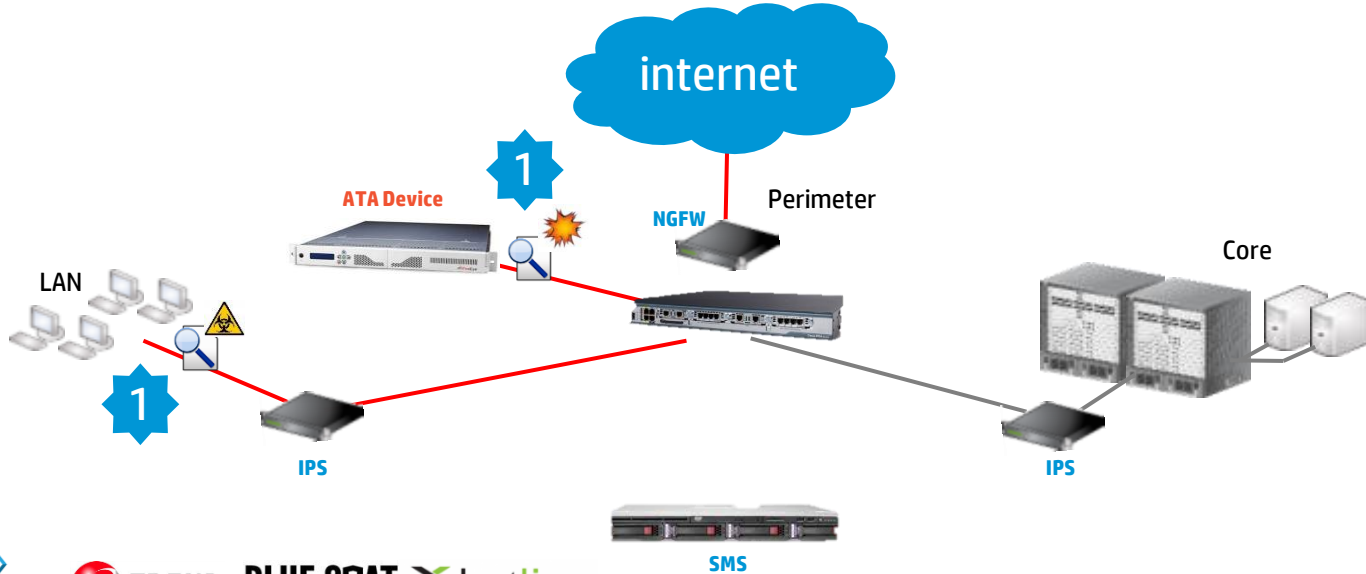
- 1 네트워크 상에 멀웨어 탐지 솔루션은 **Out of Band** 형태로, 티핑포인트 네트워크 보안시스템의 경우 **Perimeter/Core/Internal** 네트워크에 **Inline** 구성



# Advanced Threat API: Deployment Example

: Malware detonated by ATA Device but infects “patient-zero”

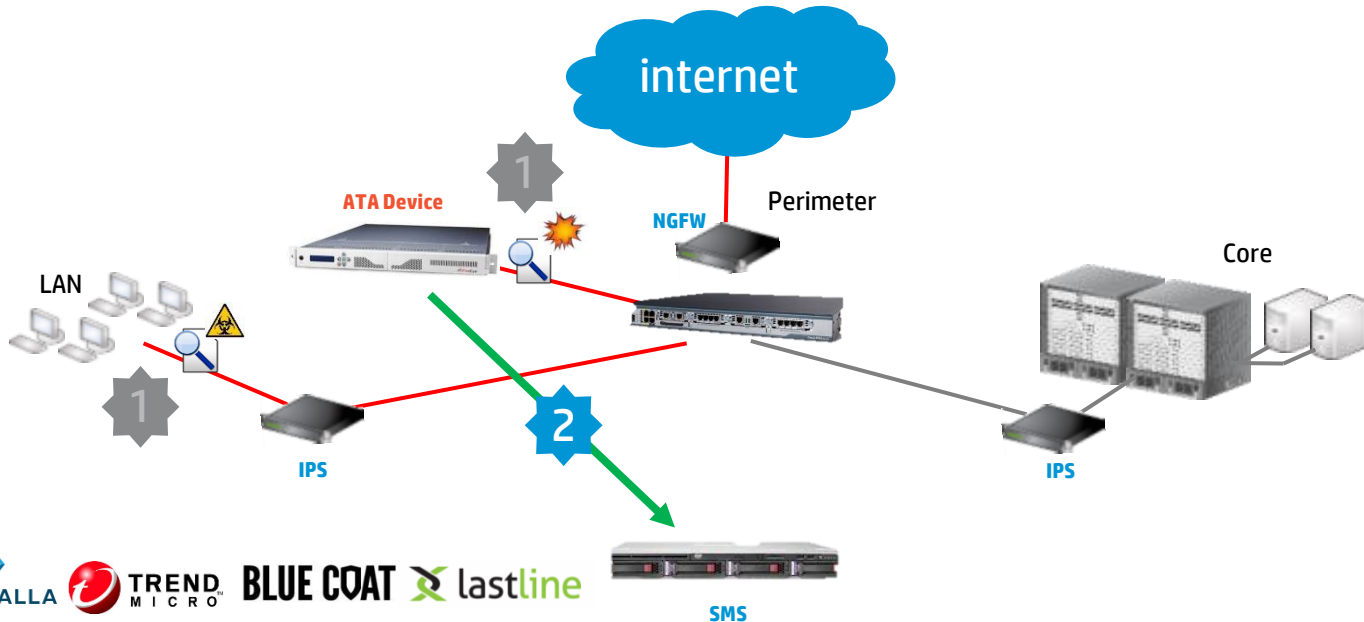
2 멀웨어는 멀웨어 탐지 솔루션에 의해 탐지되나 짧은 시간내에 전체 네트워크상으로 확산



# Advanced Threat API: Deployment Example

: ATA Device emits event to TippingPoint SMS

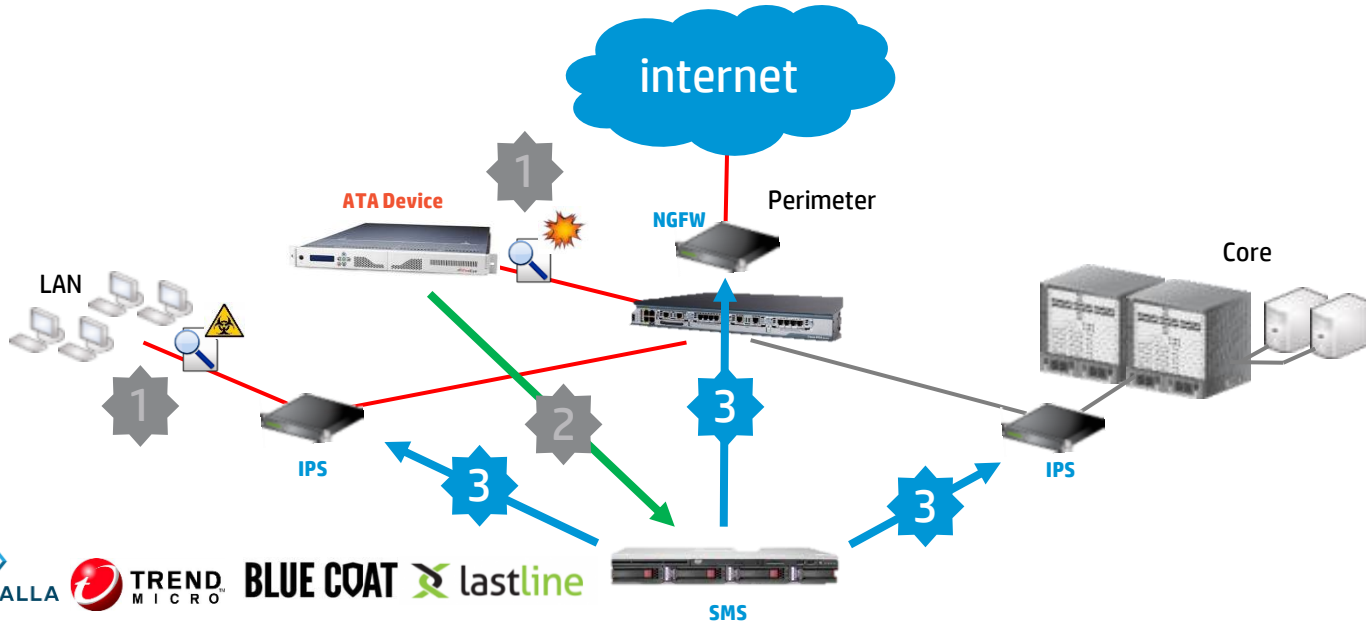
3 멀웨어 탐지 솔루션은 멀웨어 유발 IP정보를 TippingPoint SMS IPS/NGFW관리 시스템에 전달



# Advanced Threat API: Deployment Example

: SMS updates policy to quarantine the infected host, block the malware source, CnC

4 **TippingPoint SMS** IPS/NGFW관리 시스템는 해당 IP 격리명령을 **TippingPoint** 시스템 전달



**ADVERSARY**



**RESEARCH**



**INFILTRATION**

**DISCOVERY**

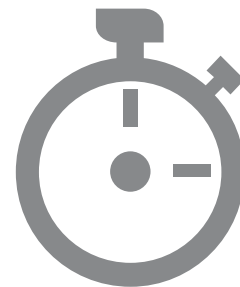




# 243 days

기업에서 보안위협을 탐지/관찰하는데 소요되는  
평균시간

**2013** January February March April May June July August **September** October November December **2014** January February March **April**



# “마이내리티 리포트”

상관관계 분석을 통한 비정상 행위 탐지  
외부C&C서버의 평판 관리를 통한 APT 방어





# The #1 Real Time Security Correlation Platform

Comprehensive solution for data collection from 350+ log generating sources



HP Software & Solutions



**ADVERSARY**



**RESEARCH**



**INFILTRATION**

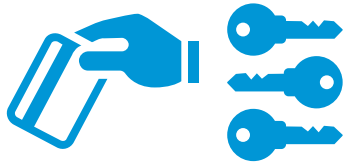
**DISCOVERY**



**CAPTURE**

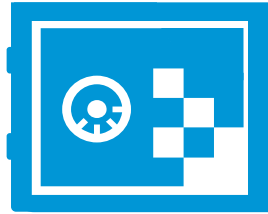
# HP Atalla secures data and payments

Protecting customers, mitigating risk, and supporting compliance requirements with leading technology for encryption and key management



## Reliable

High performance cryptography and key management for card payments and data protection



## Secure

Cryptographic keys and operations are protected by FIPS 140-2 validated solutions



## Compliant

Solutions support government and financial industry standards

# HP Information Security

## HP ESKM & Secure Encryption Encryption

Controller-based data encryption for HP ProLiant Gen8 servers

### ESKM Customer Benefits:

- Broad Encryption Coverage
- High Availability and Scalability
- Provide credible Compliance and Audit Coverage
- Simplified Deployment and management, no more SEDs



## ESKM 4.0 With KMIP

Leading industry standard for key management across storage

Manage the keys for all encryption devices with Atalla following OASIS standard



See us in the OASIS booth too!

## Information Protection and Control

New partner relationship – announcement to follow



Visit the Atalla Booth at RSA to learn more about this new partner



# HP HAVEn helps you monitor the assets that matter

## HP ArcSight – ESM with Big Data Platform (HP Autonomy – IDOL)





**ADVERSARY**



**RESEARCH**



**INFILTRATION**

**EXFILTRATION**



**DISCOVERY**



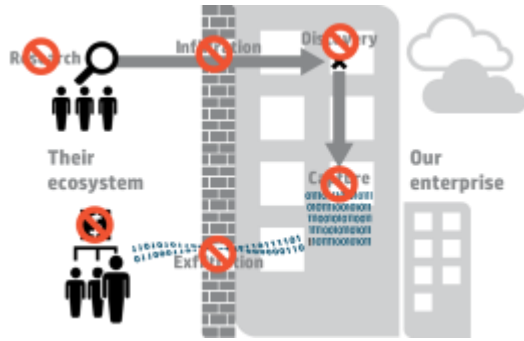
**CAPTURE**

Since 2009, time to resolve an attack **has grown**

 **130%**

# HP Security

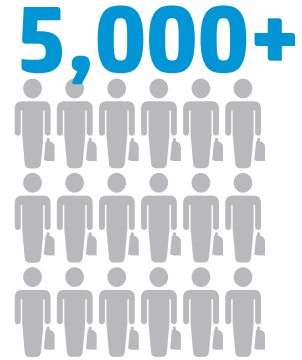
Disrupt the adversary, manage risk, and extend your capabilities



**Disrupt the adversary**  
**Security technology**



**Manage risk**  
**Risk & compliance**



**Reduce cost & complexity**  
**Advisory & management**



# HP Security's industry-leading scale

9 out of 10

Major banks



10 out of 10

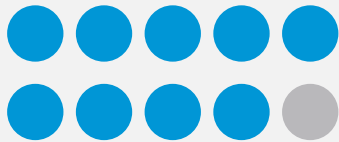
Top telecoms



5,000+

HP Security Professionals

All major branches US Department of Defense



9 out of 10

Top software companies



900+

HP managed security customers



2.3bn

Monthly security events

47m

HP Secured User Accounts



# “OpenSSL - Heartbleed”



# Heartbleed Vulnerability Protection on Day 1



## Every second matters!

- OpenSSL Vulnerability affecting 2/3 of the world's web servers
- HP TippingPoint customers are protected on Day 1 via Digital Vaccine
- Virtual patch stops attack and theft of critical customer information

## Follow our blog to learn more



### Heartbleed does not kill you. Just yet!

Sri\_Karnam | April 14, 2014

[Post a Comment](#)



There was a bug in one line of a code that nobody noticed for years. It was not an issue until recently, when somebody was able to exploit that vulnerability. How?

#### [Read Blog Article](#)

Tags: [fix](#) | [heartbleed](#) | [HP](#) | [security](#) | [solution](#) | [View All \(7\)](#)

Labels: [actionable security intelligence](#) | [ArcSight](#) | [ArcSight ESM](#) | [Big Data](#) | [cloud security](#) | [Data Security](#) | [ESP](#) | [event log analysis](#) | [HP Enterprise Security](#) | [information security](#) | [log analysis](#) | [log analytics](#) | [logger](#) | [network security](#) | [risk management](#) | [SIEM](#) | [SIRM](#)

### HP TippingPoint DVLabs--In a league of their own

MarthaAviles | April 11, 2014

[Post a Comment](#)



NTP reflection attacks can create hundreds of gigabits of traffic within seconds. See how HP Security's proactive creation of DV filters can stop those attacks.

#### [Read Blog Article](#)

Tags: [DVLabs](#) | [Microsoft](#) | [security](#) | [TippingPoint](#) | [ZDI](#) | [View All \(5\)](#)

Labels: [HP](#) | [security](#)

### Heartbleed protection with HP TippingPoint

MarthaAviles | April 10, 2014

[Post a Comment](#)



Heartbleed: It's sweeping the internet by storm. Here's what you can do to protect yourself now.

#### [Read Blog Article](#)

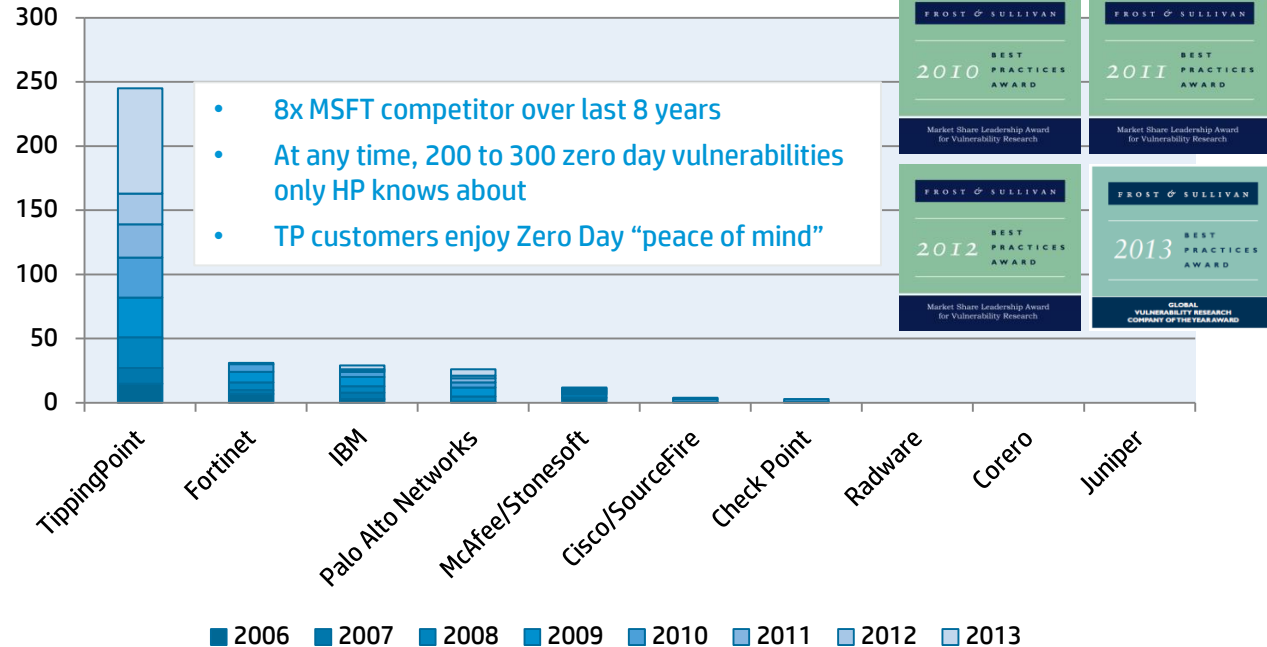


# Every Second Matters for Security Effectiveness



- Over 8,700 filters published to date
- Over 3,000 security researchers
- Focused on vulnerabilities rather than exploits
- Frost & Sullivan Market Share Leadership Award for Vulnerability Research

Microsoft Vulnerability Acknowledgements



4 years in a row!



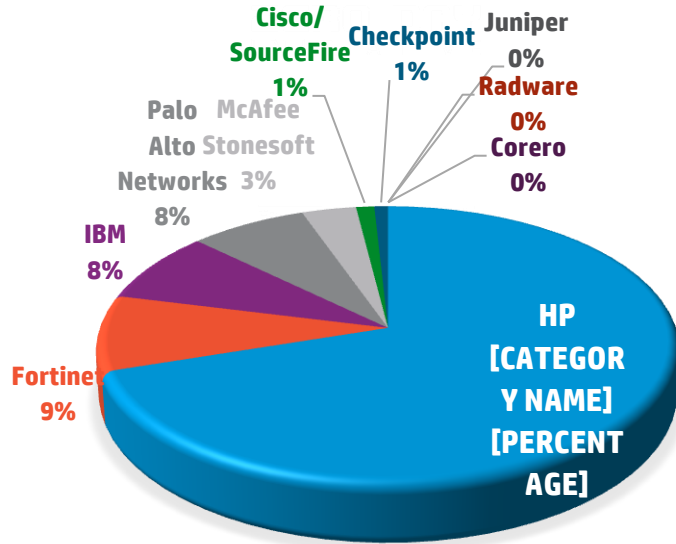
Compiled from public data available at <http://www.microsoft.com/technet/security/current.aspx> and Adobe Advisories



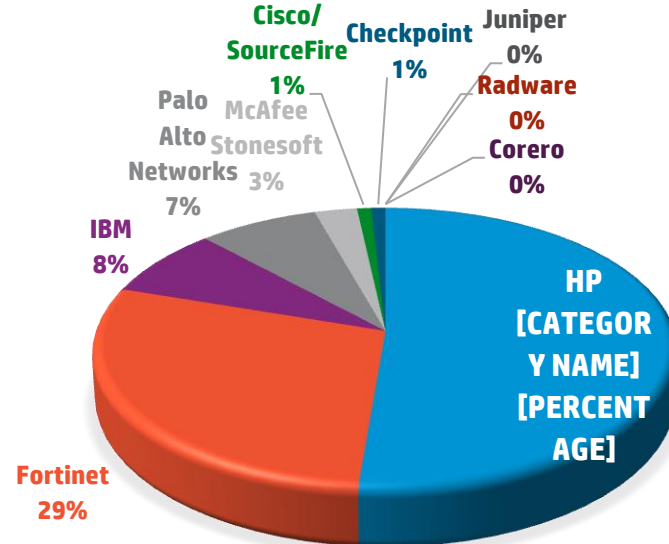
# Effective: World Class Security Research



## Microsoft Public Vulnerability Acknowledgements 2006-2013



## Adobe Public Vulnerability Acknowledgements 2007-2013



Compiled from public data available at <http://www.microsoft.com/technet/security/current.aspx>

Compiled from Adobe Advisories





# Search and Analysis Heartbleed Vulnerability by HP Fortify - WebInspect



Welcome to WebInspect [Home](#) [Manage Scans](#) [Manage Schedule](#)

**Start a Guided Scan**  
Create a scan that is optimized for your Web site.

**Start a Basic Scan**  
Scan a single Web site for vulnerabilities.

**Start a Web Service Scan**  
Find vulnerabilities in a Web service.

**Start an Enterprise Scan**  
Schedule an enterprise scan.

**Generate a Report**  
Analyze a scan using system reports.

**Start SmartUpdate**  
Update security checks and patches.

Recently Opened Scans [clear list](#)

- [clear](#) Zero
- [clear](#) Security Scope Disabled Sample
- [clear](#) Security Scope Enabled Sample
- [clear](#) Sample Scan
- [clear](#) Site: http://172.16.100.20:8080/WebGoat-5.4/attack-1

Scans Scheduled for Today

WebInspect Messages

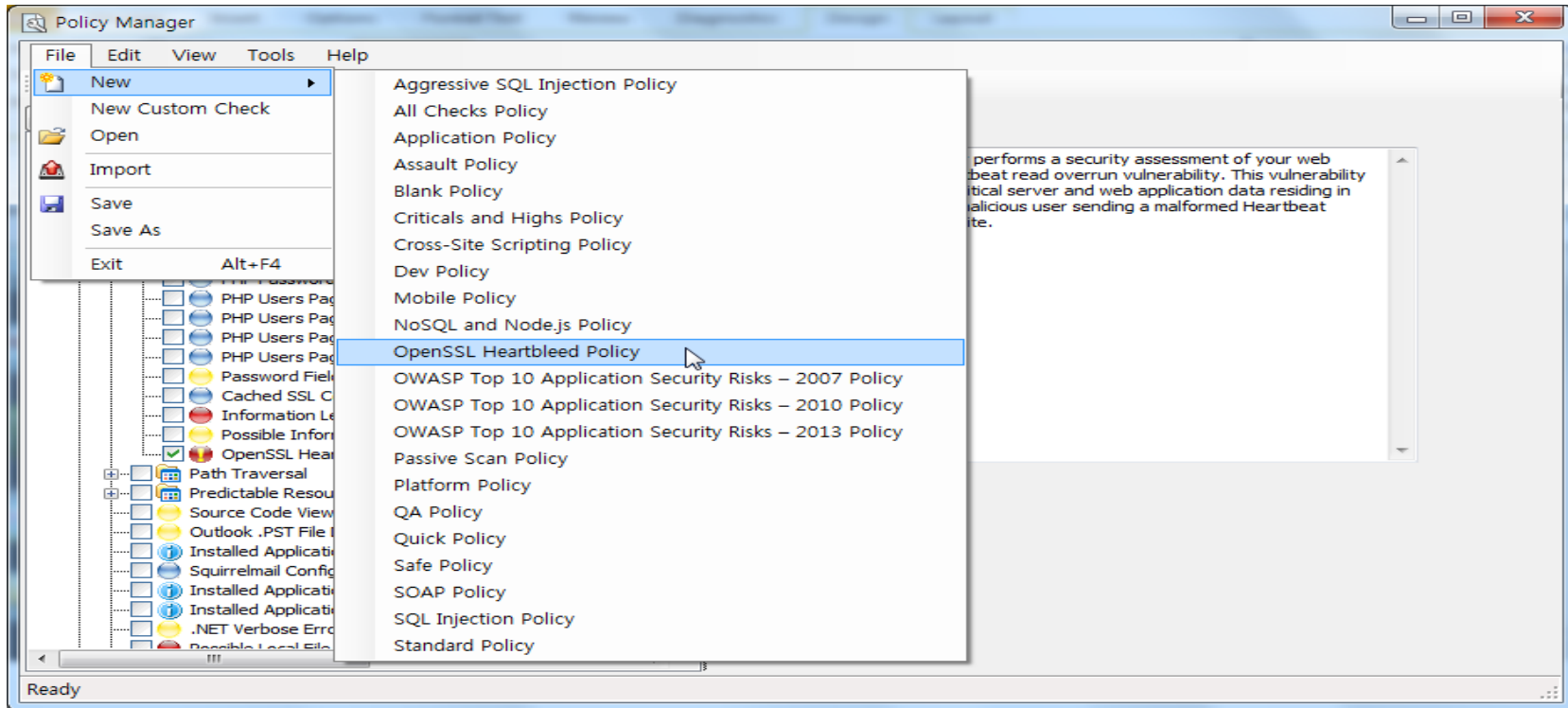
- [delete](#) **Welcome to WebInspect 10.1** 2011-03-01
- [delete](#) **HPSR Software Security Content - 2014 Update 1** 2014-04-01
- [delete](#) **HP Fortify Software Security Content - 2013 Update 4** 2013-12-20
- [delete](#) **Q3 2013 HP Fortify Software Security Content Update** 2013-10-01
- [delete](#) **Q2 2013 HP Fortify Software Security Content Update** 2013-06-28
- [delete](#) **Q1 2013 HP Fortify Software Security Content Update** 2013-03-29

What's new in WebInspect 10.1!

Introducing HP WebInspect 10.1



# Search and Analysis Heartbleed Vulnerability by HP Fortify - WebInspect



# Search and Analysis Heartbleed Vulnerability by HP Fortify - WebInspect



**Policy Manager**

File Edit View Tools Help

Standard View Search View

**Threat Classes**

- PHP Users Page (user.php5) (11232)
- PHP Test Page (test.php4) (11233)
- PHP Test Page (test.php) (11234)
- PHP Test Page (test.php5) (11235)
- PHP Password Page (passwords.php) (11236)
- PHP Password Page (passwords.php3) (11237)
- PHP Password Page (passwords.php4) (11238)
- PHP Password Page (passwords.php5) (11239)
- PHP Users Page (users.php) (11240)
- PHP Users Page (users.php3) (11241)
- PHP Users Page (users.php4) (11242)
- PHP Users Page (users.php5) (11243)
- Password Field Auto Complete Active (11276)
- Cached SSL Content (11306)
- Information Leakage via BREACH Vulnerability (11352)
- Possible Information Leakage via BREACH Vulnerability (11353)
- OpenSSL Heartbeat Read Overrun (11360)
- Path Traversal
- Predictable Resource Location
- Source Code Viewing Example Application (10261)
- Outlook .PST File Disclosure (10263)
- Installed Application: Squirrelmail (10264)
- Squirrelmail Configtest.php Information Disclosure (10265)
- Installed Application: Drupal (10267)
- Installed Application: Roller (10268)
- .NET Verbose Errors Enabled (10269)
- Disable Local File Inclusion Reading Vulnerability (10272)

**Name:** OpenSSL Heartbleed

**Description:**

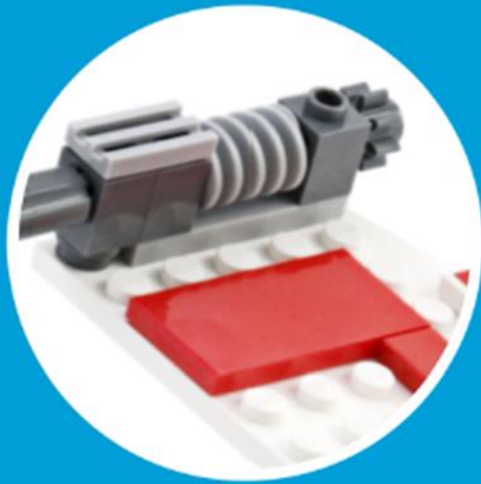
The OpenSSL Heartbleed policy performs a security assessment of your web application for critical TLS Heartbeat read overrun vulnerability. This vulnerability could potentially disclose the critical server and web application data residing in server memory at the time to malicious user sending a malformed Heartbeat request to server hosting the site.

**Properties:**

- Auto Update

Ready







정보보안 강화 업무에  
유익한 시간이 되기를  
바랍니다.



보안솔루션 관련 문의처: [espkorea@hp.com](mailto:espkorea@hp.com)

한국HP | 보안사업부(Enterprise Security Products)

