HP Enterprise Security

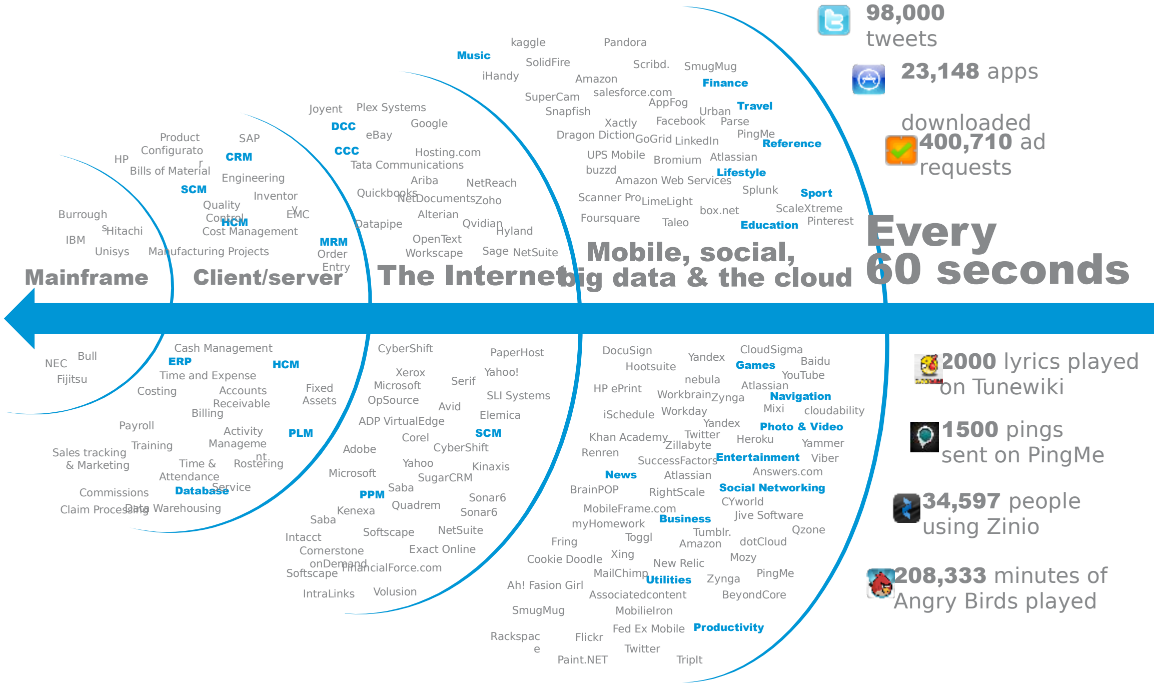
Управление рисками и инцидентами ИБ на предприятии

Артем Медведев

Коммерческий представитель

HP Enterprise Security Russia & CIS

Accelerating innovation and change



Mainframe

Burrough
Hitachi
IBM
Unisys
HP
NEC
Bull
Fijitsu

Client/server

Product Configurator
SAP
Bills of Material
CRM
Engineering
SCM
Inventory
Quality Control
EMC
HCM
Cost Management
Manufacturing Projects
MRM
Order Entry
Cash Management
ERP
HCM
Time and Expense
Costing
Accounts Receivable
Fixed Assets
Billing
Payroll
Activity Management
PLM
Sales tracking & Marketing
Training
Time & Attendance
Rostering
Database
Service
Commissions
Claim Processing
Data Warehousing

The Internet

Joyent
Plex Systems
DCC
Google
eBay
CCC
Hosting.com
Tata Communications
Ariba
NetReach
Quickbooks
NetDocuments
Zoho
Alterian
Datapipe
Qvidian
Hyland
OpenText
Workscape
Sage
NetSuite
CyberShift
PaperHost
Xerox
Serif
Yahoo!
Microsoft
OpSource
SLI Systems
Avid
ADP VirtualEdge
Elemica
Corel
SCM
Adobe
CyberShift
Yahoo
Kinaxis
Microsoft
SugarCRM
Saba
PPM
Sonar6
Kenexa
Quadrem
Sonar6
Saba
Softscape
NetSuite
Intacct
Cornerstone onDemand
Exact Online
Softscape
FinancialForce.com
IntraLinks
Volusion

Mobile, social, big data & the cloud

Music
kaggle
Pandora
SolidFire
Scribd.
SmugMug
iHandy
Amazon
Finance
SuperCam
salesforce.com
Snapfish
AppFog
Urban
Travel
Xactly
Facebook
Parse
Dragon Diction
GoGrid
LinkedIn
PingMe
Reference
UPS Mobile
Bromium
Atlassian
buzzd
Lifestyle
Amazon Web Services
Splunk
Sport
Scanner Pro
LimeLight
box.net
ScaleXtreme
Foursquare
Taleo
Education
Pinterest
DocuSign
Yandex
CloudSigma
Hootsuite
Games
Baidu
YouTube
nebula
HP ePrint
Atlassian
Workbrain
Zynga
Navigation
iSchedule
Workday
Mixi
cloudability
Yandex
Photo & Video
Khan Academy
Twitter
Heroku
Yammer
Zillabyte
Renren
SuccessFactors
Entertainment
Viber
News
Answers.com
Atlassian
BrainPOP
RightScale
Social Networking
CYworld
MobileFrame.com
Jive Software
Business
myHomework
Tumblr.
Qzone
Toggl
Fring
Amazon
dotCloud
Xing
Mozy
Cookie Doodle
New Relic
MailChimp
Utilities
Zynga
PingMe
Ah! Fasion Girl
Associatedcontent
BeyondCore
SmugMug
MobileIron
Fed Ex Mobile
Productivity
Rackspace
Flickr
Twitter
Paint.NET
TripIt

98,000 tweets

23,148 apps downloaded

400,710 ad requests

Every 60 seconds

2000 lyrics played on Tunewiki

1500 pings sent on PingMe

34,597 people using Zinio

208,333 minutes of Angry Birds played

New technology access methods

- Change how technology is consumed and value it can bring
- Open up new business models
- Remove current inhibitors and unleash power of innovation

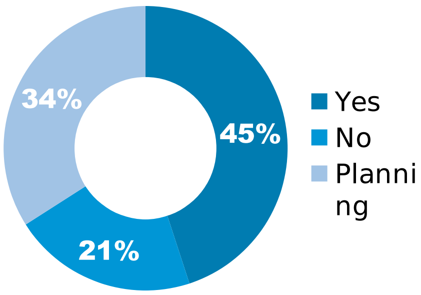
Coleman Parkes Research

Security awareness is going in the right direction

Security executives are starting to have a seat at the table

However, a majority do not have a security strategy in place

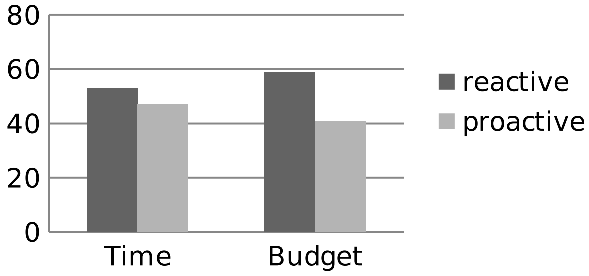
Information risk strategy



Security intelligence is on the rise

However, reactive measures still dominate resources and budget

Reactive vs proactive



Coleman Parkes Research

Innovation and technology challenges

Cloud services can often be secure

But awareness of the buyers is often lacking

Big data is a big opportunity

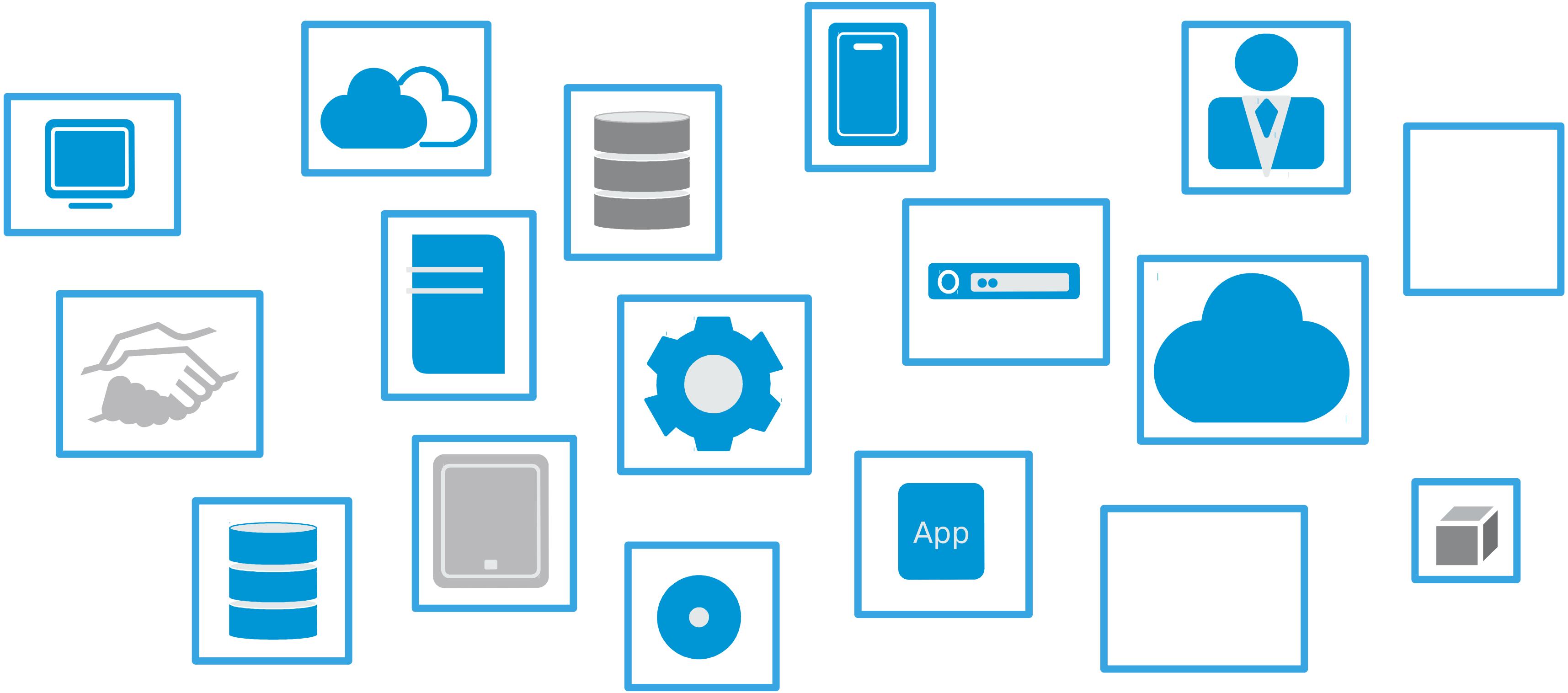
Provided the data is secure while in use, in transit, at rest

Mobility is difficult at many levels

But the number of devices, apps, locations keeps growing

Traditional approach is obsolete

One-off, bolt-on approach leads to fragmented environment



HP presents intelligent security

Build it in. Make it intelligent. Protect what matters.

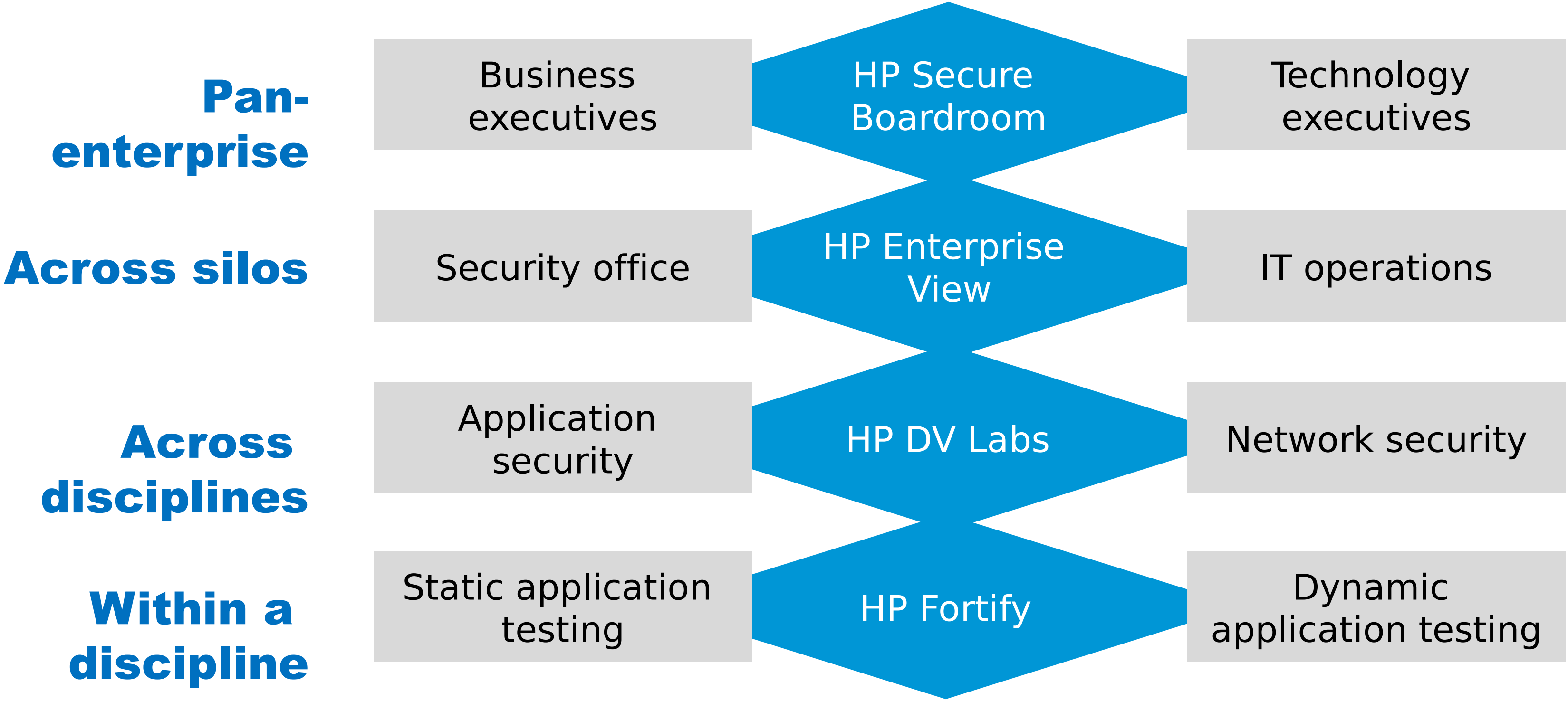
- **Market-leading technology**
- **Enterprise perspective**
- **Experienced people**

Choice of delivery models

- Products
- Services
- Hybrid

Market-leading technology

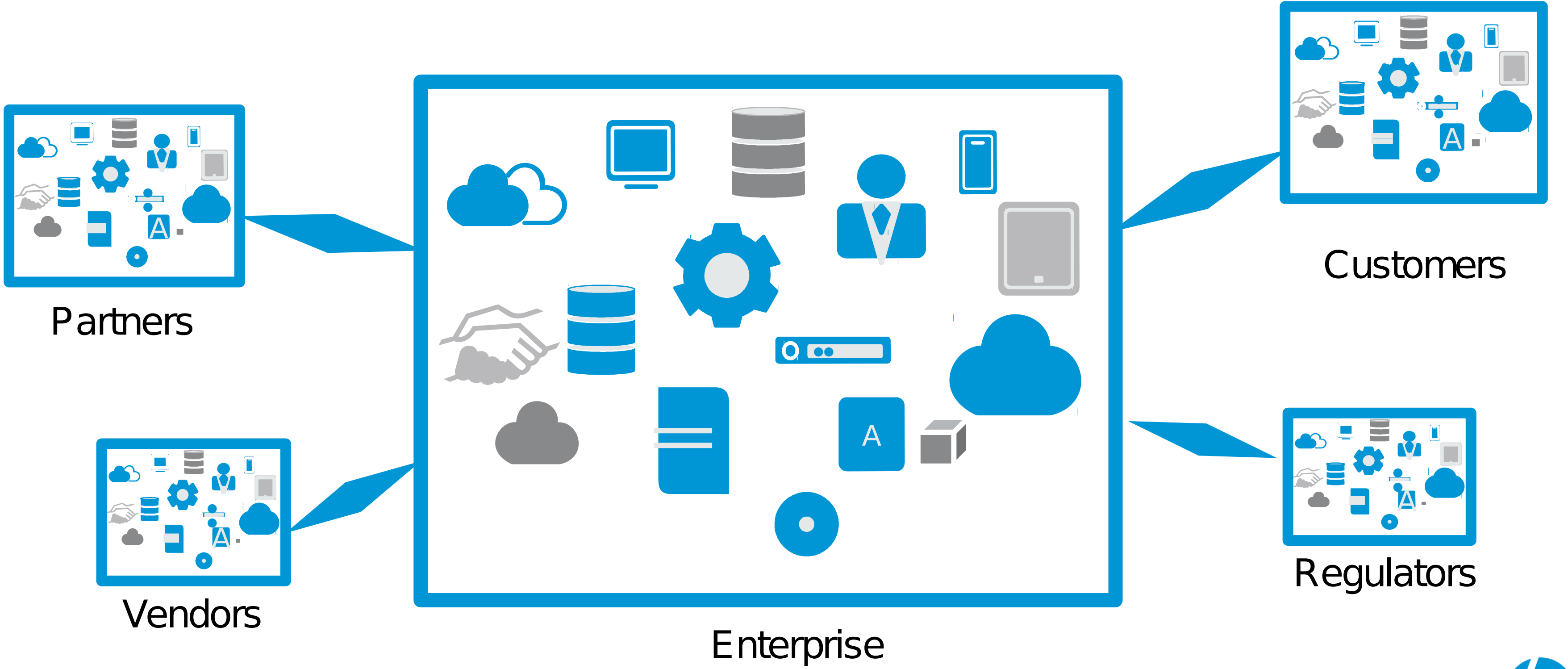
Connecting disciplines, silos, business functions



Pan-enterprise	Business executives	HP Secure Boardroom	Technology executives
Across silos	Security office	HP Enterprise View	IT operations
Across disciplines	Application security	HP DV Labs	Network security
Within a discipline	Static application testing	HP Fortify	Dynamic application testing

An extended enterprise perspective

Connecting the elements through a unifying platform



Partners

Vendors

Enterprise

Customers

Regulators

HP Enterprise security solutions delivered globally

Universal Log Management

Compliance & Risk Management

Perimeter, Data Center & Network Security

Insider Threat Mitigation

Advanced Persistent Threat Remediation

Traditional & Mobile Application Security

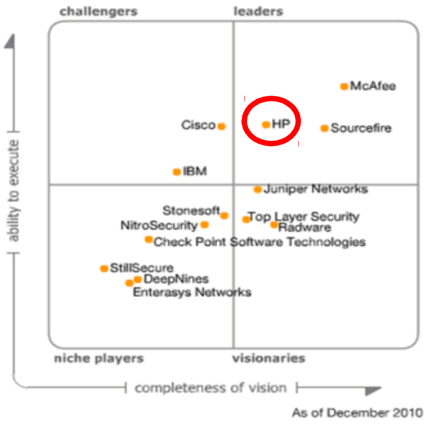
Data Privacy & Data Loss Prevention

Application & Transaction Monitoring

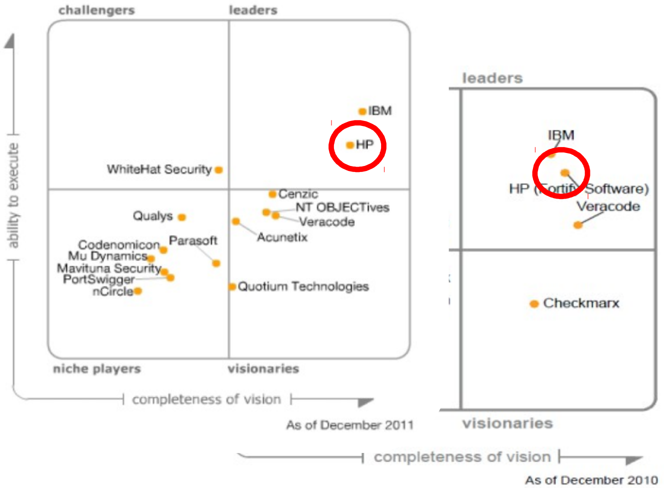
HP Enterprise Security

- 1,400 security professionals from ArcSight, Fortify and TippingPoint teams
- 1,500 security professionals in HP Enterprise Security Services
- Top five security company by market share (leader in SIEM, Log Mgt, AppSec, Network Security)

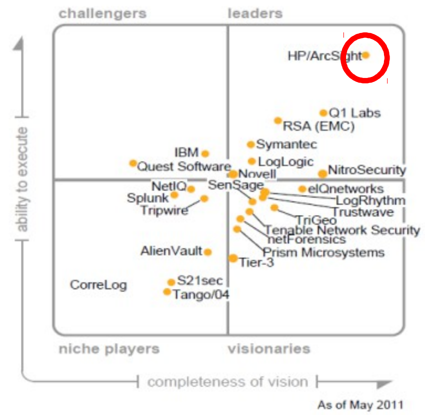
Magic Quadrant for Network Intrusion Prevention Systems
December 2010.



Magic Quadrant for Static and Dynamic Application Security Testing
2011.



Magic Quadrant for Security Information and Event Management
May 2011.



Source: Gartner (May 2011)

HP Enterprise Security

Market leading products and services

- Security Information and Event Management
- Log Management
- Application Security
- Network Security
- Data Protection
- Threat Research
- Security Services

One Team, One Vision

DVLabs

TippingPoint

ATALLA

ArcSight

VISTORM™

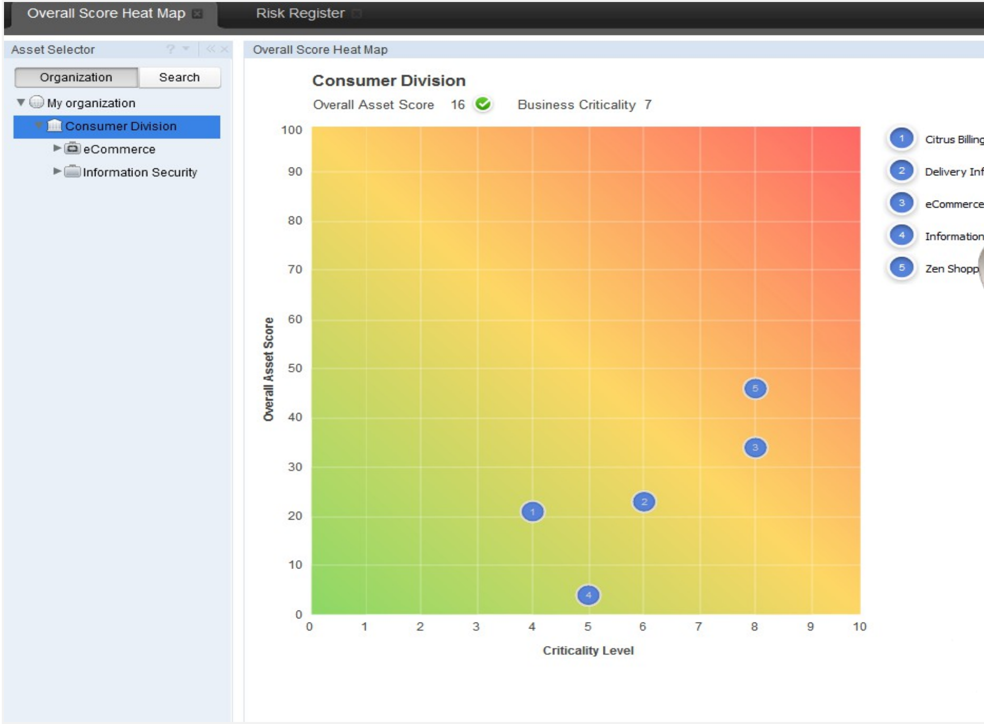
FORTIFY

SPI DYNAMICS
secure. protect. inspect.

New Intelligence Products

HP EnterpriseView:
see everything and prioritize response

NEW



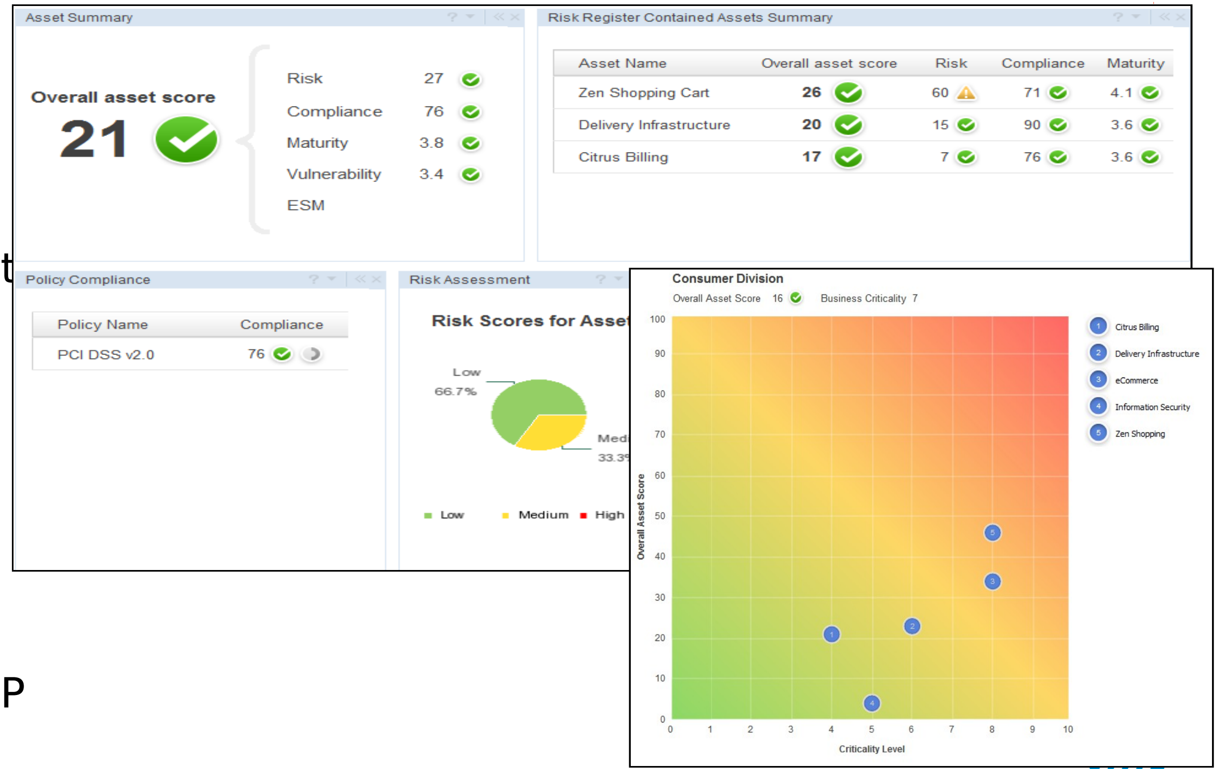
Consumer Division

Overall Asset Score 16 ✓ Business Criticality 7

EnterpriseView

NEW

- Module-Based Platform
  - Risk
  - Assets
  - Policy
  - Vulnerability
- Actionable risk management
- Aligned with business context
  - Synchronizes with uCMDB
- Real time threat data
  - ArcSight ESM
  - Scanners using ArcSight connectors
  - WebInspect
- Automated Audit
  - HP BSA
  - UCF - audit once comply many
- Robust reporting engine – SAP BO



Asset Summary

Overall asset score 21 ✓

Risk	27	✓
Compliance	76	✓
Maturity	3.8	✓
Vulnerability	3.4	✓
ESM		

Risk Register Contained Assets Summary

Asset Name	Overall asset score	Risk	Compliance	Maturity
Zen Shopping Cart	26 ✓	60 ⚠	71 ✓	4.1 ✓
Delivery Infrastructure	20 ✓	15 ✓	90 ✓	3.6 ✓
Citrus Billing	17 ✓	7 ✓	76 ✓	3.6 ✓

Policy Compliance

Policy Name	Compliance
PCI DSS v2.0	76 ✓

Risk Assessment

Risk Scores for Asse

Consumer Division

Overall Asset Score 16 ✓ Business Criticality 7

HP TippingPoint NX Platform Next Generation IPS

NEW

Features

Based on X-Armour, HP’s new break-through architecture

First in market to support 16 segments of 10GbE in a 2U form factor

A 60% performance increase from prior versions with 13Gbps inspected throughput in the 7100NX

Offers pluggable interface modules for easier customization

The four available interface modules are: 10GbE with 8 ports (4 segments), 40GbE with 2 ports, 1GbE fiber with 12 ports, 1Gbe copper with 12 port

Problem it solves

Organizations are constantly under attack. Sensitive information is accessed and pulled out of an organization through network connections

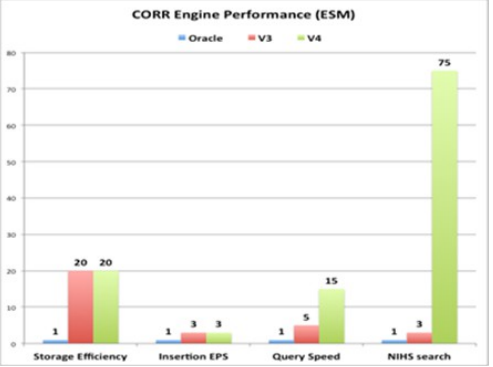
Performance and configuration become bottlenecks in the enterprises’ effort to detect and protect their organization

Customer Benefits

- Protect hybrid environments from a single console
- Reduces rack space requirements significantly
- Built to perform in the most demanding data centers with
- Updated with weekly intelligence from industry leading global researchers
- This configuration makes the HP NGIPS the best solution for current and next generation data centers where 10GbE networks are typically deployed

HP ArcSight ESM 6.0c with CORR Engine

NEW



Features

The first ArcSight SIEM software product to use the HP CORR (Correlation Optimized Retention and Retrieval) engine

Compared with advanced RDBMS versions, ESM 6.0c offers 300%-500% faster correlation

CORR engine provides highly efficient data storage-- up to 20 times less storage--for all SIEM use cases

HP ArcSight CORR technology can now be deployed as an appliance and as a software

Problem it solves

The large amount of security event data makes it extremely difficult to extract relevant, timely, and actionable information without the ability to quickly analyze

Detecting and preventing both internal and external information security risks without the help of advanced log analysis, correlation and reporting is ineffective

Customer Benefits

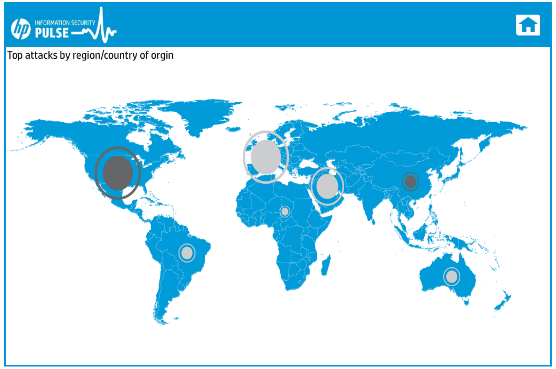
Reduces threat and risk impacting the enterprise network

Reduced cost of security via faster collection/correlation, simplified analysis and more efficient storage

Lower cost of compliance via automated regulatory reporting and continuous controls monitoring

HP Introduces Information Security Puls

NEW



Top attacks by region/country of orgin

Problem it solves

- Many enterprise organizations do not have visibility into cyber threats and attacks
- Many enterprise organizations do not realize the extent to which their information may be exposed to exploits, if they are not using HP IPS solutions

Features

- Free access to trending threat and attack data from HP DVLabs
- Provides geographic-based situational awareness information
- Provides customizable news feed feature
- Available for iPad, iPhone, Android, WebOS and web

Customer Benefits

- Provides customers with free access to HP Dvlabs proprietary cyber threat data
- Helps people in security and non-security roles to see and understand the threats and attack trends that may affect their enterprise
- Helps educate customers about cyber security situational awareness

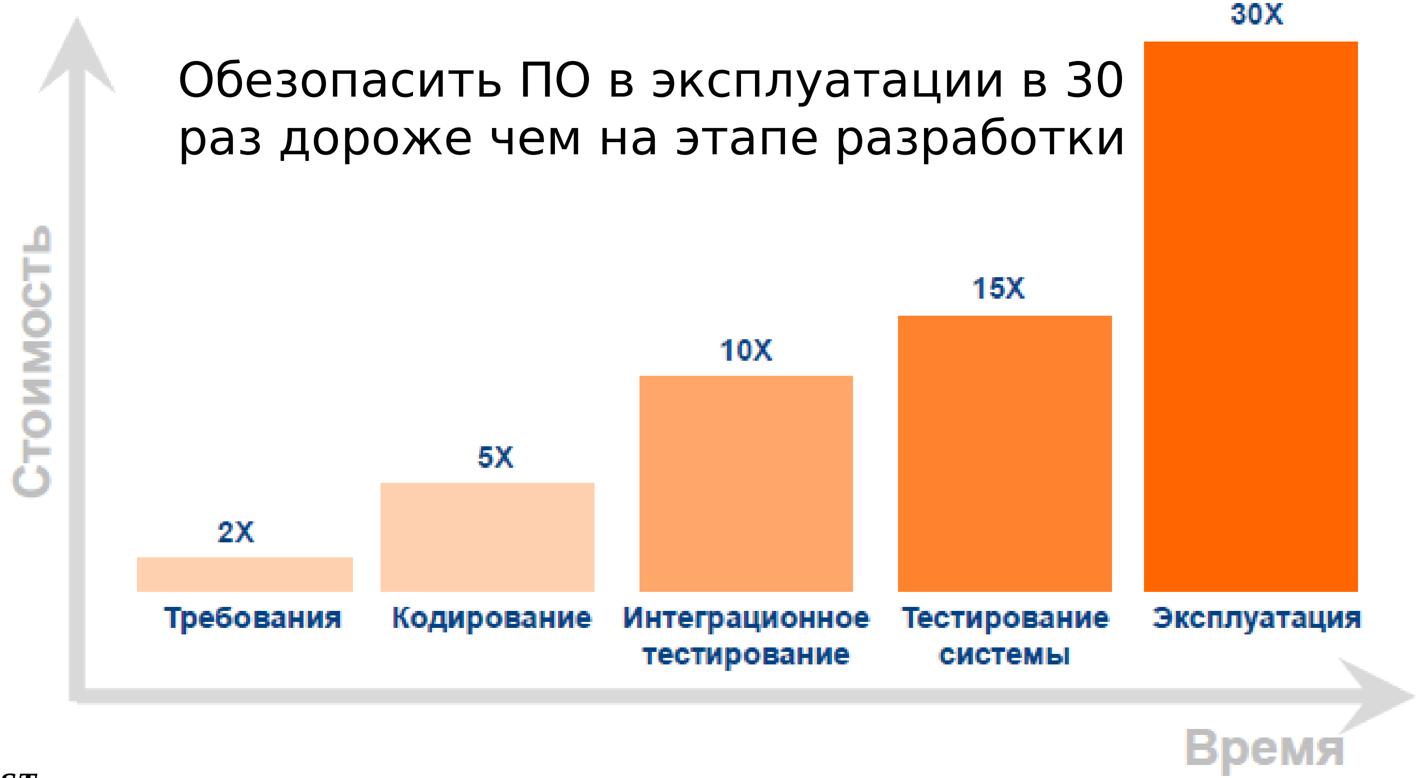
HP Fortify Software Security Assurance

технологии и услуги, направленные на управление, оценку и обработку рисков при разработке ПО

С чем боремся

- ✓ **Межсайтовый скриптинг** – выявлено в приложении электронной коммерции. Уязвимость могла быть использована для кражи данных пользовательской сессии и получения доступа к учетным записям.
- ✓ **Внедрение SQL кода** – злоумышленник имел возможность кражи полного содержимого базы данных, содержащей данные клиентов и учетные записи.
- ✓ **Раскрытие конфиденциальных данных**: информация о данных кредитных карт, деталях банковских счетов попадала в журнал событий приложения.
- ✓ **Недостаточная аутентификация** во внутренних корпоративных приложениях компании. Например, приложение для генерации отчетов позволяло менять пароли пользователей без аутентификации, тем самым позволяя злоумышленнику сменить пароль любого пользователя, включая администратора.

Дешевле и эффективнее – действовать проактивно



Обезопасить ПО в эксплуатации в 30 раз дороже чем на этапе разработки

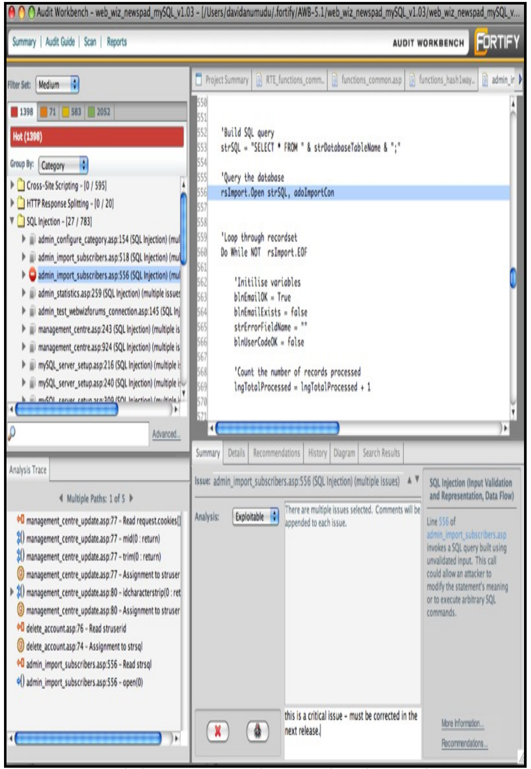
***Source:* NIST**

HP Fortify - решение в любых ситуациях

	Планирование	Разработка		Эксплуатация
Разработчик		HP Fortify SCA		
QA тестер		HP Fortify PTA	HP QAInspect	
ИБ	HP Fortify on Demand			HP WebInspect/ AMP
Эксплуатация				HP Fortify RTA
All Users	HP Fortify 360 Server HP Fortify Collaboration HP Fortify SSA Governance HP Fortify Secure Coding RulePacks/ SecureBase			

HP Fortify Static Code Analyzer

Выявление уязвимостей в исходном коде



- Cross-Site Scripting - [0 / 595]
- HTTP Response Splitting - [0 / 20]
- SQL Injection - [27 / 783]
  - admin_configure_category.asp:154 (SQL Injection) (mul
  - admin_import_subscribers.asp:518 (SQL Injection) (mul
  - admin_import_subscribers.asp:556 (SQL Injection) (mul
  - admin_statistics.asp:259 (SQL Injection) (multiple issues
  - admin_test_webwizforums_connection.asp:145 (SQL Inj
  - management_centre.asp:243 (SQL Injection) (multiple is
  - management_centre.asp:924 (SQL Injection) (multiple is
  - mySQL_server_setup.asp:216 (SQL Injection) (multiple i
  - mySQL_server_setup.asp:240 (SQL Injection) (multiple i

```
'Build SQL query
strSQL = "SELECT * FROM " & strDatabaseTableName & ";"

'Query the database
rsImport.Open strSQL, adoImportCon


'Loop through recordset
Do While NOT  rsImport.EOF

    'Initilise variables
    blnEmailOK = True
    blnEmailExists = false
    strErrorFieldName = ""
    blnUserCodeOK = false

    'Count the number of records processed
    lngTotalProcessed = lngTotalProcessed + 1
```

management_centre_update.asp:77 - Read request.cookies[]
management_centre_update.asp:77 - mid(0 : return)
management_centre_update.asp:77 - trim(0 : return)
management_centre_update.asp:77 - Assignment to struser
management_centre_update.asp:80 - idcharacterstrip(0 : ret
management_centre_update.asp:80 - Assignment to struser
delete_account.asp:76 - Read struserid
delete_account.asp:74 - Assignment to strsql
admin_import_subscribers.asp:556 - Read strsql
admin_import_subscribers.asp:556 - open(0)

Issue: admin_import_subscribers.asp:556 (SQL Injection) (multiple issues)

Analysis: Exploitable

There are multiple issues selected. Comments will be appended to each issue.

this is a critical issue - must be corrected in the next release.

SQL Injection (Input Validation and Representation, Data Flow)

Line 556 of admin_import_subscribers.asp invokes a SQL query built using unvalidated input. This call could allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.

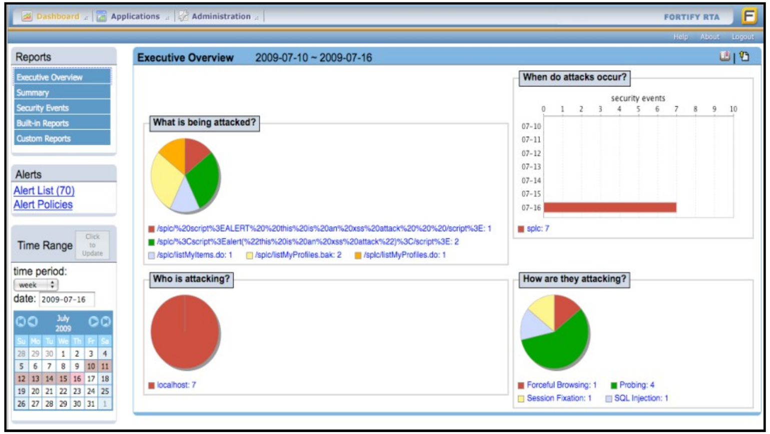
HP Fortify SCA позволяет обнаружить источник уязвимостей с помощью комплексного набора правил, поддерживающего множество языков, платформ и средств разработки.

Основные возможности:

- проведение статического анализа для выявления уязвимостей в исходном коде;
- обнаружение уязвимостей в коде на 20 языках программирования
- результаты сортируются по степени риска и рекомендациям по устранению уязвимостей.

HP Fortify Real-Time Analyzer

Защита развернутых приложений в режиме реального времени



- ✓Блокирование атак в развернутых приложениях для минимизации рисков ИБ
- ✓Немедленное решение для обеспечения соответствия требованиям стандартов и регуляторов
- ✓Обеспечение защиты до устранения уязвимостей в приложениях.

HP Fortify RTA работает внутри развернутых Java и .NET приложений для мониторинга и защиты их от атак. Он автоматически определяет каждое критическое API внутри приложения и мониторит его. Это позволяет понять существующие уязвимости и отвечать на атаки разными способами: блокированием пользователя, уведомление администратора, задержка пользовательского запроса на коммутирующем оборудовании и пр.

Дополнительно, HP Fortify RTA позволяет быстро установить определенные правила в любые приложения для противодействия обману и прочим угрозам.

HP WebInspect

Быстрое обнаружение уязвимостей в web-приложениях и сервисах

Быстрое обнаружение уязвимостей

- проверка большего количества приложений за меньшее время

Предоставление нужной информации

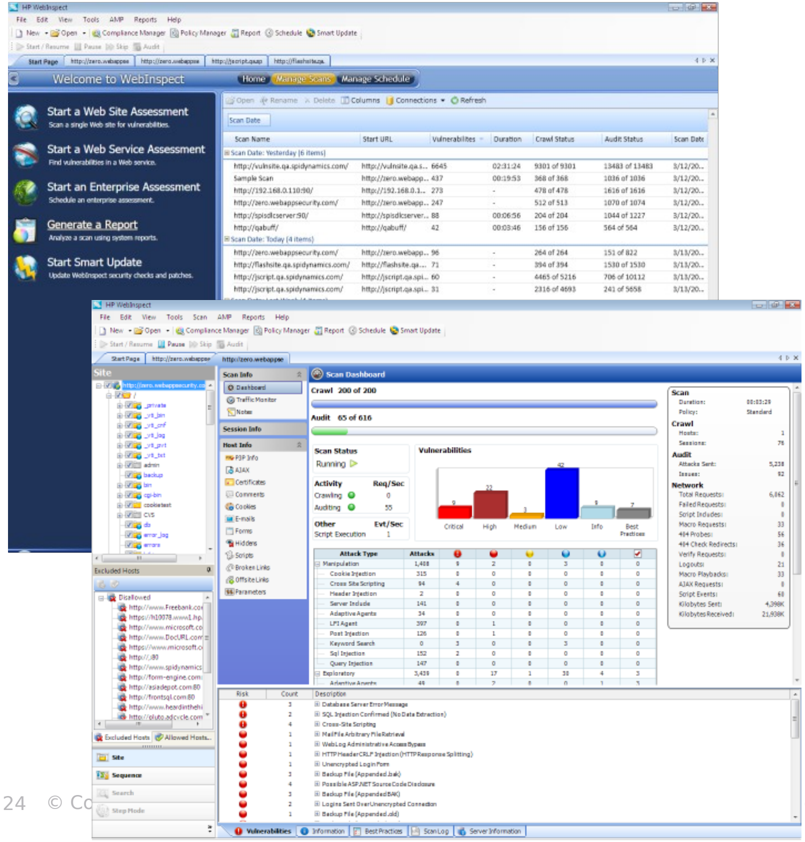
- фокус на важных аспектах

Расширение используемых технологий

- тестирование новых технологий на новые уязвимости
- J avaScript, Ajax, Flash, Oracle ADF
- поддержка HP Web Security Research Group

Эффективное устранение уязвимостей

•расширенное описание, примеры кода и контента


HP WebInspect
File Edit View Tools AMP Reports Help
New Open Compliance Manager Policy Manager Report Schedule Smart Update
Start / Resume Pause Skip Audit
Start Page
Welcome to WebInspect
Home Manage Scans Manage Schedule
Open Rename Delete Columns Connections Refresh
Scan Date

Start a Web Site Assessment
Scan a single Web site for vulnerabilities.

Start a Web Service Assessment
Find vulnerabilities in a Web service.

Start an Enterprise Assessment
Schedule an enterprise assessment.

Generate a Report
Analyze a scan using system reports.

Start Smart Update
Update WebInspect security checks and patches.

Scan Name	Start URL	Vulnerabilites	Duration	Crawl Status	Audit Status	Scan Date
Scan Date: Yesterday (6 items)						
http://vulnsite.qa.spidynamics.com/	http://vulnsite.qa.s...	6645	02:31:24	9301 of 9301	13483 of 13483	3/12/20...
Sample Scan	http://zero.webapp...	437	00:19:53	368 of 368	1036 of 1036	3/12/20...
http://192.168.0.110:90/	http://192.168.0.1...	273	-	478 of 478	1616 of 1616	3/12/20...
http://zero.webappsecurity.com/	http://zero.webapp...	247	-	512 of 513	1070 of 1074	3/12/20...
http://spisdlcserver:90/	http://spisdlcserver...	88	00:06:56	204 of 204	1044 of 1227	3/12/20...
http://qabuff/	http://qabuff/	42	00:03:46	156 of 156	564 of 564	3/12/20...
Scan Date: Today (4 items)						
http://zero.webappsecurity.com/	http://zero.webapp...	96	-	264 of 264	151 of 822	3/13/20...
http://flashsite.qa.spidynamics.com/	http://flashsite.qa....	71	-	394 of 394	1530 of 1530	3/13/20...
http://jscript.qa.spidynamics.com/	http://jscript.qa.spi...	60	-	4465 of 5216	706 of 10112	3/13/20...
http://jscript.qa.spidynamics.com/	http://jscript.qa.spi...	31	-	2316 of 4693	241 of 5658	3/13/20...

Crawl 200 of 200

Audit 65 of 616

Scan Status
Running

Activity	Req/Sec
Crawling	0
Auditing	55

Other	Evt/Sec
Script Execution	1

Scan
Duration: 00:03:29
Policy: Standard

Crawl
Hosts: 1
Sessions: 76

Audit
Attacks Sent: 5,238
Issues: 92

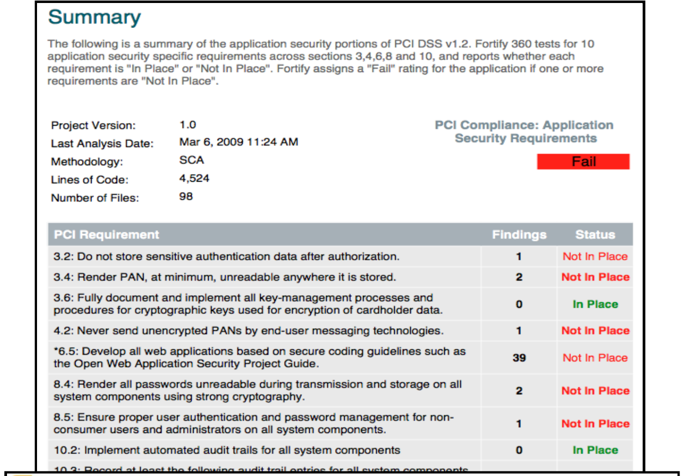
Network
Total Requests: 6,862
Failed Requests: 0
Script Includes: 0
Macro Requests: 33
404 Probes: 56
404 Check Redirects: 36
Verify Requests: 0
Logouts: 21
Macro Playbacks: 33
AJAX Requests: 0
Script Events: 68
Kilobytes Sent: 4,398K
Kilobytes Received: 21,938K

Attack Type	Attacks	●	●	●	●	●	✓
⊟ Manipulation	1,488	9	2	0	3	0	0
Cookie Injection	315	0	0	0	0	0	0
Cross Site Scripting	94	4	0	0	0	0	0
Header Injection	2	0	0	0	0	0	0
Server Include	141	0	0	0	0	0	0
Adaptive Agents	34	0	0	0	0	0	0
LFI Agent	397	0	1	0	0	0	0
Post Injection	126	0	1	0	0	0	0
Keyword Search	0	3	0	0	3	0	0
Sql Injection	152	2	0	0	0	0	0
Query Injection	147	0	0	0	0	0	0
⊟ Exploratory	3,439	0	17	1	38	4	3
Adaptive Agents	49	0	2	0	0	1	3

Risk	Count	Description
●	3	⊞ Database Server Error Message
●	2	⊞ SQL Injection Confirmed (No Data Extraction)
●	4	⊞ Cross-Site Scripting
●	1	⊞ MailFile Arbitrary File Retrieval
●	1	⊞ WebLog Administrative Access Bypass
●	1	⊞ HTTP Header CRLF Injection (HTTP Response Splitting)
●	1	⊞ Unencrypted Login Form
●	3	⊞ Backup File (Appended .bak)
●	4	⊞ Possible ASP.NET Source Code Disclosure
●	3	⊞ Backup File (Appended BAK)
●	2	⊞ Logins Sent Over Unencrypted Connection
●	1	⊞ Backup File (Appended .old)

HP Fortify Governance

Эффективное управление программой безопасности ПО



Summary

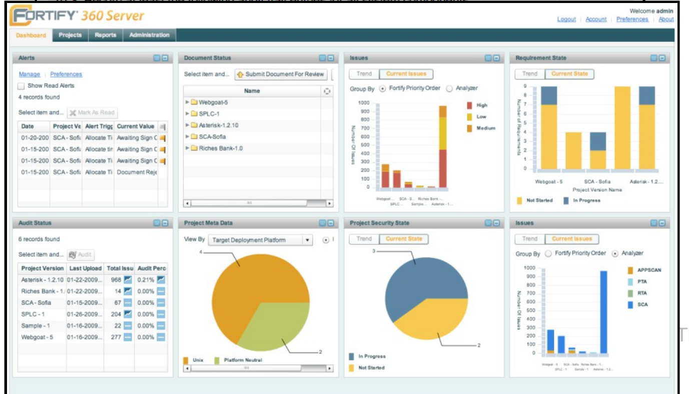
The following is a summary of the application security portions of PCI DSS v1.2. Fortify 360 tests for 10 application security specific requirements across sections 3,4,6,8 and 10, and reports whether each requirement is "In Place" or "Not In Place". Fortify assigns a "Fail" rating for the application if one or more requirements are "Not In Place".

Project Version:	1.0
Last Analysis Date:	Mar 6, 2009 11:24 AM
Methodology:	SCA
Lines of Code:	4,524
Number of Files:	98

PCI Compliance: Application Security Requirements

Fail

PCI Requirement	Findings	Status
3.2: Do not store sensitive authentication data after authorization.	1	Not In Place
3.4: Render PAN, at minimum, unreadable anywhere it is stored.	2	Not In Place
3.6: Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	0	In Place
4.2: Never send unencrypted PANs by end-user messaging technologies.	1	Not In Place
*6.5: Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project Guide.	39	Not In Place
8.4: Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	2	Not In Place
8.5: Ensure proper user authentication and password management for non-consumer users and administrators on all system components.	1	Not In Place
10.2: Implement automated audit trails for all system components	0	In Place
10.3: Record at least the following audit trail entries for all system components		



4 records found

Select item and...

Date	Project Ve	Alert Trigg	Current Value
01-20-200	SCA - Sofi	Allocate Ti	Awaiting Sign C
01-15-200	SCA - Sofi	Allocate tir	Awaiting Sign C
01-15-200	SCA - Sofi	Allocate Ti	Awaiting Sign C
01-15-200	SCA - Sofi	Allocate Ti	Document Reje

Select item and...

Name
Webgoat-5
SPLC-1
Asterisk-1.2.10
SCA-Sofia
Riches Bank-1.0

6 records found

Select item and...

Project Version	Last Upload	Total Issu	Audit Perc
Asterisk - 1.2.10	01-22-2009...	968	0.21%
Riches Bank - 1.	01-22-2009...	14	0.00%
SCA - Sofia	01-15-2009...	67	0.00%
SPLC - 1	01-26-2009...	204	0.00%
Sample - 1	01-16-2009...	22	0.00%
Webgoat - 5	01-16-2009...	277	0.00%

HP Fortify Governance – средство управления активами, деятельностью и результатами в проектах по обеспечению безопасности ПО.

Возможности:

- оптимизация инвестиций в программу управления безопасностью;
- фокусировка команды на инновациях и сдаче проекта в срок вместо «управления» безопасностью;
- поддержка инвентаризации приложений посредством централизованного менеджера рисков;
- автоматизация деятельности по снижению рисков, основанная на профиле риска.

HP Information Security Pulse

Mobile Security App

HP Introduces Information Security PULSE

The new HP mobile app designed to bring visibility and awareness to cyber threats and attacks worldwide.

Built with HP Proprietary data from HP’s DV Labs (through Tipping Point), this app can help enterprises realize the extent to which their information may be exposed to exploits, if they are not using HP IPS solutions

Customer Benefits

Provides customers with free access to HP Dvlabs proprietary cyber threat data

Helps people in security and non-security roles to see and understand the threats and attack trends that may affect their enterprise

Helps educate customers about cyber security situational awareness

App Development

Content

- Data retrieved on a daily basis from HP DV Labs ThreatLinq
- Newsfeeds aggregated daily, ability to add personal news feeds

App interface

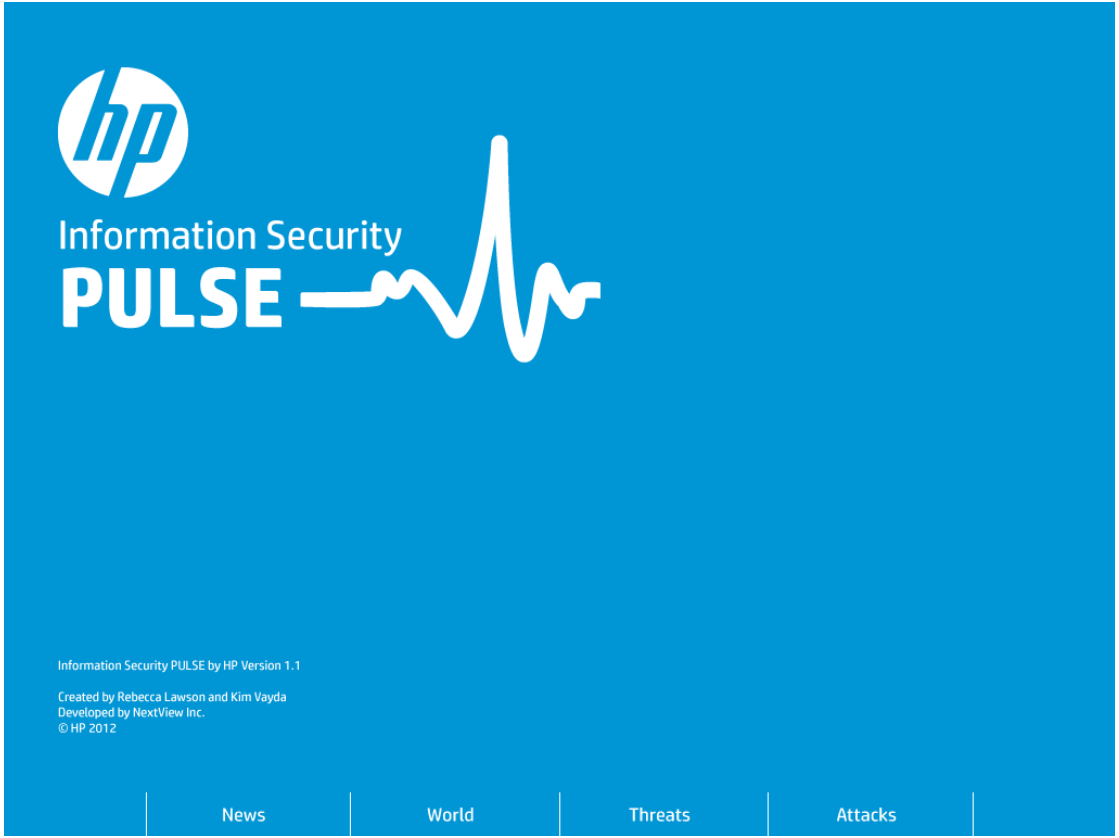
- Developed and managed by NextView (HP approved vendor)
- Support request emails go to NextView for app issues

Availability

- iPad – now in iTunes store
- iPhone – in production – target August 31
- webOS device (HP Touchpad) – now in webOS App store
- Android device - in production – target August 31
- Web browser – now at www.hpinfosecpulse.com

HP Information Security Pulse

Home page

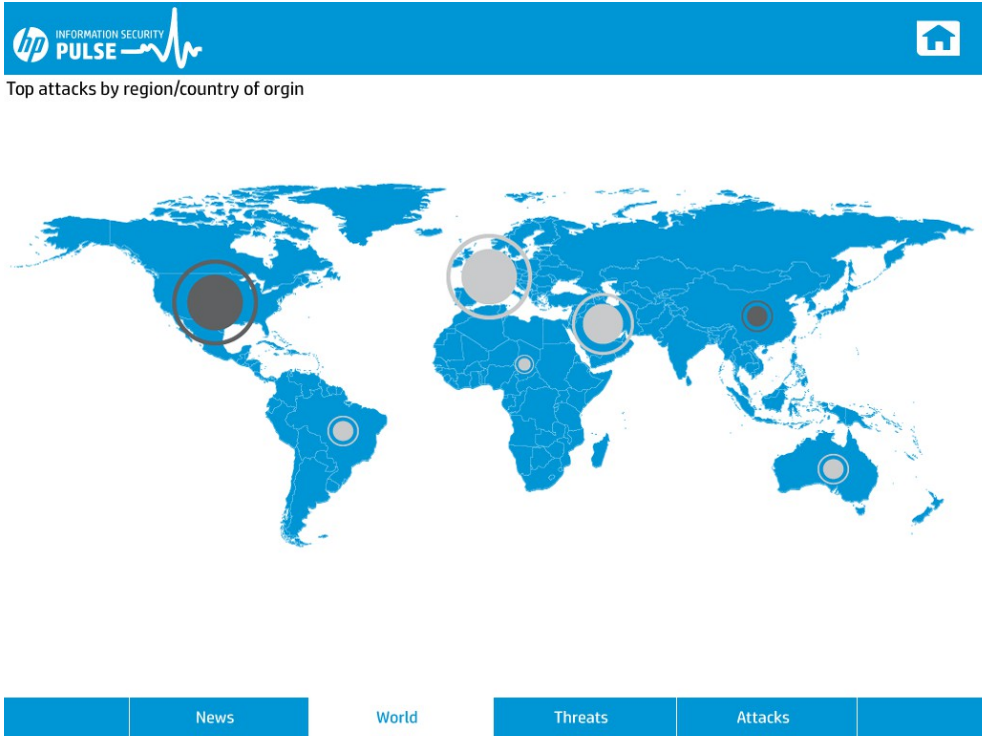


Information Security PULSE by HP Version 1.1

Created by Rebecca Lawson and Kim Vayda
Developed by NextView Inc.
© HP 2012

HP Information Security Pulse

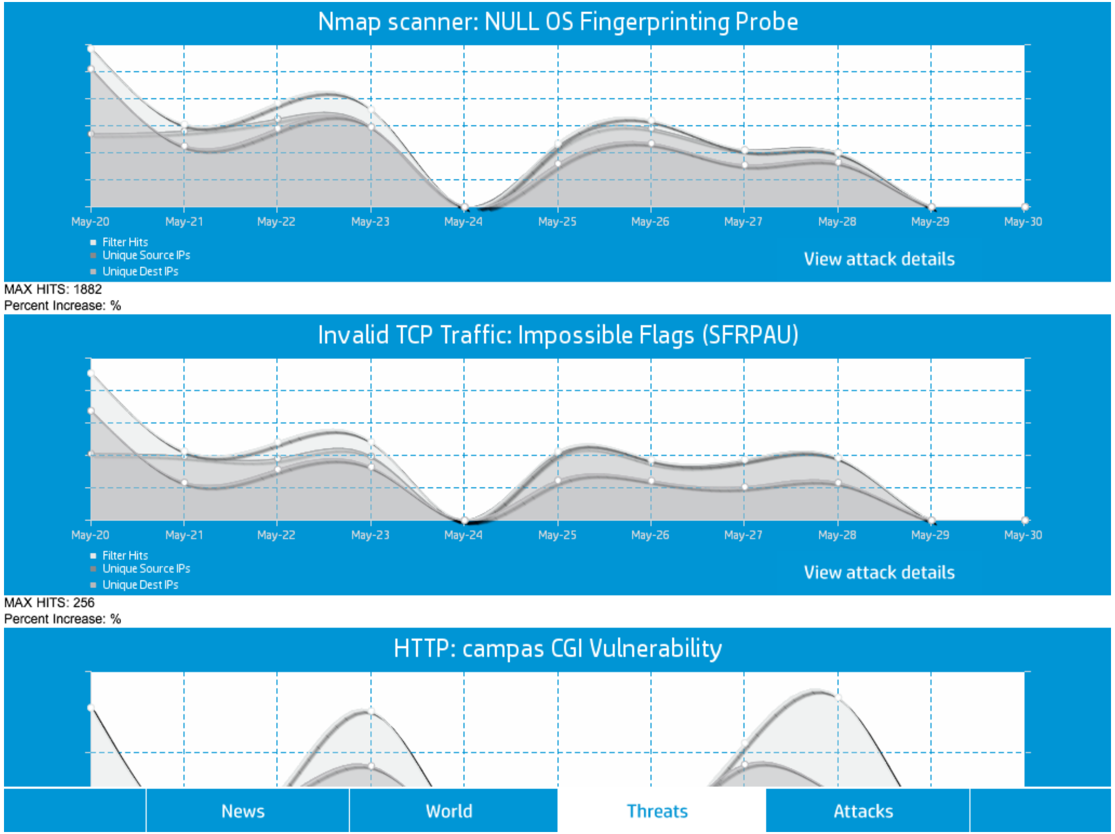
Worldwide Top Attacks



Top attacks by region/country of orgin

HP Information Security Pulse

Top trending threats



Nmap scanner: NULL OS Fingerprinting Probe

MAX HITS: 1882
Percent Increase: %

Invalid TCP Traffic: Impossible Flags (SFRPAU)

MAX HITS: 256
Percent Increase: %

HTTP: campas CGI Vulnerability

Sample screenshot showing
May 20-30, 2012

Спасибо.