

HP Fortify

¿Confías en la seguridad de tu software?



Victor Rojo
Solutions Architect – HP ESP

Victor Rojo

- Programador experimentado y pragmático que ha sido gerente y director de desarrollo de software y tecnología
- 12 años de experiencia en el “campo de batalla” en empresas de Telecomunicaciones, Pensiones, Manufactura y Consultoría
- Ingeniero en Electrónica con Especialidad en Sistemas Digitales en la Universidad Autónoma Metropolitana – Azcapotzalco
- Escribió su primer programa para Atari en 1988



Agenda

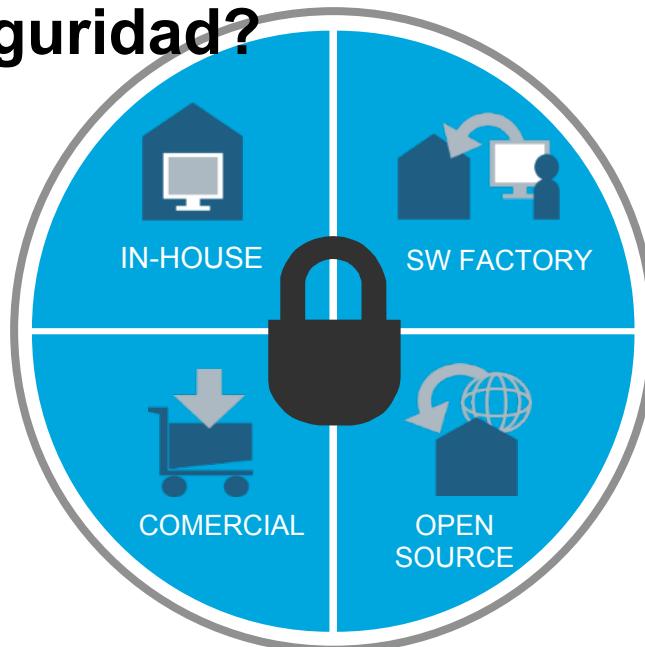
- ¿Donde hay aplicaciones?
- ¿Confiabilidad o seguridad?
- El reto de la seguridad en el software
- ¿Qué es la seguridad aplicativa?
- Software Security Assurance (SSA) Framework
- Portafolio de Soluciones HP Fortify
- Posicionamiento en la industria
- Mitos sobre las soluciones HP Fortify
- Resumen



¿Dónde hay aplicaciones?



¿Confiabilidad o seguridad?



Un software **confiable** hace lo que se supone que debe hacer...

Una software **seguro** hace lo que se supone que debe hacer...

¿Confiabilidad o seguridad?



El reto en la seguridad en el software



Beneficios

Seguridad Aplicativa

Situación Actual



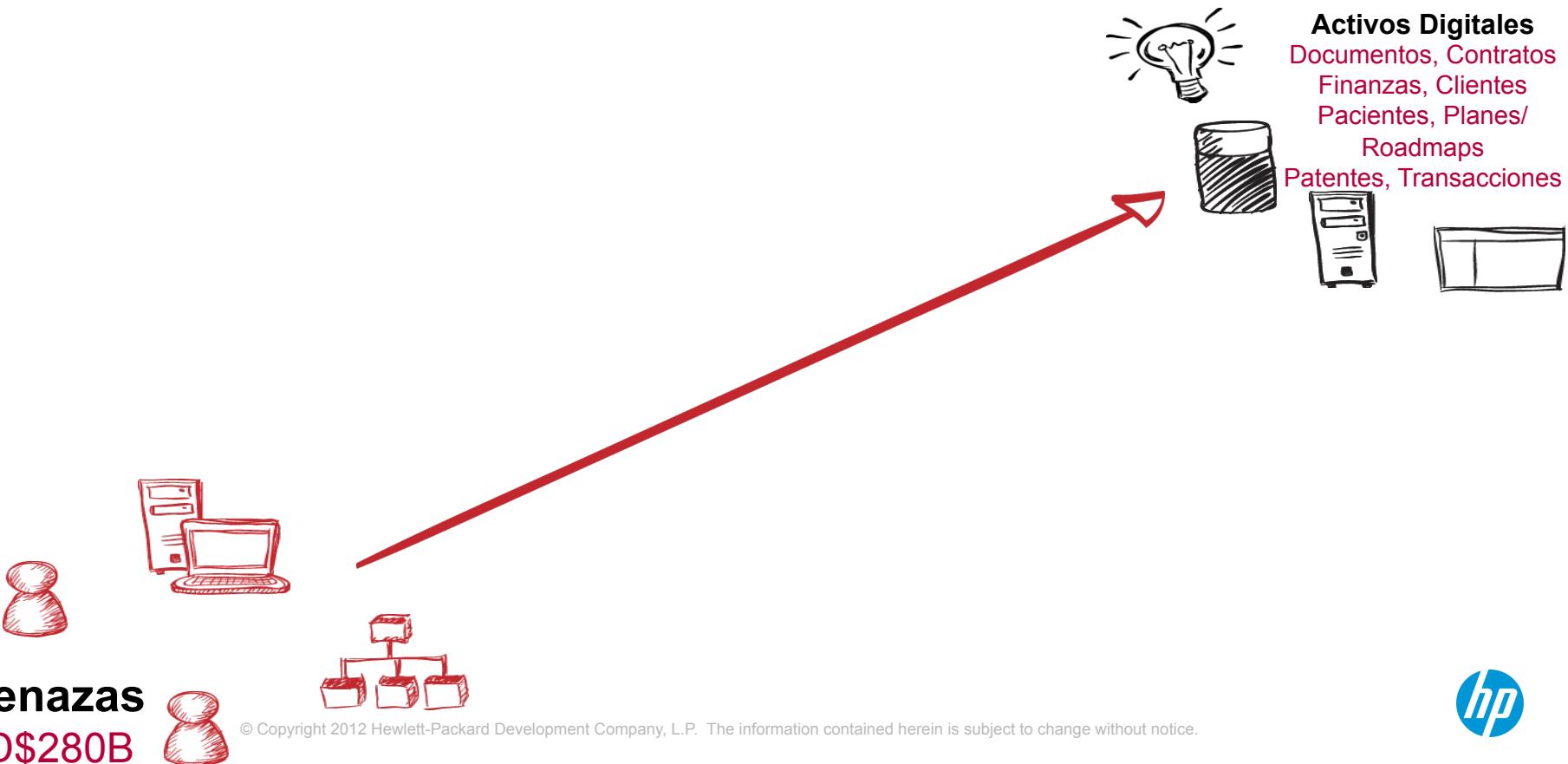
Activos Digitales

Documentos, Contratos
Finanzas, Clientes
Pacientes, Planes/
Roadmaps
Patentes, Transacciones

Beneficios

Seguridad Aplicativa

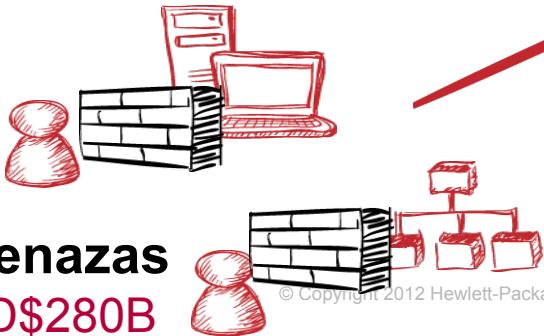
Situación Actual



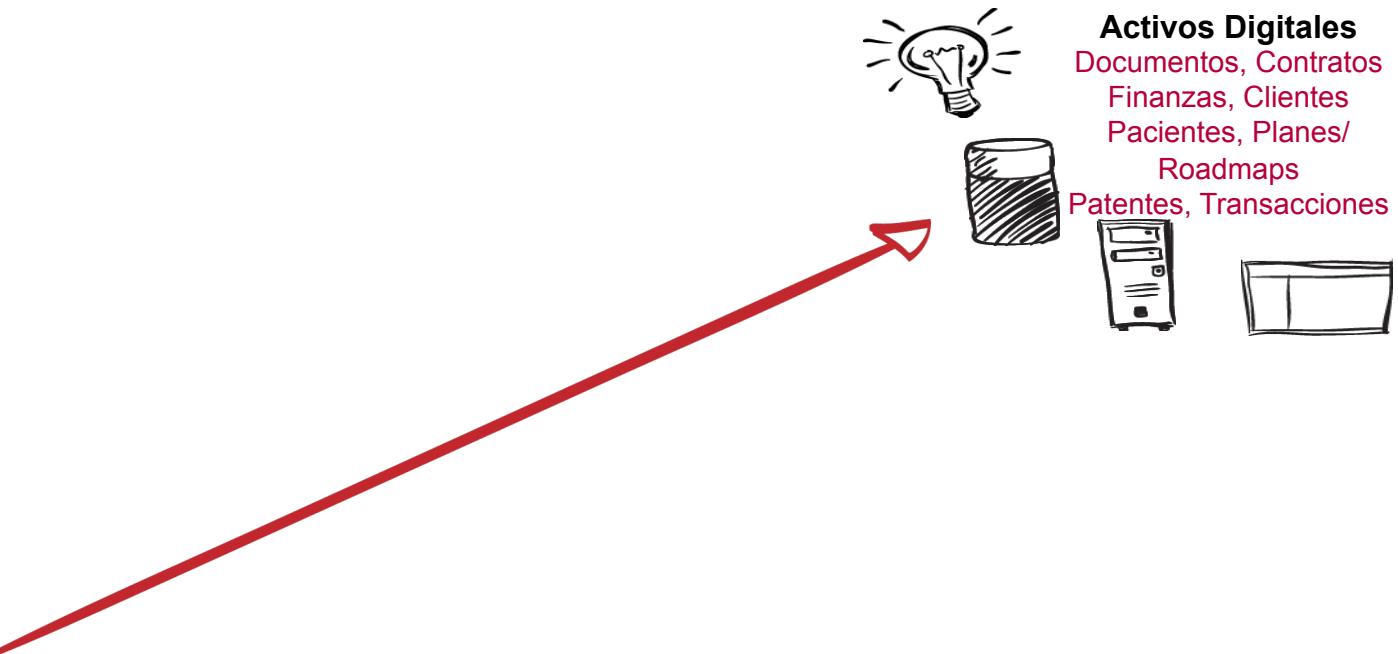
Beneficios

Seguridad Aplicativa

Situación Actual



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



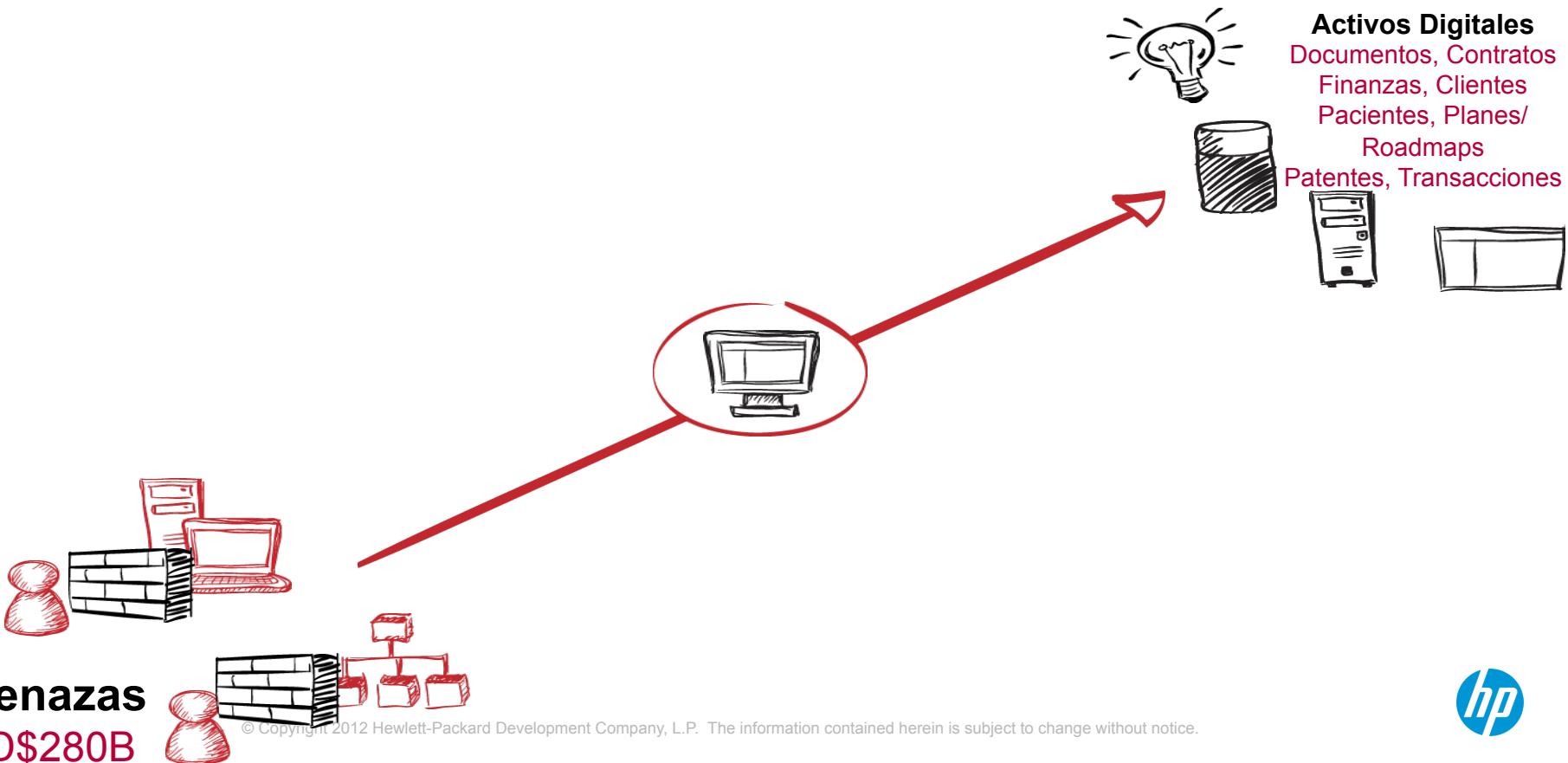
Activos Digitales
Documentos, Contratos
Finanzas, Clientes
Pacientes, Planes/
Roadmaps
Patentes, Transacciones



Beneficios

Seguridad Aplicativa

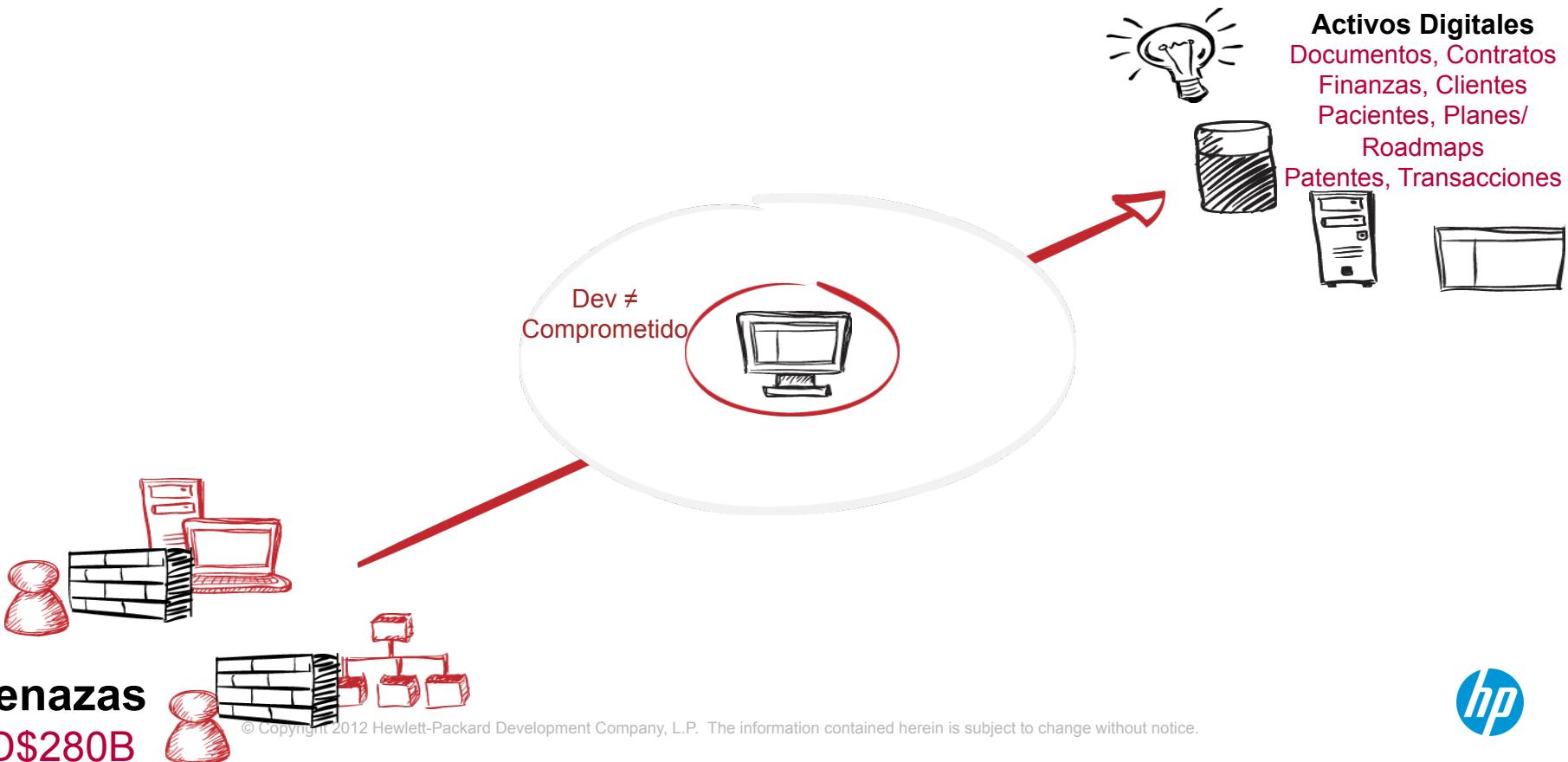
Situación Actual



Beneficios

Seguridad Aplicativa

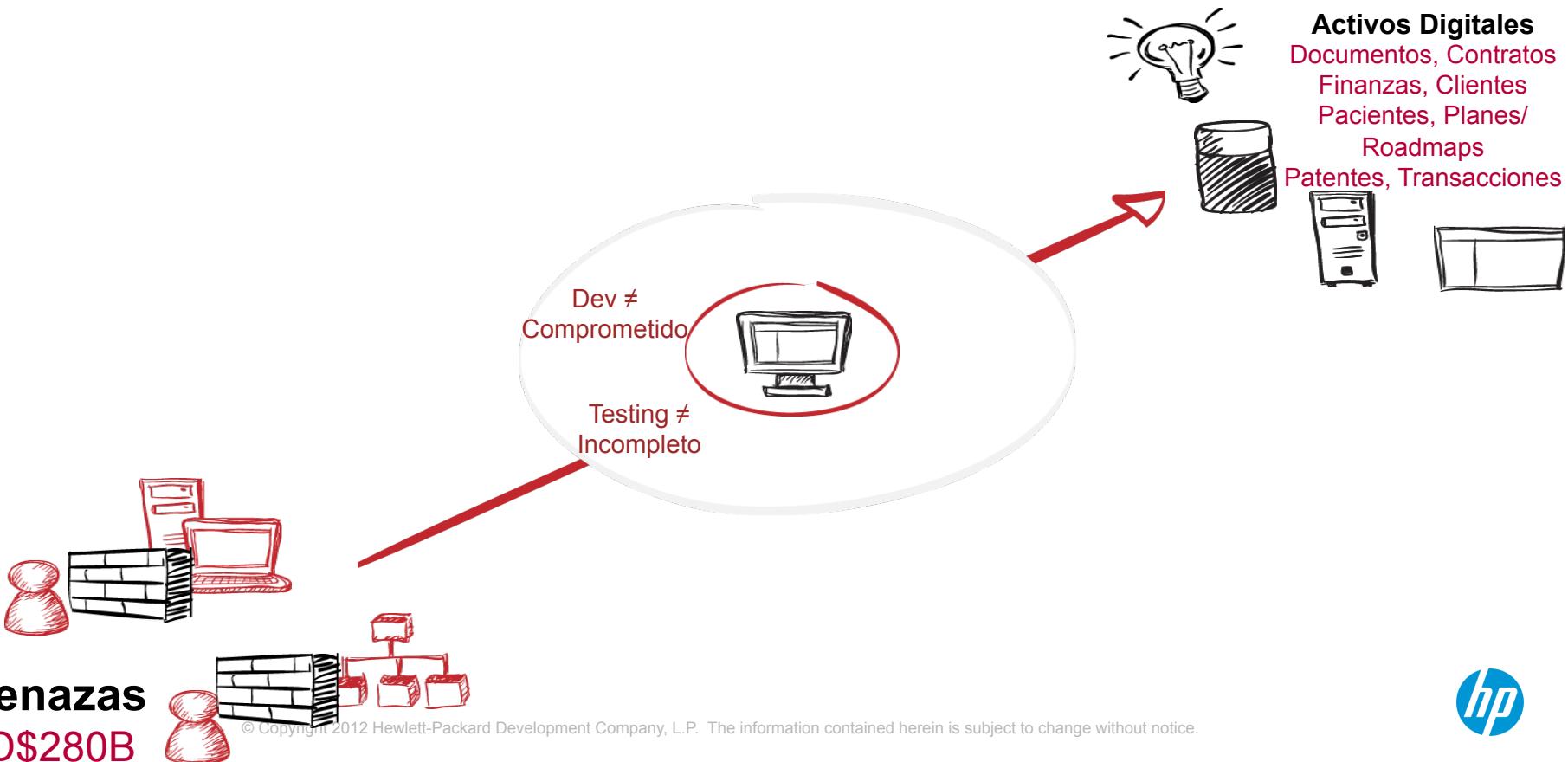
Situación Actual



Beneficios

Seguridad Aplicativa

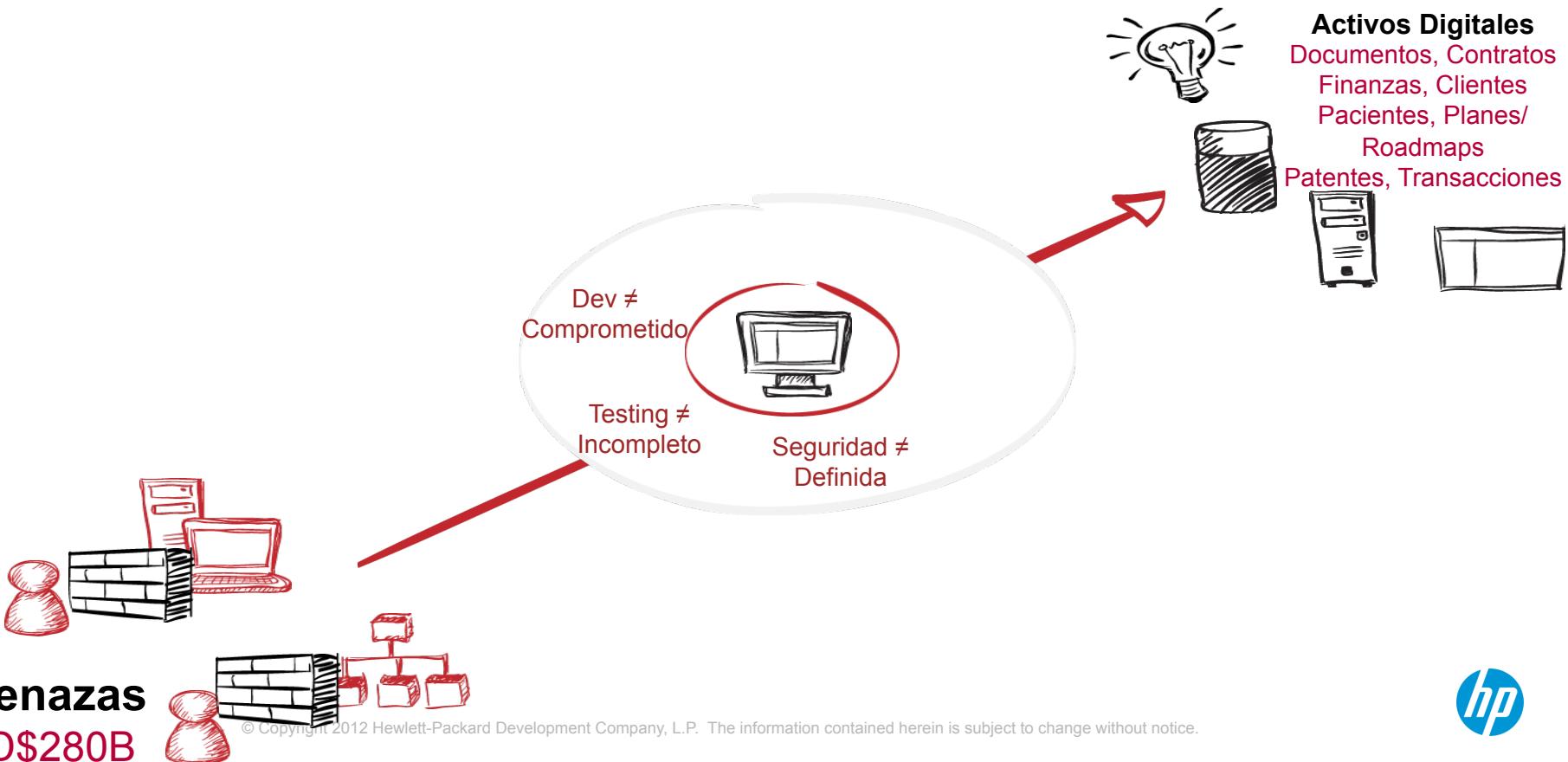
Situación Actual



Beneficios

Seguridad Aplicativa

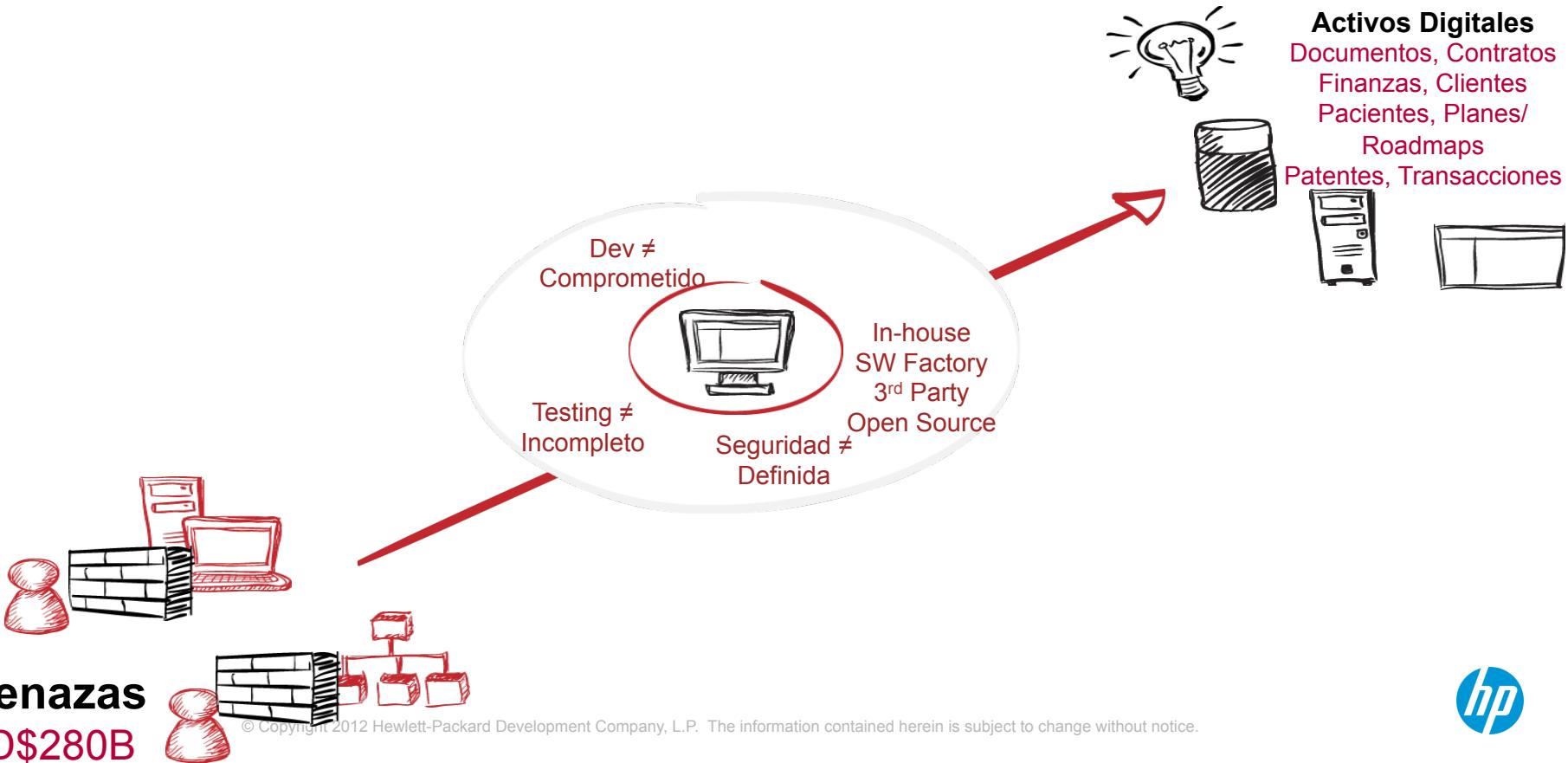
Situación Actual



Beneficios

Seguridad Aplicativa

Situación Actual



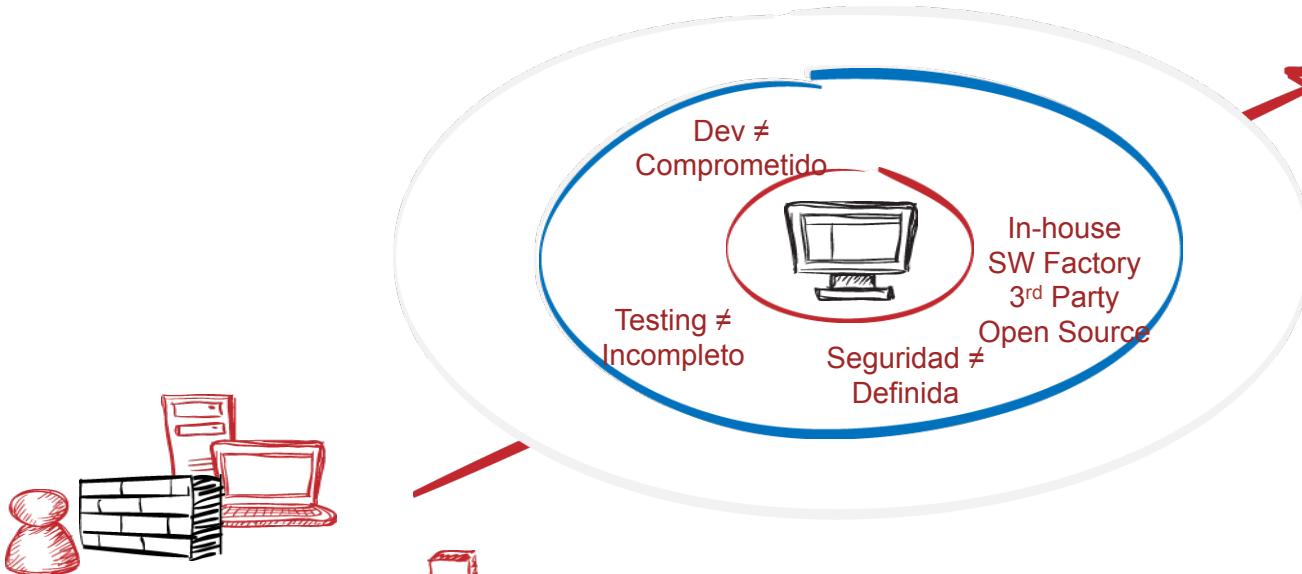
15
Amenazas
USD\$280B



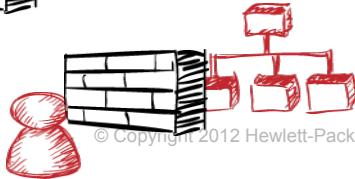
Beneficios

Seguridad Aplicativa

Situación Actual



Amenazas
16
USD\$280B



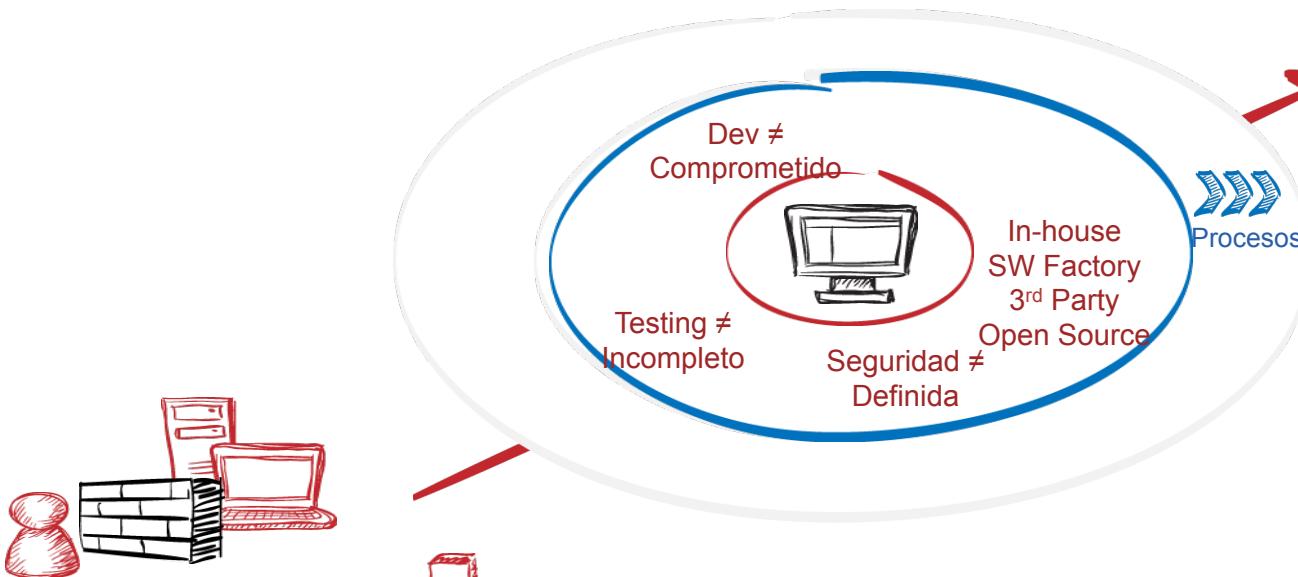
© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



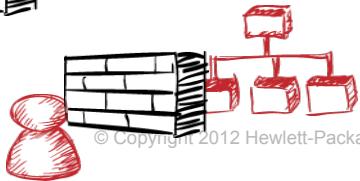
Beneficios

Seguridad Aplicativa

Situación Actual



17
Amenazas
USD\$280B



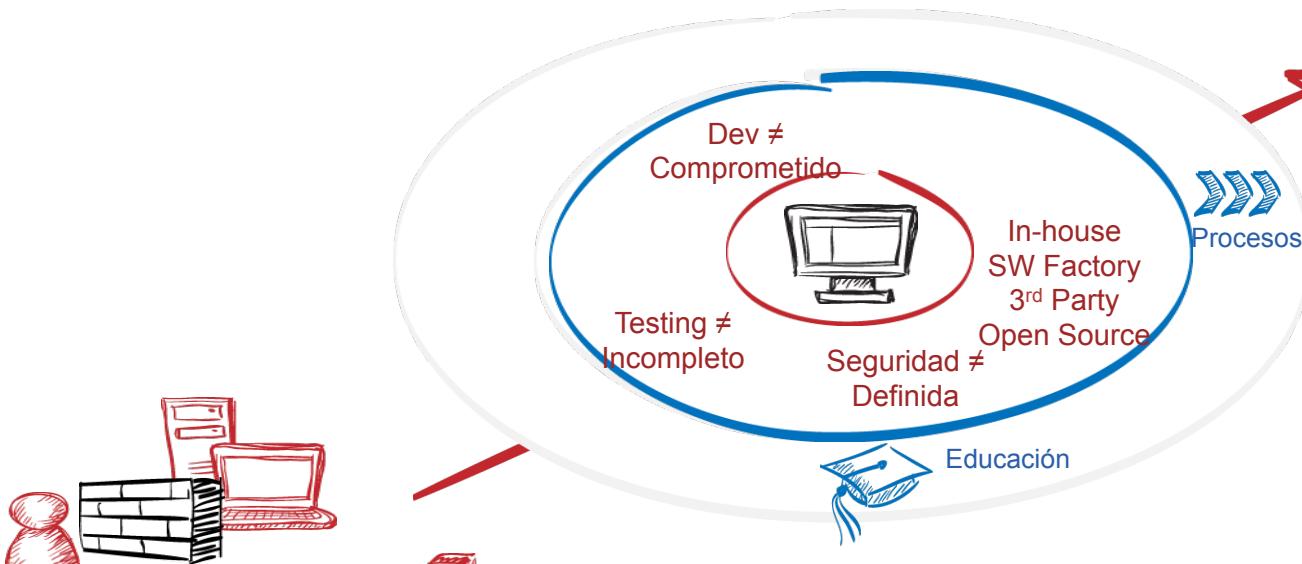
© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



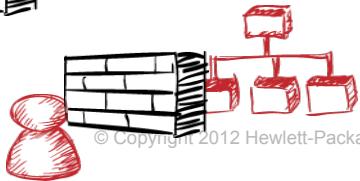
Beneficios

Seguridad Aplicativa

Situación Actual



18
Amenazas
USD\$280B



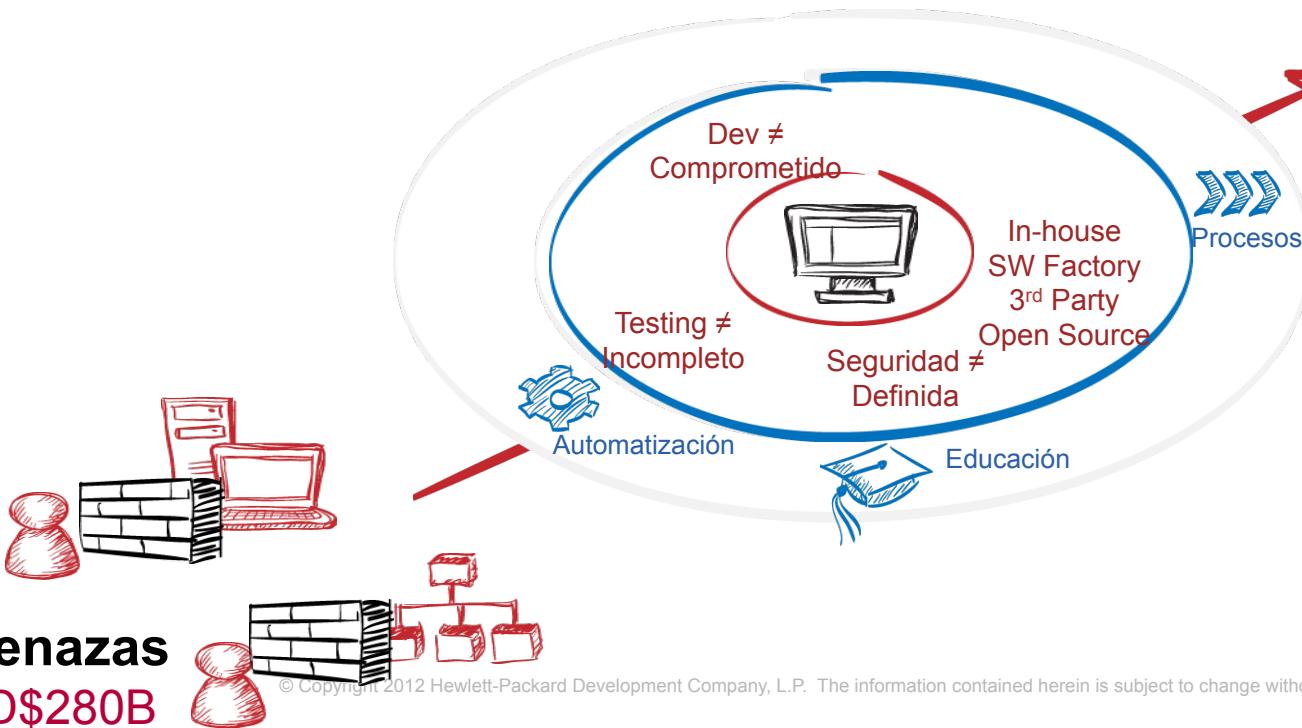
© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



Beneficios

Seguridad Aplicativa

Situación Actual



Activos Digitales
Documentos, Contratos
Finanzas, Clientes
Pacientes, Planes/
Roadmaps
Patentes, Transacciones

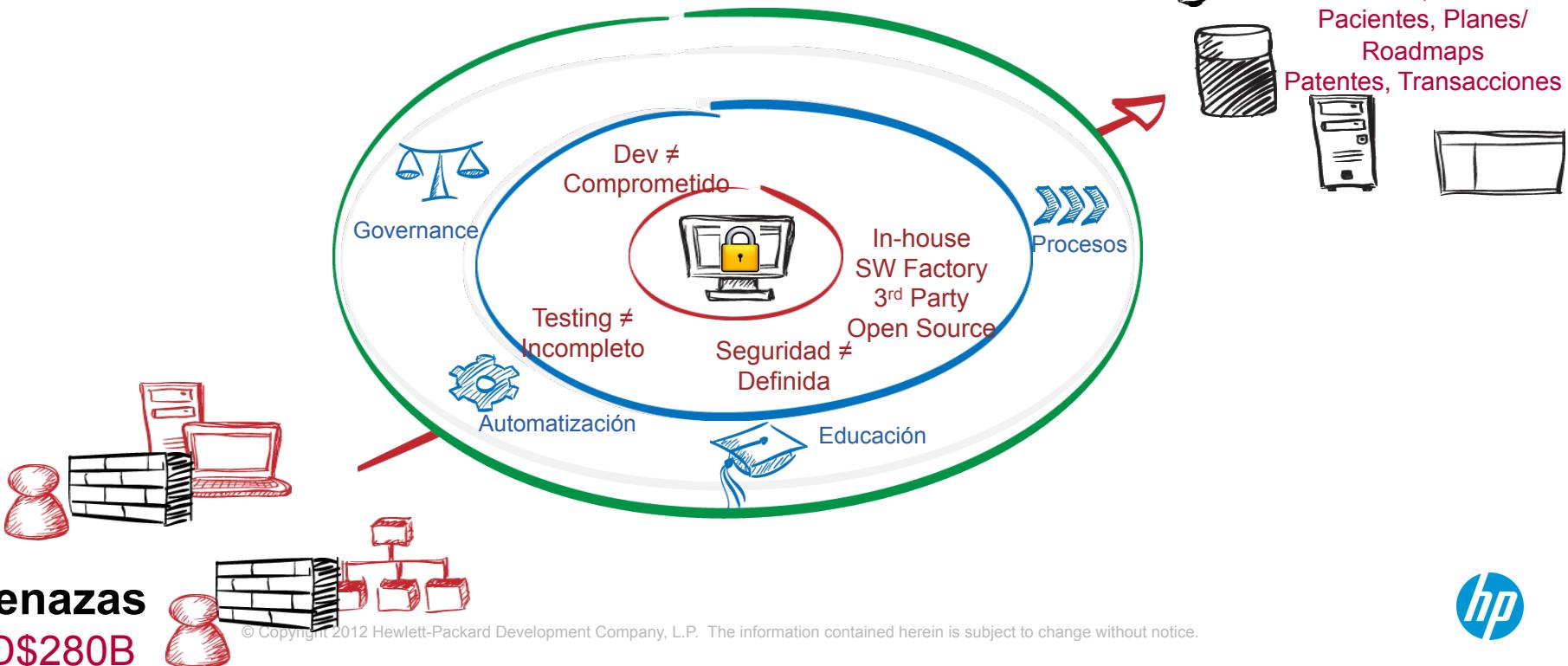
Amenazas
USD\$280B



Beneficios

Seguridad Aplicativa

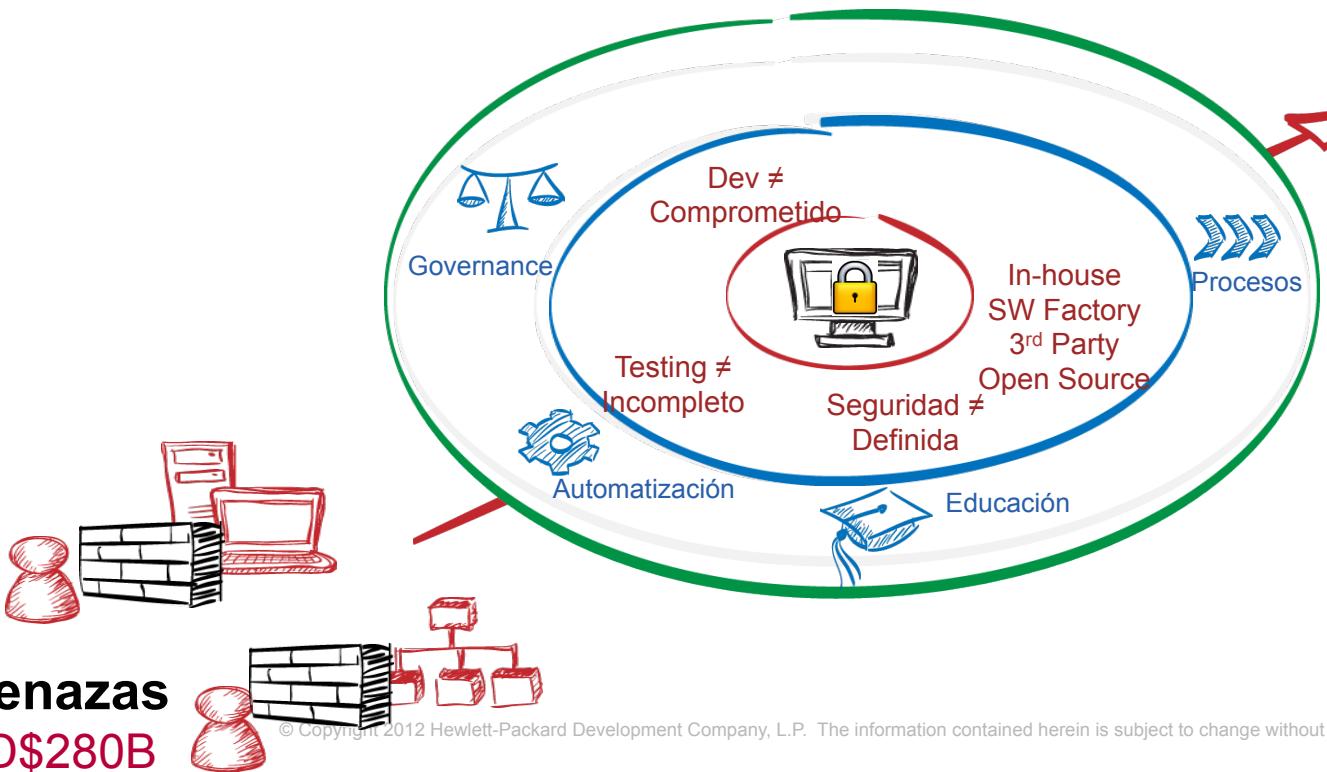
Situación Actual



Beneficios

Seguridad Aplicativa

Situación Actual



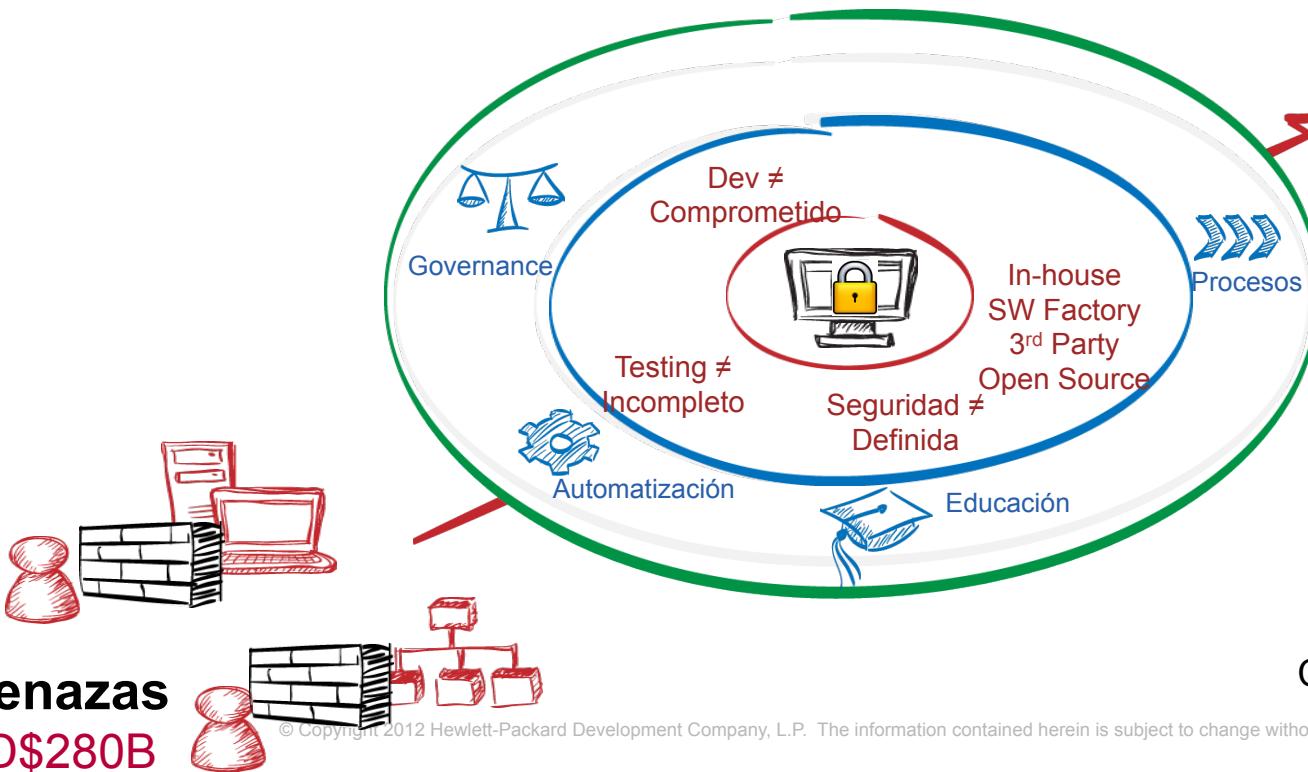
Valor para el
negocio ↗
Nivel de Riesgo



Beneficios

Seguridad Aplicativa

Situación Actual



Valor para el
negocio

Nivel de Riesgo

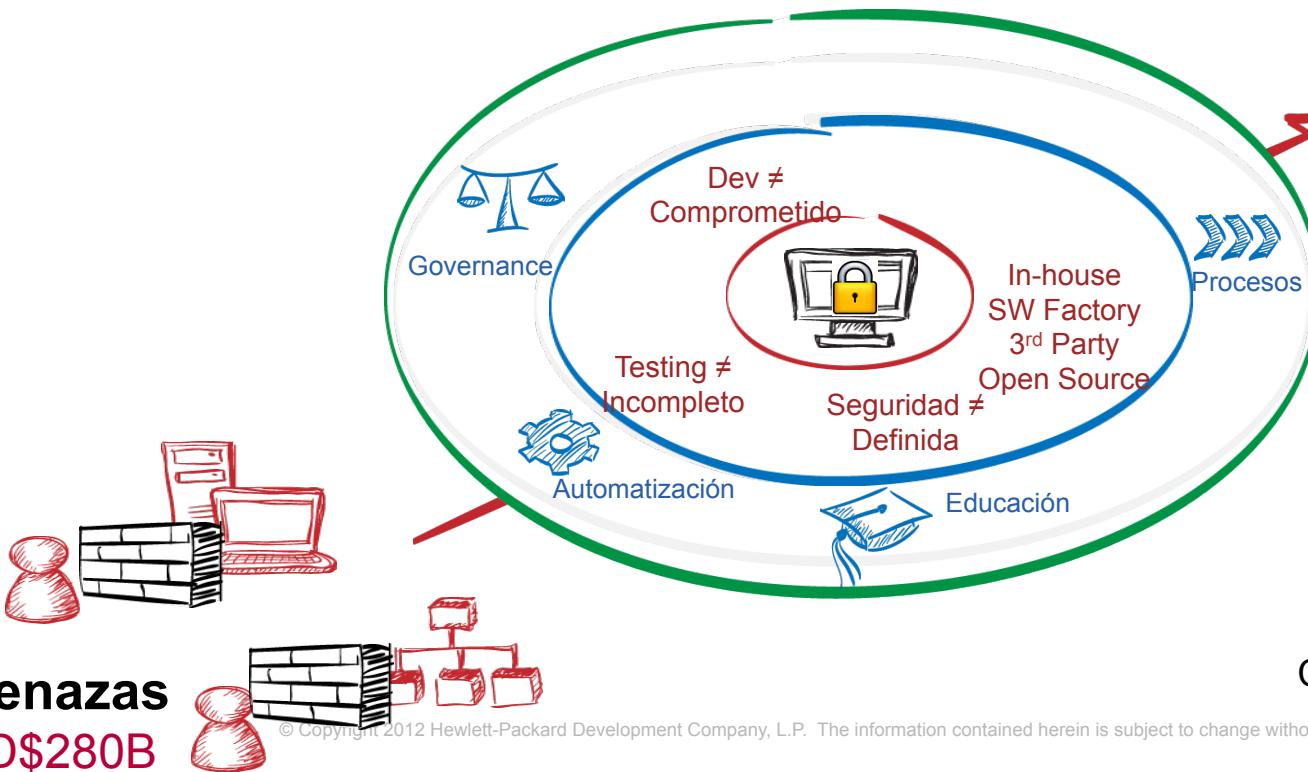
Costos de SW Dev



Beneficios

Seguridad Aplicativa

Situación Actual



Valor para el
negocio

Nivel de Riesgo

Costos de SW Dev

Ahorros \$\$



HP Fortify Software Security Assurance (SSA) Framework



- Alineado con el modelo de madurez de seguridad en el software (SAMM – www.opensamm.org)
- Modelo sistemático para organizar, implementar y medir las capacidades de seguridad aplicativa
- Consta de cuatro disciplinas y doce áreas funcionales que cubren todos los aspectos de seguridad en el software
- Integra la experiencia de HP Fortify con alrededor de 500 implementaciones a nivel global

Portafolio de Soluciones

Análisis Estático

Fortify Static Code Analyzer (SCA)

Fortify *on Demand*

Análisis Dinámico

WebsInspect, QAInspect, WI Enterprise

Fortify *on Demand*

Protección

Fortify Runtime

Remediación y Prevención

IDE Plugins
Audit Workbench
Scan Wizard



Desarrolladores y Especialistas de Seguridad

Administración de Vulnerabilidades (Estático, Dinámico, Runtime)

HP Fortify Software Security Center



Auditores y Gerentes de Seguridad, Líderes de Proyecto

Governance

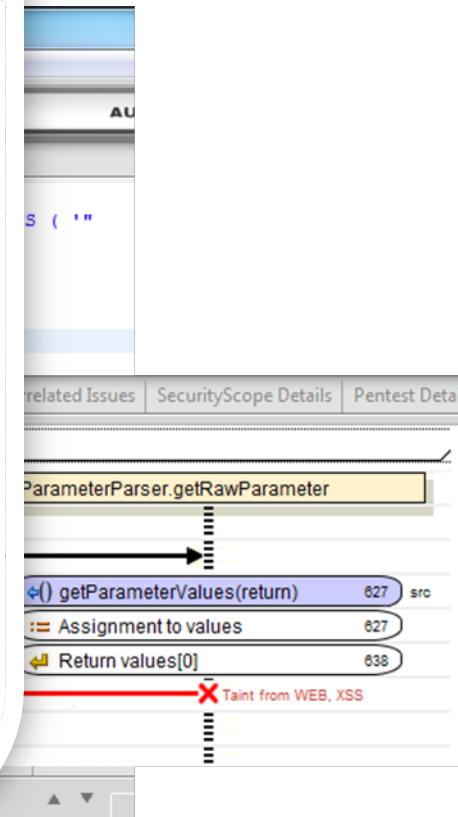
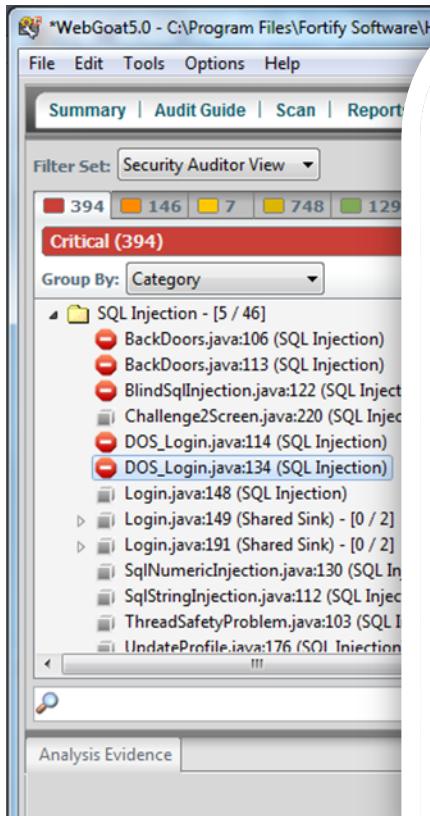
Fortify Governance Module (SSC Server Add-On)



Project, Security, and Management Stakeholders



Fortify SCA (Static Code Analyzer)



HP Fortify Software Security Center (SSC)

HP Fortify Software Security Center

Welcome admin
[Logout](#) | [Account](#) | [Preferences](#) | [About](#)

Dashboard Projects Reports Administration

Alerts

Manage | Preferences
Show Read Alerts
4 records found

Select item and... Mark As Read

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

Document Status

Select item and... Submit Document For Review

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

Issues

Trend Current Issues
Group By Fortify Priority Order Analyzer

Number Of Issues

High (Red), Low (Yellow), Medium (Orange)

Project	High	Low	Medium
Webgoat - 5	~200	~100	~100
SCA - S...	~50	~50	~50
Riches Bank - 1...	~10	~10	~10
SPLC - 1...	~5	~5	~5
Sample - 1...	~2	~2	~2
Asterix - 1...	~1	~1	~1

Requirement State

Trend Current State
Group By Fortify Priority Order Analyzer

Number Of Requirements

Not Started (Yellow), In Progress (Blue)

Project	Not Started	In Progress
Webgoat - 5	~8	~2
SCA - Sofia	~4	~4
Asterisk - 1...	~8	~2

Audit Status

6 records found

Select item and... Audit

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%

Project Meta Data

View By Target Deployment Platform

Unix (Orange), Platform Neutral (Green)

Project Security State

Trend Current State
Group By Fortify Priority Order Analyzer

In Progress (Blue), Not Started (Yellow)

Issues

Trend Current Issues
Group By Fortify Priority Order Analyzer

Number Of Issues

APPSCAN (Orange), PTA (Light Blue), RTA (Dark Green), SCA (Dark Blue)

Analyzer	Issues
APPSCAN	~100
PTA	~200
RTA	~10
SCA	~900



HP WebInspect

HP WebInspect

File Edit View Tools Scan AMP Reports Help

New Open Compliance Manager Policy Manager Report Schedule SmartUpdate

Start / Resume Pause Skip Audit

Start Page New Web Site Assessment

Site

Http://zero.webappsecurity.com/

Private vbs_bin vbt_log vbt_pvt admin aspnet_client backup cgi-bin cookiest CVS db error_log errors hbin images include linking login scripts stats test testing

Scan Info

Dashboard Session Info Host Info PSP Info AJAX Certificates Comments Cookies E-mails Forms Hidden Scripts Broken Links Offsite Links Parameters

Scan Dashboard

Crawl 348 of 348 Audit 854 of 854

Scan Status

Completed

Vulnerabilities

Activity Req/Sec Crawling - Auditing - Other Evt/Sec Script Execution -

106 Critical 92 High 8 Medium 56 Low 22 Info 25 Best Practices

Attack Type	Attacks	Information	Best Practices	Scan Log	Server Information
Manipulation	2,597	103	52	0	2
Exploratory	10,111	1	26	4	37
Other	6,216	2	14	4	27
				14	19

Scan

Duration: 00:09:59 Policy: Standard

Crawl

Hosts: 1 Sessions: 78

Audit

Attacks Sent: 18,924 Issues: 319

Network

Total Requests: 20,001 Failed Requests: 0 Script Includes: 0 Macro Requests: 40 404 Probes: 219 404 Check Redirects: 56 Verify Requests: 0 Logouts: 28 Macro Playbacks: 40 AJAX Requests: 0 Script Events: 227 Kilobytes Sent: 14,543K

Excluded Hosts Allowed Hosts Criteria

Site

Sequence

Search

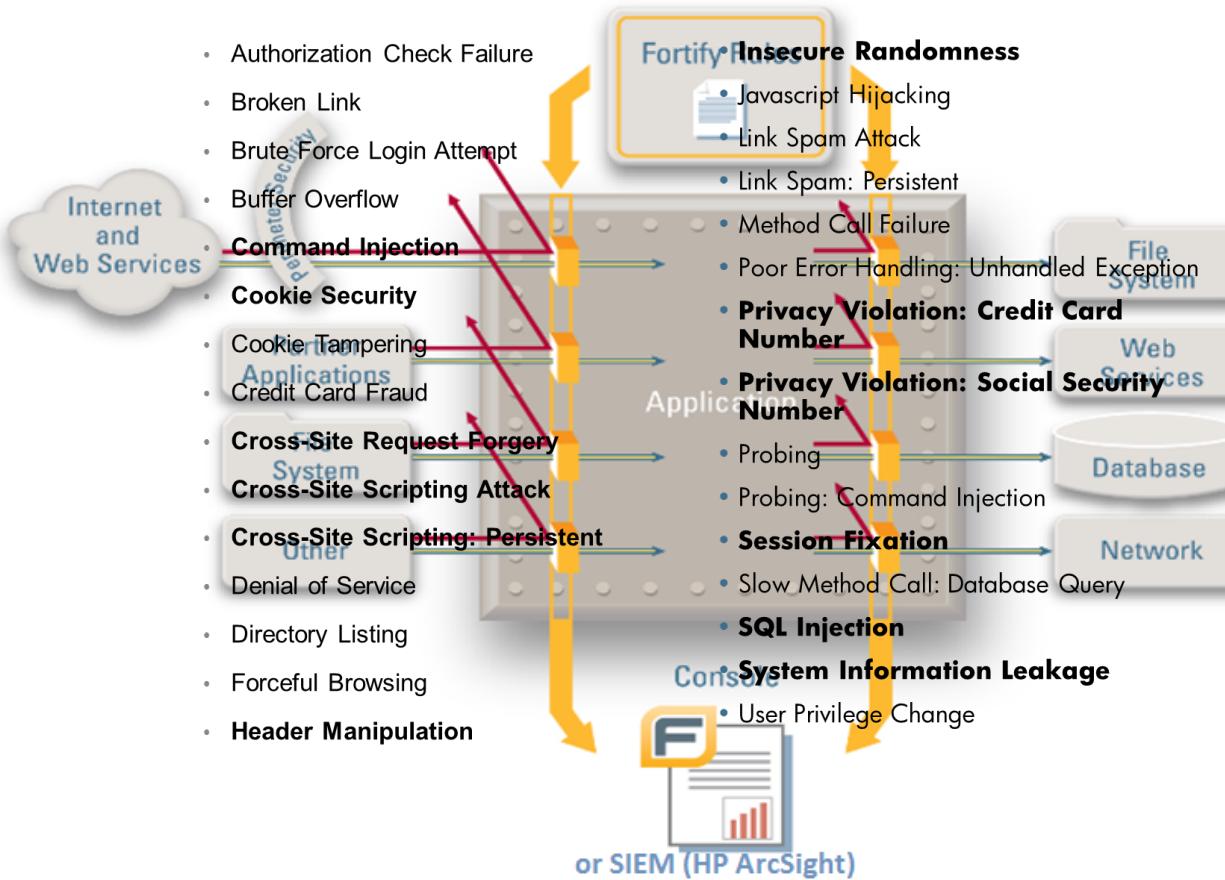
Step Mode

Vulnerabilities Information Best Practices Scan Log Server Information

The screenshot displays the HP WebInspect application window. The main area is the 'Scan Dashboard' showing 'Crawl 348 of 348' and 'Audit 854 of 854'. It features a 'Vulnerabilities' chart with categories: Critical (106), High (92), Medium (8), Low (56), Info (22), and Best Practices (25). Below the chart is a table of attack types and their counts. On the left, there's a 'Site' tree with various web application components like 'admin', 'backup', and 'scripts'. A 'Scan Info' panel on the right provides details about the current scan session, including duration, policy, and network statistics. The bottom navigation bar includes tabs for 'Vulnerabilities', 'Information', 'Best Practices', 'Scan Log', and 'Server Information'.



HP Fortify Runtime – Real Time Protection



Fortify Training

- Entrenamiento con clases abiertas en Sunnyvale, California, USA
- Entrenamiento en sitio con instructores certificados de HP ESP Fortify
- Computer Based Training (CBTs)
- Plataforma de E-Learning



HP Fortify OnDemand

FORTIFY on Demand

Projects Reports Administration

Projects

Search Filter: None
1 record found

Add ProjectVersion Select item and
ProjectVersion

SPLC

E-commerce Java/J2EE Application

Web Services (SOA) Data Classification: Customer personally identifiable

Web Access

Top 5 Prevalent Categories

Cross-Site Scripting: 35
Cross-Site Request Forgery: 13
SQL Injection: 5
SQL Injection: Hibernate: 3
Unreleased Resource: Streams: 3
Other: 5

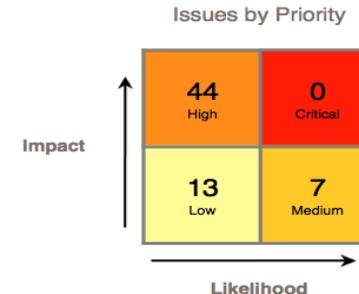
Issues by Attack Vector

Attack Vector	Issues
Database	2
Network	0
Web	41
Web Service	0
Other	21
Total	64

Fortify on Demand



Application Type: E-Commerce
Technology Stack: Java/J2EE
Interfaces: Web Services (SOA)
Project Type: Application
Data Classification: Customer personally identifiable



Remediation Roadmap

To Achieve	Major Fixes	Minor Fixes
5 stars	0	0
4 stars	0	0
3 stars	0	44
2 stars	0	0
1 star	0	0
Total	0	44

Welcome danumudu-esmp - BigBankESMP
Preferences · Terms Of Use · Contact

Re-upload Files For Analysis

Start

Complete

By now review the results and generate

Started

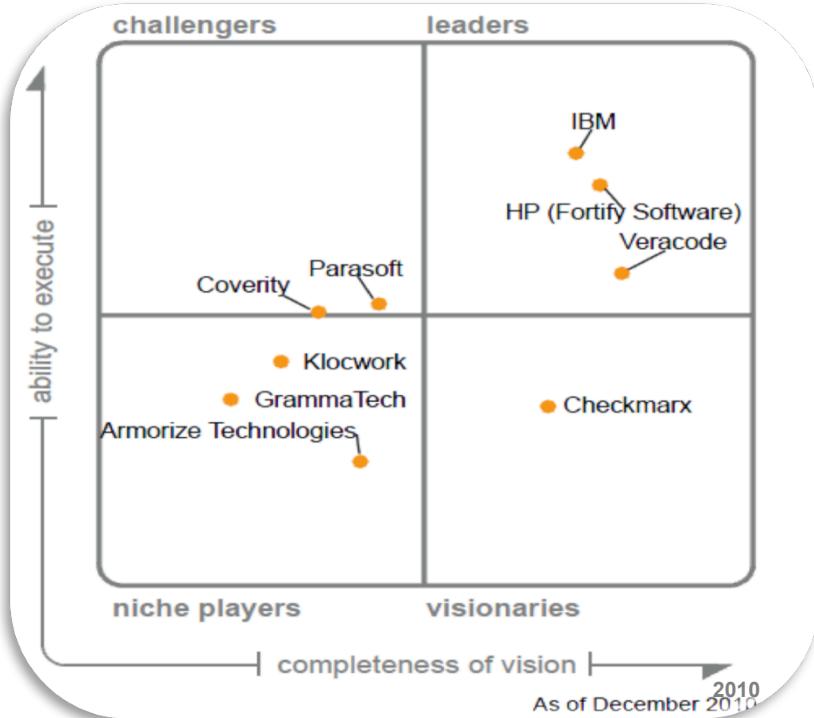
You can started for this project version.

[View More](#)



Posicionamiento en la industria

Static



Dynamic



Posicionamiento en la industria



KODAK



WIPRO
Applying Thought

33

Over 1000 enterprise customers

- 9 of the 10 largest banks
- 10 of the top 10 telecomm firms
- 5 of top 5 insurance firms
- 9 of the top 10 ISVs
- 6 of the top 10 aerospace and defense
- All branches of U.S. armed services

Plus...

- Largest app security research group
- 500+ vulnerability categories
- 21 programming languages
- The most platforms and IDEs



Mitos sobre las soluciones HP Fortify

Si los desarrolladores la usan, desaparecen los problemas

Falso

Leyendo el manual aprendes sin el apoyo de un especialista

Falso

Esta es una poderosa herramienta que te da todos los errores de seguridad y quedas certificado

Falso



Resumen

HP Fortify es una solución cuya propuesta de valor es:

- **Agilizar los tiempos** para efectuar las pruebas de seguridad en el código
- **Prevenir problemas de seguridad** desde etapas tempranas del ciclo de desarrollo
- **Reducir los costos** asociados a la corrección de problemas de seguridad detectados en producción
- **Investigación y actualización permanente** sobre las vulnerabilidades nuevas y existentes
- Ayudar a **evitar penalizaciones por incumplimiento de regulaciones** internas, locales o de industria y SLAS
- **Acelerar los tiempos de ejecución de las auditorías** externas e internas
- **Proteger la reputación e imagen pública del cliente** por hackeos
- **Tiempos de respuesta menores** ante un incidente de seguridad





¡Gracias!

Victor Rojo

victor.rojo@hp.com

+52 1 55 1069 31 57