# 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?

















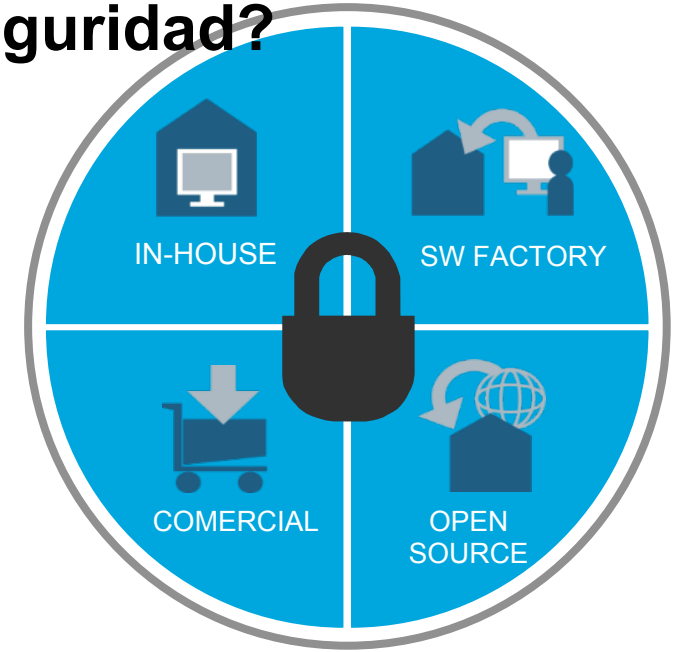








# ¿Confiabilidad o seguridad?




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

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

***y nada más***

# ¿Confiabilidad o seguridad?

# El reto en la seguridad en el software


**Corregir**

Encontrar y remediar las vulnerabilidades en el software ya desarrollado

**Prevenir**

Lograr que la seguridad sea consistente en los procesos de desarrollo de nuevo software

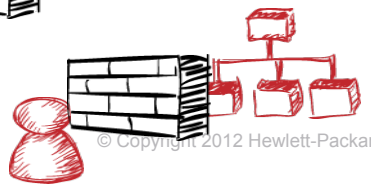
**Activos Digitales**

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

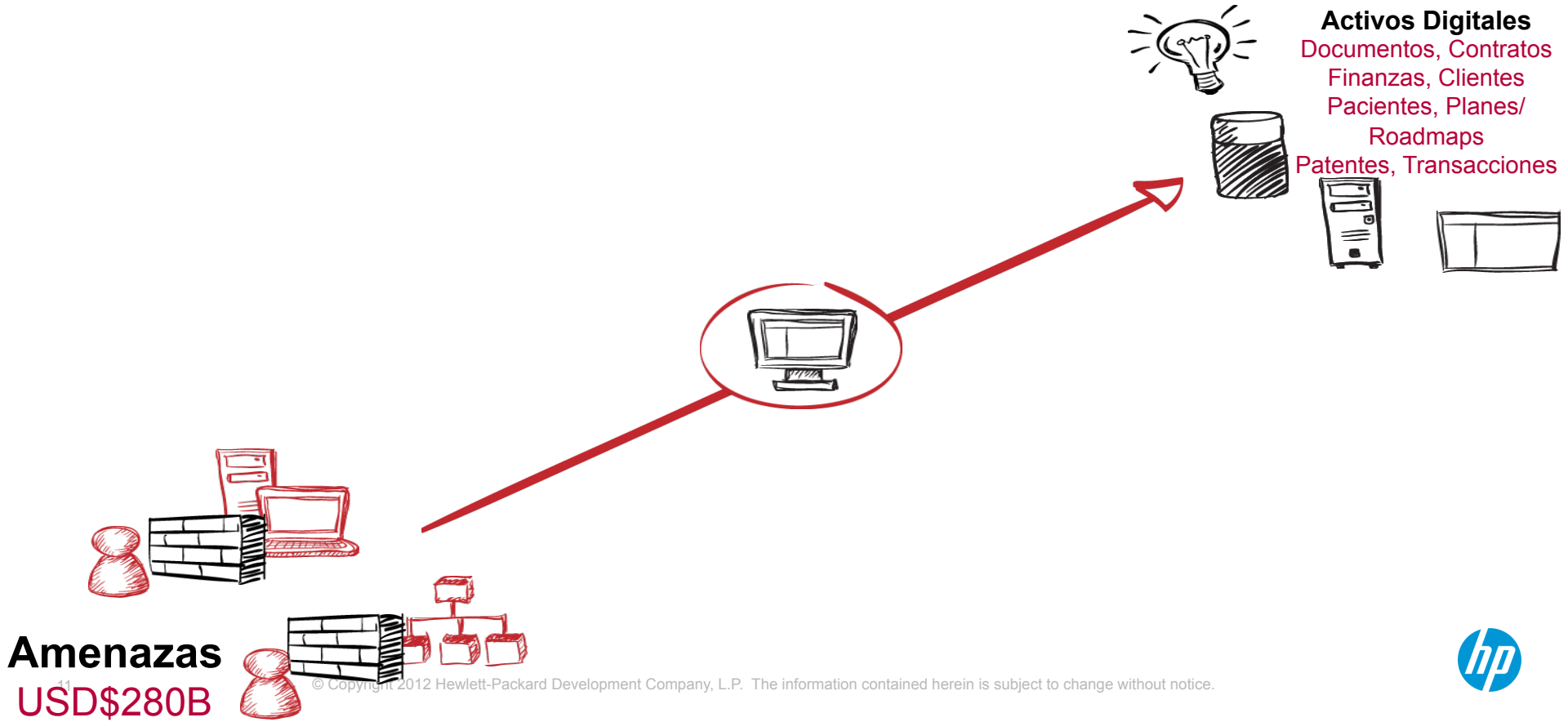
**Activos Digitales**
Documentos, Contratos
Finanzas, Clientes
Pacientes, Planes/
Roadmaps
Patentes, Transacciones

**Amenazas**
USD$280B

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

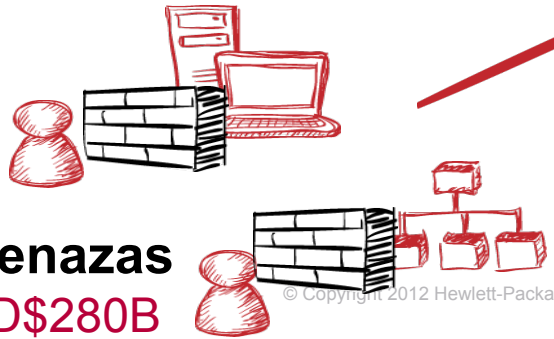


**Amenazas**
USD$280B



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

Dev ≠
Comprometido

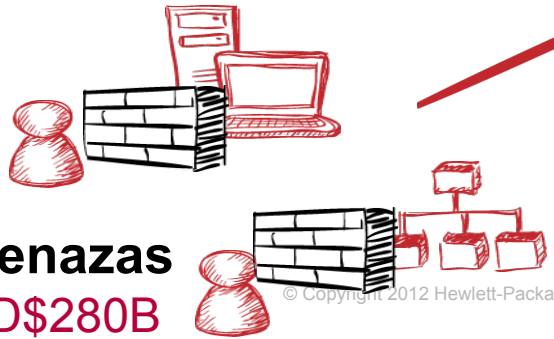


**Amenazas**
USD$280B

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

Dev ≠
Comprometido

Testing ≠
Incompleto



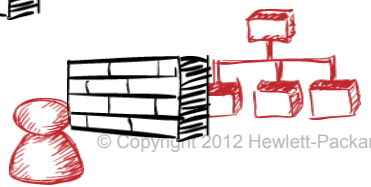
**Amenazas**
USD$280B

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

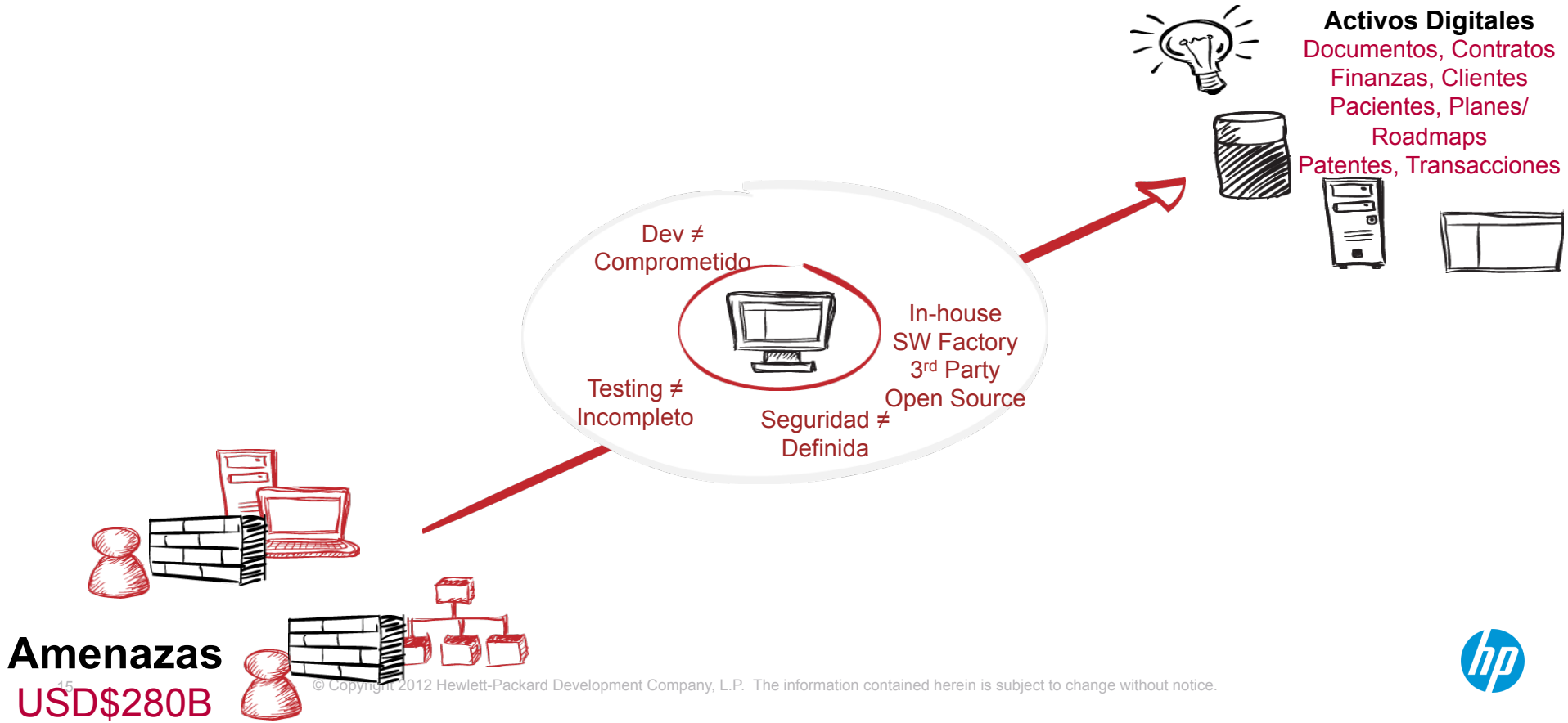
Dev ≠
Comprometido

Testing ≠
Incompleto

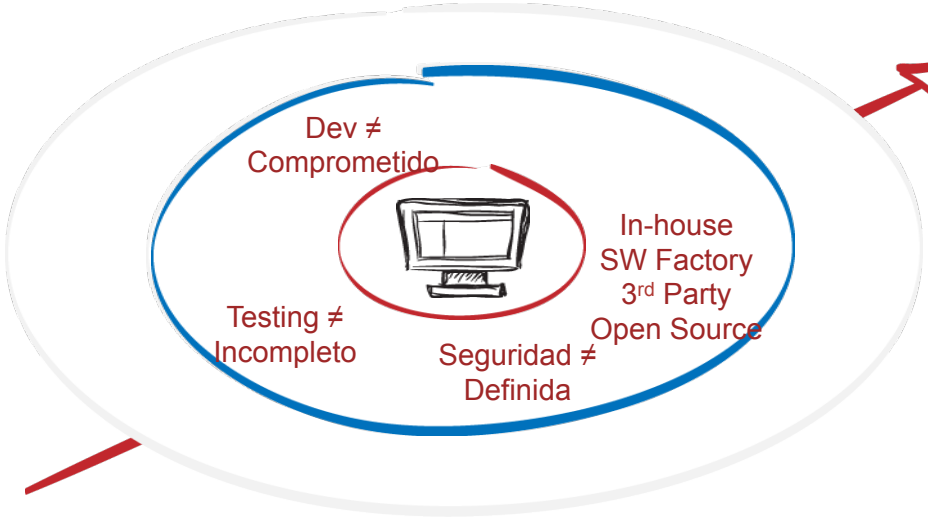
Seguridad ≠
Definida

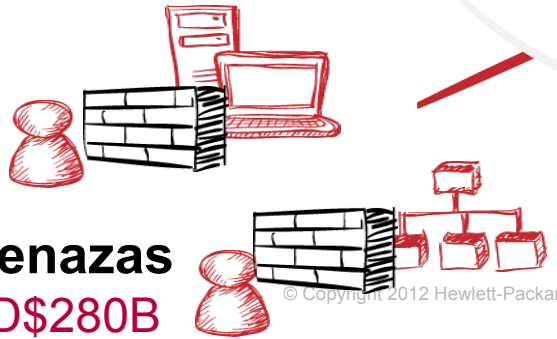


**Amenazas**
USD$280B

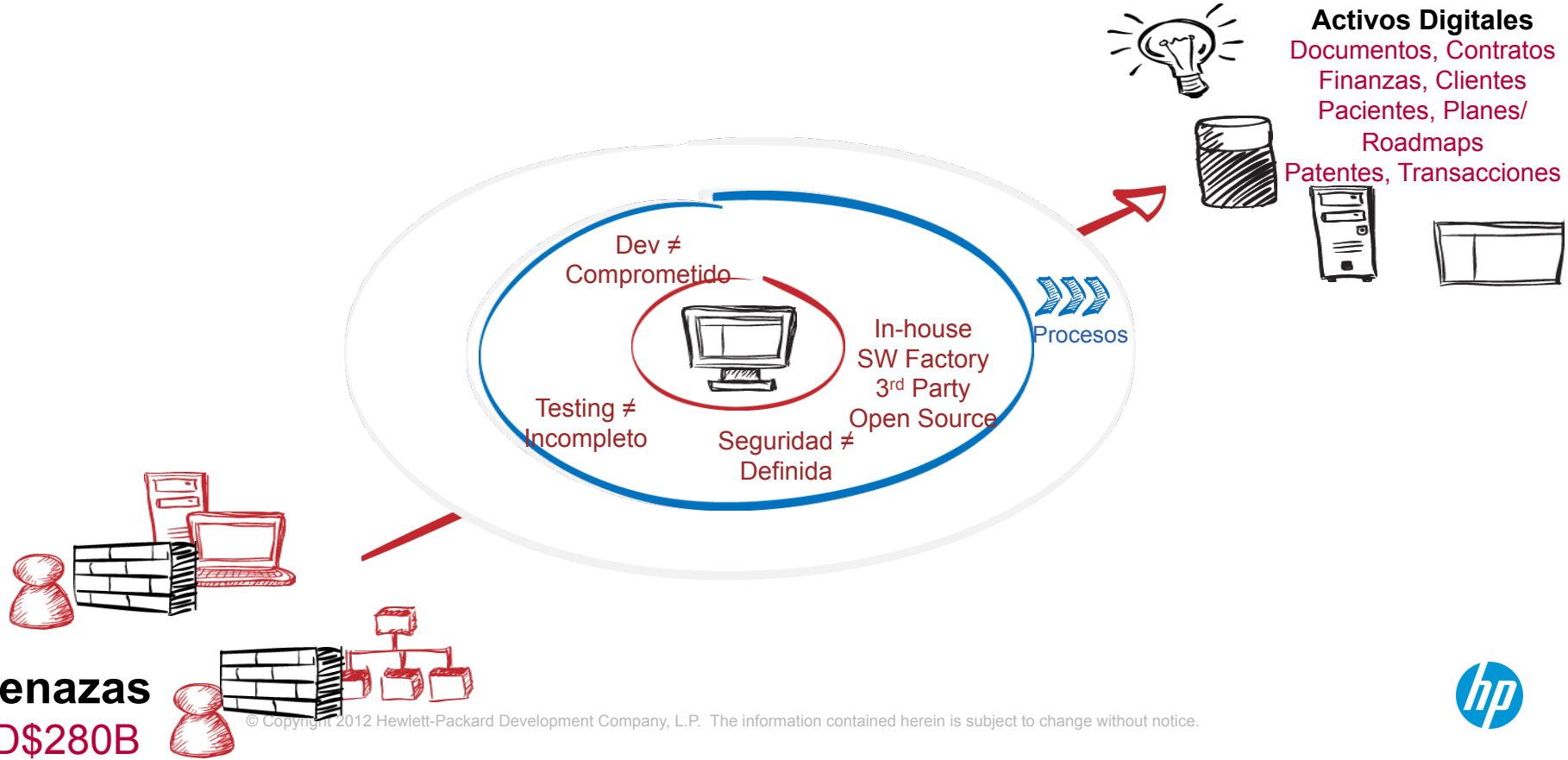


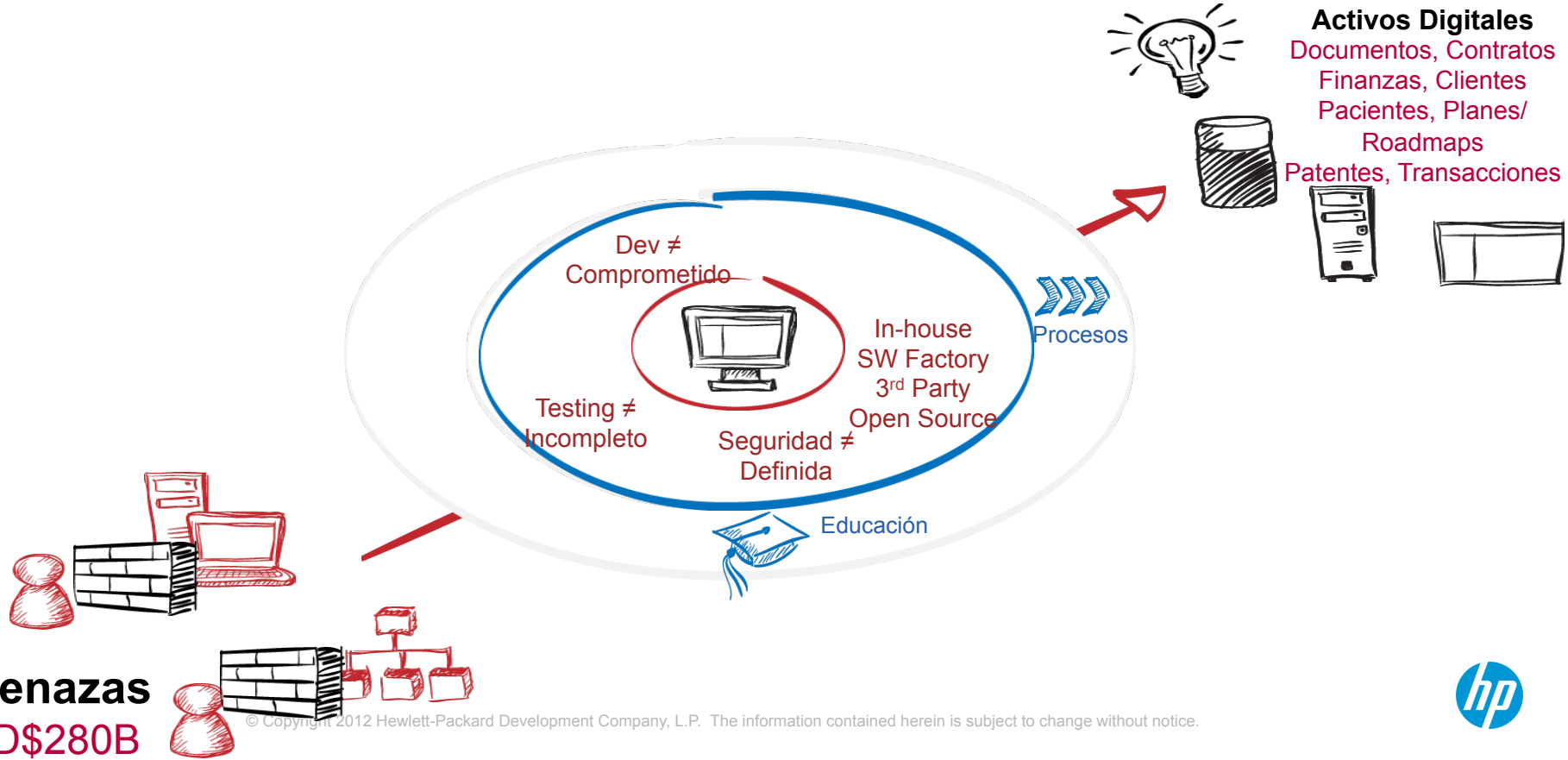
**Activos Digitales**
Documentos, Contratos
Finanzas, Clientes
Pacientes, Planes/
Roadmaps
Patentes, Transacciones

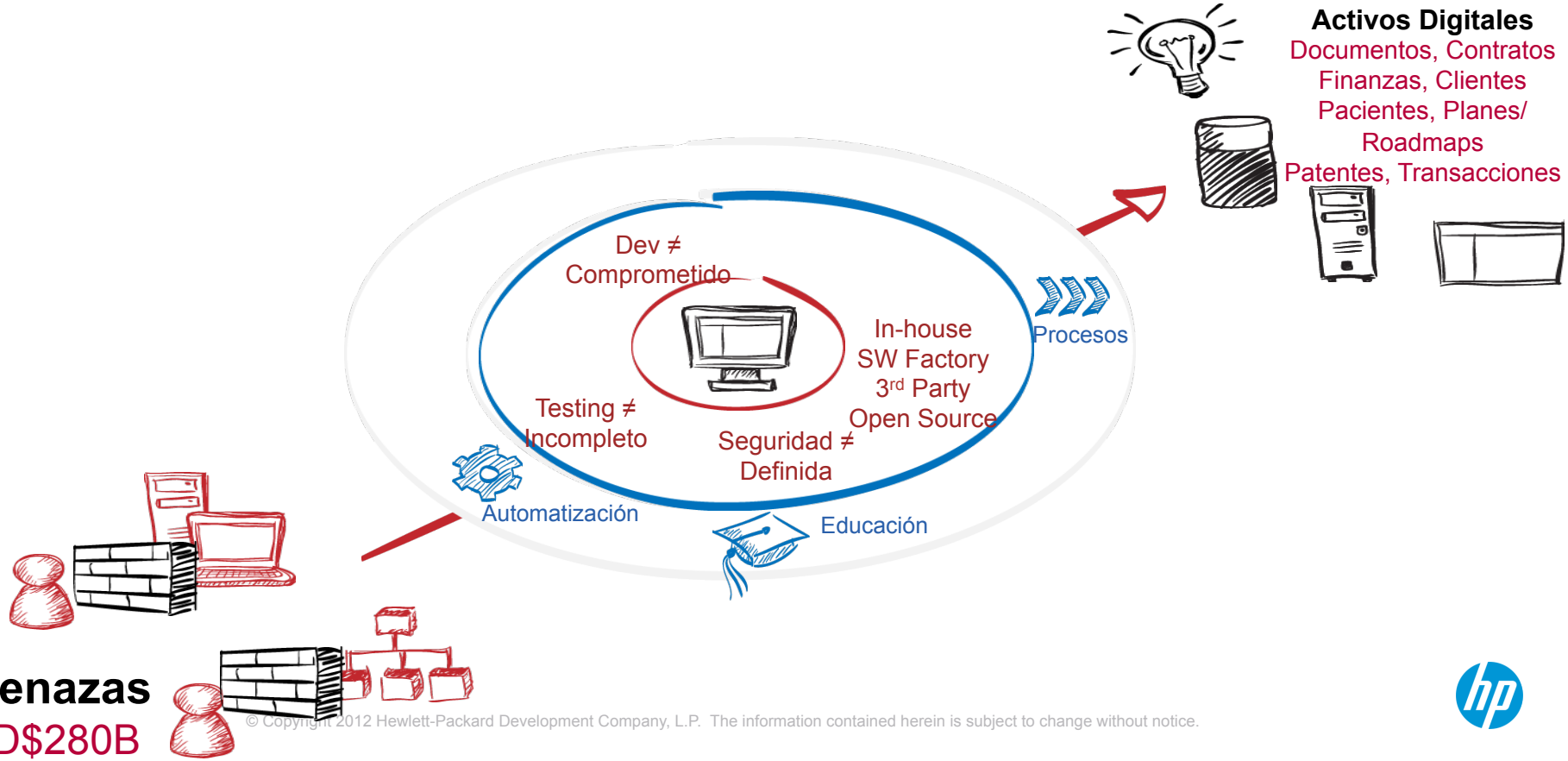


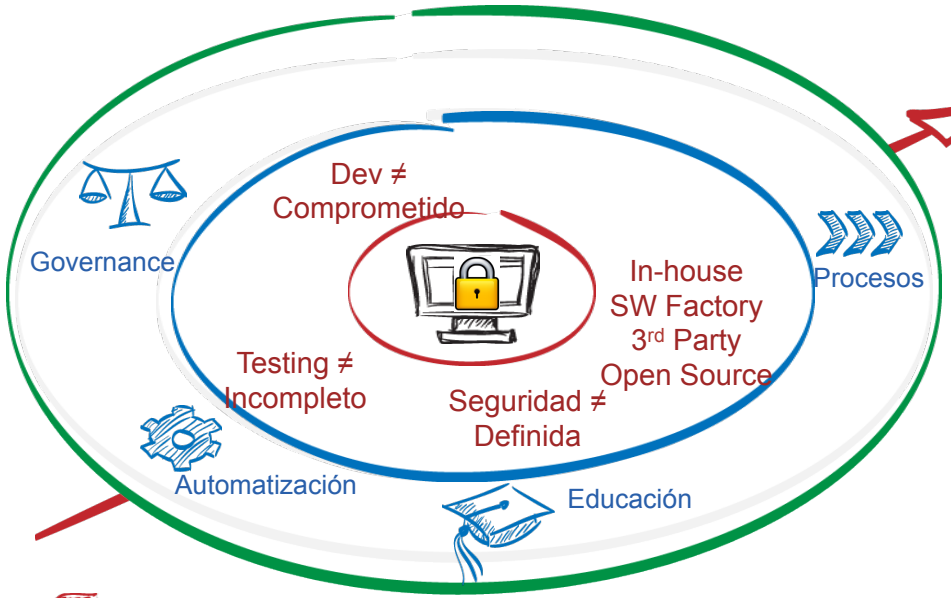



**Amenazas**
USD$280B



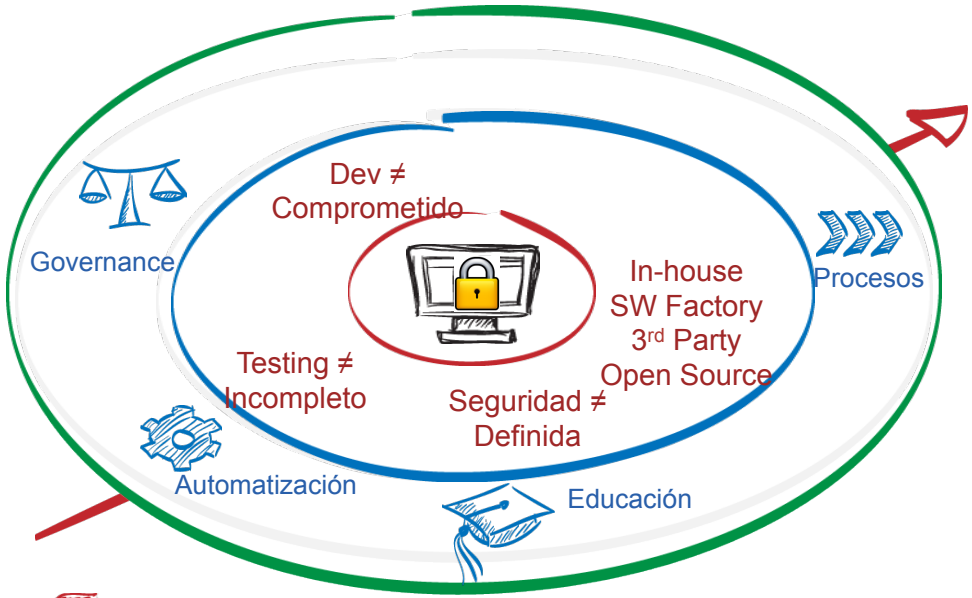







**Activos Digitales**
Documentos, Contratos
Finanzas, Clientes
Pacientes, Planes/
Roadmaps
Patentes, Transacciones

**Amenazas**
USD$280B



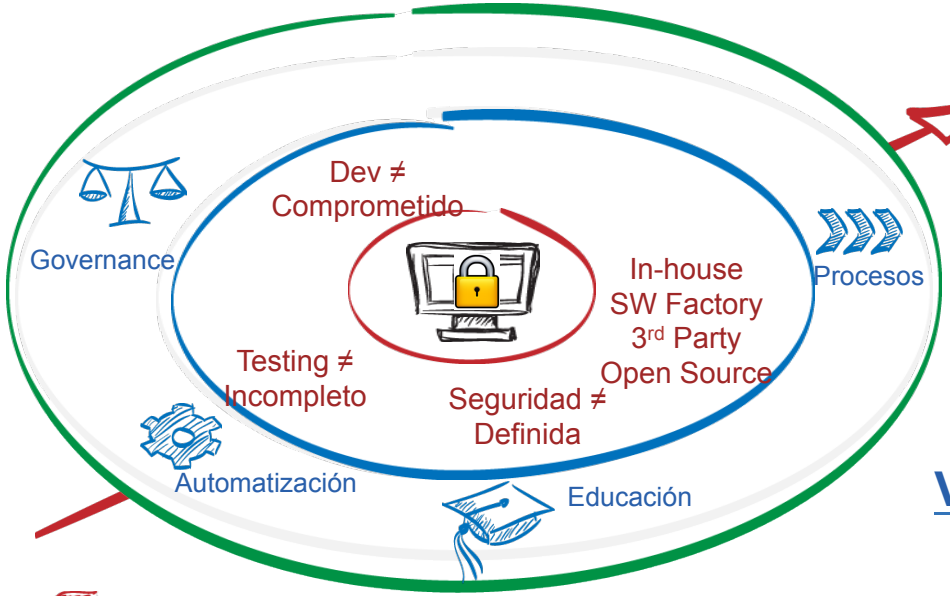

**Activos Digitales**
Documentos, Contratos
Finanzas, Clientes
Pacientes, Planes/
Roadmaps
Patentes, Transacciones

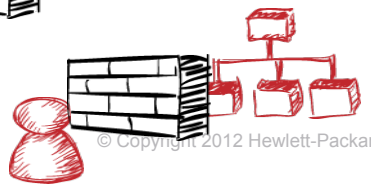
**Valor para el negocio**

Nivel de Riesgo

**Amenazas**
USD$280B

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



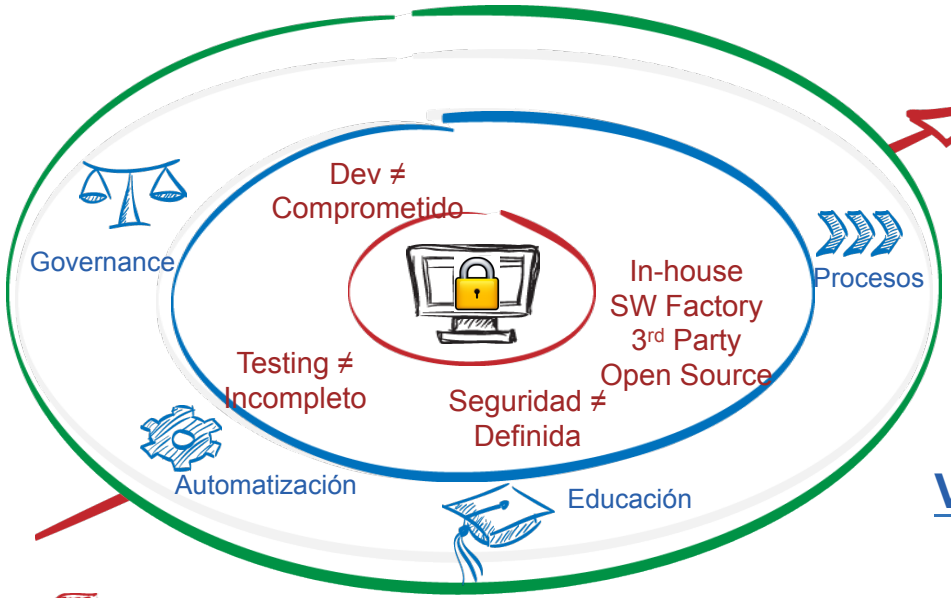



**Amenazas**
USD$280B

## Valor para el negocio

Nivel de Riesgo

Costos de SW Dev




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

**Amenazas**
USD$280B

## 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**

WebInspect, QAInspect,WI Enterprise

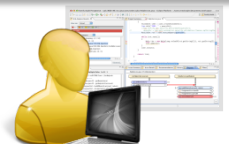
Fortify ***on Demand***

**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**

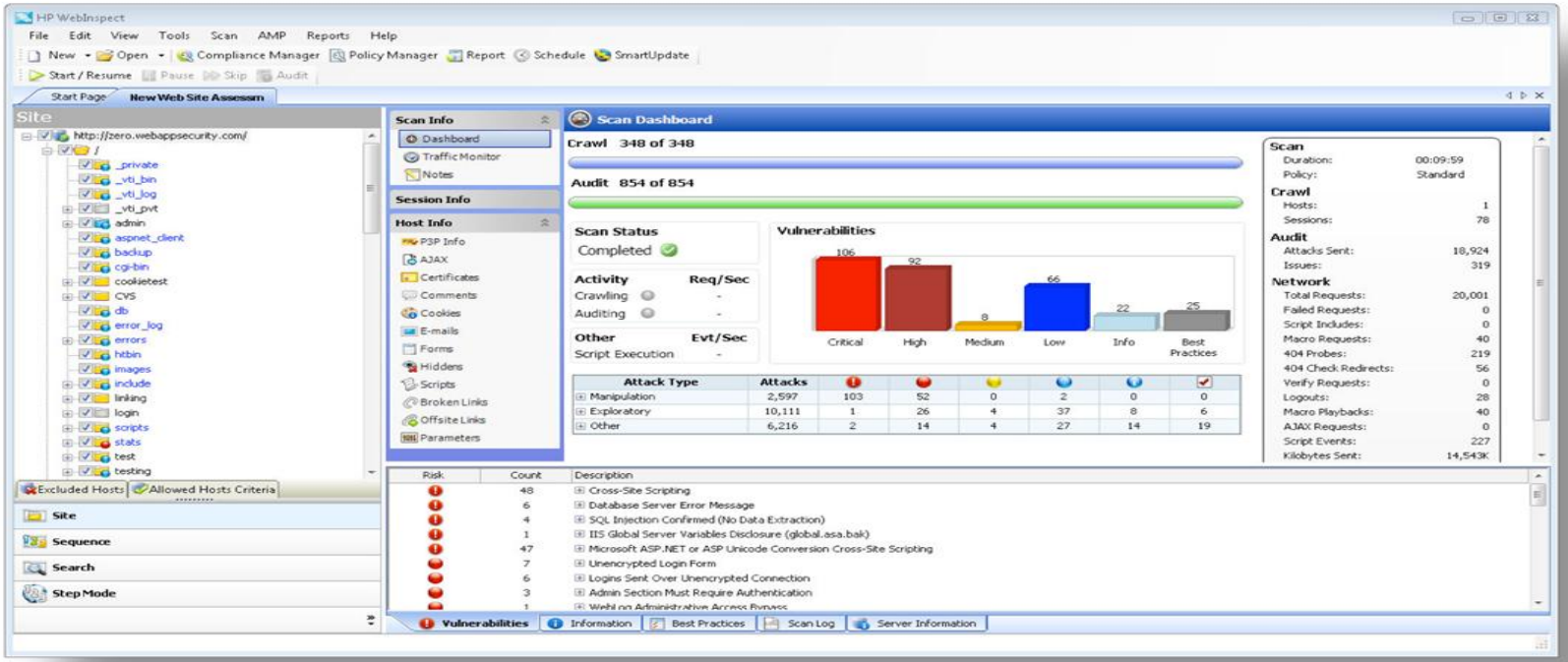
***Fortify Governance Module (SSC Server Add-On)***

**Project, Security, and Management Stakeholders**

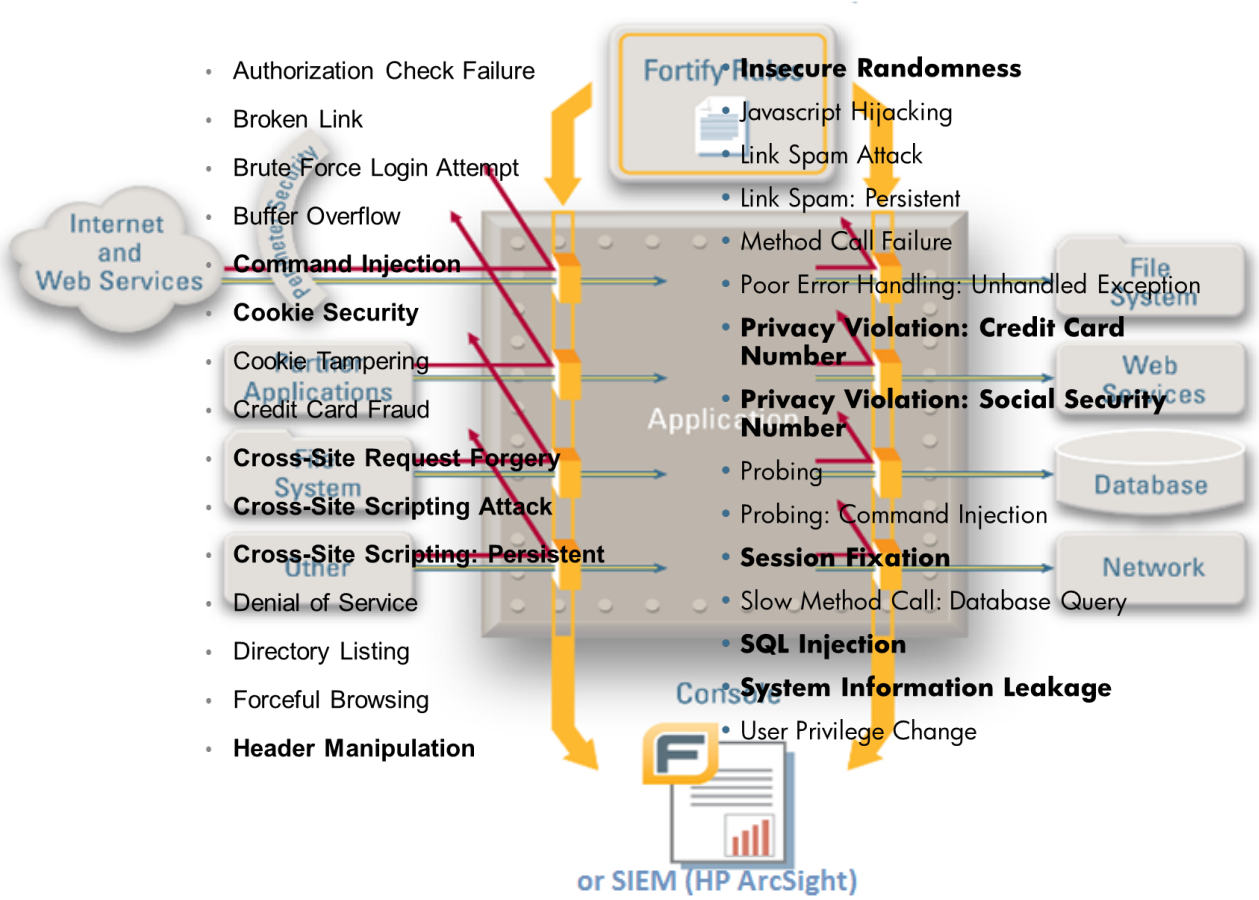
# Fortify SCA (Static Code Analyzer)

# HP Fortify Software Security Center (SSC)

# HP WebInspect



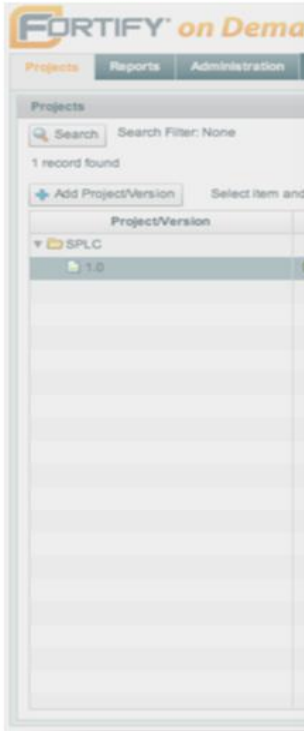
# HP Fortify Runtime – Real Time Protection

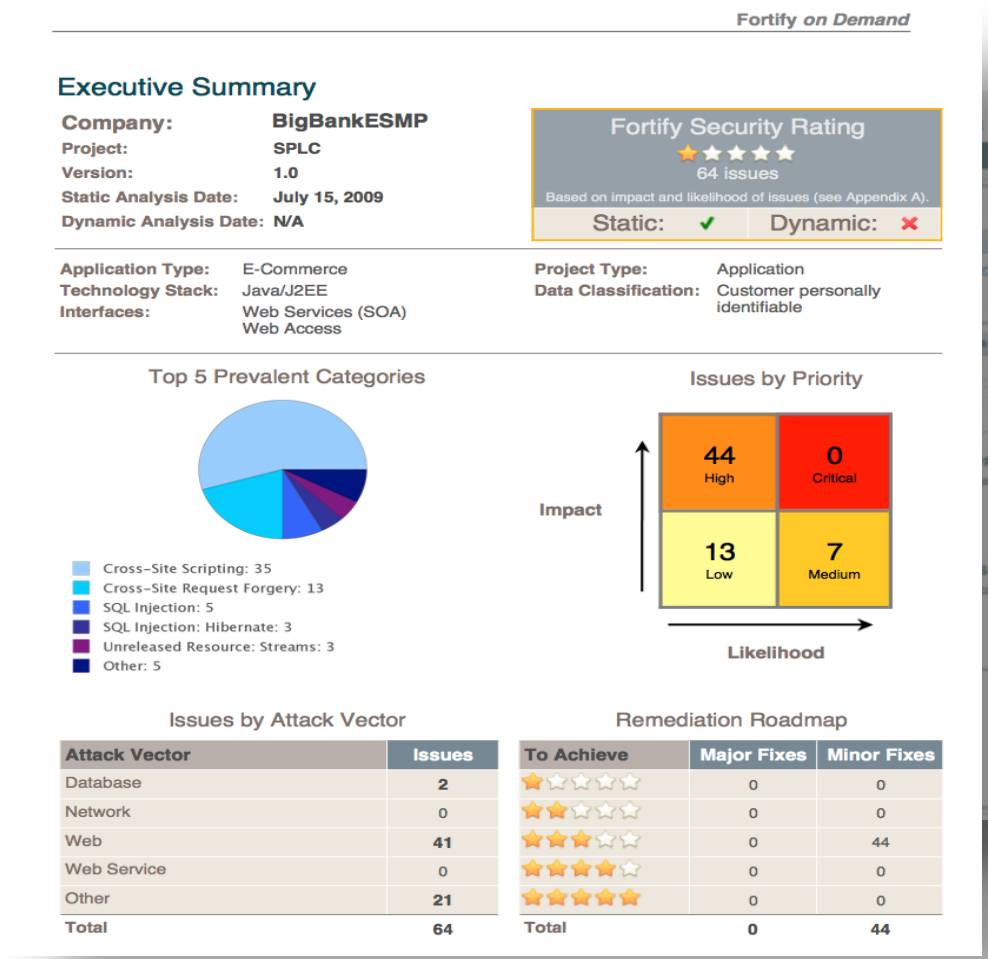


# Fortify Training

- 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*

## Executive Summary

| | |
|---|---|
| **Company:** | **BigBankESMP** |
| **Project:** | **SPLC** |
| **Version:** | **1.0** |
| **Static Analysis Date:** | **July 15, 2009** |
| **Dynamic Analysis Date:** | **N/A** |

**Fortify Security Rating**

★★★★★

64 issues

Based on impact and likelihood of issues (see Appendix A).

Static: ✓ Dynamic: ✗

| | | | |
|---|---|---|---|
| **Application Type:** | E-Commerce | **Project Type:** | Application |
| **Technology Stack:** | Java/J2EE | **Data Classification:** | Customer personally identifiable |
| **Interfaces:** | Web Services (SOA)<br>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 Priority

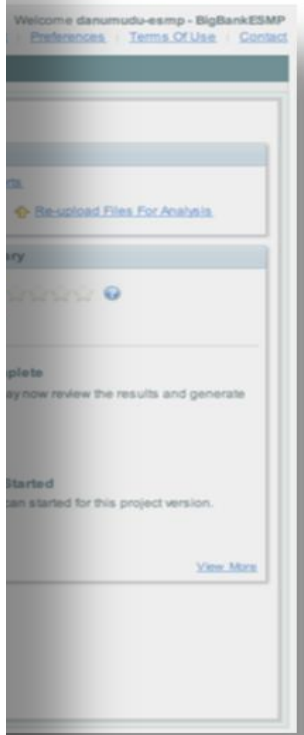



### Issues by Attack Vector

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

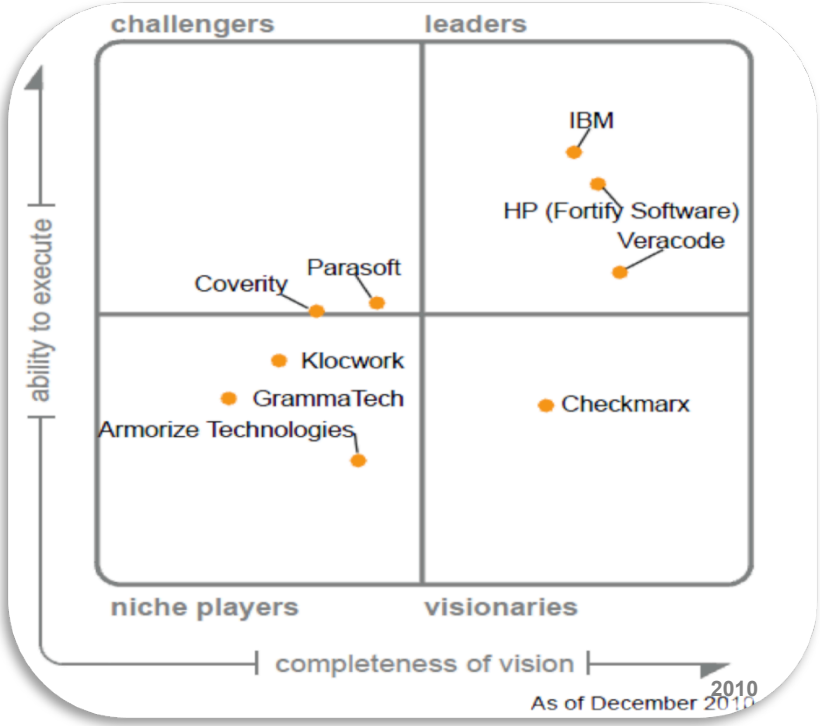
### Remediation Roadmap

| To Achieve | Major Fixes | Minor Fixes |
|---|---|---|
| ★☆☆☆☆ | 0 | 0 |
| ★★☆☆☆ | 0 | 0 |
| ★★★☆☆ | 0 | 44 |
| ★★★★☆ | 0 | 0 |
| ★★★★★ | 0 | 0 |
| **Total** | **0** | **44** |



# Posicionamiento en la industria

## Static




## Dynamic

# Posicionamiento en la industria


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