



IBM Software Group

Seguridad en las Aplicaciones Web:

Protección de los datos y cumplimiento de Normativas

Jessica Valderrama

jvalderrama@es.ibm.com

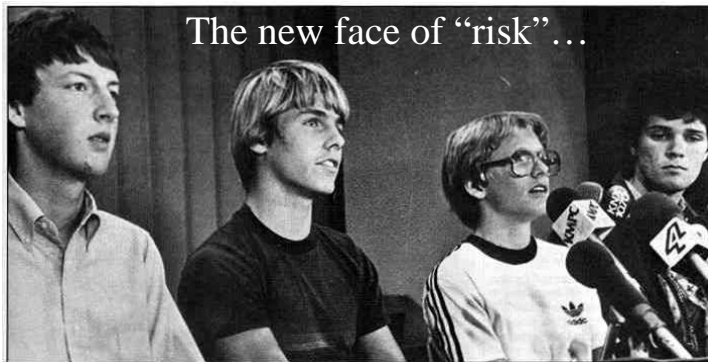
Rational Sales Specialist AppScan Spain & Portugal



Las compañías que intercambian información confidencial on-line, son **susceptibles de tener agujeros de seguridad** aun cuando invierten en seguridad de red y desktop.

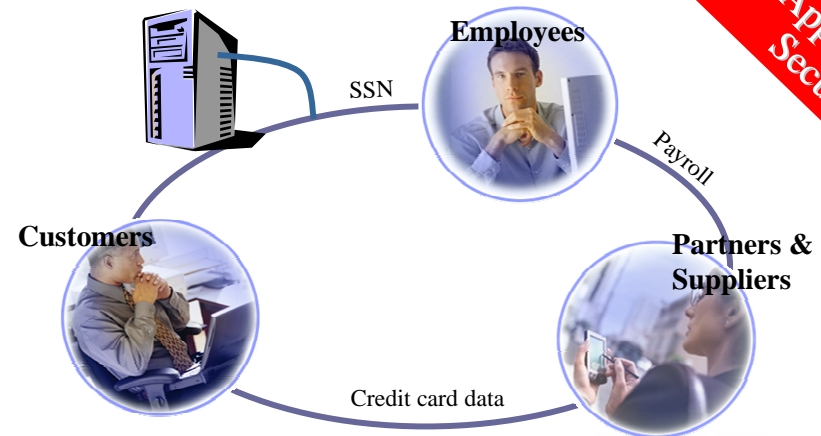


IBM Software Group



The new face of "risk" ...

Teenagers who's computers were seized by the FBI for hacking into a company web site



Application Security

Business impact of application security breaches

Point of vulnerability

"75 percent of hacks occur at the application level."

By 2009, 80 percent of companies will have suffered an application security incident.

Gartner, 2005

Increased costs

THE WALL STREET JOURNAL

"VISA will start levying fines this month for lack of [PCI] compliance" by Robin Sidel (October 6, 2007)

Public Disclosure & Brand Damage



Últimos informes de especialistas X-Force

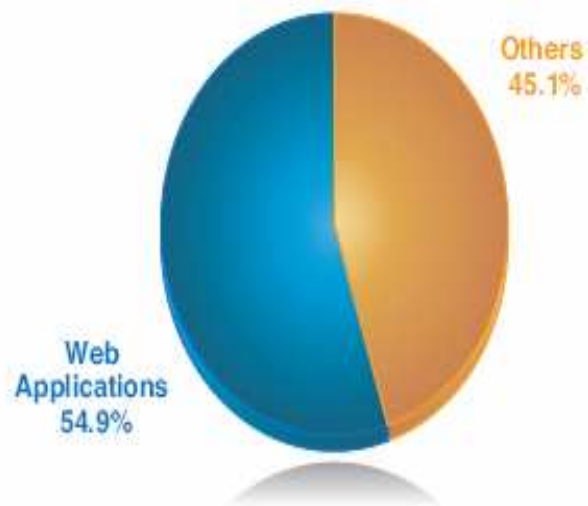


Figure 17: Percentage of Disclosures that are Web Application Vulnerabilities, 2008

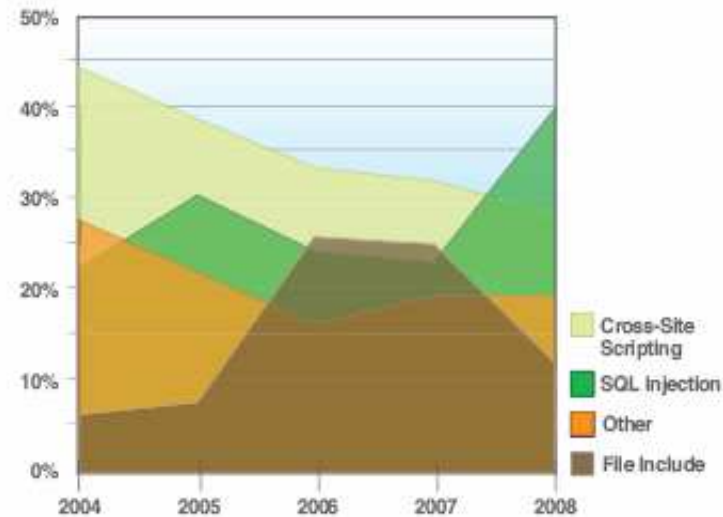


Figure 19: Web Application Vulnerabilities by Attack Technique, 2004 - 2008

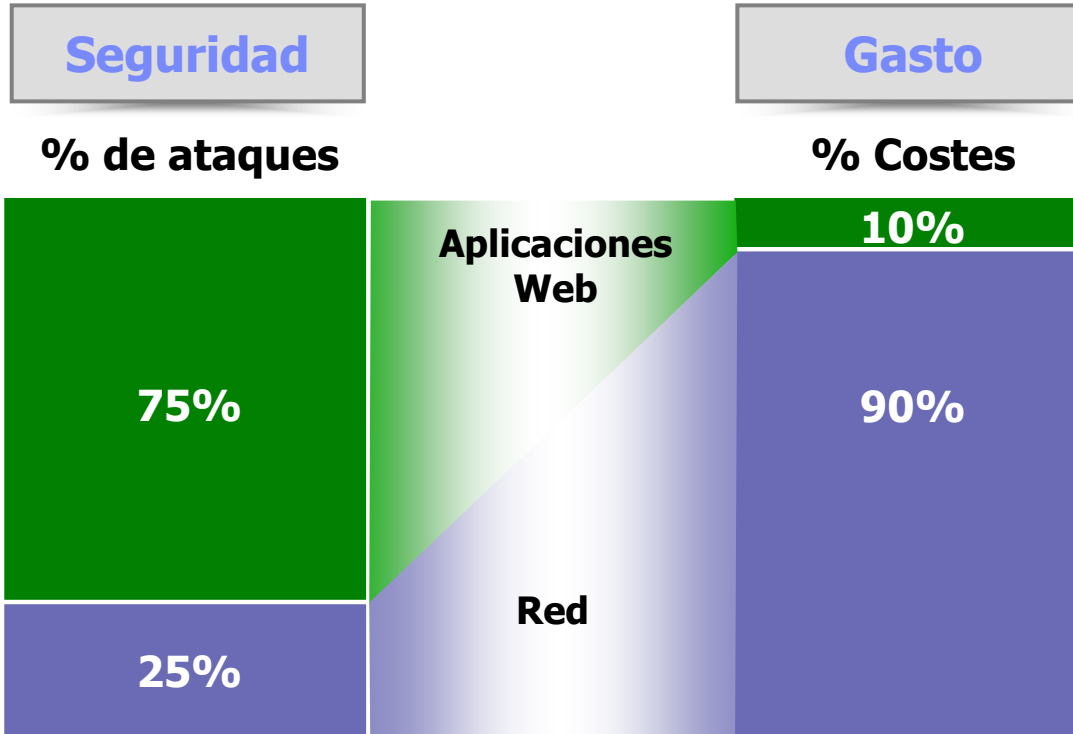


Nivel de Seguridad e inversión no están equilibrados



Security

- Buffer Overflow
- Cookie Poisoning
- Hidden Fields
- Cross Site Scripting
- Stealth Commanding
- Parameter Tampering
- Forceful Browsing
- SQL Injection
- Etc...



75% de los ataques a la seguridad informática están dirigidos hacia el nivel de las aplicaciones Web

2/3 de todas las aplicaciones Web se consideran vulnerables

Gartner

Sources: Gartner, Watchfire





Security

“Nuestro sitio Web es seguro”

Tenemos firewalls

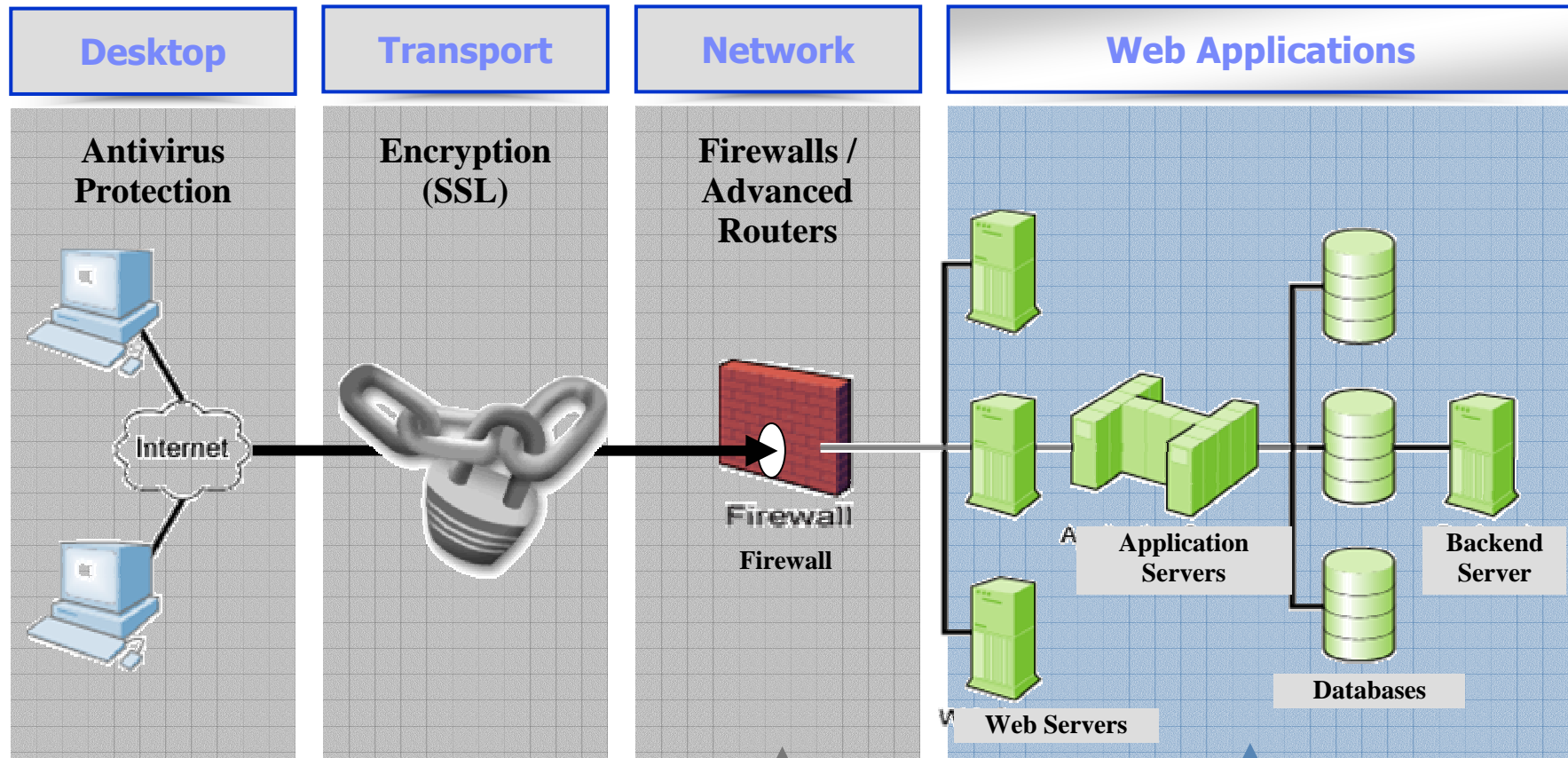
Tenemos auditores de seguridad que hacen tests de intrusiones cada trimestre

Usamos instrumentos de control de la vulnerabilidades de la red



Seguridad de red vs. seguridad de Aplicación- Soluciones complementarias.

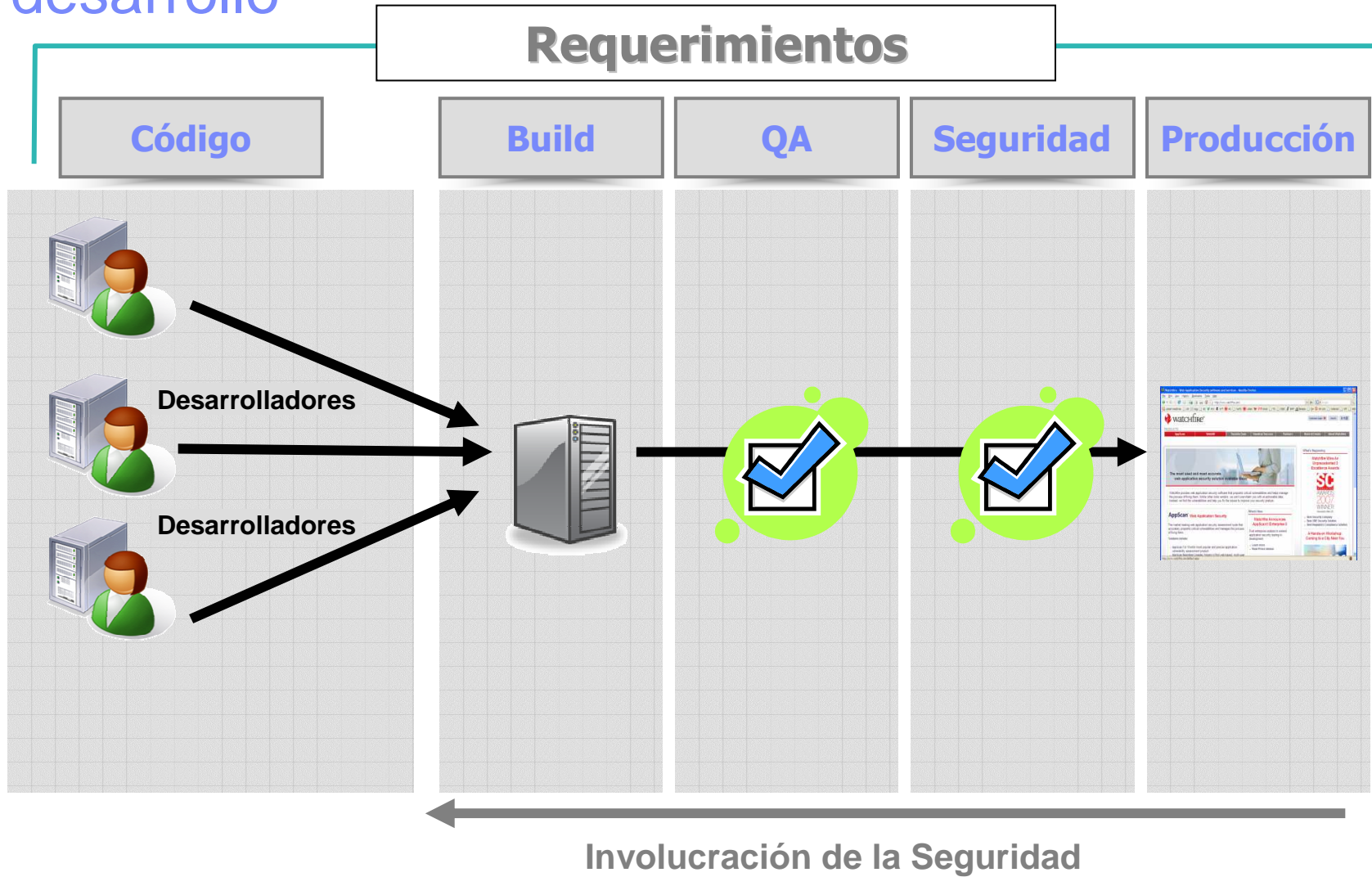
Info Security Landscape



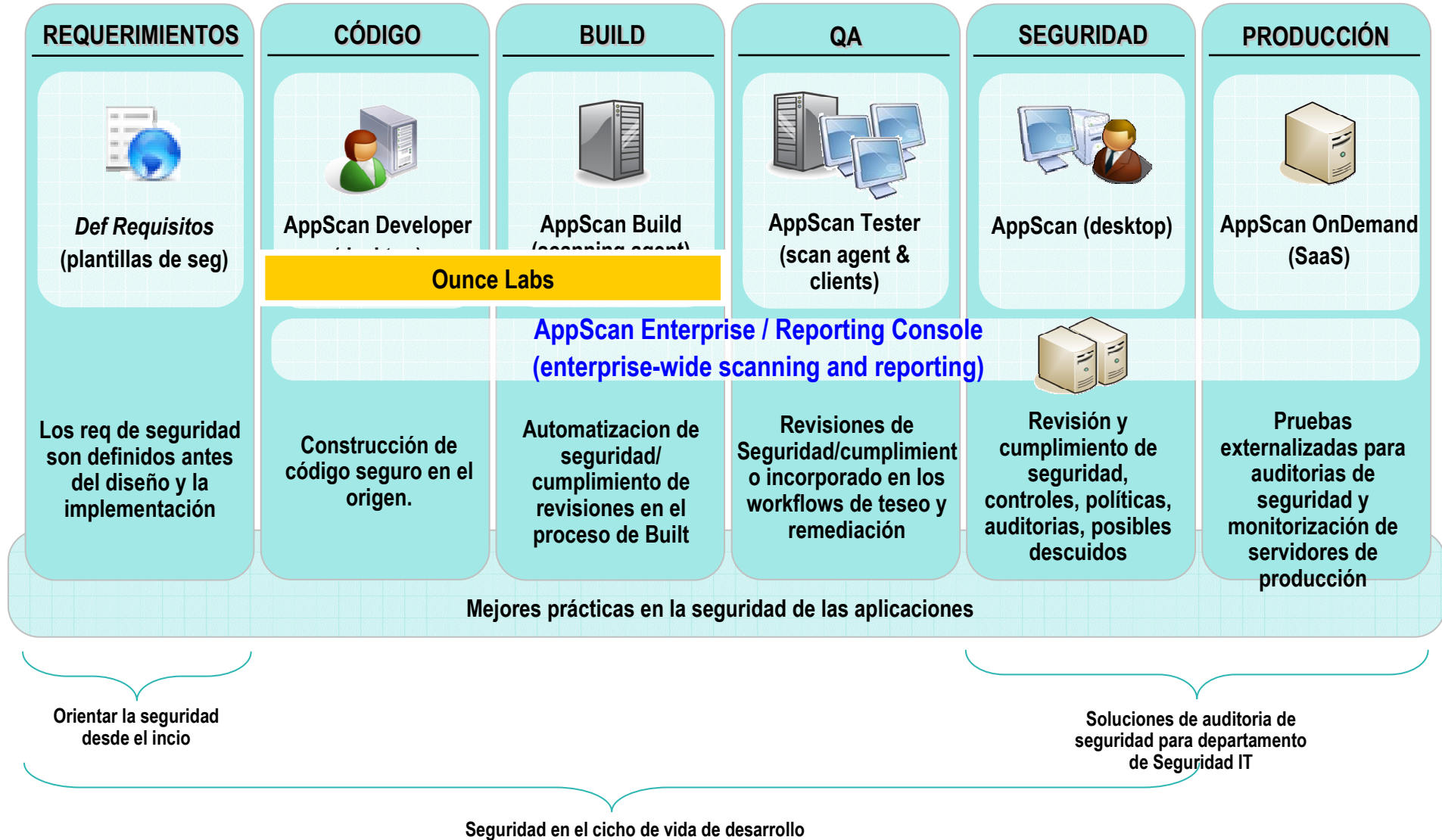
Network & Application Security solutions address different problems



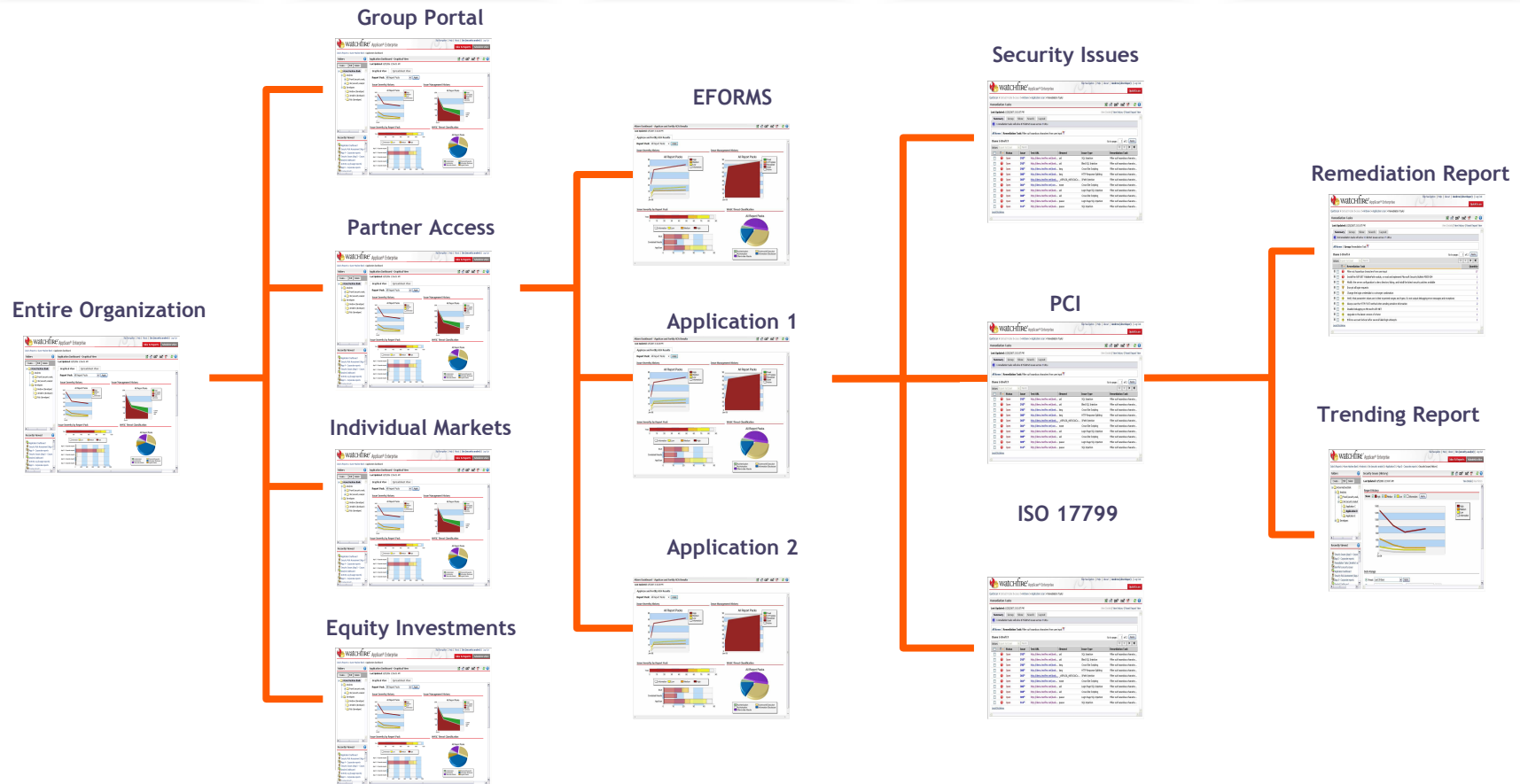
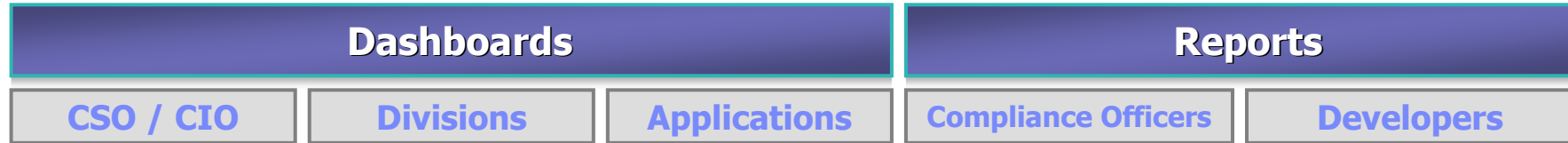
Seguridad en todas las fases del entorno de desarrollo



Rational End-to-End Application Security...with Ounce



Visibilidad para toda la empresa



IBM Adquiere Once Labs

Ounce Labs provee herramientas de revisión y control de código fuente ayudando a las empresas a reducir el riesgo y los costes asociados a posibles fallos de seguridad e incumplimiento de normativas.

- Application security is the largest category of vulnerability disclosures (55% in 2008)
- Rational acquired Watchfire in 2007 to address customers' Application Security Testing needs
 - ▶ AppScan continues to be recognized as the leader in Dynamic Analysis Security Testing (DAST)
 - ▶ Ounce Labs is a recognized leader in Static Analysis Security Testing (SAST)
- Application security markets are converging
 - ▶ The combination of these two industry leading technologies provides the most accurate solution in the market
 - ▶ Ounce's technology enables Rational to fulfill our vision of moving testing earlier in the development process
- Continues to add to our competitive advantage in the application security testing segment
 - ▶ Only vendor to offer complete solutions for both SAST & DAST
 - ▶ Only vendor to offer complete integration across the software delivery lifecycle
 - ▶ Only vendor to offer a complete IT security solution across all major domains (IBM Security Framework)
- Ounce is a good fit
 - ▶ Mature technology that supports all key development technologies and languages (Java, .NET, C/C++)
 - ▶ Excellent integrations with Rational SDLC products and for the developer – Rational's traditional user base





© Copyright IBM Corporation 2007. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, the on-demand business logo, Rational, the Rational logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

