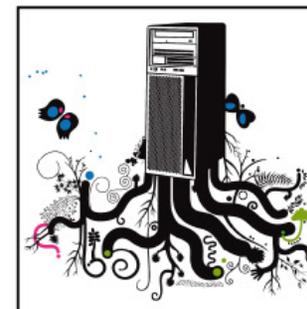
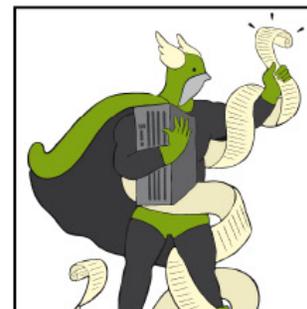
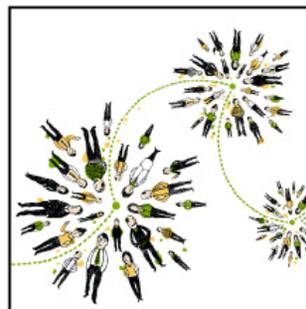
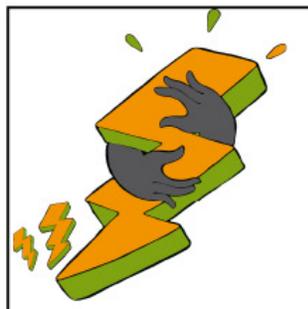
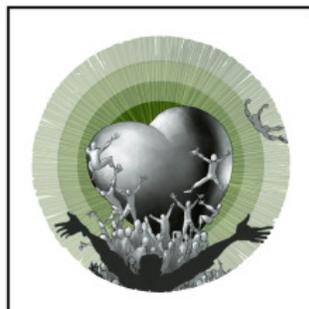


IBM SOFTWARELAND 2009.
SOLUZIONI INTELLIGENTI
PER PROSPETTIVE
CHE CAMBIANO.



Domenico Ercolani

Rational. software

Le soluzioni Rational a garanzia della sicurezza
delle applicazioni web e rispetto della compliance

Compliance and Security secondo IBM



Agenda

- Rational Software
- Compliance
 - Compliance Management per SW Team
 - Compliance Applicazioni / Portali
- Sicurezza
 - Sicurezza delle applicazioni web



Agenda

- Rational Software
- Compliance
 - Compliance Management per SW Team
 - Compliance Applicazioni / Portali
- Sicurezza
 - Sicurezza delle applicazioni web



IBM Rational software

Un partner strategico per la “business innovation & trasformazione”

Imperativi del Business

- Capacità globale
- Flessibilità
- “Time to Market”
- Gestione dei rischi e delle conformità

Governance e gestione del ciclo di vita del software

Rational. software

Governare i processi di business legati allo sviluppo ed al rilascio di software e sistemi

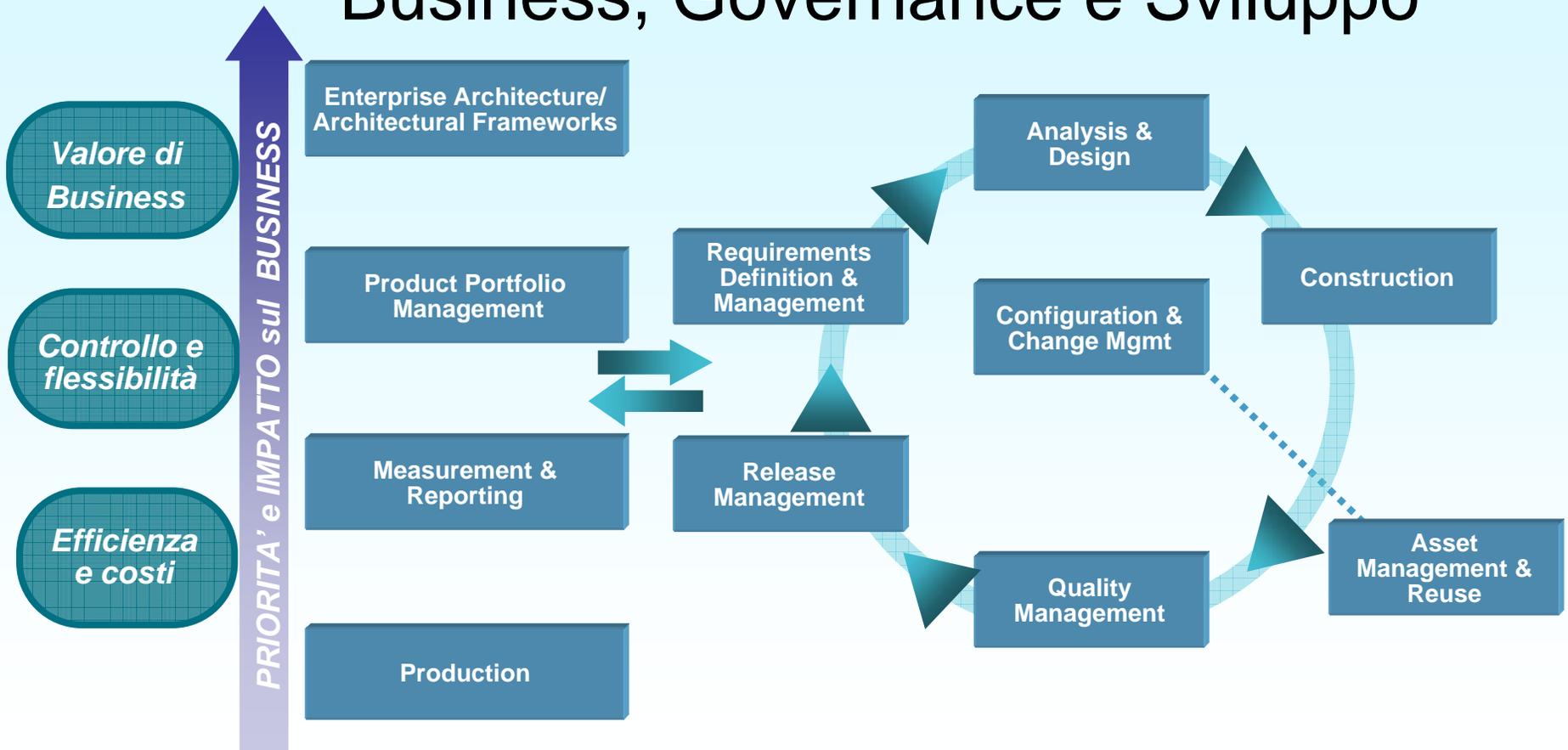
Anni di provata esperienza sui processi e sul successo dei clienti

Innovazione e Trasformazione del Business

- Allineamento
- Controllo
- Efficienza



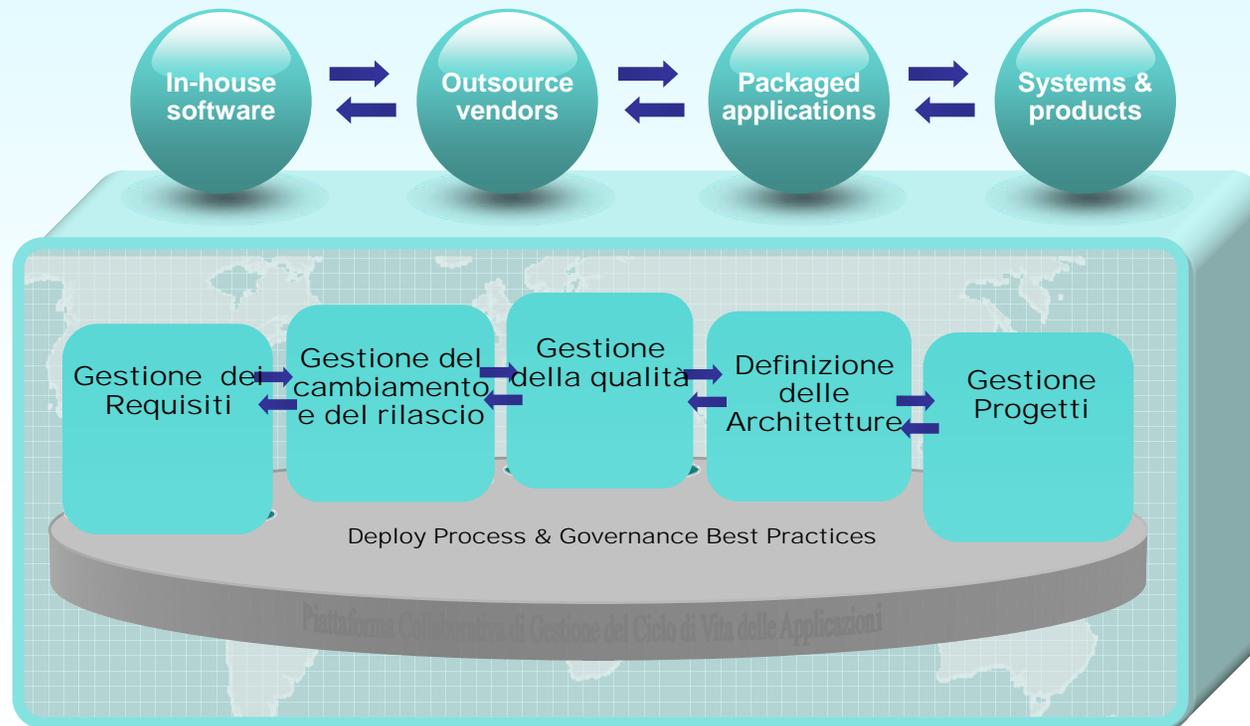
Business, Governance e Sviluppo



IBM Rational Software Delivery Platform

Rational. software

***Soluzioni** che aiutano i clienti ad incrementare il VALORE e le performance dei loro investimenti nello sviluppo software*



Produttività

Sviluppo Agile

Gestione di team distribuiti

Governance

Gestione del rischio

Compliance



Agenda

- Rational Software

- Compliance
 - Compliance Management per SW Team
 - Compliance Applicazioni / Portali

- Sicurezza
 - Sicurezza delle applicazioni web



Compliance scenario



Sarbanes-Oxley Act



Basel II



IAS



ISO27001

OSHA

PCI DSS

HIPAA

21CFR11

(Electronic Signature records for Food and Drug)

Patriot Act

(anti money laundering)

Gramm Leach-Bliley Act

(Financial confidentiality of non public info)

W3C

DoD 5015.2 / PRO

(Certification of electronic records mgt SW products)

ACORD



SEC 17a-4 / NASD 3010/3110

(Brokers, records for all correspondence)



**FEDERAL TRADE COMMISSION
FOR THE CONSUMER**



The Federal Reserve Board



U.S. Food and Drug Administration



Compliance management per SW teams

1) “Definisci cosa devi fare”

Disegna un processo di sviluppo in linea con le normative a cui sei soggetto

- “Business / Technicals controls” e workflow
- Approvazioni, autorizzazioni, punti di controllo, “separation of duties”

2) “Fai quello che hai definito”

Automatismi per rafforzare l’aderenza del processo

- Strumenti per la guida del processo, workflow automatizzati, tools che guidino al “corretto comportamento”

3) “Sii capace di dimostrare”

Generazione automatica della documentazione per l’audit

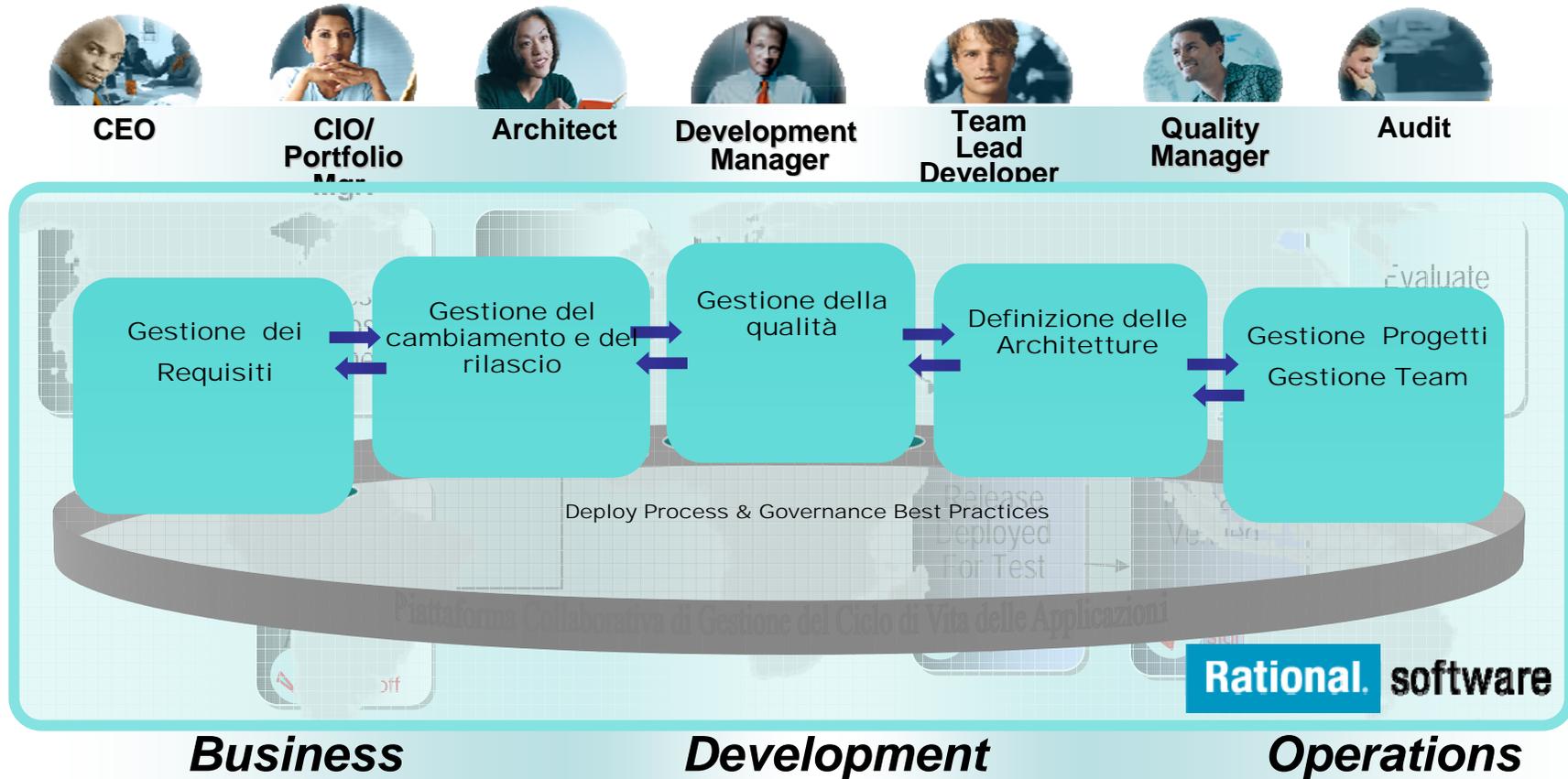
- Reports per l’Audit, Tracciabilità di quanto avviene nell’ambito della “software delivery organization”

4) Utilizza la compliance come vantaggio per il business

- Analizza le metriche del progetto e del processo
- Persegui il miglioramento continuo



Un esempio di processo di compliance



Compliance per applicazioni / portali web

Il Portale e le applicazioni rese disponibili attraverso il web sono un importante strumento per la comunicazione aziendale e parte integrante dei processi di business.

Per questo è importante curarne la qualità e la compliance con le normative di riferimento.

Quali sono i rischi?

- Clienti che abbandonano la navigazione (link non accessibili, errori applicativi, lentezza nel caricamento delle pagine)
- Controversie legali
- Aumento dei costi di supporto
- Danno all'immagine aziendale

Rational Policy Tester

- Qualità



- Accessibilità



- Privacy



Agenda

- Rational Software
- Compliance
 - Compliance Management per SW Team
 - Compliance Applicazioni / Portali
- Sicurezza
 - Sicurezza delle applicazioni web



Sicurezza delle applicazioni web: In Italia siamo tranquilli ?

The image shows a screenshot of a web browser displaying two news articles. The left article, from LA STAMPA.it, is titled "Monster violato, 4,5 milioni di dati rubati" and discusses a data breach at the Monster website. The right article, from la Repubblica.it, is titled "Se non hai SKY non sai cosa ti perdi!" and "Nel grande buco nero di eBay 'Così abbiamo violato il sito'", detailing a security vulnerability at eBay. A red circle highlights the term "cross-site scripting" in the eBay article. The browser interface includes navigation buttons, address bars, and various website menus.

LA STAMPA.it TECNOLOGIA

Archivio storico OPINIONI POLITICA ESTERI CRONACHE COSTUME ECONOMIA TECNOLOGIA

CERCA ARTE BENESSERE CUCINA MODA MOTORI SCIENZA SCUOL

NEWS 28/1/2009

Monster violato, 4,5 milioni di dati rubati

La filiale italiana rassicura i suoi iscritti, ma sembrano a rischio altri siti che dipendono dal colosso del collocamento per la gestione tecnologica

LONDRA
I dati personali di milioni di disoccupati sono stati rubati da Monster.co.uk, il sito leader per cercare lavoro nel Regno Unito, in quello che il quotidiano *The Independent* definisce il più grande furto informatico di tutti i tempi.

Gli hacker hanno violato le informazioni confidenziali fornite da 4,5 milioni di persone registrate nel sito, impossessandosi dei loro nomi, password, numeri di telefono e indirizzi email. Secondo la società, sono stati rubati anche le date di nascita degli utenti, il genere e la nazionalità, assieme ai dati demografici basilari.

Monster ha confermato in un comunicato venerdì che ignoti erano entrati nel database, ma la dimensione del furto è emersa solo ieri, scrive il quotidiano. Si teme che i pirati informatici siano riusciti ad avere accesso ai conti bancari online degli utenti, dato che molte persone usano la stessa password per accedere a diversi siti.

la Repubblica.it Tecnologia&Scienze

Home Affari&Finanza Sport Spettacoli&Cultura Tecnologia&Scienze Motori Moda Viaggi Roma Milano

Salute

Se non hai SKY non sai cosa ti perdi!

ABBONATI ORA

21-01-2008

Quella falla m

Una vulnerabilità del m
spam di grandi proporz

Tecnologie&Scienze

Prodotti
Sicurezza Web
VideoGiochi
Mondo Mac
Software
Come fare
Gallerie

TECNOLOGIA & SCIENZA

Stampa Invia

Due cronisti e un hacker aggirano il sistema di sicurezza
Milioni di utenti a rischio truffa. Possibile accedere a dati e password

Nel grande buco nero di eBay "Così abbiamo violato il sito"

di MARCO MENSURATI e FABIO TONACCI

ROMA - C'è un buco nel sistema di sicurezza di eBay. Un buco che si apre e che si chiude di continuo, come la porta automatica di un grande magazzino. E che permette a qualunque hacker minimamente capace di entrare in possesso delle informazioni personali riservate dei clienti. E di derubarli. Noi questo buco lo abbiamo individuato, lo abbiamo aperto e poi ci siamo entrati dentro (il video si può vedere sul sito di RepubblicaTV).

Dimostrando, così, quanto sia semplice rubare i dati personali e bancari degli utenti eBay che partecipavano a una determinata asta. Un'asta come tante, usata però come esca. Con l'aiuto di un hacker abbiamo sfruttato quella che tecnicamente si chiama vulnerabilità "cross-site scripting". L'operazione non è così complessa come sembra.

Ebay, il più grande sito di compravendita online, dà la possibilità agli utenti che ritiene affidabili di abbellire graficamente le proprie pagine con particolari linguaggi di programmazione. Consegna loro delle chiavi per interagire con la grafica ufficiale, personalizzando l'architettura del sito. Con quelle chiavi - ottenute piuttosto facilmente - gli hacker costruiscono delle aste trappola (non c'è modo di distinguerle da quelle originali) e le dispongono ovunque, in quel suk virtuale che è eBay.

Adesso: Sereno, 10° C Mercoledì, 9° C Giovedì, 9° C

Una falsa percezione:
“Le nostre applicazioni Web sono sicure”

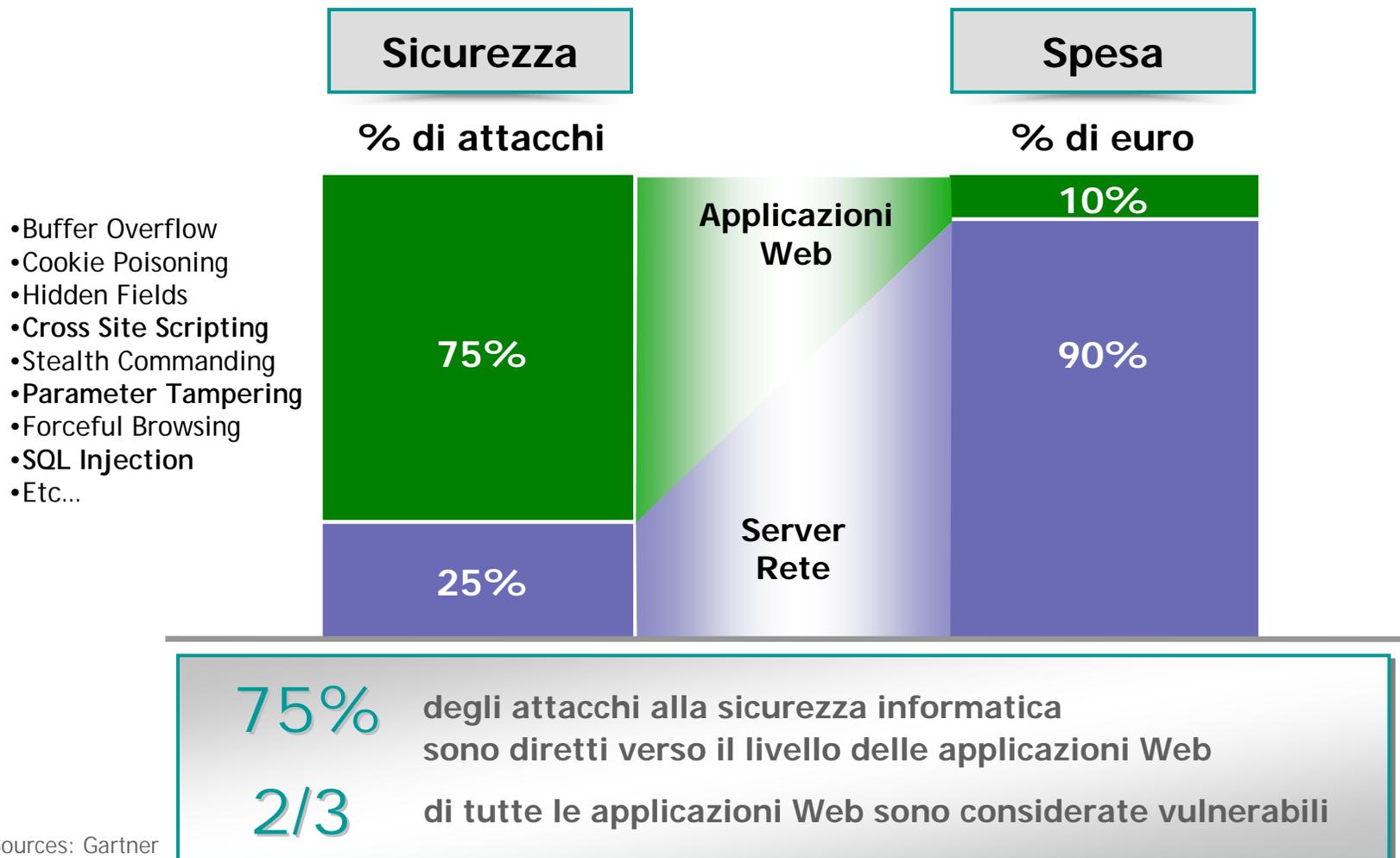
Abbiamo dei
Firewalls

Abbiamo dei revisori che
effettuano ogni trimestre
test di intrusione

Utilizziamo strumenti di
controllo della
vulnerabilità della rete



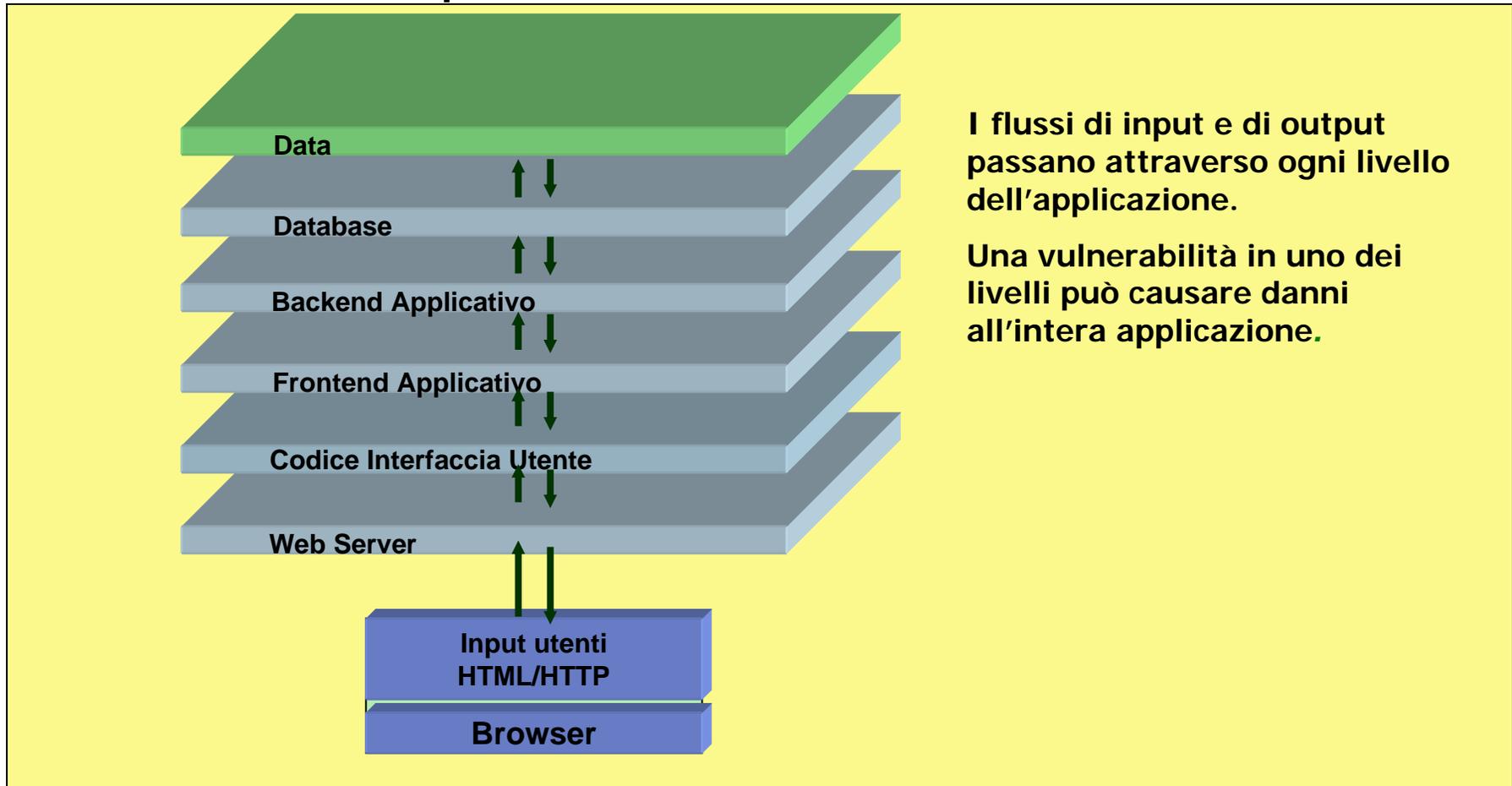
La realtà: sicurezza e spesa non sono bilanciati



Sources: Gartner



Come è fatta un'applicazione Web e perchè può essere vulnerabile?



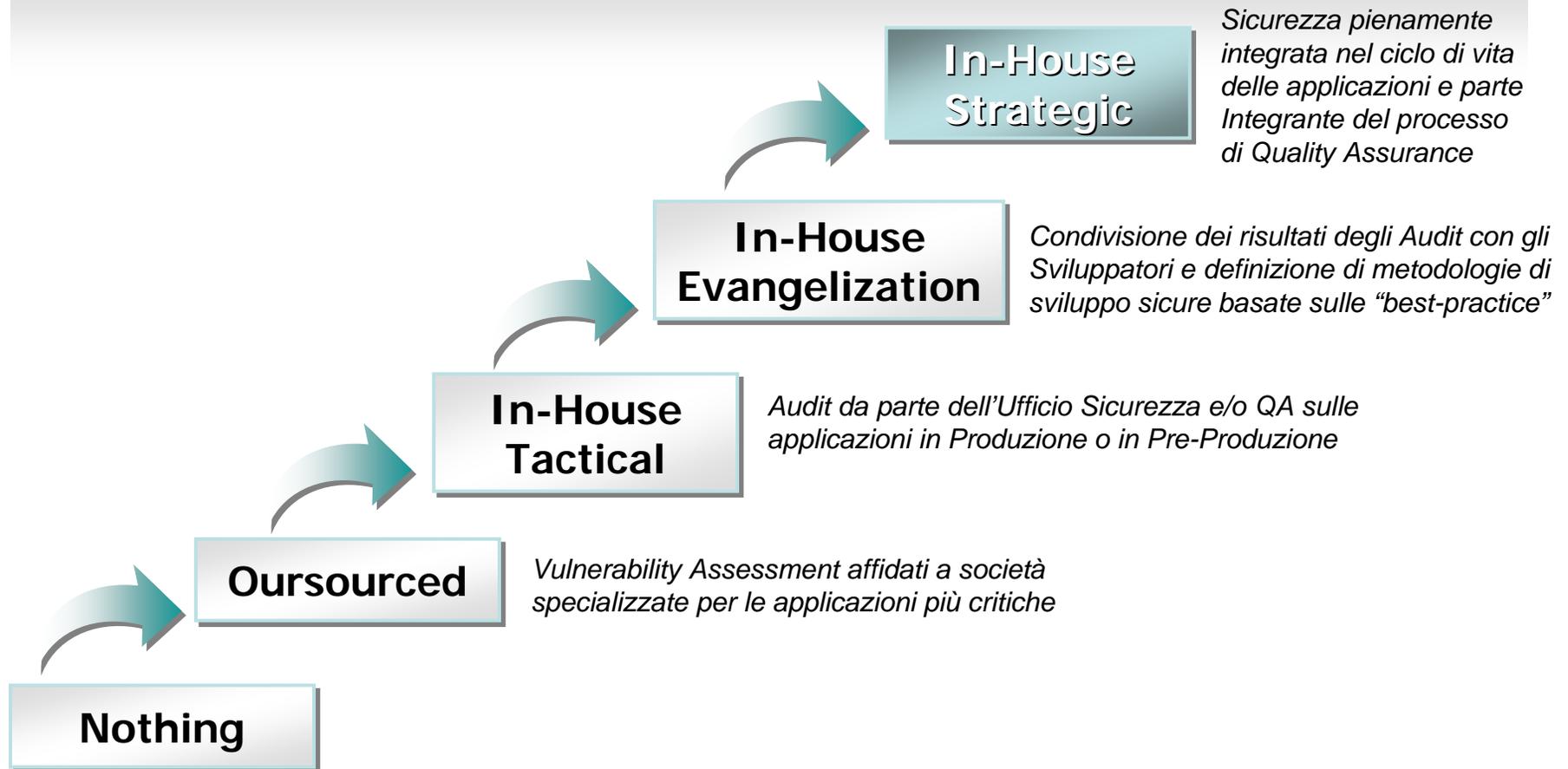
Le soluzioni di sicurezza per la infrastruttura non indirizzano questa problematica

- **Firewalls e IPS (Intrusion Prevention System) non possono bloccare tutti gli eventuali attacchi al livello applicativo**
 - La porta 80 deve essere disponibile per essere utilizzata
- **Strumenti di scansione della rete non identificano eventuali vulnerabilità applicative**
 - Nessus, IBM ISS, Qualys, Nmap, etc.
- **Chi sviluppa applicazioni Web non ha conoscenze adeguate di sicurezza applicativa**
 - 64% degli sviluppatori non sono confidenti di poter scrivere applicazioni sicure (fonte Microsoft Developer Research)

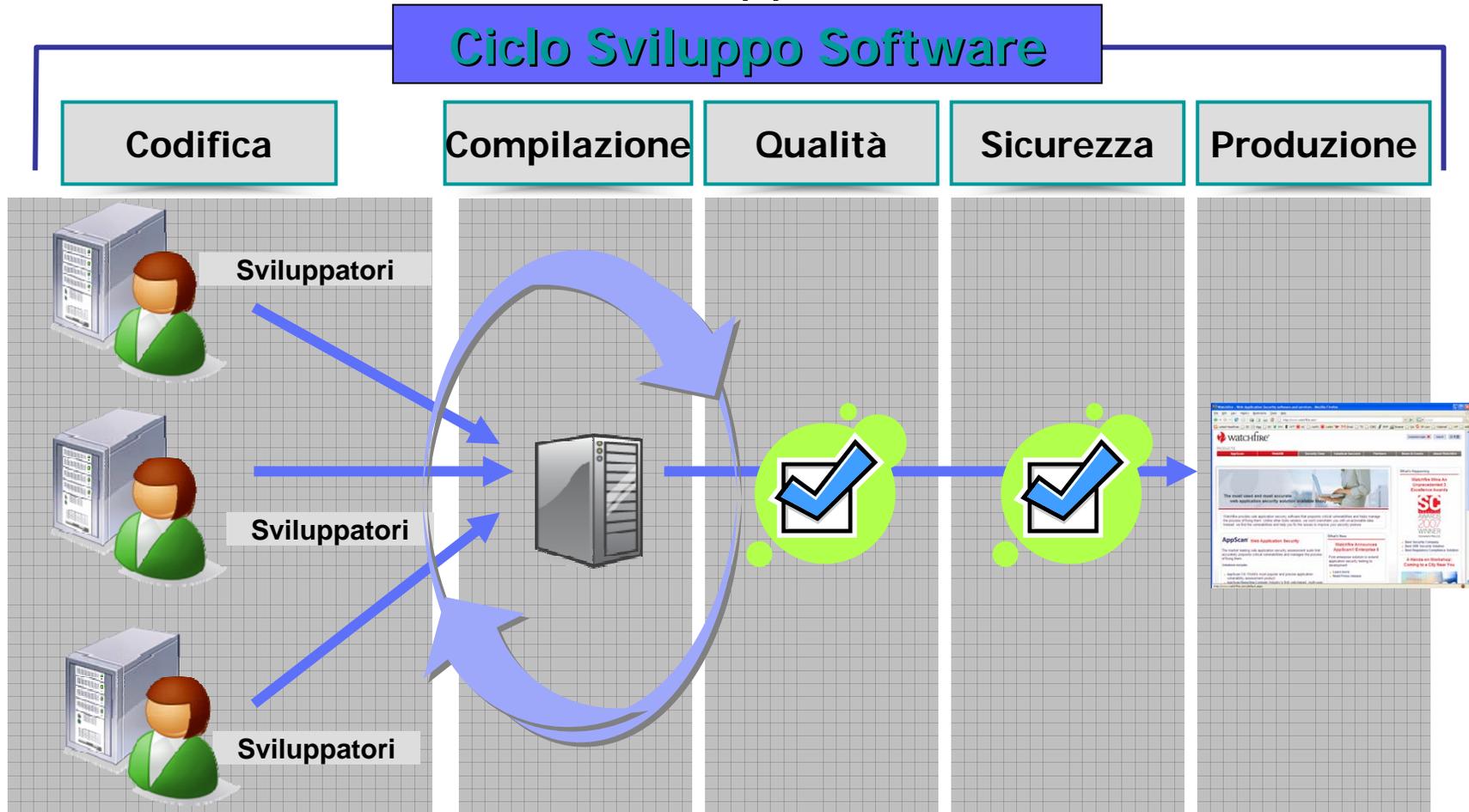


Maturità del modello di "Security Test"

Evoluzione della "Web Application Security"



Perchè è importante gestire la sicurezza durante l'intero ciclo di sviluppo?



IBM SOFTWARELAND 2009.



+ Qualità + Sicurezza = Riduzione Costi !!!!

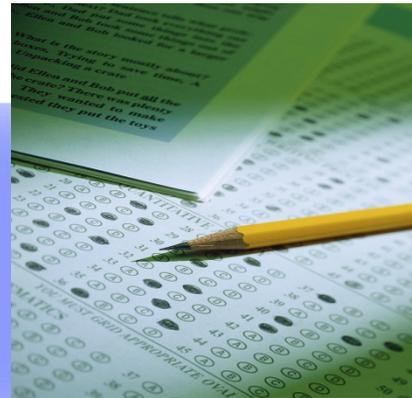
L' 80% dei costi di sviluppo è speso per individuare e correggere i difetti!



During the coding phase
\$25/defect



During the build phase
\$100/defect



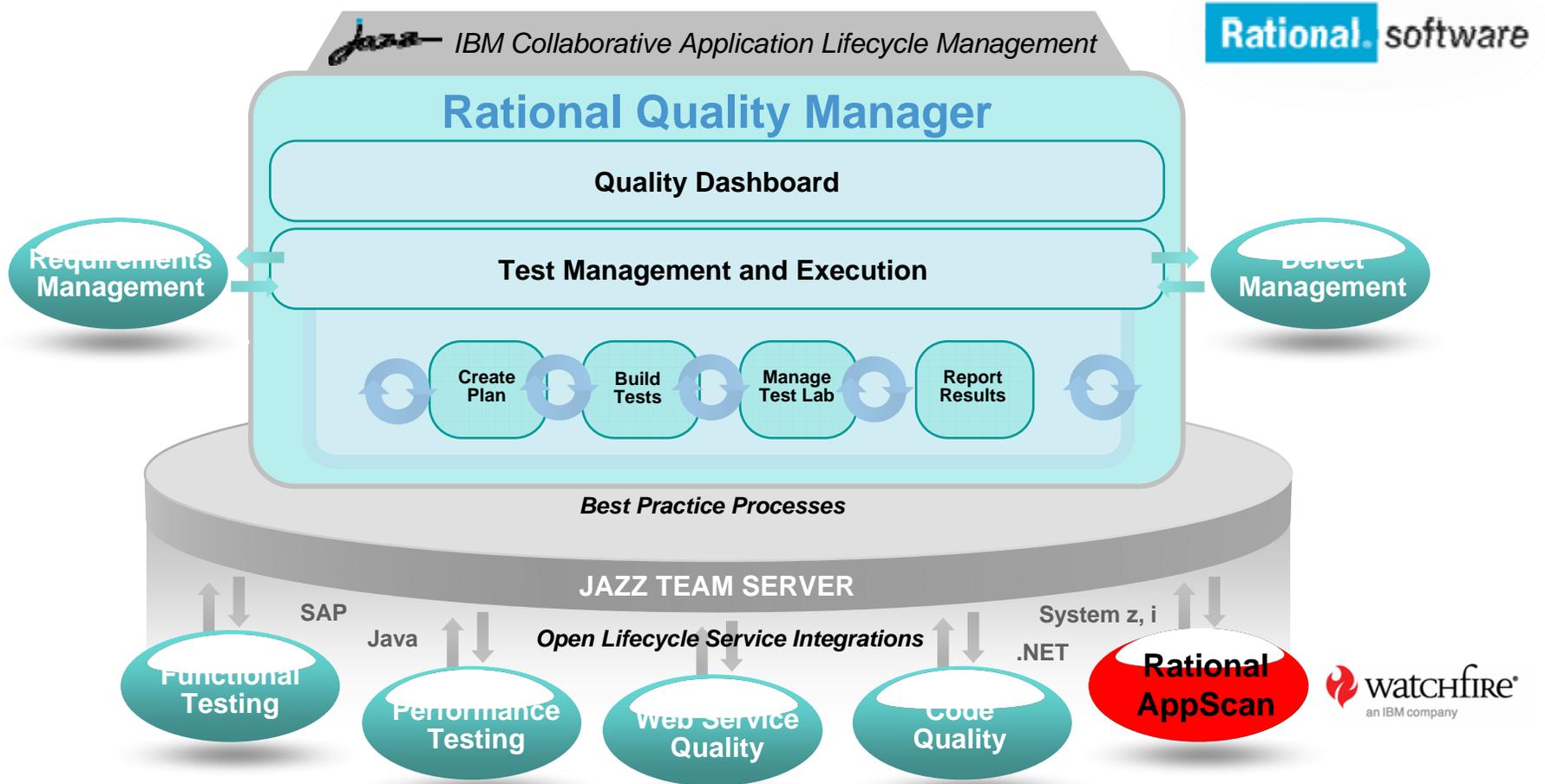
During the QA/Testing phase
\$450/defect



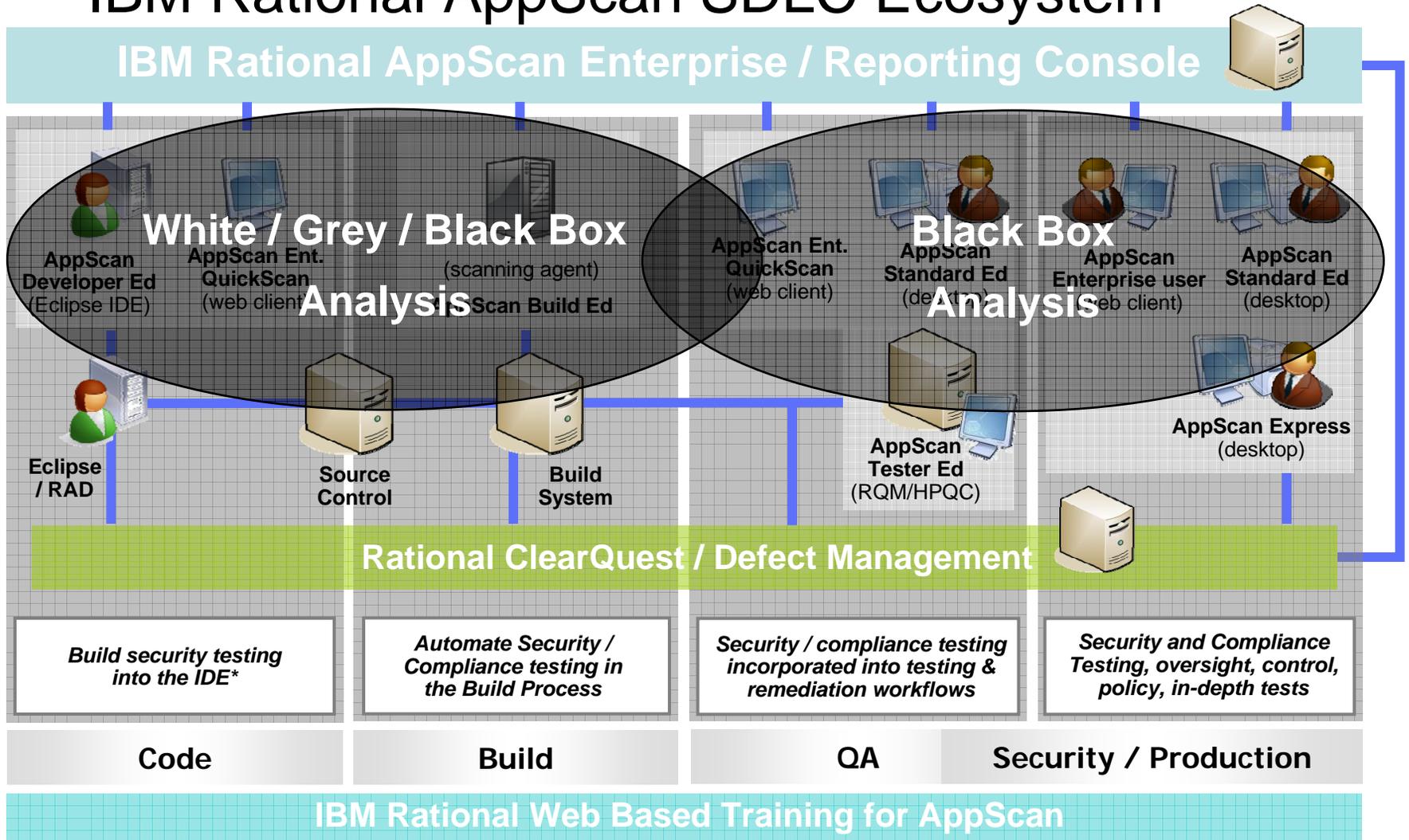
Once released as a product
\$16,000/defect



Rational Software Quality Management



IBM Rational AppScan SDLC Ecosystem



DOMANDE ?





Learn more at:

- [IBM Rational software](#)
- [IBM Rational Software Delivery Platform](#)
- [Process and portfolio management](#)
- [Change and release management](#)
- [Quality management](#)
- [Architecture management](#)
- [Rational trial downloads](#)
- [developerWorks Rational](#)
- [IBM Rational TV](#)
- [IBM Rational Business Partners](#)

© 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.

