The Unprecedented State of Web Insecurity

New and Emerging Internet Threats

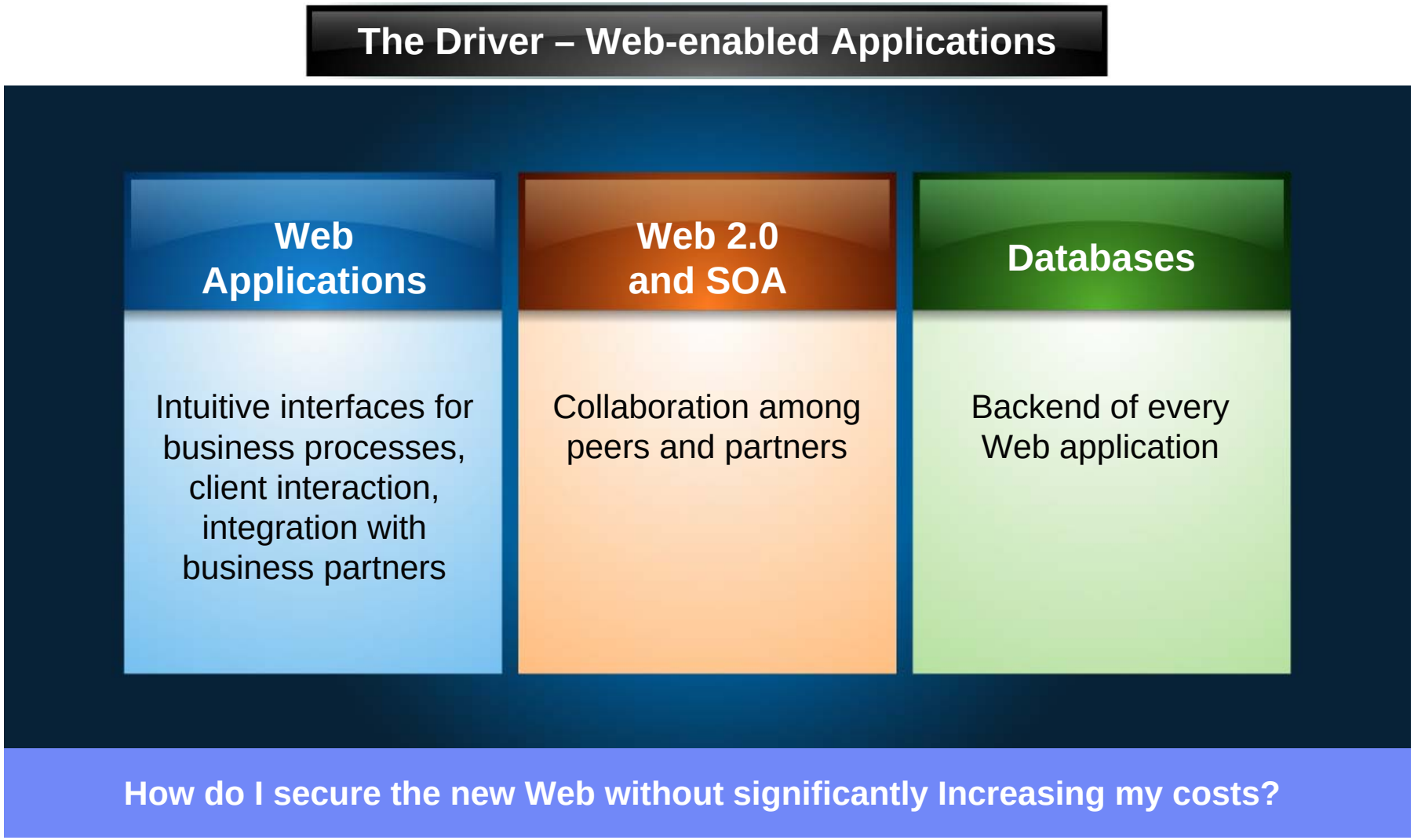
Pulse2010
The Premier Service Management Event

Adrian John Lim
Rational Software

Smarter planet opportunities driven by Web-enabled applications

The Opportunity – smarter planet

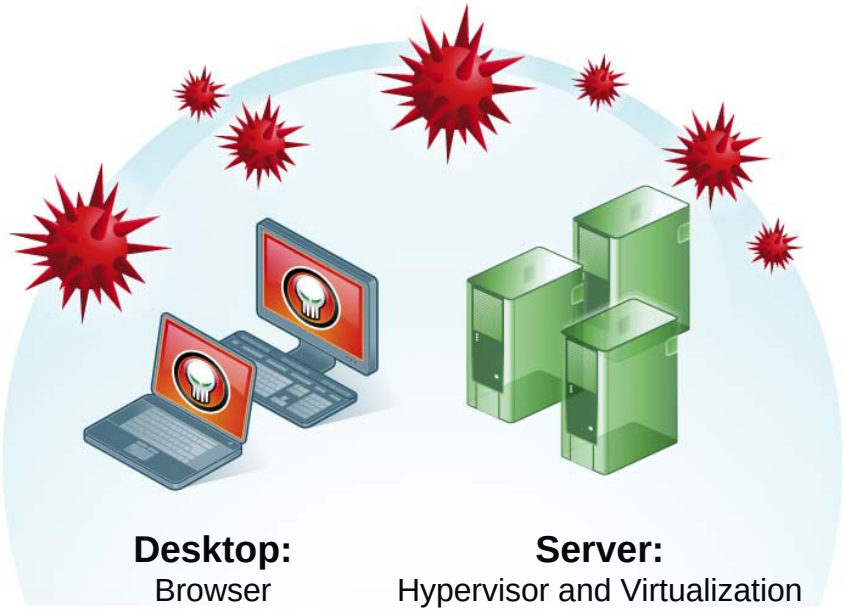
Smarter planet opportunities driven by Web-enabled applications



Changing security landscape creates complex threats

Web-enabled applications drive the need for security

- New applications are increasing the attack surface
- Complex Web applications create complex security risks
- Making applications more available to “good” users, makes them more available to “bad” users
- Web attacks are evolving to blended attacks (i.e. planting of malware on legitimate Web sites)



Desktop:
Browser

Server:
Hypervisor and Virtualization
Web Applications

The Myth: “Our Site Is Safe”

We Have Firewalls and IPS in Place

Port 80 & 443 are open for the right reasons

We Audit It Once a Quarter with Pen Testers

Applications are constantly changing

We Use Network Vulnerability Scanners

Neglect the security of the software on the network/web server

We Use SSL Encryption

Only protects data between site and user not the web application itself

SOMETHING IS STILL OUT THERE ...

BBC NEWS

Watch One-Minute World News

Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment
In the news

Last Updated: Tuesday, 21 August 2007, 10:01 GMT 11:01 UK

E-mail this to a friend Printable version

Monster attack steals user data

US job website Monster.com has suffered an online attack with the personal data of hundreds of thousands of users stolen, says a security firm.

A computer program was used to access the employers' section of the website using stolen log-in credentials.

Symantec said the log-ins were used to harvest user names, e-mail addresses, home addresses and phone numbers, which were uploaded to a remote web server.

Monster is a leading online jobs service

c|net NEWS.com

http://news.cnet.com/8

April 6, 2007 4:39 PM PDT

Asus Web site harbors threat

Posted by Joris Evers

It is not such a Good Friday for ASUStek Computer.

The main Web site of the Taiwanese hardware maker, known for its Asus branded PCs a been rigged by hackers to serve up malicious software that attempts to exploit a critical W experts said Friday.

The attackers added an invisible frame, a so-called iframe, to the front page of the Asus.c the site, a victim's browser will silently connect to another Web site that tries to install a m

"We've just confirmed multiple reports about Asus.com, a very well known hardware mar compromised," a researcher with Kaspersky Lab wrote on the company's Viruslist.com s

MY PAPER TUESDAY MARCH 3, 2009

SINGAPORE

TUE MAR 03 09 MYPAPER

Glitch spills UBS clients' info

Wealthy customers saw details of others' online accounts, but bank says number affected is small

KENNY CHEE

A TECHNICAL glitch at Swiss bank UBS gave its wealthy customers in Singapore and Hong Kong a shock last week when they logged on to their online accounts.

The private-banking clients found confidential details of other clients' bank statements and account information instead of their own. Clients' online accounts, though, do not indicate their names.

Asked how many clients were affected, all she said was that "some limited account information concerning a small number of UBS wealth-management clients was accessible by a very limited number of other system users". She added that fewer than five accessed the information.

She told *my paper* the glitch occurred "as a result of an inadvertent technical error following an information-technology system upgrade over the weekend ing to the incident and has implemented measures to prevent a similar occurrence in the future.

The bank also reported the incident to the banking authorities here and in Hong Kong: the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA).

Asked about what MAS would be doing, its spokesman said that "we are following up with the bank", but did not elaborate.

The HKMA said it is "following up with the bank on any impact... and the remedial measures that should be taken".

Its spokesman added: "We have requested the bank to sub-

Mr Tan Teik Guan, chief executive of Data Security Systems Solutions, said such accidental leaks of confidential information could lead to "embarrassing situations for clients and reputation risks for banks".

"Intentional leakages are more serious as the data... (could be) used for more malicious activities," he said.

kennyc@sph.com.sg

HELPDESK 我的字典

Glitch: 小故障 xiǎo gù zhàng

PAGE H2

STRAITS TIMES FRIDAY FEBRUARY 11, 2005

GAME OVER

Four friends spent two years amassing $15,000 worth of riches in an online game – only to lose it all to a hacker. In a new series on digital crime in Singapore, ChuaHian Hou looks at how the victims and the police teamed up to crack the first such case here

WORST CREDIT CARD IDENTITY THEFT CASE
- DONE BY SQL INJECTION : A WEB APP ATTACK!

STRAITS TIMES SINGAPORE 19AUG09

prime news

THE STRAITS TIMES WEDNESDAY, AUGUST 19 2009 PAGE A6

Hacker accused of stealing 130 million credit card numbers

WASHINGTON: A former government informant known online as "soupnazi" stole information from 130 million credit and debit card accounts in what federal prosecutors are calling the largest case of identity theft yet.

Albert Gonzalez, 28, and two other men have been charged with allegedly stealing more than 130 million credit and debit card numbers in the largest hacking and identity theft case in the United States.

Gonzalez is already in jail in connection with hacking into 40 million other accounts, which at that time was believed to be the biggest case of its kind. Two unnamed Russians were also indicted in the latest charges.

Gonzalez, who lives in Florida and was indicted on Monday in New Jersey, is a one-time informant for the US Secret Service who had once helped to hunt hackers, said the authorities.

The agency later found out that he also had been working with criminals and fed them information on investigations, even warning off at least one individual, according to the authorities.

Gonzalez and the Russians, identified as "Hacker 1" and "Hacker 2", targeted large corporations by scanning the list of Fortune 500 companies and exploring corporate websites before setting out to identify vulnerabilities. The goal was to sell the stolen data to others.

The ring targeted customers of the giant 7-Eleven convenience store and the regional Hannaford Brothers supermarket chain. He also took aim at the Heartland Payment Systems, a New Jersey-based card payment processor.

The Justice Department said the new case represents the largest alleged credit and debit card data breach ever prosecuted in the US.

Gonzalez faces up to 20 years in prison if convicted on the new charges. The scheme began in October 2006 and ended last year when he was nabbed in the earlier hacking case.

Gonzalez allegedly devised a sophisticated attack to penetrate the computer networks and steal the card data.

He then sent that data to computer servers in California, Illinois, Latvia, the Netherlands and Ukraine.

"The scope is massive," Assistant US Attorney Erez Liebermann said yesterday in an interview.

Last year, the Justice Department charged Gonzalez and others with hacking into retail companies' computers with the theft of approximately 40 million credit cards.

At the time, that was believed to have been the biggest single case of hacking private computer networks to steal credit card data, puncturing the electronic defences of retailers including T.J. Maxx, Barnes & Noble, Sports Authority and OfficeMax.

Prosecutors said Gonzalez was the ringleader of the hackers in that case and caused more than US$400 million (S$580 million) in damage.

At the time of those charges, officials said the alleged thieves were not computer geniuses, just opportunists who used a technique called "wardriving".

This involved cruising through different areas with a laptop computer and looking for accessible wireless Internet signals.

Gonzalez faces a possible life sentence if convicted in the earlier case.

Restaurants are among the most common targets for hackers, experts said, because they often fail to update their antivirus software and other computer security systems.

Mr Scott Christie, a former federal prosecutor now in private practice, said the case shows that despite the best efforts by companies to protect data privacy, there remain individuals capable of sneaking in.

"Cases like this do cause companies to sit up and take notice that this is a problem and more needs to be done," he said.

ASSOCIATED PRESS, REUTERS

Poking holes in computer security

ALBERT Gonzalez and his conspirators reviewed lists of Fortune 500 companies to decide which corporations to take aim at.

Then the men visited their stores to monitor which payment systems they used and their vulnerabilities, prosecutors said.

The online attacks took advantage of flaws in the SQL programming language, which is commonly used for databases.

Prosecutors said the defendants used malicious software known as malware and so-called injection strings to attack the computers and steal data.

They created and placed "sniffer" programs on corporate networks; the programs intercepted credit card transactions in real time as they moved through the computer networks.

These programs transmitted the numbers to computers that the defendants had leased in the United States, the Netherlands and Ukraine.

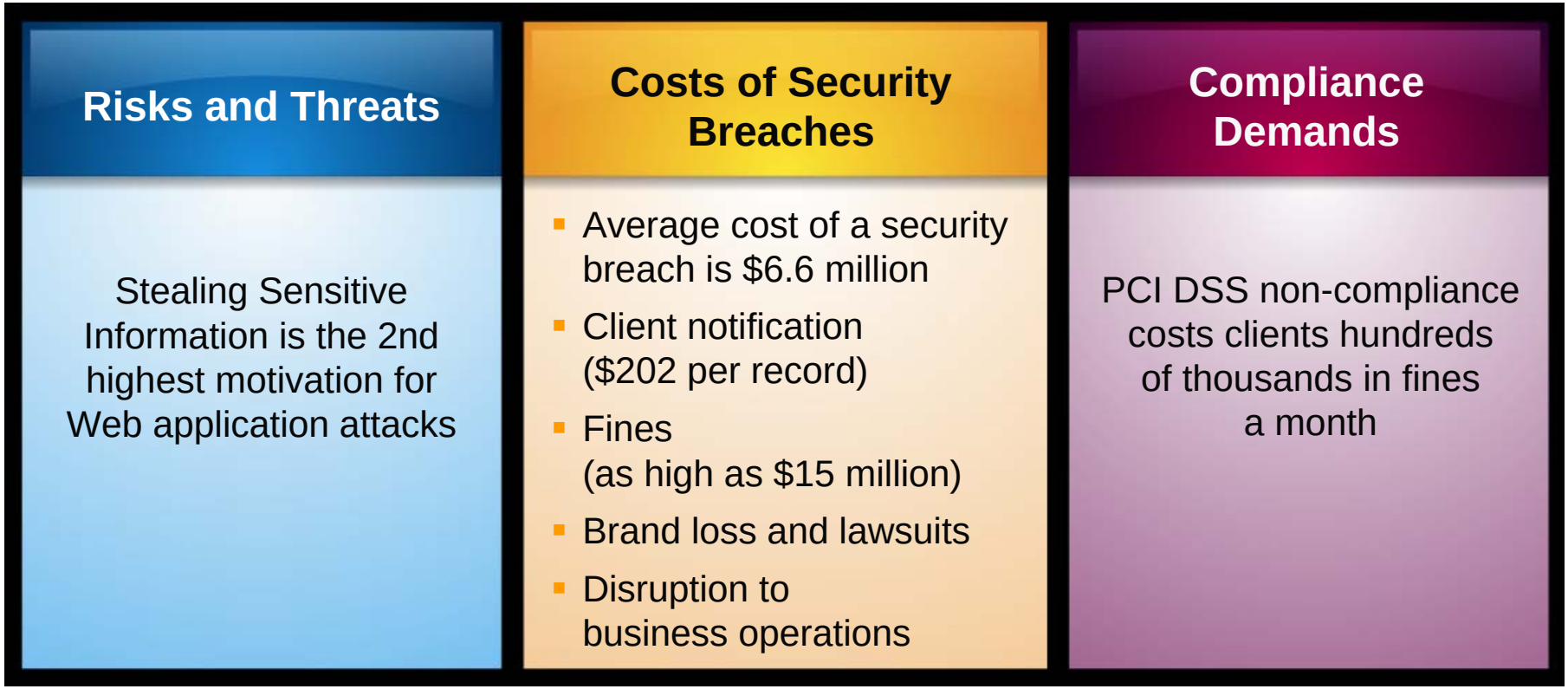
The hackers used instant messaging services to advise each other on how to navigate the systems, according to the indictment.

The conspirators attempted to erase all digital footprints left by their attacks.

They programmed malware to evade detection by antivirus software and erase files that might detect its presence, prosecutors said.

THE NEW YORK TIMES, BLOOMBERG

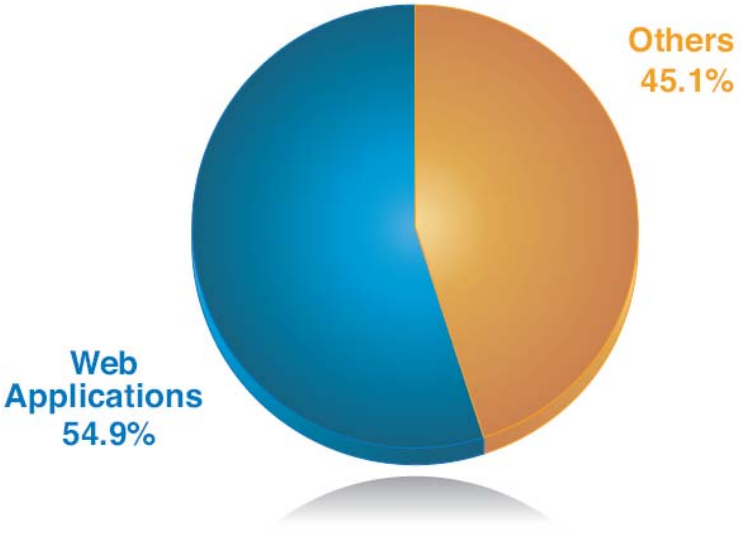
Unprotected Web applications risk sensitive data and compliance



Source: Web Incidents Hacking Database 2008 Annual report

2009 Web Threats Take Center Stage

- Web application vulnerabilities
  - Attacks here has surpassed the network /infra security ones
  - Represent largest category in vulnerability disclosures (54.9% in 2008)



Now even IBM X-Force, which normally reports on network security, is talking about Web Application Security

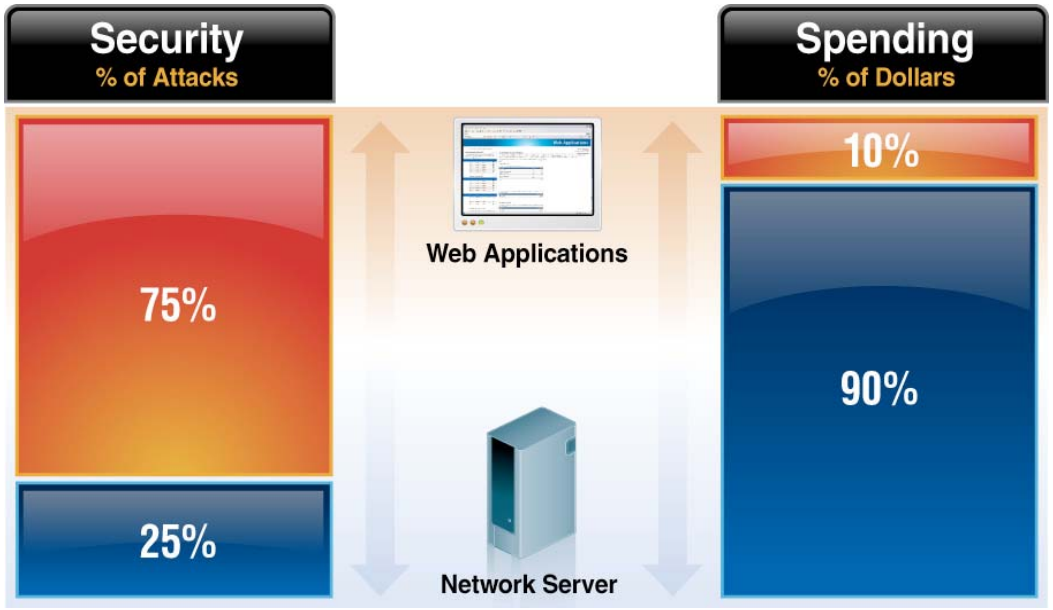
Top 10 OWASP Critical Web Application Security Risks '10

1. Injection
2. Cross-Site Scripting (XSS)
3. Broken Authentication and Session Management
4. Insecure Direct Object Reference
5. Cross-Site Request Forgery (CSRF)
6. Security Misconfiguration
7. Insecure Cryptographic Storage
8. Failure to Restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects and Forwards

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Traditional point solutions throw money at the problem and can't address the full problem

- **Vulnerability scanners**
  - Traditional vulnerability scanners don't cover Web applications
- **Penetration testing**
  - Effective at finding vulnerabilities but not scalable for ongoing tests
  - Not focused on remediation
- **Network firewall and IPS**
  - Generic Web application protection (if any) so most custom Web applications not covered
  - Most IPS solutions focus on exploits as opposed to Web application vulnerabilities
- **Web application firewall**
  - Expensive point product to deploy and manage
  - Can be effective, but difficult to deploy, tune and manage
  - Building policies can be as time consuming as remediating the vulnerability



Source: Gartner

Software Application Development Pressures

Today I'm being asked to:

- **Deliver product faster (a lot faster!)**
- **Increase product innovation**
- **Improve quality**
- **Reduce cost**
- **Deliver a secure product (?)**

Cheap
Fast
Good
- Choose 2

The Application Security Challenge

What?

1. Need to **mitigate the risk** of a Security breach
2. Need to **find** and **remediate** these vulnerabilities
3. Must utilize a **cost effective** way of doing this that makes sense

Who?

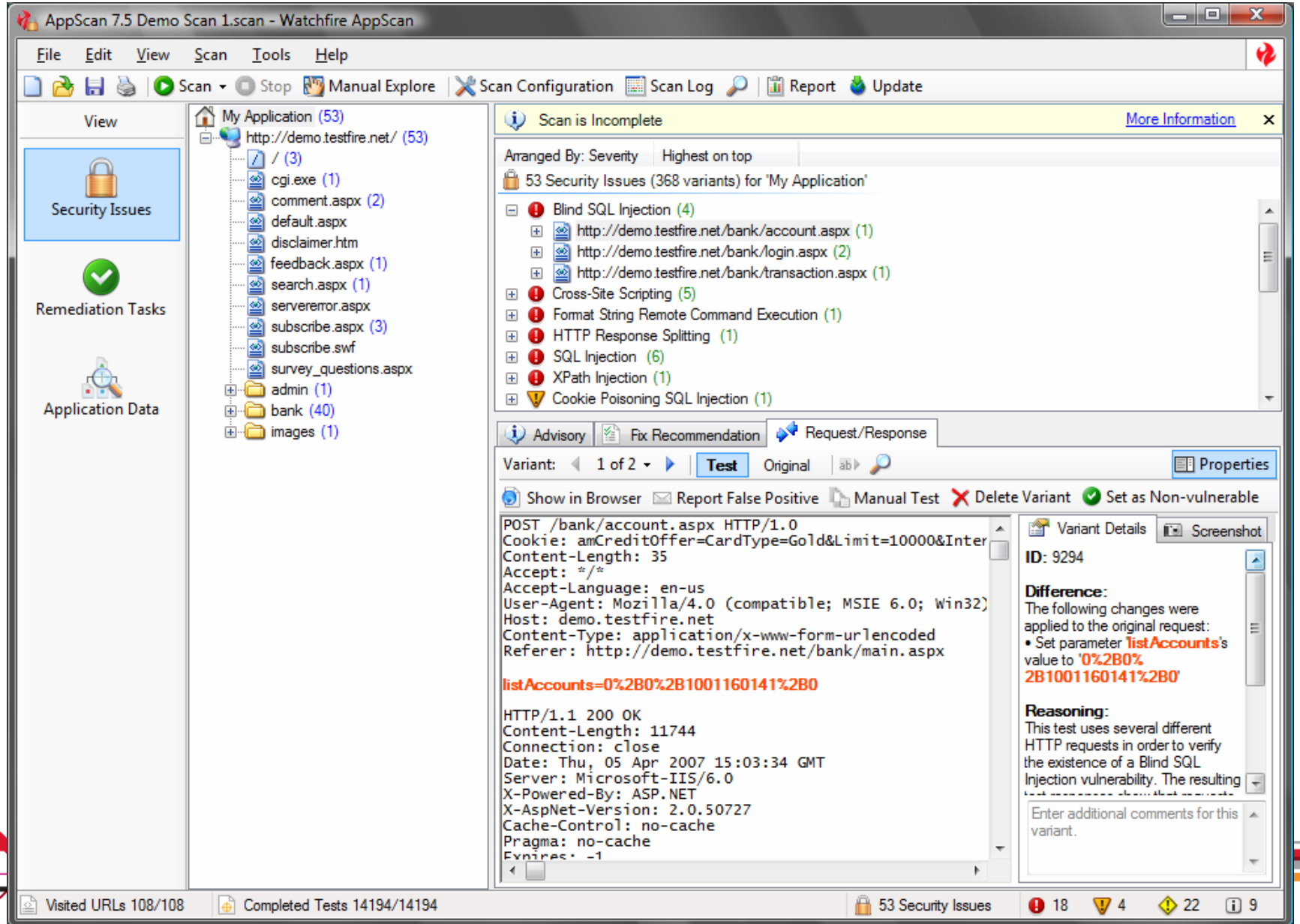
- Software security represents the **intersection between security & development** – solution needs to be a joint collaboration
- Starts with Security Auditor (can also be outsourced)
- Larger organizations require the scaling of security testing into the development organization

Web Application Security - Solution Strategy

- **Reduce Cost and Time to Market**
  - Find the issues earlier in the Software Development Life Cycle
  - Automate the process
  - Use less security-savvy employees by leveraging tools
- **Mitigate Risk and increase quality**
  - Increase coverage
  - Involve more people in the process: Developers / QA
- **Increase Visibility Of The Security Issue**
  - Distribute reports to different levels
  - Dashboards
- **Increase Productivity**
  - Build the knowledge among the team
  - Prevent making the same mistakes

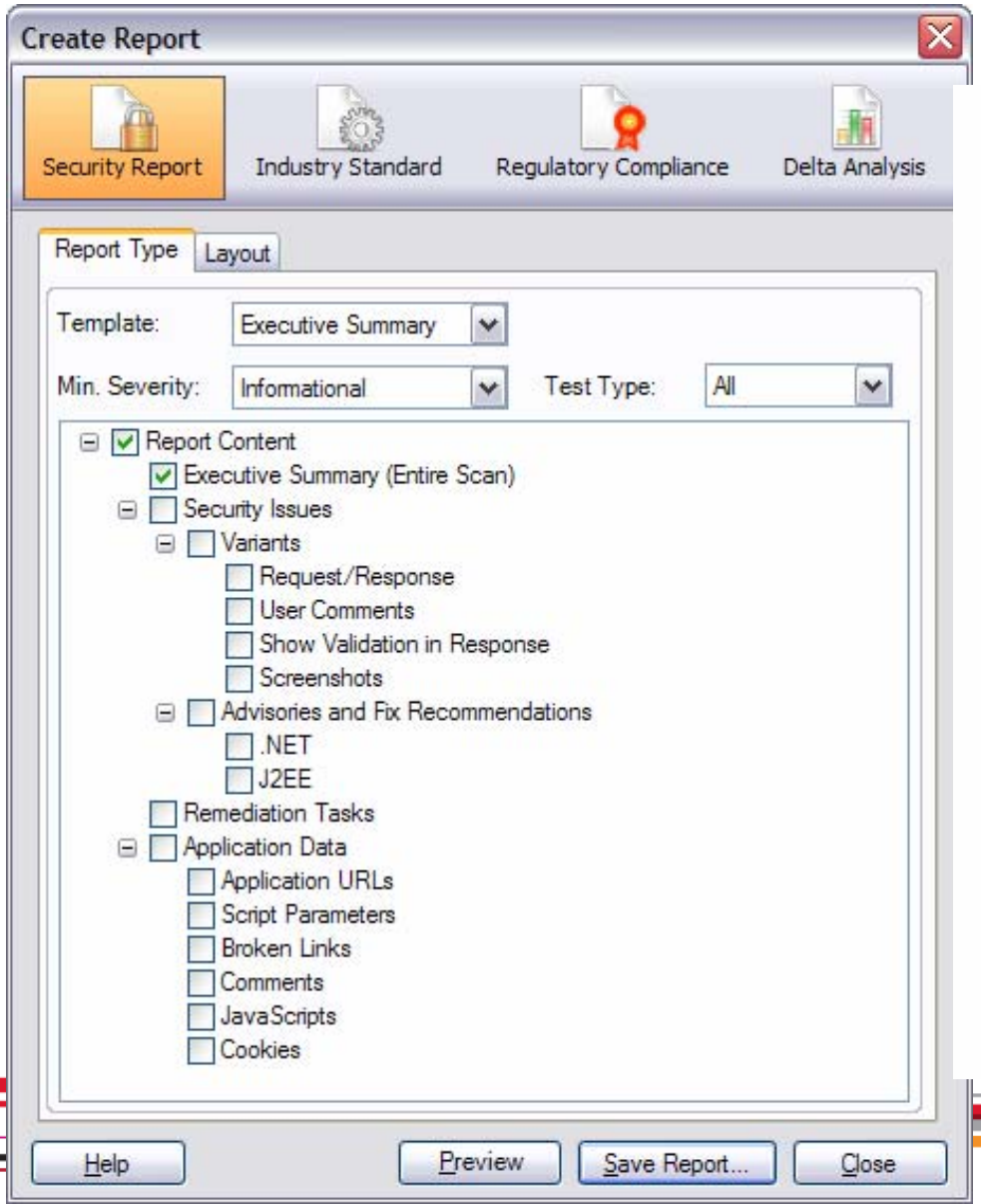
You need a professional solution to

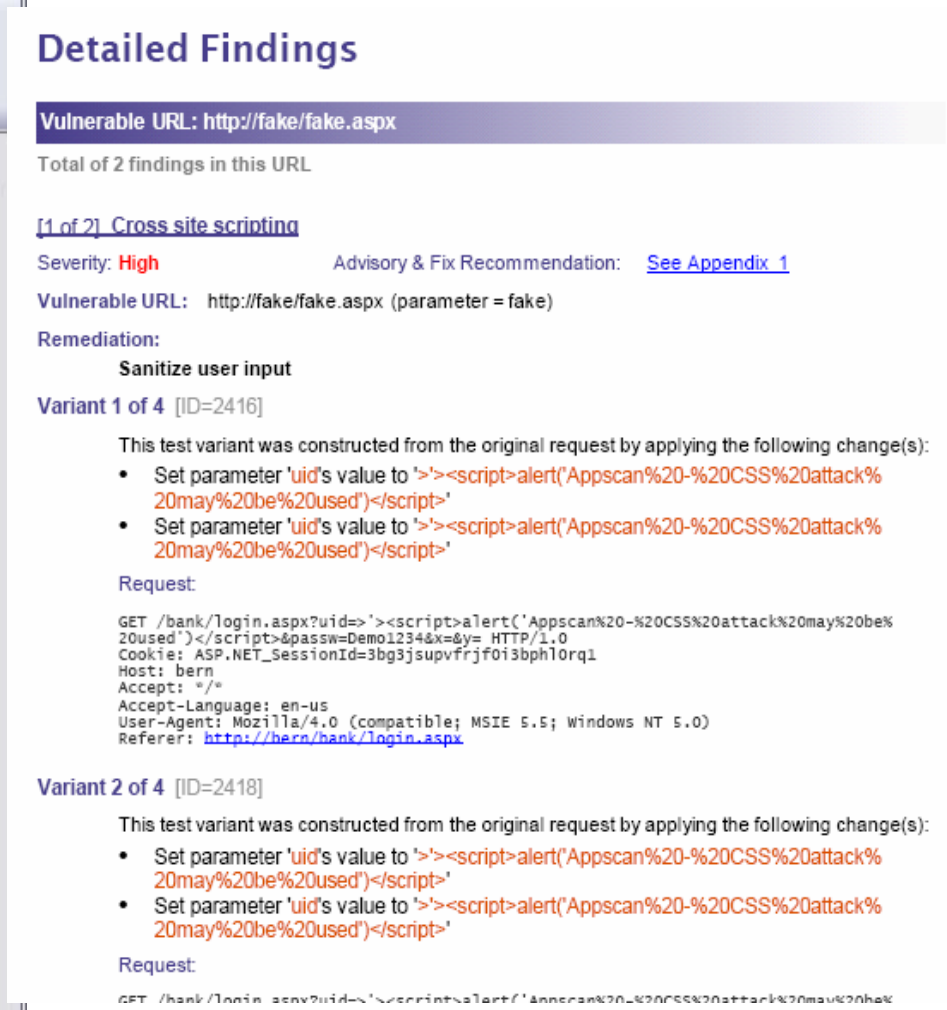
Identify Vulnerabilities



With Rich Report Options

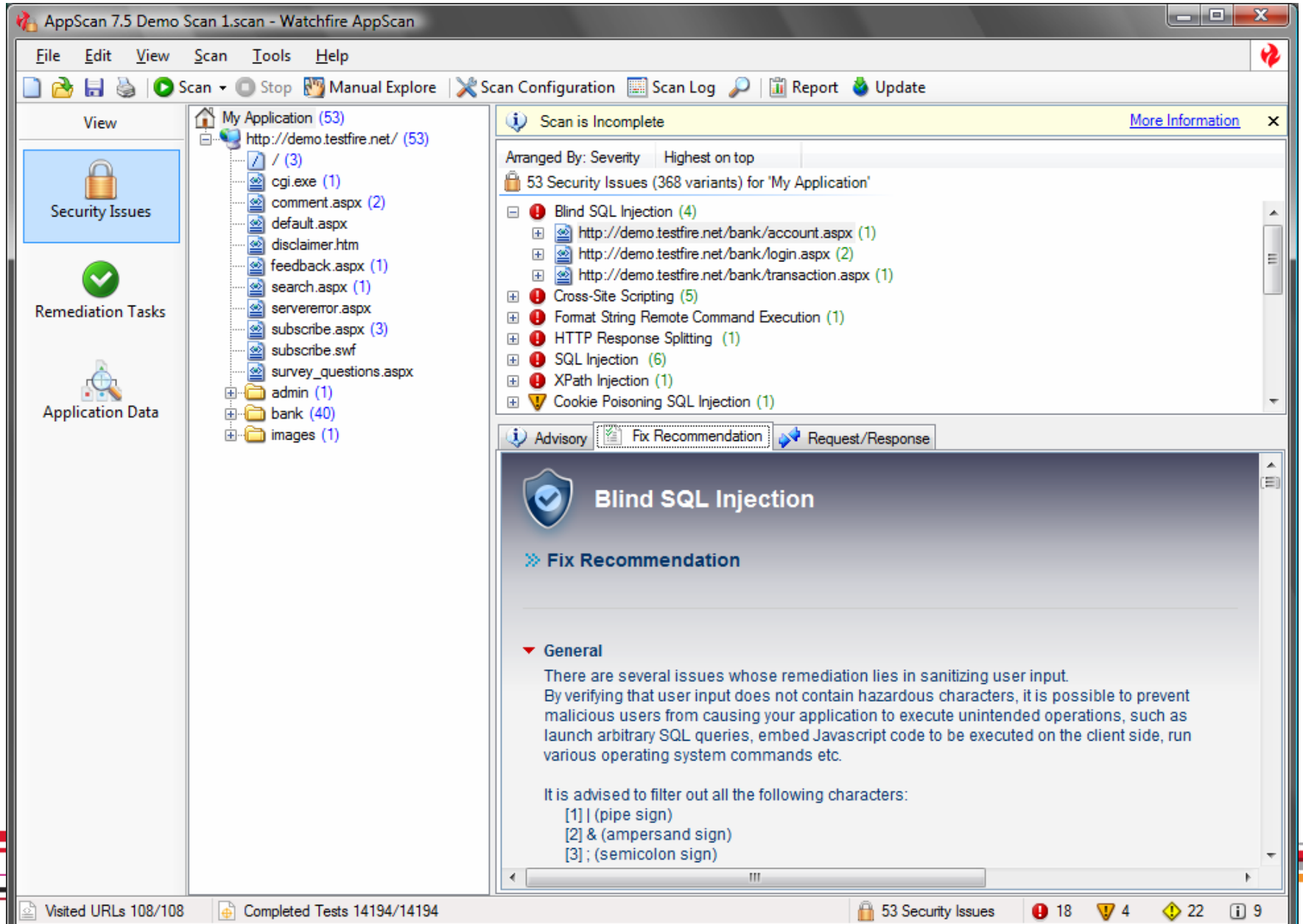
44 Regulatory Compliance Standards, for Executive, Security, Developers.





And Most Important:

Actionable Fix Recommendations



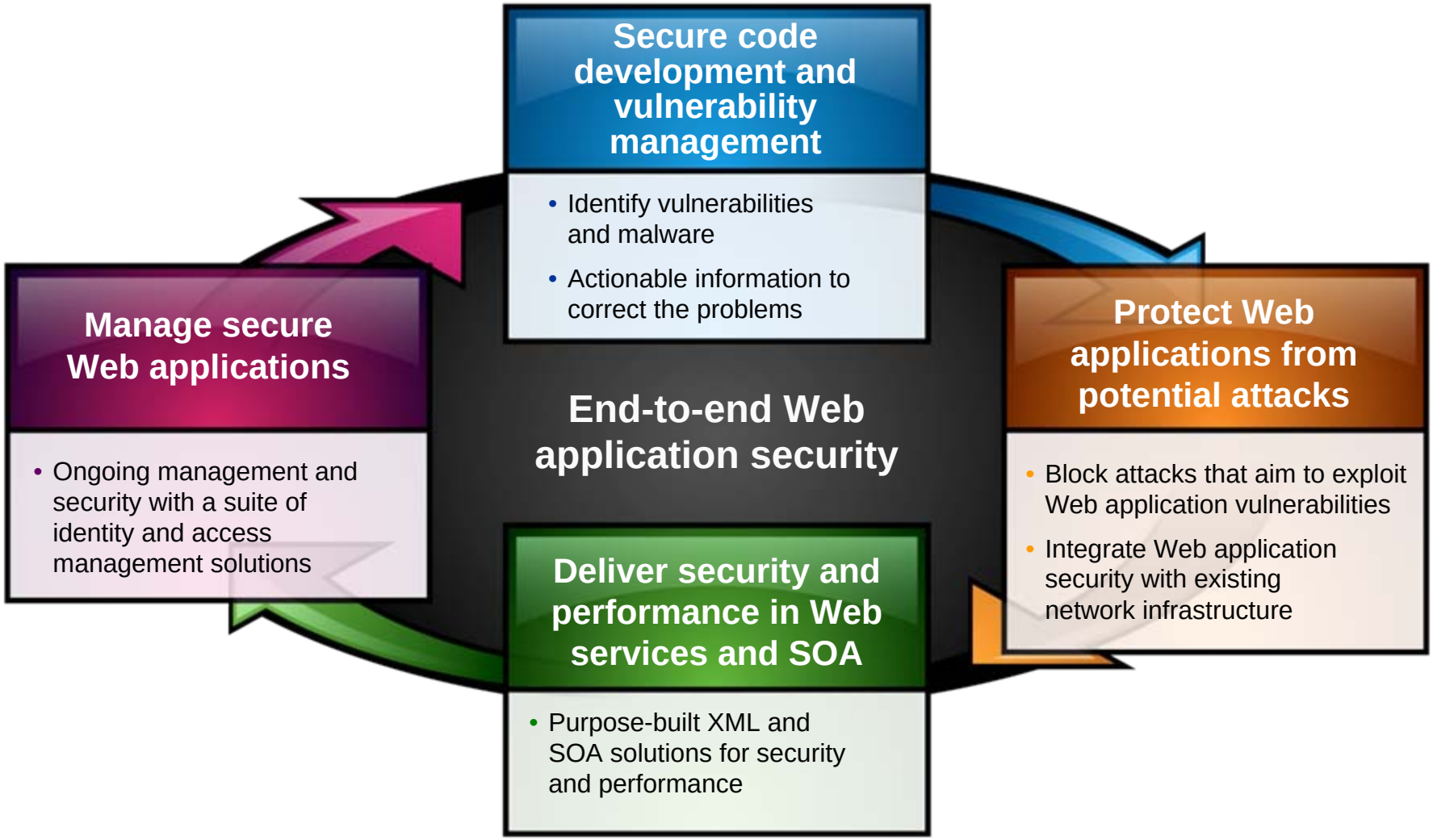
Last but not the least:
Dashboards and Metrics

IBM Security Framework includes integrated solutions for Web application security

IBM Web Application Security

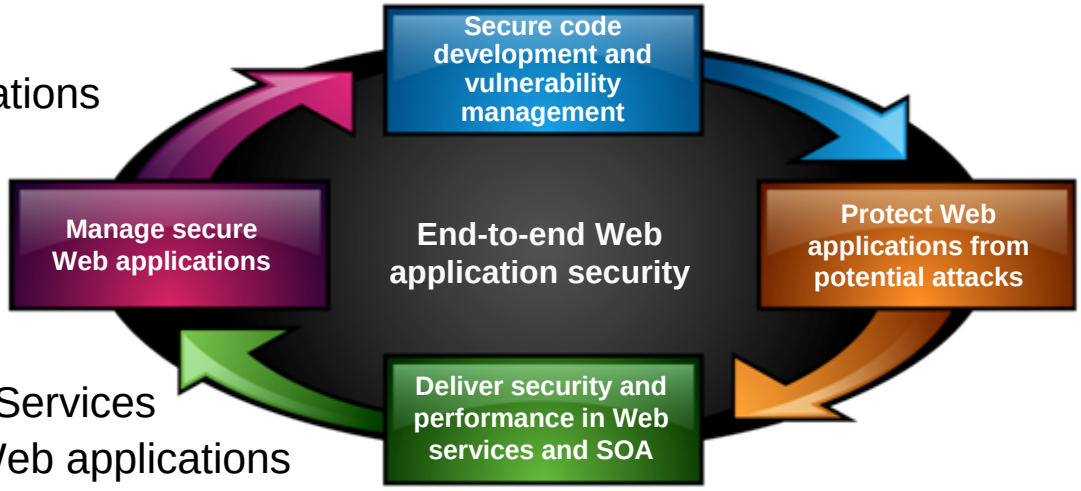
- **Assessments and professional services**
  - Identify security gaps
  - Expertise to build secure processes
  - Trusted insights to integrate Web application security into holistic security strategy
- **Software and hardware solutions**
  - Market leading solutions
  - IBM Internet Security Systems™ (ISS)
  - Rational®
  - Tivoli®
  - WebSphere®
- **Managed services**
  - Trusted experts proven to reduce the cost and complexity of security operations

Solution: IBM Web application security for a smarter planet



Solution: IBM Web application security for a smarter planet

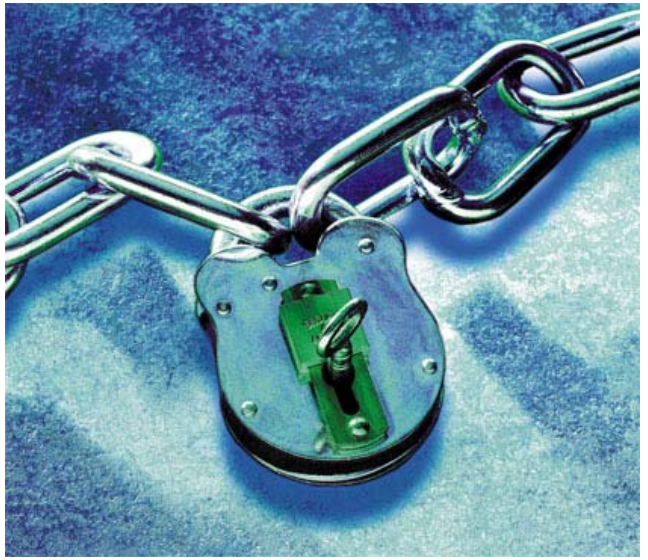
- **Best practices: Integrate secure development, vulnerability management, network protection and host protection**
  - Develop secure Web applications
  - Identify vulnerabilities in existing applications
  - Protect Web applications, Web 2.0 and databases at the network and server
  - Dedicated security for Web Services
  - Manage secure access to Web applications



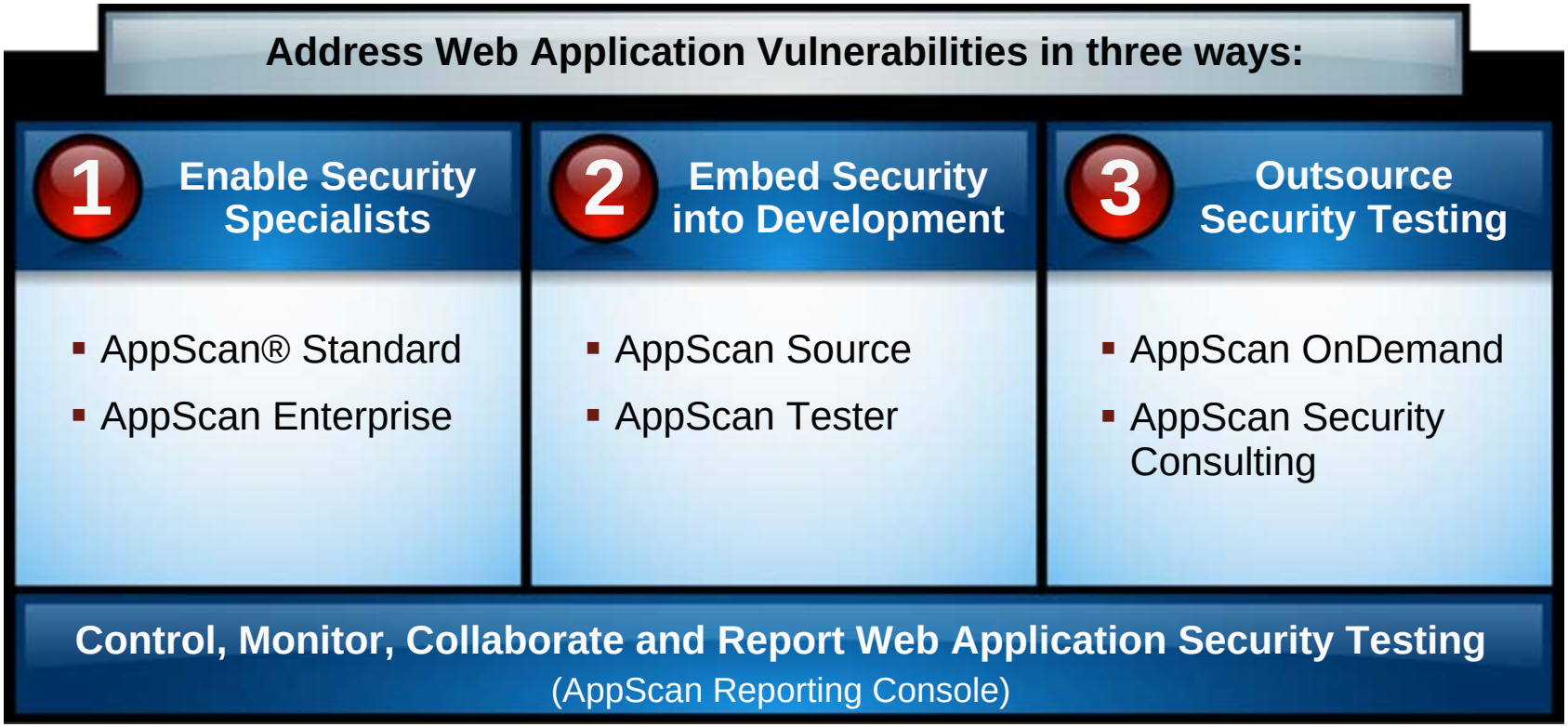
- **Centralized Management**
  - Correlate vulnerabilities vs. protection policies vs. actual security events
  - Centralize application entitlement and SOA security policy management
- **End-to-end Web security from your trusted security advisor**

Secure code development and vulnerability management – IBM Rational® AppScan®

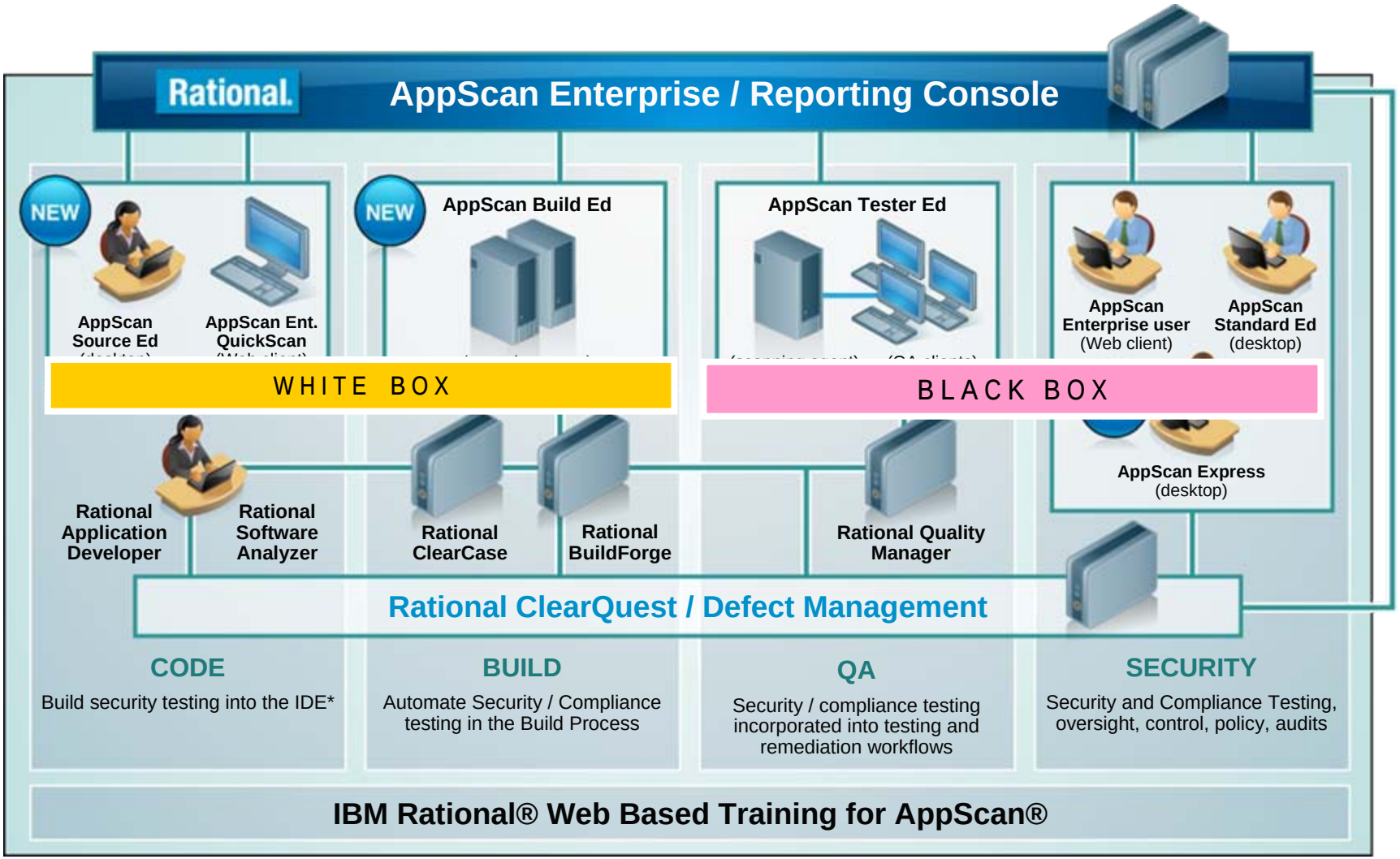
- **A market leader for Web application vulnerability scanning**
  - A leader in numerous industry “bake offs”
- **Automatically scans Web applications for vulnerabilities**
  - SQL Injection
  - Cross-site Scripting
- **Provides clear recommendations on how to remediate identified vulnerabilities**
- **Scans Web sites for embedded malware**
  - Protect your Web site from distributing the next Conficker to every Web site visitor
  - Powered by the IBM Internet Security Systems™ X-Force® malware prevention system



Enabling the operationalization of security testing



Enabling security testing through the SDLC



Secure code development and vulnerability management

Protect Web applications from potential attacks

Deliver security and performance in Web services and SOA

Manage secure Web applications

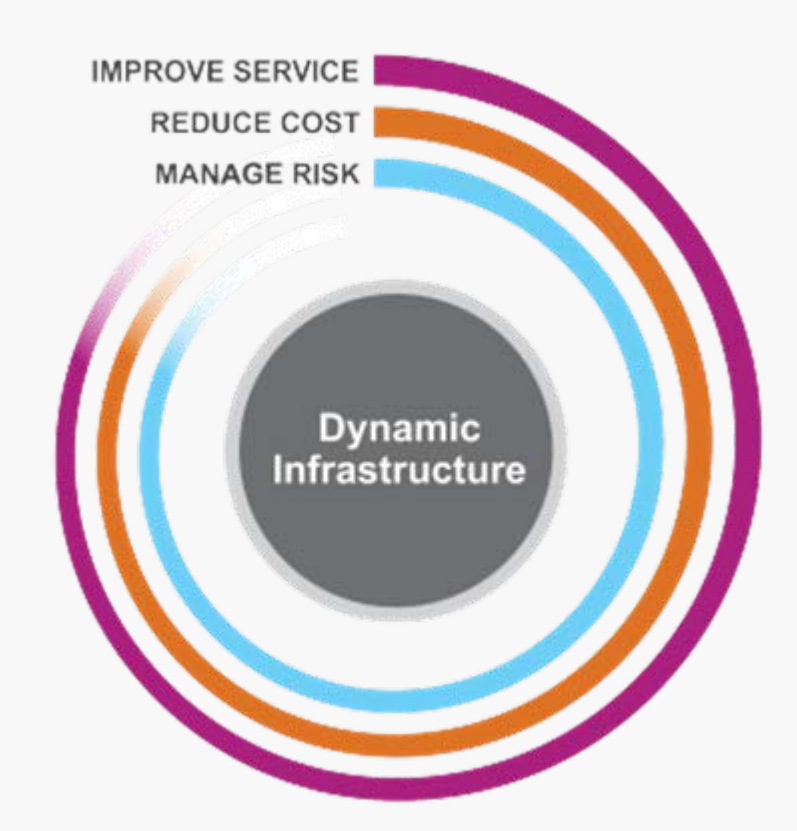
IBM Web application security for a smarter planet delivers client value

- **Integrated end-to-end Web protection**
  - Drive security into the software development life cycle
  - Malware detection and vulnerability management
  - Realtime blocking of attacks
  - Security and performance for SOA environments
- **Secure the data and integrity of Web-enabled business process**
  - Online payments
  - Trusted transactions between business partners
  - Databases
- **Meet compliance demands**
  - Achieve PCI compliance for DSS 6.6 (June 30 2008)

Why Customers Choose IBM Rational Security & Compliance

- ✓ **Broadest suite of offerings to support security testing across the development lifecycle**
- ✓ **Only web application security testing solution that provides combined static and dynamic analysis**
- ✓ **Integrated with Rational application lifecycle management portfolio allowing security to become a natural part of the software development process**
  - Minimize disruption
  - Scale to large number of users
  - Support collaboration within development
  - Integrate with development tools
- ✓ **R&D backed by IBM's $1.5B annual investment in security**
- ✓ **Comprehensive Application Security Analysis - Includes multiple analysis techniques to leverage strengths of many solutions**

Secure Web applications deliver the Dynamic Infrastructure of a smarter plant



- **Improve Service**
  - Availability and uptime
- **Reduce Cost**
  - Managed services that reduce cost and complexity of security operations
- **Manage Risk**
  - End-to-end approach to Web application security

Conclusion: Application QA for Security

- **The Application Must Defend Itself**
  - You cannot depend on firewall or infrastructure security to do so
- **Bridging the GAP between Software development and Information Security**
- **QA Testing for Security must now be integrated and strategic**
- **We need to move security QA testing back to earlier in the SDLC**
  - at production or pre-production stage is late and expensive to fix
  - Developers need to learn to write code defensively and securely

Lower Compliance & Security Costs by:

- **Ensuring Security Quality in the Application up front**
- **Not having to do a lot of rework after production**

Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at http://www.ibm.com/legal/copytrade.shtml.