




# PCTY2011



Pulse Comes to You

**Optimising the World's Infrastructure**



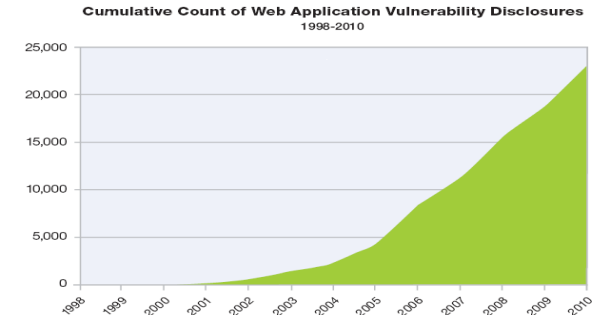
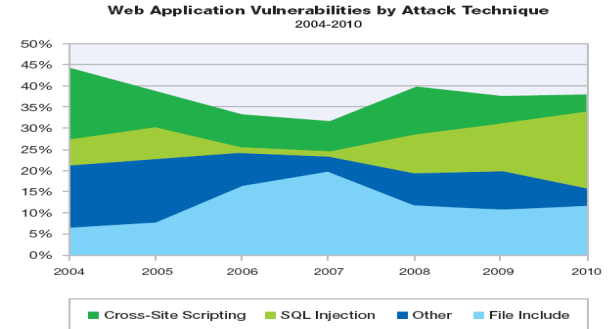
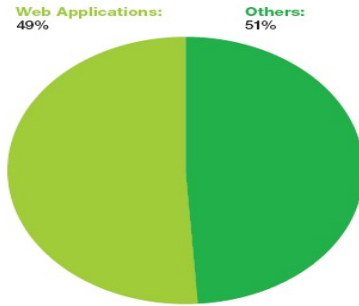
# Application vulnerabilities - and the virtual patch

Gareth O Sullivan  
IBM Rational Security Tech Sales Lead EMEA

# Web App Vulnerabilities Continue to Dominate

- Nearly half (**49%**) of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting & SQL injection vulnerabilities continue to dominate.

Web Application Vulnerabilities  
as a Percentage of All Disclosures in 2010



# The Costs from Security Breaches are Staggering

**285 MILLION RECORDS  
COMPROMISED IN 2008**

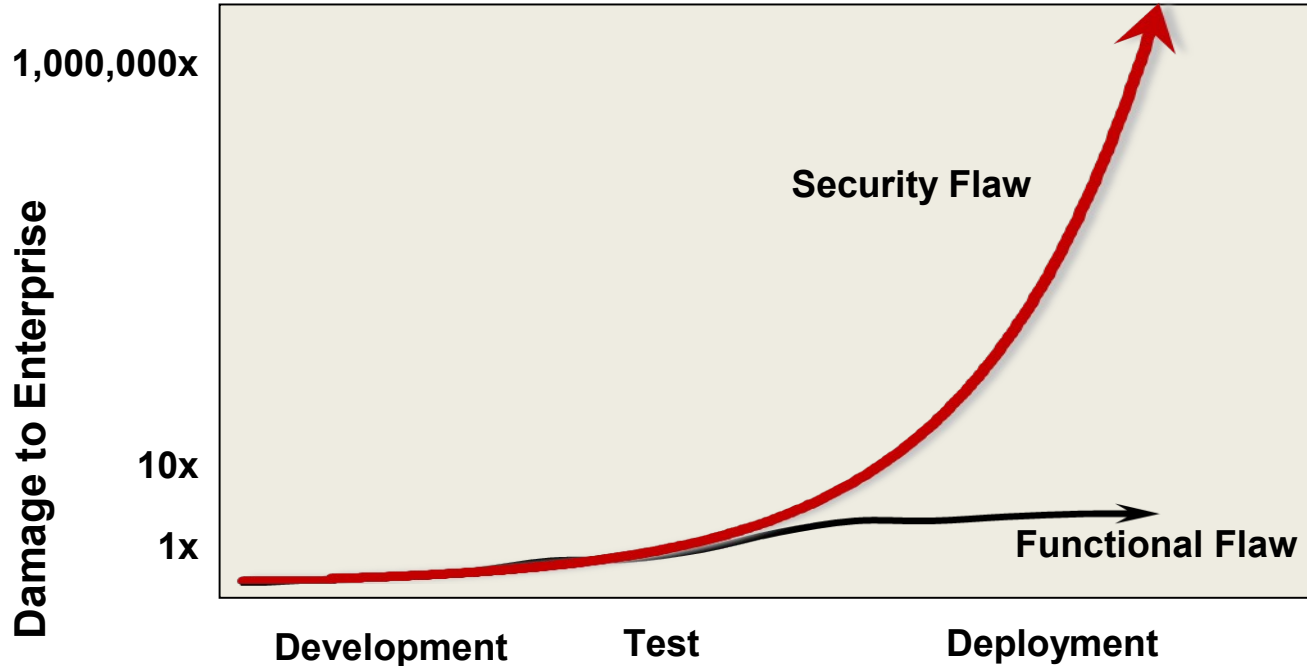
Verizon 2009 data  
Breach  
Investigations  
Report

**\$204 COST PER  
COMPROMISED  
RECORD**

Ponemon 2009-  
2010 Cost of a data  
Breach Report

**TRANSLATES TO \$58.1B  
COST TO CORPORATIONS**

# Sources of Security Breach Costs



## Unbudgeted Costs:

- Customer notification / care
- Government fines
- Litigation
- Reputational damage
- Brand erosion
- Cost to repair

# More Justification for Application Security Action

99.9% of records were compromised from servers and applications

81% of organizations subject to PCI had not been found compliant prior to the breach

79% of compromised records were compromised using Web applications as the attack pathway



Verizon 2009 data Breach  
Investigations Report

## Action:

- Adopt application security measures
- Address compliance mandates with industry regulations (such as PCI-DSS, GLBA, HIPAA, FISMA, NERC, etc)

# Why are Web Applications so Vulnerable?

- Developers are mandated to deliver functionality on-time and on-budget - but not to develop secure applications
- Developers are not generally educated in secure code practices
- Product innovation is driving development of increasingly complicated software for a Smarter Planet
- Network scanners won't find application vulnerabilities and firewalls/IPS don't block application attacks



**Volumes of applications continue to be deployed that are riddled with security flaws...**

**...and are non compliant with industry regulations**

# Pre-empt Costly Risk Mitigation – Become Secure, by Design

## Customer Speak!

Reduce today's **most significant area** of risk by **adopting a cost effective** and thorough application security program



*"We have more of our business supported by our web presence – we can't afford the business risk of deploying unsecured applications and services"*

Embed security early into the software delivery process to **enable on time and on budget delivery** of secure applications



*"Embracing security in development allowed us to get ahead of schedule disruption and increased costs from security acceptance testing"*

Establish a security blueprint to **create and maintain security governance, manage risk and ensure compliance**



*"IBM has recognized this trend and has created comprehensive security packages that leverage various products to provide for multiple layers of security to customers"*



# Make Applications Secure, by Design

## Design Phase

- Consideration is given to security requirements of the application
- Issues such as required controls and best practices are documented on par with functional requirements

## Development Phase

- Software is checked during coding for:
  - Implementation error vulnerabilities
  - Compliance with security requirements

## Build & Test Phase

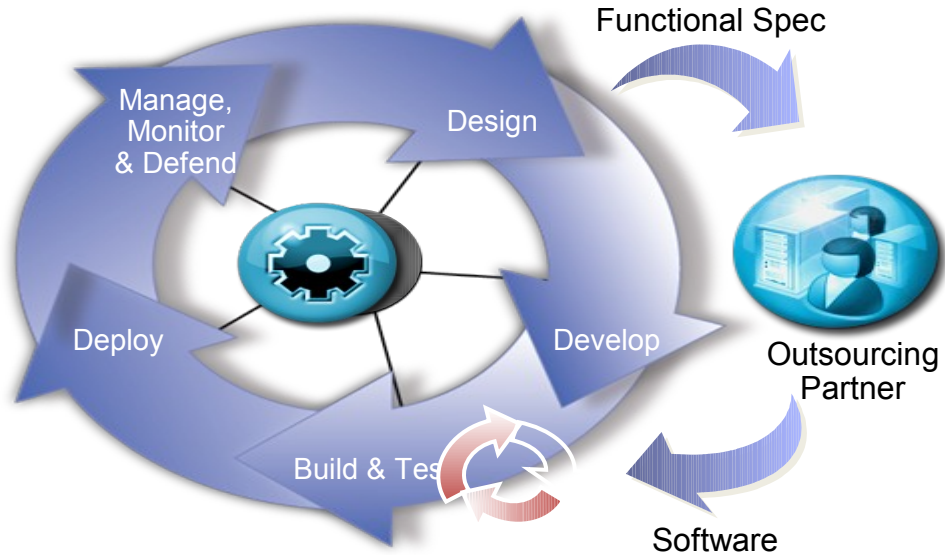
- Testing begins for errors and compliance with security requirements across the entire application
- Applications are also tested for exploitability in deployment scenario

## Deployment Phase

- Configure infrastructure for application policies
- Deploy applications into production

## Operational Phase

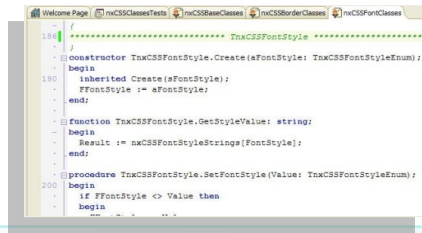
- Continuously monitor applications for appropriate application usage, vulnerabilities and defend against attacks



# Security Testing Technologies... Combination Drives Greater Solution

## Static Code Analysis (Whitebox )

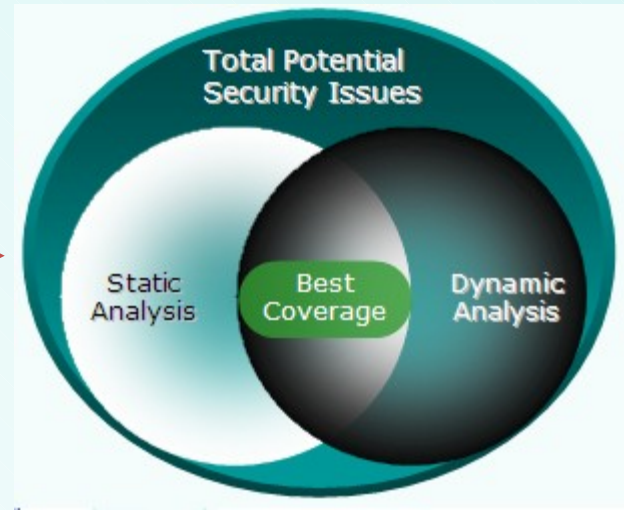
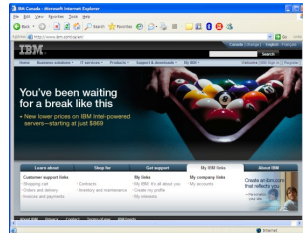
- Scanning source code for security issues



```
184 /
185 }
186
187 constructor TxmCSSFontStyle.Create(aFontStyle: TxmCSSFontStyleEnum);
188 begin
189     inherited Create(aFontStyle);
190     FFontStyle := aFontStyle;
191 end;
192
193 function TxmCSSFontStyle.GetStyleValue: string;
194 begin
195     Result := mxCSSFontStyleStrings[FontStyle];
196 end;
197
198 procedure TxmCSSFontStyle.SetFontStyle(Value: TxmCSSFontStyleEnum);
199 begin
200     begin
201         if FFontStyle <> Value then
202             begin
```

## Dynamic Analysis (Blackbox)

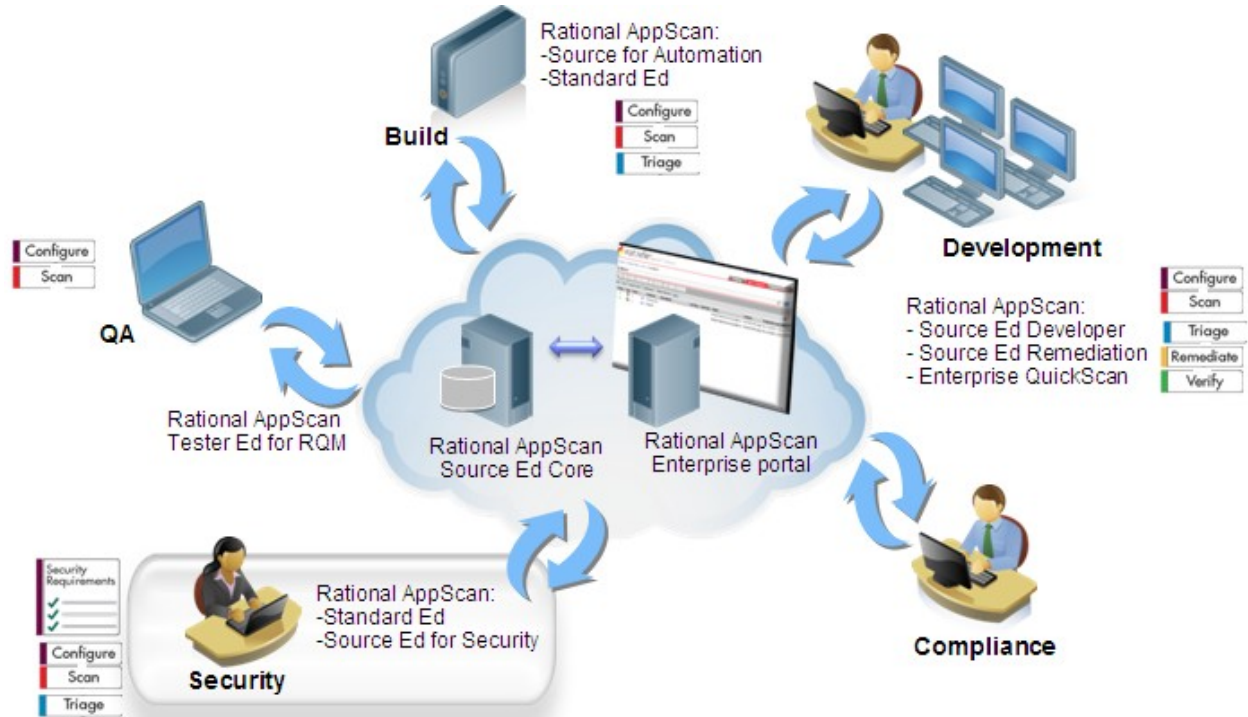
- Performing security analysis of a compiled application



# Application security scanning

Functions:

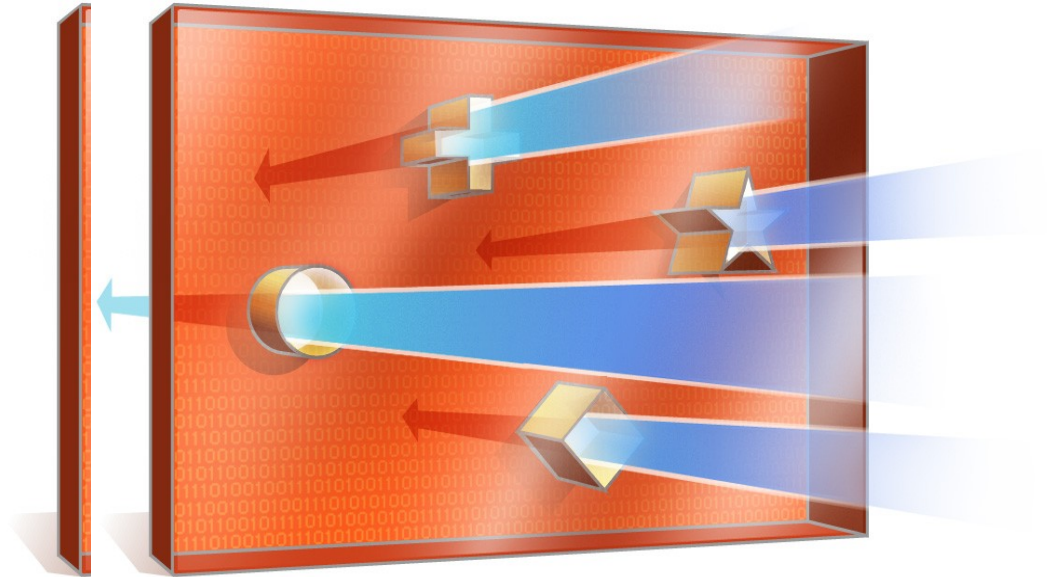
- Security Requirements
- Configure
- Scan
- Triage
- Remediate
- Verify





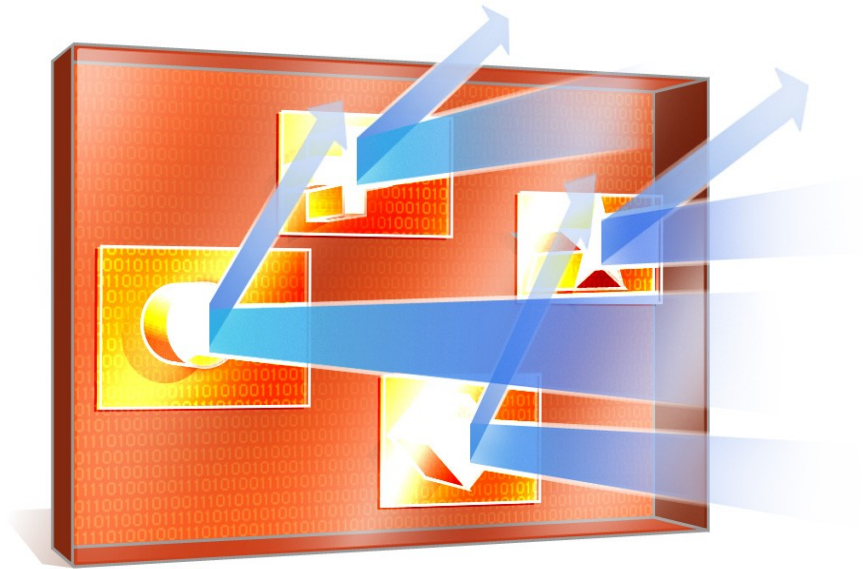
# All Threats Exploit Some Vulnerability

Internet threats take advantage of a vulnerability in the Operating system, application or network infrastructure

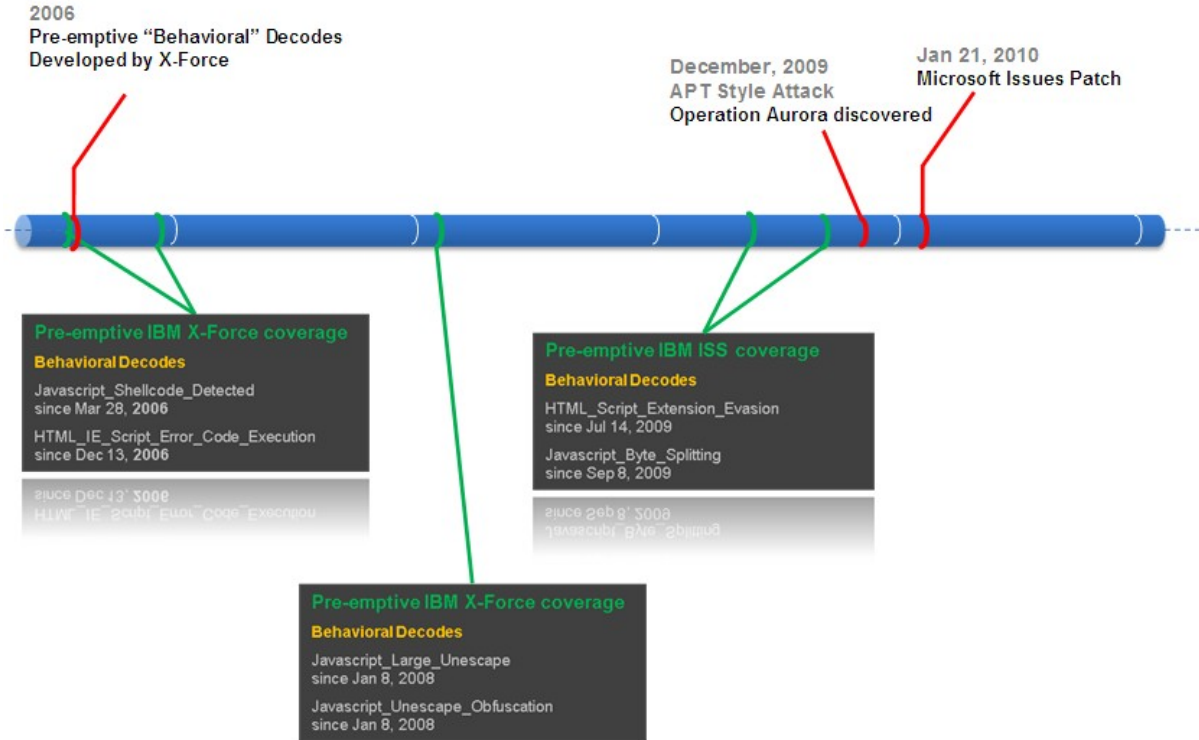


# Preemptive security works by providing a temporary shield or “**virtual patch**” for known vulnerabilities

- Provides 0-day protection by preventing the vulnerability from being exploited
- Blocks all variations of the threat
- Doesn't rely on “signatures”
- Eliminates emergency patching
- Removes the risk that a patch will break something
- Enables patches to be applied during normal maintenance windows



# Ahead of the Threat: Operation Aurora



# Application development meets service management

## Build Secure Web Applications

- Secure code development
- Identify vulnerabilities and malware
- Actionable information to correct the problems

## Protect Web applications from potential attacks

- Block attacks that aim to exploit Web application vulnerabilities
- Integrate Web application security with existing network infrastructure

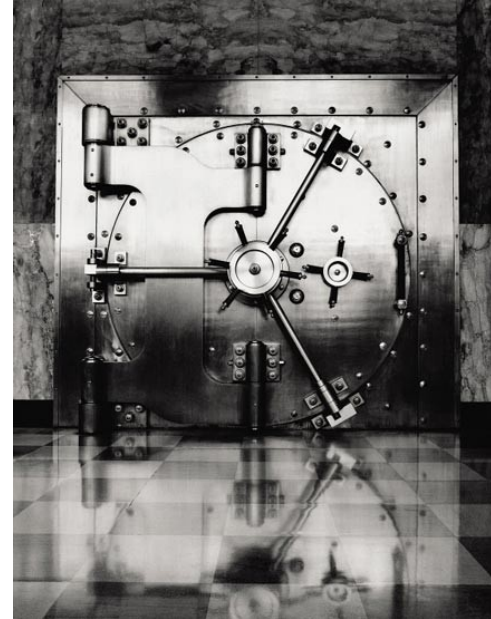
## Manage Secure Web Applications

- Single management console for vulnerabilities, events and blocking policies



# Managing secure web applications

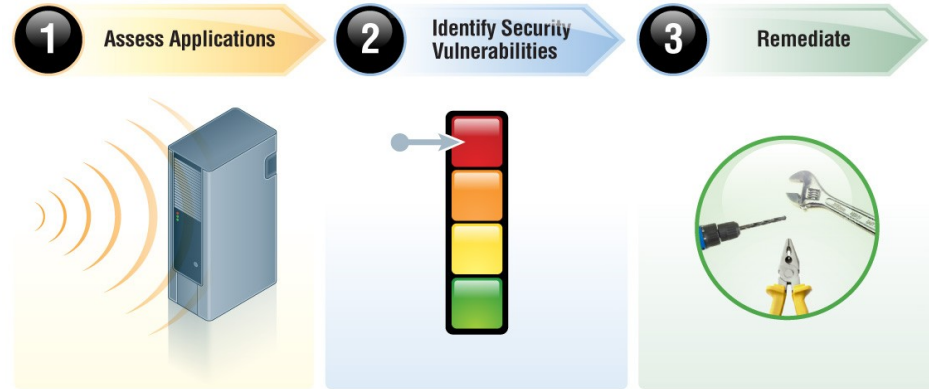
- Drive intelligent security with integrated single console for AppScan and Proventia IPS
- Centrally manage vulnerabilities, IPS blocking/alerting policies and security events from a single dashboard
- Correlate vulnerabilities with security events & attacks blocked
- Consolidate reporting for compliance requirements and improved management
- Build and apply security policies to block threats specific to your vulnerabilities





# Summary

- Reduce costs
- Decrease risk
- Speed time to market for applications
- Automate manual tasks



# Q&A



## X-Force Trend Reports

The IBM X-Force Trend & Risk Reports provide statistical information about all aspects of threats that affect Internet security. Find out more at <http://www-935.ibm.com/services/us/iss/xforce/trendreports/>



Thank  
You