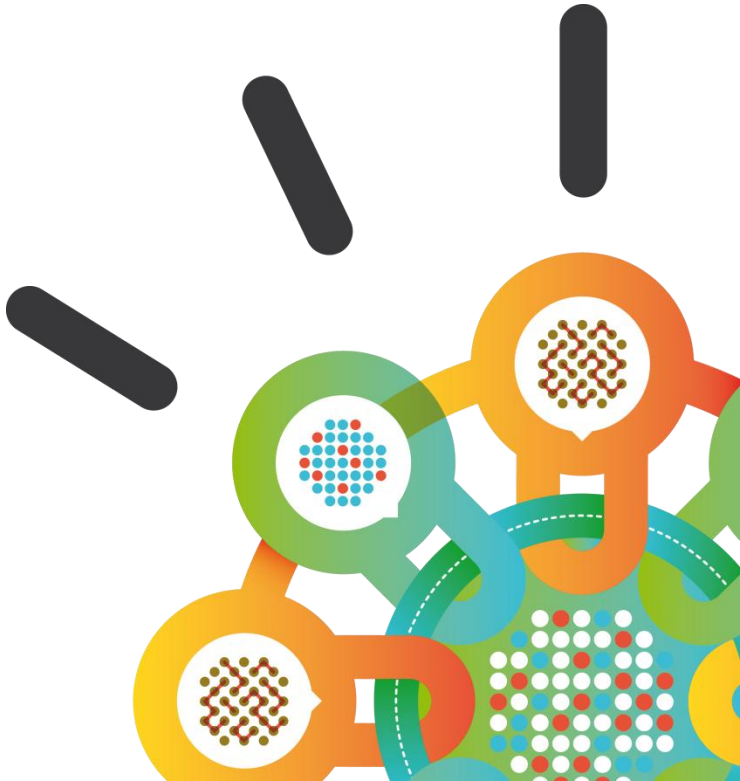
IBM Security Systems

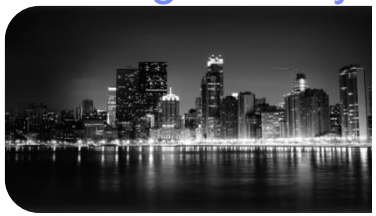
IBM Security - Application Security



Faustino Sanchez.
Application Security Sales Enablement
sanchezf@ca.ibm.com

The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks…

…making security a top concern, **from the boardroom down**



EVERYTHING IS EVERYWHERE

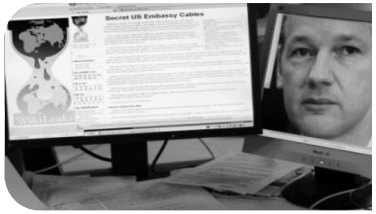
Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more

CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

DATA EXPLOSION

The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere



ATTACK SOPHISTICATION

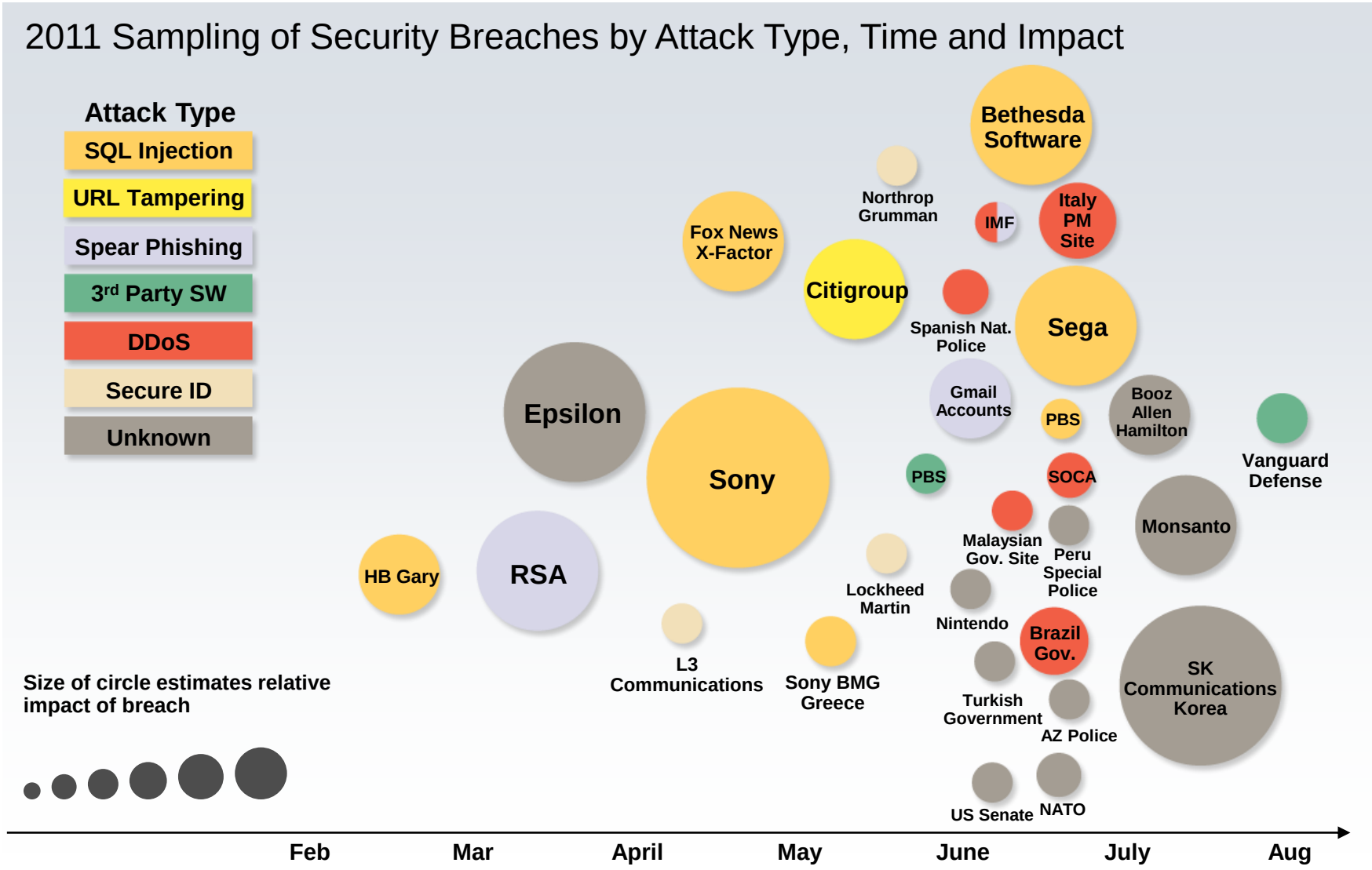
The speed and dexterity of attacks has increased coupled with new motivations from cyber crime to state sponsored to terror inspired

“Chinese hackers attack US Chamber of Commerce”

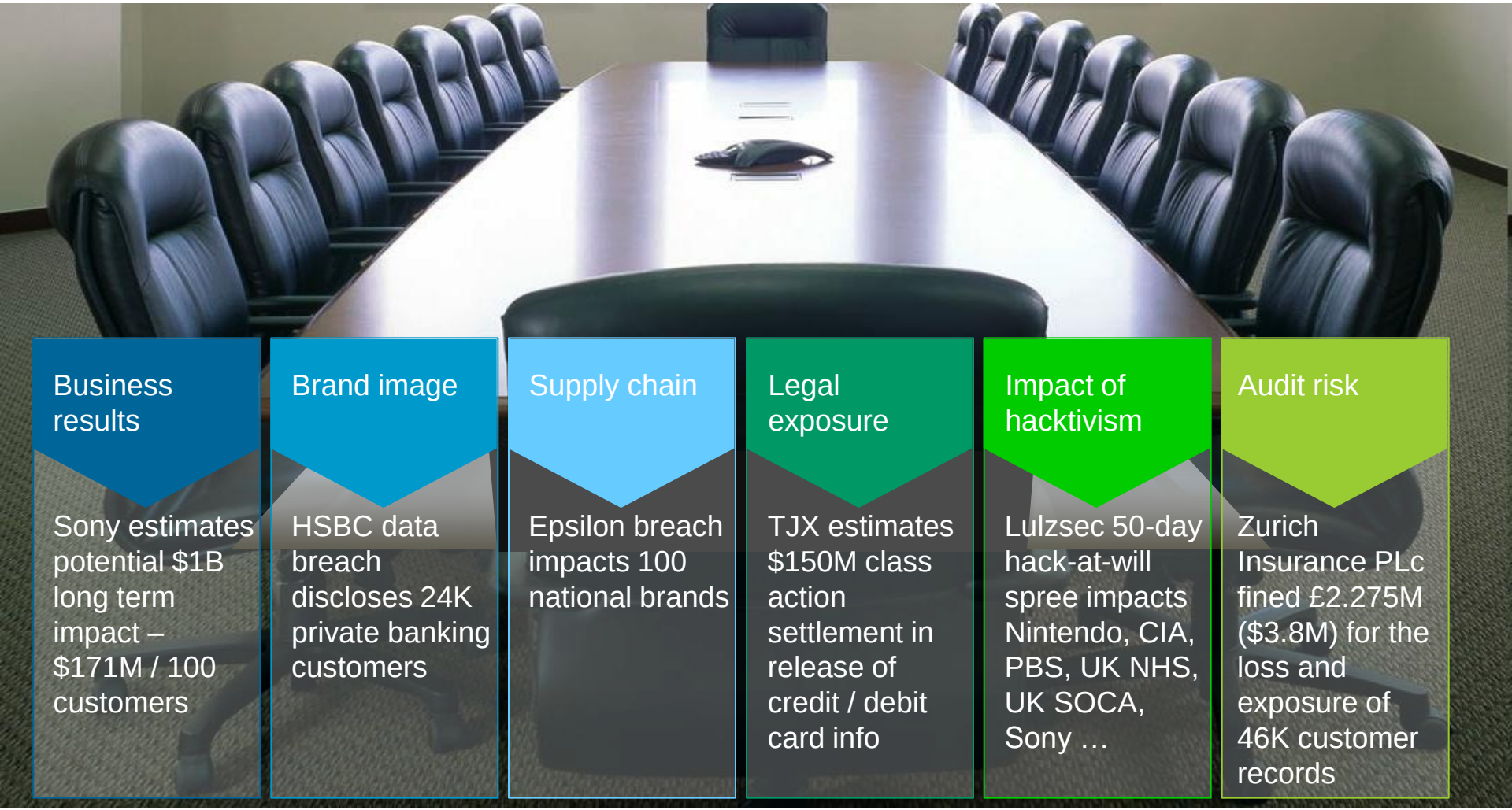
Hacktivism

Hackers Breach the Web Site of ***Stratfor Global Intelligence*** **Hackers affiliated with the Anonymous group said they are getting ready to publish emails stolen from private intelligence analysis firm Strategic Forecasting Inc, whose clients include the U.S. military, Wall Street banks and other corporations.**

Market Change 1 (cont.): Security breaches in the past 6 months



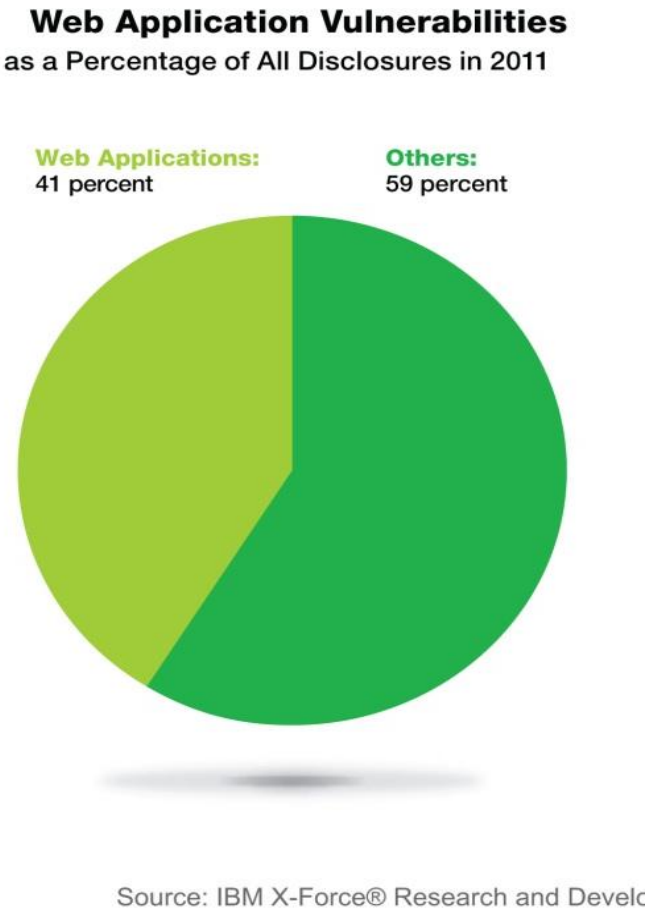
The Result: Security is becoming a board room discussion



Can this happen to us?

Manage Risks and Compliance/Governance

- 55% of respondents cited mobile security as a primary technology concern over the next two years. (IBM Center for Applied Insights)
- 76% of CEOs (Ponemo 2010) feel reducing security flaws within business-critical applications is the most important aspect of their data protection programs.
- 41% of all vulnerabilities are Web application vulnerabilities.
  (X-Force 2011)
- Cross-Site Scripting & SQL injection vulnerabilities dominate OWASP Top 10.
- 89% of records breached from hacks were related to SQL Injection flaws
- 81% of breached organizations subject to PCI were found to be non-compliant (Verizon)
- 79% of compromised records used Web Apps as the attack pathway Verizon



Market Drivers

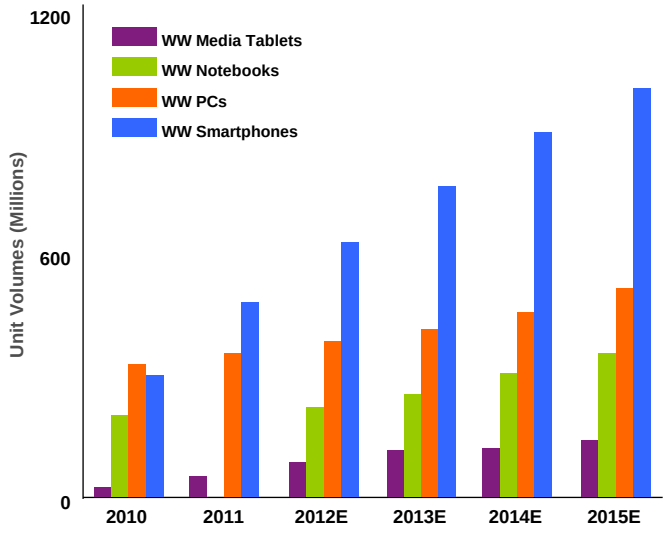
- **Regulatory & Standards Compliance**
  - eCommerce: PCI-DSS, PA-DSS
  - Financial Services: GLBA
  - Energy: NERC / FERC
  - Government: FISMA
- **User demand**
  - Rich application demand is pushing development to advanced code techniques – Web 2.0 introducing more exposures
- 81% of organizations subject to PCI had not been found compliant prior to the breach

Hackers Break Into Virginia Health Website, Demand Ransom
— Washington Post, May, 2010

Cyber Blitz Hits U.S., Korea Websites –WSJ
July 9th, 2010

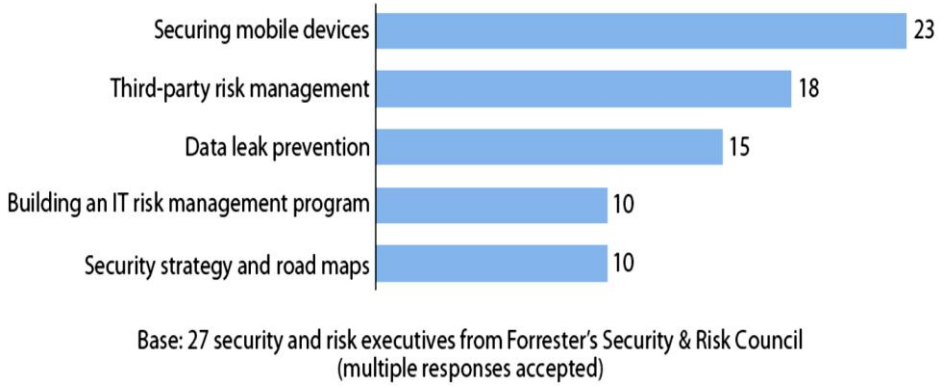
"Web-based malware up 400%, 68% hosted on legitimate sites"
— ZDnet, June 2010

Mobile Security: Organizations are rapidly embracing mobile devices and applications, leading to new security challenges



Source: *"Fostering the People: The Shift to Engagement Apps"*, Wells Fargo Securities, January 23, 2012

Select five of the *top challenges* you will face over the next six months:



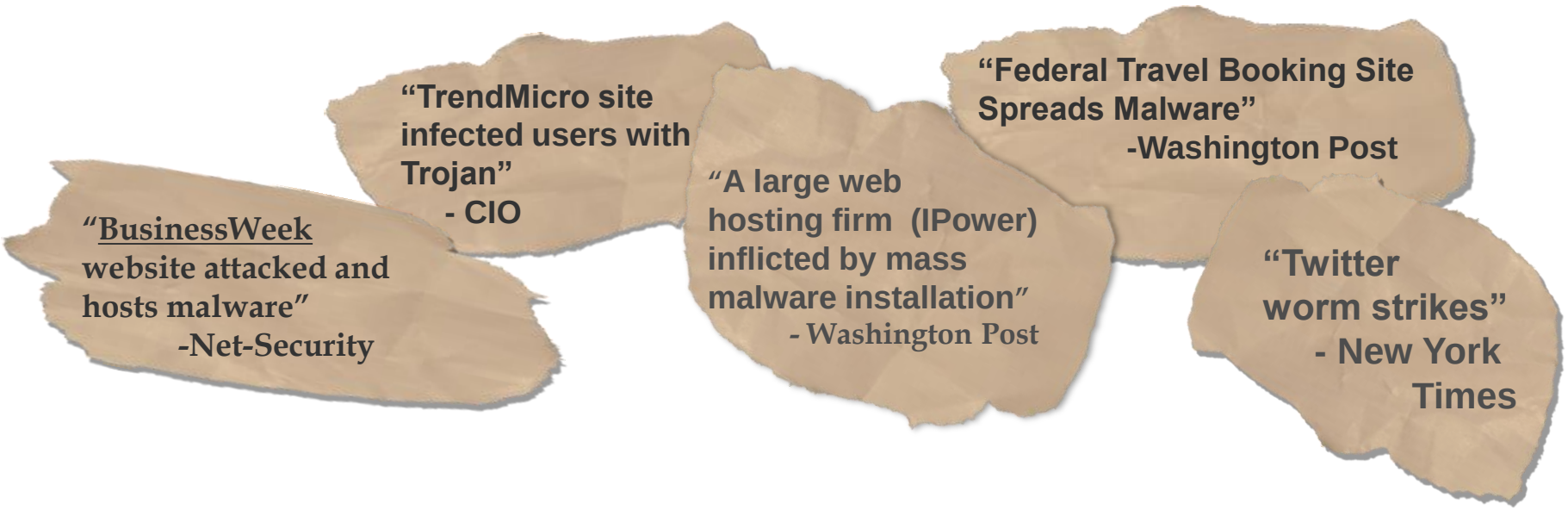
Base: 27 security and risk executives from Forrester's Security & Risk Council (multiple responses accepted)

Source: *"Executive Spotlight: Top Priorities for Security and Risk Leaders, 1H 2011"*, Forrester, April 2011

Mobile application security is top of mind for customers

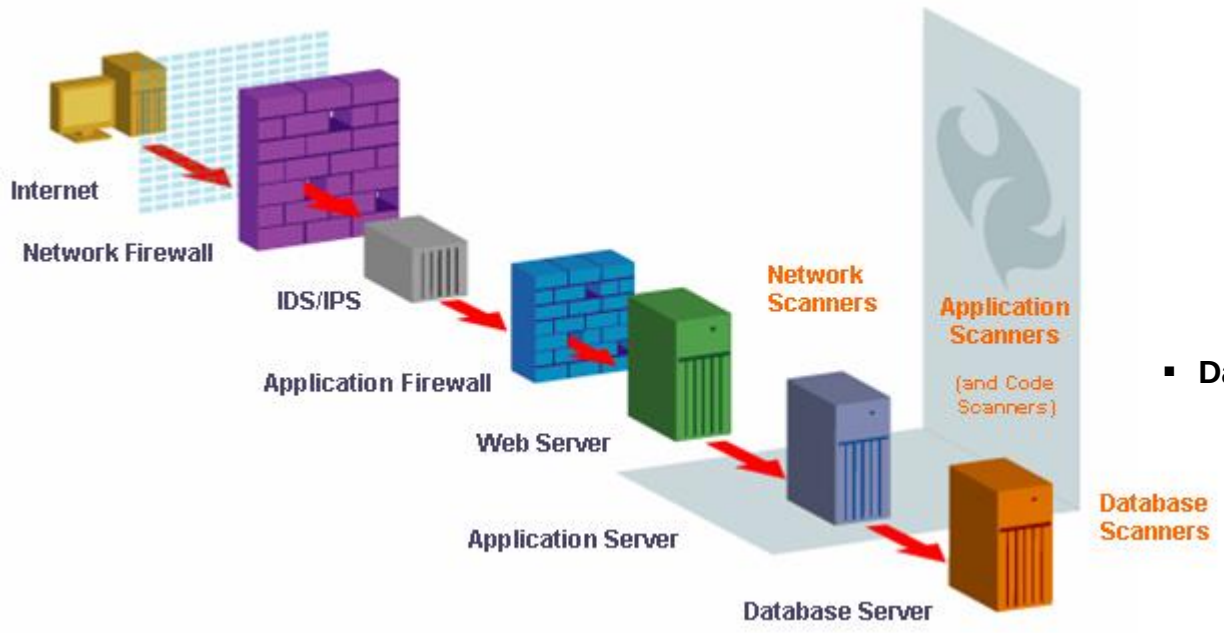
The Problem: Legitimate Sites serving Malware

- Malware is served or linked primarily from **Legitimate Sites!**



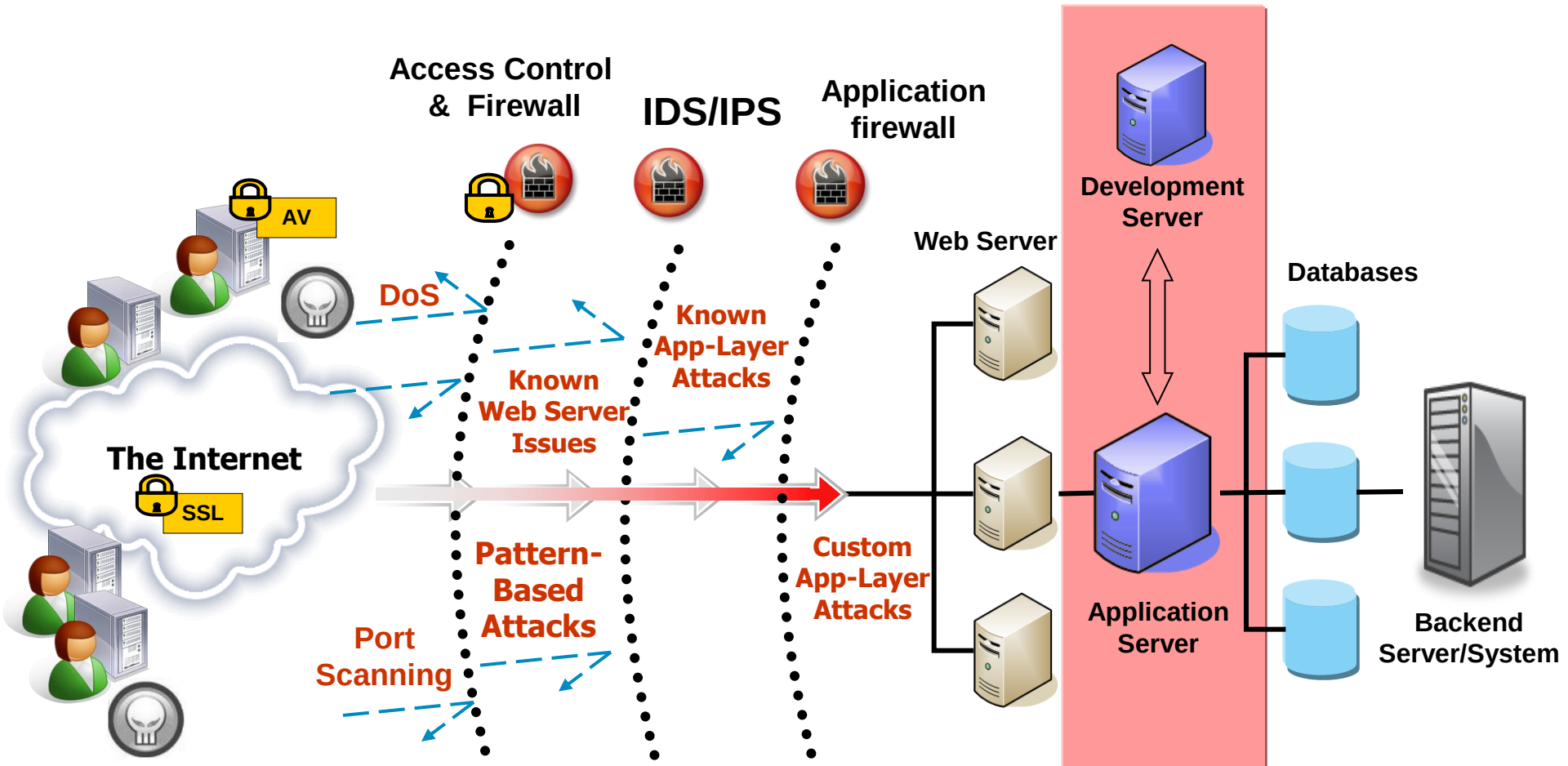
Security Landscape – Distinguishing Technologies

- **Network Firewalls**:
  - Perimeter protection mechanisms to block traffic in real-time.
  - But websites have to be publicly available, thus port 80 and port 443 are enabled for access which makes Network Firewalls incapable of blocking application-layer attacks
- **Intrusion Detection / Prevention Systems (IDS / IPS)**
  - Also considered a perimeter protection mechanism. They monitor data flow through the network in real-time.
  - They are incapable of blocking application-layer attacks since they are not application-aware operating at the network level

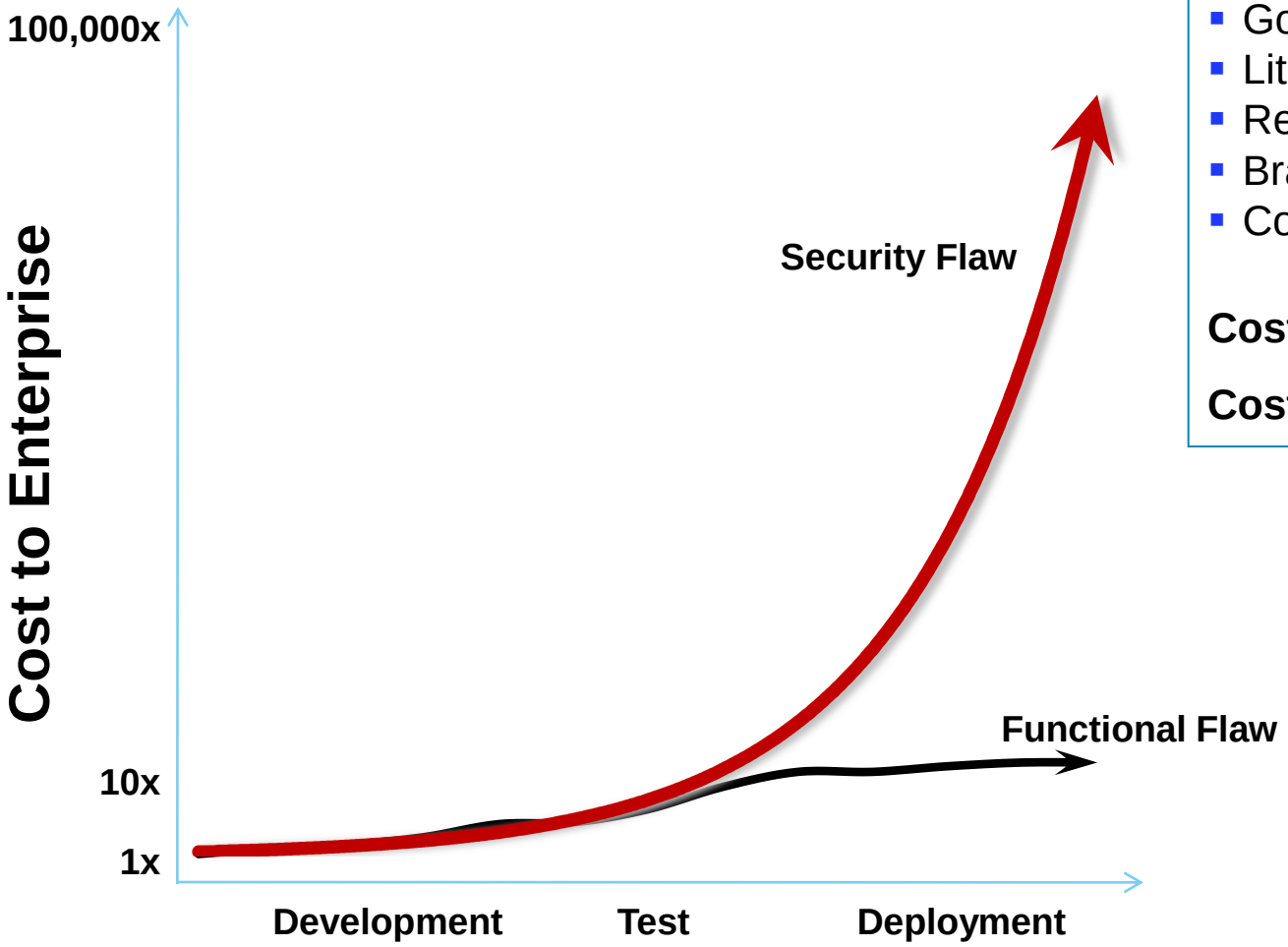


- **Application Firewalls**:
  - Perimeter protection and are generally very effective, but difficult to configure and maintain (every time an application changes the firewall needs to be reconfigured).
  - They can also reduce website response time and lead to lost revenue
  - Some percentage of “good” traffic is inadvertently blocked too
- **Network Scanners**
  - Conceptually similar to AppScan - both are vulnerability assessors.
  - However, they assess very different pieces of the IT environment
  - Network Scanners are unaware & incapable of interacting with the application layer so no matter how secure an organization makes their network, they would still be vulnerable to application-level attacks
- **Database Scanners**
  - Do not scan or test web applications
  - They focus solely on how well information is protected within the database itself

Why Web Application Scans?



Sources of incremental security breach costs



Unbudgeted Costs:

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

Cost per Record: $214*

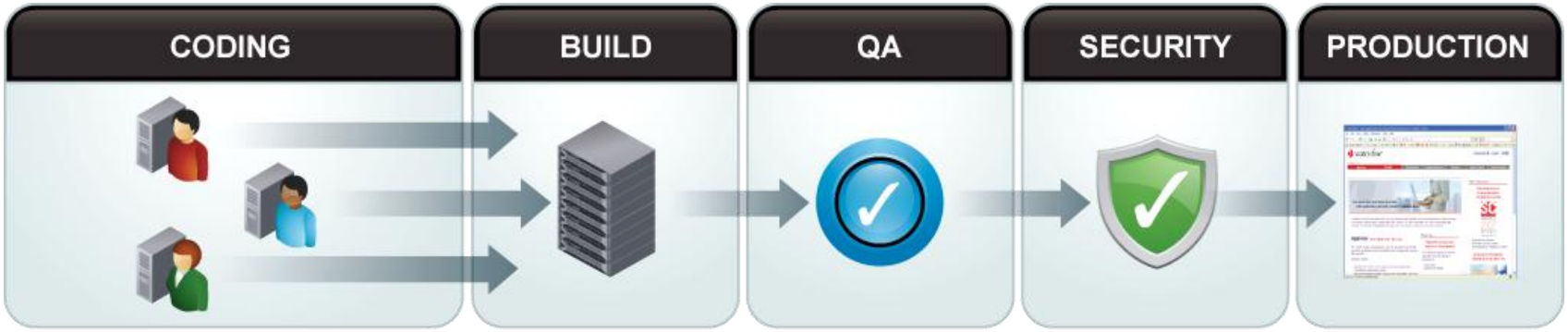
Cost per Breach: $7.2M*

* Source: Ponemon Institute 2011

Reducing Costs Through a Secure by Design Approach

*80% of development costs are spent identifying and correcting defects!****

*Average Cost of a Data Breach $7.2M** from law suits, loss of customer trust, damage to brand*



Find during Development	Find during Build	Find during QA/Test	Find in Production
$80 / defect	$240 / defect	$960 / defect	$7,600 / defect
*$8,000 / application	*$24,000 / application	*$96,000 / application	*$760,000 / application

*Based on X-Force analysis of 100 vulnerabilities per application

*** Source: National Institute of Standards and Technology

** Source: Ponemon Institute 2009-10

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

Summary of Market Drivers

- **Manage Risk**
- **Compliance/Governance**

- **Reducing Costs**

Application Security: Buyers and use cases

Penetration Testing

- **Buyers:** Security consultants, Small Security Teams & Security Auditors
- **Use cases:** need desktop solution with both advanced testing and ease of use
- **Estimated Market size/growth:** $100M-$130M / 10-12% with commoditization & price pressure from low-end vendors

Vulnerability Management

- **Buyers:** Enterprise Security Teams
- **Use cases:** Client has an AppSec team to manage application risk
- **Estimated Market size/growth:** $70M / 8-10%

Application Development

- **Buyers:** Security (development is a user and influencer)
- **Use cases:** Client security team convinced development execs to include security testing in 1 or more phases of SDLC: Code, Build, QA/Test, Pre-production security test
- **Estimated Market size/growth:** $100M / 20-22%

Customer Profiles

Industries

All but priority industries include:
- Banking
- Financial Markets
- Government
- Retail (eTailer)
- Healthcare
- Insurance
- Application Dev shops
- Manufacturing
- Energy (new energy)

We see customer spread out in all industries as they all have one common pain: **How to secure their applications?**

Target Audience

Roles: CIO, CSO, IT-Security Managers, Penetration Tester, Security Auditor, Development Managers

- Leverage IBM Account Team to understand who the players and contacts are, and to elevate the visibility to CIO/CSO
- IT Executive may drive project as they have authority and hold the budget
- Source Edition buyer can be IT Security, but to successful close the deal the involvement by developers is key

Customer Segmentation

Entry points and deal size:

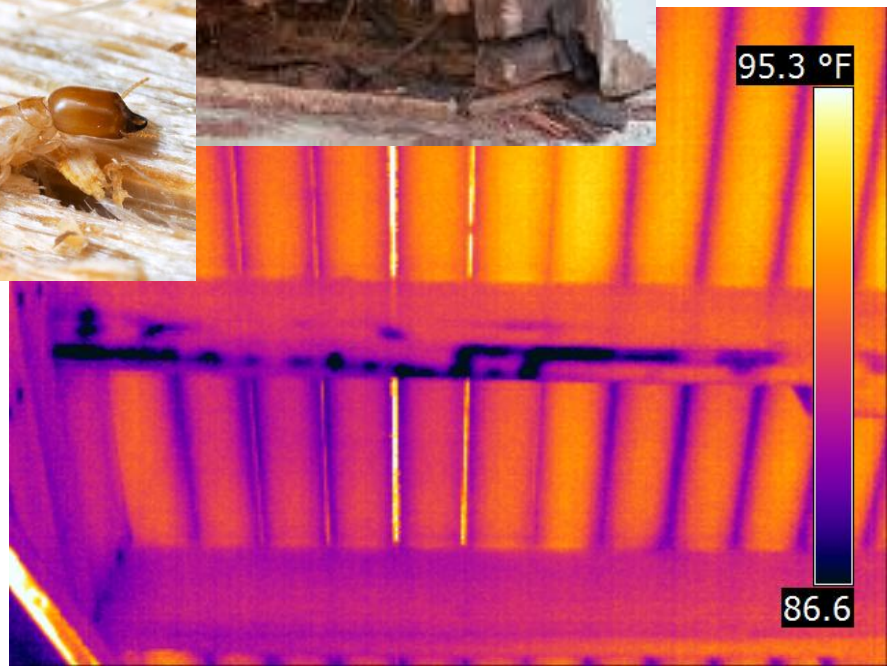
Small/Medium business:
- AppScan Standard: $19,000-$35,000

Enterprise customer:
- AppScan Enterprise: $200,000
- AppScan Source: $80,000-$300,000

- Biggest opportunity within enterprise account based on sophisticated technology and risk and compliances those customers encounter
- Customers who will purchase a large enterprise deal are still the early adopters
- Mainstream customers will buy single seats of AppScan Standard on an ad-hoc basis

Sales Cycle is like a termite inspection

1. Visible damage
2. Imposed Inspection (Regulations)
3. Proactive



Understanding Your Environment

The key to opportunity identifications is understanding your environment.

- Application profile
- Current security process
- Compliance/security requirements
- Infrastructure, Process, and Finding Blindspots

Understanding Your Environment - Application Profile

Development
- Internal and outsourced development
- Off the shelf-software
- Open Source

Deployment
- Internal & Externally Deployed Applications
- 3rd partying Hosting
- Products developed to be sold

Supply Chain
- Off the shelf software
- Third party developed applications
- Integrated products

Application Type
- Web application
- Desktop
- Mainframe
- Web Services
- Mobile
- Etc..

Understanding Your Environment - Application Profile

What kind of data does your customer have?

- Credit Card
- Personally Identifiable information (PII)
- Health information
- Social security or identify card numbers
- Intellectual Property
- Trade Secrets
- Customer information

What compliance requirements does your customer have and how do they address application security concerns?

- Payment Card Industry (PII)
- HIPAA
- NIST

Additional Questions

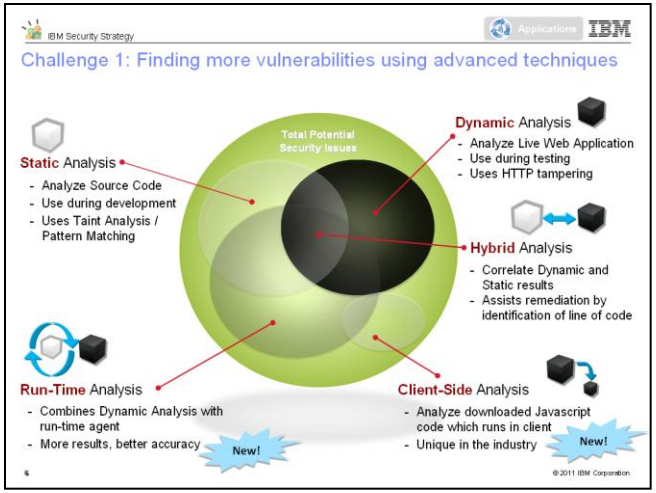
- What industries does your client belong to or sell to?
- Do they have compliance concerns?
- Even if your application does not house this data, could it be hosted in an environment that does?

Understanding Your Environment - Process

What is your client's current process for security testing?

- Customer Indicates one of the following:
  - We use Source code scanning
    or
  - We use Dynamic Analysis

We will discuss the technologies further later in the presentation, however it's important to state, that in terms of vulnerabilities, there are issues that one technology is very proficient at, but the other technology may be more proficient at locating other types of vulnerabilities. Educate the customer.



Understanding Your Environment - Process

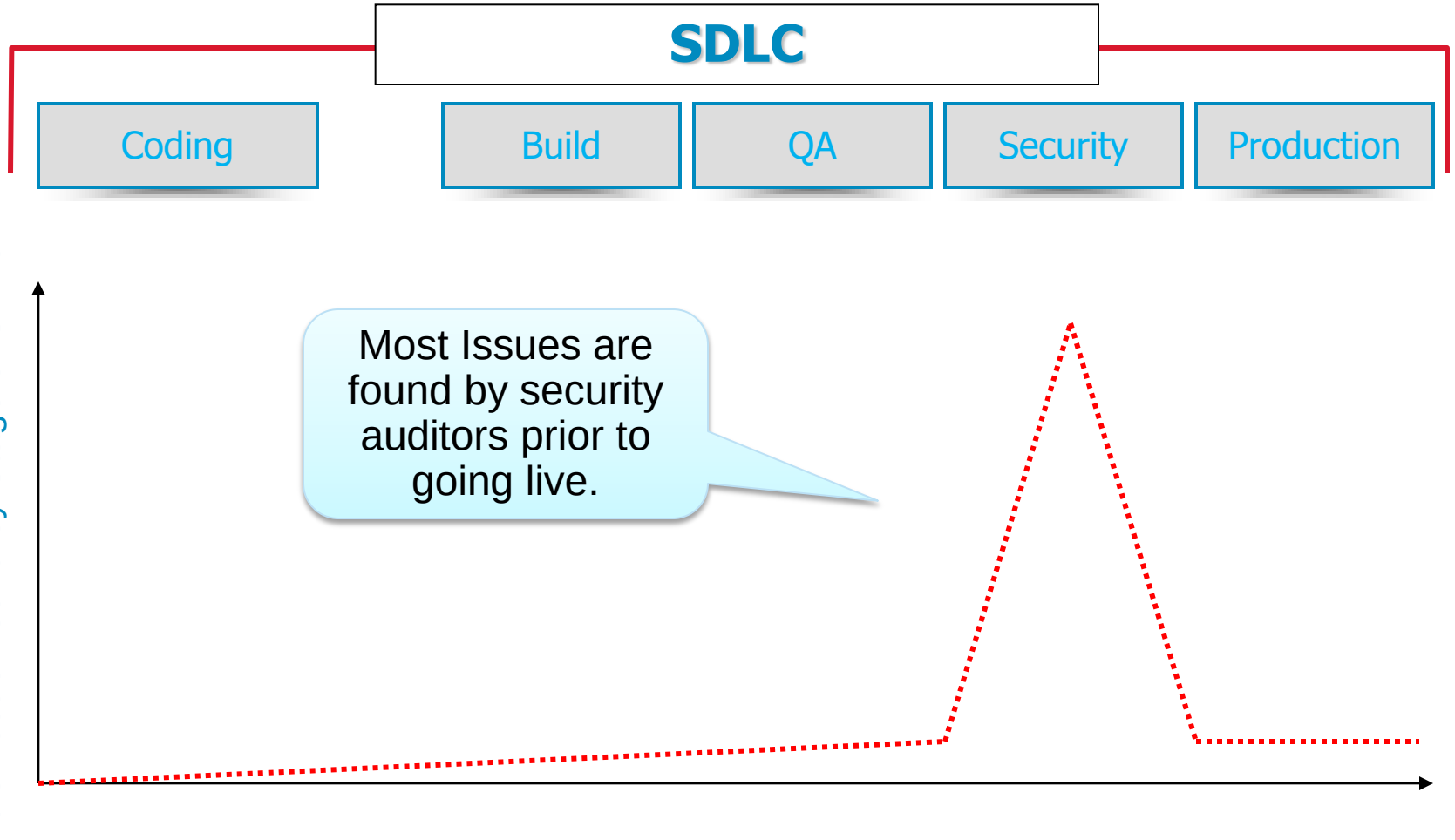
What is your client's current process?

- "Gating Process"
  - Customer tests just prior to deployment. Security team scans the application and determines if it will be deployed or not based on scan results, and possibly some manual testing.

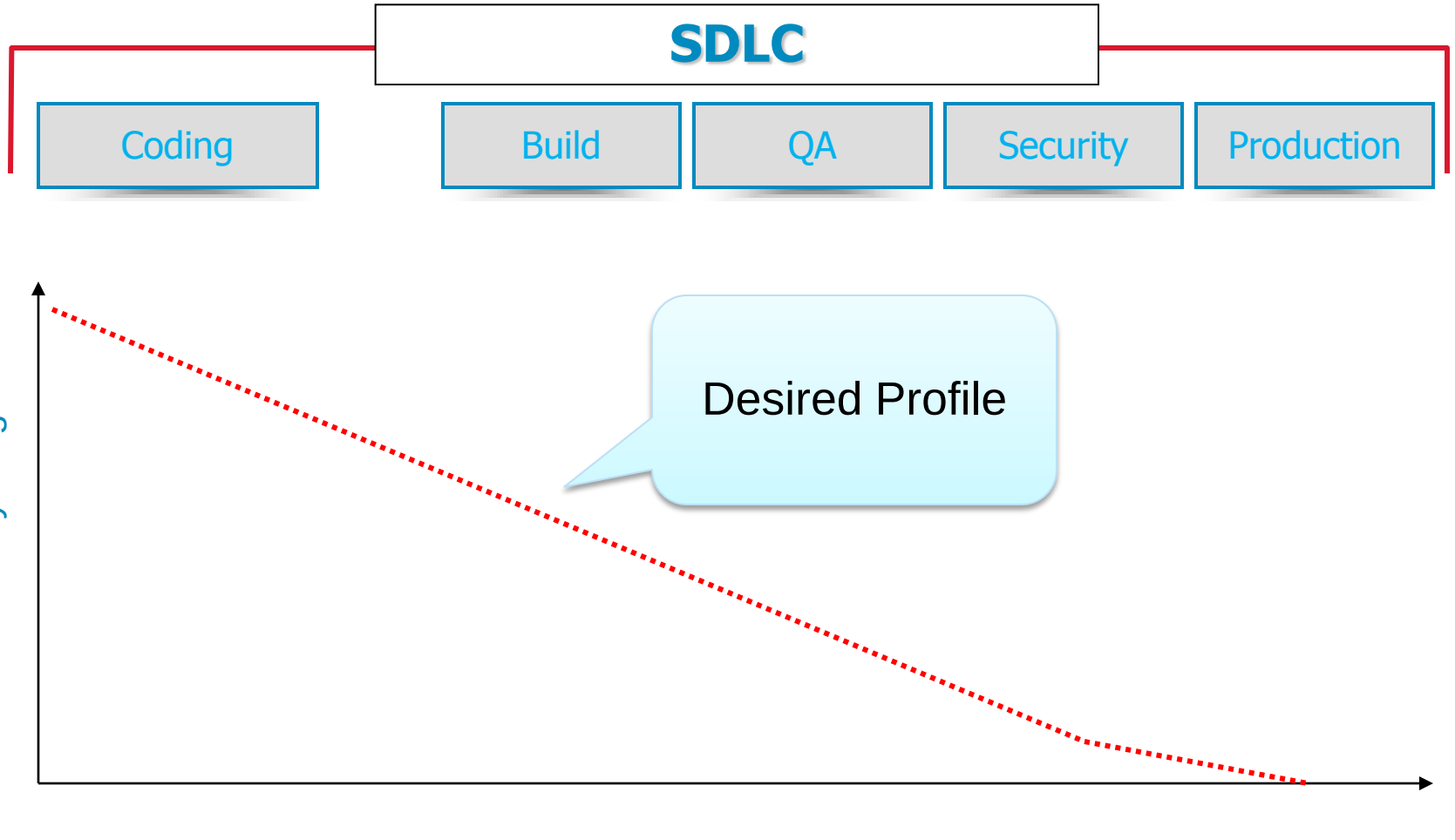
This is critical part of the process, however, if this is all the customer is doing, it is inefficient, and can incur huge costs, and some businesses will still deploy an application because of the late stage findings. Embedding security testing in the development process will ensure finding the vulnerabilities earlier, for quicker remediation, and, according to NIST and other studies, significant cost savings can be realized

Find during Development	Find during Build	Find during QA/Test	Find in Production
$80/defect	$240/defect	$960/defect	$7,600 / defect

Security Testing Within the Software Lifecycle



Security Testing Within the Software Lifecycle



Make Applications Secure, by Design

Cycle of secure application development

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

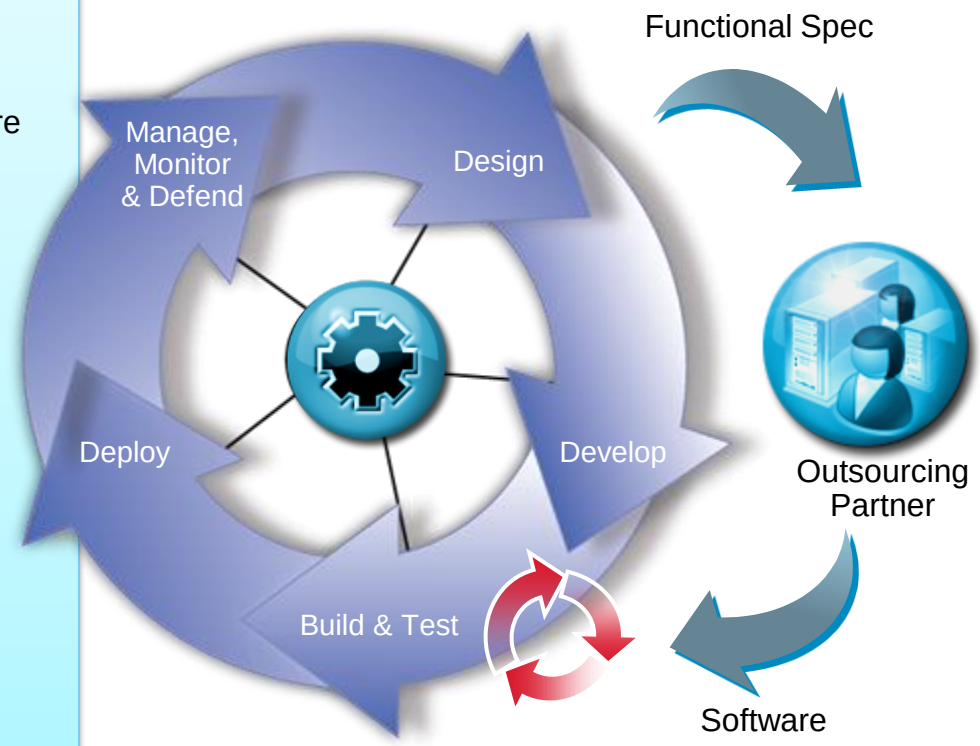
- Testing begins for errors and compliance with security requirements across the entire application
- Applications are also tested for exploitability in deployment scenario

Deployment Phase

- Configure infrastructure for application policies
- Deploy applications into production

Operational Phase

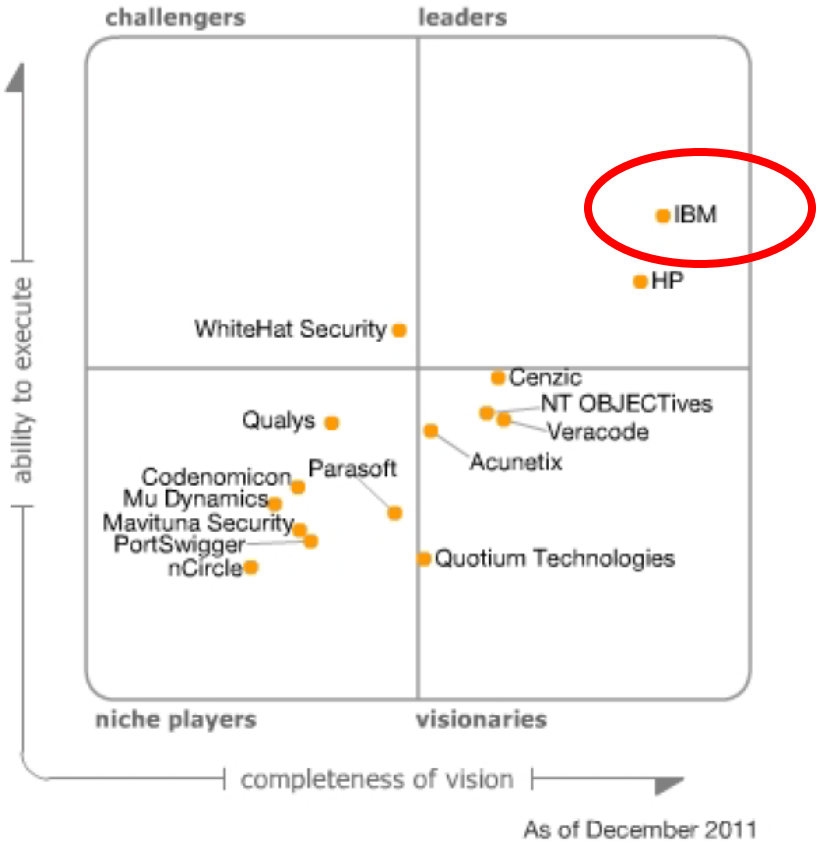
- Continuously monitor applications for appropriate application usage, vulnerabilities and defend against attacks



Gartner has recognized IBM as a leader in The Magic Quadrant for Dynamic Application Security Testing

Magic Quadrant for Dynamic Application Security Testing
Neil MacDonald, Joseph Feinman
Dec 27, 2011

Dynamic application security testing (DAST) solutions should be considered mandatory to test all Web-enabled enterprise applications, as well as packaged and cloud-based application providers.



This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from IBM.

Selling with AppScan

- **Sales Process is 5 steps:**
  1) Lead/Qualify
  2) Initial Demo (Reach out for a Security SE)
  3) Internal Scan (ENSURE you engage a Security SE)
  4) Results Review (ENSURE you engage a Security SE)
  5) Proposal/Close

Solving Customer Challenges

Application Security

Finding the vulnerabilities

Leverage advanced and extensive testing methodologies

Building products that are secure by design

Reduce costs by integrating security testing early in the development lifecycle

Bridging the Security/Development gap

Engaging Security and Development organizations to collaboratively address application vulnerabilities

Controlling access to application data

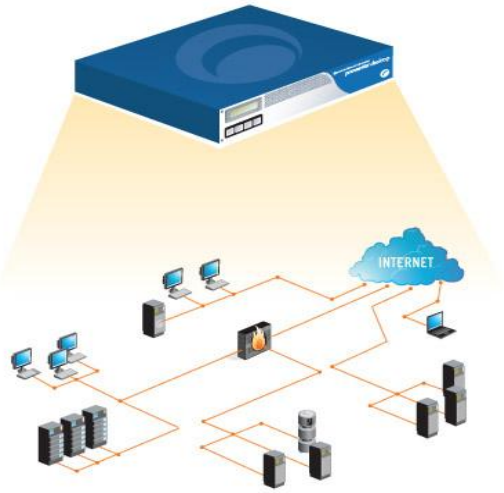
Strengthen applications and data access on a need to know basis

How does AppScan work?

Automates Application Security Testing

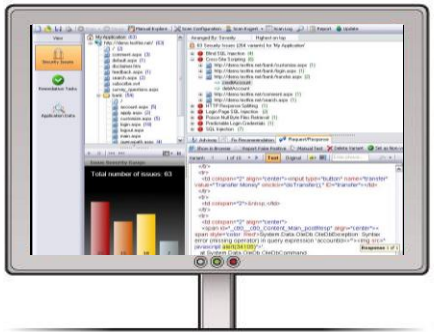
1 → 2 → 3

Scan applications



Analyze

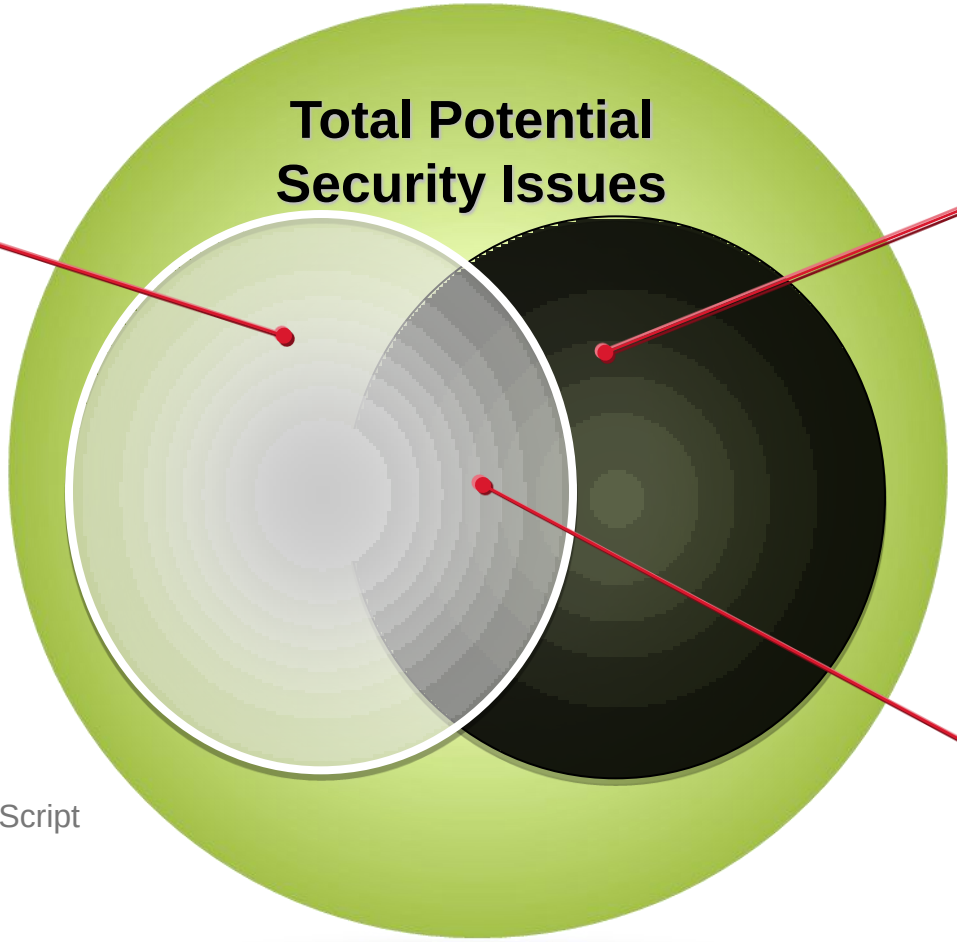
(identify issues)



Report

(detailed & actionable)

Find more vulnerabilities using the most advanced techniques



Static Analysis

- **Analyze Source Code**
- **Use during development**
- **Uses Taint Analysis / Pattern Matching**

Dynamic Analysis

- **Analyze Live Web Application**
- **Use during testing**
- **Uses HTTP tampering**

Hybrid Analysis

- Correlate Dynamic and Static results
- Assists remediation by identification of line of code

More adv. Techniques

Client-Side Analysis

- Analyze downloaded JavaScript code which runs in client
- Unique in the industry

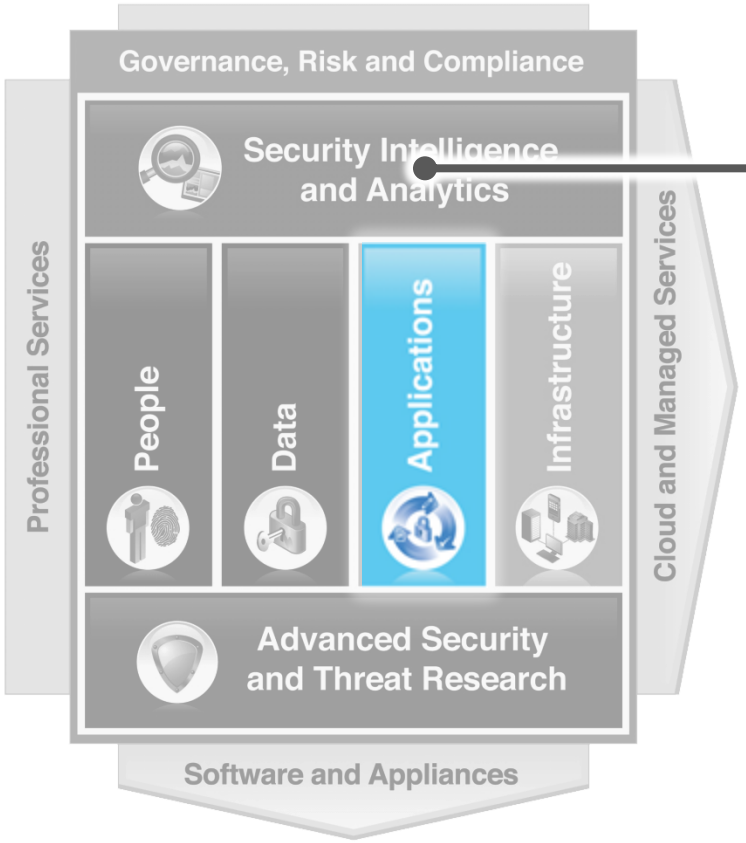
Run-Time Analysis

- Combines Dynamic Analysis with run-time agent
- More results, better accuracy

Portfolio Overview

Area of Focus

Reducing the costs of developing secure applications and assuring the privacy and integrity of trusted information



Portfolio Overview

AppScan Enterprise

- Enterprise-class solution for implementing and managing a static security testing program, includes high-level dashboards, test policies, scan templates and issue management capabilities
- Multi-user solution providing simultaneous security scanning and centralized reporting

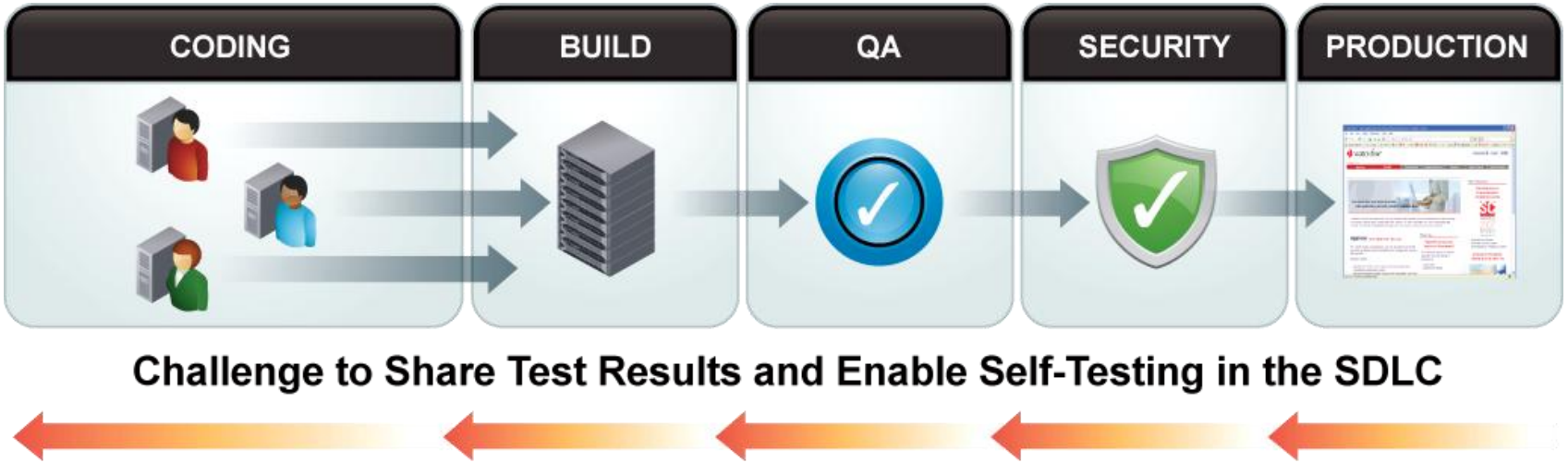
AppScan Standard

- Desktop solution to Dynamic Application Security testing for IT Security, auditors, and penetration testers

AppScan Source

- Static application security testing to identify vulnerabilities at the line of code. Enables early detection within the development life cycle.

AppScan: advanced security testing collaboration & governance through application lifecycle

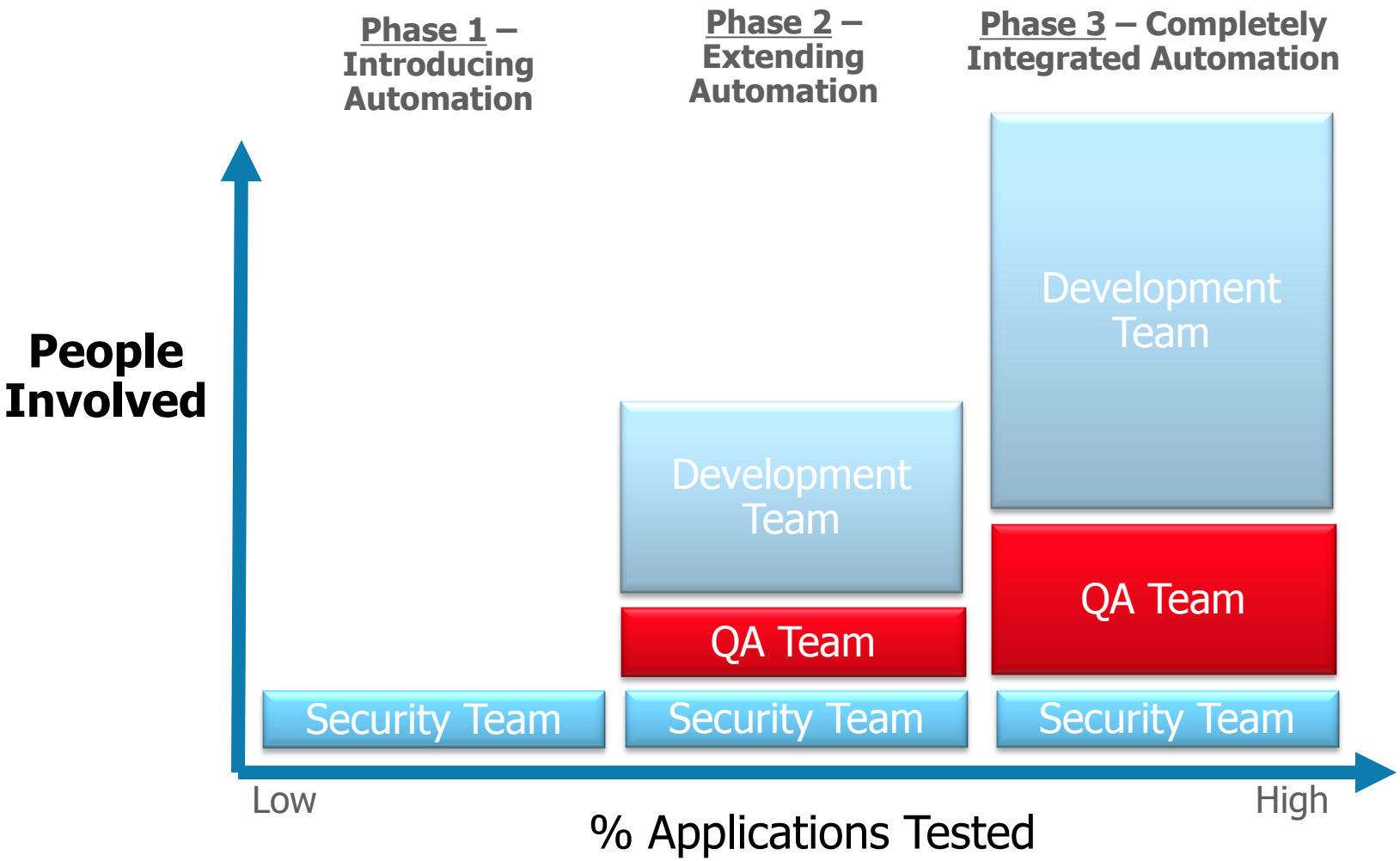


AppScan Standard

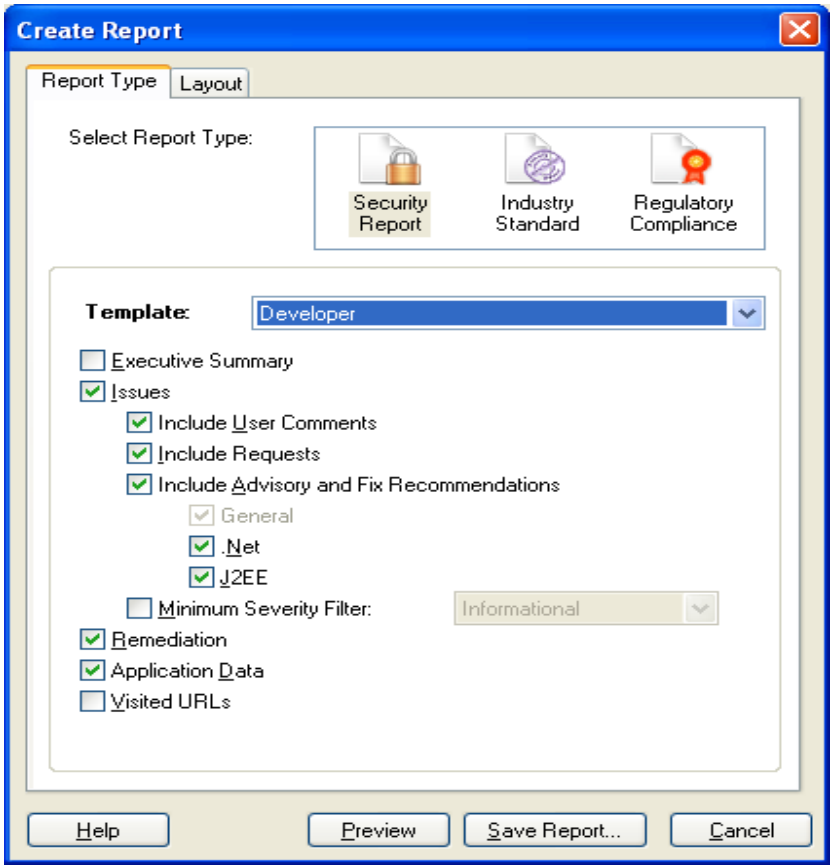
AppScan Enterprise

AppScan Source

The opportunity in front of you Maturity Model



Compliance Reporting



PCI

SOX

HIPAA

GLBA

NERC/ FERC

OWASP

+40 More

ROI Opportunity of Application Security Testing

Cost Savings – of testing early in the development process (ALM)

80% of development costs are spent identifying and correcting defects
Testing for vulnerabilities earlier in the development process can help avoid that unnecessary expense

- *Cost of finding & fixing problems:*
  - *code stage is $80, QA/Testing is $960**
  - *Ex: 50 applications annually & 25 issues per application, testing at code stage* ***saves $1.1M*** *over testing at QA stage.*

Cost Savings – of automated vs. manual testing

Automated testing provides tremendous productivity savings over manual testing
Automated source code testing with periodic penetration testing allows for cost effective security analysis of applications

- *Outsourced audits can cost $10,000 to $50,000 per application*
- *At $20,000 an app, 50 audits will cost $1M.*
- *With 1 hire + 4 quarterly outsourced audits (ex: $120,000+$80,000),* ***$800,000/yr. can be saved*** *(less the cost of testing software)*

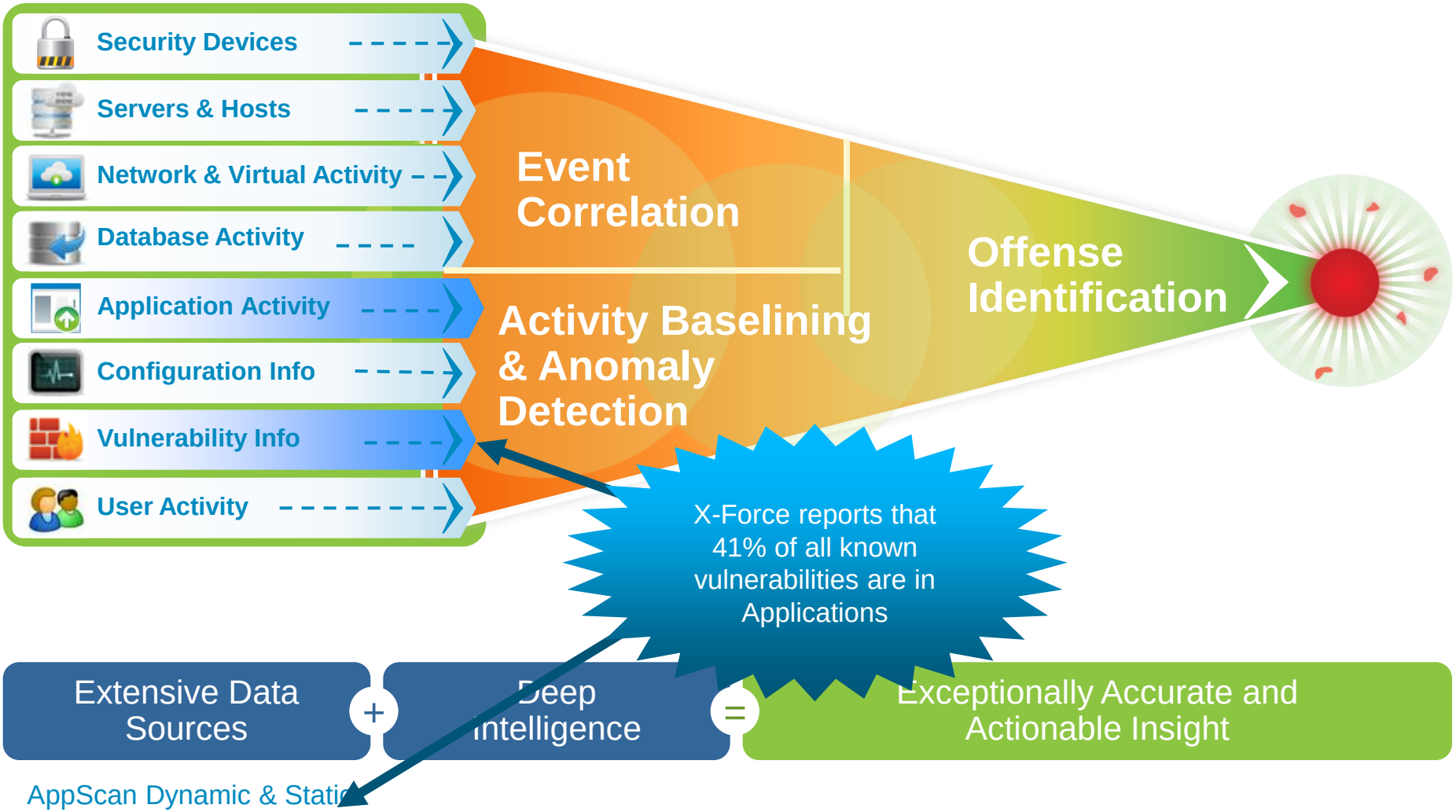
Cost Avoidance – of a security breach

Costs as a result of a security breach can include (but are not limited to) audit fees, legal fees, regulatory fines, lost customer revenue and brand damage

- *The cost to companies is* ***$240*** *per compromised record***
- *The average cost per data breach is* ***$7.2 Million*****

* Source: GBS Industry standard study
** Source: Ponemon Institute 2009-10

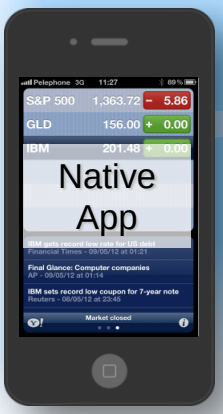
Expand: AppScan integrates with QRadar to add application vulnerability data to your security intelligence



AppScan provides *a new level of support* for mobile application analysis

Mobile Web Apps	
JavaScript / HTML5 hybrid analysis	✓ *IBM Innovation*

Server Side Logic	
SAST (source code)	✓ *Foundational*
DAST (web interfaces)	✓ *Enhanced*



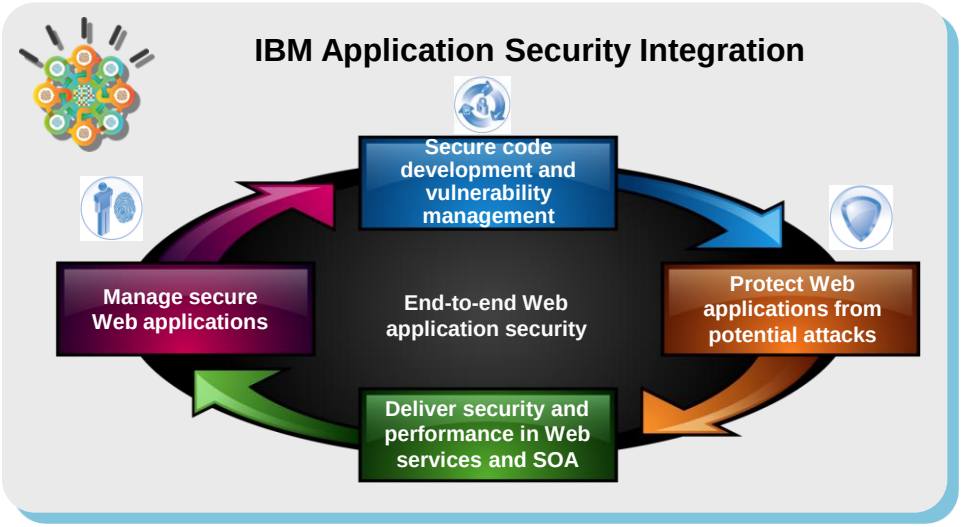
New in AppScan 8.6

Native Apps	
Android applications	✓ *Static Analysis*

Security Intelligence: Integrate with IBM application protection

Web App Protection Customized for Your Specific Vulnerabilities

- Publish security vulnerabilities from AppScan to SiteProtector
  - Security analyst publishes application vulnerabilities to SiteProtector
  - Vulnerable application assets are identified and made visible
  - Network analyst is notified
- SiteProtector displays application security vulnerabilities
  - Network analyst reviews application vulnerabilities
  - Network analyst monitors vulnerable application assets
- SiteProtector SecurityFusion™ provides security intelligence
  - IDS/IPS real-time malicious HTTP traffic is correlated with vulnerable application assets
  - SiteProtector alerts network analyst when attacks are likely to succeed
  - Network analyst takes action
- Until application fix is available, mitigate risk with IBM Security IPS
  - Network analyst creates a virtual patch by enabling IPS web application protection policy
  - Network analyst enables protection categories based on the types of discovered vulnerabilities with AppScan



AppScan Solutions for SAP Security

- Highlights:
  - Identify and remediate security vulnerabilities in your SAP applications
  - Automate the testing of SAP web portals with advanced dynamic analysis security testing
  - Analyze Advanced Business Application Programming (ABAP) source code with static analysis security testing to expose security defects
  - Integrate security testing into your SAP application development process
  - Manage application security and risk for your SAP application deployment
  - Manage regulatory requirements such as PCI, GLBA and HIPAA
- For ABAP applications, IBM has partnered with the SAP security experts at Virtual Forge GmbH to offer CodeProfiler for IBM Security AppScan Source software, which delivers advanced static analysis of ABAP source code.
- Additional details can be found here:
  - Internal
  - PartnerWorld

Contacts & Resources

- **Sales / Enablement Contacts**
  - Jason Bellomy, NA Application Security Sales Exec – bellomyj@us.ibm.com
  - Tim Bedard, WW Application Security Sales Exec – bedard@us.ibm.com
  - Bill Maynard, NA Inside Sales Manager– bmaynard@ca.ibm.com
  - Jeff Ross, WW AppScan Source Sales – jeffross@us.ibm.com
  - Chris Stewart, WW Alliance Manager cjs@ca.ibm.com
  - Greg Sabatini, WW Technical Sales Lead – gsabatin@us.ibm.com

  - Michele Sullivan, Operations Goddess msulliv@us.ibm.com
    (Entitlements, Consulting licenses, Renewal questions, history)

  - Faustino Sanchez, Application Security Sales Enablement sanchezf@ca.ibm.com
  - Robert Kennedy, Application Security Sales Enablement – kennedyr@us.ibm.com

- **Product Team**
  - Lawrence Gerard, Senior Manager, Product Management Lead – lgerard@us.ibm.com
  - Tom Mulvehill, Product Manager – tom.mulvehill@us.ibm.com
  - Constantine Grancharov, Product Manager -constantineg@ca.ibm.com