



# IBM Security

Intelligence, Integration and Expertise

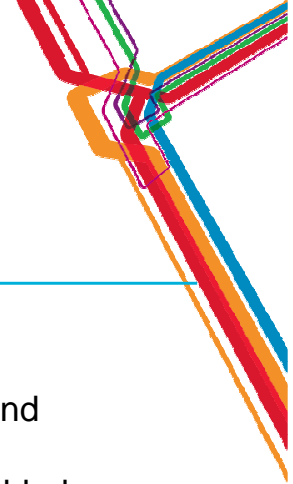
*Fabio Panada – IBM Security Technical Sales Leader*

**PCTY2012** 

Pulse Comes to You

**Optimizing the World's Infrastructure**  
**15 Maggio 2012 - Roma**

# IBM solutions are built on a core set of software capabilities



Need	Capability	Need	Capability
<b>Turn Information into Insights</b>	Business Analytics Data Management Data Warehousing Enterprise Content Management Information Governance Information Integration and Federation	<b>Enable Product and Service Innovation</b>	Application Lifecycle Management Business Planning and Alignment Complex and Embedded Systems Design, Development and Deployment Enterprise Modernization Security
<b>Drive Business Integration and Optimization</b>	Application Infrastructure Business Process Management Commerce Connectivity and Integration Enterprise Marketing Management	<b>Optimize the Impact of Business Infrastructures and Services</b>	Asset Management Business Service Management Cloud and Virtualization Management Network and Service Assurance Security Storage Management Systems Management
<b>Connect and Collaborate</b>	Social Business Application Development Social Collaboration Unified Communications Web Experience	<b>Manage Risk, Security, and Compliance</b>	Application and Process Data and Information Network, Server, and Endpoint People and Identity Physical Infrastructure Security governance, risk management and compliance

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



## 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



## 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



## EVERYTHING IS EVERYWHERE

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

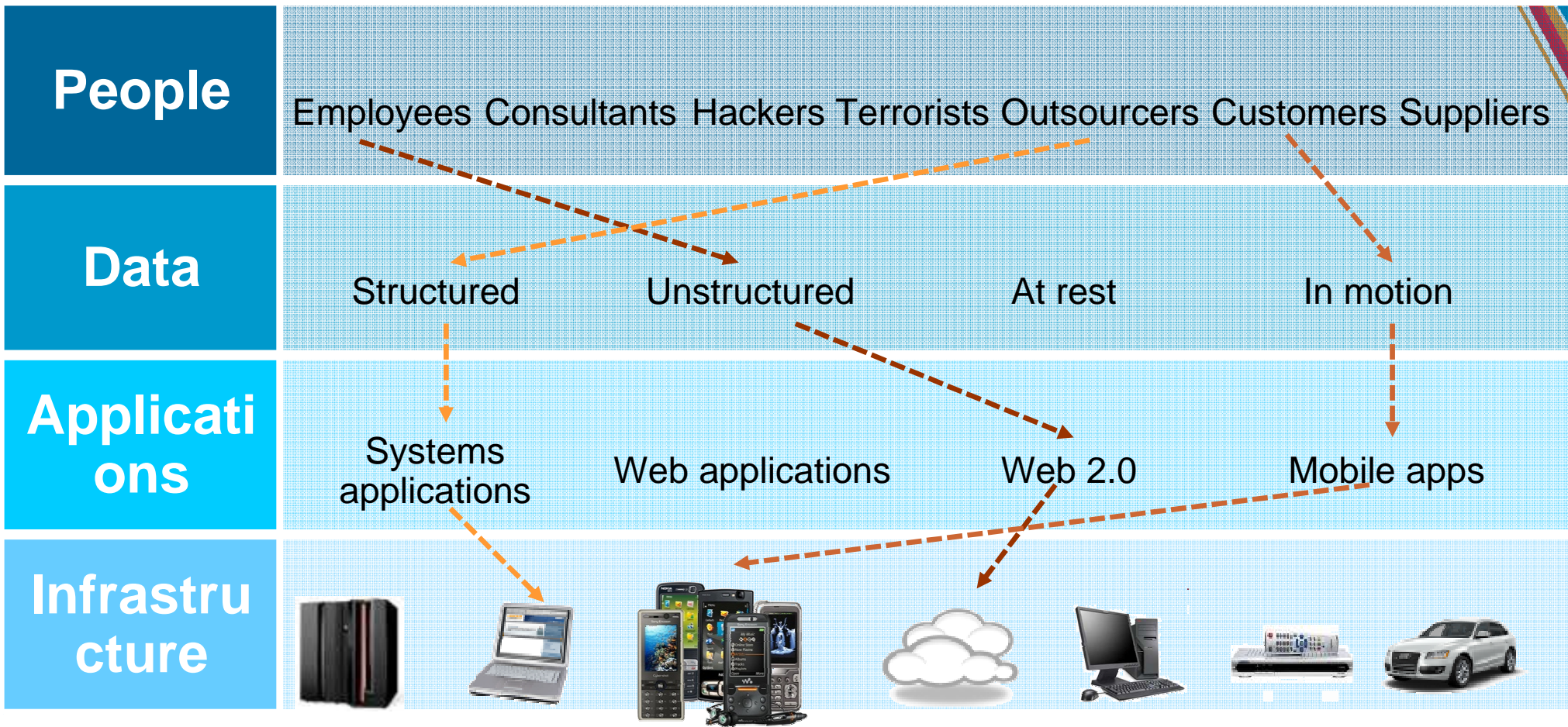


## ATTACK SOPHISTICATION

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

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

# Solving a security issue is a complex, four-dimensional puzzle



It is no longer enough to protect the perimeter – siloed point products will not secure the enterprise

# Key drivers affecting the security software business

It is no longer enough to protect the perimeter – sophisticated attacks are bypassing traditional defenses, IT resources are moving outside the firewall, and enterprise applications and data are becoming distributed across multiple devices

## 1. Advanced Threats

Sophisticated, targeted attacks, designed to gain continuous access to critical information, are increasing in severity and occurrence.



Advanced Persistent Threats  
Stealth Bots Designer Malware  
Targeted Attacks Zero-days

## 2. Cloud Computing

Security is one of the top concerns of cloud, as customers drastically rethink the way IT resources are designed, deployed and consumed.

IBM SmartCloud



## 3. Mobile Computing

Managing employee owned devices and securing connectivity to corporate applications are top of mind as CIOs broaden their support for mobile devices.



Enterprise Customers

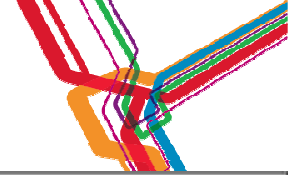
## 4. Regulations and Compliance

Regulatory and compliance pressures continue to mount as companies store sensitive data and become susceptible to audit failures.



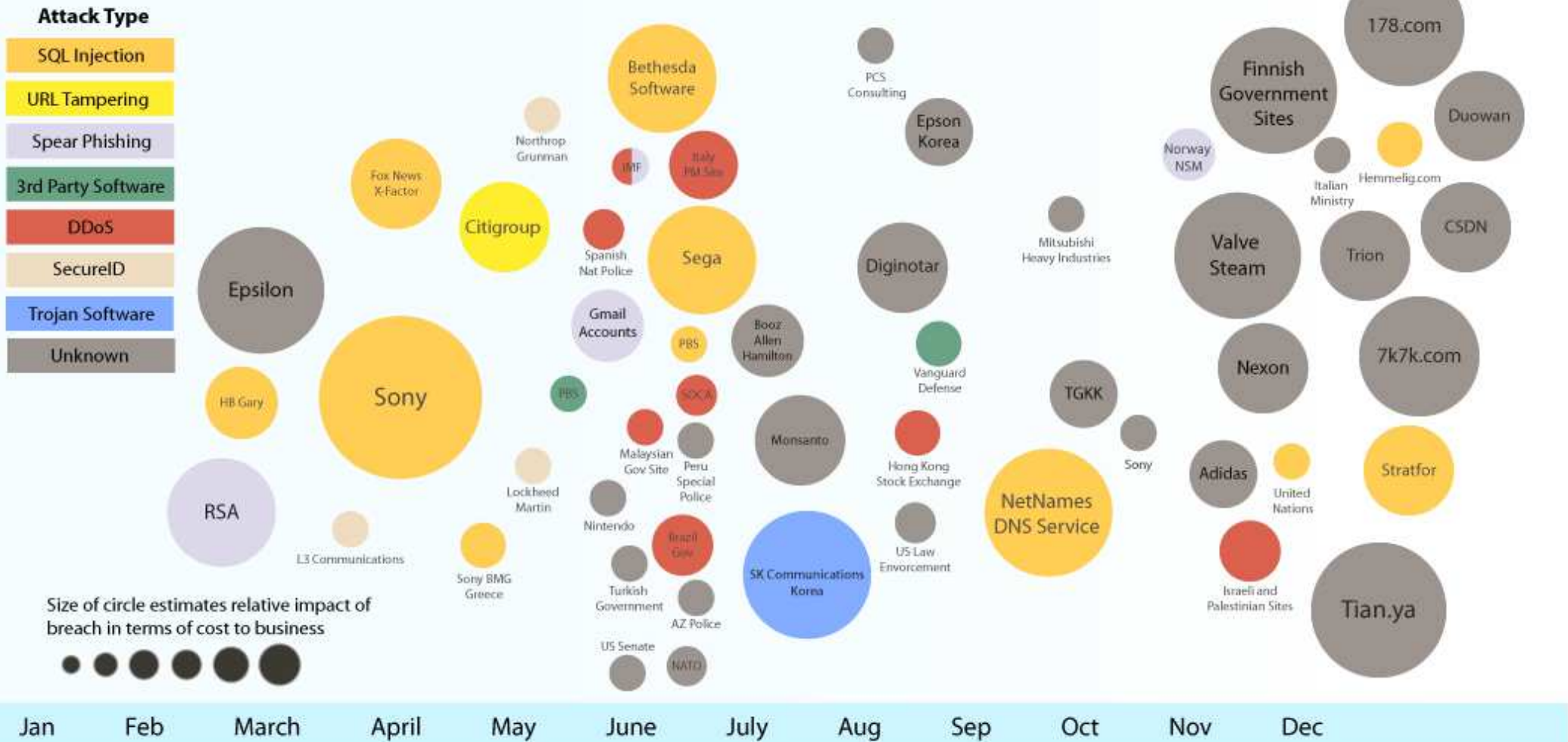


# 2011 – The Year of the Breach

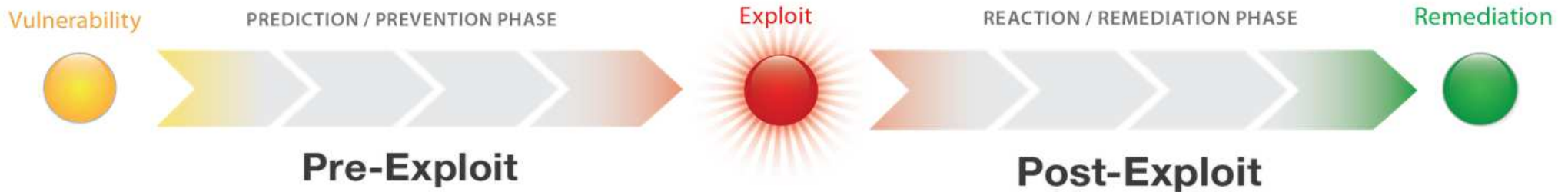


## 2011 Sampling of Security Incidents by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



# Solutions for the Full Compliance and Security Intelligence Timeline



## Prediction & Prevention

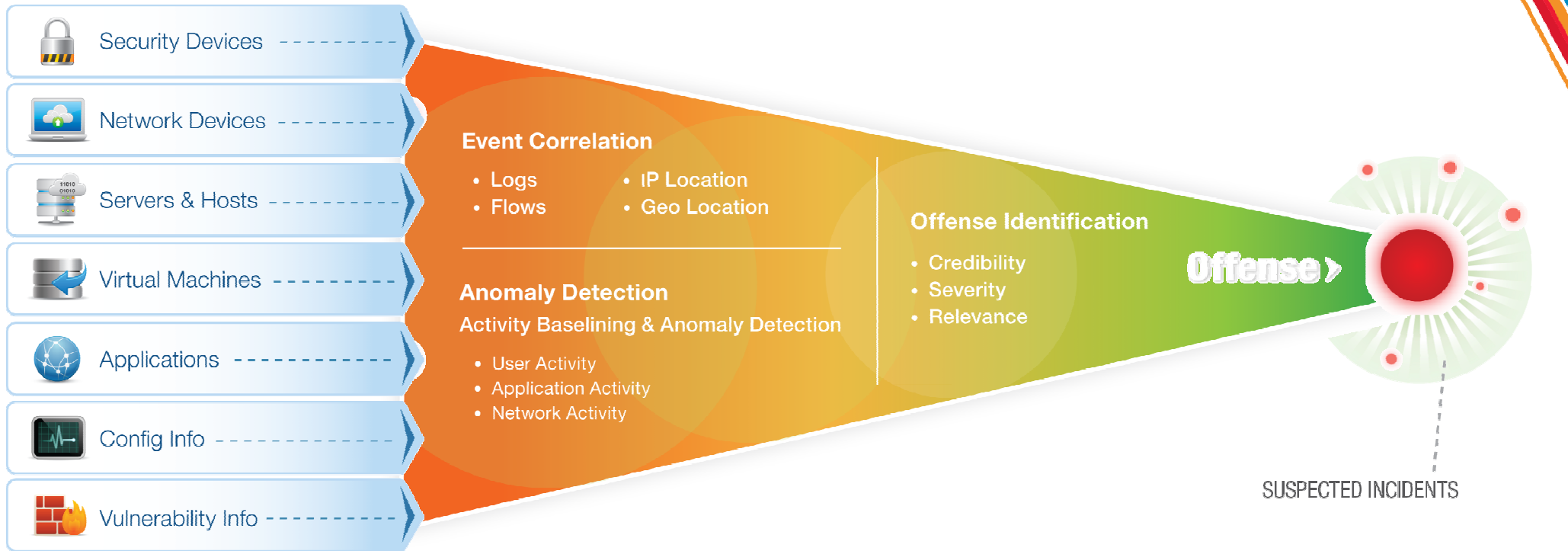
Risk Management. Vulnerability Management.  
 Configuration Monitoring. Patch Management.  
 X-Force Research and Threat Intelligence.  
 Compliance Management. Reporting and Scorecards.

## Reaction & Remediation

SIEM. Log Management. Incident Response.  
 Network and Host Intrusion Prevention.  
 Network Anomaly Detection. Packet Forensics.  
 Database Activity Monitoring. Data Loss Prevention.



# Context and Correlation Drive Deepest Insight



Extensive Data Sources



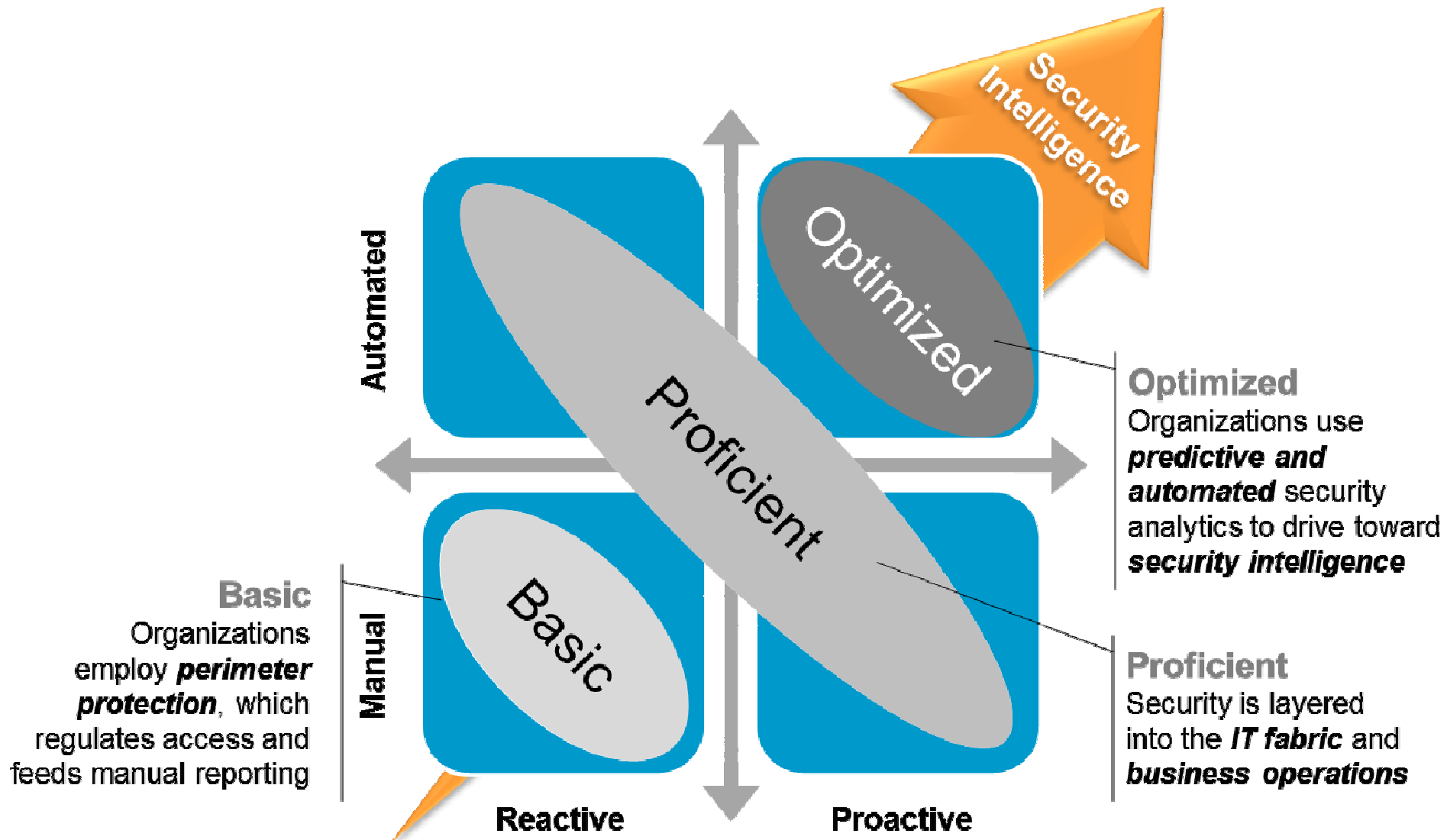
Deep Intelligence



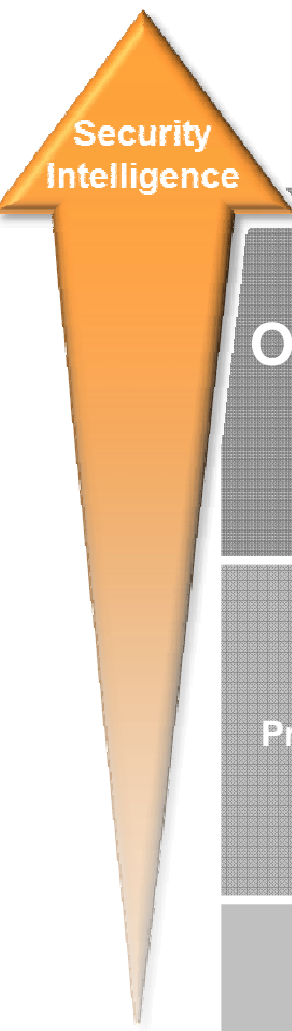
Exceptionally Accurate  
and Actionable Insight



# Organizations need an intelligent view into their security posture

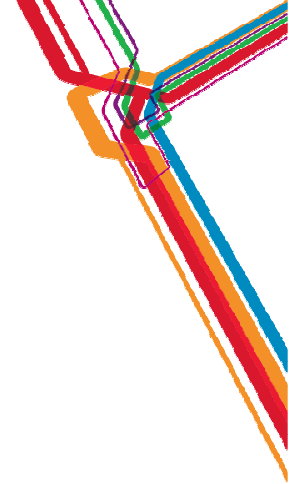


# Helping Organizations Progress in Their Security Maturity



	People	Data	Applications	Infrastructure	Security Intelligence
Optimized	<ul style="list-style-type: none"> <li>Role based analytics</li> <li>Identity governance</li> <li>Privileged user controls</li> </ul>	<ul style="list-style-type: none"> <li>Data flow analytics</li> <li>Data governance</li> </ul>	<ul style="list-style-type: none"> <li>Secure app engineering processes</li> <li>Fraud detection</li> </ul>	<ul style="list-style-type: none"> <li>Advanced network monitoring</li> <li>Forensics / data mining</li> <li>Securing systems</li> </ul>	<ul style="list-style-type: none"> <li>Advanced threat detection</li> <li>Network anomaly detection</li> <li>Predictive risk management</li> </ul>
Proficient	<ul style="list-style-type: none"> <li>User provisioning</li> <li>Access mgmt</li> <li>Strong authentication</li> </ul>	<ul style="list-style-type: none"> <li>Access monitoring</li> <li>Data loss prevention</li> </ul>	<ul style="list-style-type: none"> <li>Application firewall</li> <li>Source code scanning</li> </ul>	<ul style="list-style-type: none"> <li>Virtualization security</li> <li>Asset mgmt</li> <li>Endpoint / network security management</li> </ul>	<ul style="list-style-type: none"> <li>Real-time event correlation</li> <li>Network forensics</li> </ul>
Basic	<ul style="list-style-type: none"> <li>Centralized directory</li> </ul>	<ul style="list-style-type: none"> <li>Encryption</li> <li>Access control</li> </ul>	<ul style="list-style-type: none"> <li>Application scanning</li> </ul>	<ul style="list-style-type: none"> <li>Perimeter security</li> <li>Anti-virus</li> </ul>	<ul style="list-style-type: none"> <li>Log management</li> <li>Compliance reporting</li> </ul>

# IBM's Comprehensive, Integrated Security Portfolio



**Enterprise Governance, Risk and Compliance Management**

IBM OpenPages	Algorithmics ( <i>recent acquisition</i> )	i2 Corporation ( <i>recent acquisition</i> )
---------------	--	--



**IBM Security Portfolio**

**IT Security / Compliance Analytics & Reporting**

QRadar SIEM	QRadar Log Manager	QRadar Risk Manager	IBM Privacy, Audit and Compliance Assessment Services	
-------------	--------------------	---------------------	---	--

**IT Infrastructure – Operational Security Domains**

People	Data	Applications	Network	Infrastructure	Endpoint
Identity & Access Management Suite	Guardium Database Security	AppScan Source Edition	Network Intrusion Prevention	Endpoint Manager (BigFix)	
Federated Identity Manager	Optim Data Masking	AppScan Standard Edition	DataPower Security Gateway	zSecure, Server and Virtualization Security	
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection / QFlow	Native Server Security (RACF, IBM Systems)	
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service	Application Assessment Service	Managed Firewall, Unified Threat and Intrusion Prevention Services	Penetration Testing Services	
	Encryption and DLP Deployment	AppScan OnDemand Software as a Service			

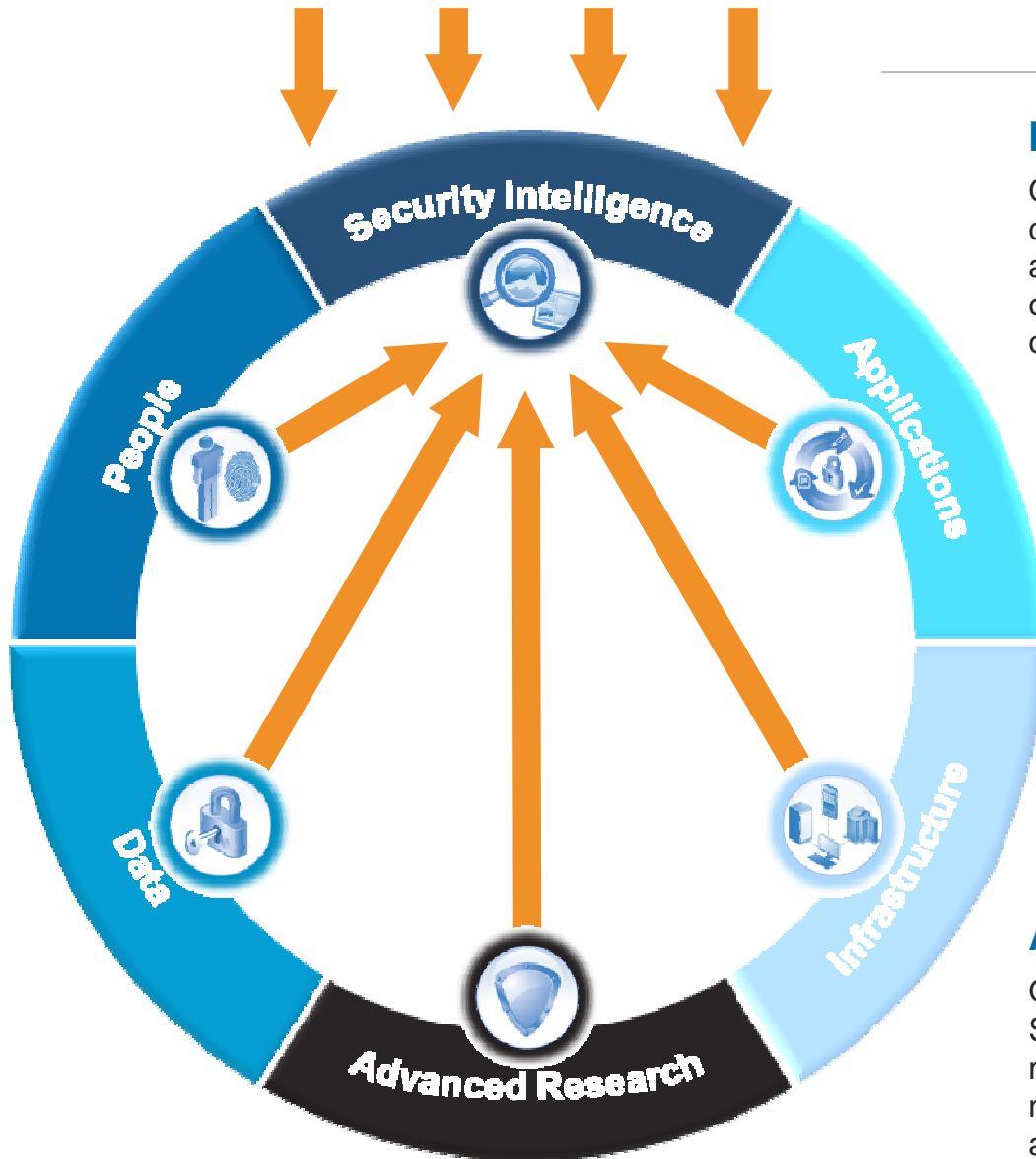
**Security Consulting**

**Managed Services**

**X-Force and IBM Research**

# Solutions Integration

Hundreds of 3<sup>rd</sup> party information sources



## Integrated Intelligence.

### Increase security awareness and accuracy

QRadar SIEM consolidates siloed information to more effectively detect and manage complex threats. Information is normalized and correlated to quickly deliver intelligence that allows organizations to detect, notify and respond to threats missed by other security solutions with isolated visibility

Support for over 400+ information sources, including many IBM products and technologies

- User and Asset Context - Contextual data from IAM products and vulnerability scanners
- Application Logs - ERP, workflow, application databases, management platforms, etc.
- Network Events - Switches, routers, servers, hosts, etc.
- Network Activity Context - Layer 7 application context from network and application traffic
- Security Events - Events from firewalls, VPNs, IPS, etc.

### Automate compliance tasks and assess risks

QRadar Risk Manager leverages and extends the value of a SIEM deployment to greatly improve the ability to automate risk management functions in mission critical areas, including network and security configuration, compliance management, and vulnerability assessment



# Integrated Research.



## Stay ahead of the changing threat landscape

The X-Force team is one of the best-known commercial security research groups in the world. These security experts research vulnerabilities and security issues, collect worldwide threat data and develop countermeasure technologies for IBM products

Examples of integrated X-Force research

- X-Force Database - 63,000+ unique vulnerabilities, threats and security checks
- Virtual Patch - Eliminates fire drills for new threats by mitigating vulnerabilities through network intrusion prevention
- X-Force Hosted threat analysis service - offers threat information collected from globally networked security operations centers



## Intelligence to assess and harden databases

Guardium contains hundreds of preconfigured vulnerability tests, encompassing CIS and STIG best practices, updated regularly through IBM's Knowledge Base service

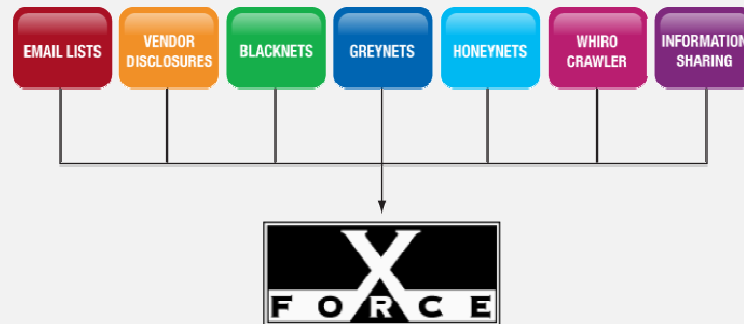
## Detect the latest web application vulnerabilities

Information on the latest threats, updated automatically when you launch a AppScan product – including OWASP and SANS top vulnerabilities

Global Threat  
Intelligence

**PCTY2012**

# Increased situational awareness by leveraging information from X-Force Research and IBM Global Threat Intelligence



QRadar SIEM

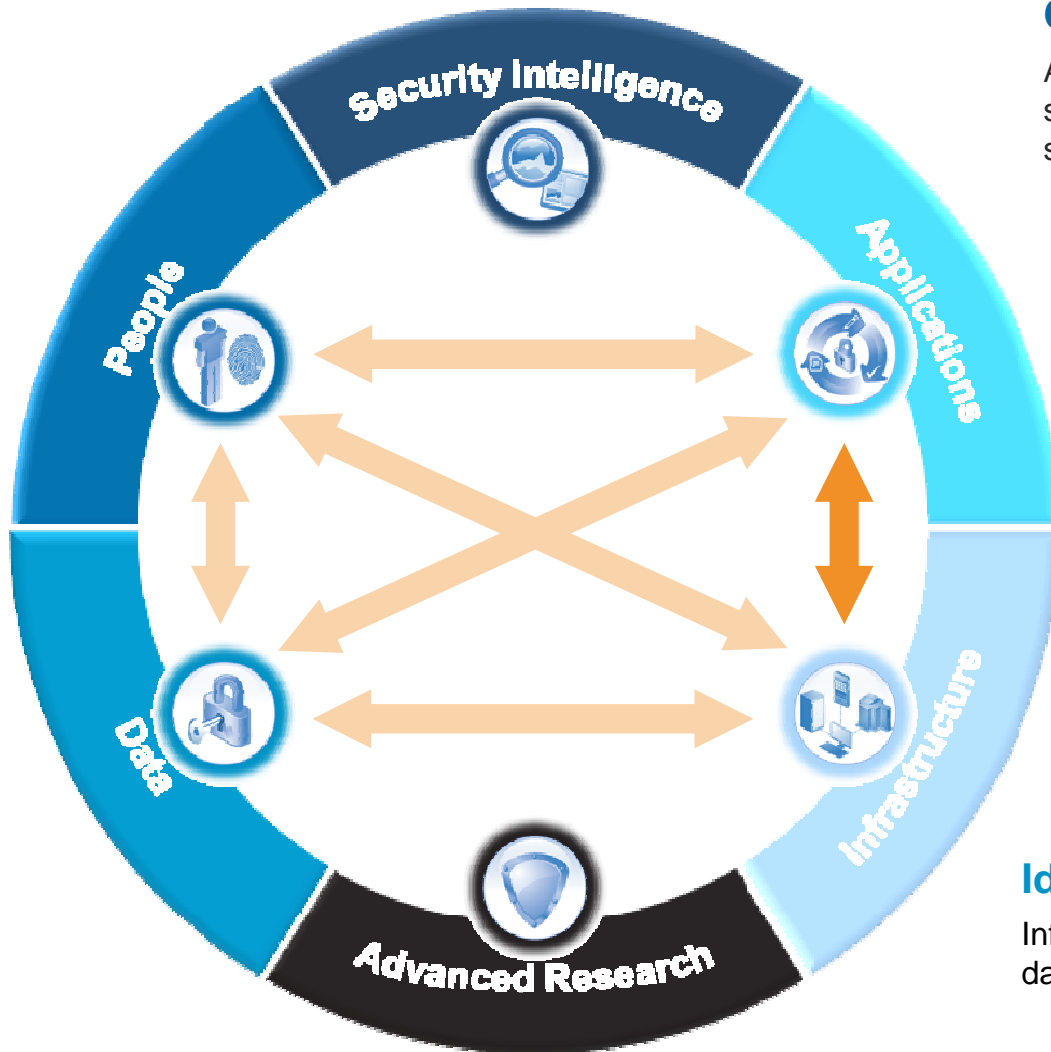


IBM Security Network  
Intrusion Prevention System

- IP Address
- Domain Name
- URL
- Content
- Checksum
- Geolocation

- How many attacks over the last 24 hours originate from this IP address?
- Is a botnet using this domain for hosting or command and control?
- What is the country of origin for this incoming connection?
- Has anyone else made this DNS request? Is there a global spike?
- Is this website known to be infected with malware?

# Integrated Protection.



## Customized protection to block web attacks

AppScan Enterprise Edition software integrates with the IBM security solution for network and server security to protect specific vulnerabilities using scan results

- ① AppScan scans and tests web applications to identify risks and vulnerabilities
- ② SiteProtector consumes AppScan results and builds recommended policies
- ③ Customized protection policies are pushed to IPS appliances and server agents

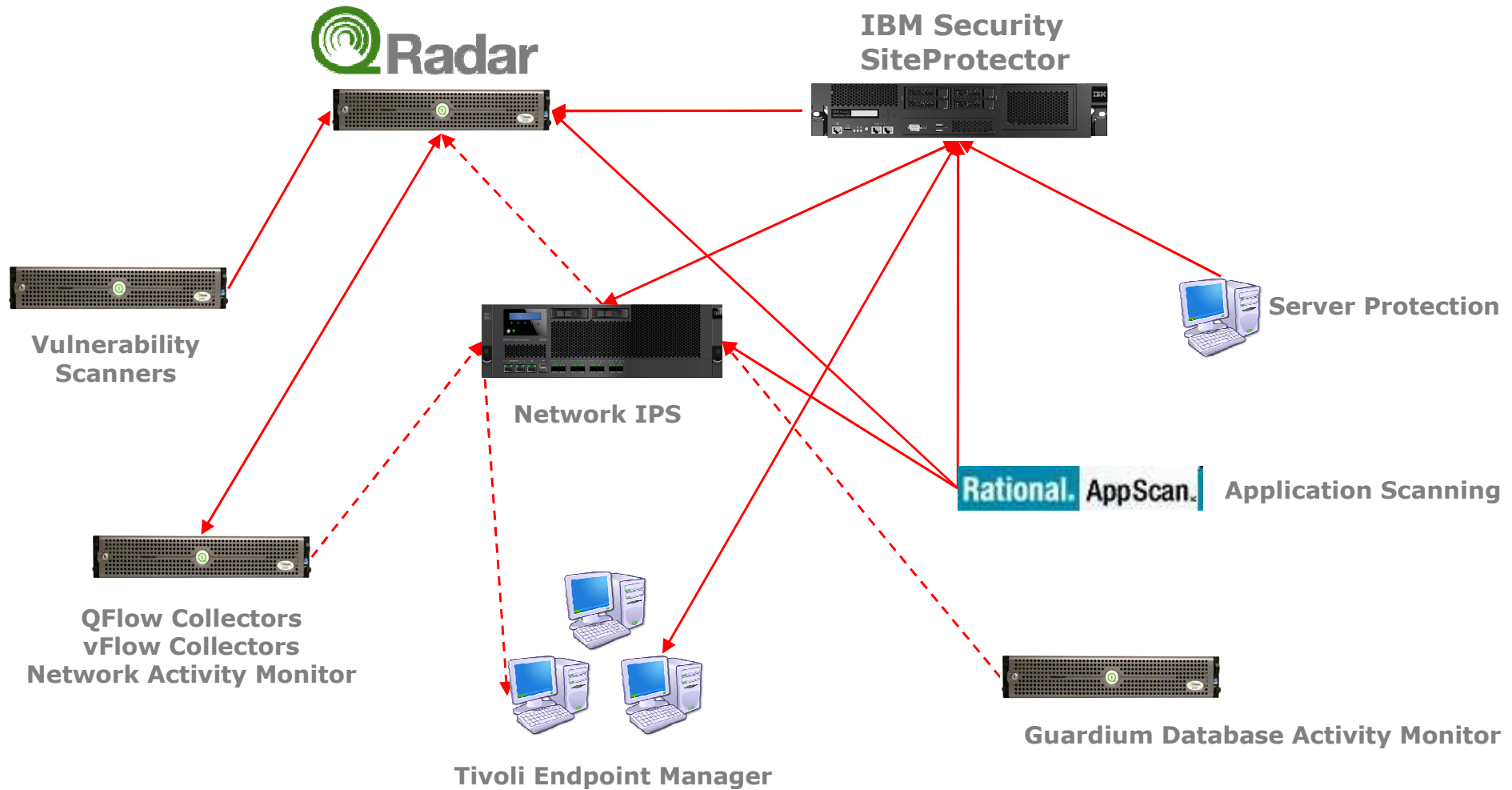
## Automated policy enforcement

IBM's suite of Identity and Access Management tools are leveraged by DataPower SOA gateways to provide central policy management and user access enforcement across web services deployments, including credentials for the gateways themselves.

## Identify users associated with database activity

InfoSphere Guardium leverages identity information for in-depth database security analysis when monitoring suspicious activity

# QRadar and SiteProtector interoperate directly across the threat protection landscape



# X-Force – Intelligence Research



# IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework



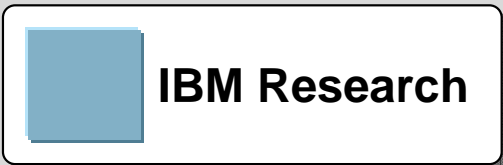
## IBM Security Systems

- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

Intelligence • Integration • Expertise



# Expertise: Unmatched global coverage and security awareness



10B analyzed Web pages & images  
 150M intrusion attempts daily  
 40M spam & phishing attacks  
 46K documented vulnerabilities  
 Millions of unique malware samples



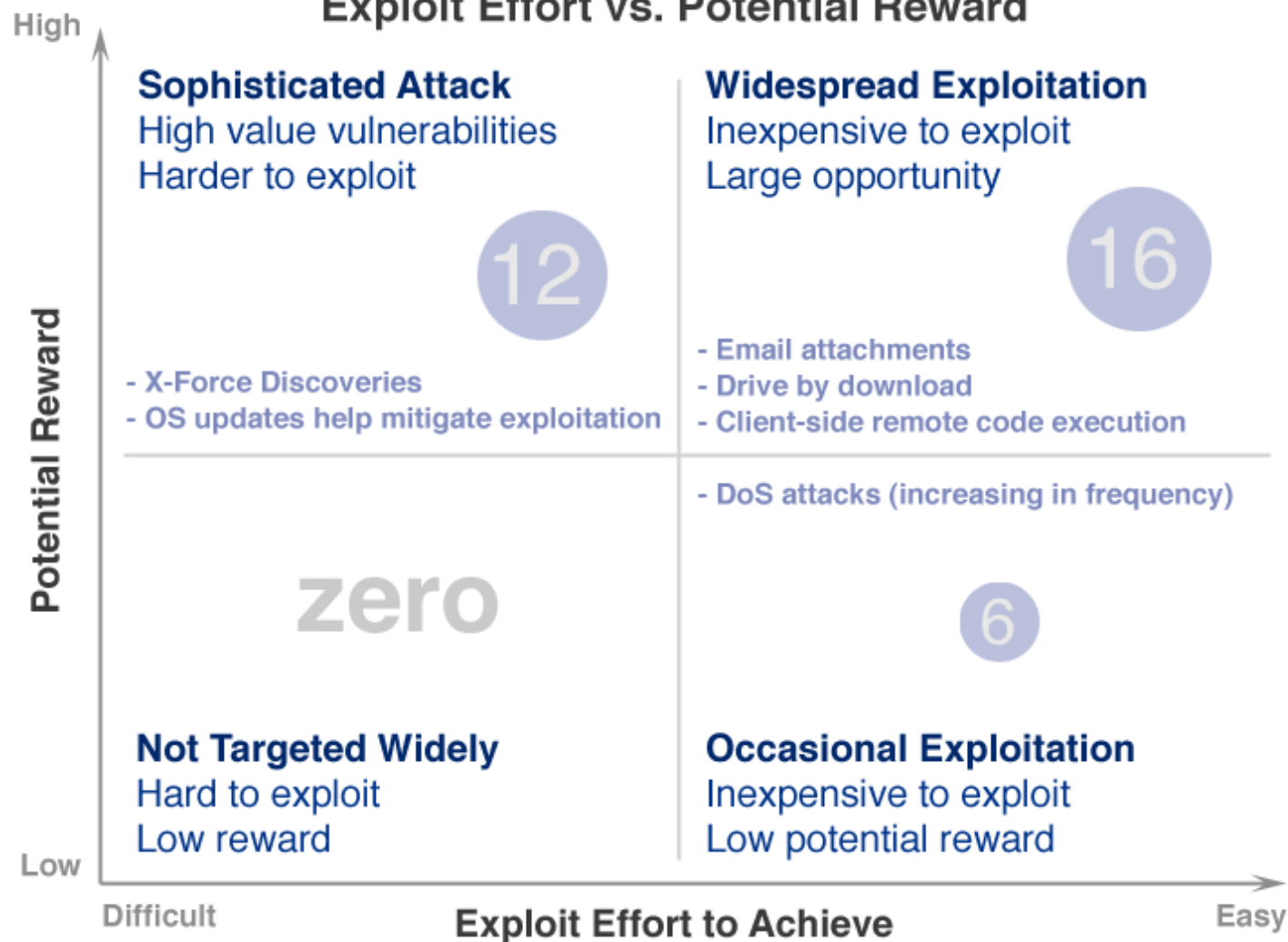
**World Wide Managed Security Services Coverage**

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 9B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

# Predict what the attacker will exploit

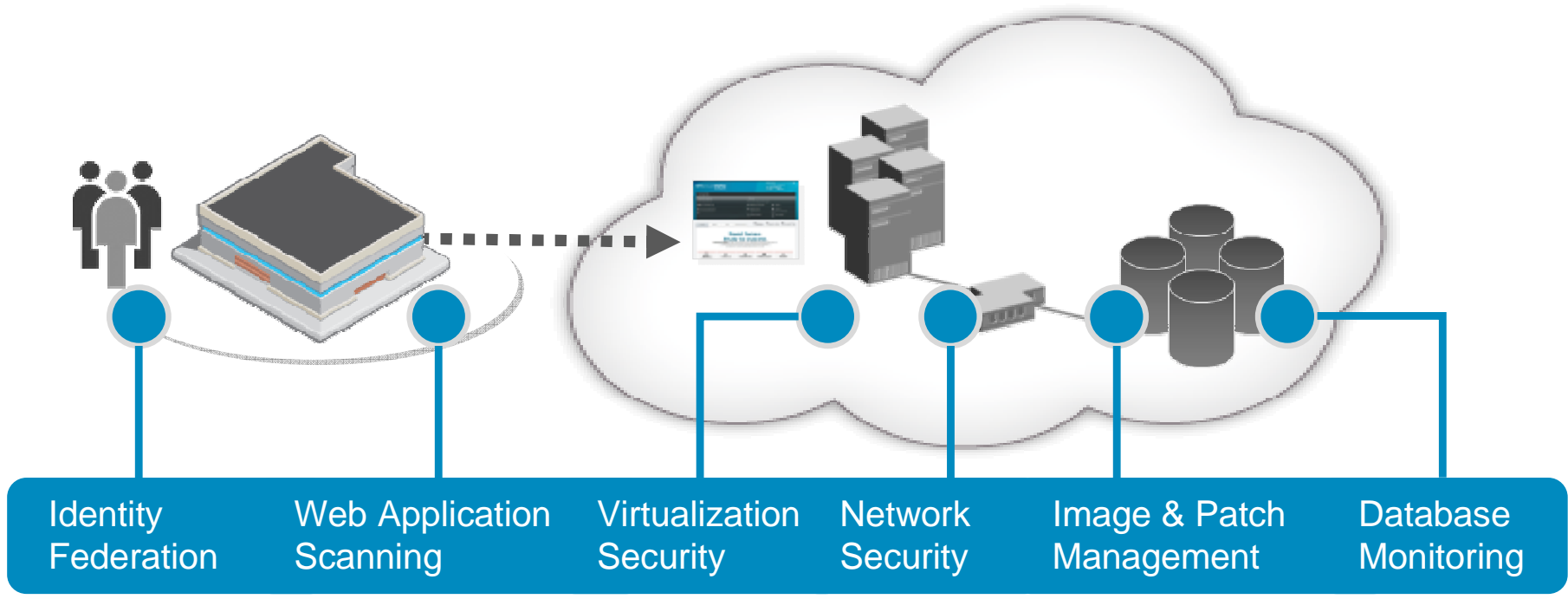
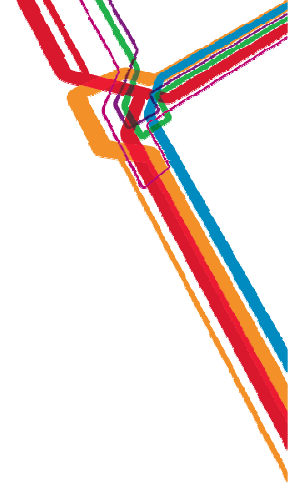


## Exploit Effort vs. Potential Reward

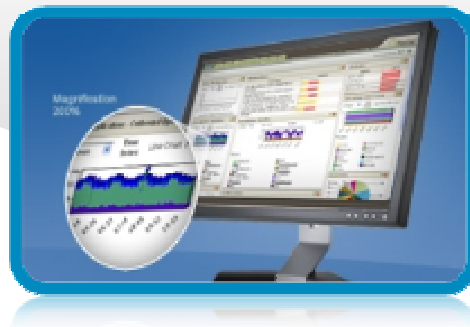


- 33 X-Force alerts and advisories in 2011
- 16 high value, cheap-to-exploit
  - Publicly available exploits for most of them
- 12 harder to exploit but high value
  - This is a higher number than in previous years

# Everything is Everywhere



## IBM Security Intelligence





# Less a technical problem, More a business challenge

- Many of the breaches could have been prevented
- However, significant effort required to inventory, identify and close every vulnerability
- Financial & operational resistance is always encountered, so how much of an investment is enough?

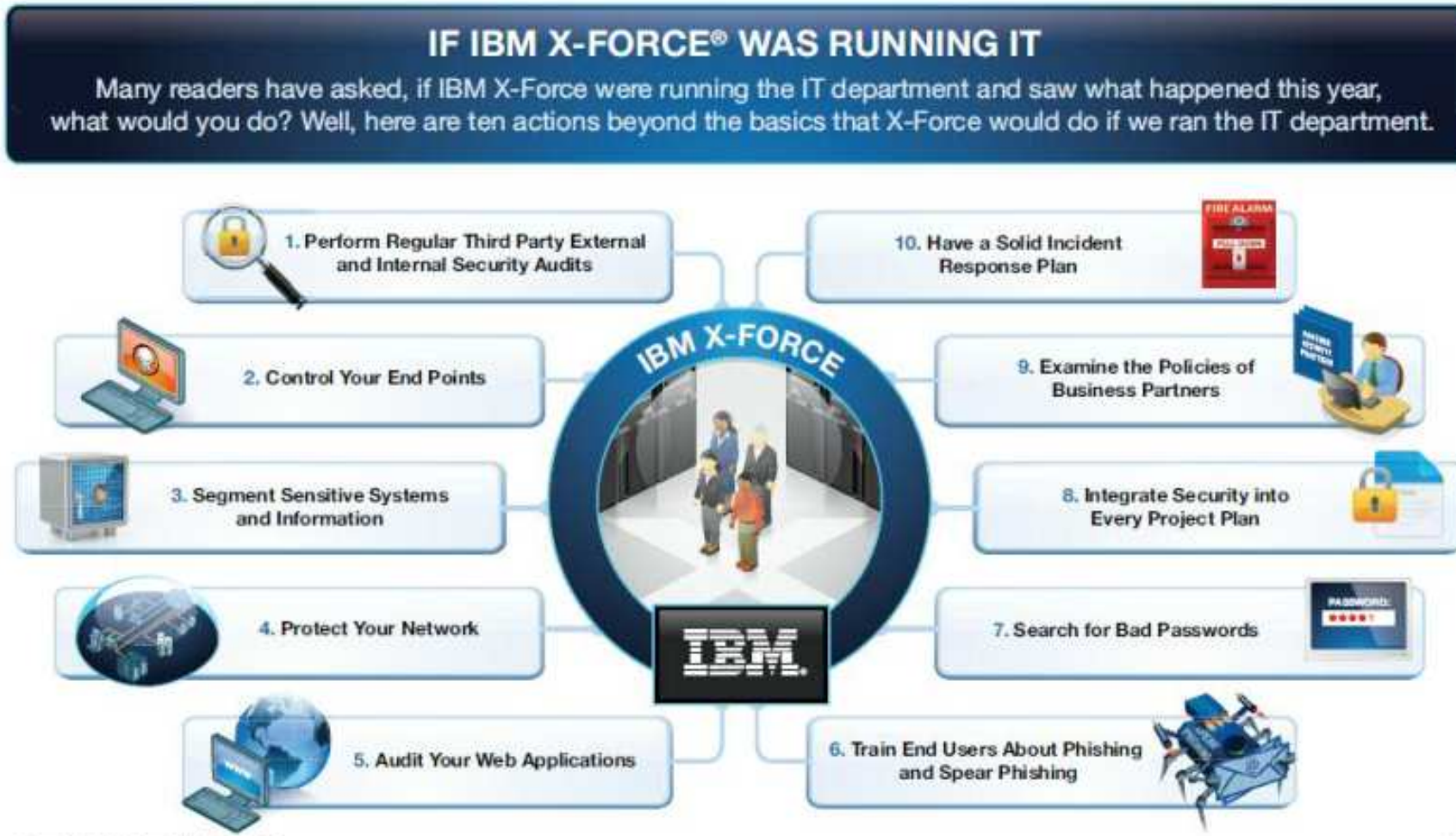


Figure 3: If IBM X-Force Was Running IT

15



## 2012 Prediction:

- Increased Hacktivism (SQLi and DDoS)
- Average increases in # of vulnerabilities and exploits
- Increases in state sponsored cyber warfare



# Get Engaged with IBM X-Force Research and Development



Follow us at @ibmsecurity  
and @ibmxforce



Download X-Force  
security trend & risk  
reports

<http://www-935.ibm.com/services/us/iss/xforce/>



Subscribe to X-Force alerts at  
<http://iss.net/rss.php> or  
Frequency X at

<http://blogs.iss.net/rss.php>



Attend in-person  
events

<http://www.ibm.com/events/calendar/>



Join the Institute for  
Advanced Security

[www.instituteforadvancedsecurity.com](http://www.instituteforadvancedsecurity.com)



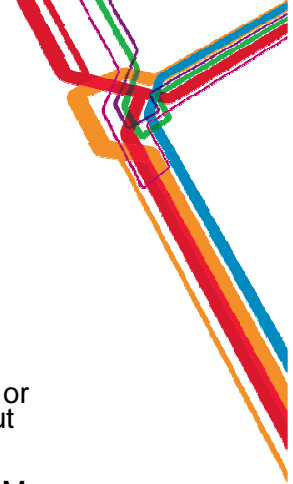
Subscribe to the security  
channel for latest security  
videos

[www.youtube.com/ibmsecuritysolutions](http://www.youtube.com/ibmsecuritysolutions)



[ibm.com/security](https://ibm.com/security)

# Acknowledgements, disclaimers and trademarks



© Copyright IBM Corporation 2012. All rights reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication 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 this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation 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. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

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.

IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)