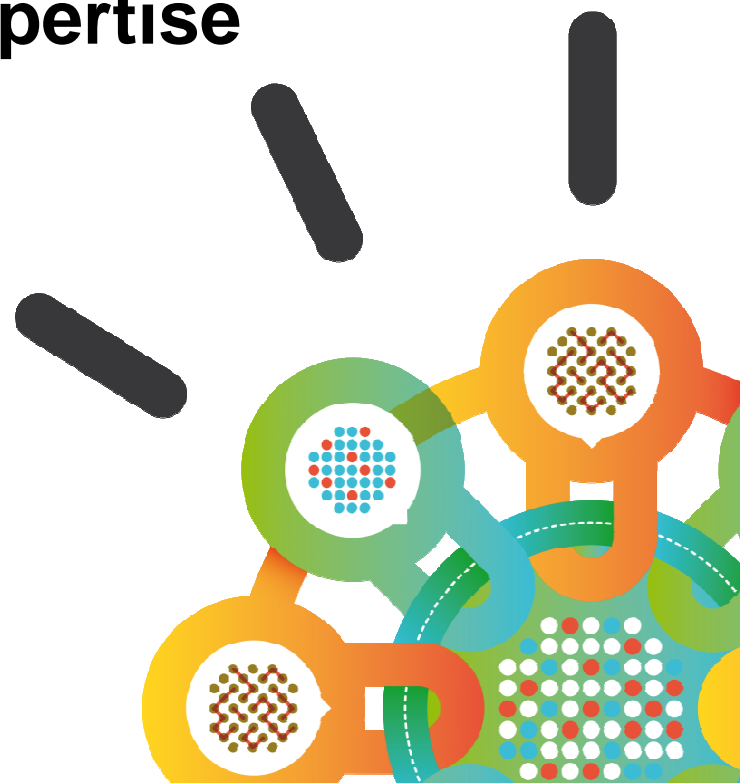


Security Intelligence.
Think Integrated.

IBM Security

Intelligence, Integration and Expertise

IBM Security Systems
May 2013

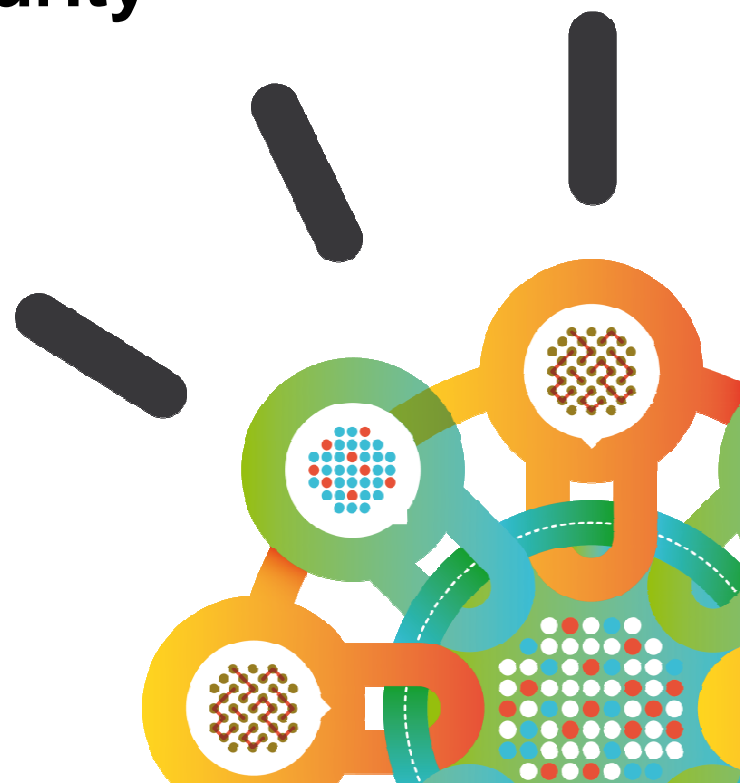


Agenda

- Welcome and Introductions
- Latest Security trends and 2012 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent threats
- Break
- **Managing Application Security**
- From Identity & Access Management to Identity Intelligence
- Securing your Cloud
- IBM Global Financing

Security Intelligence.
Think Integrated.

IBM Security – Application Security



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

Solving Customer Solutions *Application Security*

amdocs

Finding Application Vulnerabilities

“GlassBox scanning allowed us to improve results accuracy as well as test for new class of vulnerabilities undetected by conventional web application security scanning technologies”

Boris Gorin, Amdocs

SAP

Reducing the Cost of Being Secure

“AppScan not only helps us to avoid costs related to hacking attacks, but also reduces the manual effort needed for analysis and the costs for testing”

Michael Neumaier, Senior Quality Specialist, SAP AG



Providing Oversight and Governance

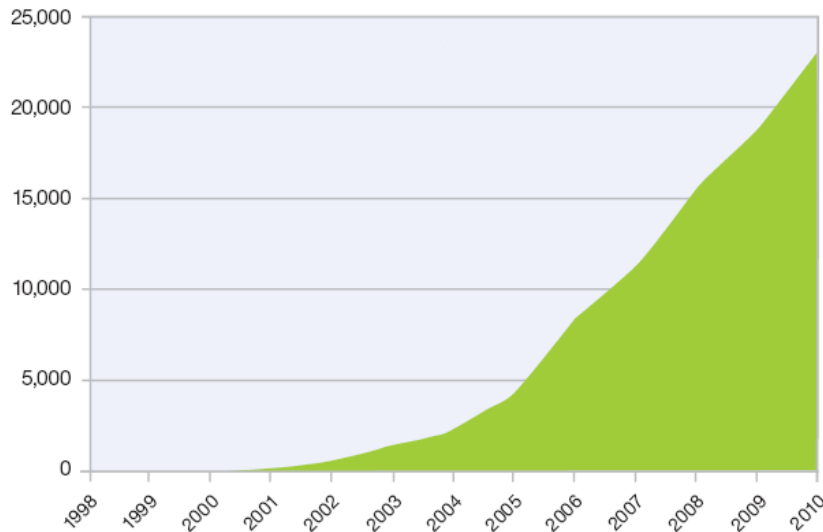
“We were able to increase the participation of the IT community in web application scanning”

Alex Jalso, Assistant Director, Office of Information Security, WVU

The Application Security landscape

Web application vulnerabilities dominate the enterprise threat landscape

Cumulative Count of Web Application Vulnerability Disclosures
1998-2010



- 37% of all new vulnerabilities are in web applications (2011 1H)*
- ~4K new application vulnerabilities reported every year from 2006-2010**

Applications in Development

- In-house development
- Outsourced development

Production Applications

- Developed in house
- Acquired
- Off-the-shelf commercial apps

- Vulnerabilities are spread through a wide variety of applications

Adopt a *Secure by Design* approach to enable you to design, deliver and manage smarter software and services

- Build security into your application development process
- Efficiently and effectively address security defects **before deployment**
- Collaborate effectively between Security and Development
- Provide Management visibility



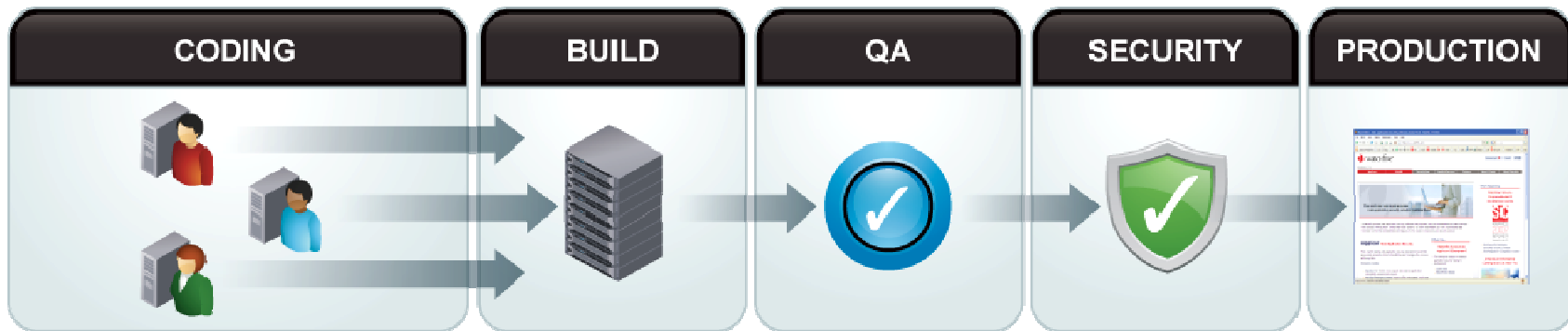
Deliver New Services Faster



Innovate Securely



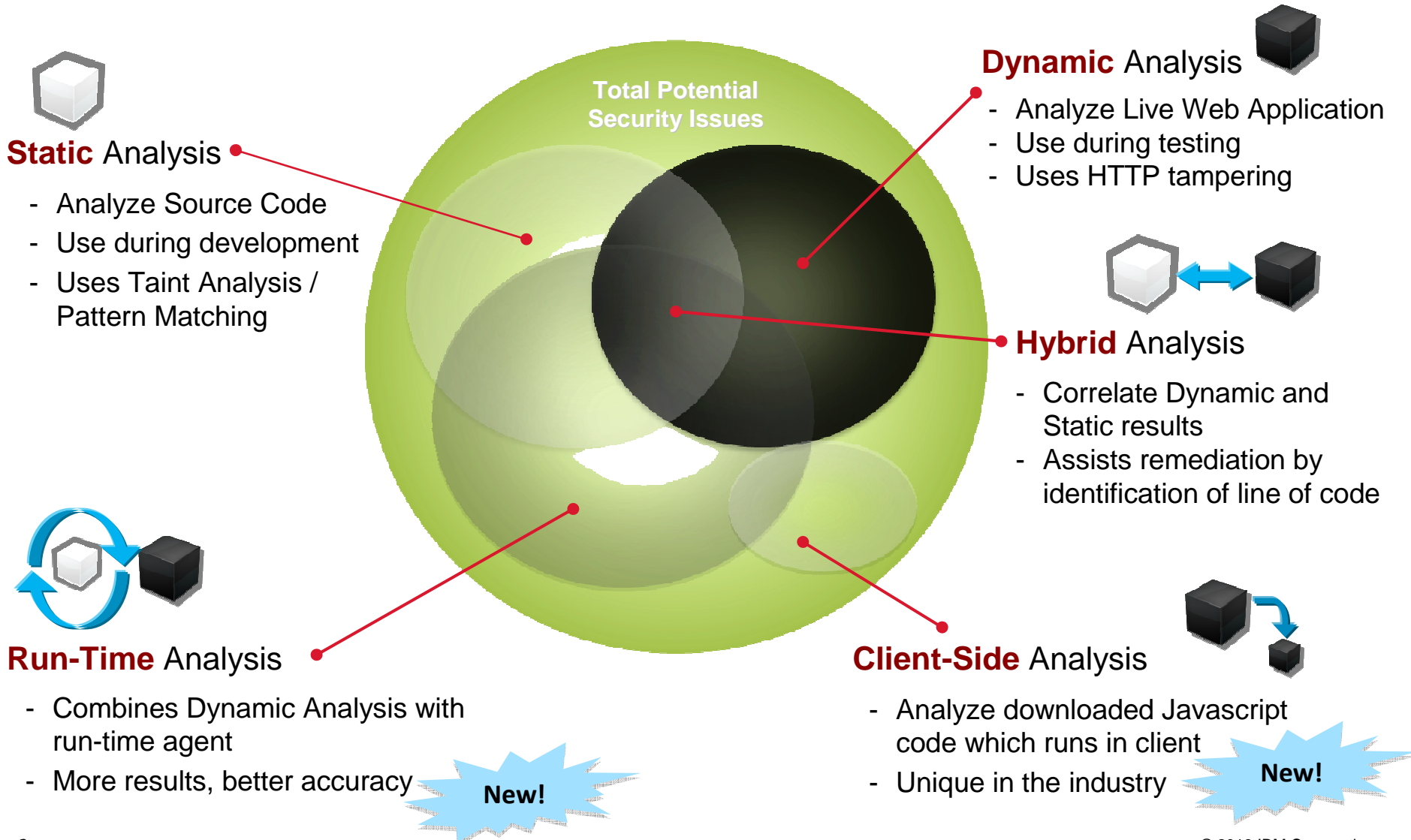
Reduce Costs



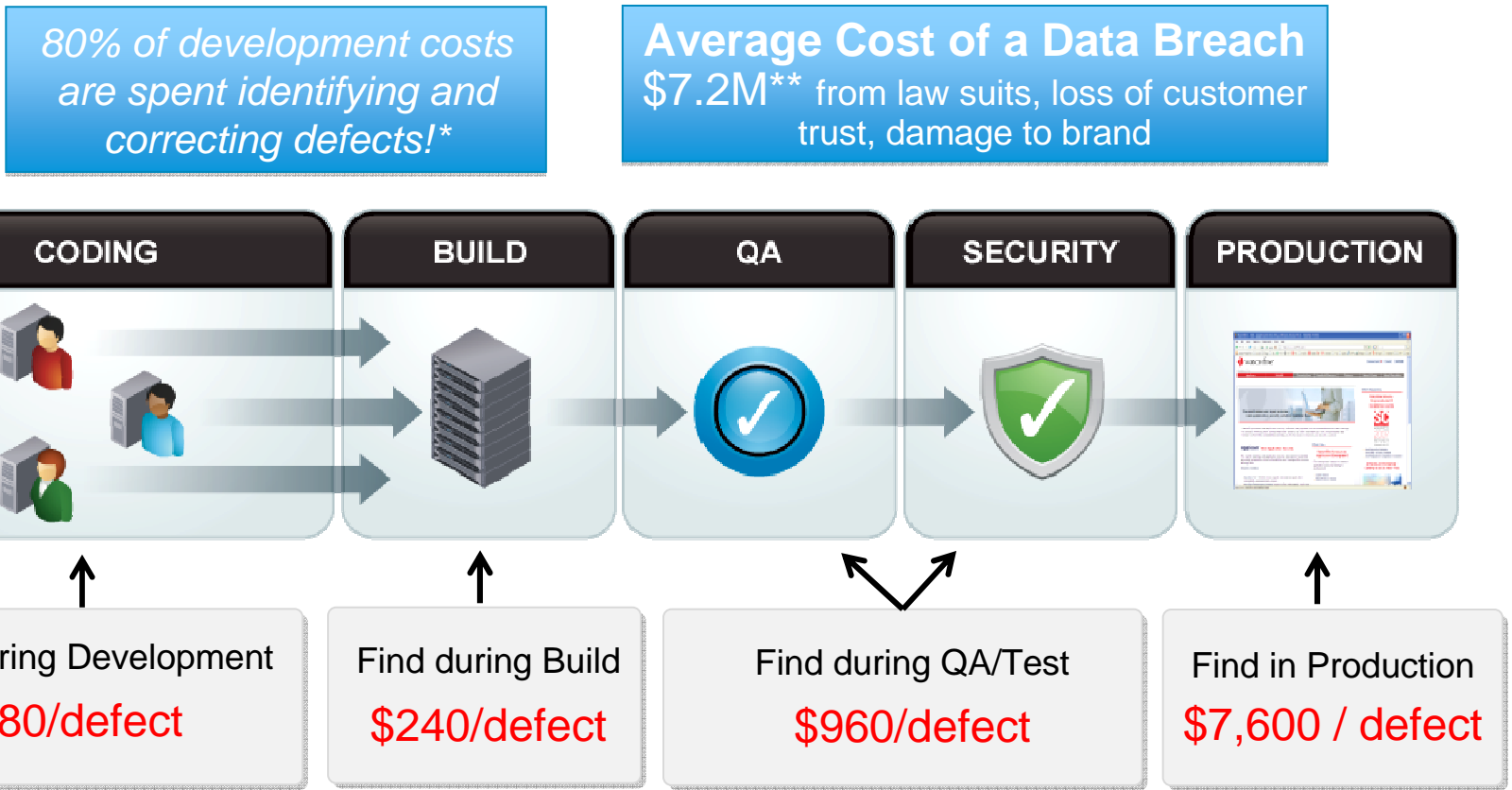
Proactively address vulnerabilities early in the development process



Challenge 1: Finding more vulnerabilities using advanced techniques



Challenge 2: Reducing Costs Through a Secure by Design Approach



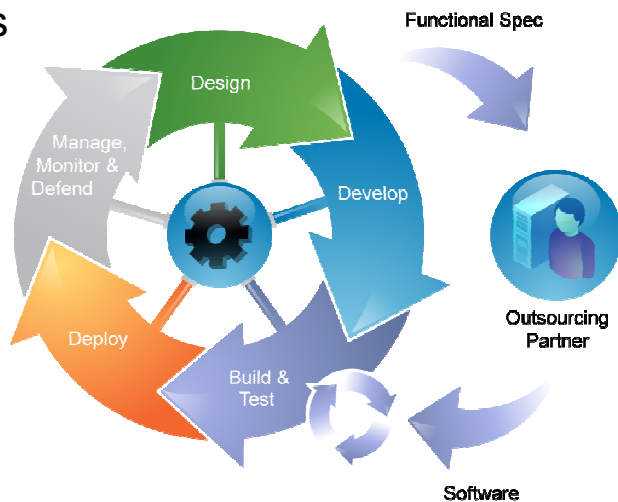
“As financially-motivated attackers have shifted their focus to applications, Web application security has become a top priority. However, the responsibility for web application security cannot rest solely with information security. Enterprises should evaluate how to identify vulnerabilities in Web applications earlier in the development process as transparently as possible using web application security testing products or services.”

Neil MacDonald, Gartner, 12-6-11

Challenge 3: Bridging the Security/Development gap

Break down organizational silos

- Security experts establish security testing policies
- Development teams test early in the cycle
- Treat vulnerabilities as development defects



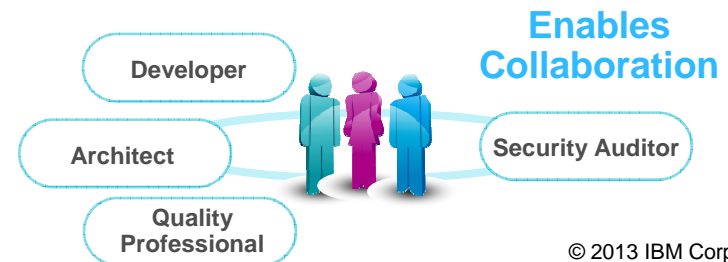
Provide Management Visibility

- Dashboard of application risk
- Enable compliance with regulation-specific reporting



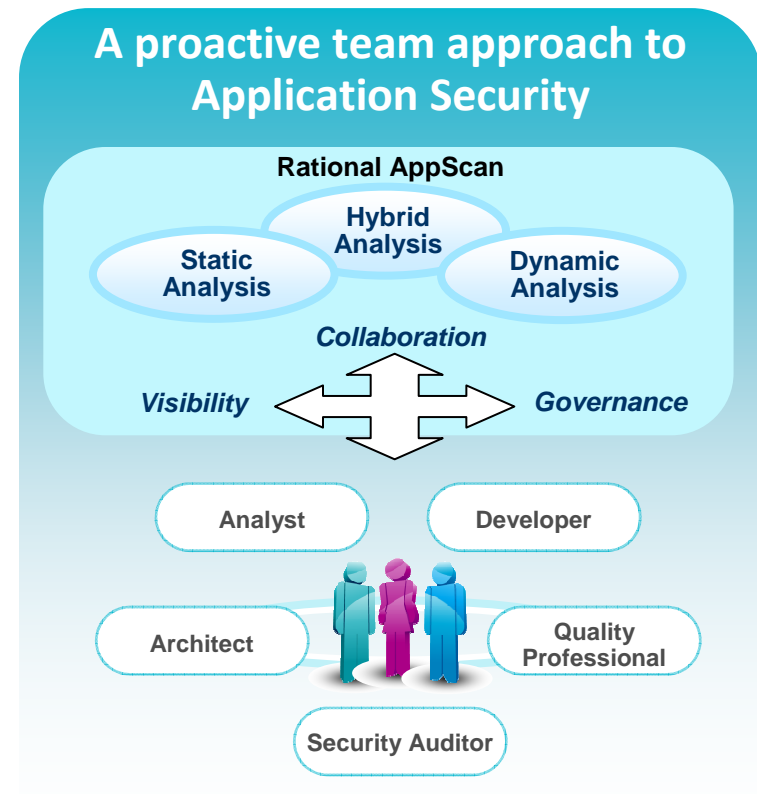
“... we wanted to go to a multiuser web-based solution that enabled us to do concurrent scans and provide our customers with a web-based portal for accessing and sharing information on identified issues.”

Alex Jalso, Asst Dir, Office of InfoSecurity, WVU



Organizations need to take a *proactive approach* to Application Security

- **Embed security testing early** in the development lifecycle to support agile delivery demands
- Bridge the gap between “Security” and “Development” through **joint collaboration and visibility**, enabling regulatory compliance
- Integrate security testing **into the development lifecycle**, through interfaces to development tools



Challenge 4: Controlling Access to Data

IBM Security Policy Manager

Manage and enforce fine-grained entitlement and message security policy management

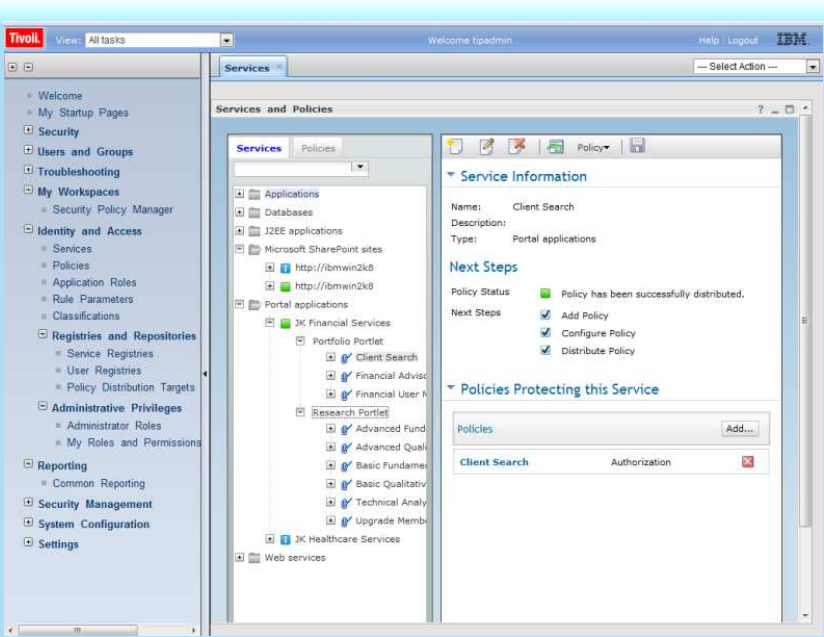
Strengthen application security and data access on a need to know basis

Business Challenge

Protect fine-grained access to data for business critical applications, databases, portals and services

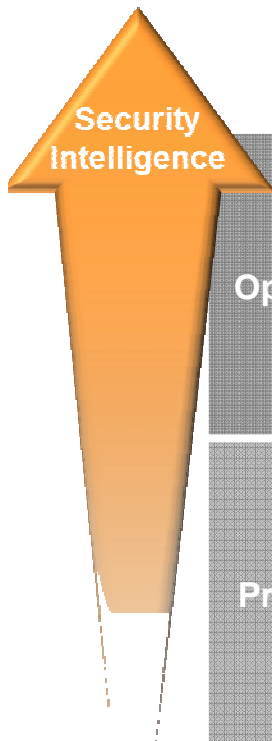
Key solution highlights

- Improved time to value for DataPower deployments with central policy management
- Enforce entitlement policy across application middleware, portals and databases
- Improved scalability for large number of services and policies
- Centralized security policy authoring and distributed enforcement



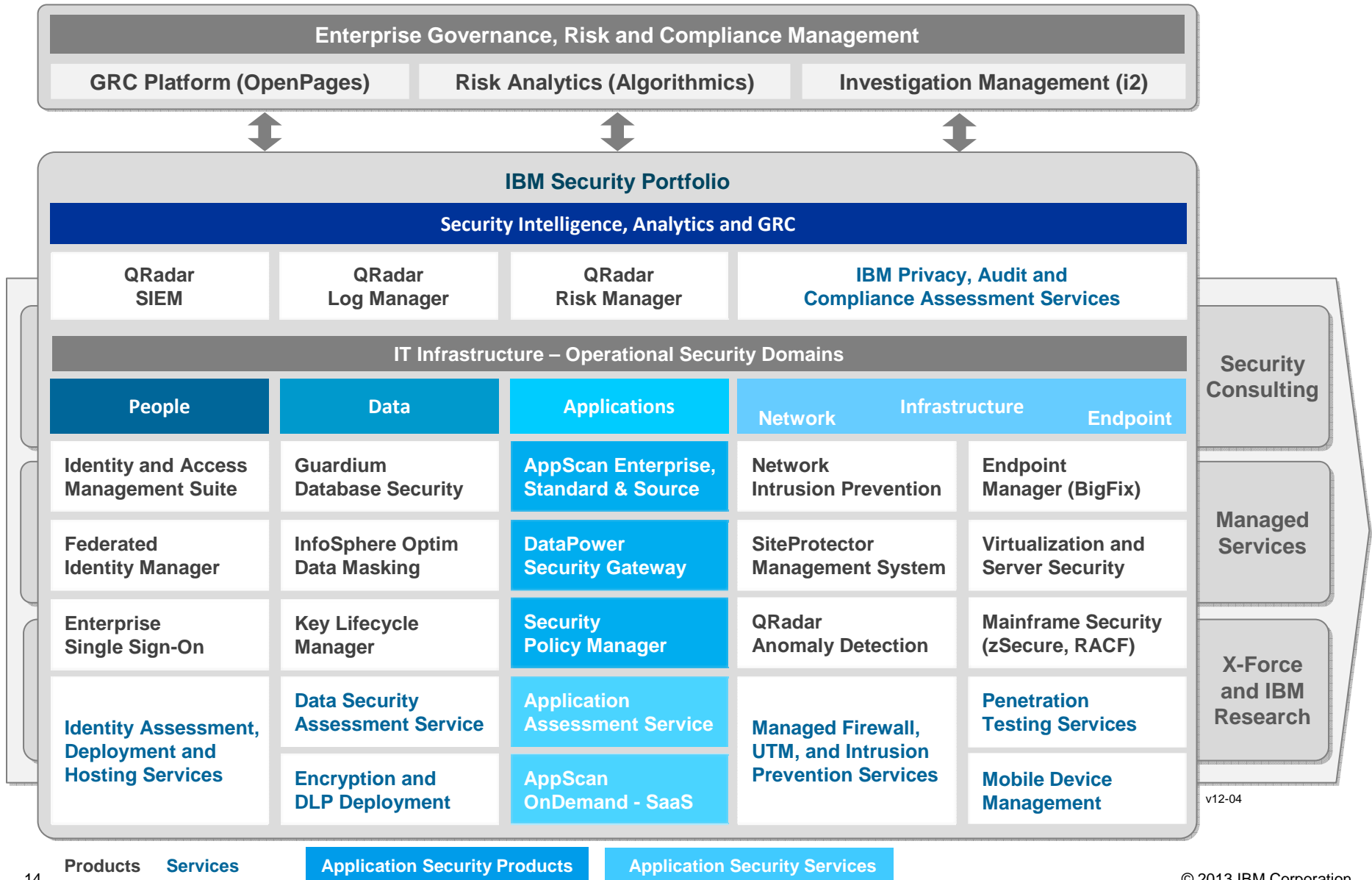
Reduce cost and risk of implementing applications security to address compliance

Helping Organizations Progress in Their Security Maturity



	People	Data	Applications	Infrastructure	Security Intelligence
Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Securing systems	Advanced threat detection Network anomaly detection Predictive risk management
Proficient	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management	Real-time event correlation Network forensics
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus	Log management Compliance reporting

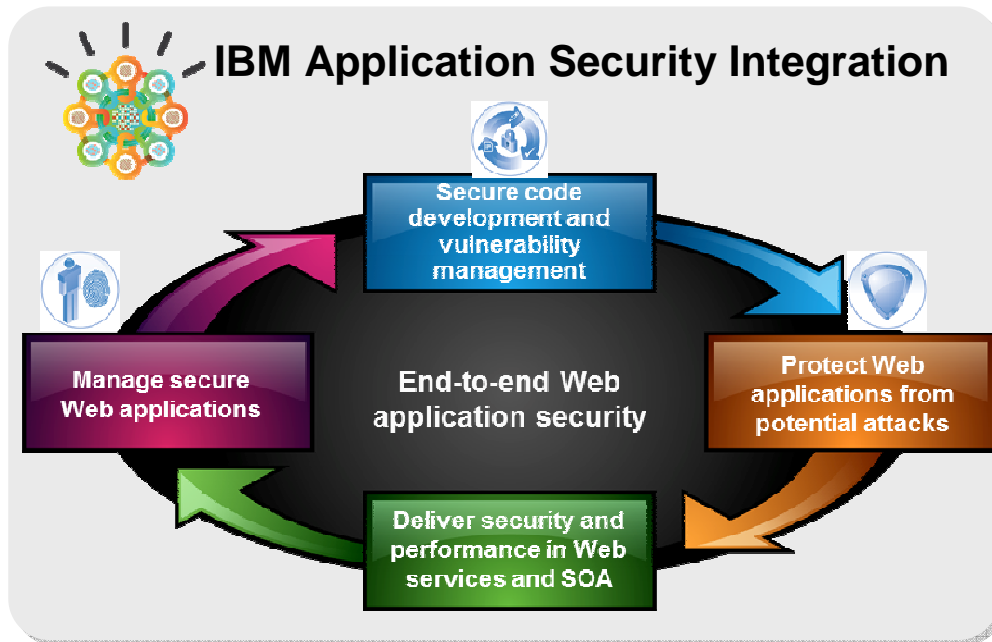
IBM's security product and service portfolio...



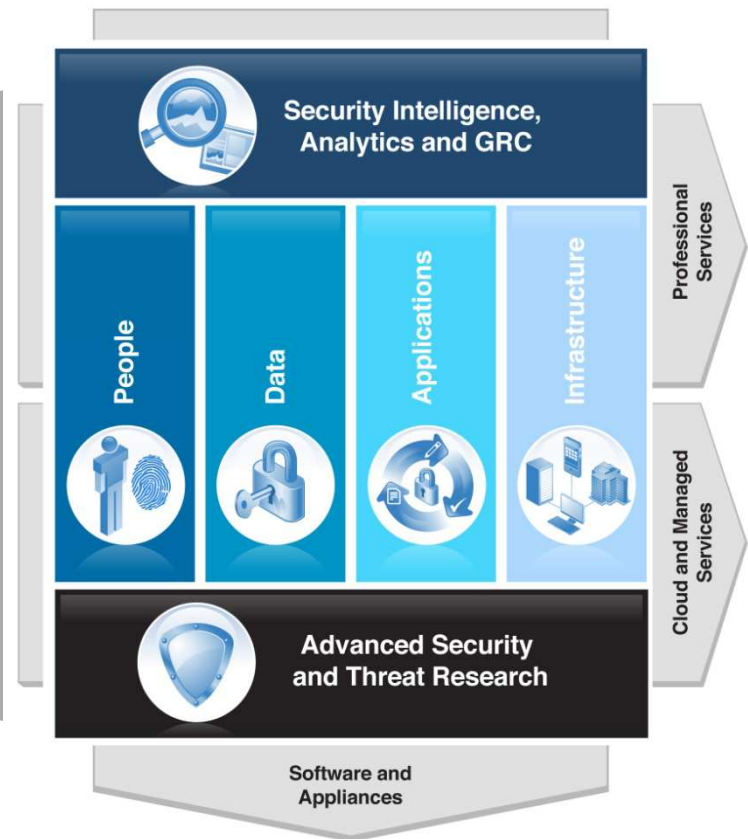
v12-04

Application Security. Think Integrated

Integrate secure development, vulnerability management, network and host protection



IBM Security Framework



Why IBM Security: Breadth, deep expertise, integration

Leadership

- “After doing our research, we determined that IBM was a leader in the field of dynamic application scanning.”
Alex Jalso, Assistant Director, Office of Information Security, WVU
- Identified as a Leader in Gartner SAST Magic Quadrant, December 2010
- Identified as a Leader in Gartner DAST Magic Quadrant, December 2011
- Pioneer of new hybrid analysis techniques, including Correlation, JavaScript Analyzer and GlassBox
- Pioneer of developer-friendly solutions

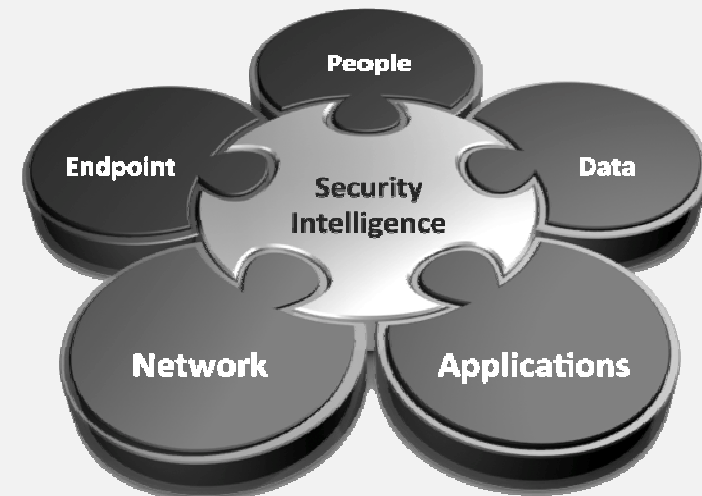
Integration

- Integration with IBM AppScan and SiteProtector to enhance web application security through IPS policy modification from application vulnerability data
- Integrates with IBM Rational development lifecycle solutions to enable collaboration between security and development teams

Expertise

- “We turned to IBM because they offered both the technology leadership and the deep security expertise...”
Marek Hlávka, Chief Security Officer, Skoda Auto

Think Integrated.



ibm.com/security



© Copyright IBM Corporation 2012. 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, 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.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Agenda

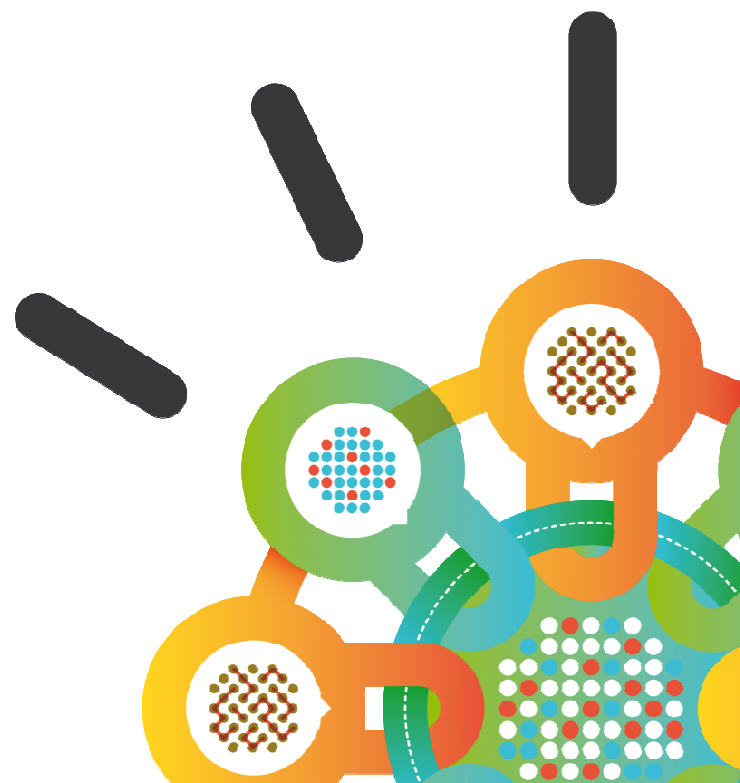
- Welcome and Introductions
- Latest Security trends and 2012 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent threats
- Break
- Managing Application Security
- **From Identity & Access Management to Identity Intelligence**
- Securing your Cloud
- IBM Global Financing

Security Intelligence.
Think Integrated.

IBM Security Strategy

Identity and Access Management

Philip Nye
May 2013

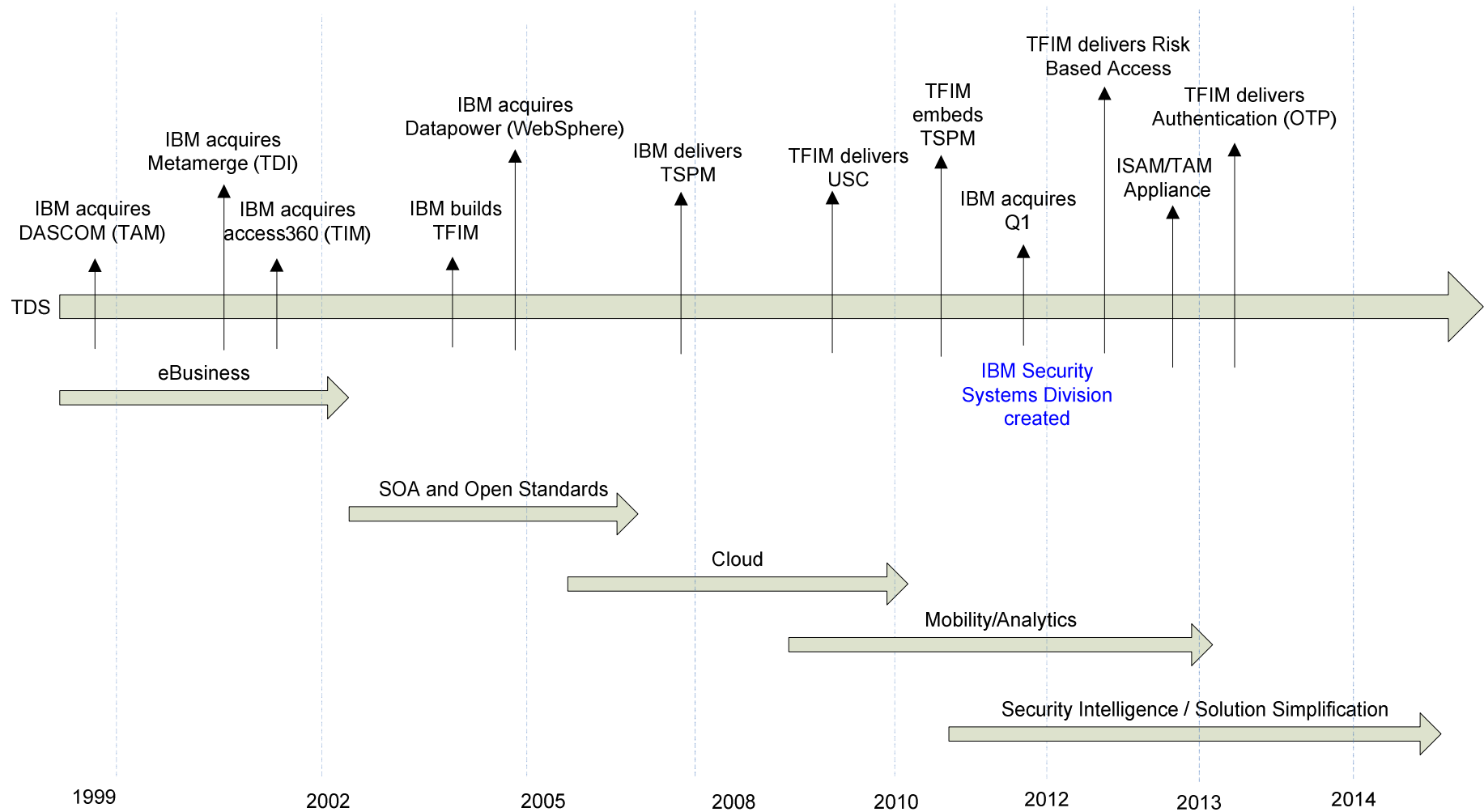


Where am I from? (IBM Security Development Lab)

- Product Development
 - IBM Security Heritage software
 - ISS software/hardware
 - Q1 (integration)
- IBM wide security components
- Integration Factory
- Customer Focussed
 - Lab Services
 - Support
 - SWAT
- Background
 - 1999 acquisition of DASCOS
 - Founded in 1996
 - Strong links to Australian Universities
- Profile
 - 90+ technical staff
 - Design, development, test, project management, documentation, support
 - World class security expertise
 - Only a “short” flight to Africa.



IBM Security Systems portfolio growth - IAM focus



The background is a solid blue color with a pattern of faint, semi-transparent geometric shapes. These shapes include circles, squares, and lines, some of which are arranged in a grid-like pattern, suggesting a digital or technological theme.

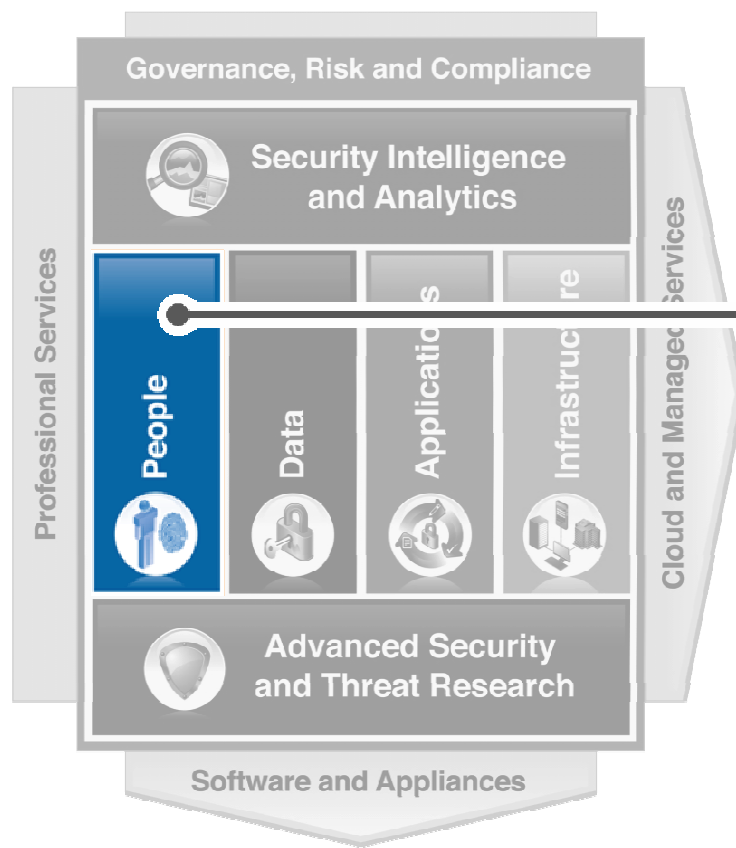
Focusing on People and Access



People

Area of Focus

Manage and extend enterprise identity context across all security domains with end-to-end Identity Intelligence



Portfolio Overview

IBM Security Identity Manager *

- Automate the creation, modification, and termination of user accounts throughout the entire lifecycle
- Identity control including role management and auditing

IBM Security Access Manager Family *

- Automates sign-on and authentication to enterprise web applications and services
- Entitlement management for fine-grained access enforcement

IBM Security zSecure suite *

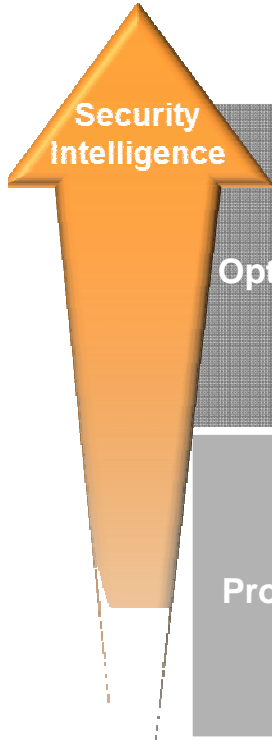
- User friendly layer over RACF to improve administration and reporting
- Monitor, audit and report on security events and exposures on mainframes.

Identity and Access Management

Managing WHO has ACCESS to WHAT



Helping organizations progress in their security maturity



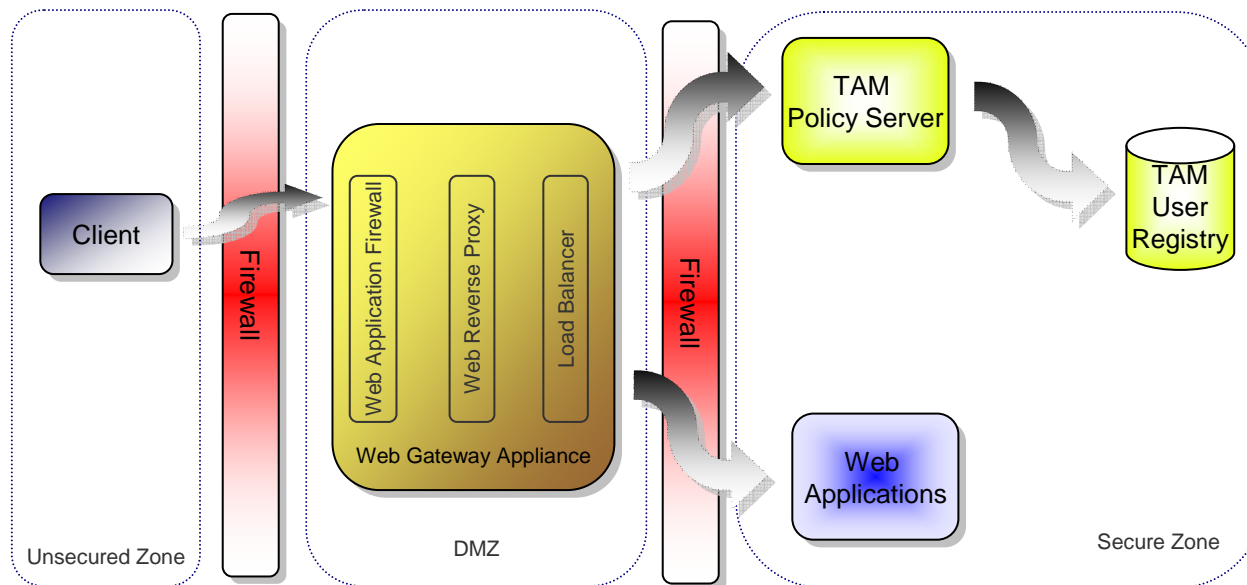
	People	Data	Applications	Infrastructure	Security Intelligence
Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Securing systems	Advanced threat detection Network anomaly detection Predictive risk management
Proficient	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management	Real-time event correlation Network forensics
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus	Log management Compliance reporting

Details of Feature/Function Recent Enhancements

ISAM 7.0 and Appliance

Appliance : Overview

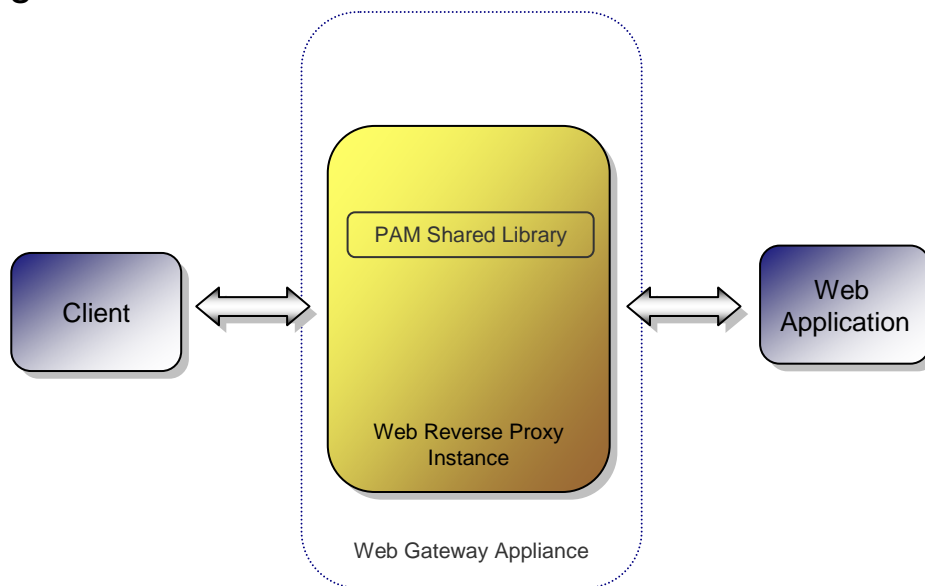
- Provides access control and protection against Web-based threats;
- Combines WebSEAL functionality with:
 - Front-end Load Balancing
 - Web Application Firewall
- Built on ISS appliance technology
- Both Hardware Appliance and Virtual



Appliance: Web Application Firewall (WAF)

- Packet inspection by ISS 'protocol analysis module'
- Integrated into WebSEAL
- Updates managed by the appliance
- Can be configured to protect both request and response
- Default/recommended 'actions' are provided by IBM X-Force
- Actions includes: drop / quarantine / audit / ignore

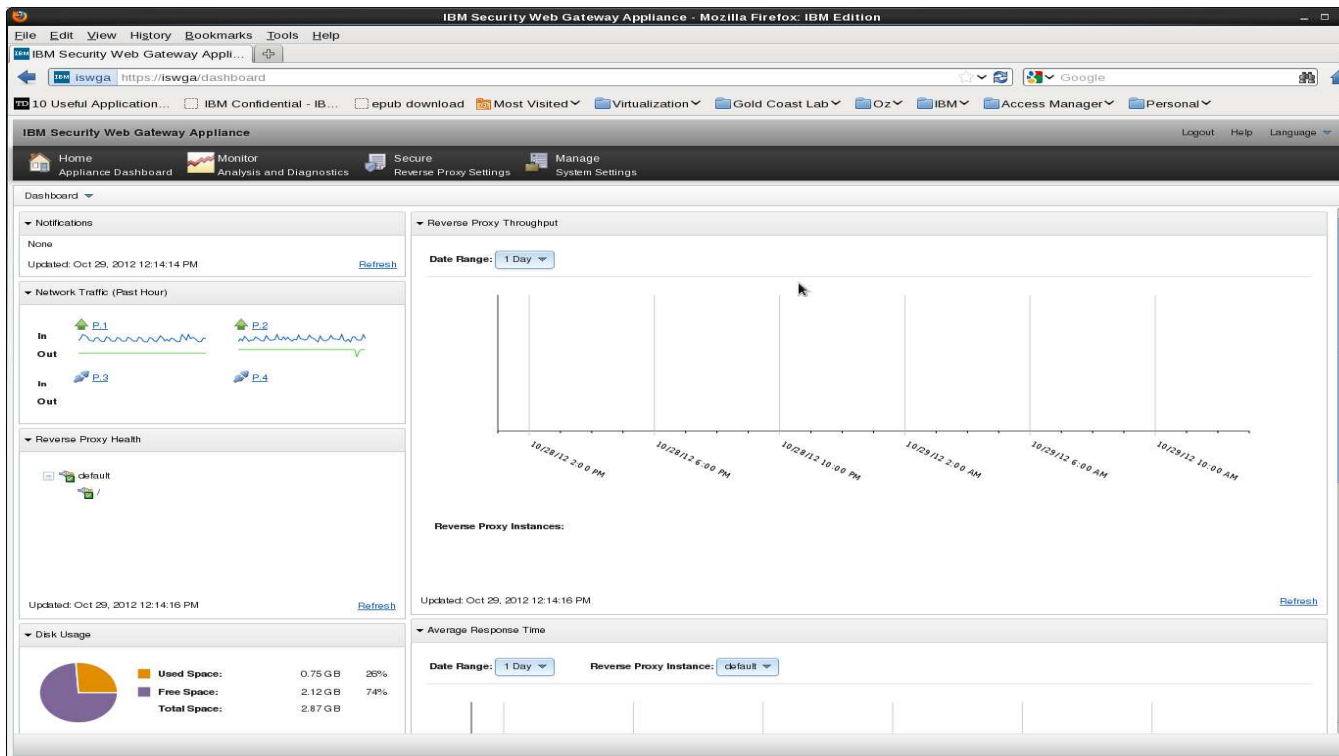
- SQL (Structured Query Language) Injection
- XSS (Cross-site scripting)
- PHP file-includes
- CSRF (Cross-site request forgery)
- Path Traversal
- HTTP Response Splitting
- Forceful Browsing



- Expands security capabilities to meet both compliance requirements and threat evolution.

Appliance : Configuration / Management

- No shell access
- Configuration and Management now performed using:
 - Web management console (aka Local Management Interface – LMI)
 - RESTful Web service
 - Command Line Interface (CLI)



ISAM 7.0 – Web Access Gateway New Features

- 64-bit support
 - Increase in number of threads
 - Increase in number of sessions
- VHJ session sharing
- OAuth v2.0 support
 - In conjunction with TFIM 6.2.2
- Improved Ajax Integration
 - Support for 'robot' pages
 - HTTP header 'macros'
 - JavaScript redirects
- HTTP Transformation Rules
 - Modify request/response based on XSLT
- RPC over HTTP support
 - Microsoft Exchange
- Single sign off to junctioned servers
 - Session timeout and logout events
- Cluster configuration support
 - Builds on v6.1.1 functionality
- Microsoft Office Session Sharing
- Internet Content Adaptation Protocol (ICAP) support
- Improved CSRF protection for WebSEAL pages
- Auditing to a remote syslog server

Risk Based Access & Stronger Authentication

Access using Context



Endpoints:

There are various unique attributes (device fingerprint).
Screen depth/resolution, Fonts, OS, Browser, Browser plug-in, TCP timings



Identity:

Groups, roles, credential attributes, organization, ancestry
(parents, siblings, grandparents)



Environment:

Geographic location, network, local time, IP reputation,
catastrophic event . . . etc



Resource / Action:

The application being requested and what is being done.



Behavior:

Analytics of user historical and current resource usage.
User activity monitoring, specific business activity monitoring

Intelligence in Access - Risk Based Access

- One example for the behavior matcher is using historical login times determine how probable the current login is coming from the actual user.
- The algorithm implemented is the kernel density estimation.
- Administrator configures a probability threshold which the calculated probability needs to be greater than for the matcher to return true.
- Calculation is based off of stored behavior event data.

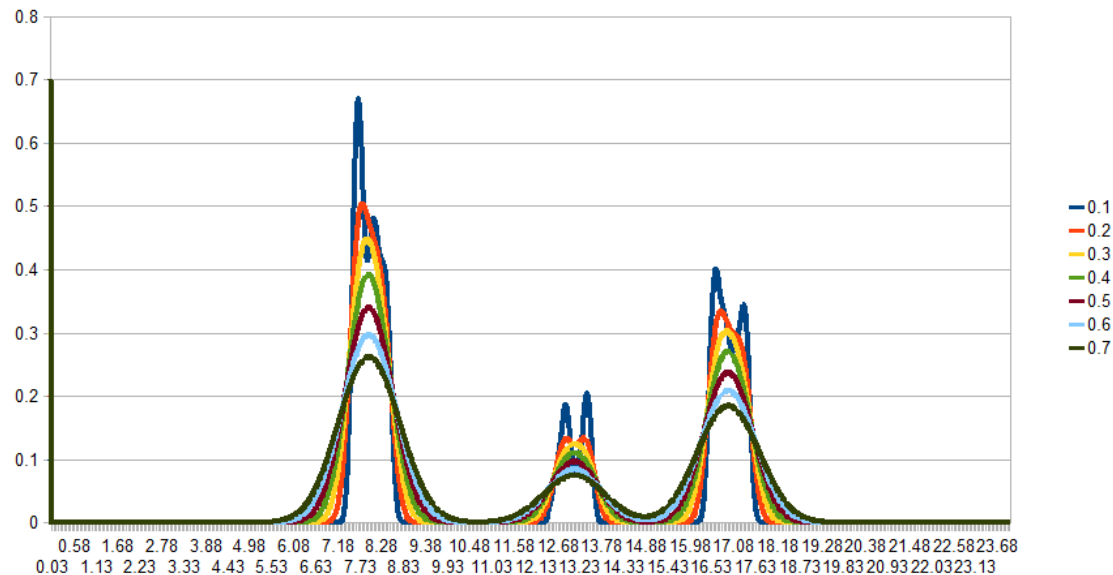
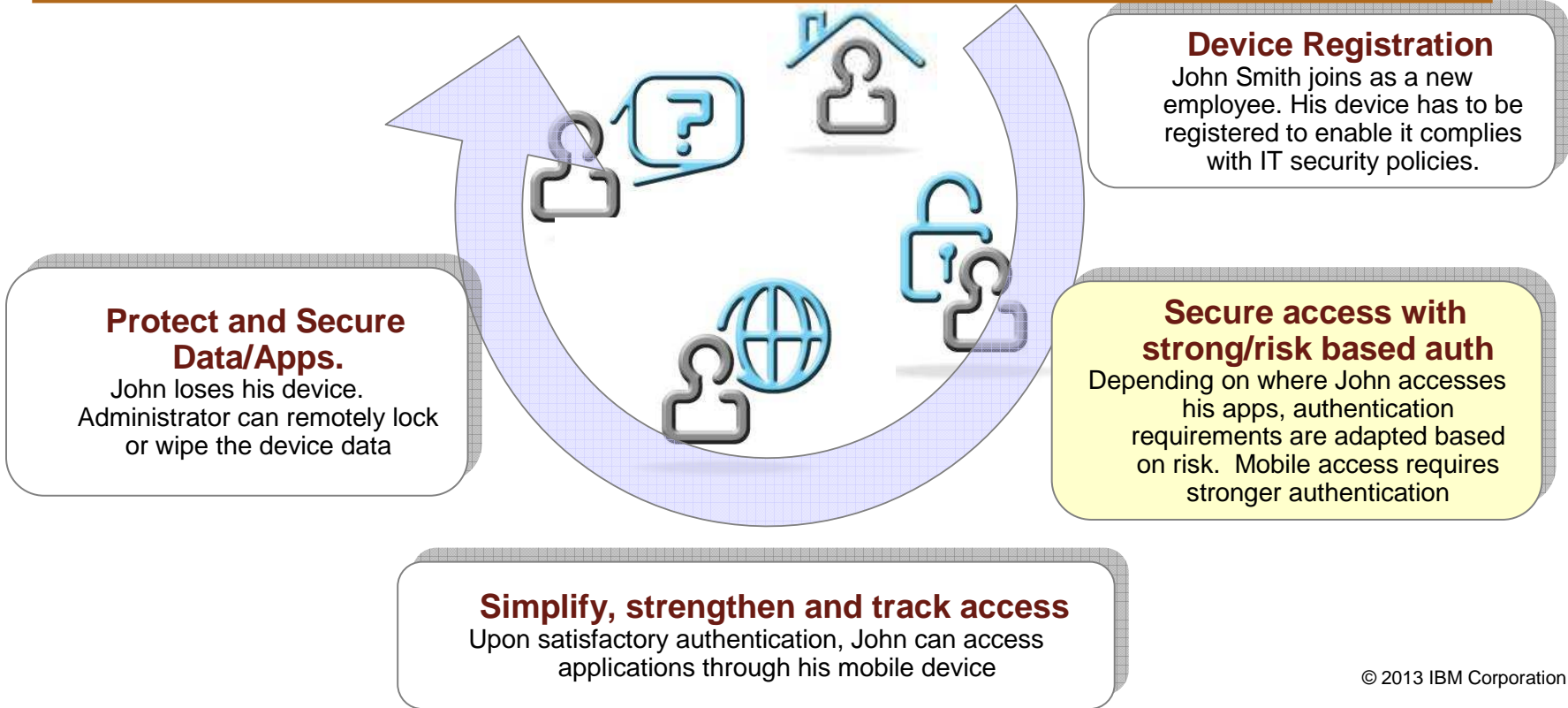


Chart shows that the user has three common login times during a 24 hour period

Access Management must now consider mobility

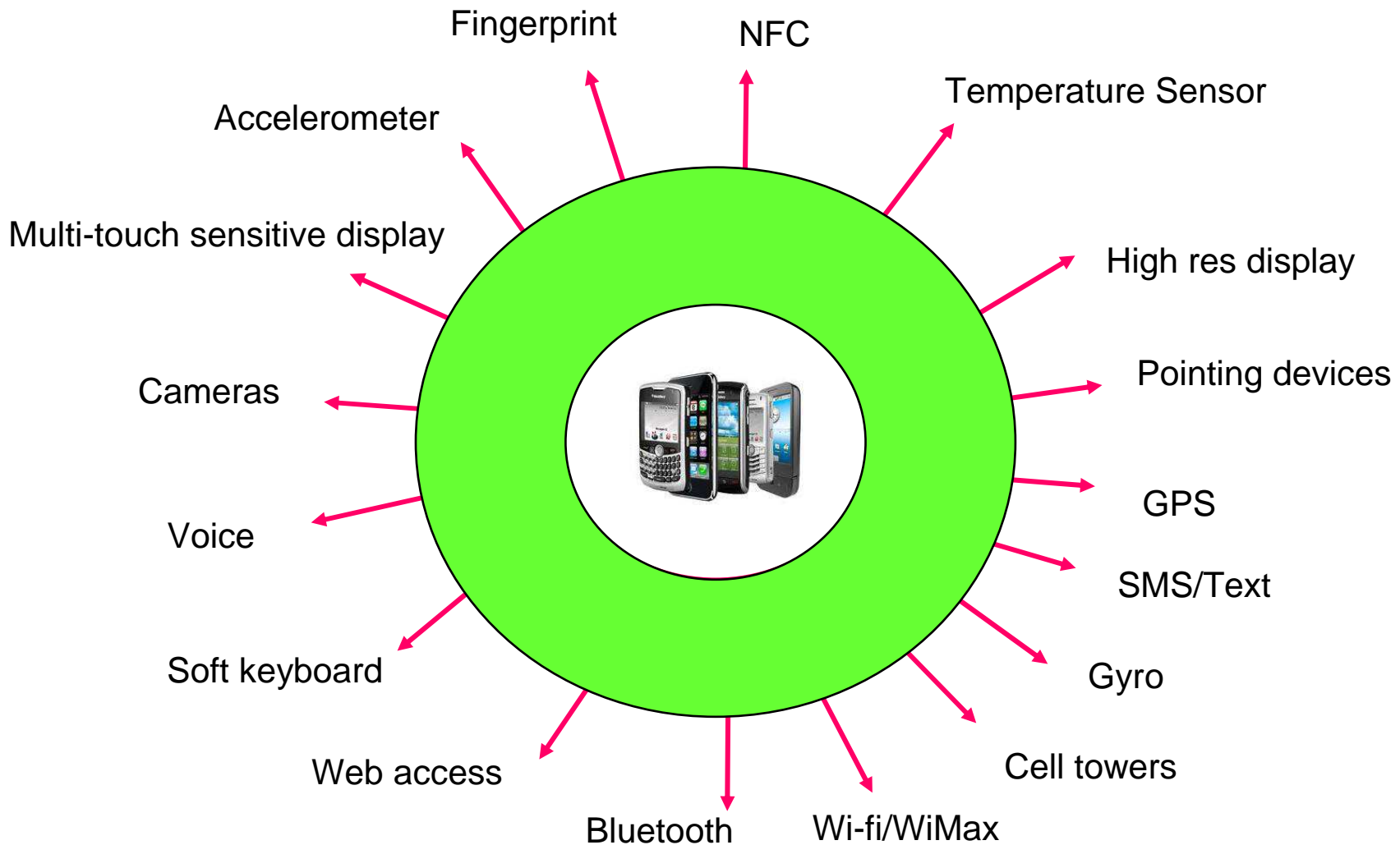
- Users are now demanding access through multiple devices
 - Creates an issue around binding identities to numerous devices with varying levels of security compliance

Who owns the security policies for the device or the application?
How do I authenticate for the IBM apps? How do I authenticate to my banking apps?
I want to be able to play Angry Birds without IBM authentication of the device
How do we make the security appropriate to the application (family?) that I want to access
When I lose the device, how do I handle informing Application Providers?

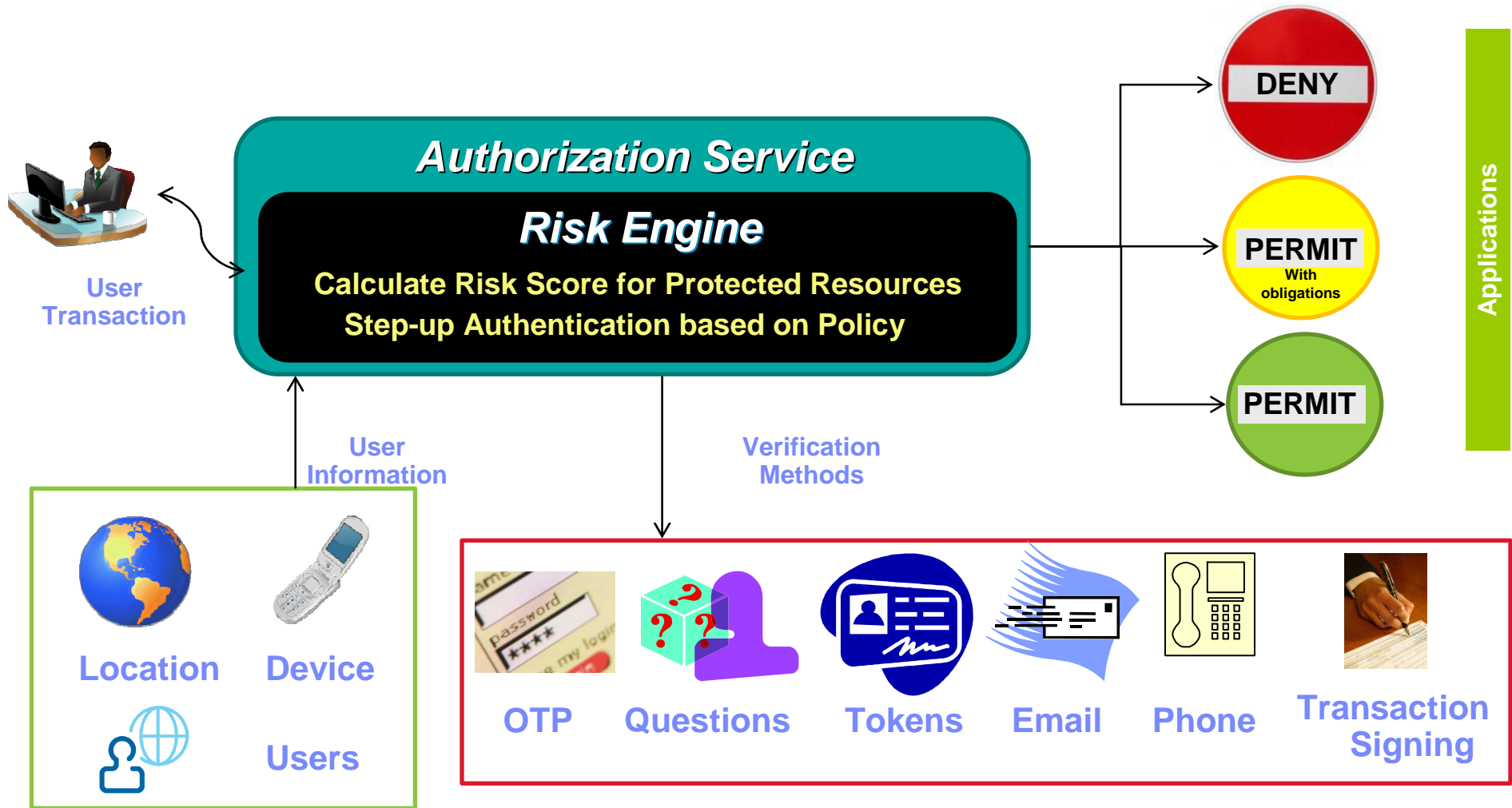


Mobility brings many opportunities

- Context needs to be considered within both authentication and authorization workflows



Architecture Overview

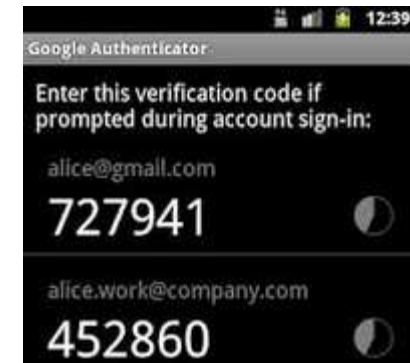


One Time Password – Stronger Authentication

- FIM now has One Time Password
 - Generate an OTP
 - Deliver OTP
 - Validate OTP

- Selective Delivery mechanisms
 - SMS
 - Push Notifications
 - Email
 - Hardware Tokens
 - Software Tokens

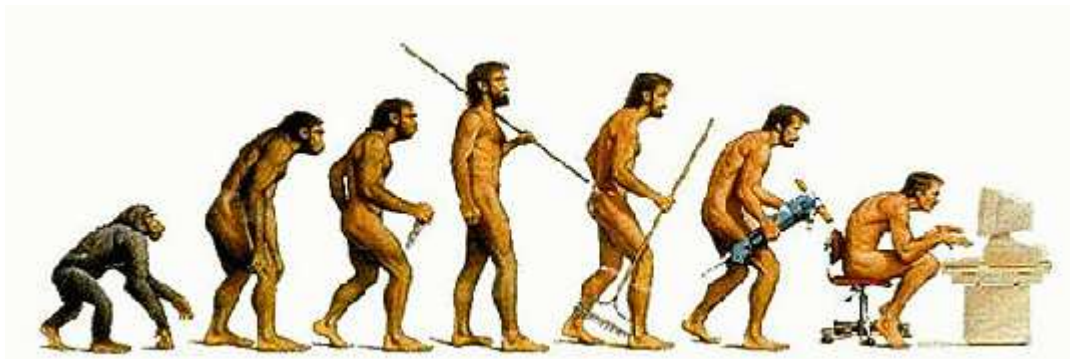
- Works in conjunction with your security policy
 - ISAM Policy
 - Risk Based Access



API-enabled business & Mobile Security

Security for the API-enabled business

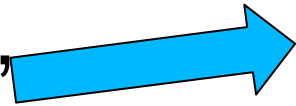
- Driven by mobile and cloud-based applications and the ability to rapidly federate with new partners to quickly solve new scenarios
 - Happens more “on the fly”
- Authorized access to data and API’s is:
 - policy driven by both the organization and the end-user
 - supporting of differing levels of trust
- Enter OAuth for delegated authorization
 - Shown in the demo



No IT → Internal IT → Web 1.0 → Business via API

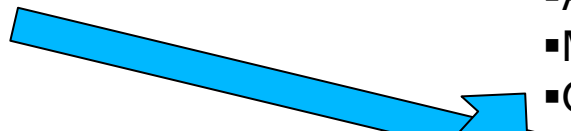
Definition of OAuth

Delegated,
Scoped



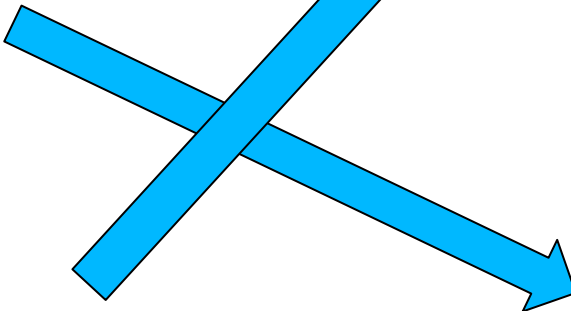
Resource Owner

Authorization



- Business API invocation
- Authentication
- Mobile Apps
- Others

to Resources



for Applications

- User Profile (eg Facebook)
- Web Service (inc AJAX)
- Other Service (eg Twitter)
- Banking API's

Consumer Application
(e.g. web site, mobile app)

Person's Private Resources

User Self Care – Device Management



My inbox
10 unread messages



Future transactions
0 scheduled



My applications
0 applications

10/10/2012 - 04:12 PM **New Device Added: 'Philips iPhone'** [Delete](#) [Preview](#)

My portfolio

Nickname / Type	BSB / Awards	Account number	Account balance	Available funds
Everyday Account	 06 4430	7599 1905	+ \$276.69	+ \$276.69
Home Deposit	 06 4430	1099 7580	+ \$8,800.55	+ \$8,800.55
Holiday	 06 4430	1099 7599	+ \$0.01	+ \$0.01
MasterCard	  Awards	1652 6244 8379 5353	- \$56.37	+ \$3,943.63
Shares		4152		

My quick links

-  [Manage my accounts](#)
-  [Statements](#)
-  [Foreign exchange rates](#)
-  [My contact details](#)
-  [Pay bill](#)

 [Customise](#)

My Devices



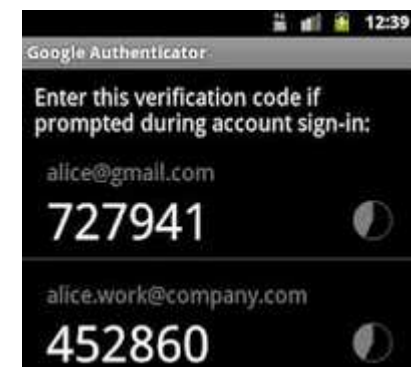
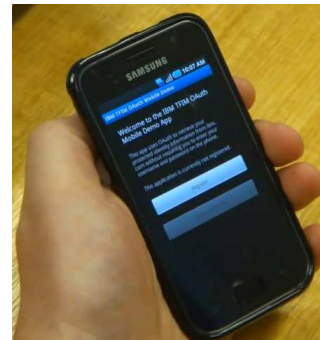
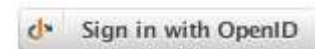
[Philips iPhone](#)

[Edit](#) [Revoke](#)

Want to see more?

Demos Available:

- Federated Single Sign On
- Bring your own ID – Using Social Media to connect to your organisation
- OAuth
 - Browser based
 - Mobile application based
- One time password
 - Email
 - SMS
 - Push Notification
 - Software Tokens



ibm.com/security



© Copyright IBM Corporation 2012. 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, 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.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

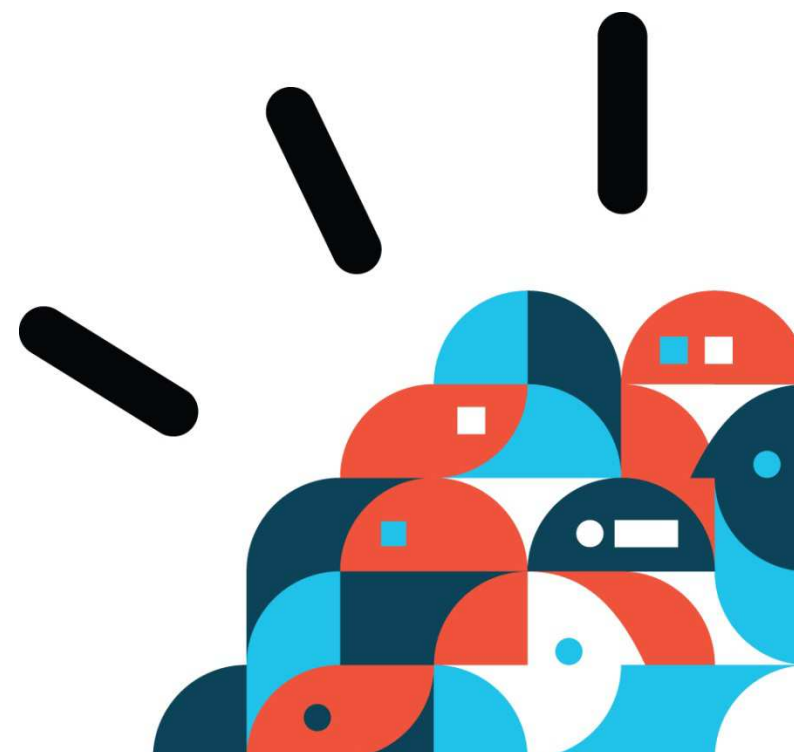
Agenda

- Welcome and Introductions
- Latest Security trends and 2012 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent threats
- Break
- Managing Application Security
- From Identity & Access Management to Identity Intelligence
- **Securing your Cloud**
- IBM Global Financing

Rethink IT.
Reinvent Business.
Smart, Secure and Ready for Business

IBM SmartCloud Security

S. Rohit
rohits@sg.ibm.com



Agenda

- Customer Feedback
- Cloud Security
- Cloud Adoption Patterns
- IBM Cloud Security Capabilities
- Summary and Resources

What our customers are saying

"Cloud providers need to really address corporate governance and risk management if cloud is going to be a core component of our IT infrastructure"

"The concern is not so much about security as it is about transparency. You can't manage what you can't see"

"The business case and TCO is more of a concern over security, the issue is making security part of the discussion early enough"

"Data level security is the biggest concern, where my data, who has access to the data, when was the data accessed, and how to support forensics in the event something has gone wrong"

Security and Privacy Expectations

Traditional IT In the Cloud



Cloud computing tests the limits of security operations and infrastructure

Security and Privacy Domains

- People and Identity
- Data and Information
- Application and Process
- Network, Server and Endpoint
- Physical Infrastructure
- Governance, Risk and Compliance



To cloud

- Multiple Logins, Onboarding Issues
- Multi-tenancy, Data Separation
- External Facing, Quick Provisioning
- Virtualization, Network Isolation
- Provider Controlled, Lack of Visibility
- Audit Silos, Compliance Controls

In a cloud environment, access expands, responsibilities change, control shifts, and the speed of provisioning resources and applications increases - **greatly affecting all aspects of IT security.**

IBM Point of View: Cloud can be made secure for business

As with most new technology paradigms, **security concerns surrounding cloud computing** have become the most widely talked about inhibitor of widespread usage.

To gain the **trust** of organizations, cloud services must deliver security and privacy expectations that meet or exceed what is available in traditional IT environments.

The same way transformational technologies of the past **overcame concerns** – PCs, outsourcing, the Internet.



Agenda

- Customer Feedback
- **Cloud Security**
- Cloud Adoption Patterns
- IBM Cloud Security Capabilities
- Summary and Resources

Different cloud deployment models also change the way we think about security



Private cloud

On or off premises cloud infrastructure operated solely for an organization and managed by the organization or a third party



Hybrid IT

Traditional IT and clouds (public and/or private) that remain separate but are bound together by technology that enables data and application portability



Public cloud

Available to the general public or a large industry group and owned by an organization selling cloud services.



Changes in Security and Privacy

- Customer responsibility for infrastructure
- More customization of security controls
- Good visibility into day-to-day operations
- Easy to access to logs and policies
- Applications and data remain "inside the firewall"

- Provider responsibility for infrastructure
- Less customization of security controls
- No visibility into day-to-day operations
- Difficult to access to logs and policies
- Applications and data are publically exposed

Minimizing the risks of cloud computing requires a strategic approach

Define a cloud strategy with security in mind

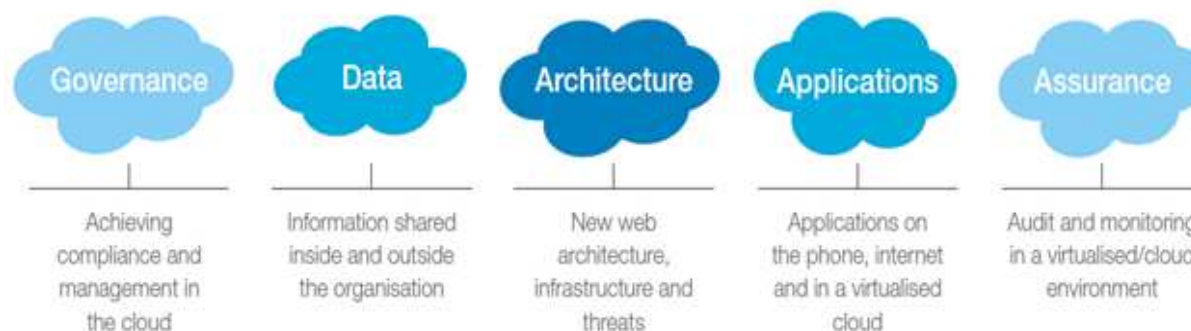
- Identify the different workloads and how they need to interact.
- Which models are appropriate based on their security and trust requirements and the systems they need to interface to?

Identify the security measures needed

- Using a methodology such as the IBM Security Framework allows teams to measure what is needed in areas such as governance, architecture, applications and assurance.

Enabling security for the cloud

- Define the upfront set of assurance measures that must be taken.
- Assess that the applications, infrastructure and other elements meet the security requirements, as well as operational security measures.



Our approach to delivering cloud security aligns with each phase of a clients project or initiative



Design

Establish a cloud strategy and implementation plan to get there.



Deploy

Build cloud services, in the enterprise and/or as a cloud services provider.



Consume

Manage and optimize consumption of cloud services.

IBM Cloud Security Approach

Secure by Design

Focus on building security into the fabric of the cloud.

Workload Driven

Secure cloud resources with innovative features and products.

Service Enabled

Govern the cloud through ongoing security operations and workflow.

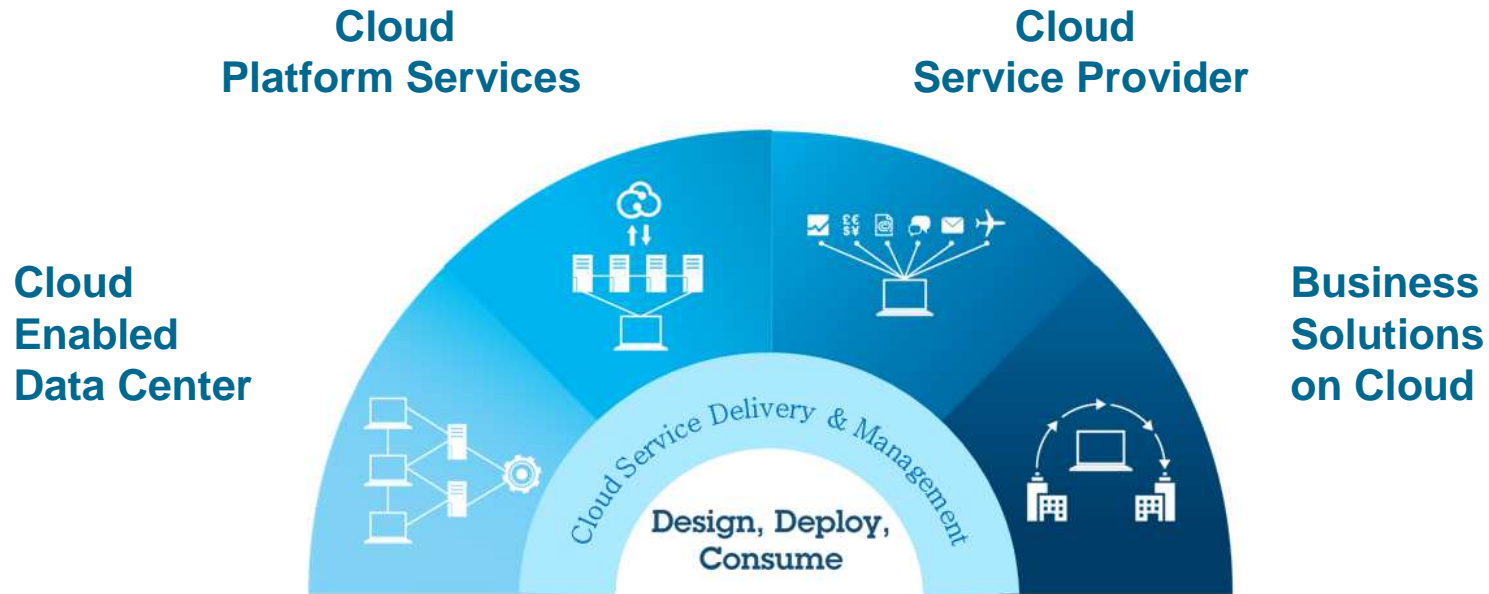
Example security capabilities

- | | | |
|---|--|--|
| <ul style="list-style-type: none"> ▪ Cloud security roadmap ▪ Secure development ▪ Network threat protection ▪ Server security ▪ Database security | <ul style="list-style-type: none"> ▪ Application security ▪ Virtualization security ▪ Endpoint protection ▪ Configuration and patch management | <ul style="list-style-type: none"> ▪ Identity and access management ▪ Secure cloud communications ▪ Managed security services |
|---|--|--|

Agenda

- Customer Feedback
- Cloud Security
- **Cloud Adoption Patterns**
- IBM Cloud Security Capabilities
- Summary and Resources

IBM SmartCloud Security: One Size Does Not Fit All



Different security controls are appropriate for different cloud needs – the challenge becomes one of integration, coexistence, and recognizing what solution is best for a given workload

IBM is a proven leader in delivering best in class solutions and services for all types of clouds

Each pattern has its own set of key security concerns

<p>Infrastructure as a Service (IaaS): Cut IT expense and complexity through cloud data centers</p>	<p>Platform-as-a-Service (PaaS): Accelerate time to market with cloud platform services</p>	<p>Innovate business models by becoming a cloud service provider</p>	<p>Software as a Service (SaaS): Gain immediate access with business solutions on cloud</p>
<p>Cloud Enabled Data Center</p>	<p>Cloud Platform Services</p>	<p>Cloud Service Provider</p>	<p>Business Solutions on Cloud</p>
<p><i>Integrated service management, automation, provisioning, self service</i></p>	<p><i>Pre-built, pre-integrated IT infrastructures tuned to application-specific needs</i></p>	<p><i>Advanced platform for creating, managing, and monetizing cloud services</i></p>	<p><i>Capabilities provided to consumers for using a provider's applications</i></p>
<p>Key security focus: Infrastructure and Identity</p> <ul style="list-style-type: none"> ▪ Manage datacenter identities ▪ Secure virtual machines ▪ Patch default images ▪ Monitor logs on all resources ▪ Network isolation 	<p>Key security focus: Applications and Data</p> <ul style="list-style-type: none"> ▪ Secure shared databases ▪ Encrypt private information ▪ Build secure applications ▪ Audit and compliance reporting 	<p>Key security focus: Data and Compliance</p> <ul style="list-style-type: none"> ▪ Isolate cloud tenants ▪ Policy and regulations ▪ Manage security operations ▪ Build compliant data centers ▪ Offer backup & resiliency 	<p>Key security focus: Compliance and Governance</p> <ul style="list-style-type: none"> ▪ Harden applications ▪ Securely federate identity ▪ Deploy access controls ▪ Encrypt communications ▪ Manage application policies
<p>Security Intelligence – threat intelligence, user activity monitoring, real time insights</p>			

IaaS Business Drivers and Requirements

IaaS Business Drivers

- Use cloud infrastructure with confidence that they're secure, compliant, and meet regulatory requirements
- Leverage existing investment & extend current infrastructure to implement security for virtual infrastructure
- Ease of Use - Automation of security steps to provide out-of-the-box capabilities for cloud
- Maintain service level compliance, accuracy, repeatability and traceability for the cloud environment

Security Requirements

Identity & Access Management

- Provide users single sign on to the applications
- Manage datacenter identities and securely connect users to the cloud (Authentication & Authorization). Provide role based access to cloud resources - Image library, Storage
- Provision and Manage user ids on the cloud resources (for e.g., VMs)
- Manage Confidentiality & integrity of the storage, images and meta-data associated with the master image.

Protect Virtual Infrastructure

- Secure and protect the virtual infrastructure (VM instances, hypervisors) as per IT Security Policy.

Endpoint Management

- Manage patches for hypervisors, virtual machines (offline & online), VM Templates (Images)

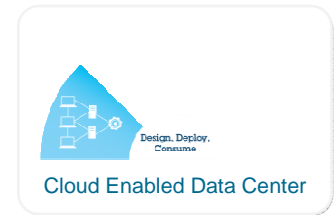
Security Information & Event Management

- Maintain audit logs for virtual infrastructure compliance and audit readiness
- Provide visibility into virtual Infrastructure
- Patch Management

Automation

- Integrate with existing security capabilities and provide automation for identity and access management, end point management and log management and visibility into the cloud infrastructure.

IBM example - securing the cloud for service agility and assurance



Helping clients ensure their cloud services are secure and reliable.

Business challenge

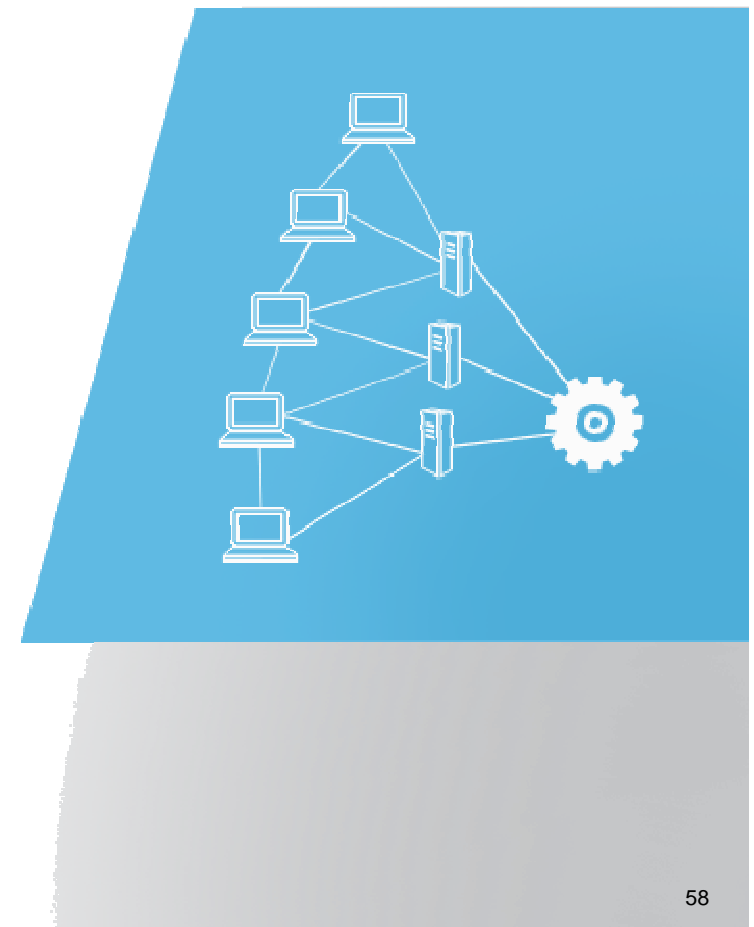
Deploy applications to the cloud with confidence that they're secure, compliant, and meet regulatory requirements.

Key security requirements

- **Identity and Access Control**
securely connect users to the cloud
- **Virtualization Security**
protection for the virtual infrastructure
- **Image and Patch Management**
keep cloud resources up-do-date and compliant

IBM Security Solutions

- **Federated Identity Manager**
- **Virtual Server Protection for VMware**
- **Tivoli Endpoint Manager**



PaaS Securing Platform as a Service Cloud

High Level Business Drivers



Key Business Drivers

- Key Security Focus on Application and Data including securing shared databases, encrypting private information, and keeping audit trail.
- Leverage existing investment & extend current infrastructure to implement security for virtual Platform
- Ease of Use - Automation of security steps to provide out-of-the-box capabilities for cloud
- Maintain service level compliance, accuracy, repeatability and traceability for the cloud environment

Approaches

Loosely Couple Security Management:

- Leverage existing investments and extend the current security infrastructure to manage the PaaS environment.
- Extend existing investment to add necessary capabilities to secure the cloud.

Integrate Security Management

- Provide an out of the box a complete set of security capabilities.
- Capabilities are delivered as a set of patterns within a PaaS offering.

IBM example - security for a hosted cloud provider

Provide best-in-class security services through a cloud hosting infrastructure.



Business challenge

Increase the availability of information across the program and reduce the amount of effort spent maintaining existing security logic and infrastructure.

Key security requirements

- *Strengthen security efforts with a more versatile solution*
- *Shorten the deployment cycle for new customers*
- *Reduce hardware costs and energy use*

IBM security solutions

- **IBM Security Network Intrusion Prevention System**
- **IBM Virtualized Network Security Platform**
- **IBM Managed Security Services**



IBM example - Securing access to public clouds

Secure, worldwide access to Software as a Service applications.



Business challenge

Client required secure access using a centralized identity management solution to public SaaS applications – including Google Apps and Salesforce.com.

Key security requirements

- *Strong authentication solution for secure access to the cloud infrastructure*
- Provision and de-provision of users in the cloud providers registry

IBM security solutions

- **Federated Identity Manager**
- **Identity Manager**

} Hosted in an IBM environment

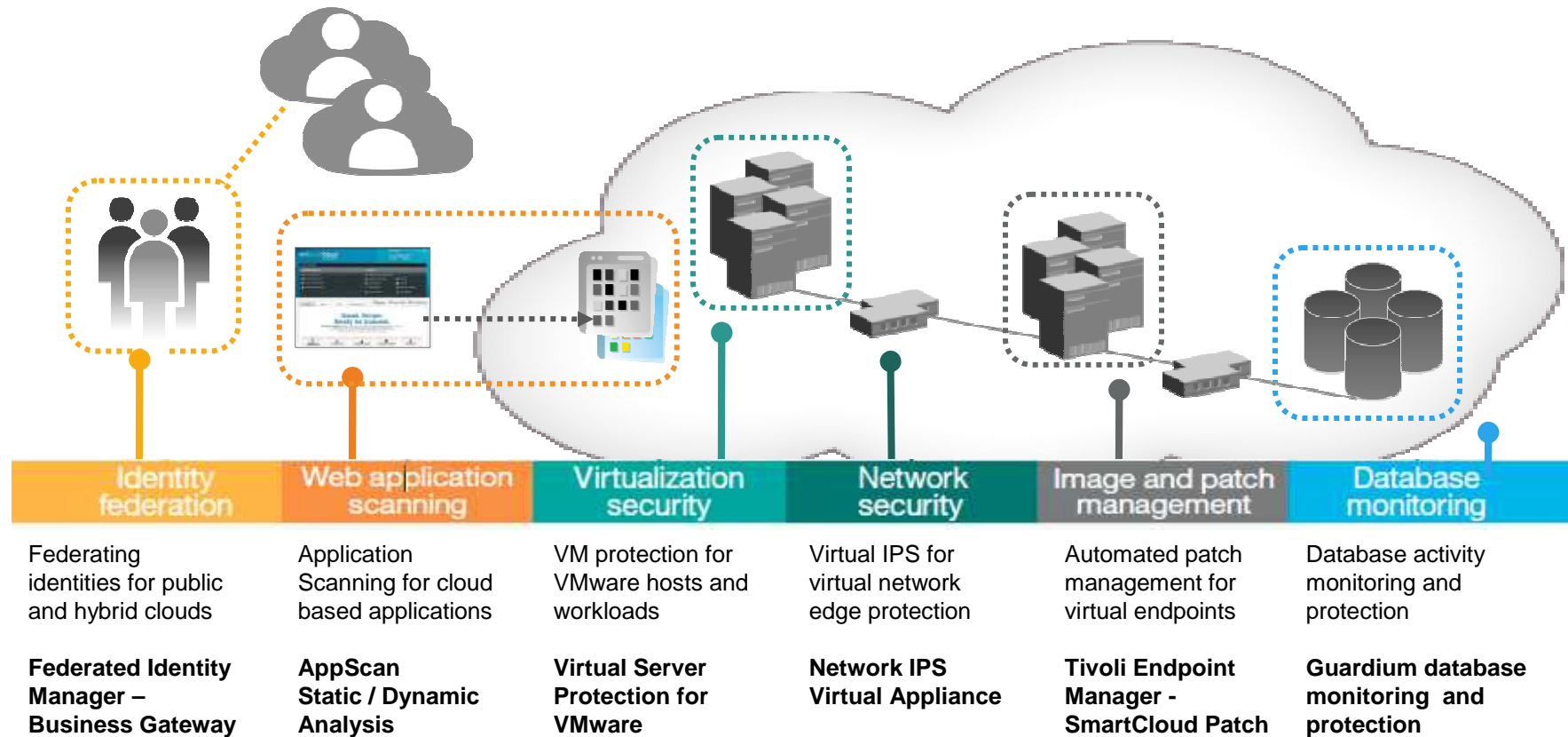
French Energy Company



Agenda

- Customer Feedback
- Cloud Security
- Cloud Adoption Patterns
- **IBM Cloud Security Capabilities**
- Summary and Resources

Securing the cloud today with products from IBM Security Systems



Security Intelligence and Analytics

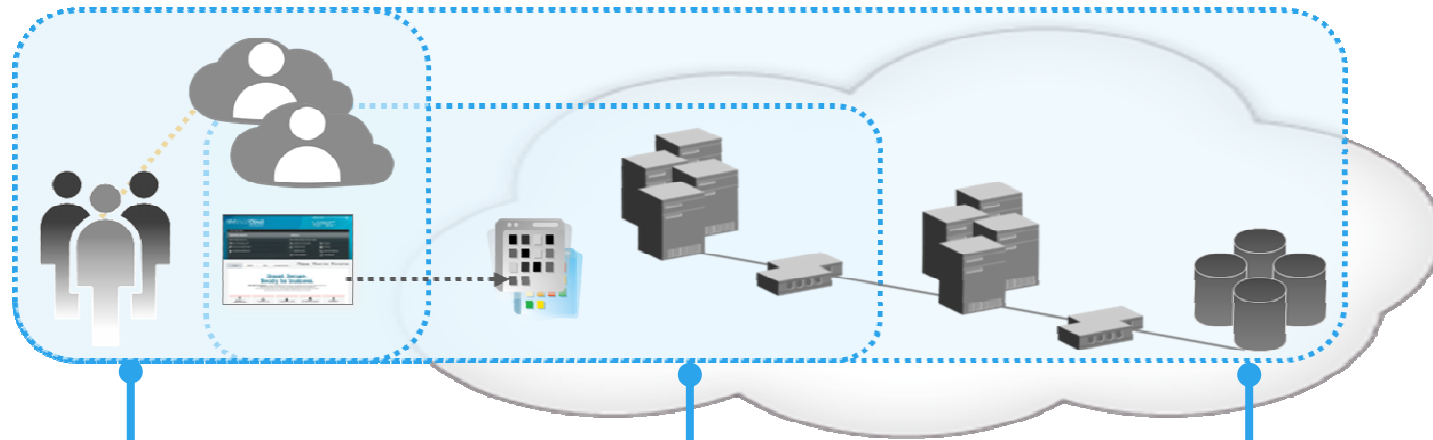
QRadar Security Intelligence Platform

IBM won Best Cloud Security Solutions Company
Honored in the U.S.

Creating a secure hybrid private cloud with FIM / VSP

Built a cloud-based, endpoint management service with TEM

SmartCloud Security Capabilities*



SmartCloud Security Identity Protection

Administer, secure, and extend identity and access to and from the cloud

- IBM Security Identity Manager
- IBM Security Access Manager
- IBM Security Federated Identity Manager - Business Gateway

SmartCloud Security Application Protection

Build, test and maintain secure cloud applications

- IBM AppScan Standard
- IBM AppScan OnDemand

SmartCloud Security Threat Protection

Prevent advanced threats with layered protection and analytics

- IBM QRadar SIEM (SmartCloud Audit)
- IBM Security Network IPS
- IBM Virtual Server Protection
- IBM Endpoint Manager (SmartCloud Patch)

Cloud Enabled Data Center

Dev Ops Cloud

Virtualization Optimization
Cloud Enabled Data Center

Managed Service Providers (MSP)



Security as a Service: IBM Security Services from the Cloud



NEW !! 2012 Fall Announcements for Cloud Security



"Besides the cost reduction, one major advantage is that we will be able to offer cloud-based services for our customers with confidence."- Mr. Masaru Ito, Sales and Business Planning Leader, Cloud Services Division EXA Corporation

- ✓ Reduce security exposures in Cloud environments
- ✓ Integrate event data



Optimize patch management for dynamic cloud environments

– *IBM SmartCloud for Patch Management*

- Reduce threat of attack and compliance risk by slashing remediation cycles from weeks to hours
- Help secure traditional and cloud environments and gain complete visibility of all endpoints

Identity mediation across cloud service providers

– *IBM Security Access Manager for Cloud and Mobile**

- Enables federated SSO and identity mediation across different cloud service providers

Enable visibility and monitoring of mainframe-based private clouds

– *IBM Security zSecure*

- Integration of mainframe event data into QRadar for enhanced monitoring

Extend security monitoring throughout the cloud

– *QRadar Security Intelligence Platform*

- Utilize cloud infrastructures to monitor activity across geographically distributed locations, such as bank branches and retail stores, for greater threat detection

Protect cloud platform from insider threats

– *IBM Security Privileged Identity Manager*

- Help prevent misuse of privileged identities to servers, applications and databases
- Control and track shared access to sensitive user IDs and demonstrate compliance

Integrate IAM with cloud

– *IBM Security Identity Manager*

- Rapid IAM integration with cloud, SaaS and on-premise services across heterogeneous environment

Agenda

- Customer Feedback
- Cloud Security
- Cloud Adoption Patterns
- IBM Cloud Security Capabilities
- **Summary and Resources**

IBM has extensive real-world experience delivering public and private cloud services

2,000

successful private cloud engagements in 2010.

4.5M

daily client transactions through public cloud.

1M

managed virtual machines.

“IBM has one of the most comprehensive cloud portfolios, with the cloud integrated throughout its many lines of business. Moreover, IBM’s consulting arm has put them in touch with numerous early adopters and special use cases—all of which helps the company stay ahead of competitors.”

– **Jeff Vance**, Datamation

IBM continues to research, test and document more focused approaches to cloud security

IBM Research & Papers

Special research concentration in cloud security, including White Papers, Redbooks, [Solution Brief – Cloud Security](#)

IBM X-Force

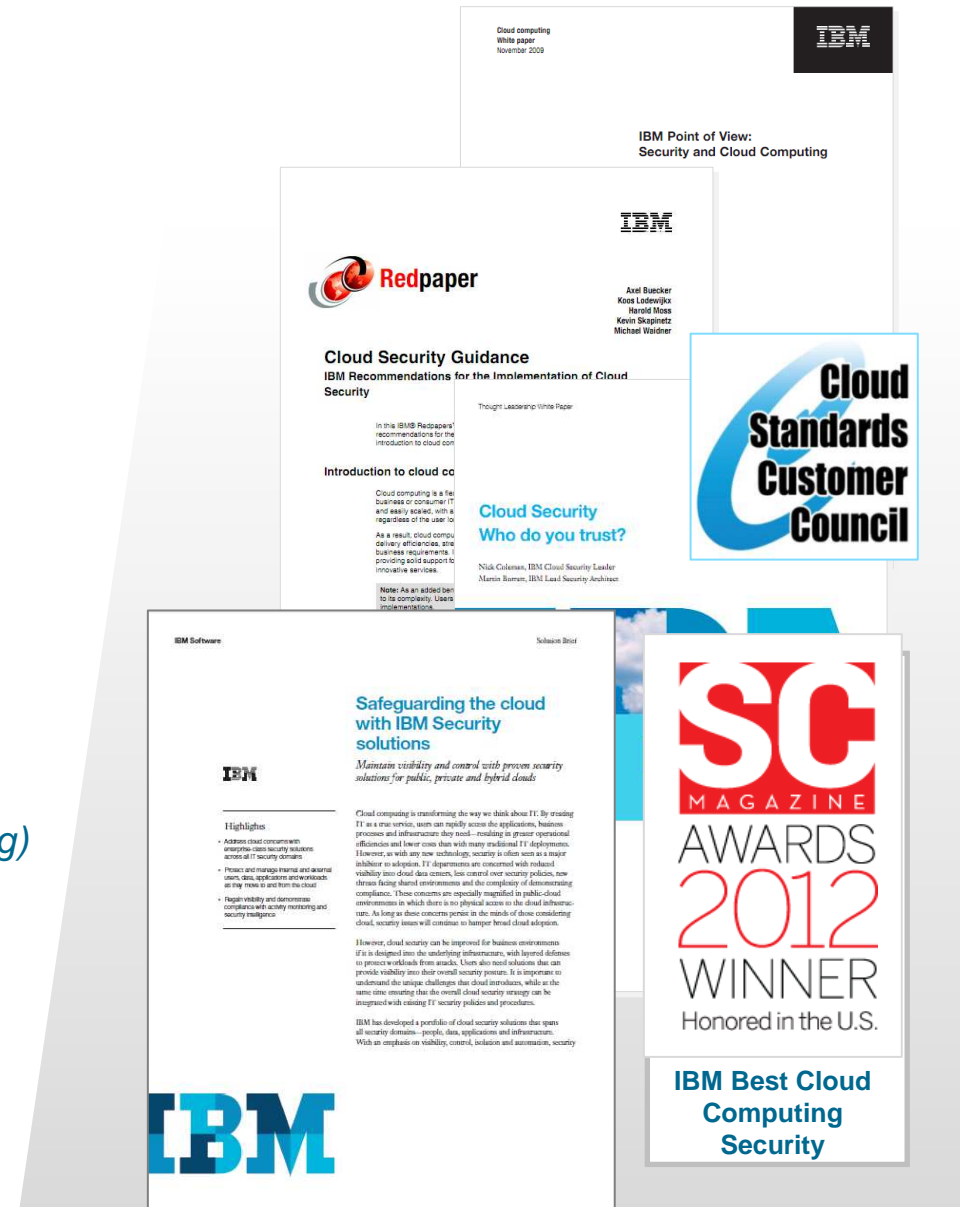
Proactive counter intelligence and public education <http://www-03.ibm.com/security/xforce/>

Customer Councils, Standards Participation and Analyst verification

Client-focused open standards and interoperability and real-world feedback from clients adopting cloud e.g. [CSCC](http://www.cloud-council.org/) <http://www.cloud-council.org/>. External customer verification of practical application (SC Mag)

IBM Institute for Advanced Security

Collaboration between academia, industry, government, and the IBM technical community <http://instituteforadvancedsecurity.com/>



ibm.com/security



© Copyright IBM Corporation 2012. 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, 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.

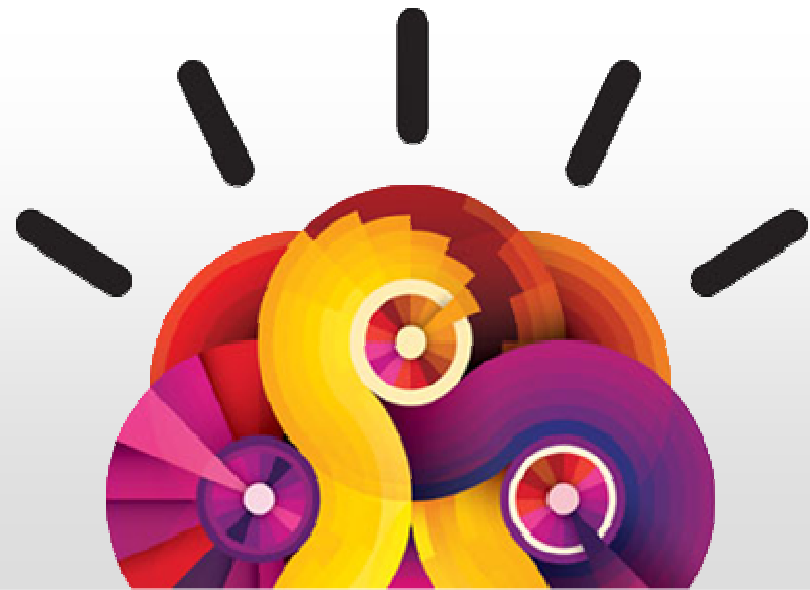
Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Agenda

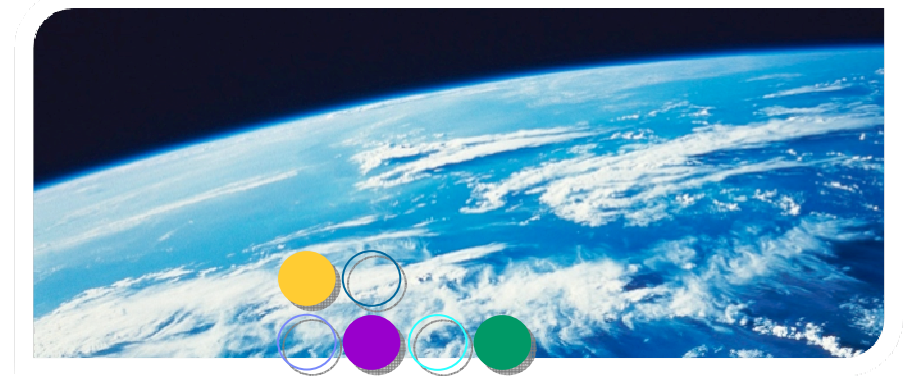
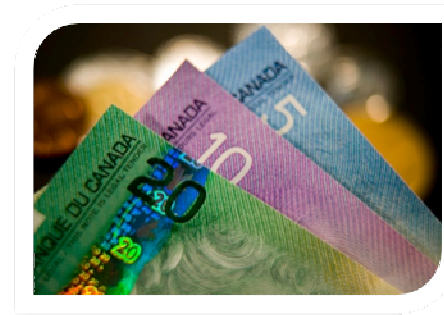
- Welcome and Introductions
- Latest Security trends and 2012 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent threats
- Break
- Managing Application Security
- From Identity & Access Management to Identity Intelligence
- Securing your Cloud
- **IBM Global Financing**

IBM Global Financing

Sharina Garach
IGF Complex Deal Maker



- IBM Global Financing helps companies acquire the IT solutions they need, more easily and cost-effectively, so they can:
 - Preserve cash for strategic business needs
 - Obtain the solutions they need—potentially without cutting back
- We are the world's largest technology financier, providing services in more than 55 countries
- We work with more than 125,000 clients, from small businesses to large enterprises, including roughly 91 of the Fortune 100
- Our decades of IT expertise give us an exceptional understanding of a company's technology and financial needs
- Hardware, Software and Services



55+
countries

125,000+
clients

Work with IGF early – and talk to us early – to help close your sale.

Additional Resources:

Software and Services Financing

This **white paper** looks at the growing trend toward financing software and services.

IBM Global Financing sales kit

Software Financing kit helps you through every step of the sales cycle

The Simple Way to Acquire IBM Software

Solution brief to help you give an overview of IGF and Software **References**

Check the **IBM Client Reference Database** for examples of IGF and software successes



0% Software Financing

Rates as low as 0% over 12 months for credit qualified clients purchasing new IBM software licenses and first-year subscription and support charges. Just divide the total amount to be financed by 12 to calculate the low monthly payment.

There's no better way to:

- Reduce the total cost of operation with no interest
- Realize big savings compared to an outright purchase
- Preserve cash flow and other lines of credit
- Free up funds for other crucial technology requirements

Flexible terms and payment options

Ask about our other financing structures with flexible terms and payment options that can help match payments to anticipated cash flow, which include:

- Flat monthly or quarterly payments
- Step payments
- Balloon payments
- Deferrals
- Customized terms and conditions
- Terms as long as 60 months
- No hardware requirement
- Competitive rates on 24- and 36-month payment terms

Control expenses, conserve cash and get the software you need today with IBM Global Financing!

For more information, visit ibm.com/financing

© Copyright IBM Corporation 2011. February 2011. All Rights Reserved. IBM, the IBM logo and ibm.com are registered trademarks of International Business Machines Corporation in the United States, other countries or both.

GFF00011-USEN-02

ibm.com/financing/za

Questions

Agenda

- Welcome and Introductions
- Latest Security trends and 2012 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent threats
- Break
- Managing Application Security
- From Identity & Access Management to Identity Intelligence
- Securing your Cloud
- IBM Global Financing
- **Close**

Security Intelligence.
Think Integrated.

IBM Security

Intelligence, Integration and Expertise

IBM Security Systems
May 2013

