



# Who can you trust?

*Enabling Secure Collaboration in Today's  
Dynamic Enterprise*



# People & Identity: Mega-Trends and Challenges

## Advanced Threats

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



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

## Mobile Computing

Securing employee-owned devices and connectivity to corporate applications are top of mind as CIOs broaden support for mobility



## Enterprise Customers



## Cloud Computing

Cloud security is a key concern as customers rethink how IT resources are designed, deployed and consumed



## Regulation and Compliance

Regulatory and compliance pressures are mounting as companies store more data and can become susceptible to audit failures



# Why is this important to organizations today?



## Must address advanced threats

- Insider threat – monitor shared and privileged accounts to manage risk
- Monitor, identify and correct security violations



## Must safeguard access in Cloud / SaaS environments

- Provision to cloud environments
- Help secure user access/SSO in cloud environments



## Must securely accommodate/leverage mobile computing

- Same fail-safe, security solution that addresses laptop/workstation access
- Address full range of mobile clients

GLBA



Sarbanes-Oxley

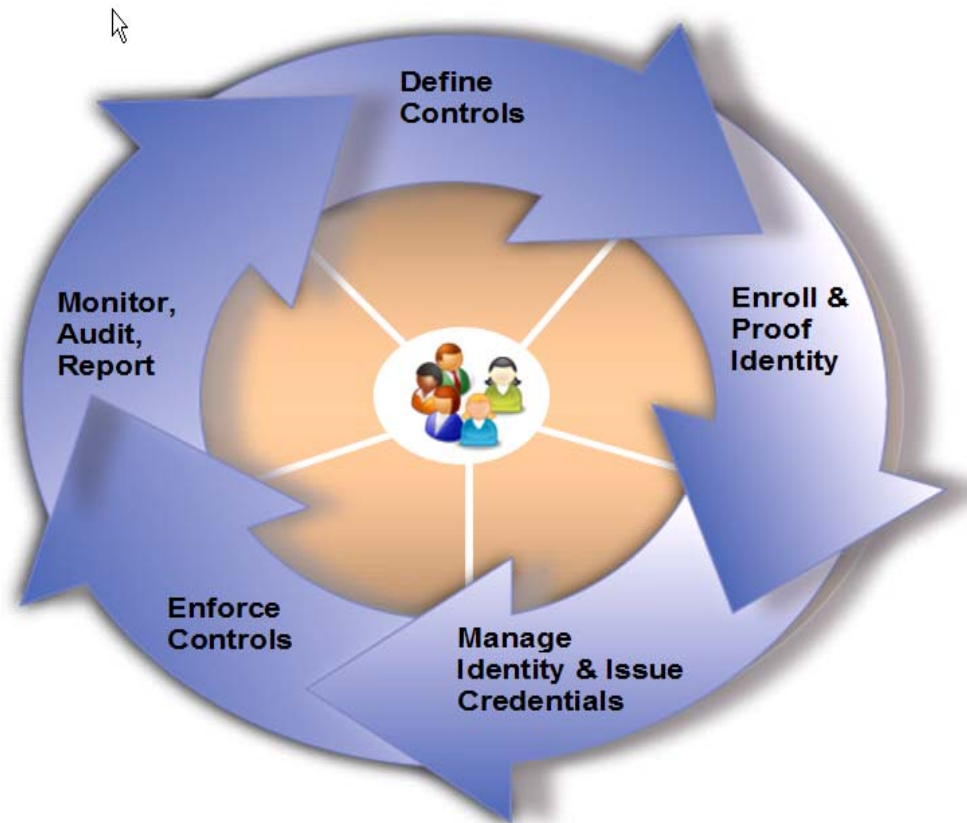
## Must address regulations and achieve security best practices

- Produce audit reports to help demonstrate compliance with security regulations
- Monitor, identify and correct security violations

# Key considerations to progress in the 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>Secure 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>

## A closed-loop identity and access assurance approach can help build trust and secure collaboration using System z



Optimizing security methodology to improve visibility and control into 'who' and 'what' is connecting in the mainframe.

# 1. Enroll and Proof Identity

## Public and Financial organizations seek to:

- Go beyond traditional approach to give person credentials with manual, tedious vetting
- Discover and detect suspicious relationships of interest
- Uniquely identify individuals with biographic and biometric proofing
- **Continuous vetting for obvious and non-obvious relationships in real time**

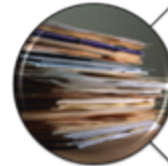
## Understanding Identity



**Role Alert:** When entities are resolved or related

Examples

- Employee is a vendor
- Employee shares address with vendor
- POI shares last name and phone number with police officer
- Employee shares bank account with employee
- Person has more than one name



**Attribute Alert:** When an entity with specific set of attributes is found

Examples

- If a name is ever encountered
- When an address of a suspect is ever encountered
- When any collection of one of more attributes is found



**Event Alert:** When an transactions and identities match alert rules

Examples

- Five money transfers in 24 hours over \$10,000 by one person
- More than one account opened in 2 days by same person
- 10 or more code violations reported in 5 days by same inspector

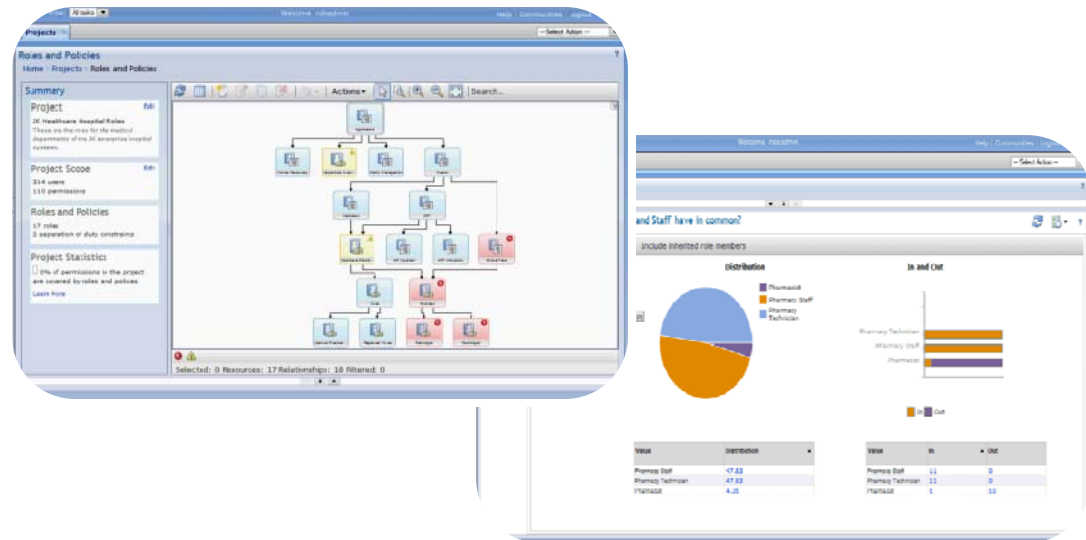
**InfoSphere Identity Insight Solution**  
(Linux on System z)

*In an highly interconnected environment, Intentional Identity Ambiguities compounds naturally occurring phenomena, and more sophisticated techniques are required*

## 2. Manage Identities and Issue Credentials

### Healthcare & Educational organizations seek to:

- Reduce time to provision new users with authoritative LDAP on z
- Minimize risk of insider threat
- Reduce help desk cost through self-service and password reset
- Reduce time and cost for regulatory compliance with automated work flow
- Reduce staff needed to manage identities, including admins and super user type accounts



**Identity Manager**  
(Linux on System z)

User → Role → Entitlements

*“The Identity management solution helped address issues in more than half of the HIPAA security standards...” — George Vasquez, Chief Technology Officer, Community Medical Centers*

# Traditional thinking in managing privileged users

Each administrator / user to have a userid on every system they administer

- Exponential increase in privileged userids
- Increased risk of mismanagement of privileged userids
- Increased userid administration costs

Administrators / user share privileged userids

- Risk of losing Individual Accountability
- Issues with password management and security
- Out of step with regulatory thinking

To improve trust, organizations need to combine the best features of both approaches, without the disadvantages



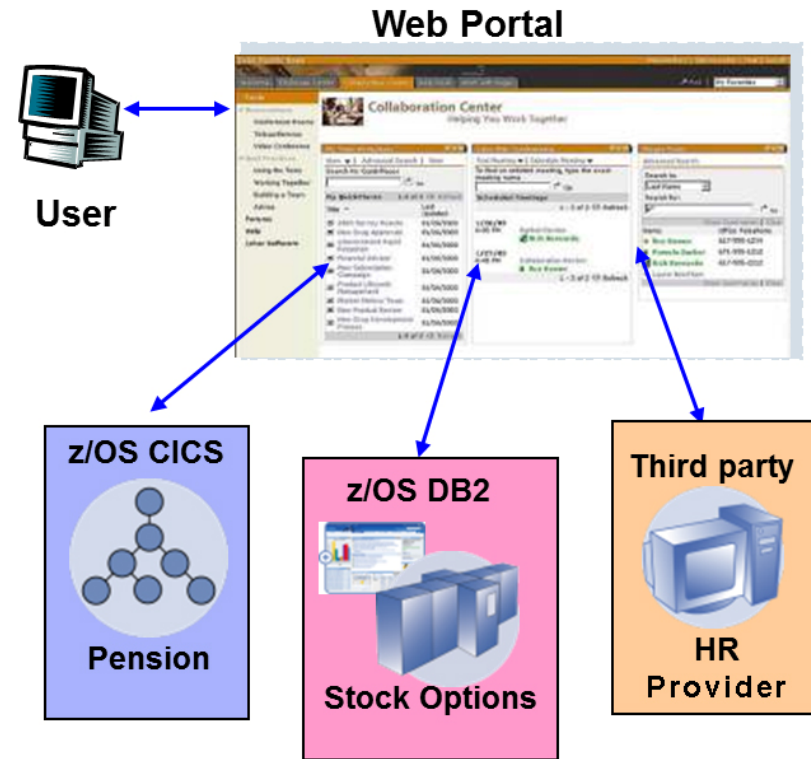
# IBM Privileged Identity Management Services

- **Privileged Identity Management (PIM)** centralizes management of shared and privileged accounts to improve compliance, lower cost and reduce risk
  
- **Key PIM functions include:**
  - Provision, de-provision and share privileged and shared identities
  - Secure access and storage of shared identities (secure Credential Vault)
  - Request, approve and re-validate privileged access
  - Single sign-on with automated check in and check out of shared and privileged IDs
  - End to end monitoring and reporting
  
- **Benefits**
  - Centralized Privileged ID management improves IT control and **reduces risk**
  - Automated sign on and check-in/out simplifies usage and **reduces cost**
  - Comprehensive tracking and reporting **enhances accountability and compliance**

### 3. Enforce Controls (Internal, External User Access)

#### Retail and Manufacturing organizations needs:

- Propagate identity from portal to RACF for improved visibility
- Secure B2B and B2C access and collaboration with single sign-on
- Enforce user access to mainframe on a need-to-know basis
- Secure workstations shared by multiple users and single source LDAP on z
- Improve user acceptance to new security policy and compliance regulations



**Access Manager and Federated Identity Manager**  
(Linux on System z)

“All users need is a device and a browser to gain access on demand—anytime, anywhere, via any device and personalized for their roles. - Vijay Sonty, CIO, School Board of Broward County (SBBC)

# Traditional thinking in enforcing fine-grained access

Application is responsible for fine-grained access, react and remediate to incidents when they occur

- Hard to detect outsider manipulating insider
- Costly to fix and change
- More reactive in nature to address malicious insider

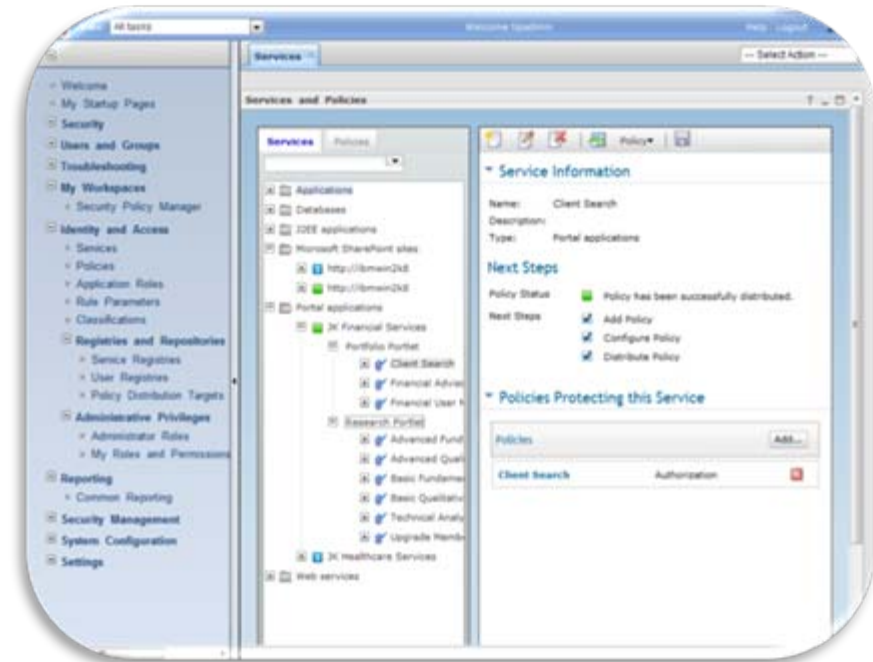
Security is responsible for access on a need-to-know basis, detect and change to incidents when they occur

- More upfront work to externalize security from applications
- Less expensive to fix and change
- More proactive in nature to address malicious insider

To address insider threat, organizations need to combine the best features of both approaches, without the disadvantages

# IBM Security Policy Management

- **Manage & enforce access on a need to know basis**
  - Context-based access using XACML
  - Message security using WS-SecurityPolicy
- **Support flexible policy enforcement**
  - Intermediary, App Server
  - Application and Database on System z

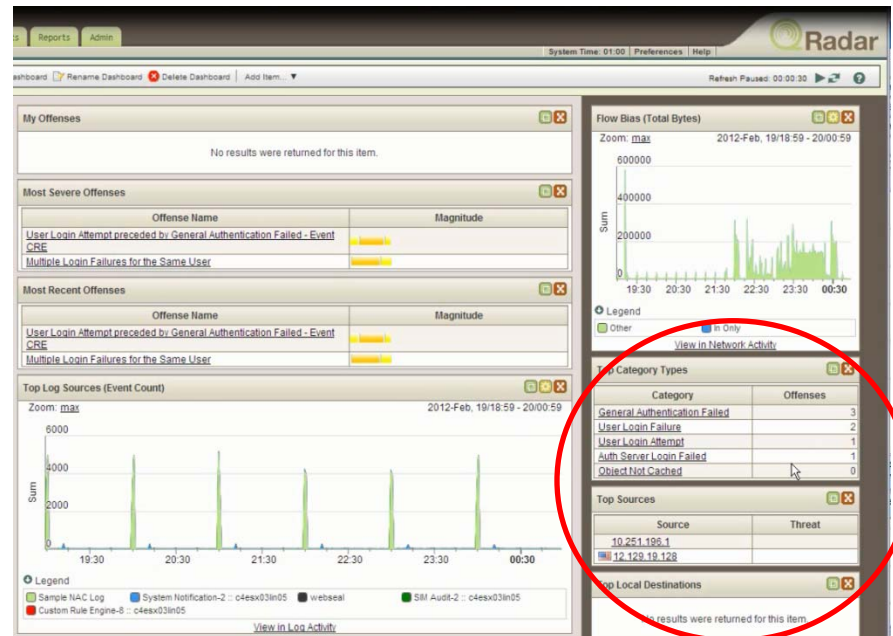


**Security Policy Manager**  
*(Linux on System z)*

## 4. Monitor & Report on User rights & activities

### Energy Utility & Electronics organizations needs:

- Total visibility of user activities and information across mainframe and distributed IT environments
- Monitor and report both internal and external privileged users activities
- Provide identity context across all security domains (System z, data, applications, infrastructure)
- Compliance with regulations such as NERC-CIP, SOX, PCI, and more



**Integration of QRadar SIEM with IAM to stay ahead of internal threats including those driven by privileged users.**

**“..we have got full control over highly privileged users both internally at Philips or externally at our outsourcing partner... “Trusting people is good, controlling is better”- Mr. Gabriel van de Luitgaarden, Senior VP Operations**

# Integrated Identity and Access Management with Mainframe Security Administration is key to improving Trust end-to-end

Integrated zSecure and IAM propagates trusted identities from Portal to data on z

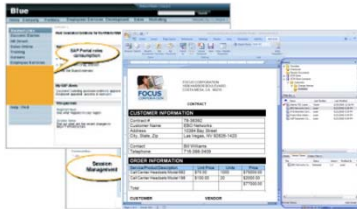
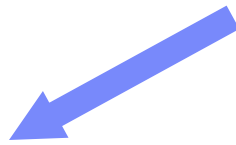


Identity & Access Management  
(Linux on System z)



zSecure Suite

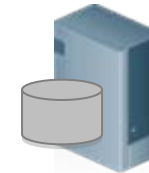
Supports mainframe and heterogeneous application and data environment



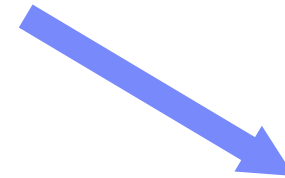
e.g. WebSphere Portal,  
SharePoint, FileNet



e.g. DataPower,  
ESBs, MB



e.g. WebSphere  
App Server, .NET



e.g. RACF, ACF2,  
Top Secret

## Enable organization wide, end-to-end compliance and governance

- Improved visibility, control and automation
- Less code to develop, test and maintain
- Quicker deployment of secure portal using mainframe applications and services

# IBM Implementation Success Story

Simplifying identity management for 400,000 employees, 120,000 servers, 100,000+ contractors and business partners, in 170 countries






## ■ Business challenge:

- Improve compliance for privacy and regulations
- Manage user identity and access lifecycle consistently
- Audit inappropriate access, both inadvertent and intentional
- Consolidate legacy systems and reduce costs
- Minimize risk and improve security for telecommuting, mobile users



***“Streamlining and automating access and administration processes is driving significant savings and productivity improvements while strengthening security controls.”***

***— Terry Escamilla, DE, Security and Privacy Programs, Office of the CIO, IBM***

-  Major Employee Sites
-  Customer Fulfillment
-  Manufacturing
-  Employee Service Centers
-  IBM Research Centers

# Retail Customer Case Study

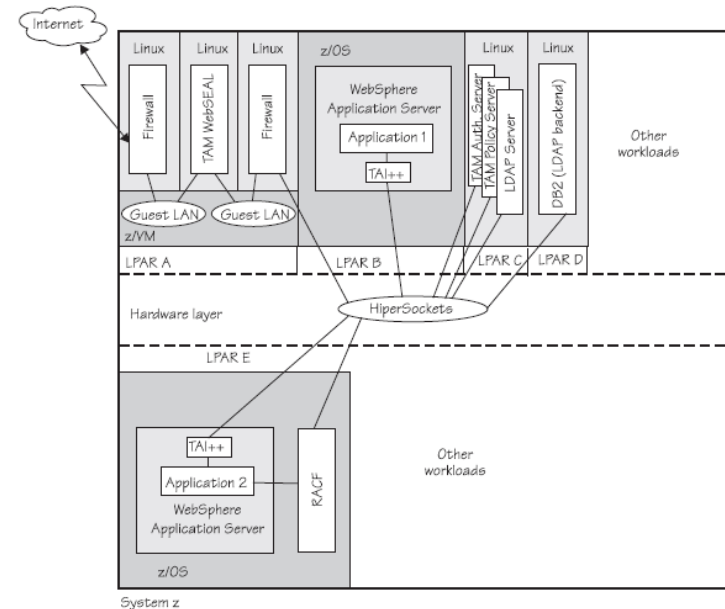
Simplifying identity and access management for 150,000 associates,  
10,000 vendors in North America

## ■ Business challenge:

- Migrating key application workload on to zLinux
- Demonstrate compliance for privacy and regulations
- Manage and enforce user identity and access lifecycle consistently
- Establish trust and federated access for vendors and business partner

## ■ Solution implemented:

- Identity & Access Management on System z Linux
- zSecure suite





# IBM continued leadership in industry standards

## ■ Open Standards:

- OpenID, OAuth
- OASIS: Identity MetaSystem Interoperability, standards development (SAML, XACML)



## ■ IBM Delivery of Standards Support:

- Federated Identity Manager  
(SAML, WS-Trust, RACF PassTicket, OpenID, OAuth)
- Security Policy Manager  
(WS-SecurityPolicies, XACML)

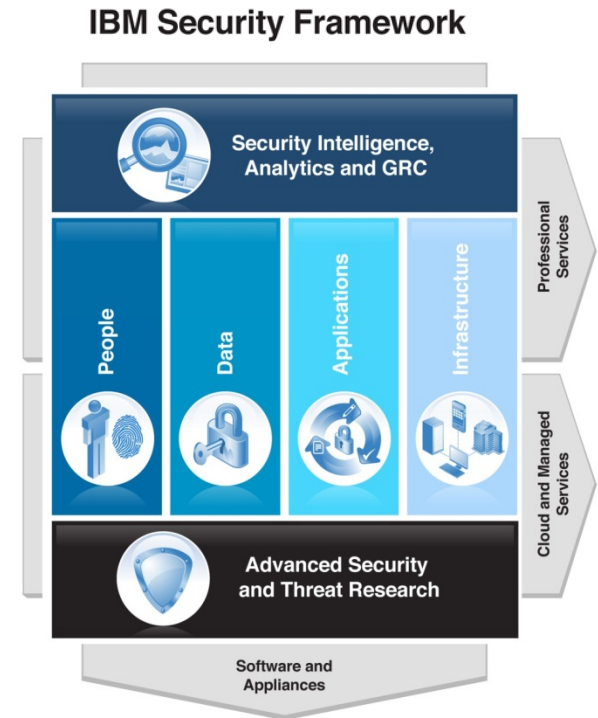
## ■ Industry Interoperability:

- Kantara Initiatives: SAML 2.0 conformance



# Why IBM to address the Security & Trust needs?

- Breadth and depth of solution
- Best in class mainframe security
- Flexible delivery model
- Expertise in thousands of customer projects
- Open security standards and leadership





[ibm.com/security](http://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.

# Our focus is in two areas of cloud security

## 1 Security from the Cloud

**Cloud-based  
Security  
Services**

Use cloud to deliver security **as-a-Service** - focusing on services such as vulnerability scanning, web and email security, etc.

## 2 Security for the Cloud

**Public cloud  
Off premise**

Secure usage of Public Cloud applications – focusing on Audit, Access and Secure Connectivity

**Private cloud  
On premise**

**Securing the Private Cloud stack**  
– focusing on building security into the cloud infrastructure and its workloads

# Leverage the Mainframe as the Enterprise Security Hub

**Resource Access Control Facility**

**Security zSecure Suite**

**Security Key Lifecycle Manager for z/OS**

**InfoSphere Guardium Family**

**InfoSphere Guardium Data Encryption for DB2 and IMS Databases**

**Security Information and Event Management**

**IBM Security Network Intrusion Prevention System**

**Communications Server & Netview for z/OS/**



**Security Identity Manager**

**Security Access Manager**

**Security Federated Identity Manager**

**Security Directory Integrator**

**Security Directory Server**

**WebSphere Application Server**

**WebSphere DataPower Server**

**Rational AppScan**

**Solution Edition for Security**

**Security Identity & Access Assurance**