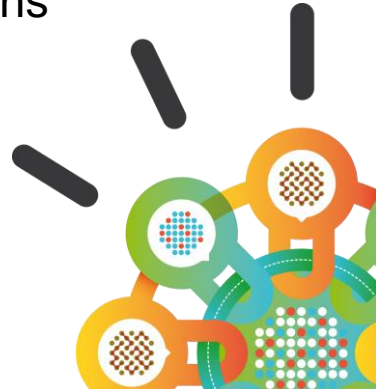


Security Intelligence.  
Think Integrated.



## IBM Cloud Security Solutions

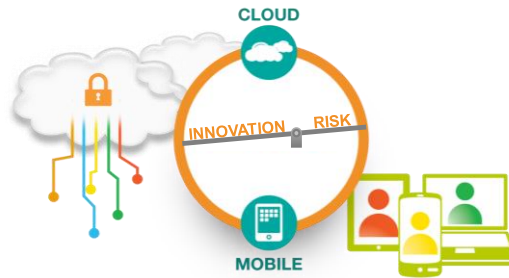
July 3<sup>rd</sup> 2014



### Disclaimer

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

## Customers are faced with challenge of balancing innovation and risk



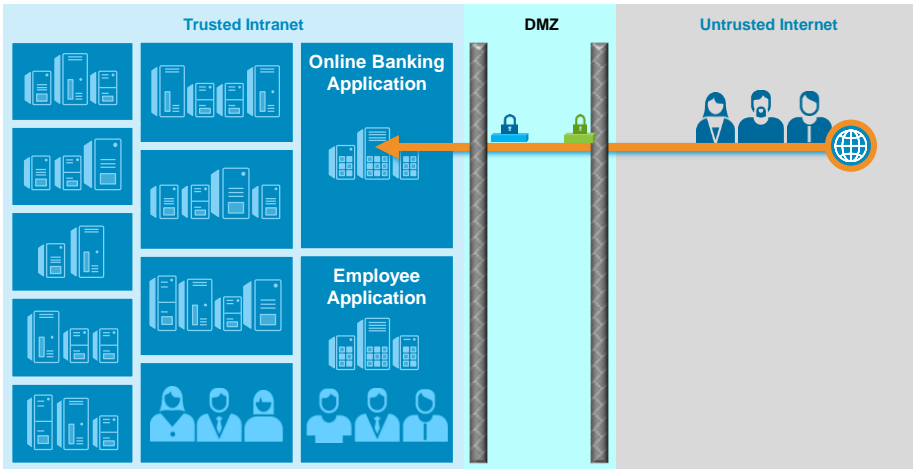
- 1 Cloud creates opportunities for enhanced security
- 2 Cloud security is a shared responsibility between customers and Cloud providers
- 3 IBM Cloud platforms and IBM Security portfolio help enterprise customers adopt Cloud with confidence

## Clients' security objectives reflect their responsibilities when adopting Cloud

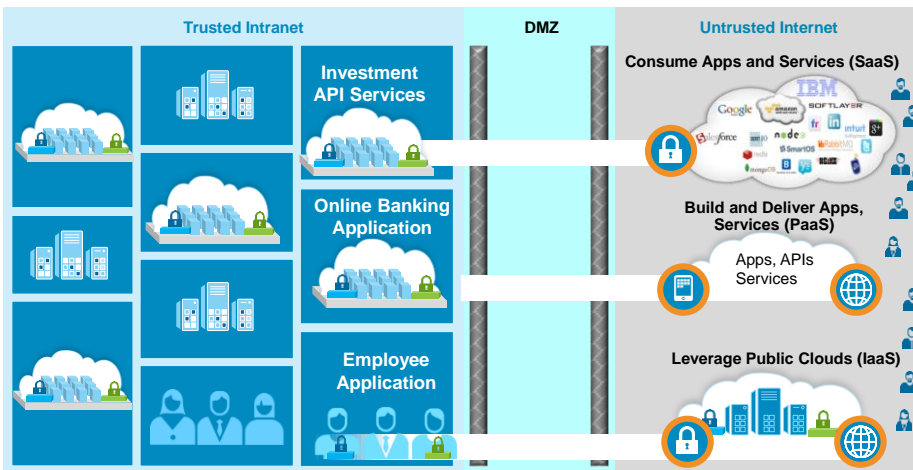


Services Acquired	Organization / Buyers	Security Responsibilities and Objectives
<b>Software as a Service (SaaS)</b>	CxOs (CIO, CMO, CHRO, ...)	<ul style="list-style-type: none"> <li>▪ Complete visibility to enterprise SaaS usage and risk profiling</li> <li>▪ Governance of user access to SaaS and identity federation</li> </ul>
<b>Platform as a Service (PaaS)</b>	Application teams, LOBs	<ul style="list-style-type: none"> <li>▪ Enable developers to compose secure cloud applications and APIs, with enhanced user experience</li> <li>▪ Visibility and protection against fraud and applications threats</li> </ul>
<b>Infrastructure as a Service (IaaS)</b>	CIO, IT teams	<ul style="list-style-type: none"> <li>▪ Protect the cloud infrastructure to securely deploy workloads and meet compliance objectives</li> <li>▪ Have full operational visibility across hybrid cloud deployments, and govern usage</li> </ul>

### Traditional perimeter-based security controls ...



### Traditional perimeter-based security controls ... ... are changing to security centered around applications and data



## We see three sets of security capabilities to help enterprise clients...



SaaS: Secure usage of business applications



PaaS: Secure service composition and apps



IaaS: Securing infrastructure and workloads

### Cloud Security Capabilities



#### Identity

Manage identities and govern user access



#### Protection

Protect infrastructure, applications, and data from threats



#### Insight

Auditable intelligence on cloud access, activity, cost and compliance



## ... delivered via cloud-enabled technologies and managed services



SaaS: Secure usage of business applications



PaaS: Secure service composition and apps



IaaS: Securing infrastructure and workloads

### Cloud Security Capabilities



#### Identity

Manage identities and govern user access



#### Protection

Protect infrastructure, applications, and data from threats



#### Insight

Auditable intelligence on cloud access, activity, cost and compliance



### Client Consumption Models

Security SaaS



APIs

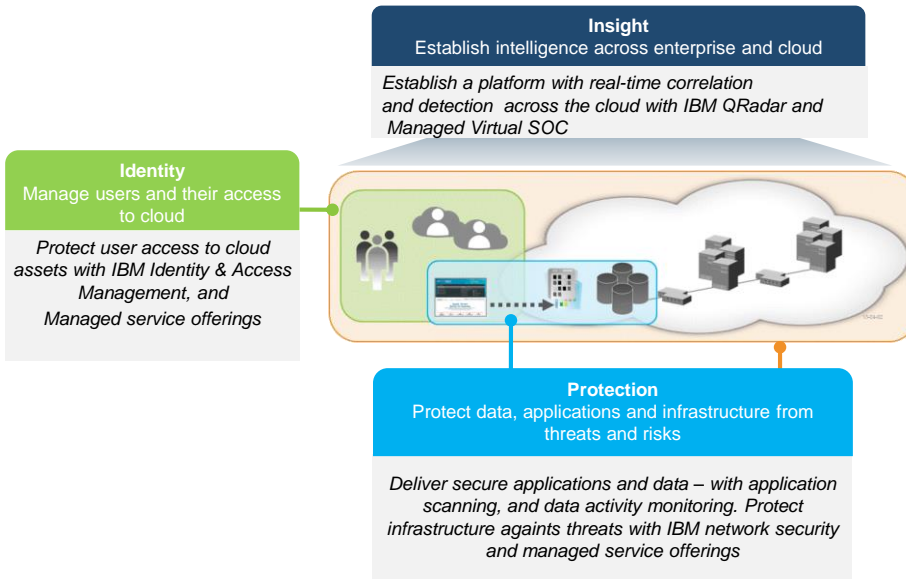


Virtual Appliances



Professional Security Services  
Managed Security Services

## IBM Security capabilities for the Cloud



## Examples - Enterprise hybrid cloud requires integrated solutions

	Identity	Protection	Insight
<b>Software as a Service (SaaS)</b>	Enable employees to connect securely to SaaS <ul style="list-style-type: none"> <li>• <b>SaaS access governance</b></li> <li>• Identity federation</li> </ul>	Secure connectivity and data movement to SaaS <ul style="list-style-type: none"> <li>• <b>Data tokenization</b></li> <li>• Secure proxy to SaaS</li> <li>• Application control</li> </ul>	Monitoring and risk profiling of enterprise SaaS usage <ul style="list-style-type: none"> <li>• <b>Monitor SaaS usage</b></li> <li>• Risk profiling of SaaS apps</li> <li>• Compliance reporting</li> </ul>
<b>Platform as a Service (PaaS)</b>	Integrate identity and access into services and applications <ul style="list-style-type: none"> <li>• <b>DevOps access management</b></li> <li>• Authentication and authorization APIs</li> </ul>	Build and deploy secure services and applications <ul style="list-style-type: none"> <li>• <b>Database encryption</b></li> <li>• App security scanning</li> <li>• Fraud protection and threats</li> </ul>	Log, audit at service and application level <ul style="list-style-type: none"> <li>• <b>Monitor application, services and platform</b></li> <li>• Service vulnerabilities</li> <li>• Compliance reporting</li> </ul>
<b>Infrastructure as a Service (IaaS)</b>	Manage cloud administration and workload access <ul style="list-style-type: none"> <li>• <b>Privileged admin management</b></li> <li>• Access management of web workloads</li> </ul>	Protect the cloud infrastructure to securely deploy workloads <ul style="list-style-type: none"> <li>• <b>Storage encryption</b></li> <li>• Network protection – firewalls, IPS</li> <li>• Host security, vulnerability scanning</li> </ul>	Security monitoring and intelligence <ul style="list-style-type: none"> <li>• <b>Monitor hybrid cloud infrastructure</b></li> <li>• Monitor workloads</li> <li>• Log, audit, analysis and compliance reporting</li> </ul>

Bold text indicates one example per protection stack read top to bottom through SaaS, PaaS, and IaaS models

Note: Listed capabilities in the above table are examples of capabilities, and not a comprehensive list






## Infrastructure as a Service


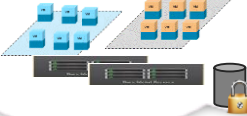

11


IBM Security Solutions IBM

### SoftLayer provides a Secure Enterprise Cloud platform

 <b>Integrated user management</b> <ul style="list-style-type: none"><li>• Manage administrator roles</li><li>• Federated administrators from enterprise identity infrastructure</li></ul>	 <b>Security hardened infrastructure</b> <ul style="list-style-type: none"><li>• Bare metal , VM isolation</li><li>• Network security - Firewalls, VPNs</li><li>• 'VM Server group' management</li><li>• Encrypted object store and hardware protected keys</li></ul>	 <b>Log and Event Collection</b> <ul style="list-style-type: none"><li>• Basic access logs</li><li>• Enhanced APIs to integrate with enterprise security monitoring</li></ul>
---	--	--

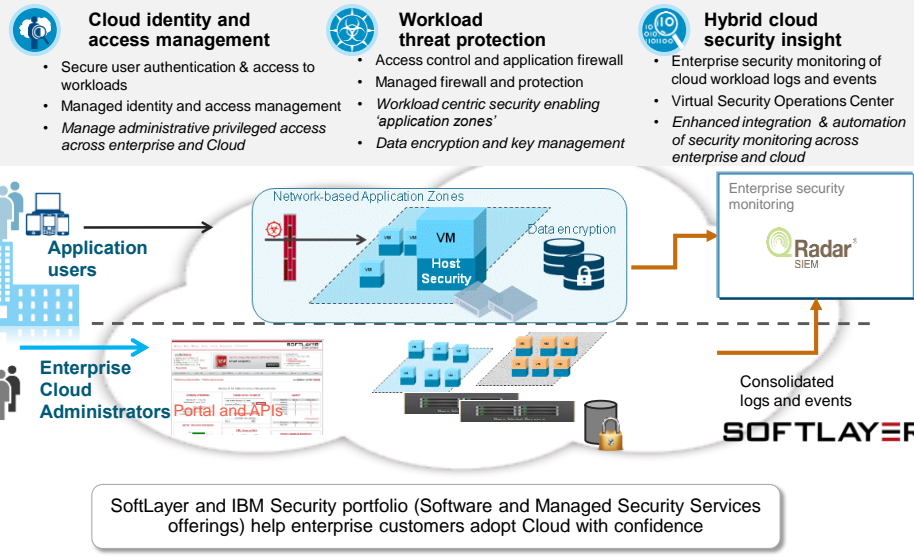
Enterprise security monitoring

Enterprise Cloud Administrators   Consolidated logs and events 

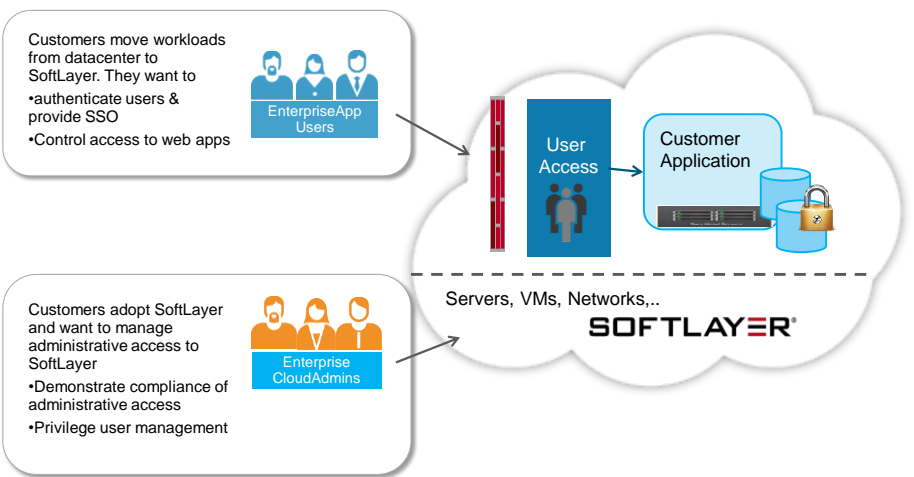
Enterprise security monitoring 

12 © 2014 IBM Corporation

## IBM Security capabilities enhance security of customer workloads



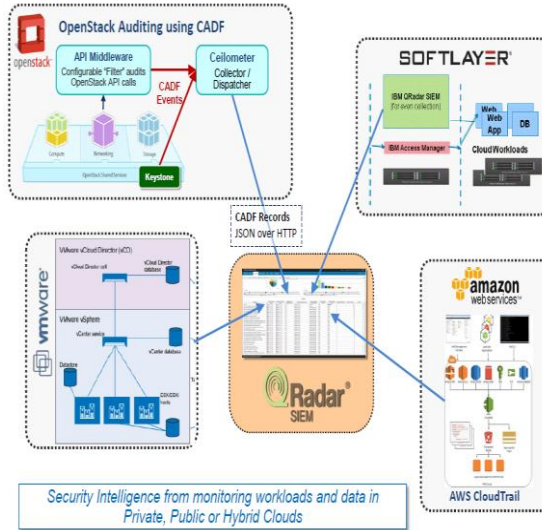
## Authenticating users and managing their access "on" SoftLayer using IBM Security Access Manager



## Customers need full visibility to hybrid cloud environments using IBM Security QRadar

- Visibility across hybrid cloud deployments using QRadar
- Out of the box integration with logs and event collection
- Compliance and vulnerability management

- Unified visibility across cloud and CPE
- IBM Virtual SOC & Managed SIEM Services



Security Intelligence from monitoring workloads and data in Private, Public or Hybrid Clouds



## Platform as a Service



## Use cases “in” Bluemix - strengthening security of the foundation



### Easy and integrated security management

- Manage developer roles
- Manage access according to scope
- Federated developers from enterprise identity infrastructure



### Security hardened infrastructure

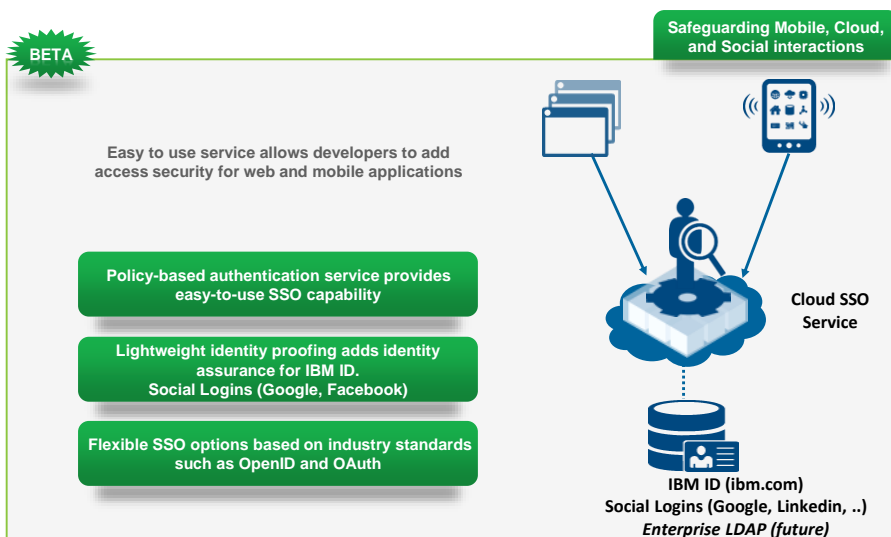
- Application and container isolation
- Data security, privacy and protection
- Security engineering, assurance and compliance



### Log and Event Collection for Differentiating Services

- APIs to integrate with enterprise security monitoring
- Enable advanced security services
- Audit, logging and compliance

## Identity Service (IDaaS) on Bluemix: Simplified Security for App Developers



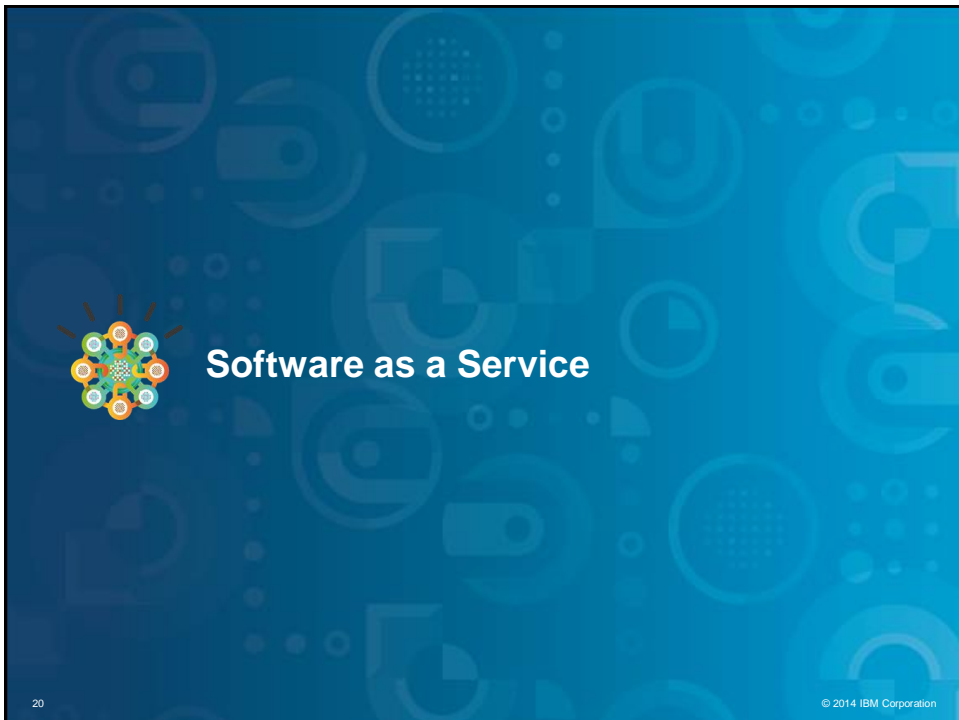
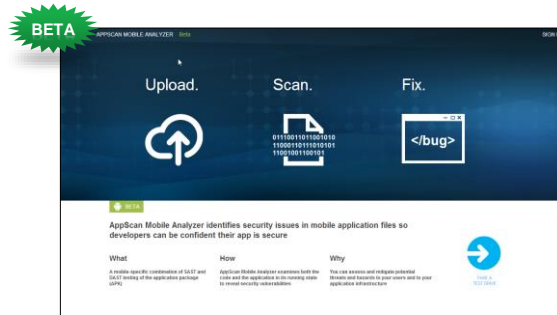
## AppScan services soon available through Bluemix

### AppScan Mobile Analyzer

- Ability to upload Android APKs to the cloud for an IAST (interactive application security scan)
  - Service available through BlueMix catalog
  - Upload an APK and receive a security PDF report
  - Public APIs to integrate to 3<sup>rd</sup> party
  - Environment deployed on SoftLayer

### AppScan DAST on BlueMix

- Run a DAST scan on web application deployed on BlueMix
  - Service available through BlueMix catalog
  - Almost zero configuration (User Name/Password)
  - Public APIs to integrate to 3<sup>rd</sup> party
  - Environment deployed on SoftLayer



## Secure user access to Cloud services

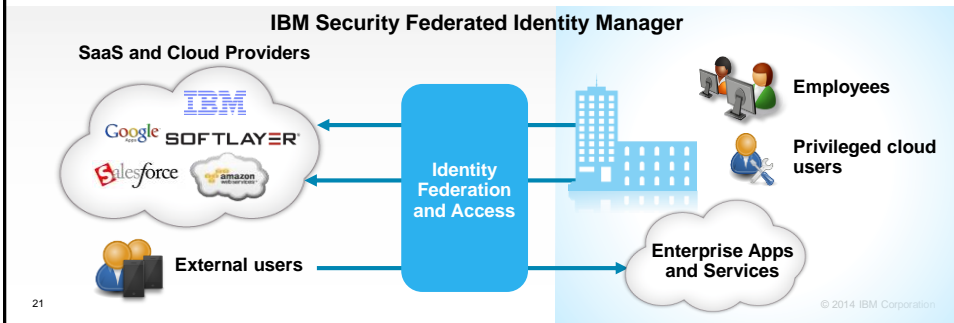
Use case: Enterprise expansion, securing public cloud access users

### Business Challenge:

- Extend on-premise IAM infrastructure to cloud apps
- Secure employee access to SaaS applications (IBM, Google Apps, Salesforce)
- Manage identity and federated SSO for internal / traditional applications and new external SaaS ones
- Provision / de-provision users in SaaS partner's registry

### Solution:

- Common identity management solution for user provisioning and password management
  - Role-based provisioning and de-provisioning
  - User- and manager-initiated entitlement requests
  - BU administrators manage their users' rights
- Federate access in context, based on web launch points; federated SSO access based on role



## Available Today – Security capabilities delivered as Cloud service

Fraud Prevention	Mobile Security	Web Protection
<ul style="list-style-type: none"> <li>• Delivered as a cloud service protecting millions of endpoints for the world's top financial institutions</li> </ul>	<ul style="list-style-type: none"> <li>• Delivered as a cloud service managing millions of mobile devices for thousands of global customers</li> </ul>	<ul style="list-style-type: none"> <li>• Delivered a service in the cloud, providing Distributed Denial of Service (DDoS) protection for enterprise customers</li> </ul>
<b>Fraud Prevention</b>	<b>Mobile Security</b>	<b>Web Protection</b>
<p><b>Millions</b> of endpoints protected for the world's top financial institutions</p> <p style="background-color: #FF8C00; color: white; padding: 2px;"><b>IBM Trusteer</b></p>	<p><b>Millions</b> of cloud-managed devices for thousands of global customers</p> <p style="background-color: #FF8C00; color: white; padding: 2px;"><b>IBM Fiberlink</b></p>	<p><b>Thousands</b> of servers providing DDoS protection in the cloud</p> <p style="background-color: #FF8C00; color: white; padding: 2px;"><b>IBM + Akamai</b></p>




# Summary

23

© 2014 IBM Corporation

IBM Security Solutions IBM

## Summary: security for the cloud and from the cloud






Professional, Managed, and Cloud Services




**Differentiated Security Capabilities...**

- Security analytics and intelligence**  
Establish a platform with real-time correlation and detection across the cloud with IBM QRadar SIEM
- Manage distributed identities and user access**  
Protect user access to cloud assets with IBM Identity and Access Management
- Scan, monitor and audit applications and data**  
Deliver secure *mobile and web apps*, and monitor data access in real time with AppScan and Guardium
- Protect the network from threats**  
Protect servers, endpoints and networks against threats with IBM Network Security

... based on open standards

International Organization for Standardization

© 2014 IBM Corporation

## Key Cloud Resources

### IBM Research and 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/>

### IBM Institute for Advanced Security

- Cloud Security Zone and Blog [\(Link\)](#)

### Customer Case Study

- EXA Corporation creates a secure and resilient private cloud [\(Link\)](#)

### Collateral Sales Support:

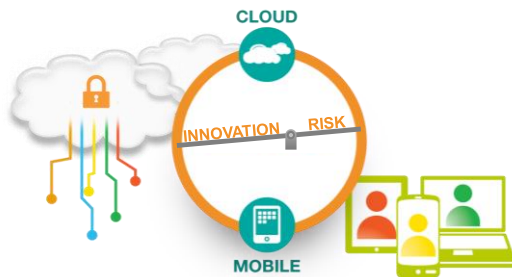
- NEW** IBM Cloud Security Strategy and Community connections page [\(Link\)](#)
- NEW** Internal IBM SWG Sellers Workplace – Cloud Security Collateral - [\(Link\)](#)
- SmartCloud Security Solutions Sales Kit – [\(Link\)](#)

### Other Links:

- IBM Media series – SEI Cloud Security [\(Link\)](#)
- External IBM.COM : IBM Security Solutions [\(Link\)](#)
- External IBM.COM : IBM SmartCloud– security [\(Link\)](#)
- IBM SmartCloud security video [\(Link\)](#)



## Key takeaways



**1** Cloud creates opportunities for enhanced security

**2** Cloud security is a shared responsibility between customers and Cloud providers

**3** IBM Cloud platforms and IBM Security portfolio help enterprise customers adopt Cloud with confidence

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.

# Thank You

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



© Copyright IBM Corporation 2014. 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.