IBM SolutionsConnect 2015

Seize the Moment. Dive into Next Generation Technologies.
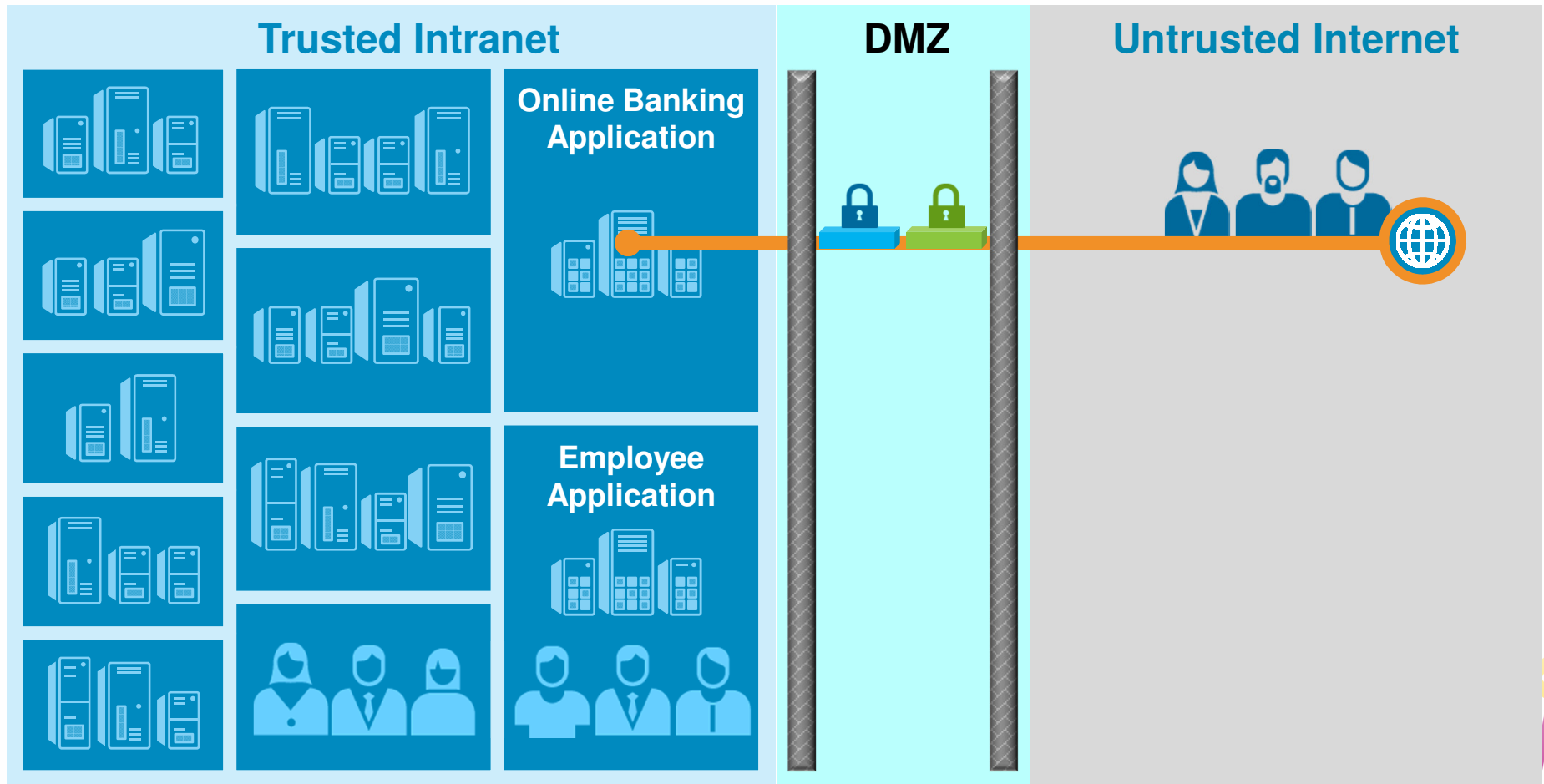
Cloud Security

Addressing the Elephant in the Room.
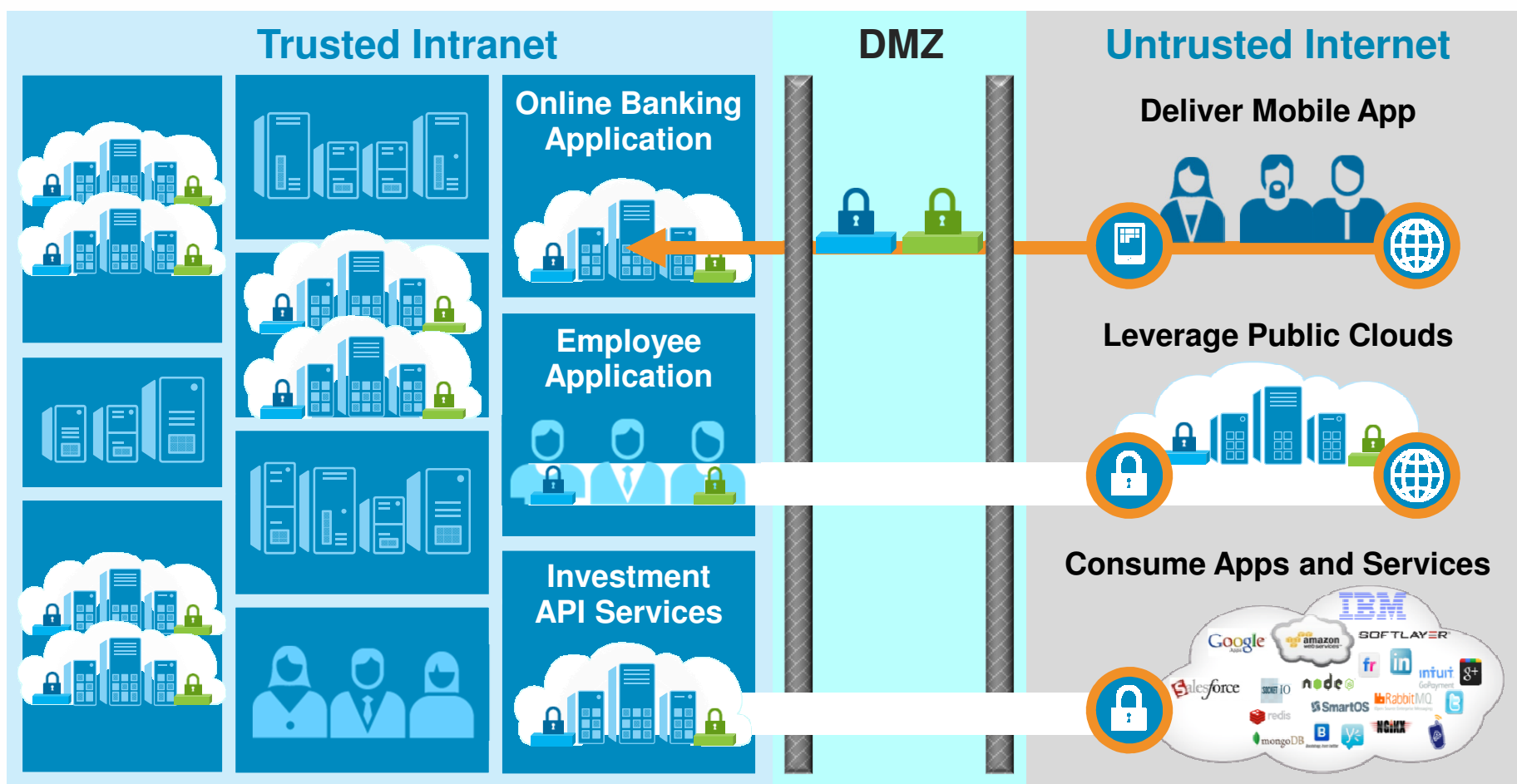
Collin Penman

IBM

Cloud IT infrastructure - *Moving toward enterprise security obtained through "application zones"*

Trusted Intranet

DMZ

Untrusted Internet

Online Banking Application

Employee Application

Investment API Services

Deliver Mobile App

Leverage Public Clouds

Consume Apps and Services

Cloud is rapidly transforming the enterprise
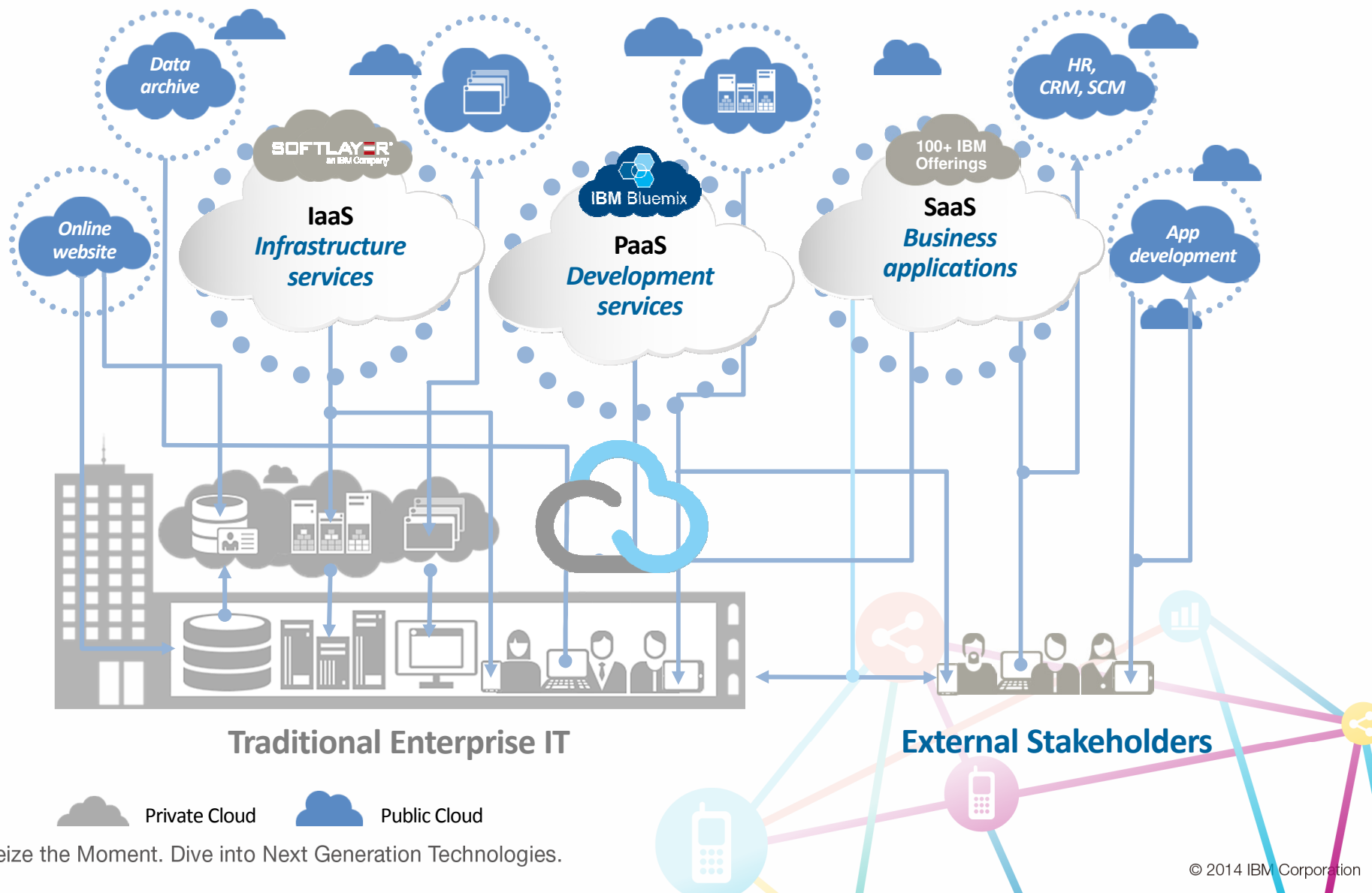
Security is in fact, a key inhibitor for growth in cloud adoption

73%

of firms discovered cloud usage outside of IT or security policies.[1]

50%

of firms are worried about unauthorized access of leakage of sensitive data.[2]

75%

of security breaches take days, weeks or even months to discover.[3]

1. 2013, IDC US Cloud Security Survey
2. Sept 2013, Information Week Cloud Security and Risk Survey
3. Verizon 2014 Data Breach Investigations Report

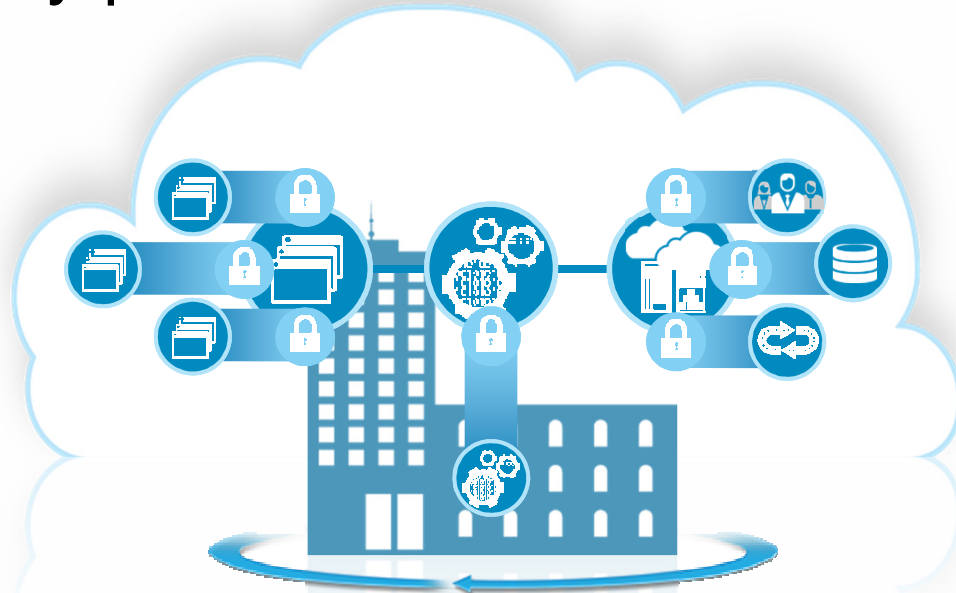Seize the Moment. Dive into Next Generation Technologies.

Cloud is an opportunity to radically transform security practices

Traditional Security
Manual, static,
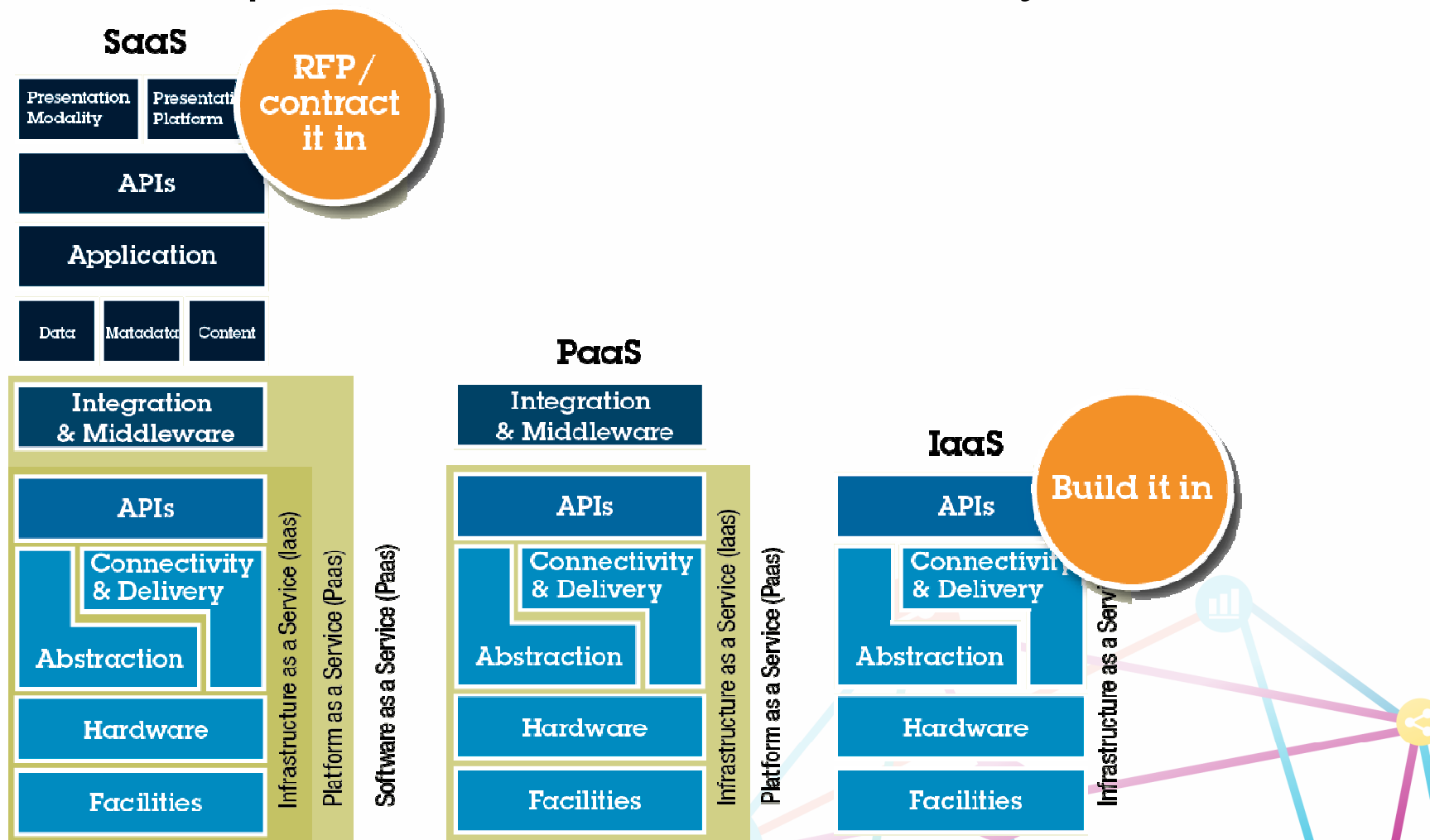and reactive

Cloud-enhanced Security
Standardized, automated,
customizable, and elastic

IBM Point of View:

*Cloud security is an opportunity
to improve defenses and reduce risk*

Know your and your provider's security responsibilities at each cloud layer

cloud
security
alliance®
CSA

SaaS

Presentation Modality	Presentation Platform

RFP / contract it in

APIs

Application

Data	Metadata	Content

Integration & Middleware

APIs

Connectivity & Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (Iaas)
Platform as a Service (Paas)
Software as a Service (Paas)

PaaS

Integration & Middleware

APIs

Connectivity & Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (Iaas)
Platform as a Service (Paas)

IaaS

Build it in

APIs

Connectivity & Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Serv

Your strategy begins by assessing compliance and controls

CSA *cloud security alliance®*

Cloud Model

Presentation Modality	Presentation Platform

APIs

Application

Data	Metadata	Content

Integration & Middleware

APIs

Connectivity & Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (Iaas)
Platform as a Service (Paas)
Software as a Service (Paas)
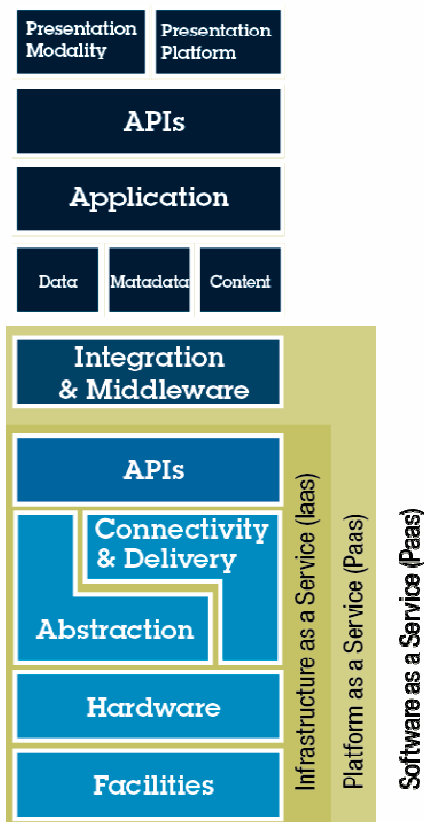
Source: The Cloud Security Alliance

Example: PCI Compliance

Security Control Model

Applications — SDLC, binary analysis, scanners, webapp firewalls, transactional sec.

Information — DLP, CMR, database activity monitoring, encryption

Management — GRC, IAM, VA/VM, patch management, configuration management, monitoring

Network — NIDS/NIPS, firewalls, DPI, anti-DDoS, QoS, DNSSEC, OAuth

Trusted Computing — Hardware & Software RoT & API's

Compute & Storage — Host-based firewalls, HIDS/HIPS, integrity & file/log management, encryption, masking

Physical — Physical plant security, CCTV, guards

Compliance Model

PCI

- Firewalls
- Code review
- WAF
- Encryption
- Unique user IDs
- Anti-virus
- Monitoring/IDS/IPS
- Patch/vulnerability management
- Physical access control
- Two-factor authentication

HIPAA

GLBA

SOX

Seize the Moment. Dive into Next Generation Technologies.

© 2014 IBM Corporation

Your focus needs to be on three imperatives for improving security

How can I understand who is accessing the cloud from anywhere, at anytime?	*How can I fix vulnerabilities and defend against attacks before they're exploited?*	*How can I obtain a comprehensive view of cloud and traditional environments?*
Govern the usage of cloud	**Protect workloads and data in the cloud**	**Detect threats with visibility across clouds**
"Going to the cloud gives me a single choke point for all user access – it provides much more control."	*"Cloud gives me security APIs and preconfigured policies to help protect my data and workloads"*	*"I can take advantage of centralized cloud logging and auditing interfaces to hunt for attacks."*

Where should customers turn?

Seize the Moment. Dive into Next Generation Technologies.

© 2014 IBM Corporation

IBM is uniquely positioned to offer Security for the Cloud

IBM Cloud

40 IBM global data centers *expanded from 25*

15 Countries and 5 continents covered by IBM Cloud

500 IBM developers working on cloud open source

40K+ IBM Cloud experts with deep industry knowledge

80% Of Fortune 100 companies use IBM Cloud capabilities

30K+ IBM Cloud clients

300K+ Trading communities connected to IBM's B2B cloud network

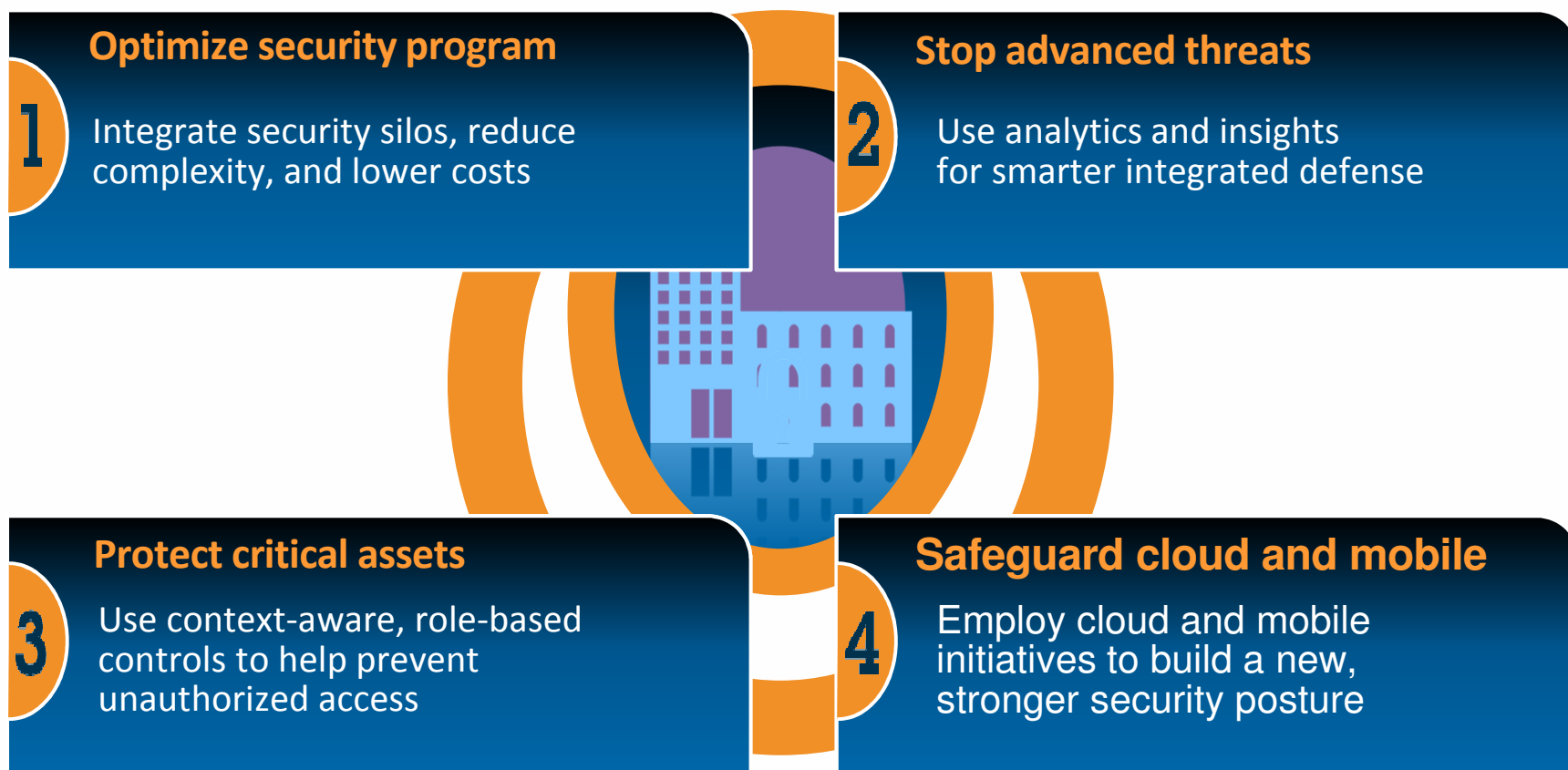**10B+** Commuters get to work with the help of IBM Cloud

IBM Security

13 Security market segments with industry leading capabilities

10 IBM Security Operations Centers (SOCs)

133 IBM Security supported countries

6K+ IBM Security professionals worldwide

10K+ IBM Security customers worldwide

270M+ Endpoints protected from the cloud

20B Customer security events monitored each day

X-FORCE Industry leading security research team

IBM Security will be essential to clients in 2015

Optimize security program

1 Integrate security silos, reduce complexity, and lower costs

Stop advanced threats

2 Use analytics and insights for smarter integrated defense

Protect critical assets

3 Use context-aware, role-based controls to help prevent unauthorized access

Safeguard cloud and mobile

4 Employ cloud and mobile initiatives to build a new, stronger security posture

Seize the Moment. Dive into Next Generation Technologies.

1

Optimize your security program

1

Risk-Aware Culture & Strategy

End-to-End Security Intelligence

Intelligent Threat Protection & Response

Assess and transform your security maturity

Build a next generation security operations capability

Get help from the experts

Seize the Moment. Dive into Next Generation Technologies.

1

Stop advanced threats

2

Protect against fraud and targeted attacks

Detect advanced threats with security intelligence

Deploy integrated security

Seize the Moment. Dive into Next Generation Technologies.

1

Protect critical assets

3

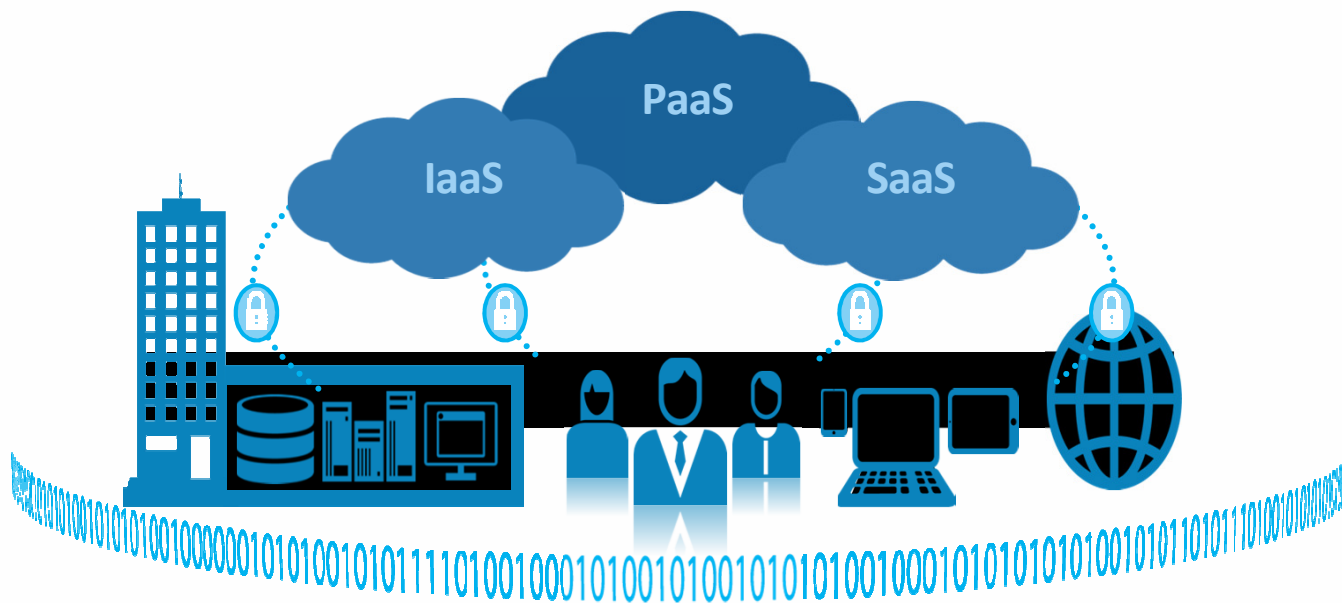**Use context-aware controls to prevent unauthorized access**

Identify and protect your "crown jewels"

Manage application security risk

Seize the Moment. Dive into Next Generation Technologies.

Safeguard cloud and mobile

4

PaaS

IaaS

SaaS

Maintain cloud visibility and control

Help protect the mobile enterprise

Seize the Moment. Dive into Next Generation Technologies.

Introducing the world's most comprehensive portfolio of cloud security products and services

IBM Cloud Security

Seize the Moment. Dive into Next Generation Technologies.

© 2014 IBM Corporation
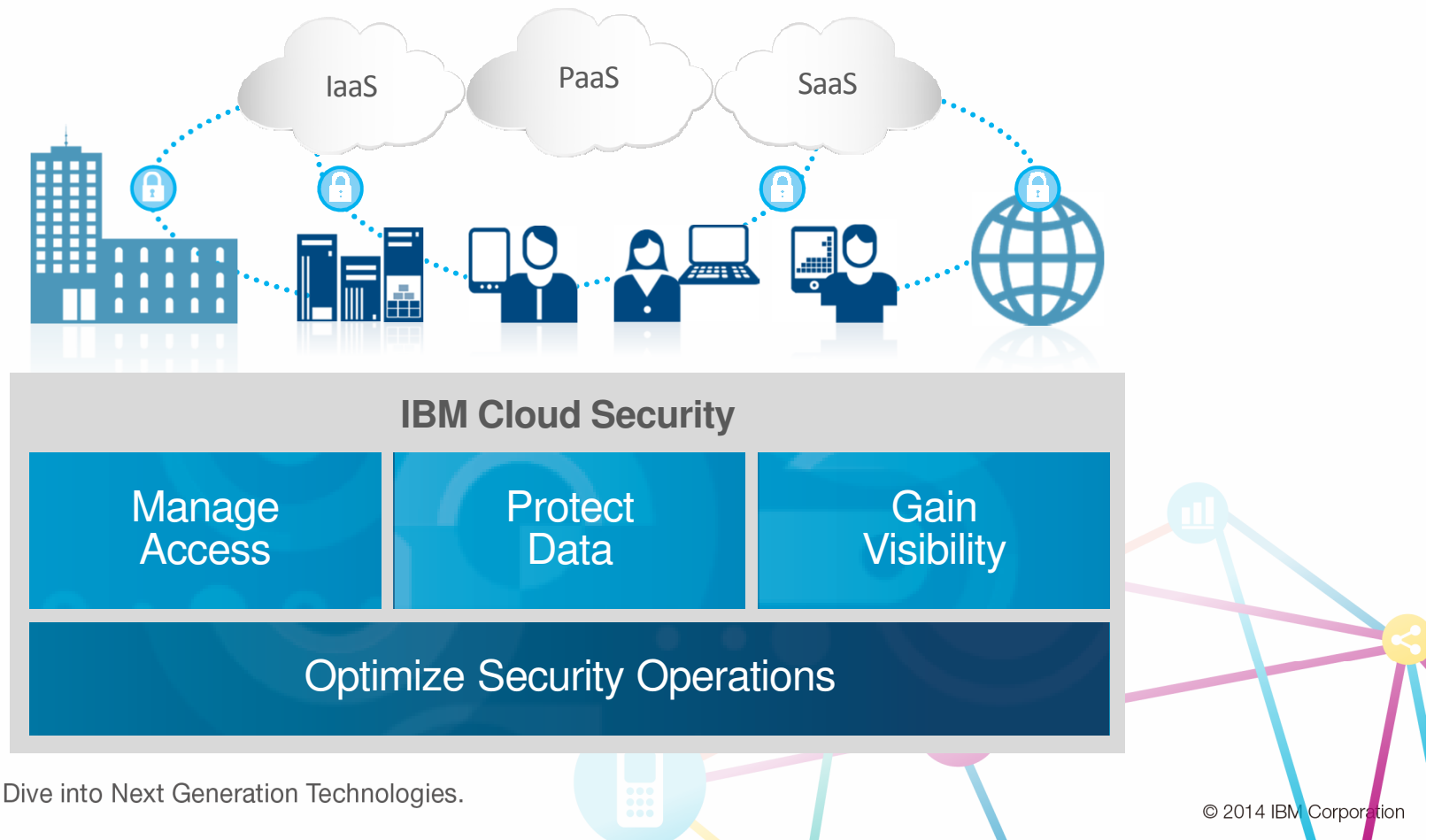
Help securely connect people, devices, and applications to the cloud

Manage identity and access with speed

NEW! **Cloud Identity Services**
Easily onboard and manage users through IBM-hosted infrastructure and expertise

Safeguard access to cloud-deployed apps

NEW! **Cloud Sign On Service** *(for Bluemix)*
Allow developers to quickly introduce single sign on to web and mobile apps via APIs with OpenID, OAuth 2.0 support

NEW! **Cloud Access Manager** *(for SoftLayer)*
Defend cloud applications with pattern-based protection, multi-factor authentication, and context-based access control

Govern privileged user access

NEW! **Cloud Privileged Identity Manager** *(for SoftLayer)*
Audit privileged SoftLayer accounts and track app-to-app credentials

Manage Access	Protect Data	Gain Visibility

Optimize Security Operations

Identify vulnerabilities and prevent attacks targeting sensitive data

Protect enterprise data in cloud repositories

NEW! **Cloud Data Activity Monitoring** *(for SoftLayer and AWS)*

Automatically discover, classify, and assess, monitor, and audit sensitive data access in cloud repositories

NEW! **Cloud Data Encryption and Key Management** *(partner offerings for Bluemix and SoftLayer)*

Store and encrypt data in data services and manage keys on Bluemix (with Cloudant or Analytics Warehouse Service)

Encrypt data and manage keys on SoftLayer (with Vormetric)

Discover vulnerabilities in cloud and mobile apps

NEW! **Cloud Web and Mobile Application Analyzer Services** *(for Bluemix)*

API-based access to application scanning services to help developers easily identify and remediate vulnerabilities in web applications (Dynamic Analyzer) and mobile apps (Mobile Analyzer) prior to placing them into production or app stores

Manage Access	Protect Data	Gain Visibility

Optimize Security Operations

Continuous monitoring for security breaches and compliance violations

Dynamically analyze security posture of users, apps, networks, and other assets across the enterprise and in the cloud

NEW! **Cloud Security Intelligence**
(QRadar support for hybrid clouds and SoftLayer)

- Integration with multiple cloud services
  - IBM SoftLayer
  - Amazon CloudTrail
  - Salesforce.com
  - Zscaler
  - Qualys
  - CloudPassage
  - IBM Security Trusteer Apex
  - OpenStack

- Deployment on SoftLayer and/or Amazon Web Services for visibility across physical, virtual, and cloud infrastructures

SOFTLAYER an IBM Company

IBM Bluemix

IaaS   **PaaS**   **SaaS**

Manage Access	Protect Data	Gain Visibility

Optimize Security Operations

Optimize security intelligence and operations for the cloud

Deploy intelligence-driven security maturity across all environments

IBM security experts to help keep your cloud secure and compliant

Enhanced monitoring and correlation of hybrid cloud security events

NEW! Security Intelligence and Operations Consulting Services

Assess security practices, plan, design and build out world-class Security Operations Centers to extend security to the cloud
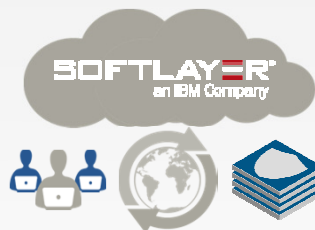
NEW! Cloud Security Managed Services *(for SoftLayer)*

Highly trained analysts in global Security Operations Centers manage security and provide emergency response services

NEW! Intelligent Threat Protection Cloud

Consolidated view using big data, visualization, and intelligent threat analysis with expert knowledge to respond to security incidents
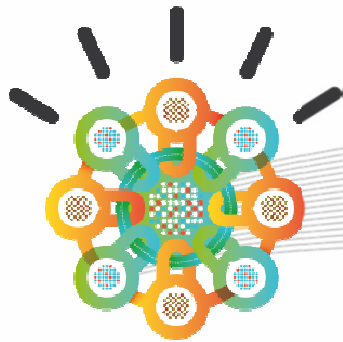
| Manage Access | Protect Data | Gain Visibility |

Optimize Security Operations

Learn more about IBM Security

IBM Security

Intelligence. Integration. Expertise.
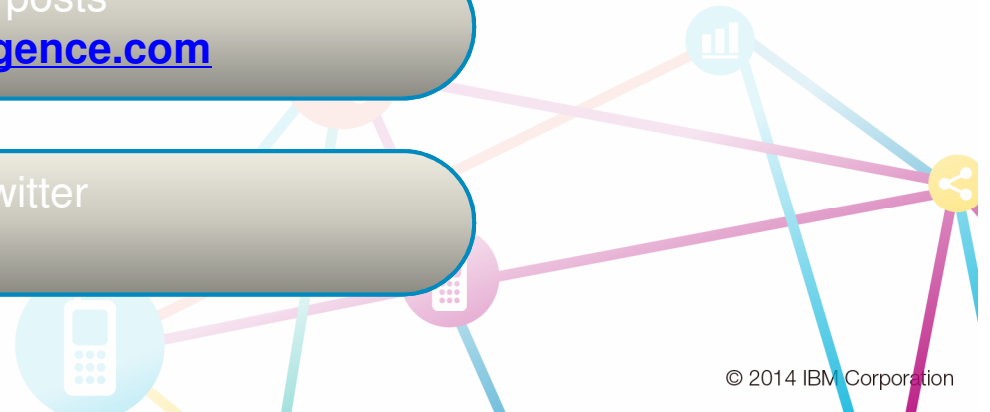
Visit our website
IBM Security Website

Watch our videos
IBM Security YouTube Channel

Read new blog posts
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity

Seize the Moment. Dive into Next Generation Technologies.

IBM SolutionsConnect 2015

Seize the Moment. Dive into Next Generation Technologies.

Thank You

IBM