TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

Security of Cloud Computing for the Power Grid

Industry Panel

November 12, 2014

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

Please Note

- Where a specific IBM product or service is mentioned, 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.

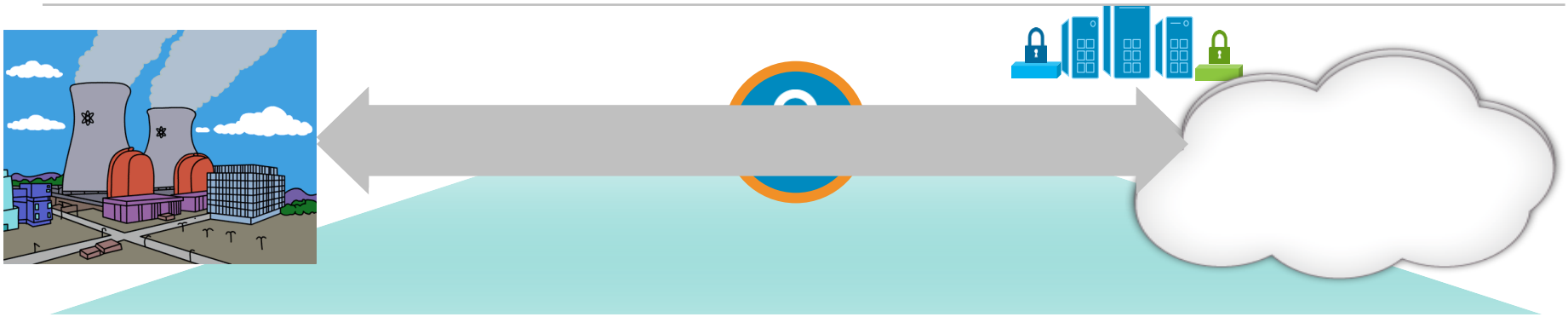
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, 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.

Security objectives reflect Cloud adoption

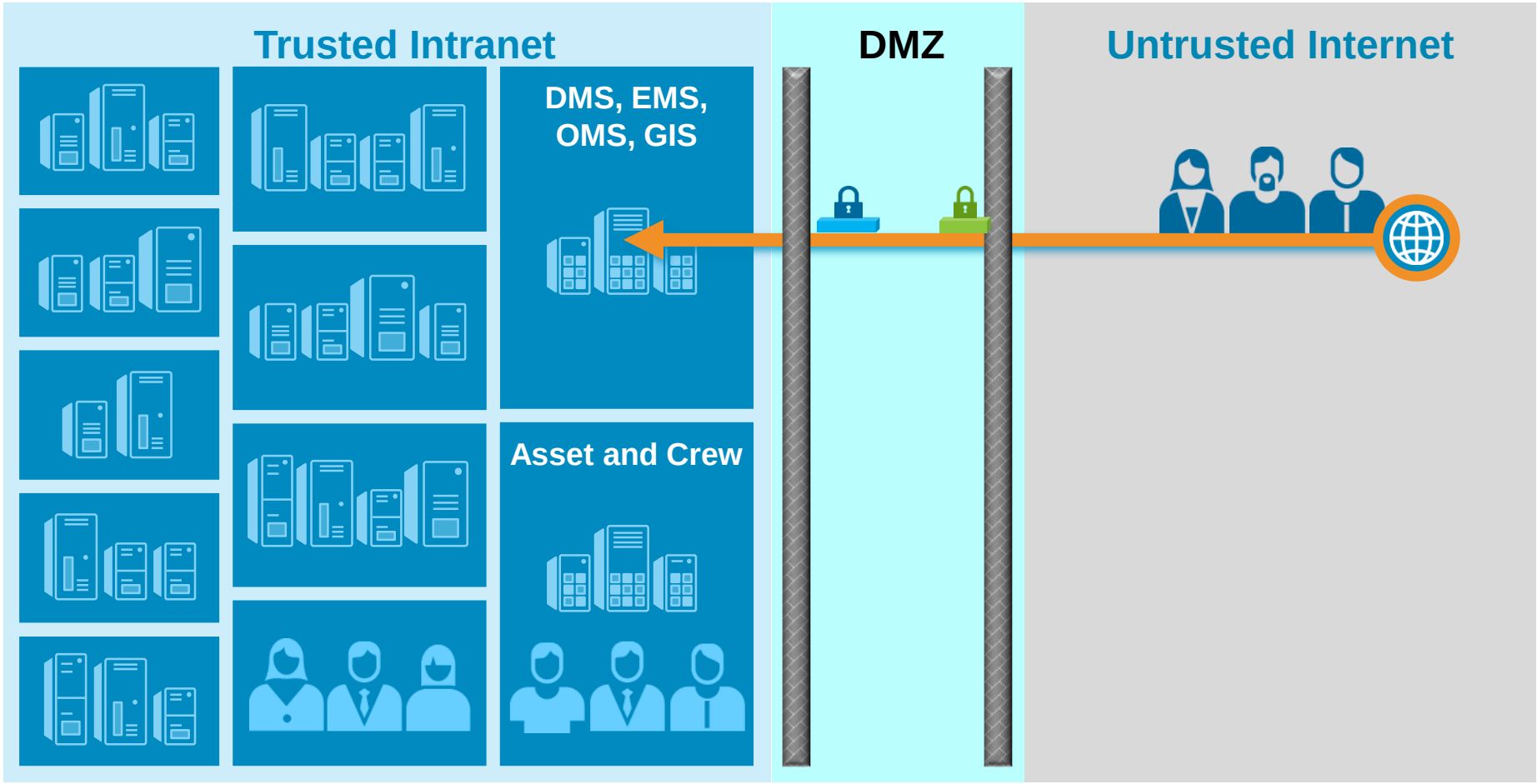
Security objectives reflect Cloud adoption

Securely connect and consume Cloud business applications (SaaS)

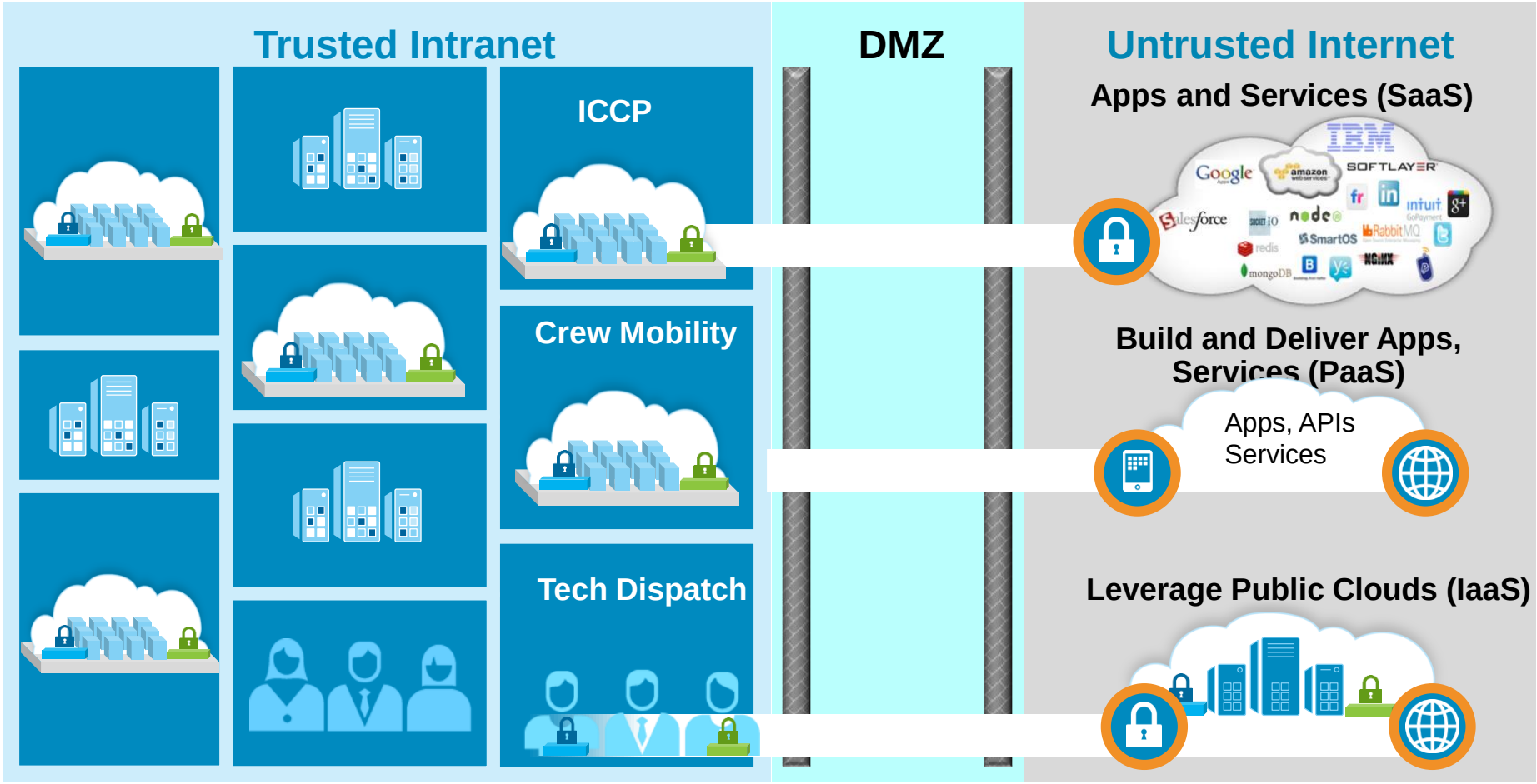
Services	Organization	Security Responsibilities and Objectives
Software as a Service (SaaS)	VP T&D, VP Gen, CNO, …	▪ Complete visibility to SaaS usage and risk profiling ▪ Governance of user access to SaaS and identity federation



Traditional perimeter based security controls …



… are changing to security centered around applications and data



Three imperatives for improving security

Understand who is accessing the cloud from anywhere, at anytime

Govern the usage of cloud

"Going to the cloud gives me a single choke point for all user access – it provides much more control."

Fix vulnerabilities and defend against attacks before they're exploited

Secure workloads and data

"Cloud gives me security APIs, preconfigured policies and a structured way to manage security of my data and workloads"

Obtain a complete view of cloud and traditional environments

Detect cloud threats with full visibility

"I can take advantage of centralized logging and auditing interfaces to get a full view of my security posture and hunt for attacks."

Three sets of security capabilities

SaaS: Secure usage of business applications

PaaS: Secure service composition and apps

IaaS: Securing infrastructure and workloads

Cloud Security Capabilities

Manage Access

Manage identities and govern user access

Protect Data

Protect infrastructure, applications, and data from threats

Gain Visibility

Auditable intelligence on cloud access, activity, cost and compliance

… delivered via cloud-enabled technologies and managed services

KeneXa, workday., Google Apps, Salesforce, box, Dropbox, CONCUR

SaaS: Secure usage of business applications

Blue Mix, Windows Azure, force.com cloud platform

PaaS: Secure service composition and apps

SOFTLAYER, openstack, vmware, amazon web services

IaaS: Securing infrastructure and workloads

Cloud Security Capabilities

Manage Access

Manage identities and govern user access

Protect Data

Protect infrastructure, applications, and data from threats

Gain Visibility

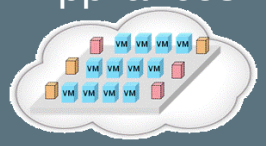
Auditable intelligence on cloud access, activity, cost and compliance

Client Consumption Models

Security SaaS

APIs

Virtual Appliances



Managed Security Services

Professional Security Services

Cloud Security Framework mapping security capabilities to Cloud stacks

	Manage Access	Protect Data	Gain Visibility
Software as a service (SaaS)			
Platform as a Service (PaaS)			
Infrastructure as a Service (IaaS)			

Use cases around IaaS and sample security capabilities

	Manage Access	Protect Data	Gain Visibility
Software as a Service (SaaS)			
Platform as a Service (PaaS)			
Infrastructure as a Service (IaaS)	Manage cloud administration and workload access • Privileged admin management • Access management of web workloads	Protect the cloud infrastructure to securely deploy workloads • Storage encryption • Network protection – firewalls, IPS • Host security, vulnerability scanning	Security monitoring and intelligence • Monitor hybrid cloud infrastructure • Monitor workloads • Log, audit, analysis and compliance reporting

Use cases around protection and sample security capabilities

	Manage Access	Protect Data	Gain Visibility
Software as a Service (SaaS)		Secure connectivity and data movement to SaaS • Data tokenization • Secure proxy to SaaS • Application control	
Platform as a Service (PaaS)		Build and deploy secure services and applications • Database encryption • App security scanning • Fraud protection and threats	
Infrastructure as a Service (IaaS)		Protect the cloud infrastructure to securely deploy workloads • Storage encryption • Network protection – firewalls, IPS • Host security, vulnerability scanning	

Hybrid cloud adoption requires integrated security solutions

	Manage Access	Protect Data	Gain Visibility
Software as a service (SaaS)	Enable employees to connect securely to SaaS • SaaS access governance • Identity federation	Secure connectivity and data movement to SaaS • Data tokenization • Secure proxy to SaaS • Application control	Monitoring and risk profiling of enterprise SaaS usage • Monitor SaaS usage • Risk profiling of SaaS apps • Compliance reporting
Platform as a Service (PaaS)	Integrate identity and access into services and applications • DevOps access management • Authentication and authorization APIs	Build and deploy secure services and applications • Database encryption • App security scanning • Fraud protection and threats	Log, audit at service and application level • Monitor application, services and platform • Service vulnerabilities • Compliance reporting
Infrastructure as a Service (IaaS)	Manage cloud administration and workload access • Privileged admin management • Access management of web workloads	Protect the cloud infrastructure to securely deploy workloads • Storage encryption • Network protection – firewalls, IPS • Host security, vulnerability scanning	Security monitoring and intelligence • Monitor hybrid cloud infrastructure and workloads • Log, audit, analysis and compliance reporting

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

Manage Access

Securely connect people, devices, and applications to the cloud

Manage identity and access with speed

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

Safeguard access to cloud applications

Cloud Federated Identity Management *(SaaS)*
Allow employees to access SaaS applications through identity federation

Cloud Sign On Service *(e.g. Blue Mix)*
Allow developers to quickly introduce single sign on to web and mobile apps via APIs with OpenID, OAuth 2.0 support

Cloud Access Manager *(e.g. Soft Layer)*
Defend cloud applications with pattern-based protection, multi-factor authentication, and context-based access control

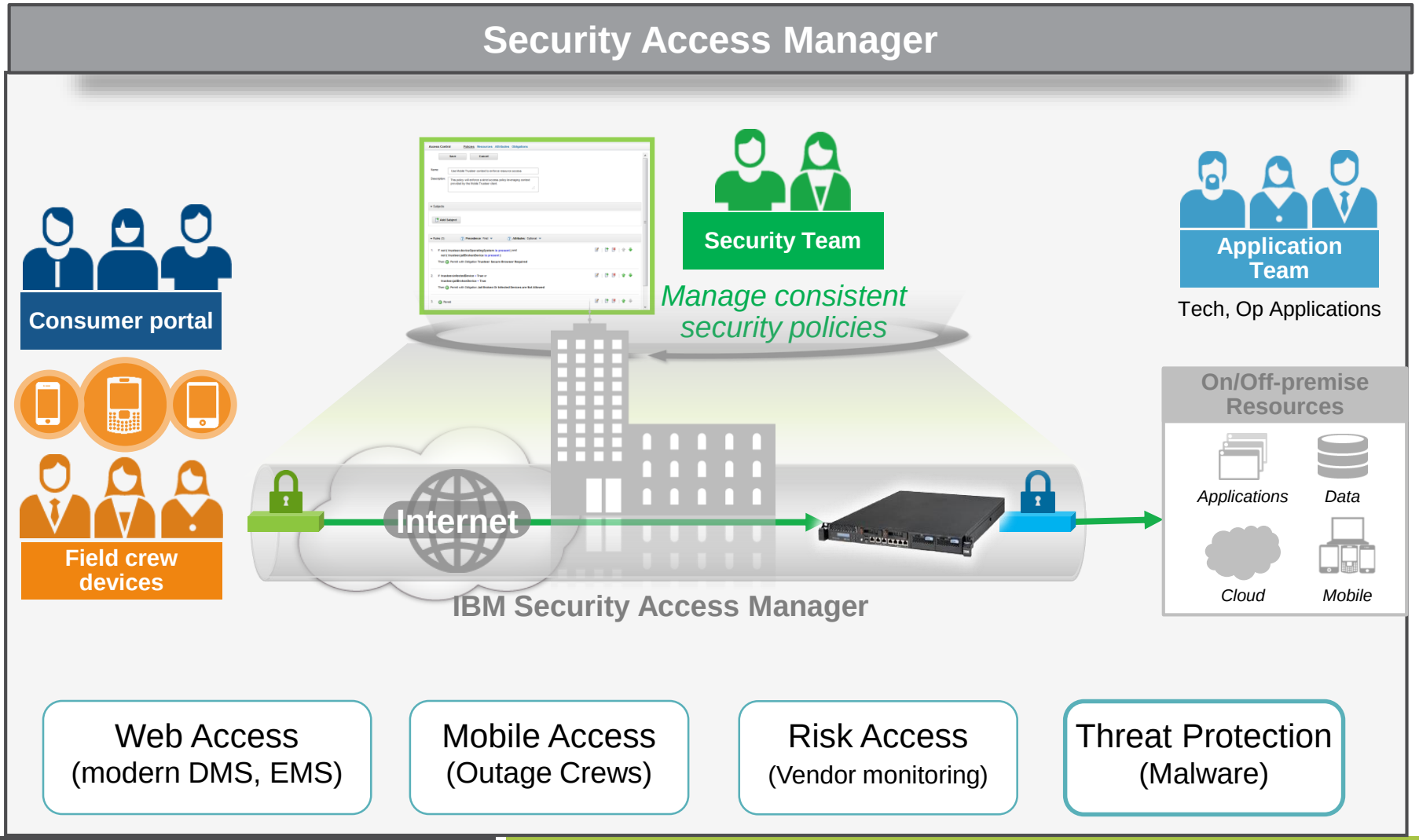
Govern privileged user access

Cloud Privileged Identity Manager *(e.g. Soft Layer)*
Audit privileged Soft Layer accounts and track app-to-app credentials

Manage Access | Protect Data | Gain Visibility

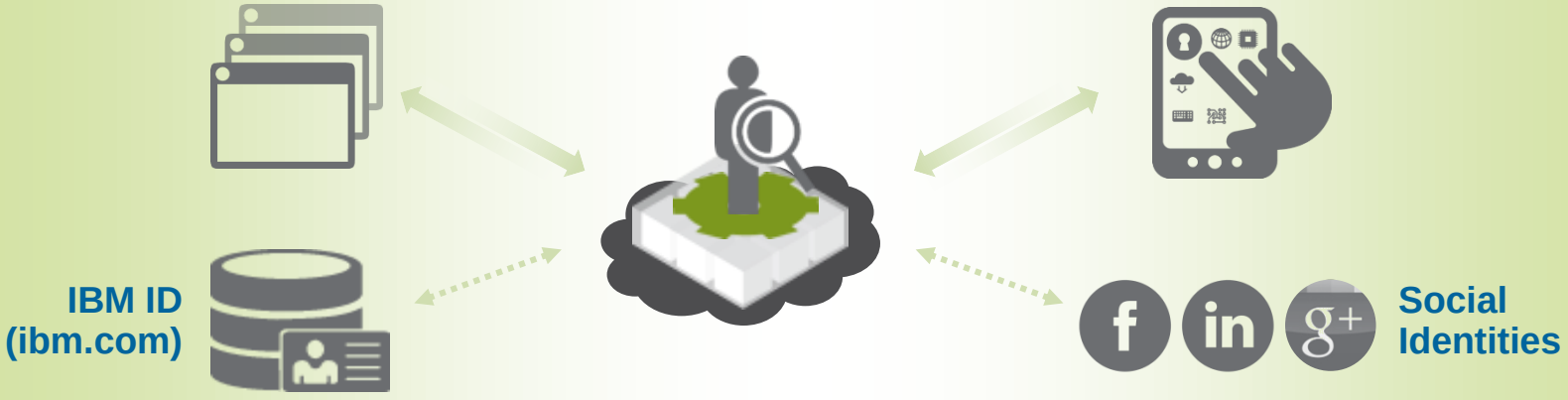
Optimize Security Operations

Defend web workloads running on Cloud
(e.g. Soft Layer)



Manage Access

Example API identity security for app developers



Single-Sign-On (e.g. Blue Mix)

Solution Benefits

- Easily add user authentication and single sign on to on-premise and cloud applications
- APIs for single-sign-on via utility and social identities for consumer web and mobile apps
- Support for open standards (e.g., OpenID, OAuth 2.0)

Monitor privileged user access on Cloud (e.g. Soft Layer)

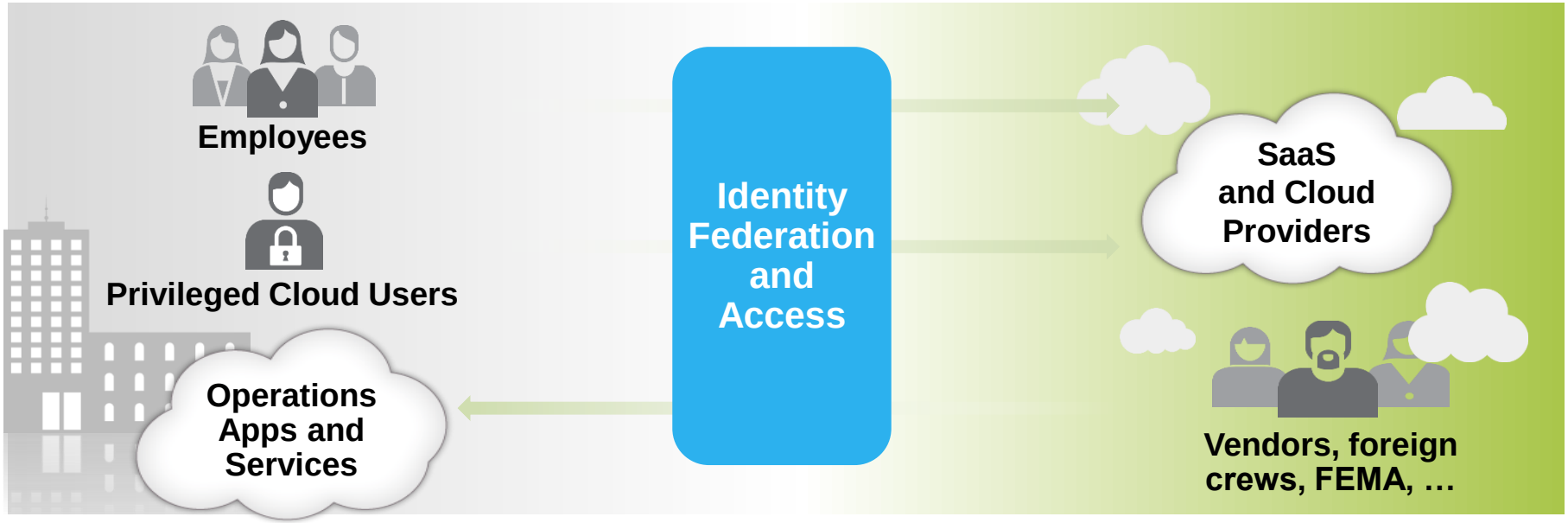
Security Privileged Identity Manager *(e.g. Soft Layer)*

Security Privileged Identity Manager

Solution Benefits

- Manage cloud services (e.g. IBM Soft Layer) administrative accounts from on-premise PIM (i.e., Soft Layer “adapter”)
- Monitor and track usage, control shared access
- Approve, revalidate privileged IDs and shared ID pools
- Automate Single Sign On and password management including strong authentication
- Optional Session Recorder and PIM for applications
- Common identity infrastructure for privileged and non-privileged users, in the data center and on the cloud

Safeguard user access to cloud properties



Security Federated Identity Manager

Solution Benefits

- Enables web single sign on across applications
- Access controls on cloud applications
- Provide users with the ability to single sign on to multiple web-based cloud applications with disparate user IDs / passwords
- Self-service identity registration, validation and processing user credentials

Protect Data

Protect data and identify vulnerabilities targeting sensitive data

Discover vulnerabilities before putting cloud and mobile apps into production

Cloud Web and Mobile Application Analyzers
(e.g. Blue Mix)

- Scan web and mobile applications prior to putting them into production

Monitor data activities in cloud repositories

Cloud Data Activity Monitoring
(e.g. Soft Layer and AWS)

- Monitor sensitive data access in cloud repositories and create centralized auditing for data sources deployed on cloud virtual images

Protect enterprise data in cloud

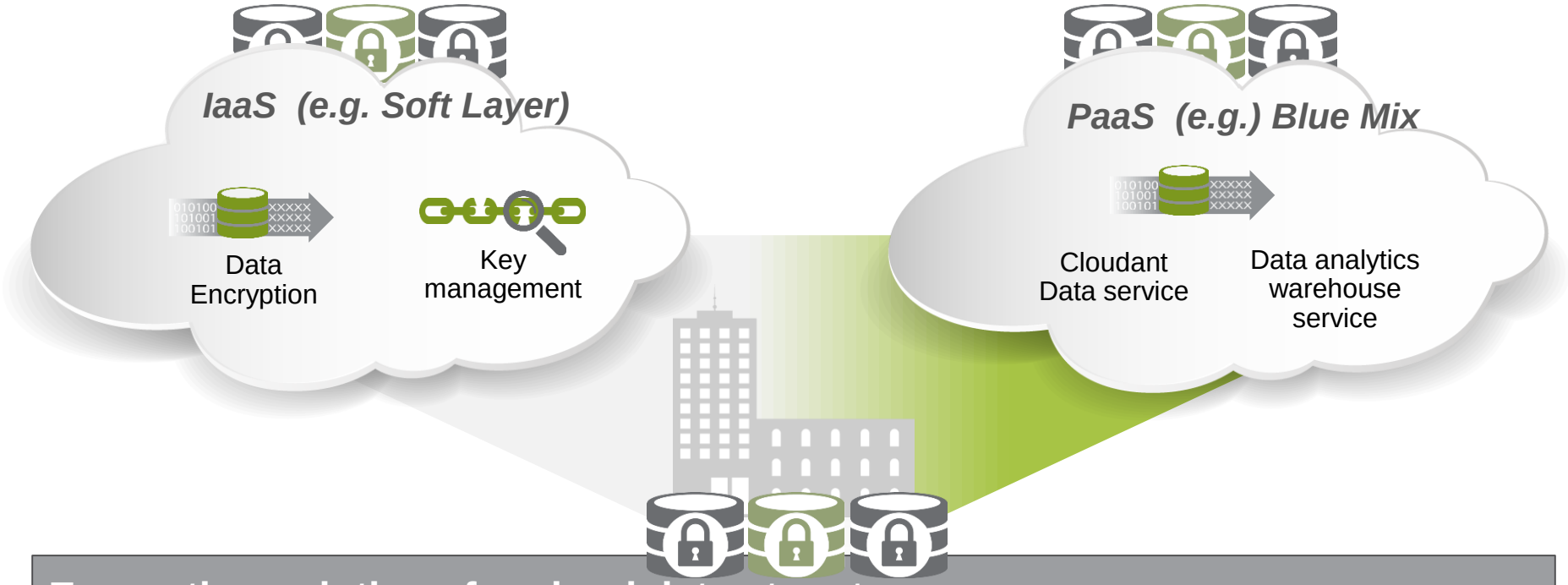
Cloud Data Encryption *(e.g. Soft Layer and Blue Mix)*

- Encrypt files in your cloud instances (e.g. Soft Layer)
- Encrypt data in Cloud Data services (e.g. Cloudant, dashDB)

Manage Access | **Protect Data** | Gain Visibility

Optimize Security Operations

Encrypt data at rest in the cloud

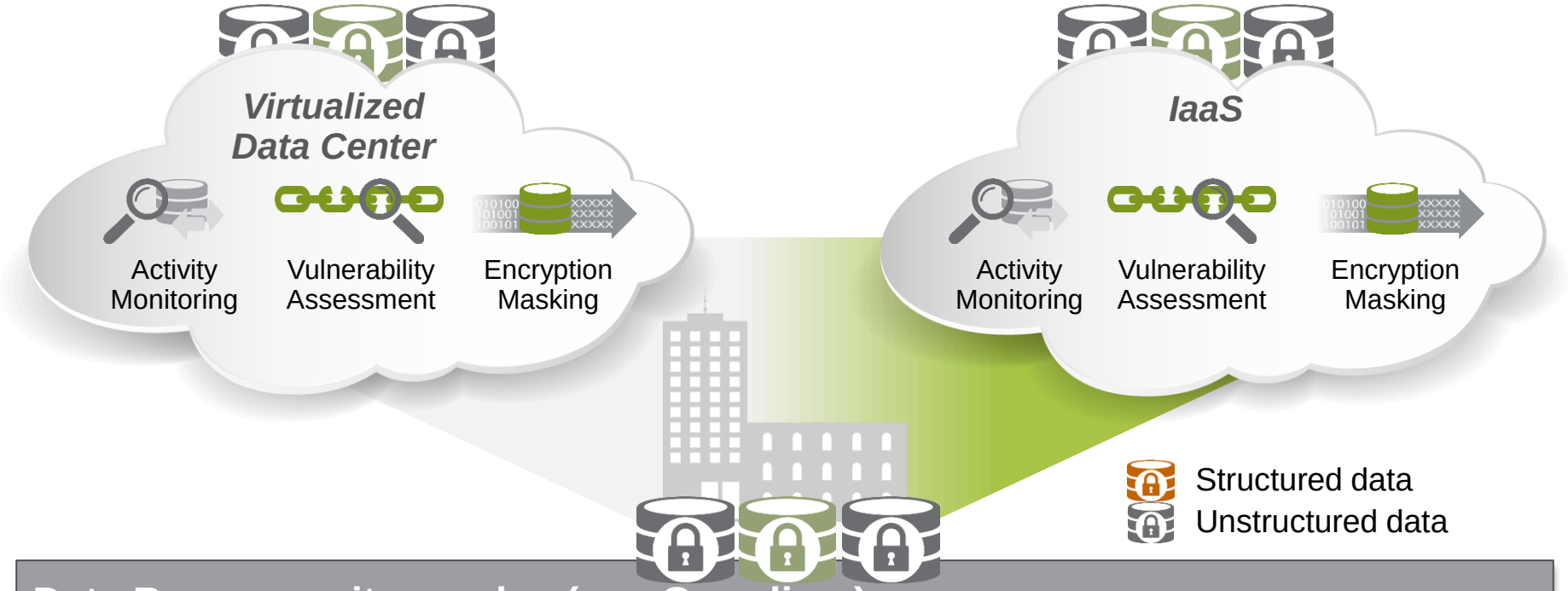


Encryption solutions for cloud data at rest

Solution Benefits

- Encrypt data at rest on Soft Layer using partner solutions.
- When developers store data in Cloud data services (e.g. Cloudant, dashDB), data can be encrypted and secured
- Utility can manage the key management, key rotation

Extend data security and privacy to the cloud

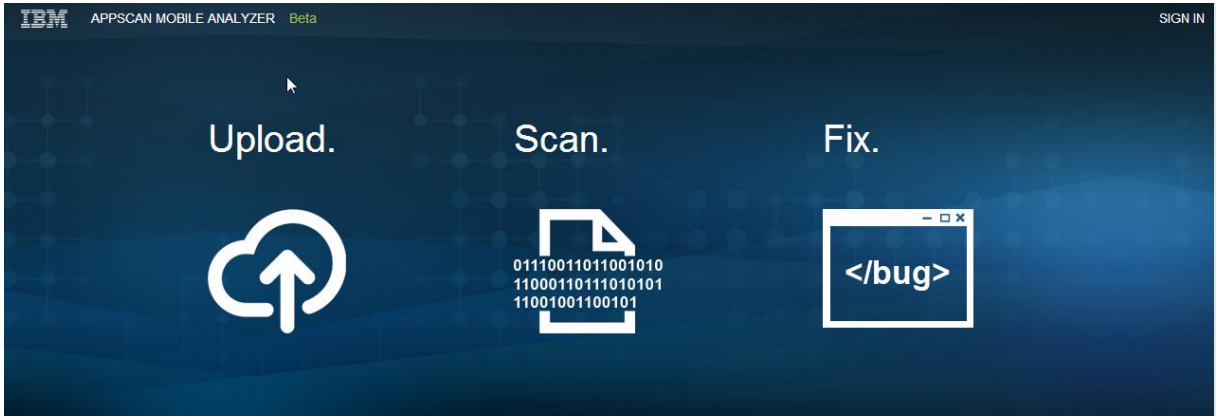


Data Base security overlay (e.g. Guardium)

Solution Benefits

- Data security as a virtual appliance deployed on the cloud
- Data activity monitoring to verify and audit data outsourced to the cloud
- Vulnerability assessment to harden data sources on the cloud
- Encrypt and mask sensitive data to protect privacy of data in the cloud

Changing the way developers build more secure applications



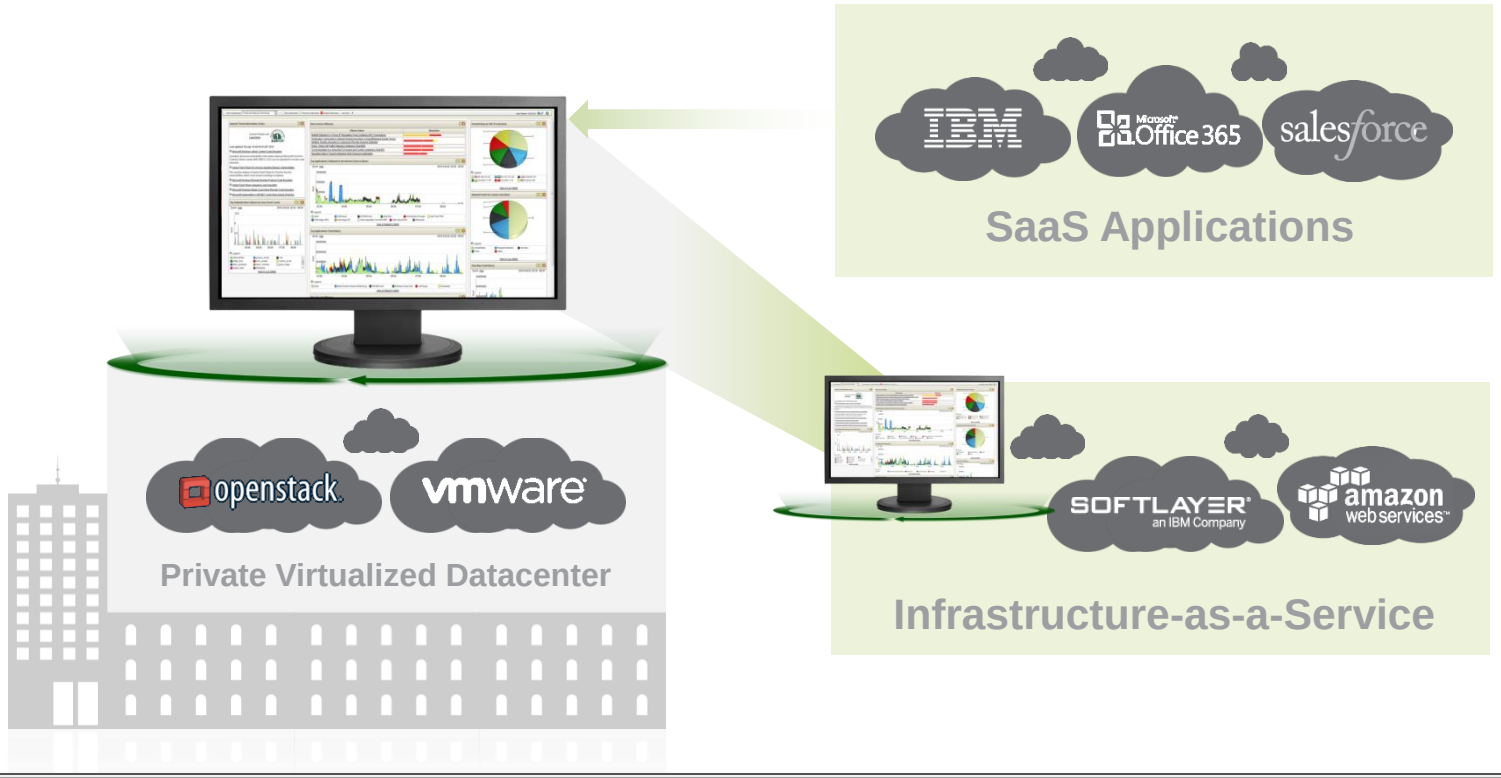
Source Code Security (e.g. AppScan)

Solution Benefits

- Mobile Analyzer permits app scanning via API prior to deployment in app repositories
- Dynamic Analyzer permits code scanning prior to being placed into production
- Minimal tech training and preparation required
- Detailed report containing potential vulnerabilities is generated immediately
- Comprehensive report formulates action plan for vulnerability remediation if utility has a BYOD policy

Gain Visibility

Security Intelligence for the hybrid cloud



Security Incident and Event Manager (e.g. QRadar)

Solution Benefits

- Improved security and visibility into virtual Infrastructures
- Better visibility into logs coming from their sensors across the environment
- Support ad hoc search across large data

IBM Security solutions for the Hybrid Cloud

Manage Access

Safeguard people, applications, and devices connecting to the cloud

- Cloud Identity Services
- Cloud Sign On Service
- Cloud Access Manager

Protect Data

Identify vulnerabilities and help prevent attacks targeting sensitive data

- Cloud Data Activity Monitoring
- Cloud Mobile App Analyzer Service
- Cloud Web App Analyzer Service

Gain Visibility

Monitor the cloud for security breaches and compliance violations

- Cloud Security Intelligence

Optimize Security Operations

Deliver a consolidated view of your security operations – at unprecedented speed and agility

- Security Intelligence and Operations Consulting Services
- Cloud Security Managed Services

Security addressing multiple Cloud scenarios

Security for the Cloud

Securing workloads on virtual infrastructures

Public Cloud

Secure usage of Public Cloud applications

Private Cloud

Protect applications, infrastructure and workloads in private Cloud stacks

Security from the Cloud

Delivering and consuming secure applications

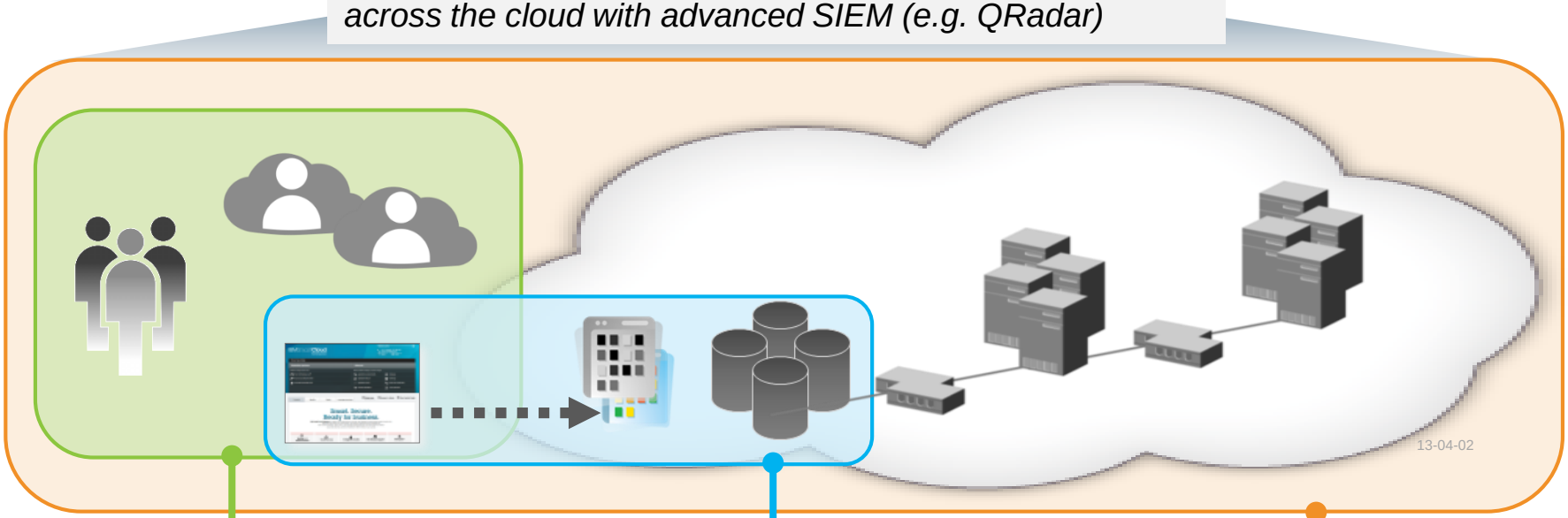
Security-as-a-Service

Deliver security capabilities as cloud services

Intelligent Security for the Cloud

Establish intelligence across the cloud

Establish a platform with real-time correlation and detection across the cloud with advanced SIEM (e.g. QRadar)



Manage identities and access

*Protect user access to cloud assets with **Identity & Access Management***

Monitor and audit applications and data

Deliver secure mobile and web apps, and monitor data access in real time with source code, data base, XML encryption HW

Scan and protect the infrastructure from

*Protect servers, endpoints and networks against threats with **Network IPS/Protection**;*

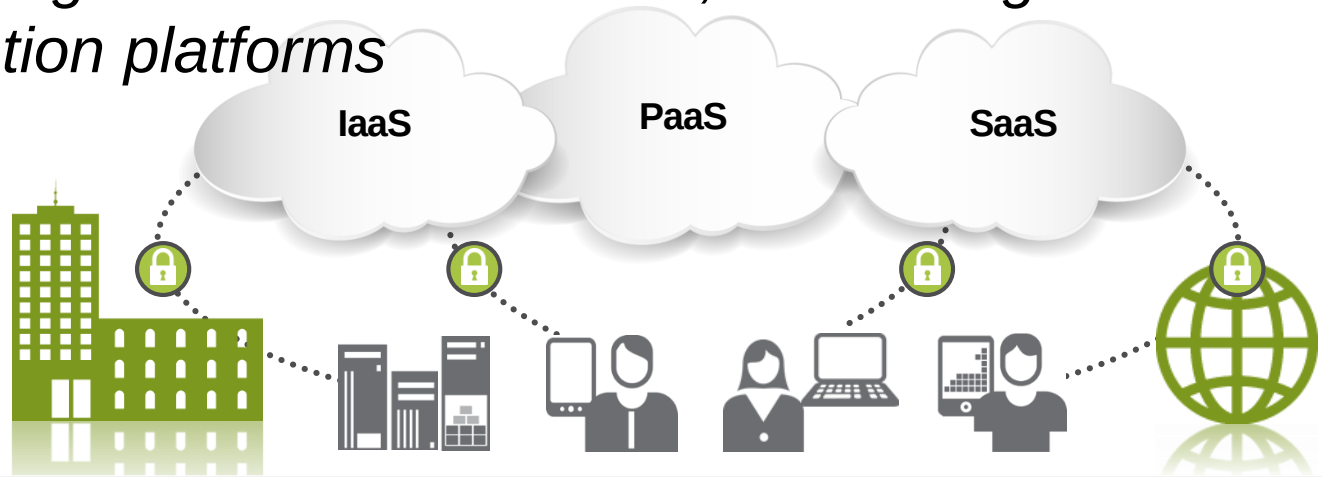
Endpoint/Mobile devices

4 Steps to Data Security in the Cloud

1	**Understand, define policy**	▪ Discover critical data relationships and schemas ▪ Discover where sensitive data resides ▪ Classify and define data types ▪ Define policies and metrics
2	**Secure and protect**	▪ Detect/block unauthorized/suspicious activity ▪ Encrypt, redact and mask virtualized databases ▪ De-identify confidential data in non-production environments
3	**Actively monitor and audit**	▪ Monitor virtualized databases and enforce review of policy exceptions ▪ Automate and centralize the controls needed for auditing and compliance (e.g., NERC CIP, NIST CSF, SOX, PCI) ▪ Assess database vulnerabilities
4	**Establish compliance and security intelligence**	▪ Automate reporting customized for different regulations to demonstrate compliance in the Cloud ▪ Integrate data activity monitoring with security information and event management (SIEM)

Integrated security for public and private clouds

Protecting the cloud data center, and next-gen business and application platforms



Manage Identities and Protect User Access	Monitor and Audit Applications and Data	Scan and Protect the Network from Threats	Establish Intelligence Across the Cloud
Security Solutions			
• Federated Identity Manager • Directory Integrator • Access Manager Virtual Appliance • Privileged Identity Manager	• Data Base (e.g. Guardium) • Source Code (e.g. AppScan) • Key Life Cycle Manager	• Network Protection • Intrusion Prevention System	• SIEM • Log Manager • Net Flow

Three Sets of Cloud Security Capabilities

- ✓ Identity
- ✓ Protection
- ✓ Insight

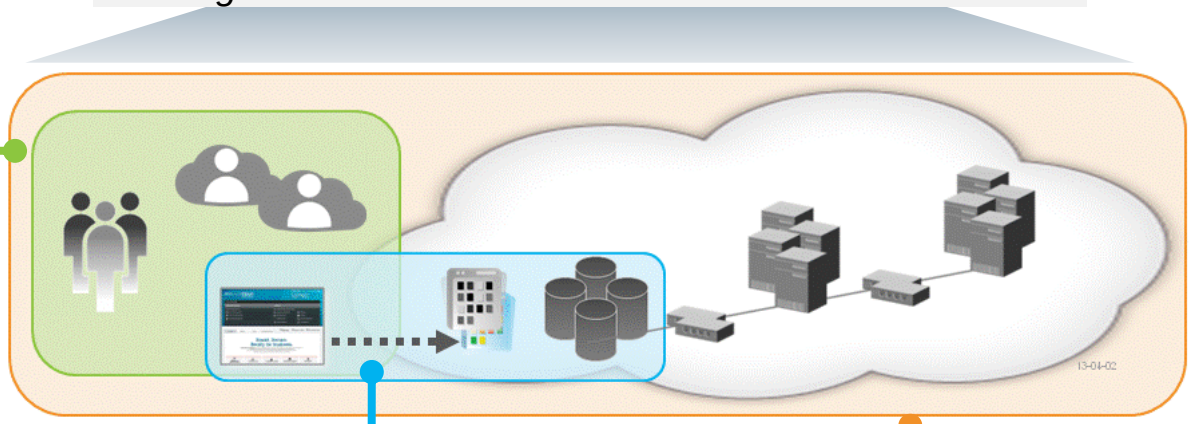
Insight
Establish intelligence across enterprise and cloud

Establish a platform with real-time correlation and detection across the cloud with SIEM and Managed Virtual SOC

Identity
Manage users and their access to cloud

Protect user access to cloud assets with Identity & Access Management, and

Managed service offerings



Protection
Protect data, applications and infrastructure from threats and risks

Deliver secure applications and data – with application scanning, and data activity monitoring. Protect infrastructure against threats with network security and managed service offerings

Professional Security Services & Managed Security Services develop the strategies and the operational design for secure cloud computing models.

Additional Considerations

- Remote physical secured cabinet lock/unlock/surveillance/card key
- Federal agency ruling on virtualization of “cyber assets”
- Broader use of security as retaining reliable operation
  - Redundancy of Cloud Points of Presence
  - Speed guarantees for SCADA data communication

Acknowledgements and Disclaimers

Availability. References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates.

The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it 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, this presentation or any other materials. Nothing contained in this presentation 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.

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

— Please update paragraph below for the particular product or family brand trademarks you mention such as Web Sphere, DB2,Maximo, Clear Case, Lotus, etc

IBM, the IBM logo, ibm.com, [IBM Brand, if trademarked], and [IBM Product, if trademarked] are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or TM), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at

•"Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

•If you have mentioned trademarks that are not from IBM, please update and add the following lines:[Insert any special 3rd party trademark names/attributions here]

•Other company, product, or service names may be trademarks or service marks of others.