Hands-on Lab - Session 3024 Securing your microservices application on cloud

Sreekanth (Sreek) Iyer
Cloud Security Architect
IBM Watson & Cloud Platform - Security Developer Services

Karna Bojjireddy (Karna)
Program Director, Offering Management and Strategy
IBM Watson & Cloud Platform - Security Developer Services

Jeffrey Kwong
Software Engineer
Cloud Architecture & Solution Engineering

InterConnect 2017

Please note

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.

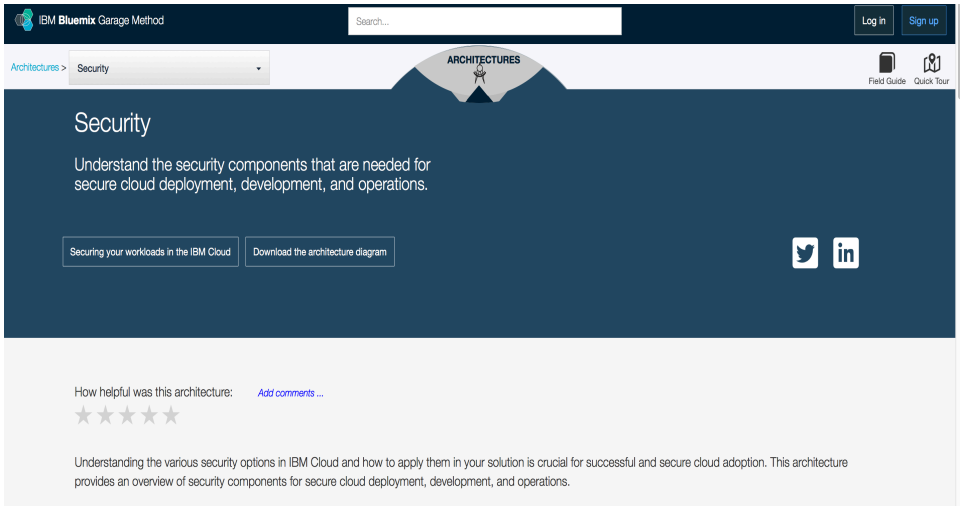
The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

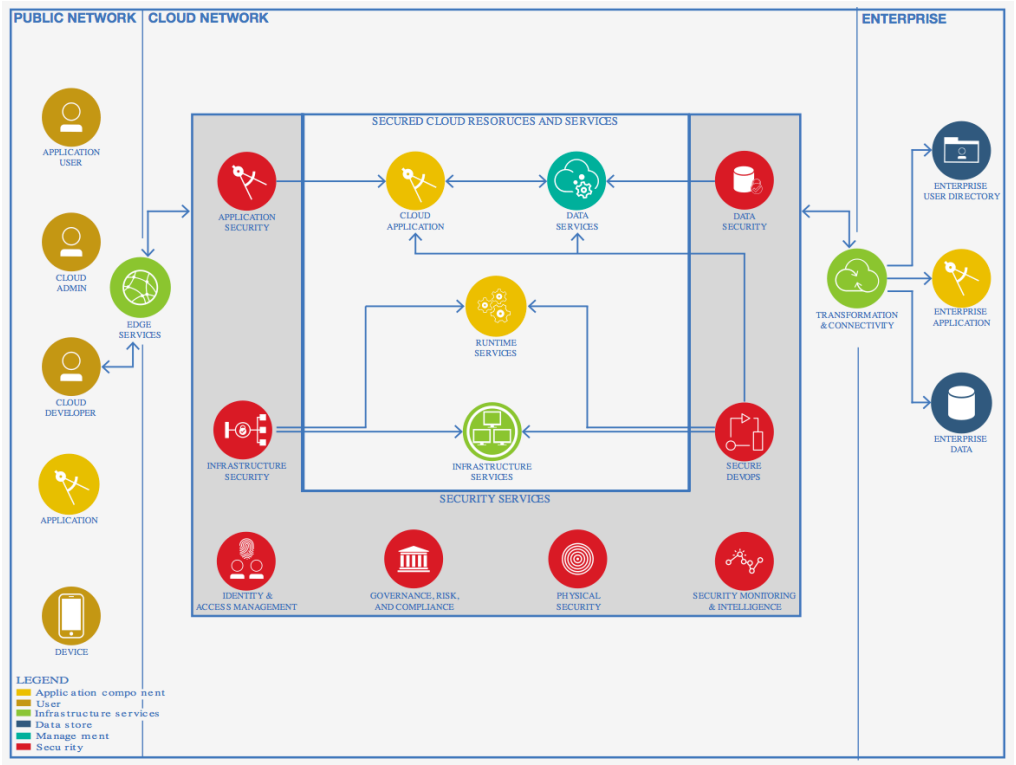
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream,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

Agenda

- Microservices & Reference Architecture for Cloud Native Application
- Security for the Cloud
    1. Identity & Access
    2. Network Security
    3. Data Protection
    4. Secure Dev-Ops
    5. Security Monitoring & Intelligence

Cloud Security Reference Architecture

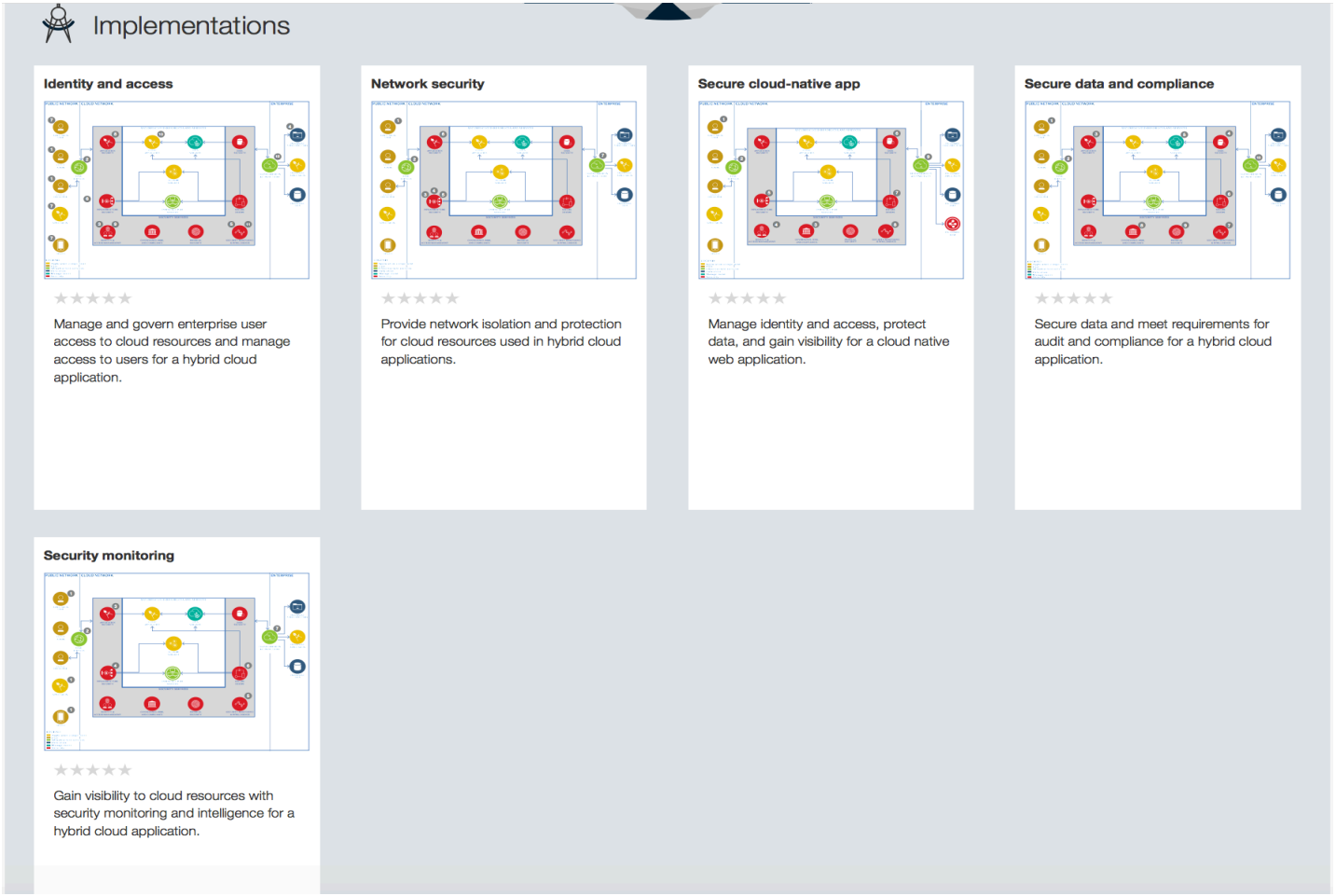




https://www.ibm.com/devops/method/content/architecture/securityArchitecture

Implementations

- Identity and Access
- Network Security
- Secure Data and Compliance
- Security Monitoring
- Secure Cloud-Native App



Agenda

- Microservices & Reference Architecture for Cloud Native Application
- Security for the Cloud
    1. Identity & Access
    2. Data Protection
    3. Secure Dev-Ops
    4. Security Monitoring & Intelligence

Log into IBM Cloud

Pre-requisites

You should have an IBM ID and registered for using IBM Bluemix
https://console.ng.bluemix.net
You should have a github account and access to https://github.com/ibm-cloud-architecture/refarch-cloudnative

Log into IBM Bluemix

Use your IBM ID and log into IBM Bluemix - https://console.ng.bluemix.net

Create security services & database instances

- Create an instance of AppID Service - https://console.ng.bluemix.net/catalog/services/mobile-client-access/
- Create an instance of Application Security on Cloud https://console.ng.bluemix.net/catalog/services/application-security-on-cloud/
- Create an instance of a IBM Key Protect service - https://console.ng.bluemix.net/catalog/services/key-protect/
- Create an instance of a Access Trail service - https://console.ng.bluemix.net/catalog/services/access-trail/
- Create the Database service instance (Cloudant NoSQL DB) https://console.ng.bluemix.net/catalog/services/cloudant-nosql-db
  - Name your Cloudant service name like refarch-cloudantdb

Create the microservices Application

Create the Customer Microservice

1. Follow the instructions here – https://github.com/jkwong888/refarch-cloudnative-micro-customer
2. Do a single deploy using the create toolchain button.

Create the web-UI microservice

- Please follow the instructions in this link - https://github.com/ibm-cloud-architecture/refarch-cloudnative-bluecompute-web
- cf push -n bluecompute-web-yourname -d mybluemix.net

1. Identity & Access

- Cloud IAM
- AppID

1 Customers want to manage two sets of Cloud users

Bluemix Platform users (through Platform IAM)	App Users (thru "IBM Bluemix App ID")

Manage platform identities

e.g., Developers login to Bluemix using IBM id

- Next Gen IBM ID
- Foundation to IBM Cloud & Digital
- Authentication & Federation
- SSO with IBM.com applications
- Service IDs and API keys

Granular access control

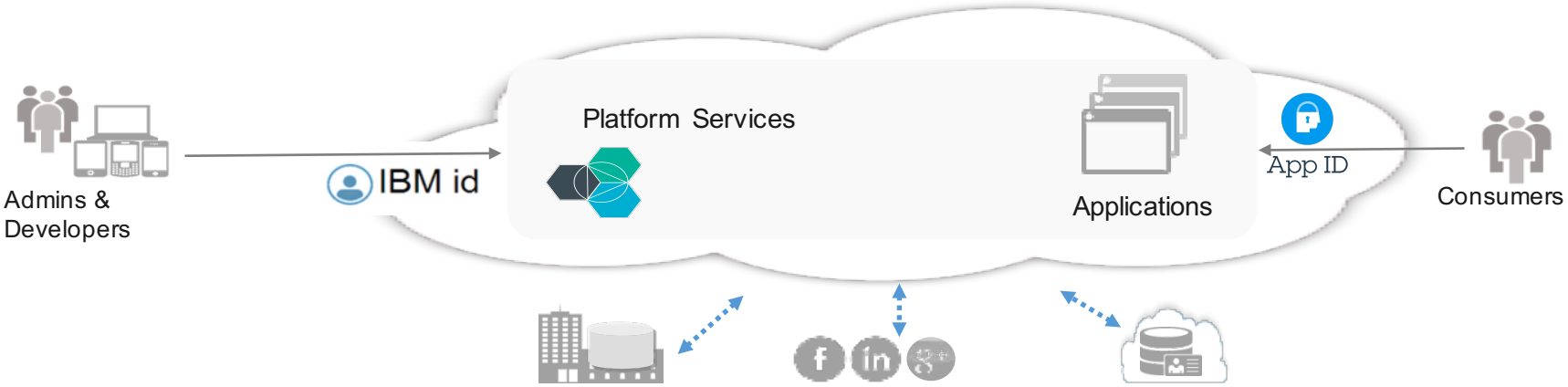
e.g., Configure that security admins can change encryption keys

- Service level access control
- Object level enabling privacy
- Consistent model across services, roles, users and apps

Application users and integration

e.g., Airline customers being directed to their rented car

- Application user authentications
- Progressive user profiling
- Developer focused APIs, SDKs
- Omni-channel interactions – web, mobile, IoT, API

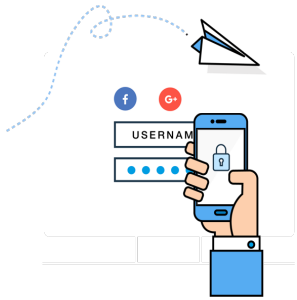


IBM Bluemix App ID

NEW

IBM Bluemix App ID helps developers to easily add authentication to their web and mobile apps with few lines of code, and secure their Cloud-native applications & services on Bluemix. App ID also helps manage user specific data that developers can use to build personalized app experiences.

Authentication



- Simple on-boarding wizard for a developer to have a working a sample app with Google and Facebook authentication
- Developers can quickly integrate authentication into their app using Client SDKs for iOS and Android, REST APIs, Server SDKs for node.js and Swift, and a customizable log in UI widget
- Secure Cloud native applications & services from unauthorized access using authentication filters
- Built with open standards (OAUTH2, OIDC)

User Profiles

- Store end user data, like app preferences, or info from their public social profiles that developers can leverage in their apps
- Support engagement for both anonymous and authenticated users. And if users start out anonymously and later authenticate, you can continue to use info previously stored for them

Implement Authentication (Social Login) for the Web-App

- Hands-on Exercise

2. Network & Application Security

- Network Isolation & Protection
- Application Security

2 Network security is getting re-defined, enabling defense-in-depth

Network security from the Cloud
e.g., Customers use Akamai to protect banking app from DDoS attacks

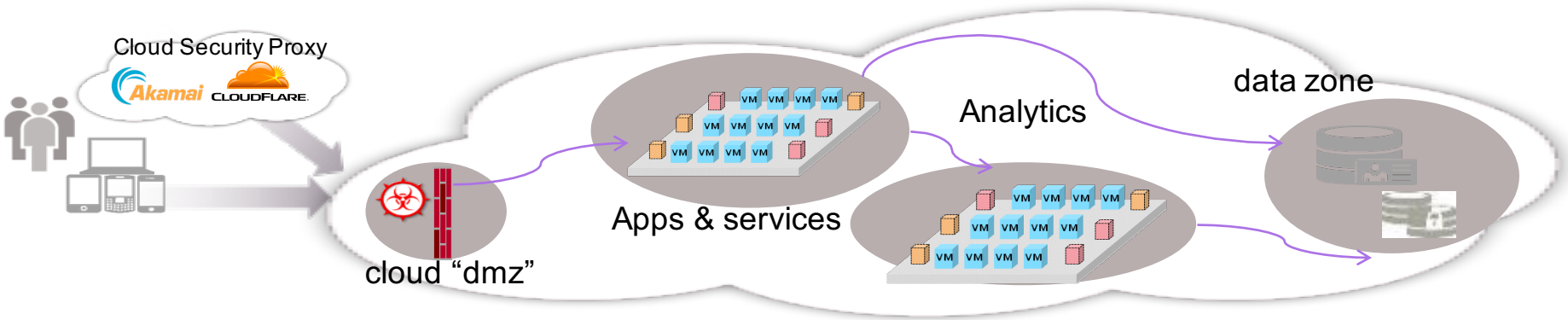
- Cloud hosted proxies
- Cloud-scale protection from DDoS
- Web application firewalls

Firewalls & IPS are table stakes
e.g., Customer uses firewall and IPS to build DMZ in Cloud

- Firewalls, Intrusion Prevention (IPS)
- Web application firewalls
- VPN for enterprise connectivity

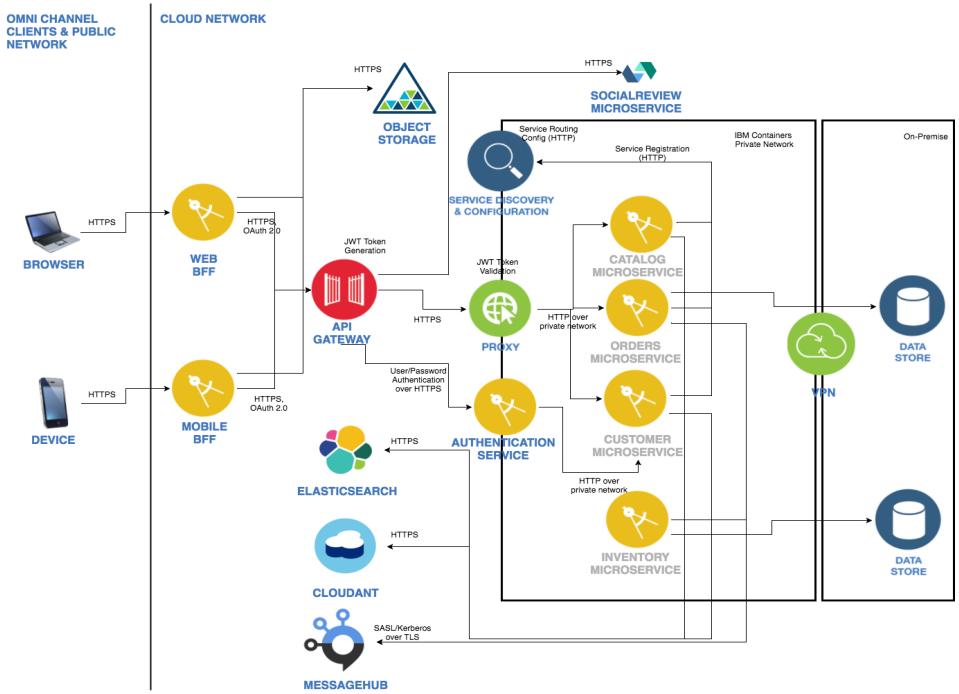
Micro-segmentation is evolving
e.g., Isolate data tier from web apps using network segments

- Software defined networks
- Network security groups
- Workload-centric connectivity and security



Application Security

- Mobile client and Web application accesses APIs hosted by IBM API Connect over HTTPs
- Mobile and Web client authenticates against the authentication service (redirected by APIC)
  - The authentication service communicates with the Customer Microservice over the private container network
- Mobile and Web client grant access to resources via OAuth 2.0 where APIC is the OAuth Provider
- API Connect generates JWT (JSON Web Token) to access the downstream Zuul proxy
- API Connect invokes Zuul proxy over HTTPs
- Zuul proxy validates the JWT Token to allow access only to APIC initiated workload
- Zuul invokes the data access microservices over Bluemix private network (Container Service)



https://github.com/ibm-cloud-architecture/refarch-cloudnative/blob/integration/static/security.md

3. Data Security

- Securing Data at Rest
- Securing Data in Motion

3 Data protection objectives drive Cloud deployment models

Classification-based decisions
e.g., CISOs decide that confidential data should be deployed in Bluemix Dedicated

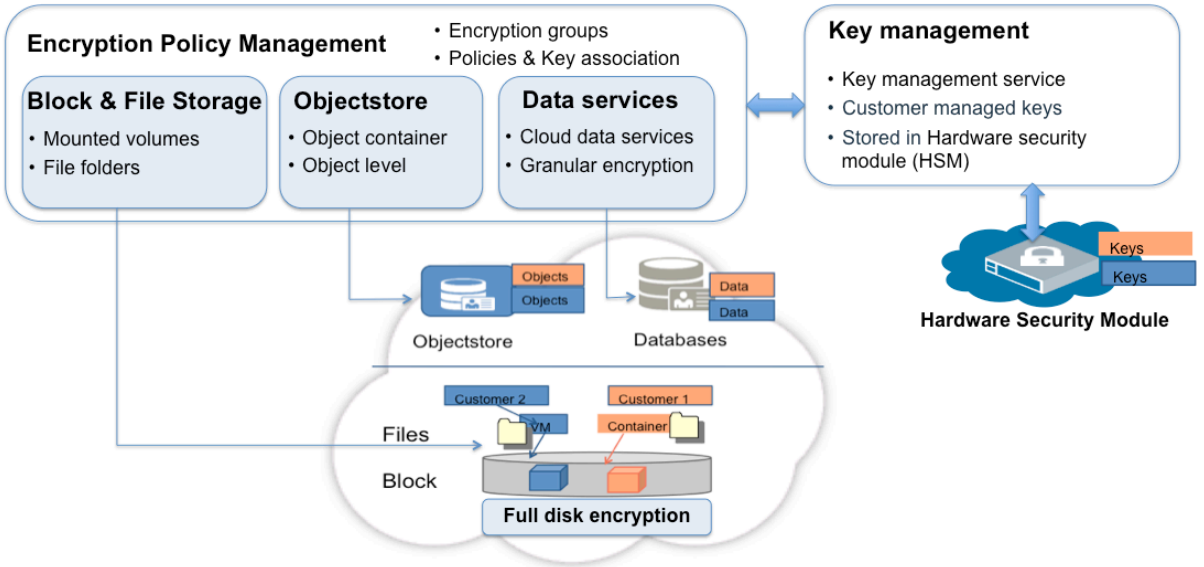
- Sensitive data stays on-prem
- Confidential data considered
- Regulatory compliance drives decisions

Policy driven encryption
e.g., Customer uses solution from partner (SecurityFirst) to encrypt all files in /confidential

- Consistency across storage types
- Files, Block, Objects, and Data services
- Policies reflecting data separation and risks

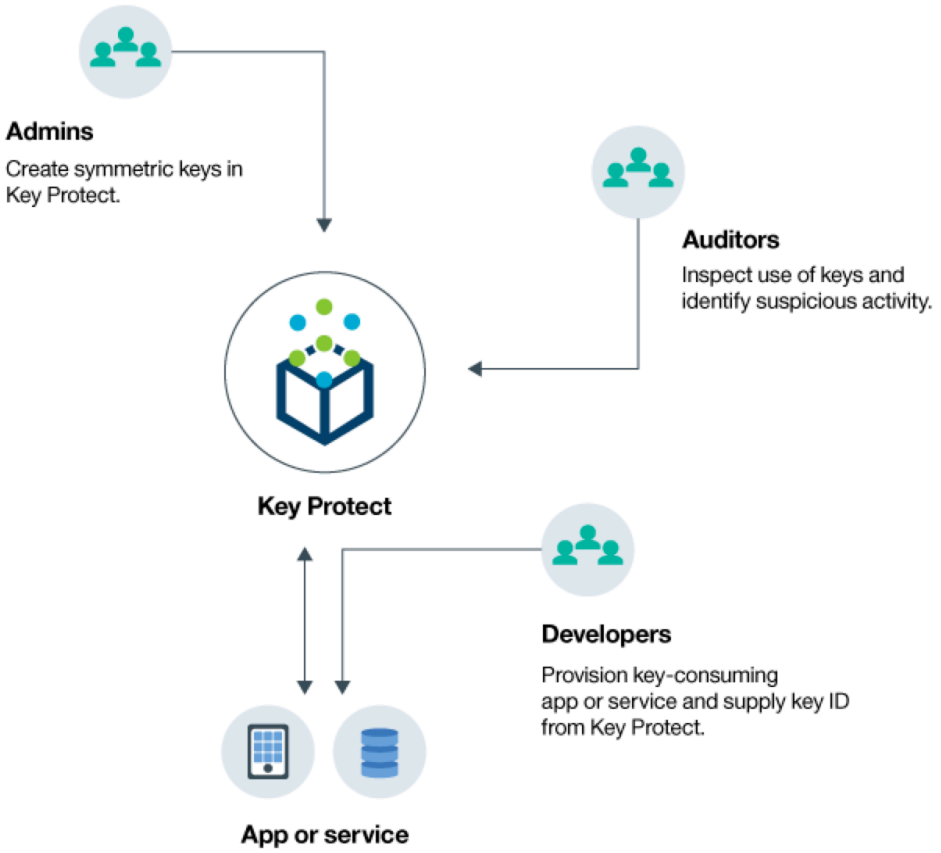
Key management
e.g., Customer uses IBM KeyProtect to create their encryption keys

- Customer managed encryption keys
- Key management service
- Hardware security modules



Key Protect

Scenario	Reason
You need to encrypt high volumes of sensitive data, such as medical records, by individual resource.	You can integrate the Key Protect service with storage solutions, such as Object Storage, to encrypt your data at rest in the cloud. Each document can be protected by a different key, so you have granular control of your data.
As an IT admin for a large corporation, you need to integrate, track, and rotate keys for many different service offerings.	The Key Protect interface simplifies the management of multiple encryption services. With the service, you can manage and sort keys in one centralized location, or you can separate keys by project and house them in different Bluemix® spaces.
You are a security admin in an industry, such as finance or legal, that must adhere to governance over how data is protected. You need to grant controlled access of keys without compromising the data that it secures.	With the service, you can control user access to manage keys by assigning different Bluemix roles. For example, you can grant read-only access to users who need to view key creation information without viewing the key material.
As a developer, you can integrate pre-existing applications, such as self-encrypting storage, to Key Protect. You can also develop your own apps that integrate with the service.	Apps on or outside Bluemix can integrate with the Key Protect APIs. You can use your own existing keys for your apps.
Your development team has stringent policies, and you need a way to generate and rotate keys every 14 days.	With Key Protect, you can rapidly generate keys from a hardware security module (HSM) to meet your on-going security needs.

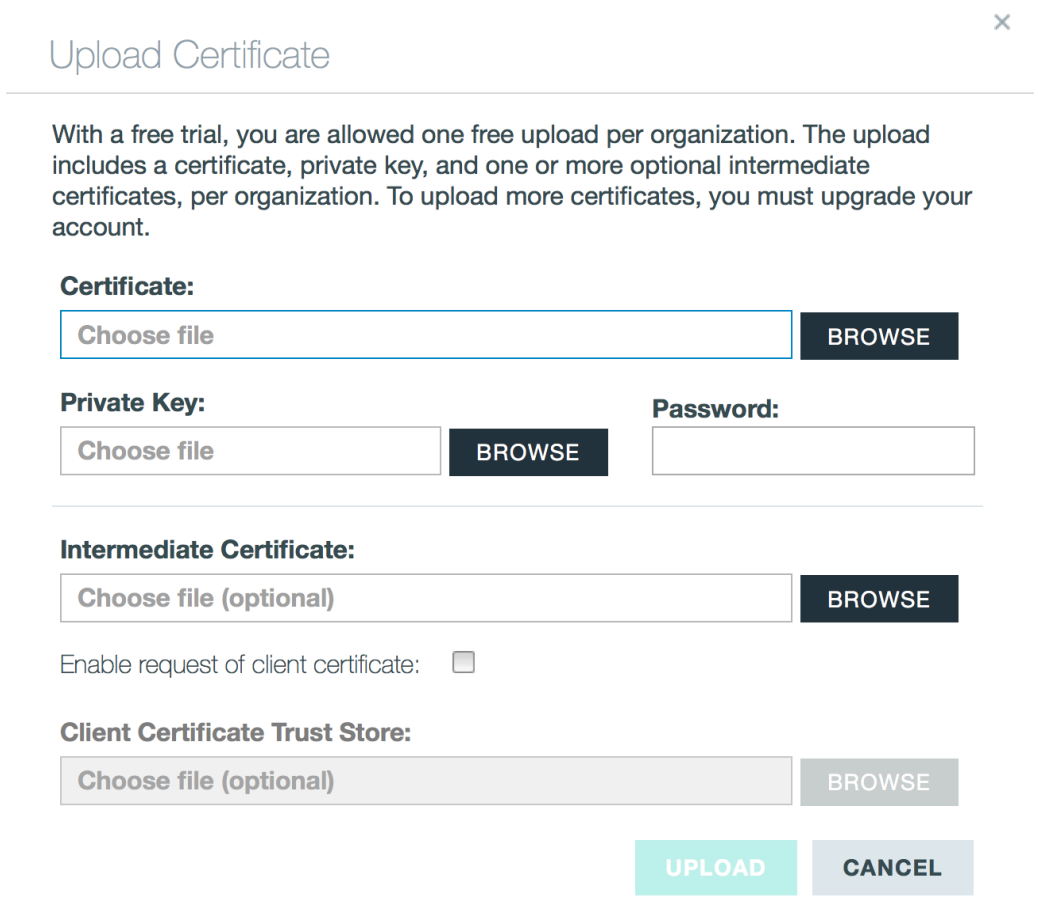


Using Key Protect for Application Level Encryption

- Hands-on Exercise

Certificate Management

- For every organization in Bluemix with an account owner who has a Pay as you Go or Subscription plan in place, you are allowed four free certificate uploads.
- For every organization with an account owner who has a free trial account, you are allowed one free certificate upload.
- When you use a custom domain, to serve the SSL certificate, use the following region endpoints to provide the URL route that is allocated to your organization in Bluemix:
  - US-South: secure.us-south.bluemix.net
  - EU-GB: secure.eu-gb.bluemix.net
  - AU-SYD: secure.au-syd.bluemix.net
- The following types of certificates are supported in Bluemix:
  - PEM (pem, .crt, .cer, and .cert)
  - DER (.der or .cer)
  - PKCS #7 (p7b, p7r, spc)



4. Secure Dev-Ops

- Infrastructure Vulnerability Management
- Application Vulnerability Management

4 Secure devOps drives secure engineering and deployment practices

Containers enables new model
e.g., Customer uses Vulnerability Advisor to assess container images

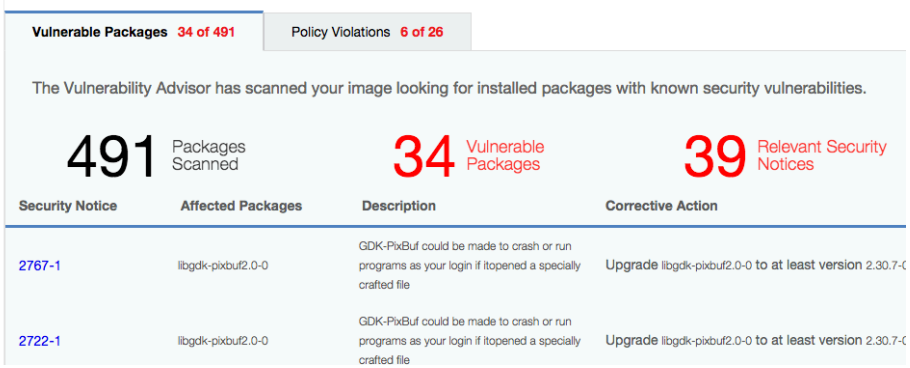
- Vulnerability analysis
- Enterprise security policies
- Remediation in devOps

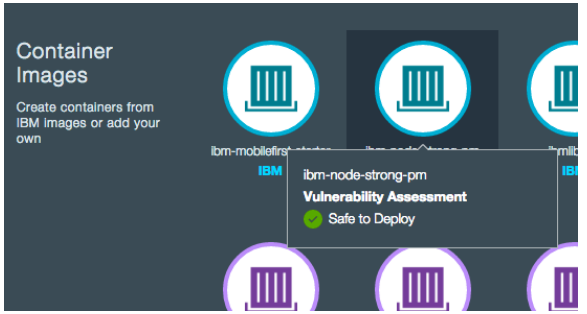
VMs are still traditional
e.g., Customer uses BigFix to patch all VMs and fix Linux security vulnerability

- Configuration and patch management
- VMs based models for lift & shift apps
- Compliance reporting

Application security
e.g., Customer uses Application Security service to scan web apps and mobile

- Application security scanning
- Mobile and web apps
- Secure engineering and proactive

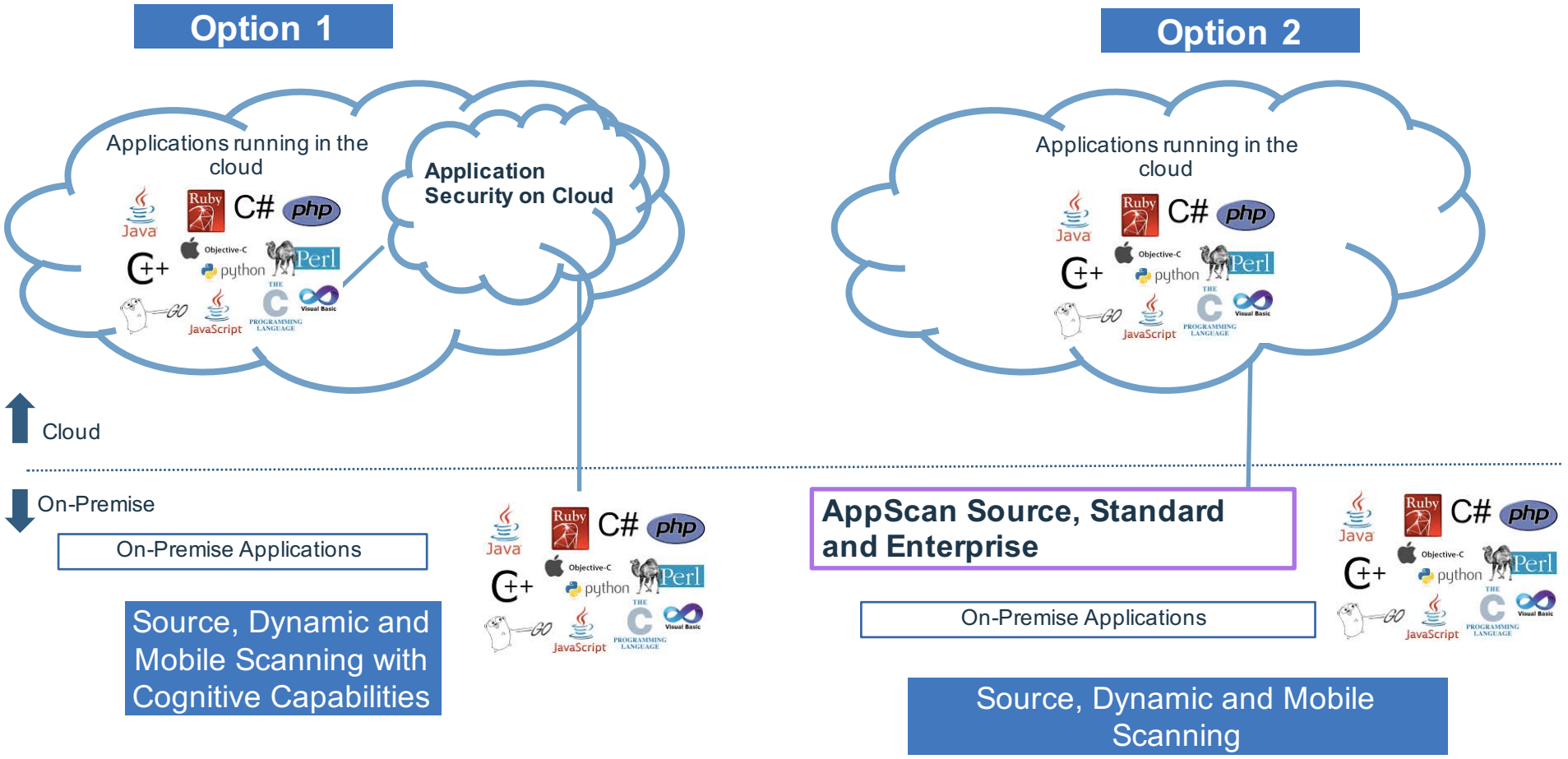




Understanding Vulnerability Explorer

- Hands-on Exercise

AppScan and ASoC Options for Cloud



Easy Integration with Guardium, PIM, and QRadar

Securing Cloud with IBM Application Security

ASoC/AppScan	Protects IaaS	Protects PaaS	Protects SaaS	Protects On-Premise
Source Scanning	✓	✓		✓
Dynamic Scanning	✓	✓	✓	✓
Mobile Applications	✓	✓	✓	✓

ASoC includes Cognitive Capabilities for better results and less analysis by developers.

Perform Dynamic scan of the Web-App

- Hands-on Exercise

5. Security Monitoring & Intelligence

5 Security monitoring and intelligence are required to gain confidence

Access trails and audit logs
e.g., All administrative access is logged in Bluemix

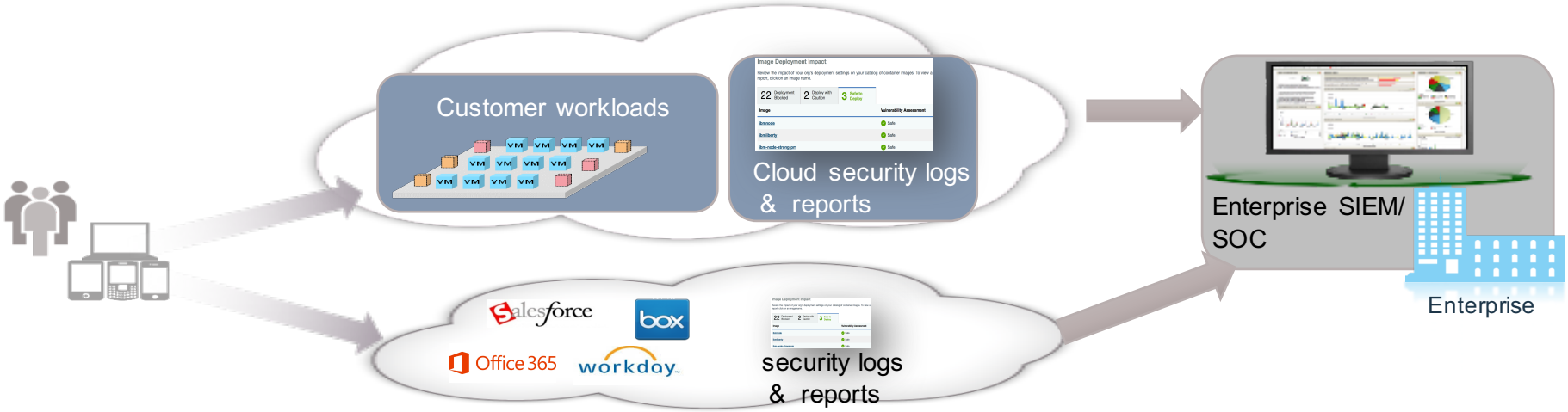
- Log all access to platform and services
- API, web and mobile access
- Application logs integration

Identify Cloud incidents
e.g., Customer uses analytics tools to correlate Cloud traffic to identify malicious app

- Security and vulnerability posture
- All platform logs and events
- Continuous monitoring for attacks and threats

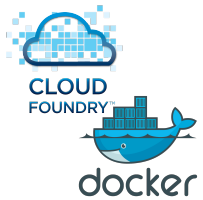
Enterprise security intelligence
e.g., CISO wants all logs and events integrated into their on-prem SIEM

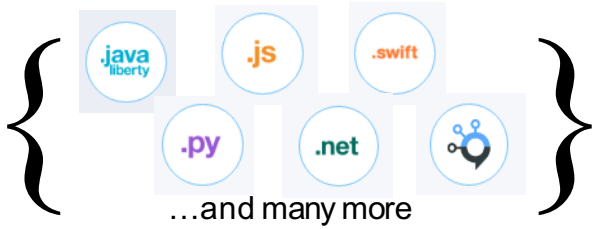
- Integrated view across hybrid deployments
- Cloud and on-prem security monitoring
- Incident management and reporting

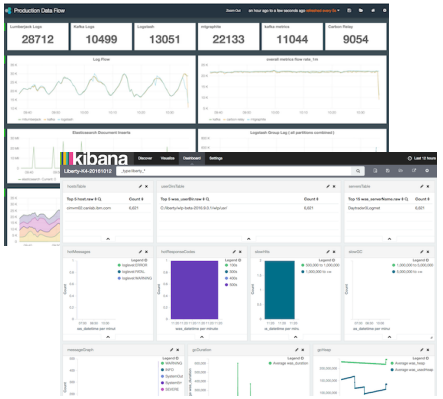


Zero Effort Logs and Metrics in IBM Cloud

Automated log & metric collection from your interconnected cloud-hosted microservices







Review the trail of your cloud activities

Analyze and interact with your data with open technology viewers

Bluemix platform offerings. Enabled by default.

IBM Access Trail

Beta

Capture and store Bluemix cloud service activities

- Visibility into applications and user interactions within Bluemix
- Captured from API and Bluemix Console activities
- Interact with your data through API or Kibana

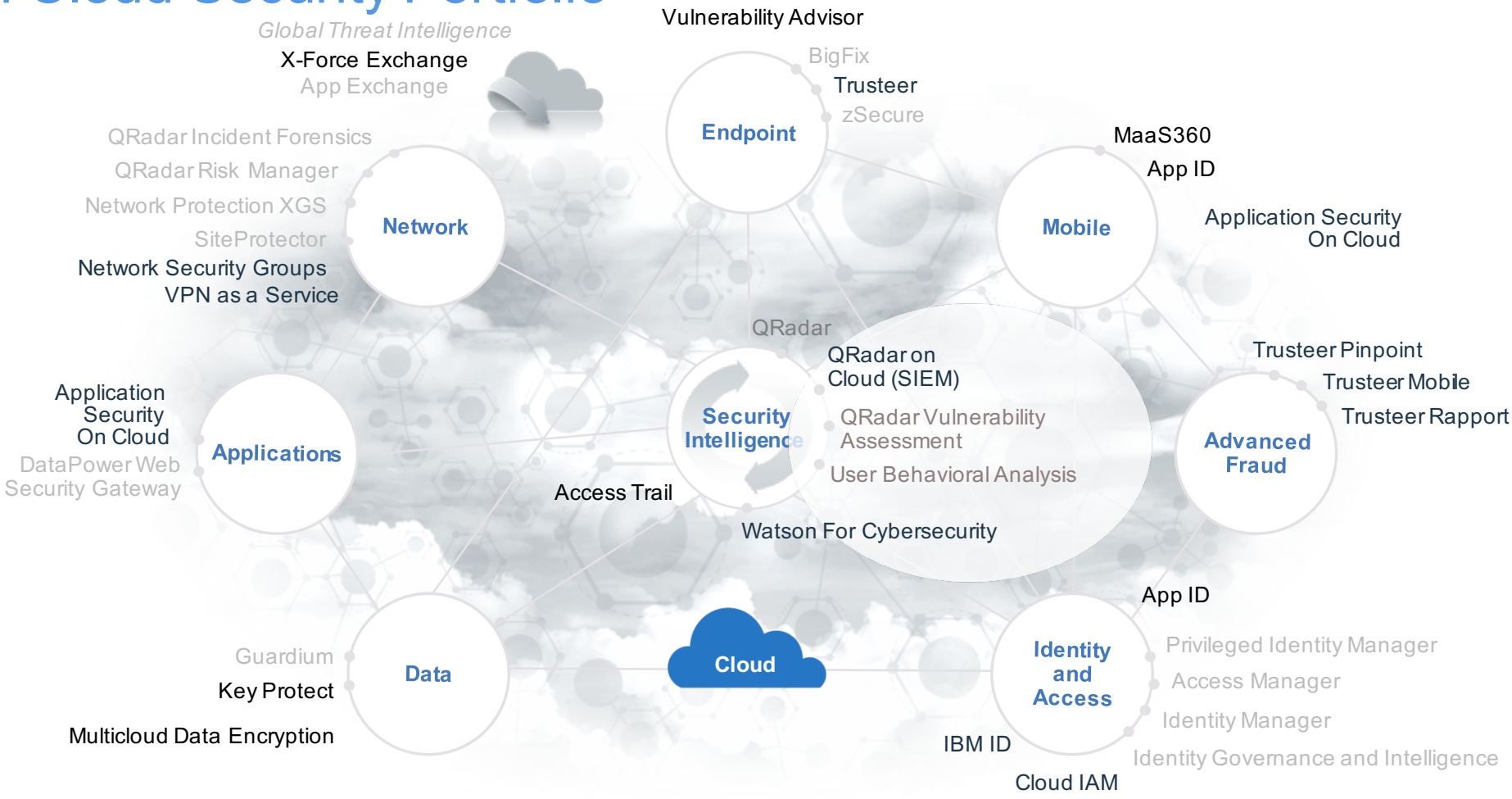
Debug, Optimization and Audit Use cases

- Debug with knowledge of additional platform transparency
- Planning and optimization to identify poorly used resources or identify growing needs
- Audit and security for user behavior and security incident investigations

Bluemix platform offering. Enabled by default.

IBM Cloud Security Portfolio

Enhance security through intelligence and integration – IBM Cloud Security Portfolio

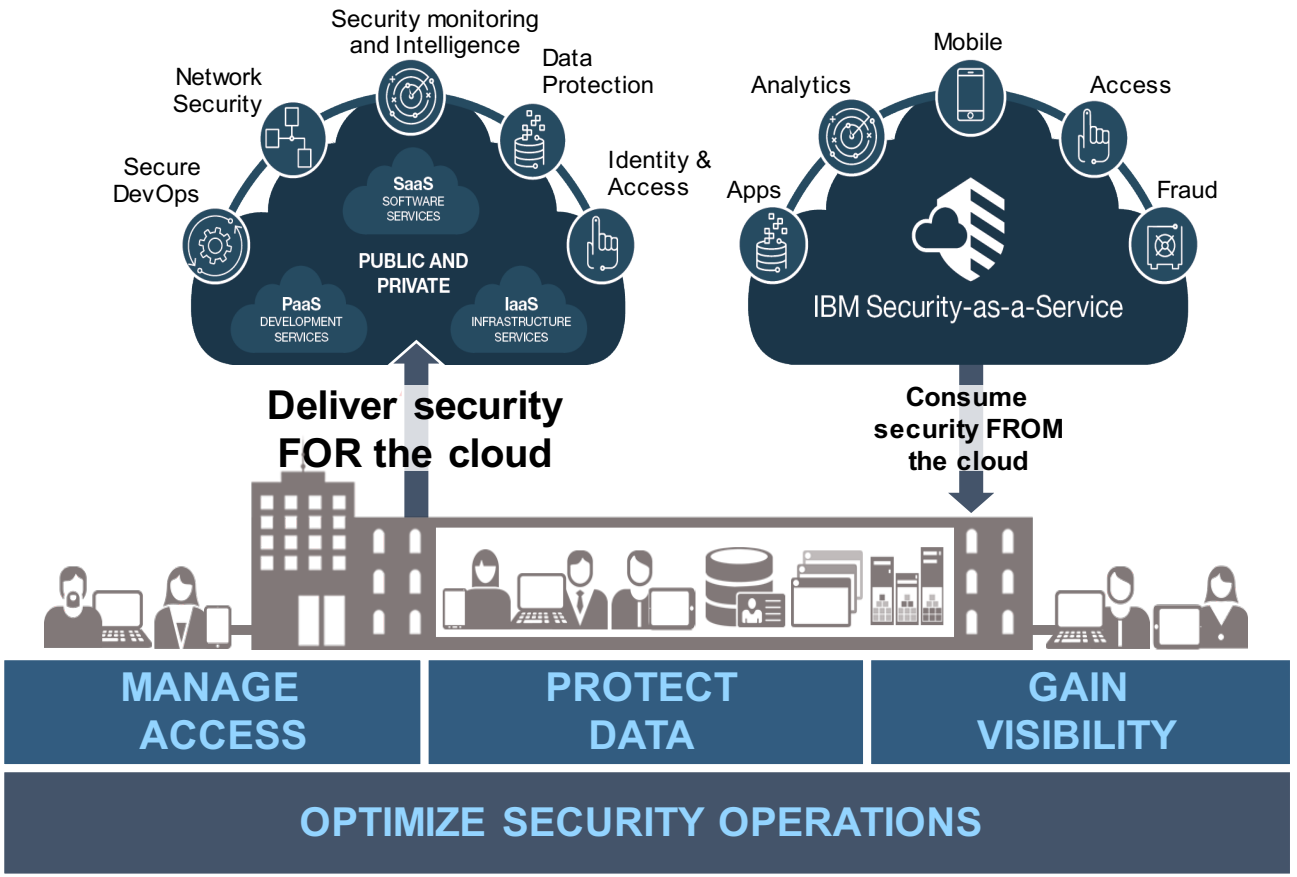


Cloud Security Portfolio

1. Cloud is an opportunity to radically transform security practices

2. Enterprises must take a structured approach to securely adopt hybrid Clouds

3. IBM Cloud Security portfolio provides prescriptive solutions to adopt hybrid cloud with confidence



Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular, purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

InterConnect
2017