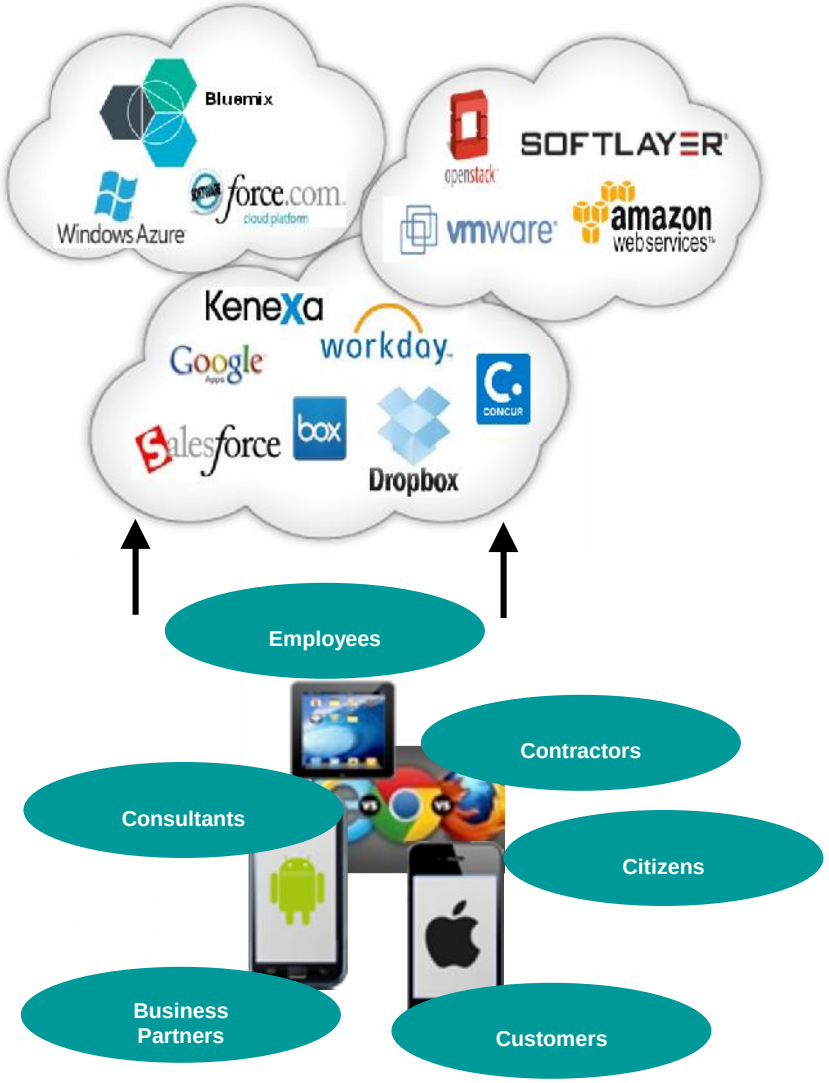
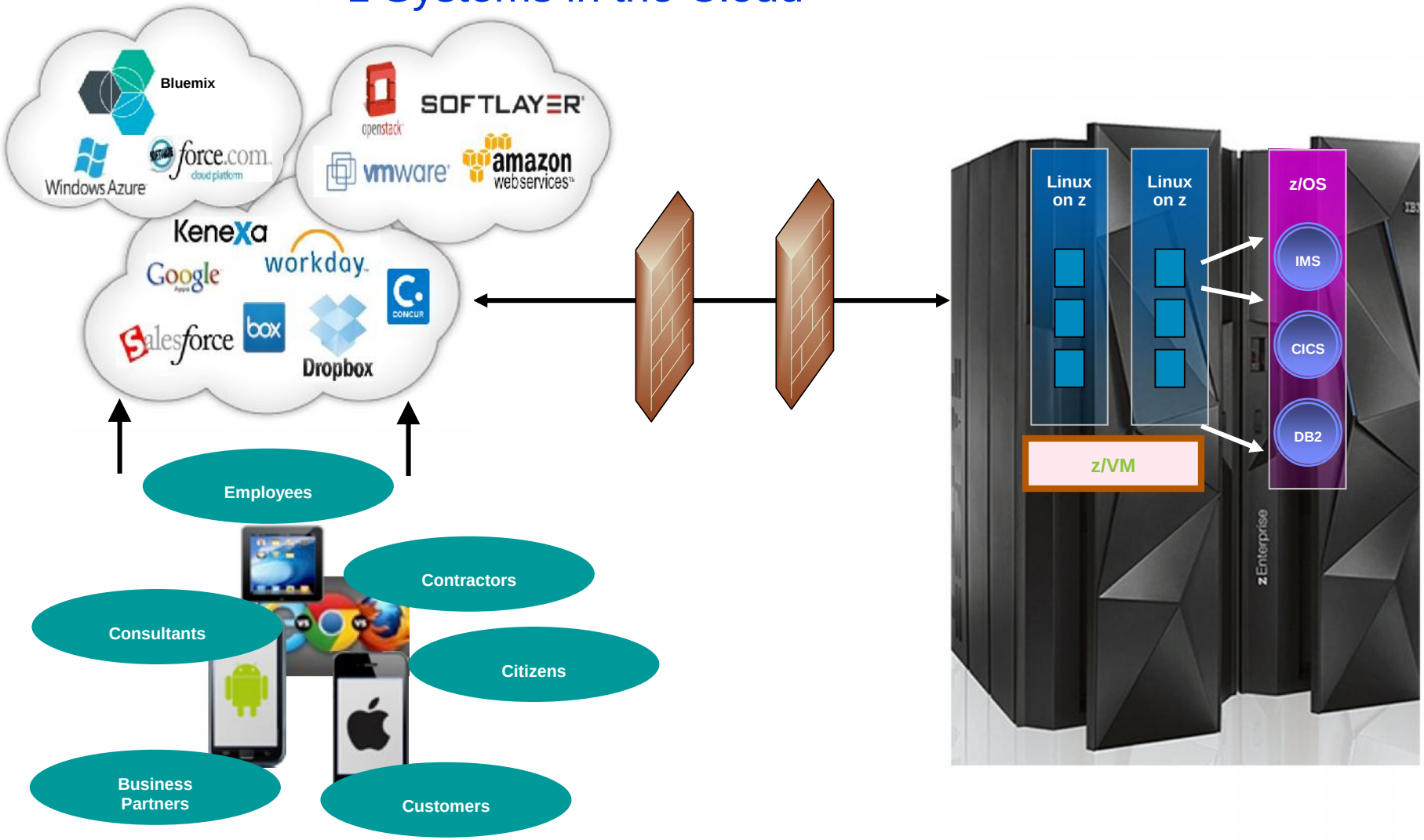
IBM z Systems – Security in the Cloud

“Traditional” Cloud Environment



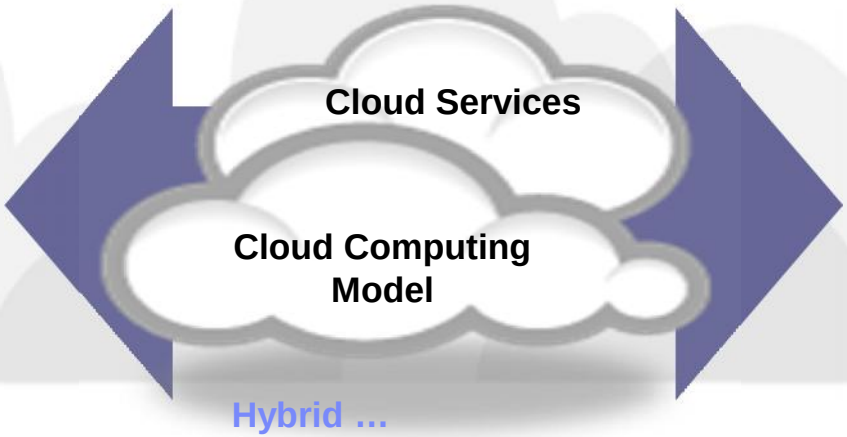
z Systems in the Cloud



Cloud Computing Delivery Models

Flexible Delivery Models

Public …
- Service provider owned and managed
- Access by subscription
- Delivers select set of standardized business process, application and/or infrastructure services on a flexible price per use basis



Hybrid …

Access to client, partner network, and third party

Private …
- Privately owned and managed.
- Access limited to client and its partner network.
- Drives efficiency, standardization and best practices while retaining greater customization and control

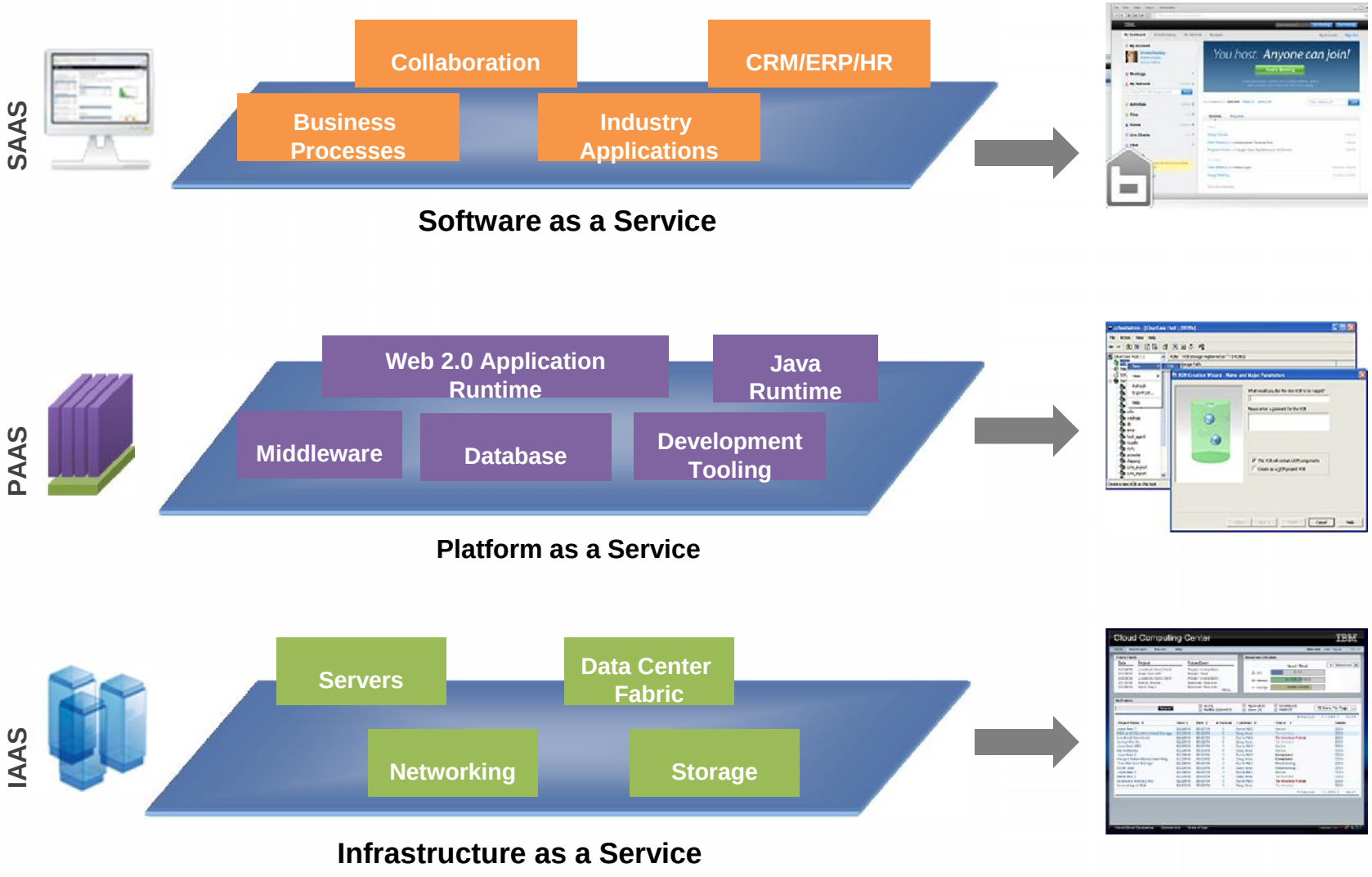
….Standardization, capital preservation, flexibility and time to deploy

…. Customization, efficiency, availability, resiliency, security and privacy

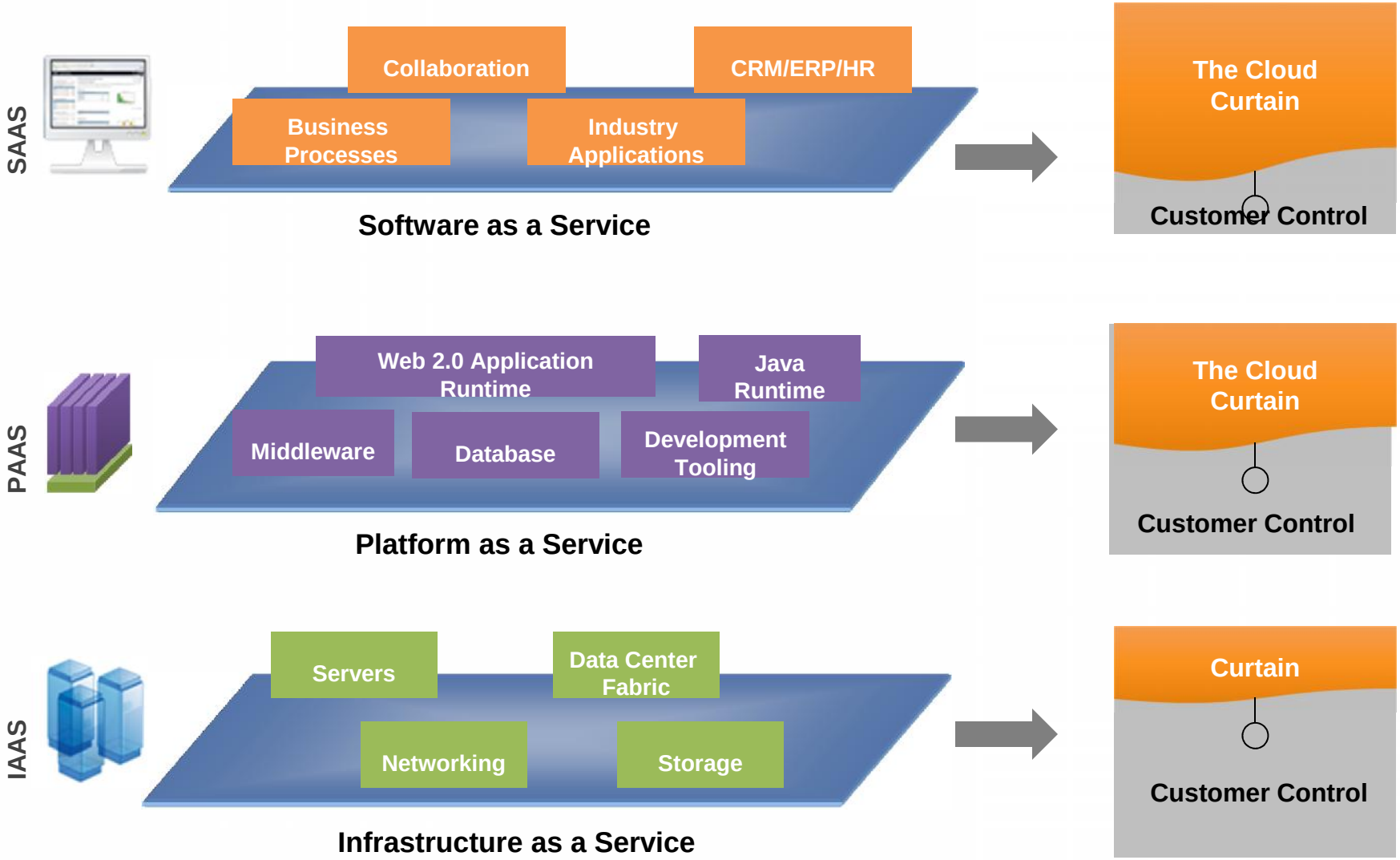
ORGANIZATION → CULTURE → GOVERNANCE

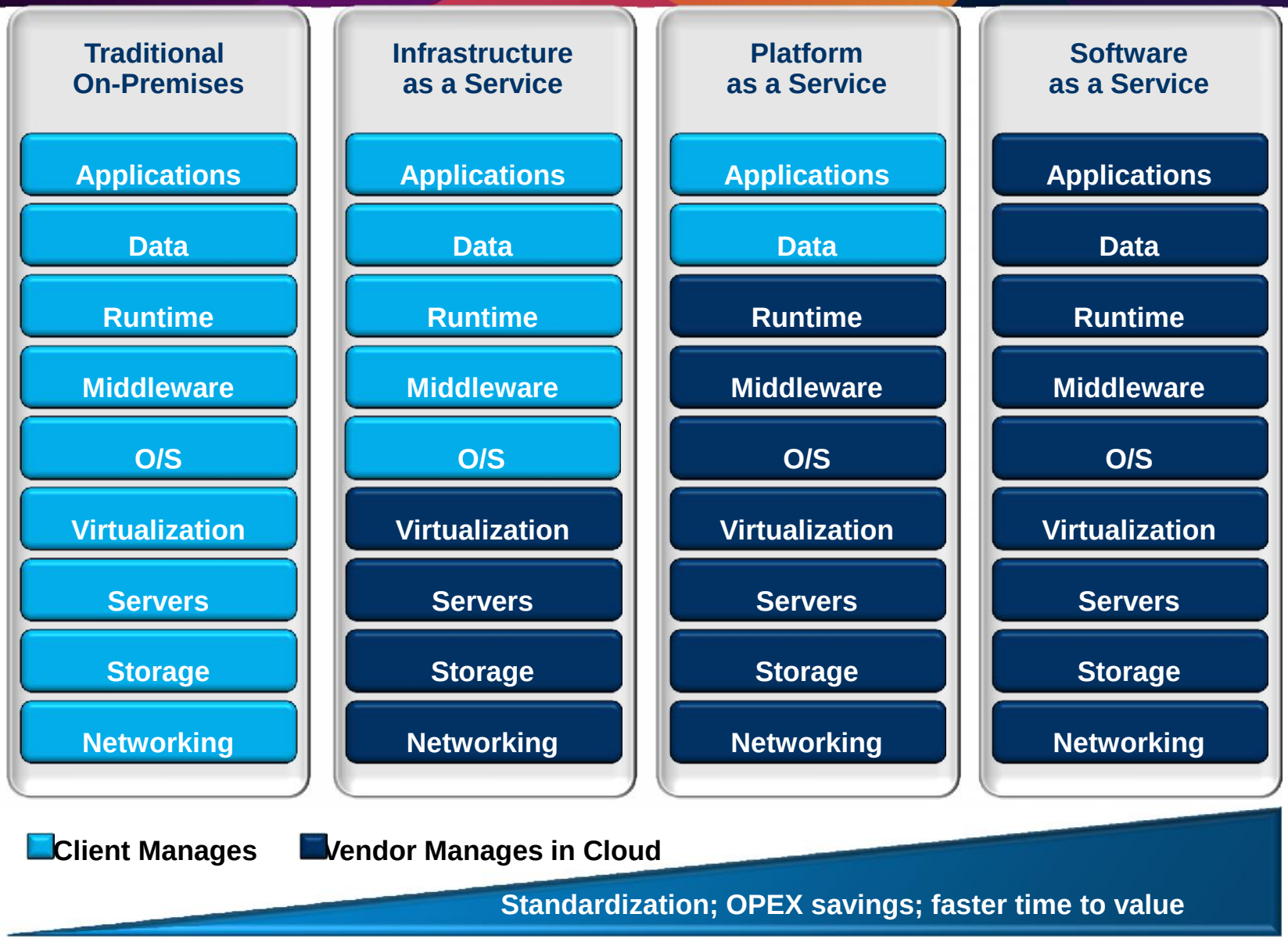
...service sourcing and service value

The Layers of IT-as-a-Service

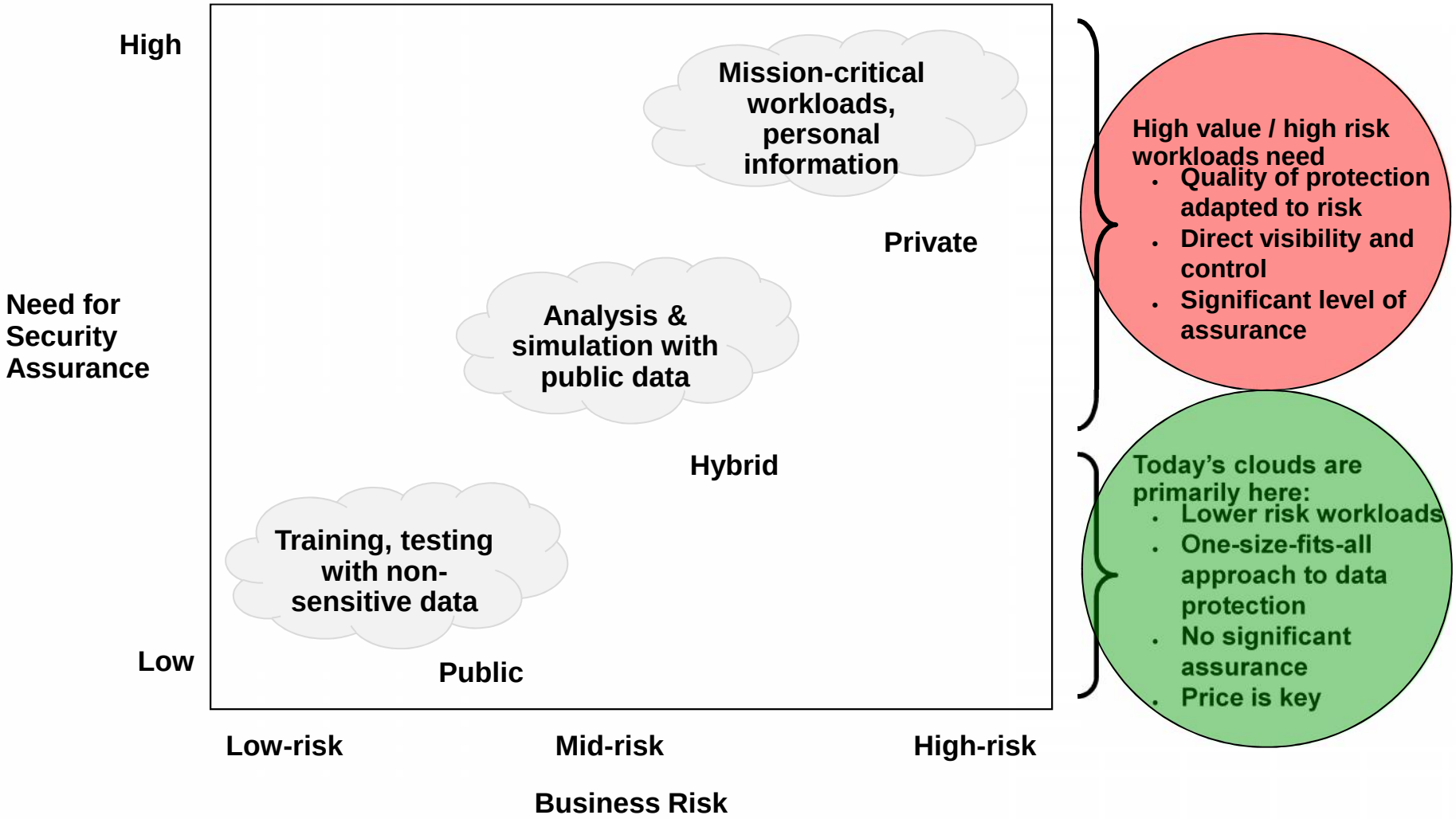


Different Clouds, Different Responsibilities




Traditional On-Premises
Infrastructure as a Service
Platform as a Service
Software as a Service
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
Client Manages
Vendor Manages in Cloud
Standardization; OPEX savings; faster time to value

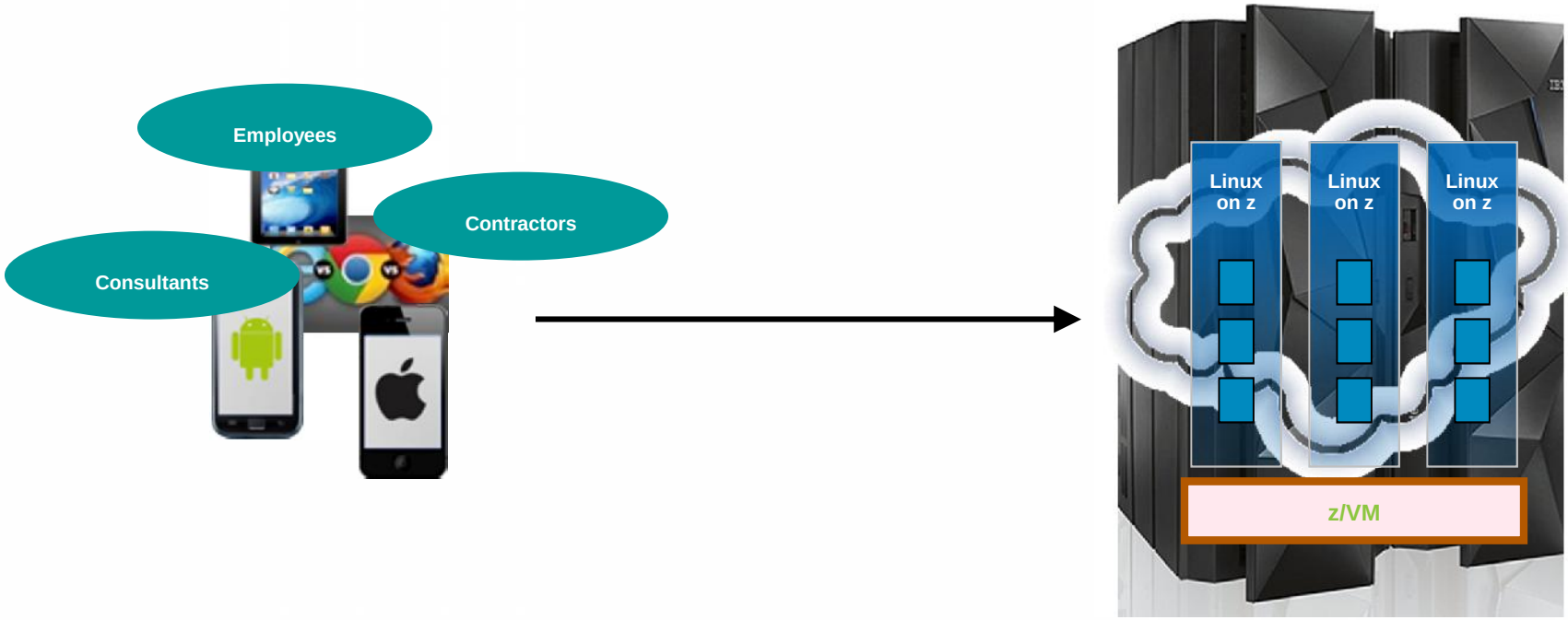
Security as a Potential Market Differentiator:
Different Workloads have Different Risk Profiles



8

z Systems Cloud Scenario #1: Private Cloud with Linux on z

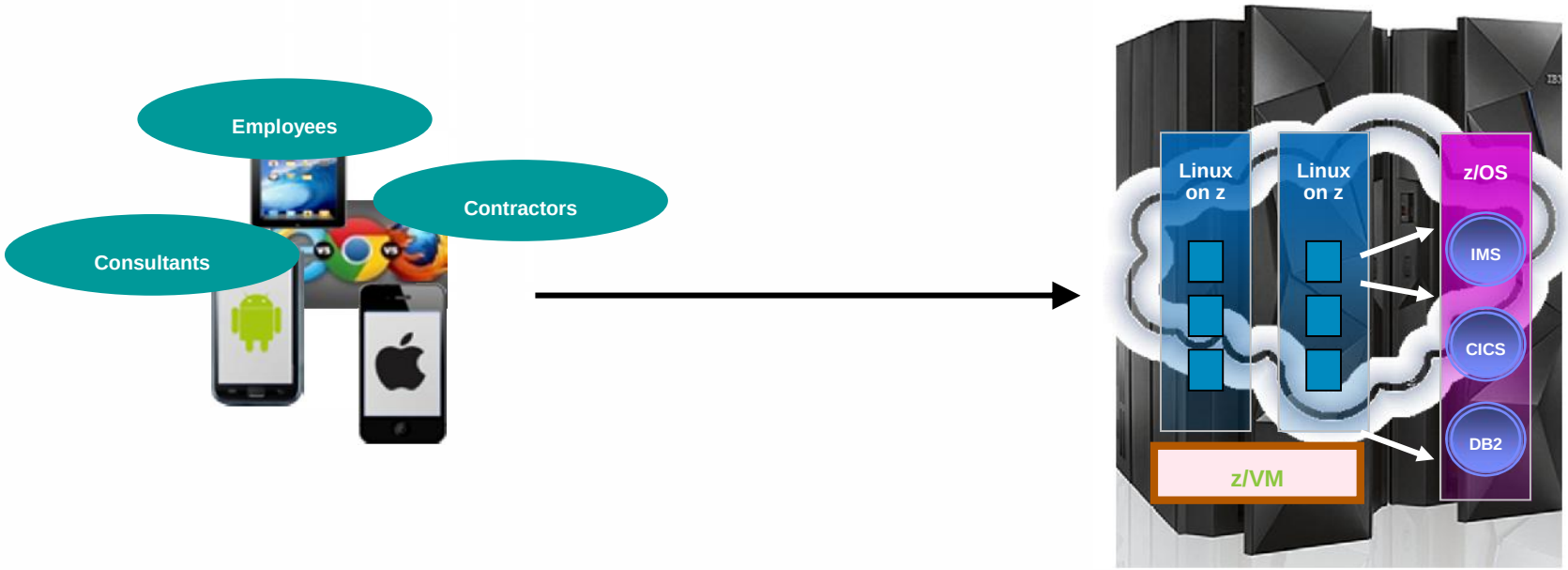
Multiple workloads from distributed platforms consolidated into a single, scalable footprint utilizing Linux on z



- Web servers, portals, applications and data reside on the VM's on System z utilizing zLinux
- Theoretically, this would be equivalent to a VMWare ESX server type of deployment
- Likely, it would only involve applications and data accessible by an organization's employees, contractors and consultants.

z Systems Cloud Scenario #2: Private Cloud with Linux & z/OS

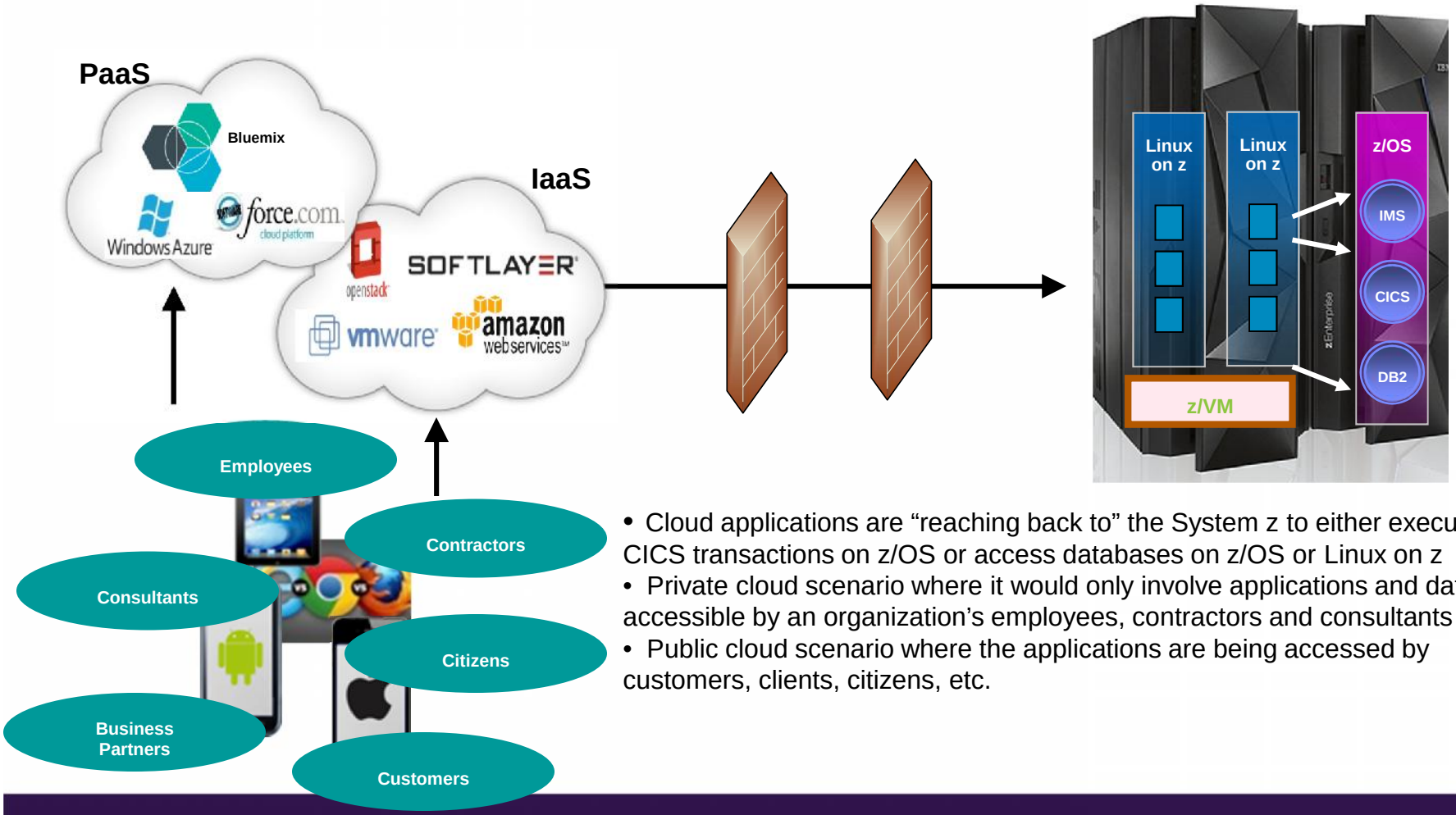
Multiple workloads from distributed platforms consolidated into a single, scalable footprint utilizing Linux on z and leveraging critical System z transactions and data



- Web servers, portals, applications and data would reside on one, or more, VM's utilizing zLinux **<u>and</u>** on z/OS. Examples:
  - CICS transactions running under z/OS accessing databases running on zLinux
  - Java applications running on zLinux accessing databases running on z/OS
  - Java applications running on zLinux "kicking off" CICS transactions on z/OS
- As in the first scenario, it likely would only involve applications and data accessible by an organization's employees, contractors and consultants.

z Systems Cloud Scenario #3: Hybrid Cloud (IaaS and PaaS)

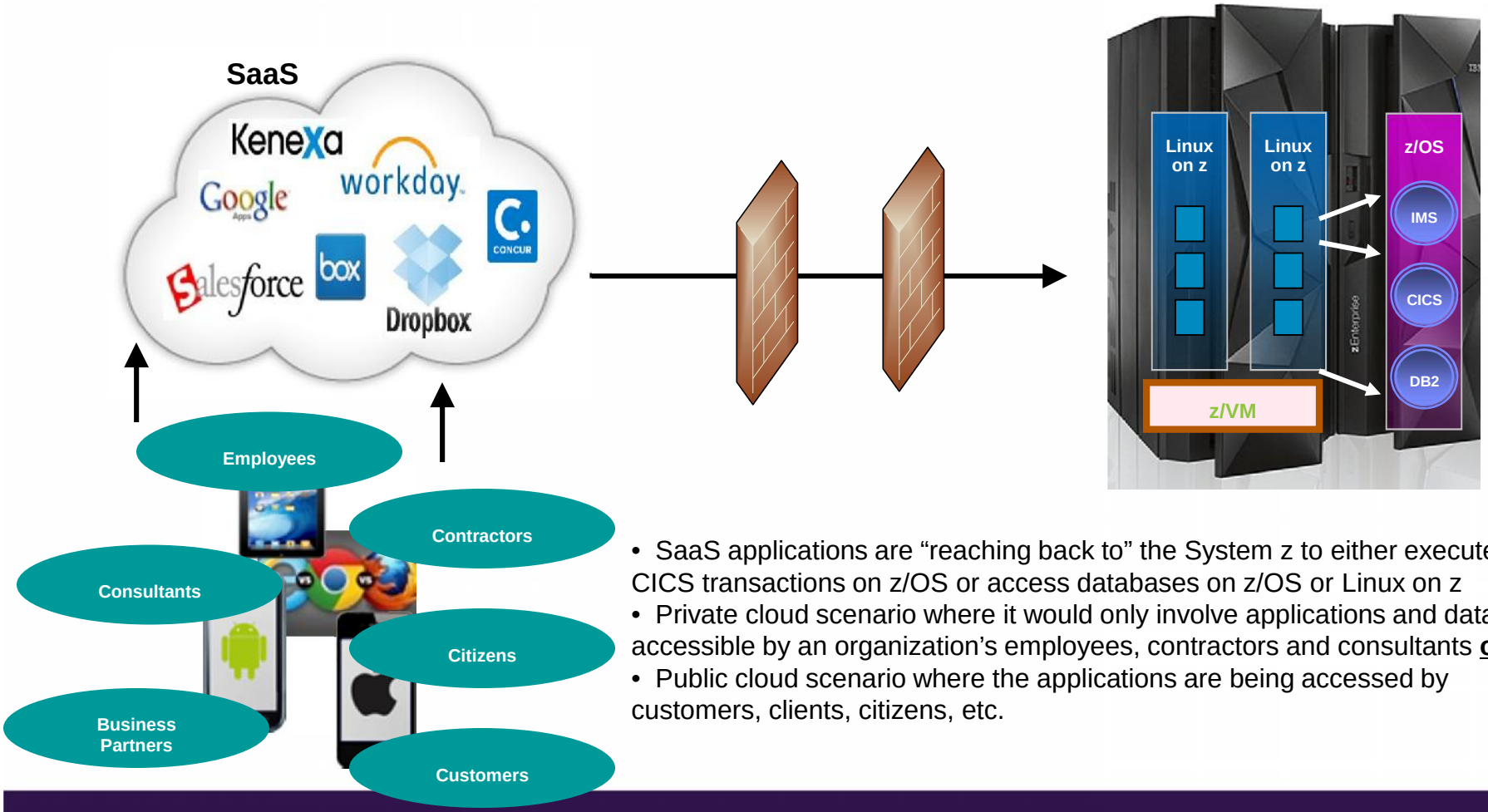
Enterprise applications moved to public cloud environments, including IaaS and PaaS, and integrating with Systems of Record deployed on System z within the enterprise



- Cloud applications are "reaching back to" the System z to either execute CICS transactions on z/OS or access databases on z/OS or Linux on z
- Private cloud scenario where it would only involve applications and data accessible by an organization's employees, contractors and consultants **<u>or</u>**
- Public cloud scenario where the applications are being accessed by customers, clients, citizens, etc.

z Systems Cloud Scenario #4: Hybrid Cloud (SaaS)

Enterprises consuming SaaS applications delivered from the Cloud, which integrate with Systems of Record deployed on System z within the enterprise



- SaaS applications are "reaching back to" the System z to either execute CICS transactions on z/OS or access databases on z/OS or Linux on z
- Private cloud scenario where it would only involve applications and data accessible by an organization's employees, contractors and consultants **or**
- Public cloud scenario where the applications are being accessed by customers, clients, citizens, etc.

Typical Client Security Requirements

Governance, Risk Management, Compliance

- 3rd-party audit (SAS 70(2), ISO27001, PCI)
- Client access to tenant-specific log and audit data
- Effective incident reporting for tenants
- Visibility into change, incident, image management, etc.
- SLAs, option to transfer risk from tenant to provider
- Support for forensics
- Support for e-Discovery

Application and Process

- Application security requirements for cloud are phrased in terms of image security
- Compliance with secure development best practices

Physical

- Monitoring and control of physical access

People and Identity

- Privileged user monitoring, including logging activities, physical monitoring and background checking
- Federated identity / onboarding: Coordinating authentication and authorization with enterprise or third party systems
- Standards-based SSO

Data and Information

- Data segregation
- Client control over geographic location of data
- Government: Cloud-wide data classification

Network, Server, Endpoint

- Isolation between tenant domains
- Trusted virtual domains: policy-based security zones
- Built-in intrusion detection and prevention
- Vulnerability Management
- Protect machine images from corruption and abuse
- Government: MILS-type separation

Based on interviews with clients and various analyst reports

IBM z Systems are a highly securable environment

Security is embedded into the z Systems architecture

- Processor
- Hypervisor
- Operating system
- Communications
- Storage
- Applications

Z Systems security addresses regulatory compliance for:

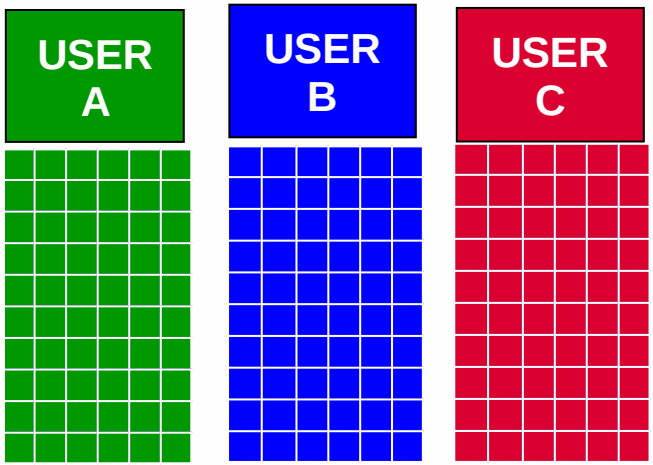
- Identity and access management
- Hardware and software encryption
- Communication security capabilities
- Extensive security event logging and reporting capabilities
- Extensive security certifications including EAL5+ *(e.g., Common Criteria and FIPS 140)*

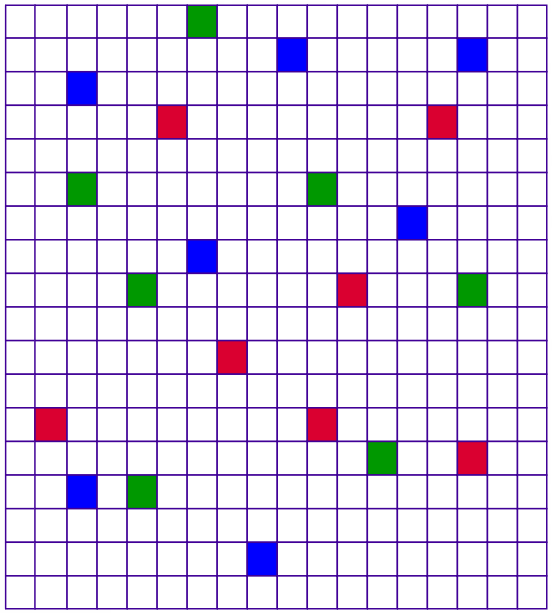
But today's mainframe must interoperate in a complex environment including cloud, mobile, big data and social networking and is susceptible to multiple vulnerabilities.

- Highly secure platform for virtual environments and workloads
- **80%** of all active code runs on the Mainframe1
- **80%** of enterprise business data is housed on the Mainframe
- ***This makes the Mainframe a desirable target for hackers***

Integrity of Virtual Machines

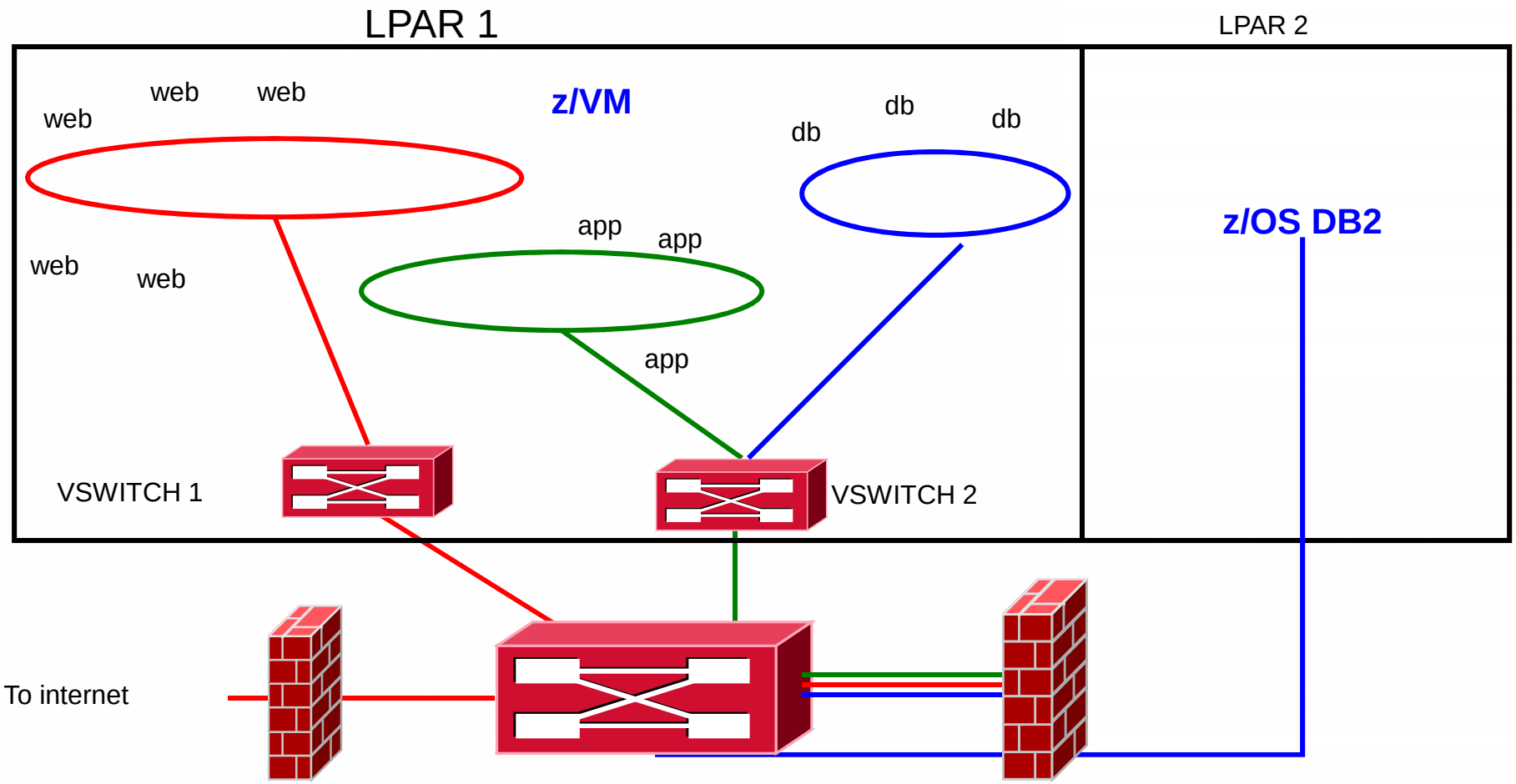
- The z/VM System Integrity Statement: http://www.vm.ibm.com/security/zvminteg.html
- The z/VM Control Program enforces the separation of virtual machines, and manages the ability to touch memory.





CP Real Memory

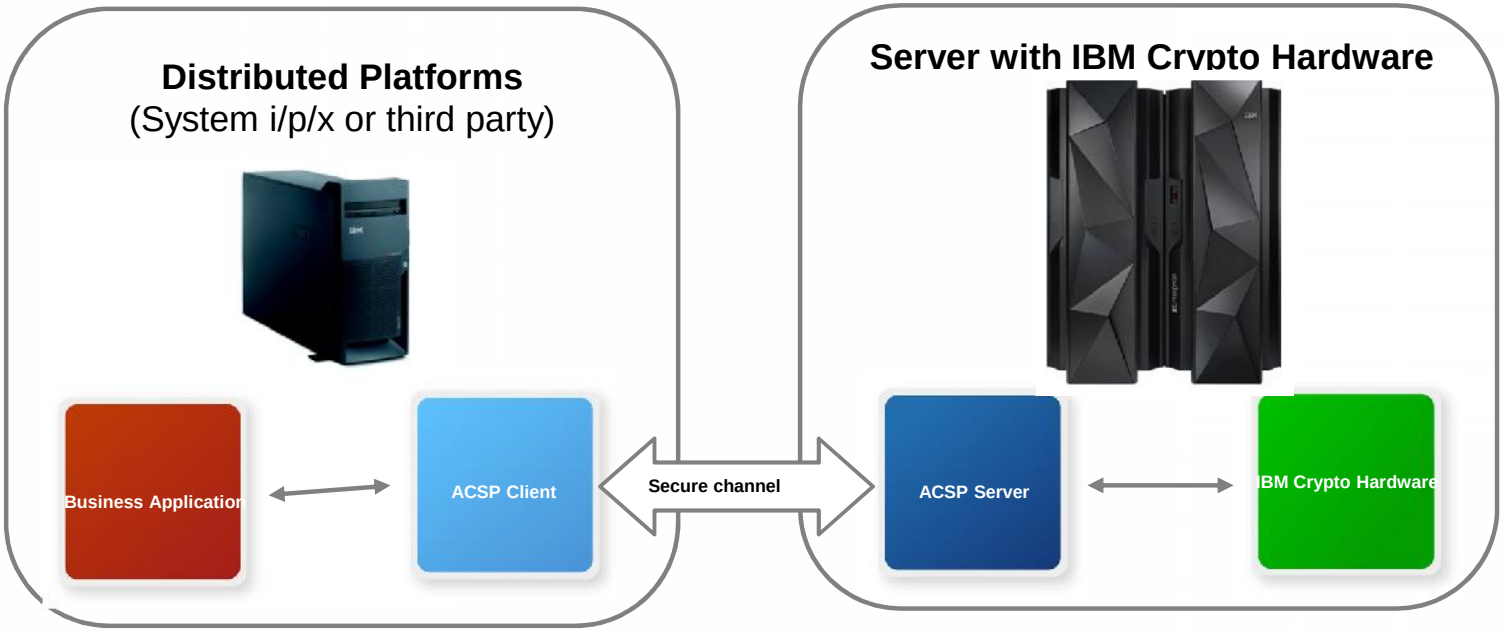
VSWITCH and VLANs



With 1 VSWITCH, 3 VLANs, and a multi-domain firewall

EKMP-ACSP Components – Crypto as a Service

- The IBM EKMP- ACSP is a client/server solution that enables distributed platforms to use cryptographic hardware on a System z resulting in a cost effective use of available cryptographic capacity; and centralized key storage on System z helping simplify key management



- ACSP client platforms
  - AIX, i5, Linux, Windows
  - PureSystems
  - (in reality any Java platform)
- ACSP client APIs
  - CCA in Java and C
  - PKCS#11, JCE

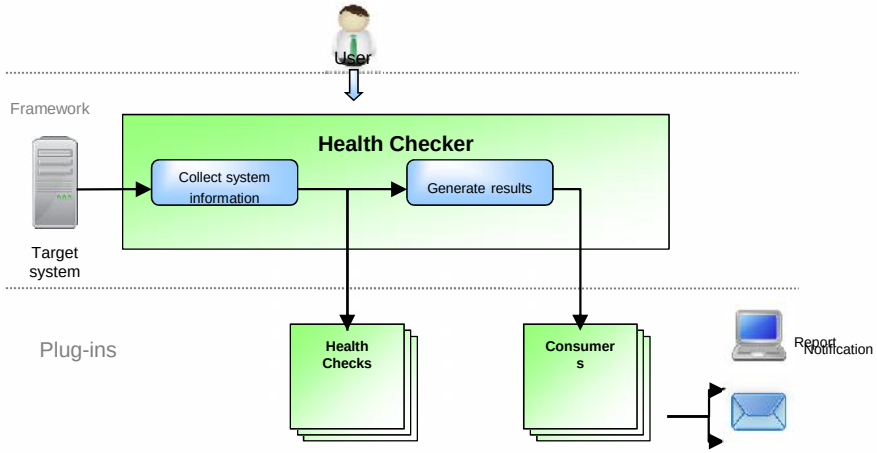
- Transport network
  - IP
  - SSL/TLS protected (client/server auth,)

- ACSP server platform
  - System z: z/OS (CEX3/4)
  - System p: AIX (4765)
  - System x: SLES, RHEL (4765)
  - PureSystems

Crypto Health Checks

Linux Health Checker (LNXHC)

- http://lnxhc.sourceforge.net/
- a framework & tool to check whether the set up of a system is correct or follows best practices
- the set of checks is extensible
- adaptable profiles to match set of *applicable* checks to customer environment
- provides
  - indications of problems found
  - Explanation of the problems
- hints to resolve problems




```
linux:~ # lnxhc run
Collecting system information
Running checks (50 checks)
CHECK NAME                                HOST                  RESULT
==========================================================================
boot_runlevel_recommended ............... linux                 SUCCESS
cpu_capacity ............................ linux                 SUCCESS
css_ccw_blacklist ....................... linux                 SUCCESS
css_ccw_chpid_status .................... linux                 EXCEPTION-LOW

 >EXCEPTION css_ccw_chpid_status.unused_cfg_off(low)
    One or more CHPIDs are in the "standby" configuration state (34-37,
    3f-43, 47, 4e, ...)

css_ccw_device_availability ............ linux                 SUCCESS
css_ccw_device_usage .................... linux                 EXCEPTION-LOW

 >EXCEPTION css_ccw_device_usage.many_unused_devices(low)
    Of 7816 I/O devices, 7806 (99.87%) are unused

css_ccw_driver_association ............. linux                 EXCEPTION-MED

 >EXCEPTION css_ccw_driver_association.no_driver(medium)
    One or more I/O devices are not associated with a device driver:
    0.0.b47f, 0.0.f5fe, 0.0.f7fe
```

Crypto health checks to validate crypto configuration:

- crypto_cca_stack
- crypto_cpacf
- crypto_opencryptoki_ckc
- crypto_opencryptoki_ckc_32bit
- crypto_opencryptoki_skc
- crypto_opencryptoki_skc_32bit
- crypto_openssl_ibmca_config
- crypto_openssl_stack
- crypto_openssl_stack_32bit
- crypto_z_module_loaded

Mainframe Security Management

Mainframe Security Intelligence
System z identity and access context, real-time event correlation

Mainframe Governance, Risk and Compliance
Regulations, IT Security Policies and Third Party Integrations

Mainframe Administration

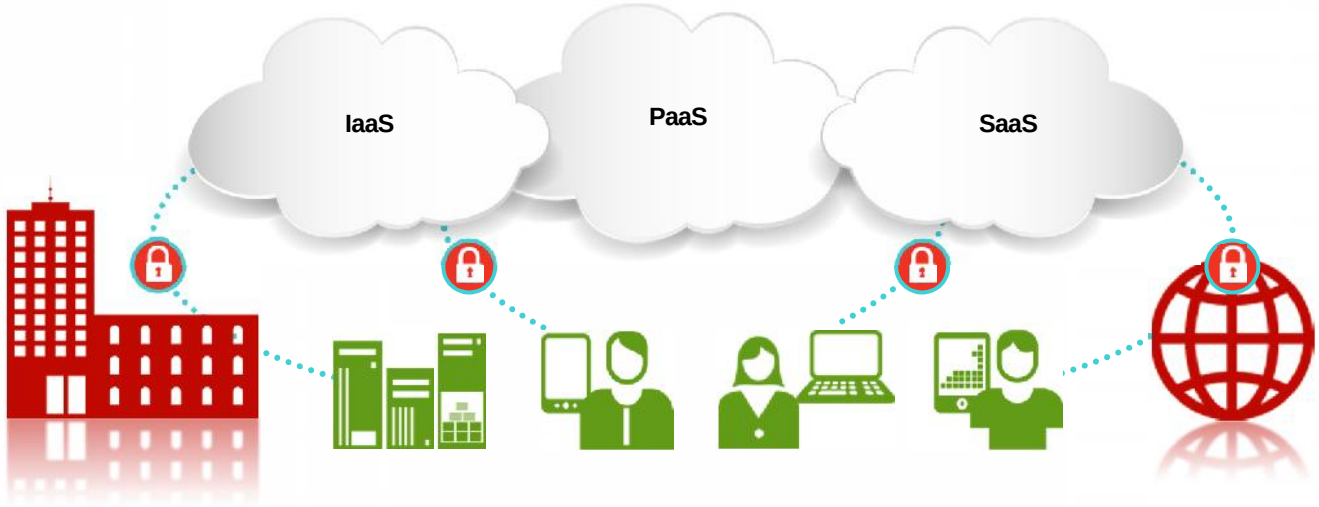
- Effective user and access control administration for z/OS
- Simplifies user and resource management
- Offers a Windows GUI to administer security

Mainframe Compliance and Auditing

- Provides automated monitoring, analysis and auditing
- Enforces compliance best practices and security policy
- Provides intrusion detection and generates real time alerts

Mainframe | Data | Applications | RACF | Cloud Computing

Securing the Cloud Environment



So, let's talk about the security requirements for such a powerful and dynamic environment.

You will need to be able to:

- Secure the hypervisor, i.e. z/VM
- Provide administrator access to the VM's
- Be able to Provision users to the applications and data
- Manage and Control access to the applications and data
- Monitor, Alert, Audit and Report on accesses to and attempted access to the applications and data
- Detect and Prevent against vulnerabilities, threats, malware and fraud
- Safeguard the data and protect from data loss

Does this sound familiar?

Enterprise hybrid cloud adoption requires integrated security solutions

	Identity	Protection	Insight
Software as a service (SaaS)	Enable users 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 services and platform • Service vulnerabilities • Compliance reporting
Infrastructure as a Service (IaaS)	Manage cloud administration and workload access • Privileged user management • Access management of web workloads • Identity federation for B2B	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

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

Components of IBM's end-to-end security solution for the hybrid cloud

Manage Access	Protect Data	Gain Visibility
Securely connect people, applications, and devices to the cloud	Identify vulnerabilities and prevent attacks targeting sensitive data	Monitor the cloud for security breaches and compliance violations
▪ IBM Security Identity and Access Management Suite ▪ IBM Security Federated Identity Manager - Business Gateway ▪ IBM Security Privileged Identity Manager ▪ IBM Security zSecure portfolio	▪ IBM InfoSphere Guardium ▪ IBM Enterprise Key Management Foundation ▪ IBM Security Key Life Cycle Manager ▪ IBM Security AppScan	▪ IBM Security QRadar SIEM ▪ IBM Security zSecure Manager for RACF z/VM ▪ IBM Security zSecure Compliance and Auditing ▪ IBM Security Network IPS and Virtual IPS

IBM offers end-to-end security for the hybrid cloud

Manage Access

Securely connect people, applications, and devices to the cloud

Identity federation to SaaS applications
Allow employees to federation and single sign-on from enterprise to SaaS services

Single Sign On APIs
Allows developers to add access security to apps built on the IBM Cloud (Bluemix) using IBM id and popular social identities

Access and privileged Identity management for Cloud
Allows customers, employees and administrators to securely access Cloud resources enforcing separation of duties and privileged user monitoring

Managed Cloud Identity Solution
Comprehensive cloud-based Identity and Access management built upon IBM's IAM software and global delivery capabilities

Protect Data

Identify vulnerabilities and prevent attacks targeting sensitive data

Network Protection for virtualized infrastructure
A new high-speed threat protection appliance to control and defend virtualized infrastructure

Application Security Scanning as Cloud service
Mobile and Web application scanning services for Bluemix developers to quickly find software vulnerabilities

Data activity monitoring for Cloud
Database monitoring and control for AWS and SoftLayer, using Guardium

Managed Security for SoftLayer
Fully incorporates IBM's managed security services into SoftLayer, with Vyatta support

Data encryption and key management
Data encryption and standards-based encryption key lifecycle management

Gain Visibility

Monitor the cloud for security breaches and compliance violations

Visibility across hybrid cloud environments
Security monitoring of IaaS, PaaS, and SaaS platforms, as well as cloud-based applications with automated customizable reporting and alerts

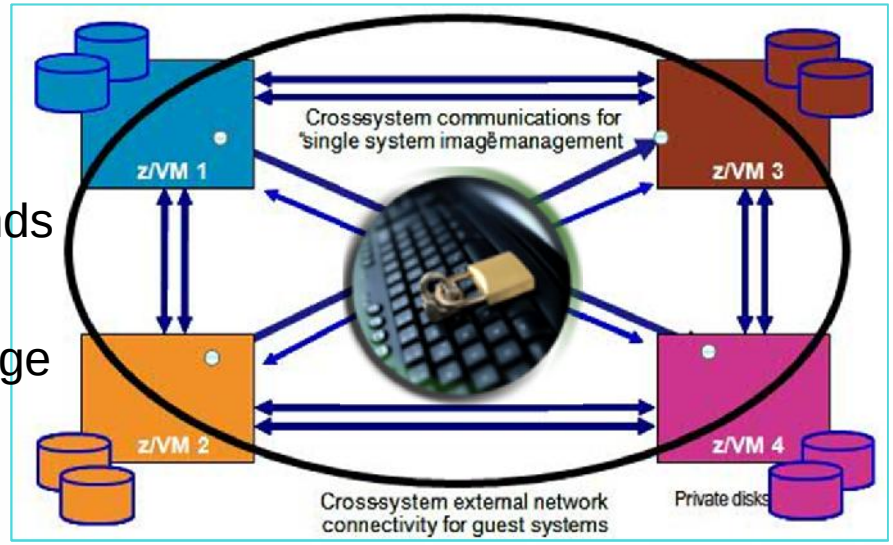
Security intelligence
Enabling IBM Cloud customers to easily deploy Security Intelligence to detect threats and monitor regulatory compliance such as PCI, SOX, STIGs, etc.

Next Gen Threat Protection Center
New managed security services platform to seamlessly monitor customer security from traditional to cloud environments

Virtual Machine protection
Specific security support for virtual machine isolation providing administration, auditing and compliance that includes Linux on z Systems

Infrastructure Security with RACF for z/VM

- A **requirement** for meeting today's enterprise security requirements
- RACF enhances z/VM by providing:
  - Extensive auditing of system events
  - Encryption of passwords and password phrases
  - Control of privileged system commands
  - Extensibility in z/VM environments clustered through Single System Image
  - Security Labeling and Zoning for multi-tenancy within a single LPAR



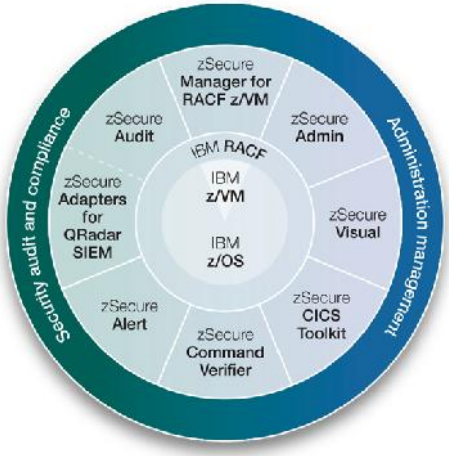
- RACF for z/VM is an integral component of z/VM's *Common Criteria evaluations (OSPP-LS at EAL 4+)*

Cloud Hypervisor Security

IBM Security zSecure Manager for RACF z/VM key features

- Combined administration and audit functionality for the z/VM environment:
- Automate complex, time consuming z/VM security management tasks with simple, one-step actions that can be performed without detailed knowledge of RACF commands
- Create comprehensive audit trails without substantial manual effort (RACF SMF records & more) from both z/VM & Linux for System z

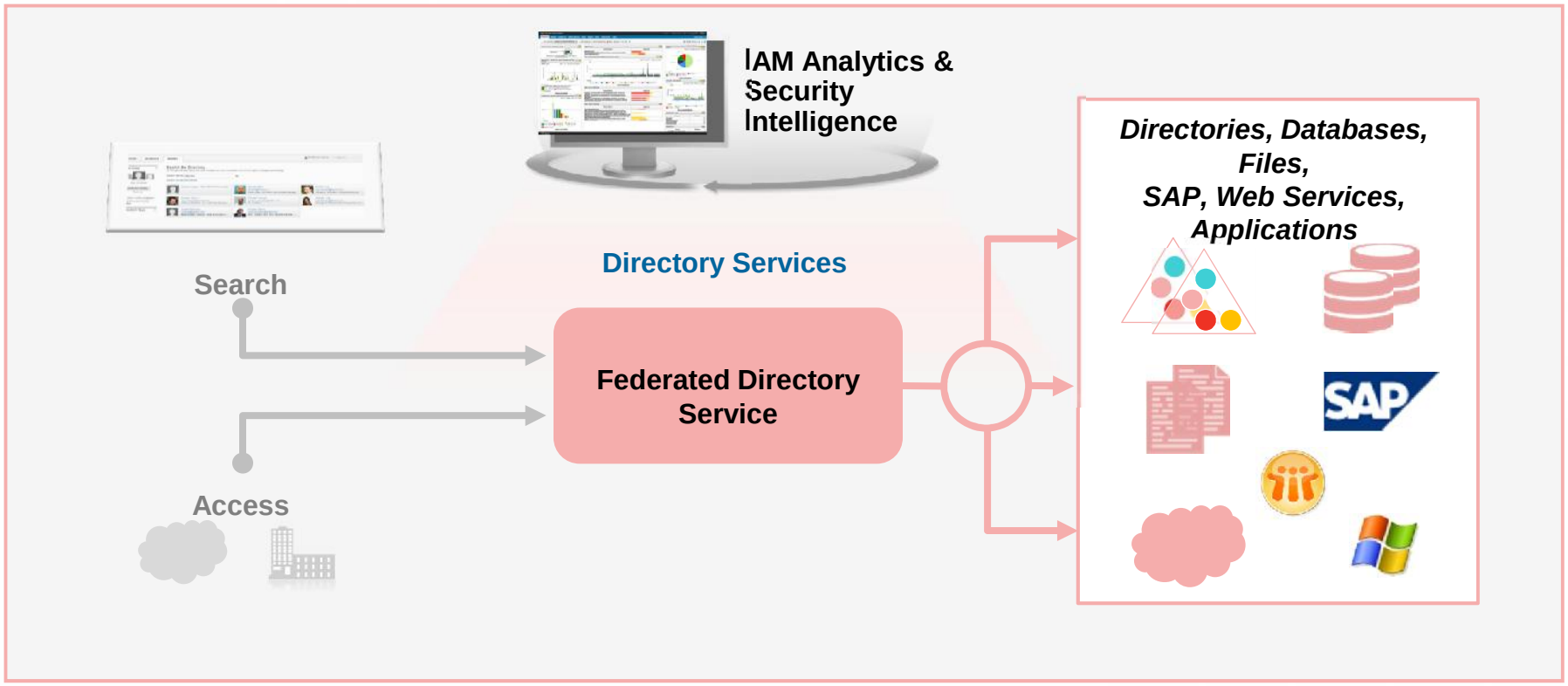
- Quickly identify and prevent problems in RACF before they become a threat to security and compliance
- Help ease the burden of database consolidation
- Generate customized reports



Note:
- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™

Cloud Directory Services

Federated Directory Services



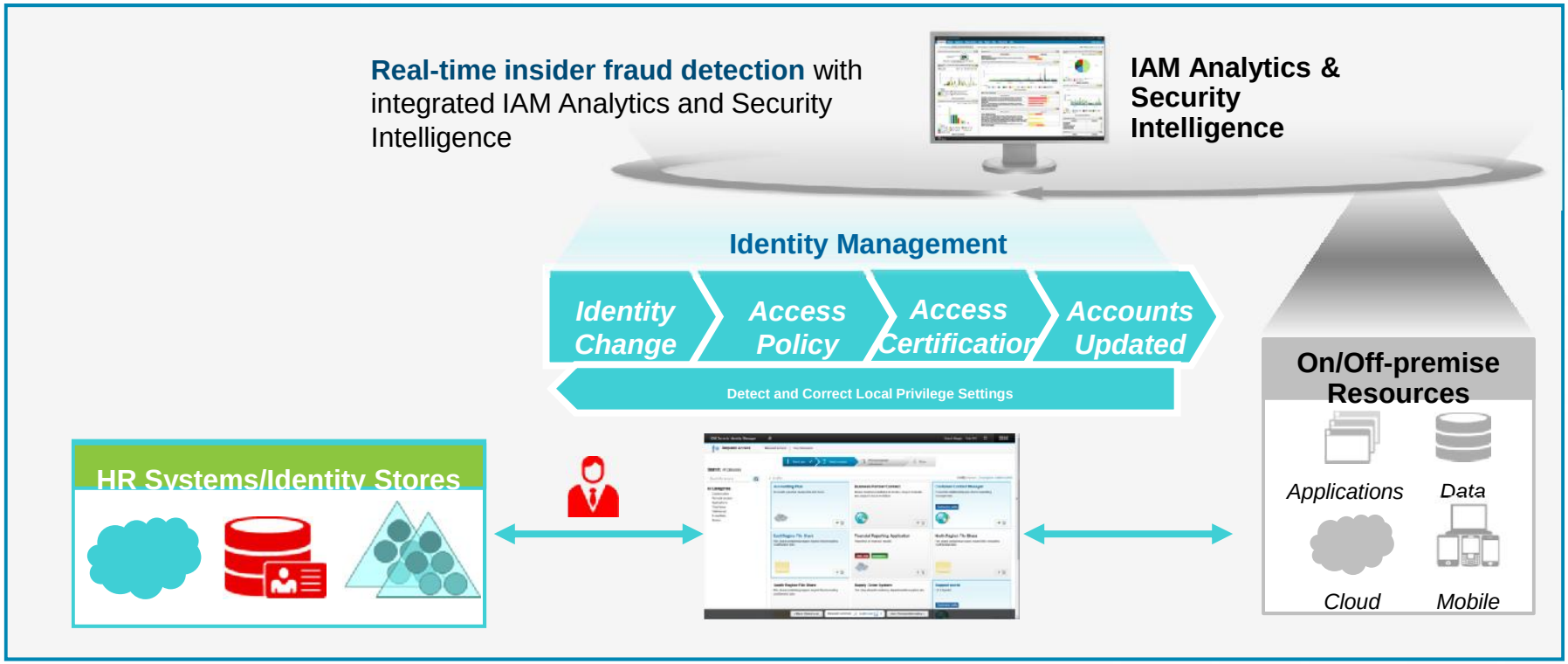
Enterprise Directory (hybrid, virtual)

Cloud Intgregation (SCIM)

Authentication (multi-directory)

Cloud Identity Management

IBM Security Identity Manager



User Provisioning (B2E, B2B)

Failed Audits (B2E, B2B)

Governance (CrossIdeas)

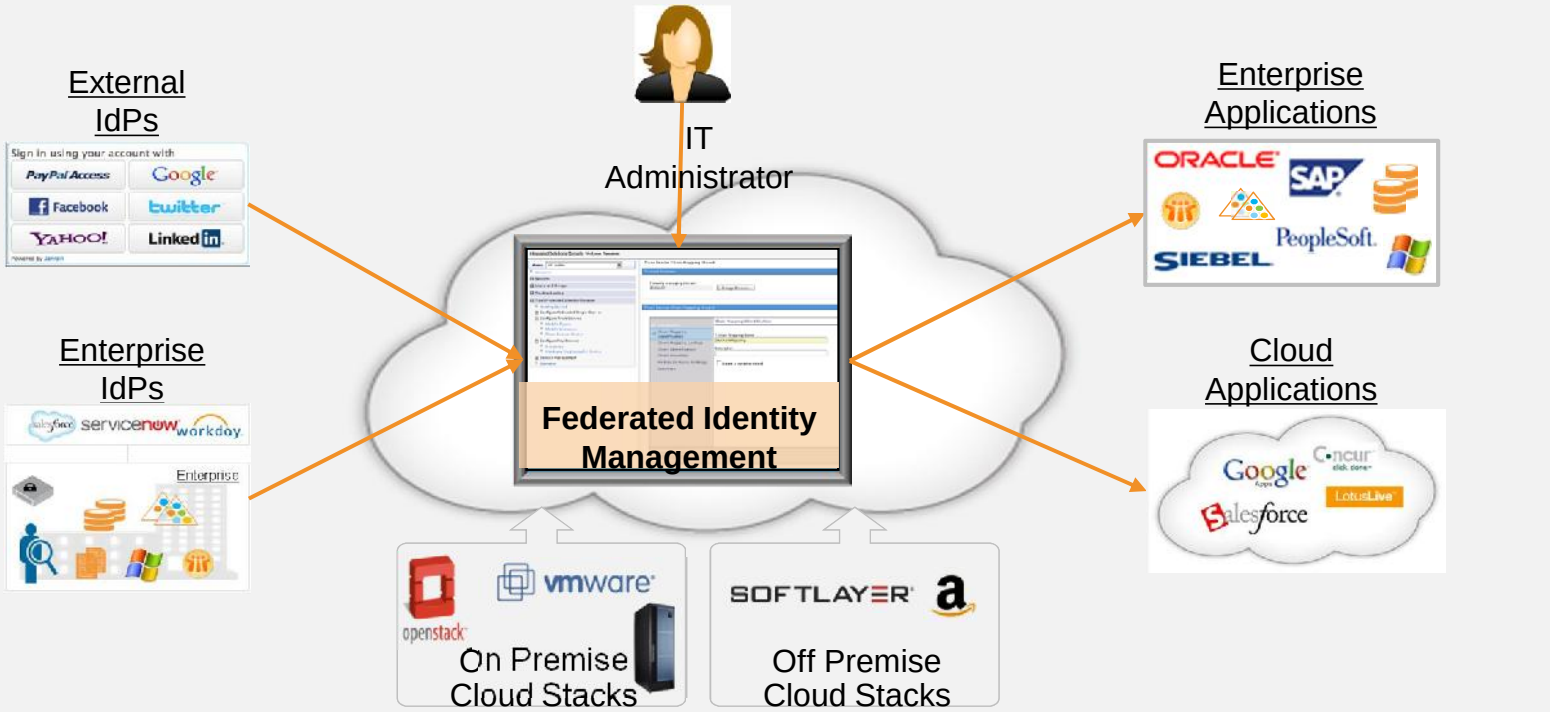
Cloud Access Management

IBM Security Access Manager

Web Access (B2E, B2C, WAF)	Mobile Access (BYOD, B2C)	Risk Access (B2B, B2C)	Fed. SSO (B2B, B2C)

Cloud Federation

Tivoli Federated Identity Manager – Made for clouds



Cloud Access (B2E, B2C)	Cloud Administration	BYO ID (B2C)	Fed. SSO (B2B, B2C)

Cloud Administrator Access Management

Privileged Identity Management: *Centralized management of privileged and shared identities*

Addressing insider threat with privileged users access management

Business challenge

Track and audit activities of privileged users (e.g., root, financial app administrators) for effective governance

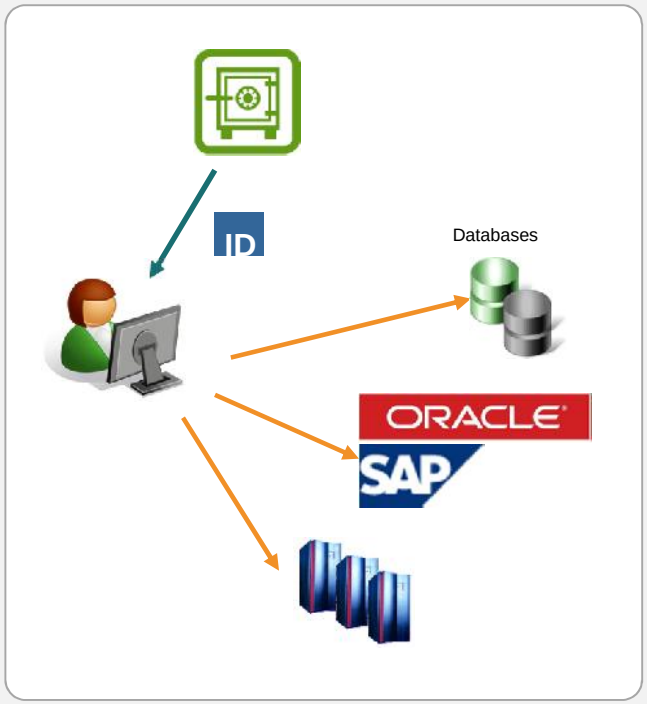
Key solution highlights

Check in / check out using secure credential vault	Control shared access to sensitive user IDs
Request, approve and re-validate privileged access	Reduce risk, enhance compliance
Track usage of shared identities	Provide increased accountability and audit trail
Automated password management	Automated checkout of IDs, hide password from requesting employee, automate password reset to eliminate password theft

IBM security solution

New Privileged Identity Management (PIM) solution providing complete identity management and enterprise single sign-on capabilities for privileged users

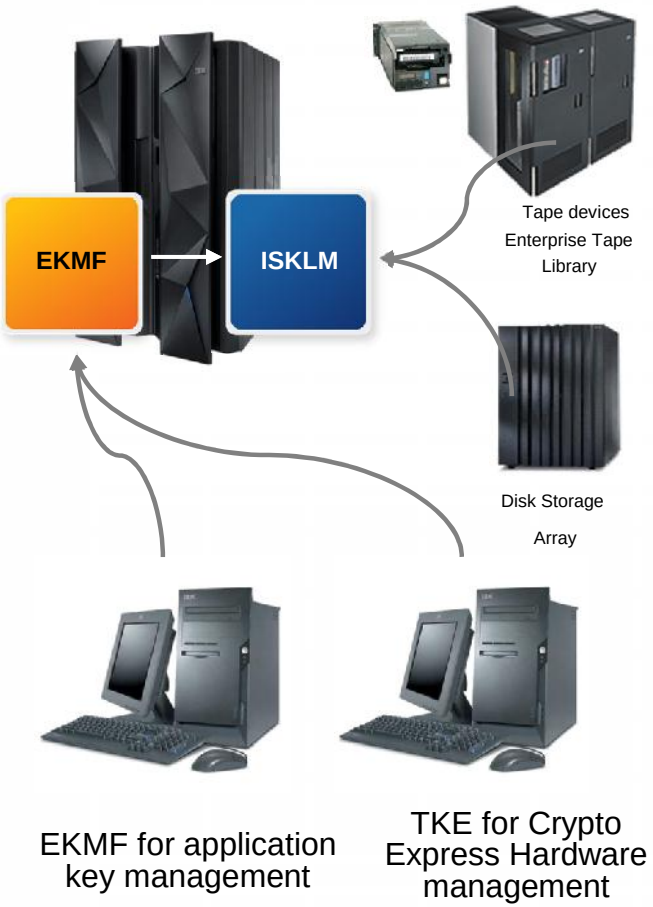
IBM Security
Privileged Identity Management



Cloud Data Protection

EKMF and SKLM for Integrated Key Management

- IBM Enterprise Key Management Foundation powered by DKMS Centralized key lifecycle management with single point of control, policy, reporting, and standardized processes for compliance
- All new keys are generated on the secured workstation by users authenticated with smart cards. The EKMF Workstation includes a IBM 4765.
- Trusted Key Entry (TKE) workstation provides a secure environment for the management of crypto hardware and host master keys
- The EKMF Browser application features monitoring capabilities and enables planning of future key handling session to be executed on the workstation.
- The central repository contains keys and metadata for all cryptographic keys produced by the EKMF workstation. This enables easy backup and recovery of key material.
- ISKLM for z/OS provides proven key serving and management for self encrypting tape and disk storage capabilities to devices



IBM provides the foundation for Integrated and Extensible Key Management

What does the enabling zSecure of with Guardium provide?

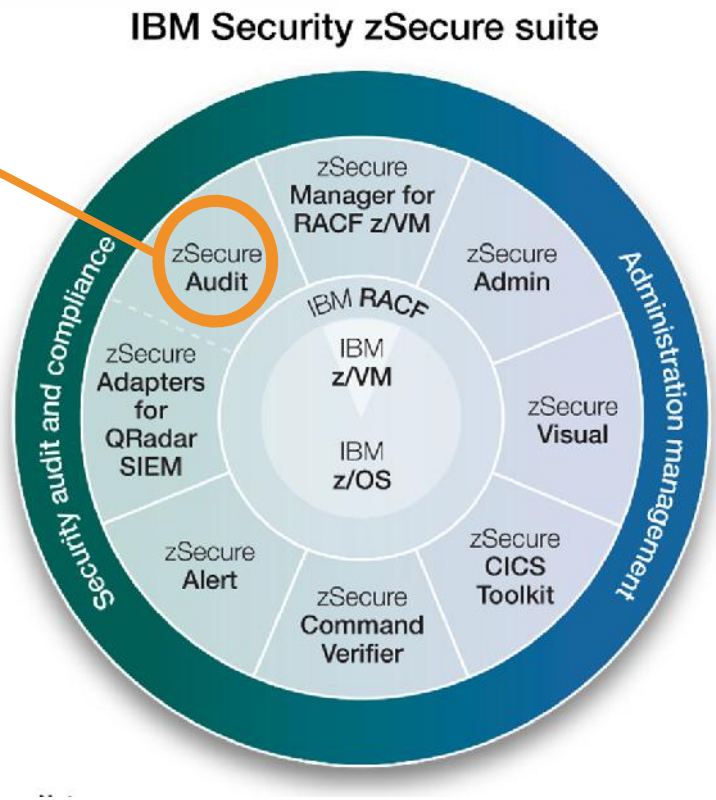
Guardium Vulnerability Assessment Tool

zSecure Audit:

- zSecure Audit job loads DB2 with CKADBVA tables
- Date and time of zSecure extract for each DB2 region
- User, Group and Connect information
- Pass RACF_DB2_ACL for all supported object types, in 2 forms:
- ACL NORMAL
- ACL EFFECTIVE

Guardium:

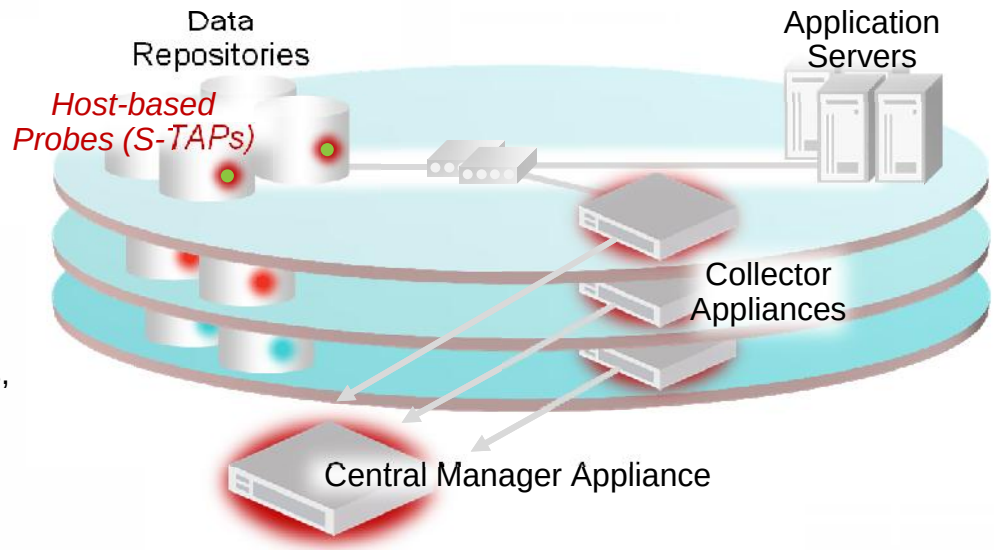
- Guardium VA 9.1 inside Guardium appliance
- picks up tables if new information
- applies policy
- creates exception reports



- IBM Security zSecure Audit for RACF, CA ACF2 or CA Top Secret

IBM InfoSphere Guardium real-time activity monitoring

- **Activity Monitoring**
  Continuous policy-based real-time monitoring of all data traffic activities, including actions by privileged users
- **Blocking and Masking**
  Automated data protection compliance
- **Vulnerability Assessment**
  Database infrastructure scanning for missing patches, misconfigured privileges, and other vulnerabilities

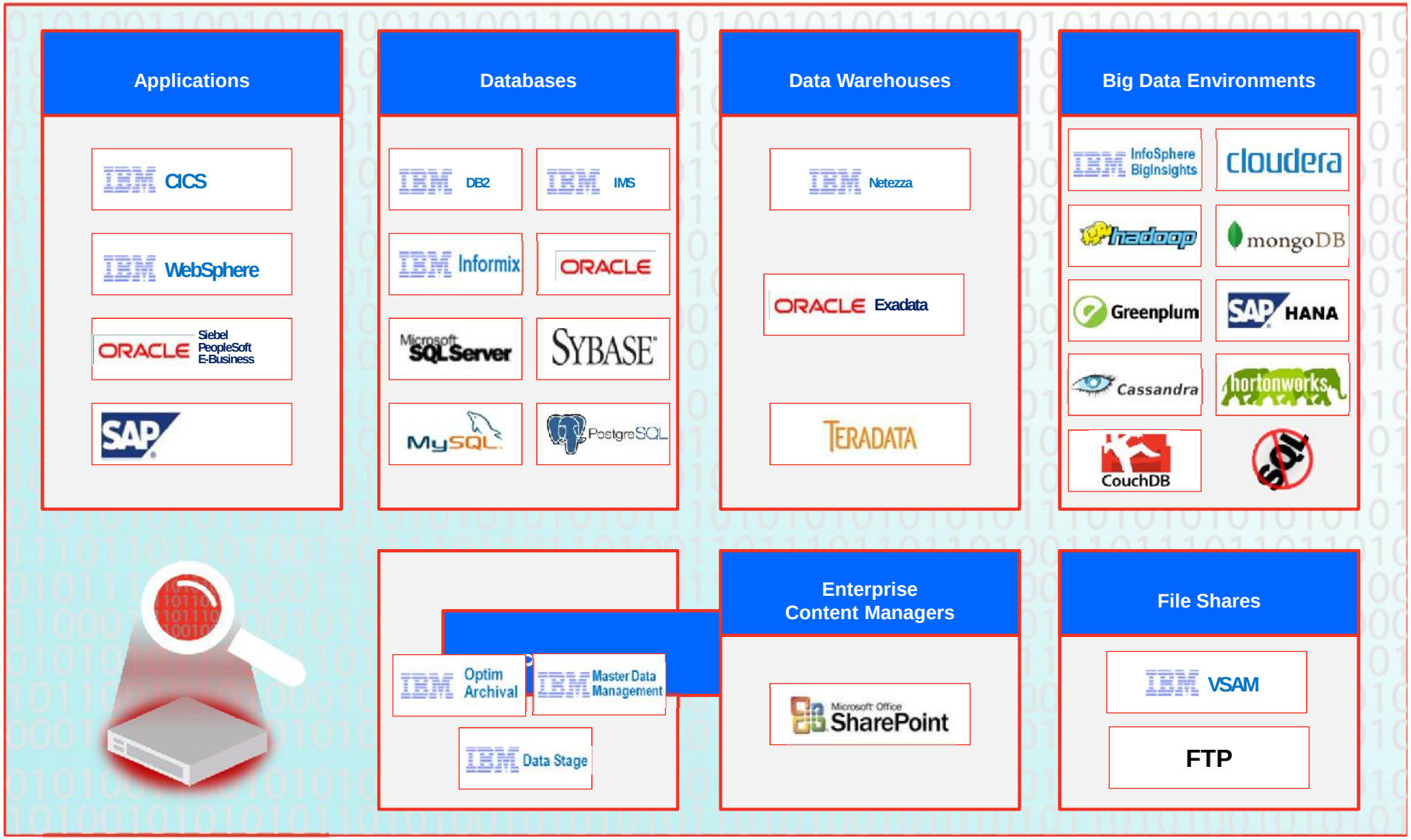


Key functionality

- Non-invasive / disruptive, cross-platform architecture
- Dynamically scalable
- Separation of Duties enforcement for DBA access
- Auto discover sensitive resources and data
- Detect or block unauthorized and suspicious activity
- Granular, real-time policies (w*ho, what, when, how)*
- Doesn't rely on resident logs that are easily erased by attackers and rogue insiders
- No environment changes
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

Real-time Data Activity Monitoring across the enterprise

For data warehouses, Big Data environments, and file shares



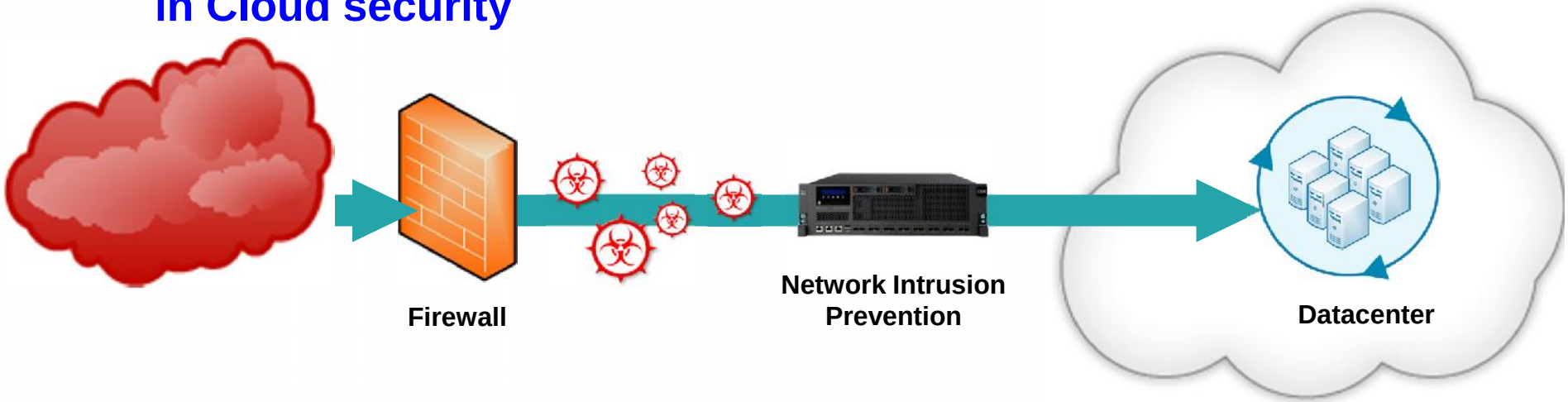
Cloud Application Security

Application security concerns in Cloud environments

- Applications natively connected to the Cloud and remotely accessible to outsiders increase the attack surfaces
- Rapid pace of development and provisioning of Web services puts pressure on developers to deliver functionality on-time and on-budget – but not to develop secure applications
- Security tests executed just before launch adds time and cost to fix vulnerabilities late in the process
- Growing number of web applications but small security staff
  - Most enterprises scan ~10% of all applications
- Continuous monitoring of production apps limited or non-existent
  - Unidentified vulnerabilities and risk

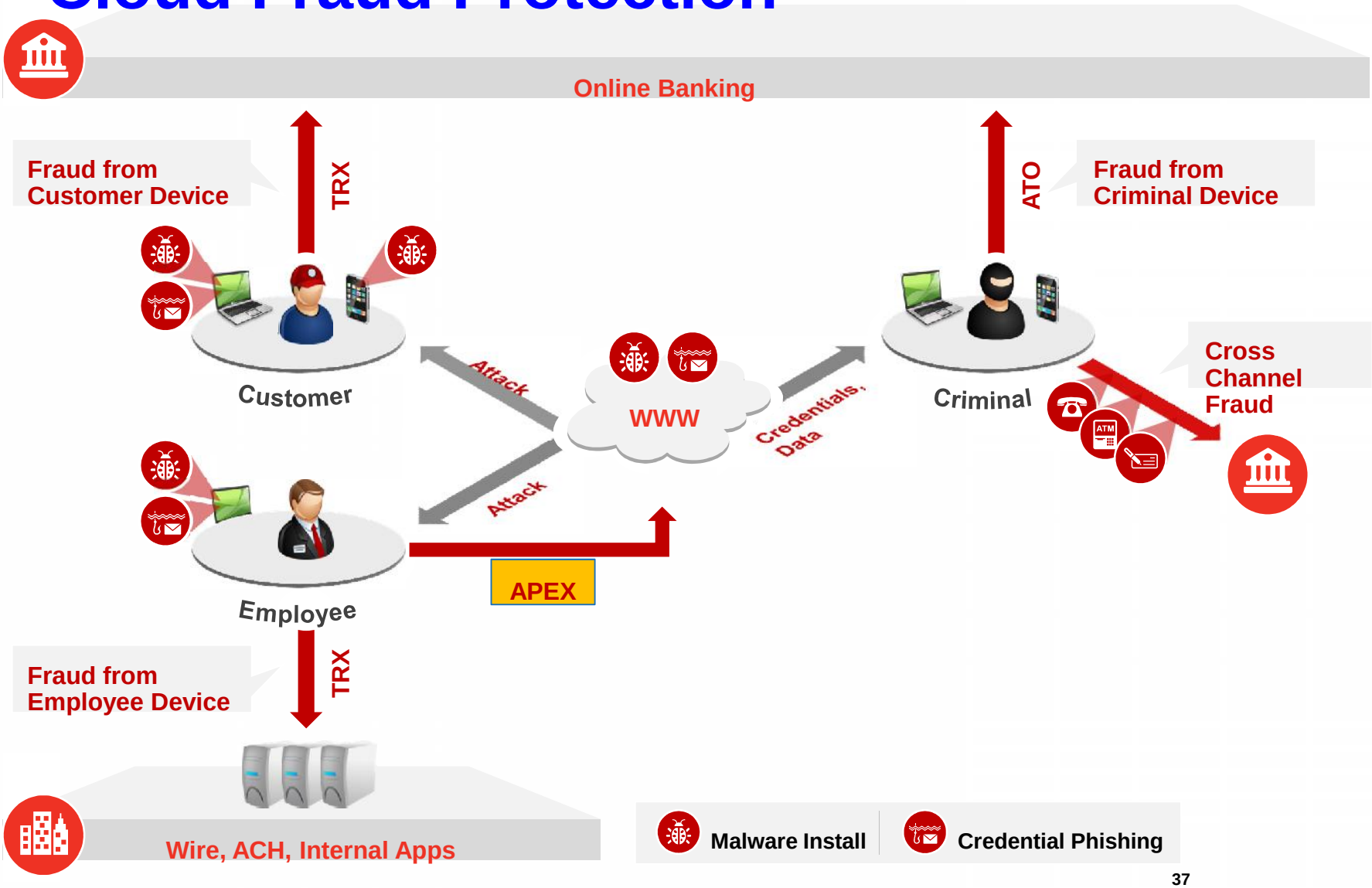
Cloud Threat Protection

Network intrusion protection is a primary building block in Cloud security



- Protect both applications and network from being exploited
- Control protocols and applications
- Monitor traffic for anomalous traffic patterns
- Protect users from being attacked (e.g., through malicious documents)
- Prove compliance with regulation requirements (e.g., PCI)
- Enforce corporate policy with employees and 3rd parties (e.g., consultants)
- Monitor network traffic for sensitive information leaving the company
- Prevent data from being stolen from databases via web applications

Cloud Fraud Protection



Cloud Intelligence and Analytics

IBM X-Force® Threat Information Center

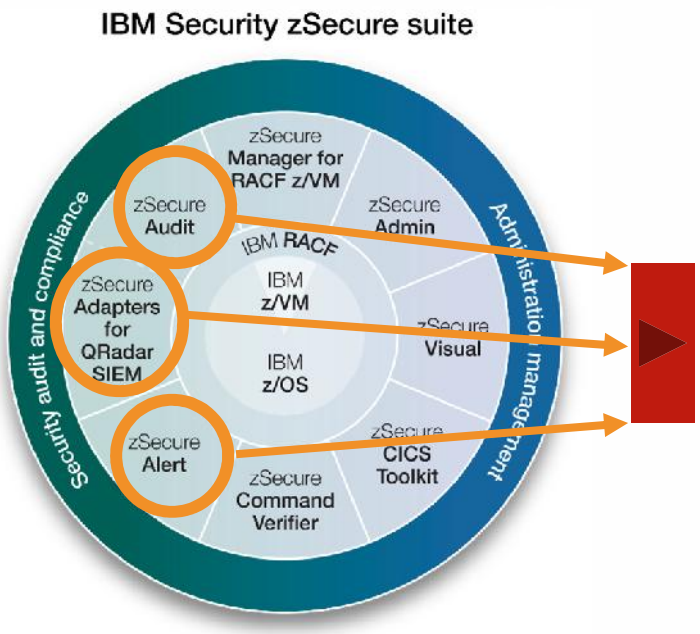
Real-time Security Overview w/ IP Reputation Correlation

Identity and User Context

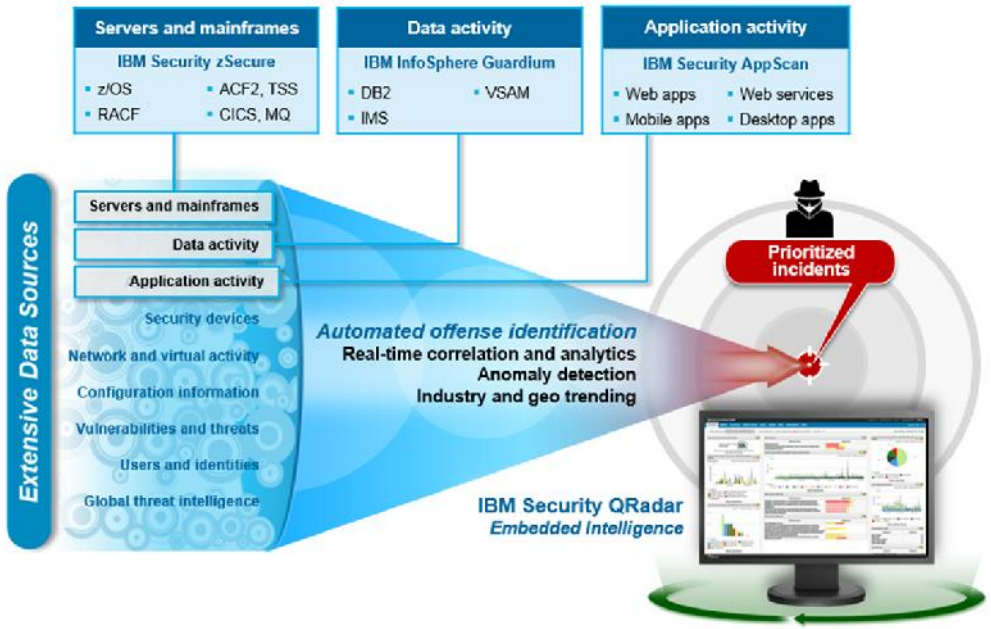
Real-time Network Visualization and Application Statistics

Inbound Security Events

zSecure QRadar integration



Note:
- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™



Event sources from System z . . .

z/OS

RACF

CA ACF2

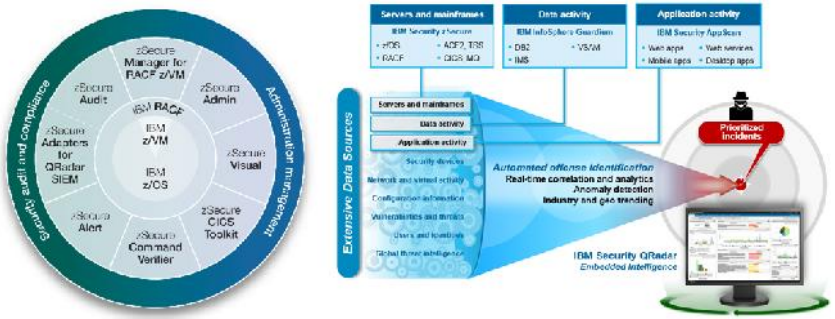
CA Top Secret

CICS

DB2

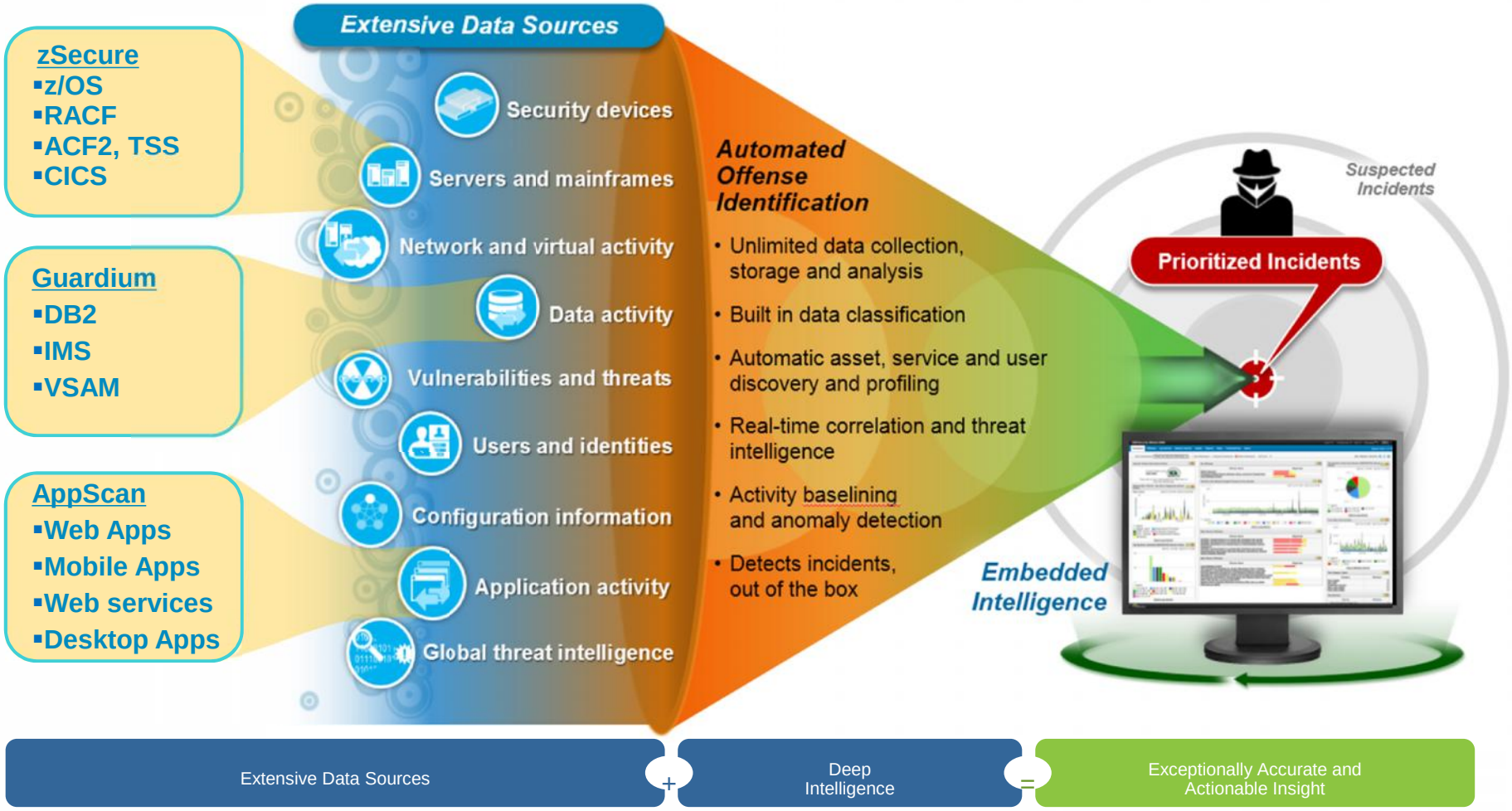
Value of zSecure integration with QRadar

- Plugs a hole in the Enterprise Security Monitoring practice
- Provides a holistic, centralised approach for Security Monitoring
- Supports separation of duties – stop the legacy practice of self-policing!
- Maximize QRadar capabilities for:
  - Log management
  - Security Information and Event Management
  - Anomaly detection
  - Incident forensics
  - Configuration Management
  - Vulnerability Management
  - Risk management



- Enhances the monitoring experience with graphical displays and user friendly reporting
- Extend best practices and comply with regulatory/legal/compliance requirements

zSecure, Guardium, AppScan with QRadar improves your Security Intelligence



✓ Centralized views; automatic alerts; increased accuracy; simplified compliance

Security Solutions for System z Cloud Scenarios

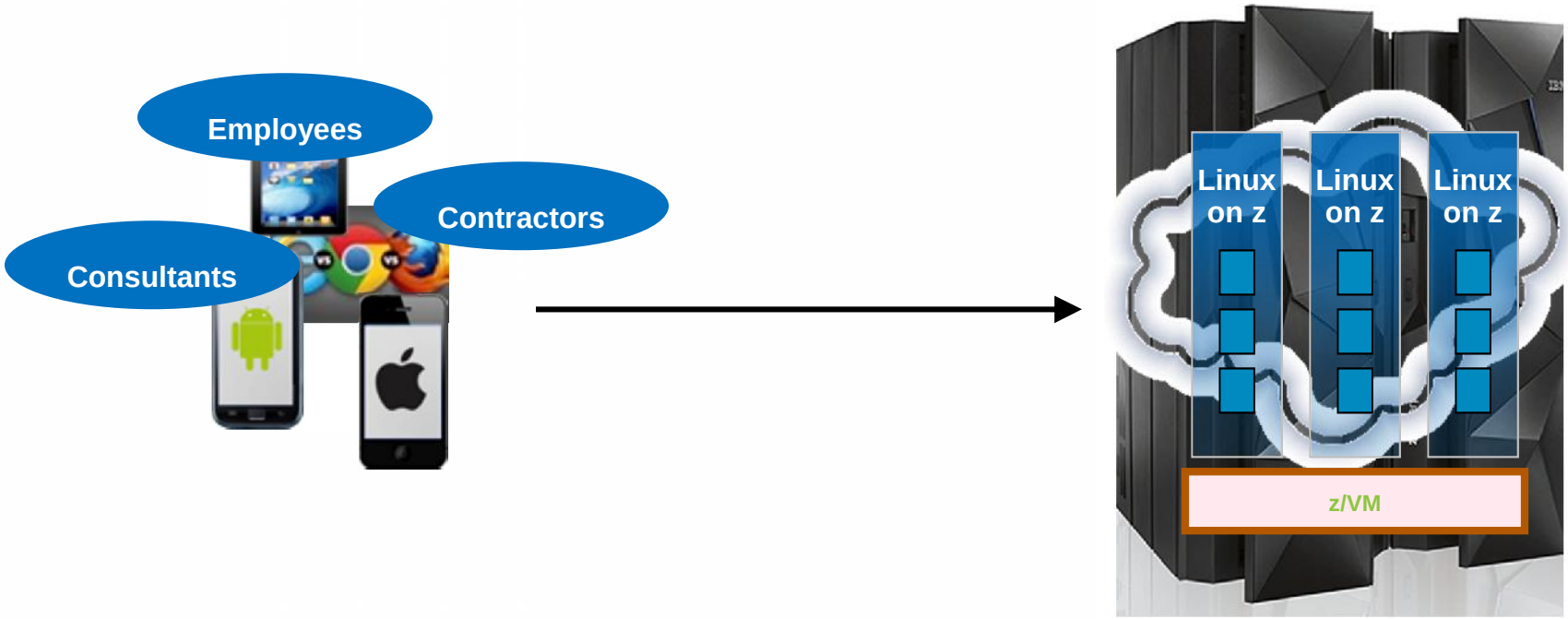
	Private Cloud with Linux on Z	Private Cloud with Linux & z/OS	Hybrid Cloud (IaaS and PaaS)	Hybrid Cloud (SaaS)
People & Identity:				
• Identity Management	Yes	Yes	Yes	Yes
• Privileged ID Management	Yes	Yes	Yes	Possibly
• Federated Directory Services	Yes	Yes	Yes	Possibly
• Federated ID Management	Likely not	Likely not	Possibly	Yes
• Access Management for Web	Yes	Yes	Yes	Yes
• Access Management for Mobile	Possibly	Possibly	Yes	Yes
Applications:				
• Application Vulnerability	Yes	Yes	Yes	Possibly
Data:				
• Database Protection	Yes	Yes	Possibly	Possibly
• Encryption Key Management	Yes	Yes	Possibly	Possibly

Security Solutions for System z Cloud Scenarios

	Private Cloud with Linux on Z	Private Cloud with Linux on Z & z/OS	Hybrid Cloud (IaaS and PaaS)	Hybrid Cloud (SaaS)
Infrastructure:				
• IDS/IPS	Yes	Yes	Yes	Yes
zSecure:				
• Admin	No	Yes	Yes	Yes
• Audit	No	Yes	Yes	Yes
• Alert	No	Yes	Yes	Yes
• Command Verifier	No	Yes	Yes	Yes
• Visual	No	Yes	Yes	Yes
• Manager for RACF z/VM	Yes	Yes	Possibly	Possibly
• CICS Toolkit	No	Possibly	Possibly	Possibly
Fraud:				
• Fraud Prevention	Yes	Yes	Yes	Yes
Intelligence/Analytics:				
• SIEM	Yes	Yes	Yes	Yes

System z Cloud Scenario #1: Private Cloud with Linux on z

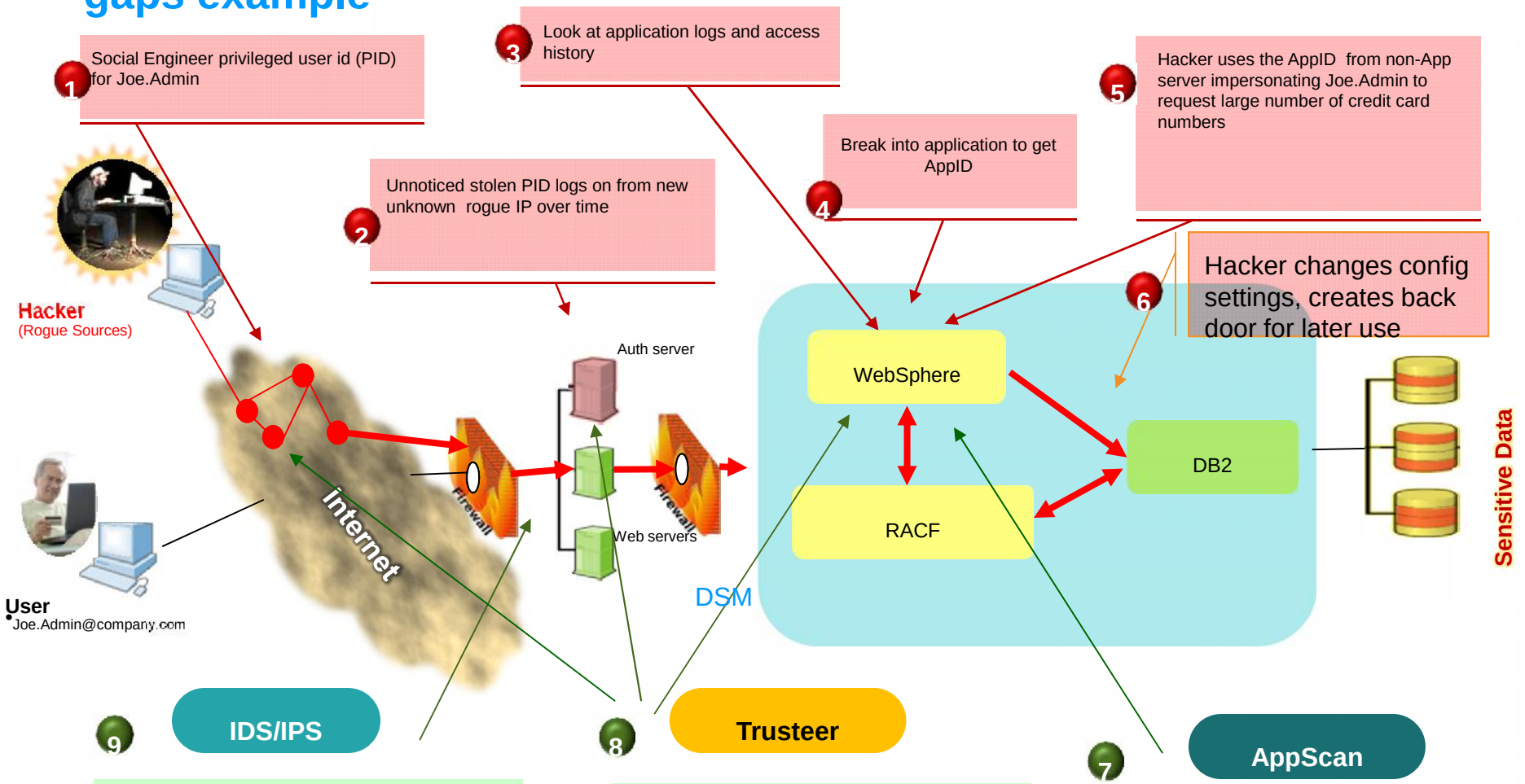
Multiple workloads from distributed platforms consolidated into a single, scalable footprint utilizing Linux on z



So, going back to this first scenario, lets take a look at how security solutions detect and prevent exploitations of security vulnerabilities.

Cloud Security – the Total Picture

Anatomy of an attack: Preventing losses and closing security gaps example



9 **IDS/IPS**

Detects attempted exploitations of security vulnerabilities
Prevents intrusion attacks such as SQL injections, cross site scripting
Provides zero day protection against security vulnerabilities

8 **Trusteer**

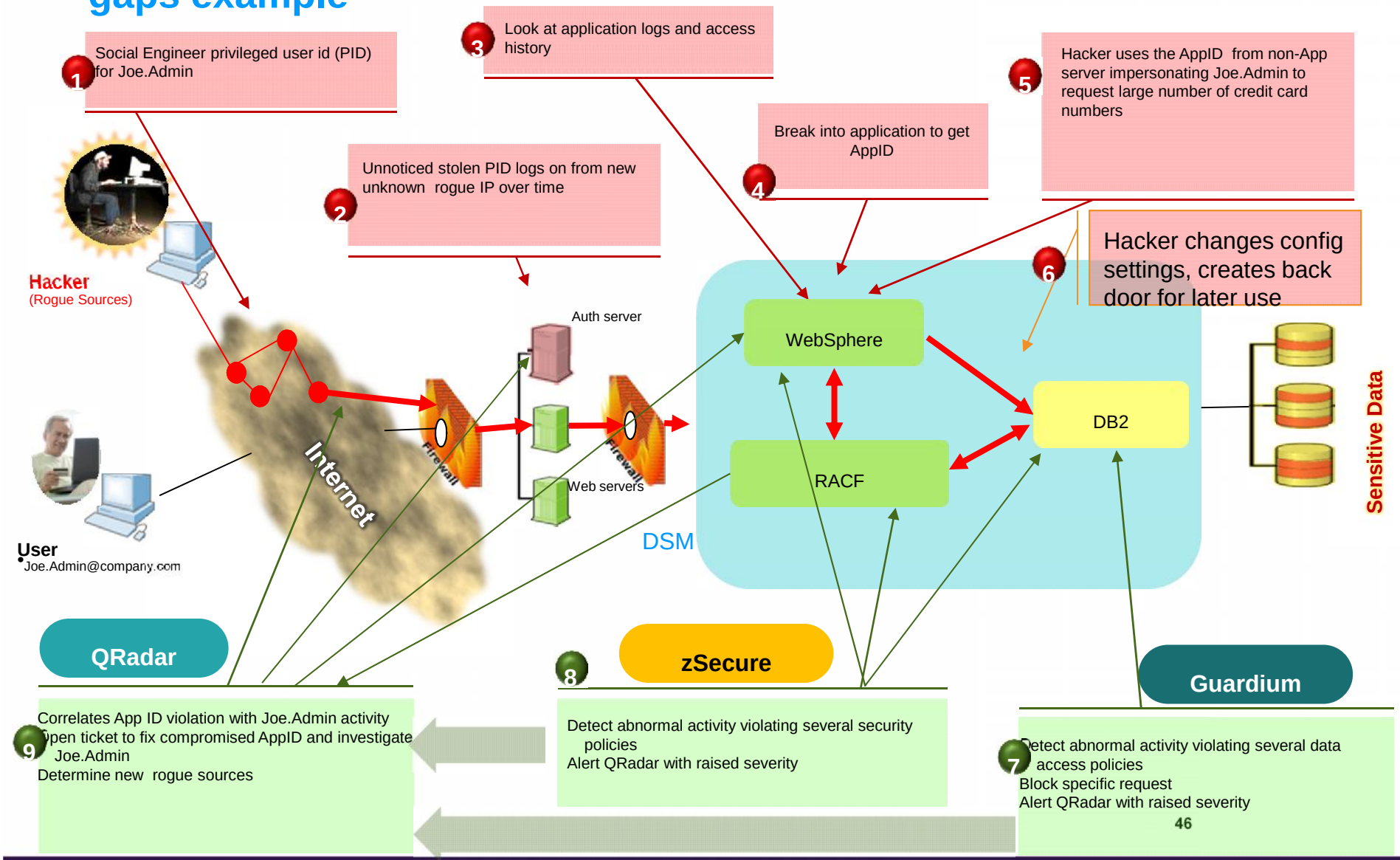
Detects abnormal activity violating comprised credentials
Detects and prevents attempts at account takeover

7 **AppScan**

Detects application vulnerabilities
Alert IDS/IPS to modify protection policies
Alert QRadar with raised severity

Cloud Security – the Total Picture

Anatomy of an attack: Preventing losses and closing security gaps example



System z – Security in the Cloud

Summary:

Cloud – 3 delivery models:
- Private Cloud
- Public Cloud
- Hybrid Cloud

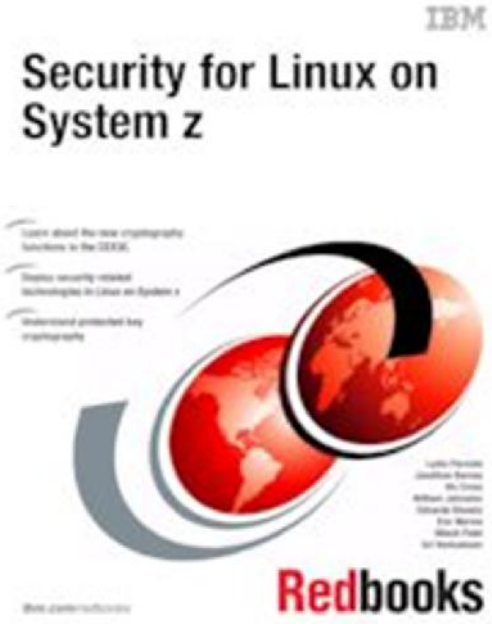
Cloud – 3 layers:
- IaaS
- PaaS
- SaaS

Security Domains:
- Identity
- Data
- Security Intelligence and Analytics
- Applications
- Infrastructure

System z – 4 Typical Scenarios:
- Private Cloud with Linux on z
- Private Cloud with Linux and z/OS
- Hybrid Cloud (IaaS & PaaS)
- Hybrid Cloud (SaaS)

Z Systems in the Cloud

Linux on z Systems Redbook



- Introduction
  - Hardware, z/VM and Storage Configuration
- The z/VM security management support utilities
- Configuring and using the z Systems LDAP servers
  - For both z/OS and z/VM
- Authentication and access control
- Cryptographic hardware
  - Clear and secure key and CPACF
- Physical and infrastructure security on z Systems
  - Protecting the HMC, system configuration, disk security, z/VM minidisks, firewall
- Security implications of z/VM SSI and LGR
- Best Practices

- Where to find: http://www.IBM.com/redbooks/pdfs/sg247728.pdf

Questions?

Thank You!