IBM

Rethink IT.
Reinvent Business.
Smart, Secure and Ready for Business

IBM Cloud Computing Reference Architecture 3.0 – Security

Table of Contents

Cloud Security – IBM Point of View

Security is a top concern in cloud adoption

There is universal interest in cloud computing across all industries and geographies

Cost Take-out is Key Driver

- #1 reason to move to a public cloud is lower total cost of ownership
- Top reasons for moving to a private cloud include cost/resource efficiencies, as well as enhancing speed and flexibility

Security is Top Concern

- Security concerns are the top barrier to adoption of both public and private clouds
- Experience managing large outsourcing engagements gives IBM the tools to manage customers' top cloud concerns

Adoption Patterns are Emerging

- Three distinctive end-user cloud buying patterns are emerging: exploratory, solution-focused and transformational
- There are reports that public clouds are being adopted faster than originally forecast

Cloud computing tests the limits of security operations and infrastructure

In a cloud environment, access expands, responsibilities change, control shifts, and the speed of provisioning resources and applications increases - **greatly affecting all aspects of IT security**.

Different cloud deployment models also change the way we think about security

Private cloud

On or off premises cloud infrastructure operated solely for an organization and managed by the organization or a third party

Hybrid IT

Traditional IT and clouds (public and/or private) that remain separate but are bound together by technology that enables data and application portability

Public cloud

Available to the general public or a large industry group and owned by an organization selling cloud services.

Changes in Security and Privacy

- *Customer responsibility for infrastructure*
- *More customization of security controls*
- *Good visibility into day-to-day operations*
- *Easy to access to logs and policies*
- *Applications and data remain "inside the firewall"*

- *Provider responsibility for infrastructure*
- *Less customization of security controls*
- *No visibility into day-to-day operations*
- *Difficult to access to logs and policies*
- *Applications and data are publically exposed*

Resultant client security requirements vary, depending on cloud model that a client adopts

Private cloud
On premise

Hybrid IT

Breadth in Security and Privacy Requirements

Identity and Access Management - *data center identities & single sign-on, access management to VMs, images; privileged identity*

Virtual Infrastructure protection and integrity – *endpoint management for VMs; inventory management; integrity of cloud environment; network and VM isolation*

Integration and Ease of Use - *extend existing infrastructure to implement security for virtual infrastructure, easy of use through automated security flows*

Compliance *reporting and* **vulnerability** *management in virtual environments; mapped to clients security policies and controls*

Identity and Access Management - *identity on-boarding, federation and SSO. Privileged identity & access*

Protecting Data & Information Assets- *Data jurisdiction, location visibility; encryption, destruction; privacy ; physical data center protection*

Security Governance & Compliance - *visibility to compliance posture; reports & logs; regulations, certifications, and mapping to enterprise security controls*

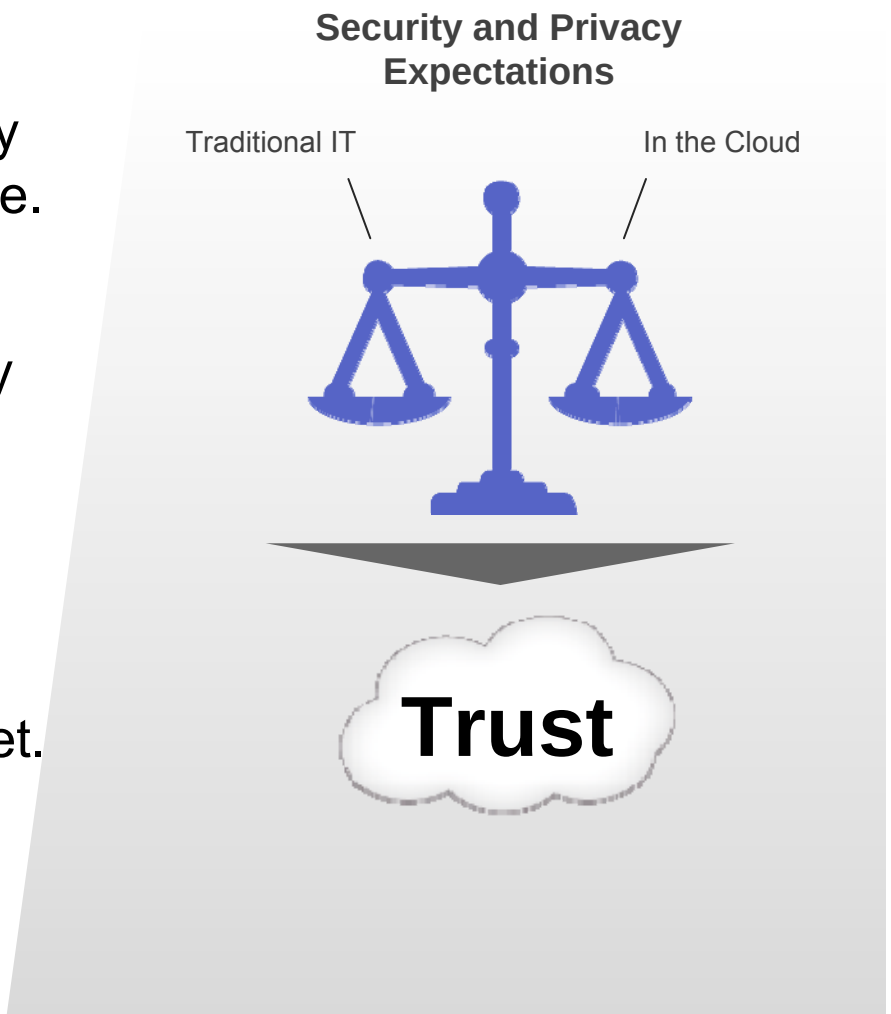
IT Risk Management - *Threat and vulnerability management ; monitoring, reporting, incident management; network isolation; physical security*

IBM Point of View - Cloud can be made secure for business

As with most new technology paradigms, **security concerns surrounding cloud computing** have become the most widely talked about inhibitor of widespread usage.

To gain the **trust** of organizations, cloud services must deliver security and privacy expectations that meet or exceed what is available in traditional IT environments.

The same way transformational technologies of the past **overcame concerns** – PCs, outsourcing, the Internet.



Cloud Security –
Method & Solution Approach

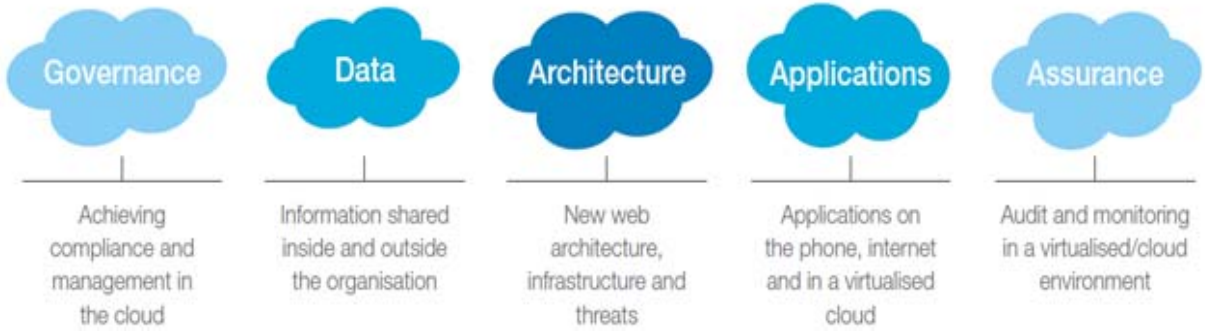
Minimizing the risks of cloud computing requires a strategic approach

- **Define a cloud strategy with security in mind**
  - Identify the different workloads and how they need to interact.
  - Which models are appropriate based on their security and trust requirements and the systems they need to interface to?

- **Identify the security measures needed**
  - Using a methodology such as the IBM Security Framework allows teams to measure what is needed in areas such as governance, architecture, applications and assurance.

Enabling security for the cloud

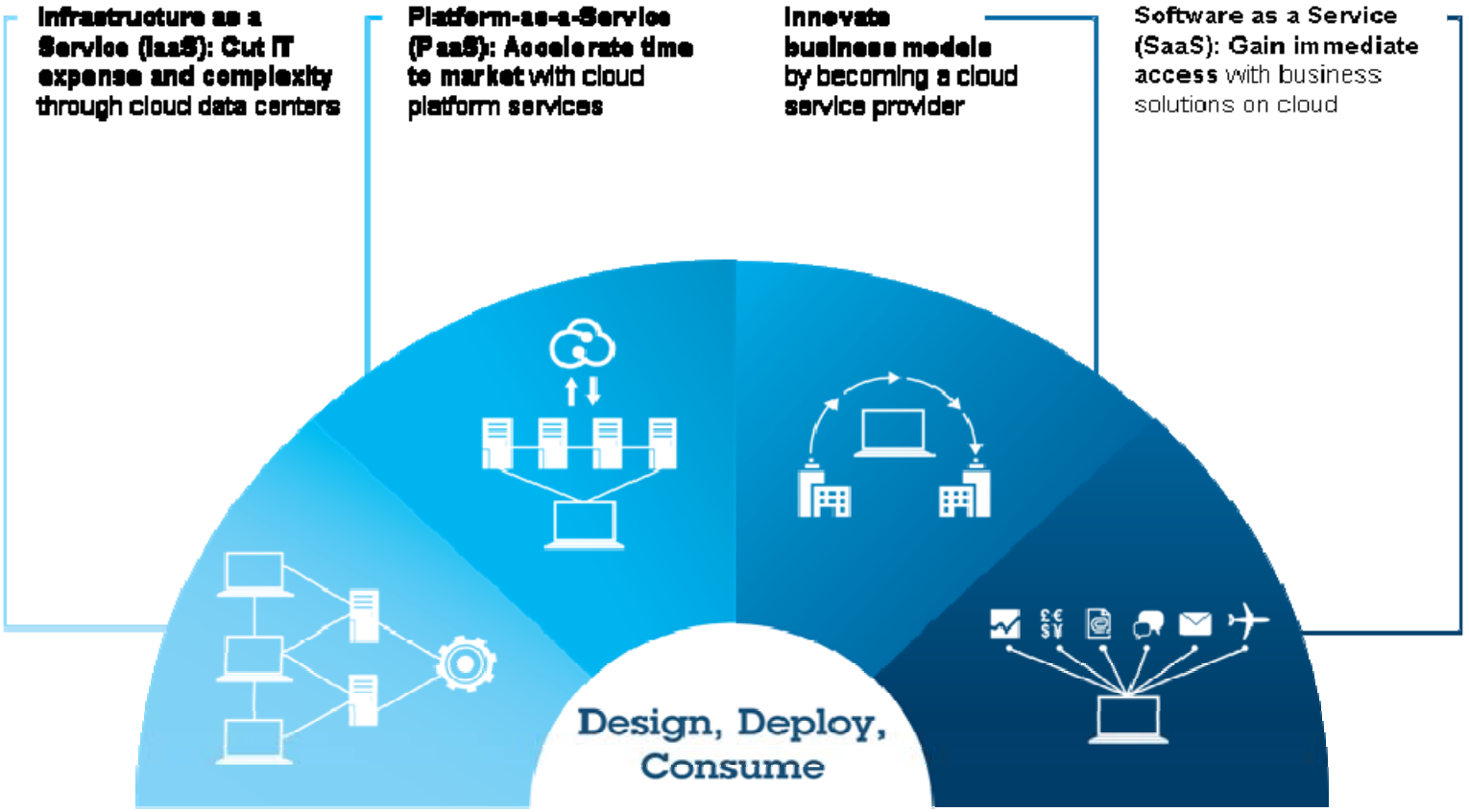
- Define the upfront set of assurance measures that must be taken.
- Assess that the applications, infrastructure and other elements meet the security requirements, as well as operational security measures.



Our approach to delivering security aligns with each phase of a client's cloud project or initiative

	Design	Deploy	Consume
	Establish a cloud strategy and implementation plan to get there.	Build cloud services, in the enterprise and/or as a cloud services provider.	Manage and optimize consumption of cloud services.
IBM Cloud Security Approach	***Secure by Design*** *Focus on building security into the fabric of the cloud.*	***Workload Driven*** *Secure cloud resources with innovative features and products.*	***Service Enabled*** *Govern the cloud through ongoing security operations and workflow.*
Example security capabilities	▪ Cloud security roadmap ▪ Secure development ▪ Network threat protection ▪ Server security ▪ Database security	▪ Application security ▪ Virtualization security ▪ Endpoint protection ▪ Configuration and patch management	Identity and access management Secure cloud communications Managed security services

Adoption patterns are emerging for successfully beginning and progressing cloud initiatives



IBM Cloud Security - One Size Does Not Fit All

Different security controls are appropriate for different cloud needs - the challenge becomes one of integration, coexistence, and recognizing what solution is best for a given workload.

Each pattern has its own set of key security concerns

Infrastructure as a Service (IaaS): Cut IT expense and complexity through cloud data centers

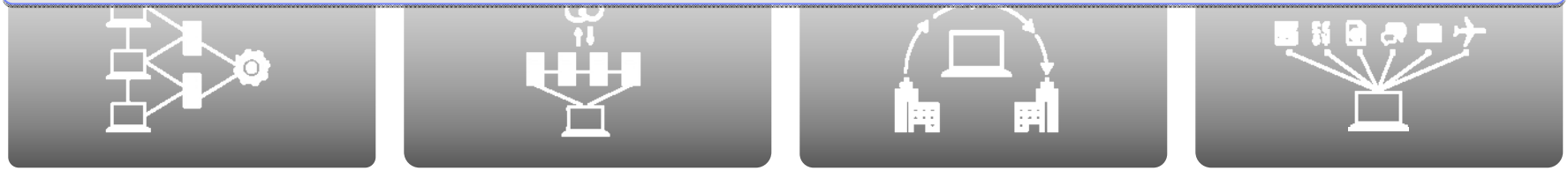
Platform-as-a-Service (PaaS): Accelerate time to market with cloud platform services

Innovate business models by becoming a cloud service provider

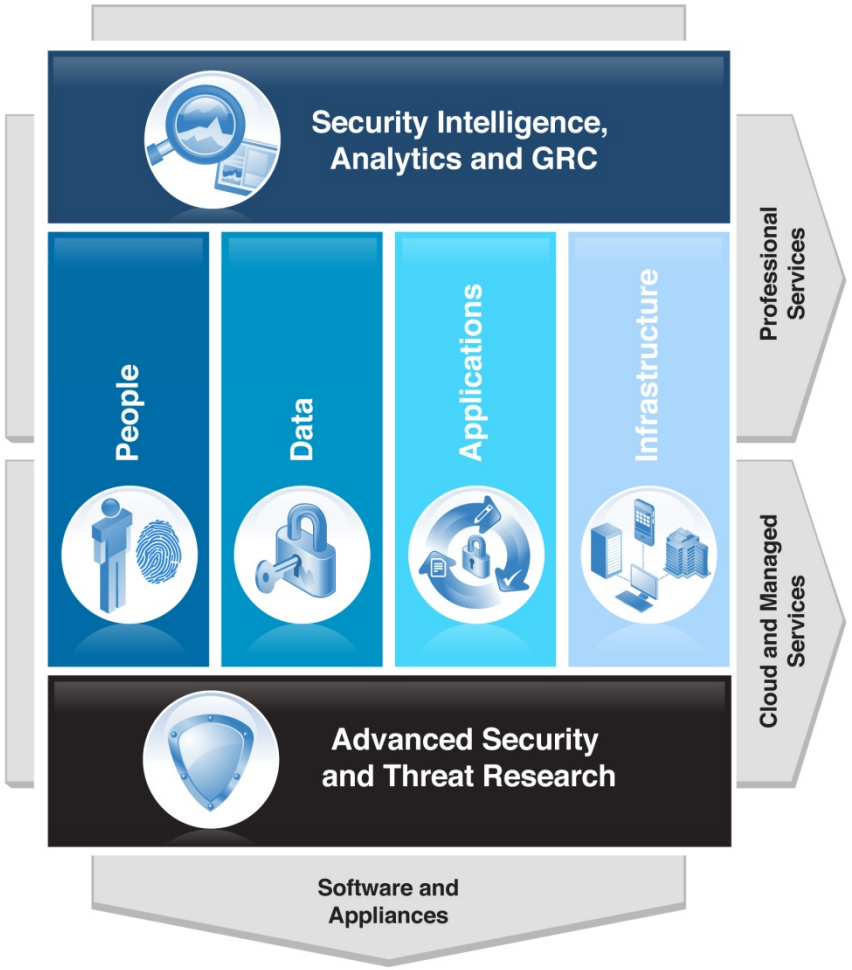
Software as a Service (SaaS): Gain immediate access with business solutions on cloud

Cloud Enabled Data Center	Cloud Platform Services	Cloud Service Provider	Business Solutions on Cloud
Integrated service management, automation, provisioning, self service	***Pre-built, pre-integrated IT infrastructures tuned to application-specific needs***	***Advanced platform for creating, managing, and monetizing cloud services***	***Capabilities provided to consumers for using a provider's applications***
Key security focus: **Infrastructure and Identity**	Key security focus: **Applications and Data**	Key security focus: **Data and Compliance**	Key security focus: **Compliance and Governance**
▪Manage datacenter identities ▪Secure virtual machines ▪Patch default images ▪Monitor logs on all resources ▪Network isolation	▪Secure shared databases ▪Encrypt private information ▪Build secure applications ▪Keep an audit trail ▪Integrate existing security	▪Isolate cloud tenants ▪Policy and regulations ▪Manage security operations ▪Build compliant data centers ▪Offer backup and resiliency	▪Harden exposed applications ▪Securely federate identity ▪Deploy access controls ▪Encrypt communications ▪Manage application policies

Security Intelligence – threat intelligence, user activity monitoring, real time insights



Using the Security Framework we articulate the way we address security in the Cloud in terms of Foundational Controls



Design

Cloud Governance
Cloud specific security governance including directory synchronization and geo locational support

Discover, Categorize, Protect Data & Information Assets
Strong focus on protection of data at rest or in transit

Deploy

Security Governance, Risk Management & Compliance
Security governance including maintaining security policy and audit and compliance measures

Information Systems Acquisition, Development, and Maintenance
Management of application and virtual Machine deployment

Problem & Information Security Incident Management
Management and responding to expected and unexpected events

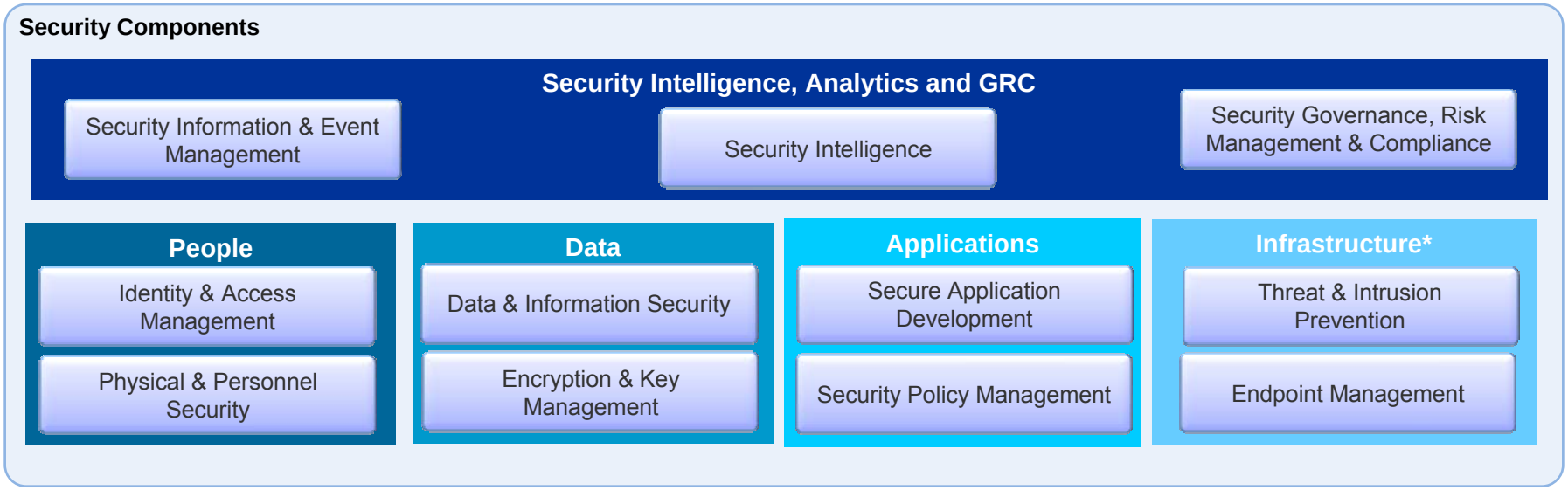
Secure Infrastructure Against Threats and Vulnerabilities
Management of vulnerabilities and their associated mitigations with strong focus on network and endpoint protection

Consume

Identity and Access Management
Strong focus on authentication of users and management of identity

Physical and Personnel Security
Protection for physical assets and locations including networks and data centers, as well as employee security

CCRA Security Component Model



*Infrastructure Includes – Server, Network, Storage

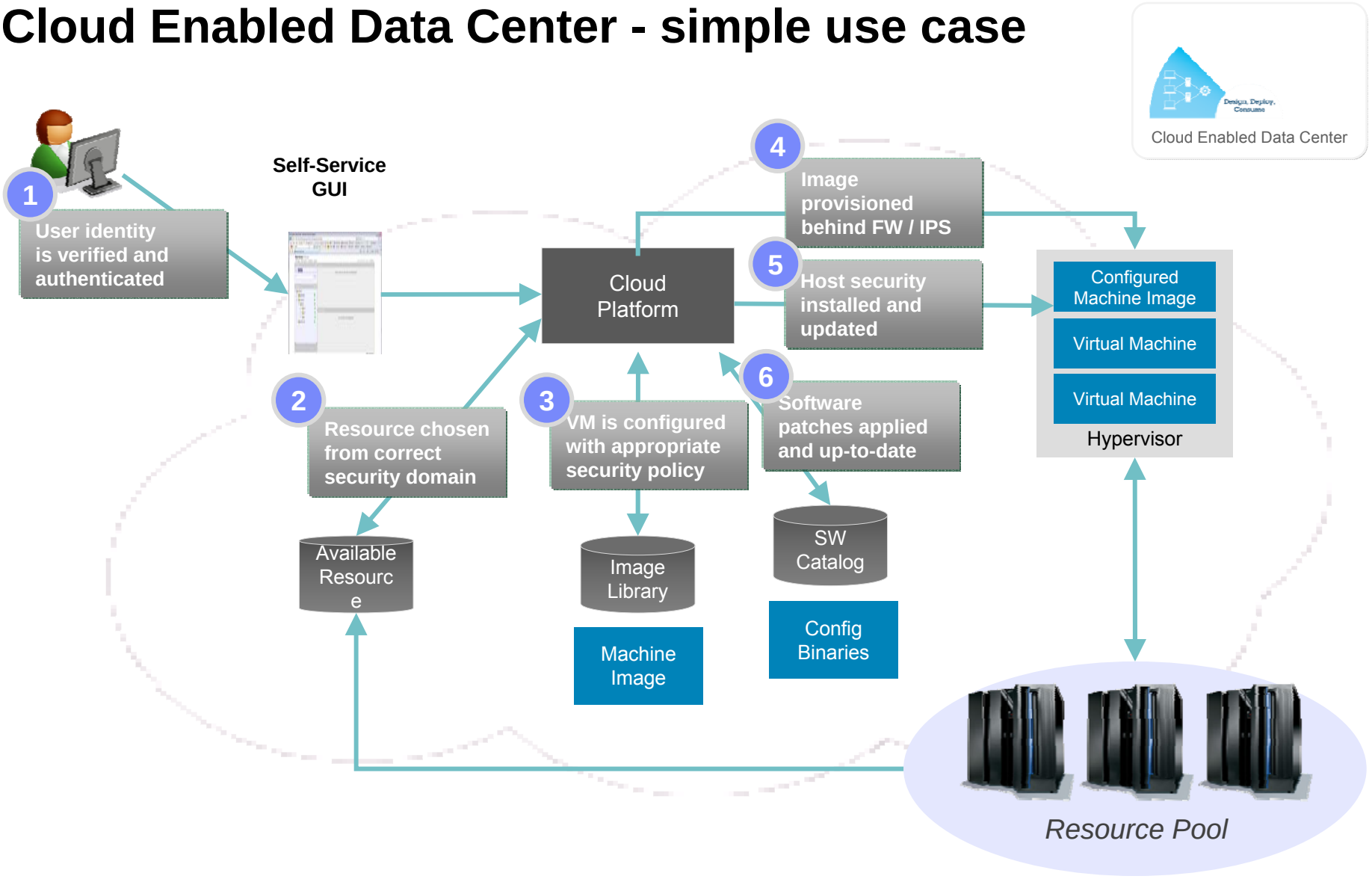
Solution Approach - Summary

Understand Client	Business Driver	Get a thorough understanding of their existing IT environment and identify the client's ***Cloud Adoption Pattern***
Define Client Requirements	Actors and use cases Non-functional requirements	Identify **actors**, **workloads** and associated **use cases** and identify **security requirements** for each scenario Define the **Architecture Overview**
Design Solution	System context Architecture decisions Architecture overview	Identify the building blocks and controls needed leveraging the **IBM Security Framework** and **Cloud Foundational Controls**
Detail Design	Component model Operational model Solution integration Details	Use the CCRA Security **Component Model** to identify required components and their interactions for the solution Realize the component by mapping to the capabilities in our **products / services portfolio**
Define Roadmap & 1st Project	Cloud roadmap Project description Viability Assessment	Leverage **assets** to build the deployment architecture and integration requirements Define the **project plan** with overall timeline, phases and key milestones, and overall delivery

This deck contains the material common to all patterns.
Refer to the pattern specific documents for details on each pattern

Cloud Security Requirements (based on Cloud Adoption Pattern)

Cloud Enabled Data Center - simple use case



Securing Cloud Enabled Data Center – Business Drivers & Use cases

Cloud Enabled Data Center

Key Business Drivers

- Use cloud infrastructure with confidence that they're secure, compliant, and meet regulatory requirements.
- Leverage existing investment & extend current infrastructure to implement security for virtual infrastructure
- Ease of Use - Automation of security steps to provide out-of-the-box capabilities for cloud
- Maintain service level compliance, accuracy, repeatability and traceability for the cloud environment

Use Cases / Key Security Requirements

Identity & Access Management:

- Manage datacenter identities and securely connect users to the cloud (Authentication & Authorization)
- Provide role based access to cloud resources - Image library, Storage
- Provision user ids on the VM for access to the VM
- Manage Confidentiality & integrity of the storage, images and meta-data associated with the master image.

Protect Virtual Infrastructure

- Secure and protect the virtual infrastructure (VM instances, hypervisors) as per IT Security Policy.

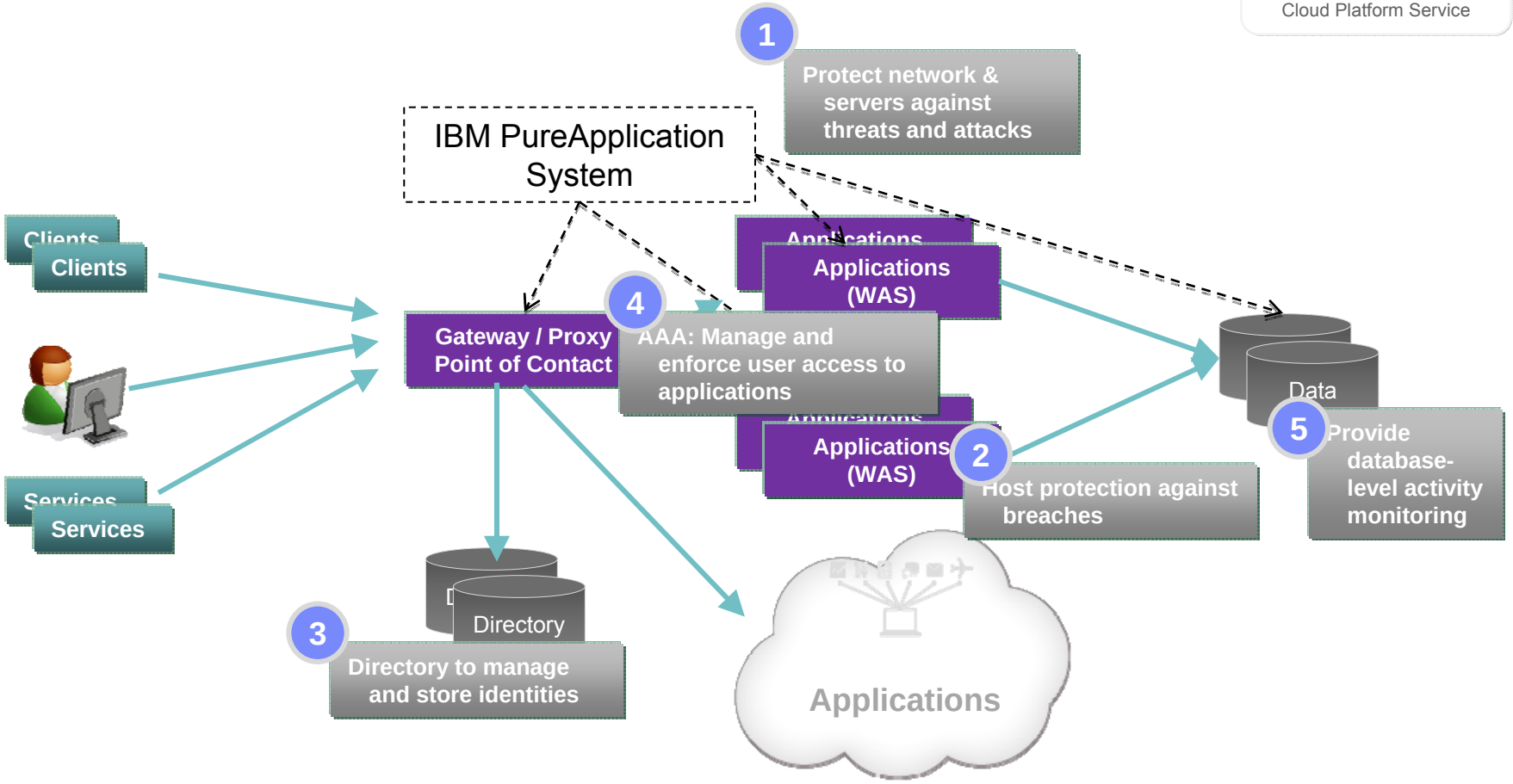
Provide visibility into virtual Infrastructure

- Maintaining audit logs for virtual infrastructure compliance and audit readiness

Integrate with Existing Infrastructure and automate complex services

- Integrate with existing security capabilities and provide automation for identity and access management, end point management and log management and visibility into the cloud infrastructure.

Cloud Platform Services - simple use case



Securing a Cloud Platform Service – Business Drivers & Use Cases

Cloud Platform Service

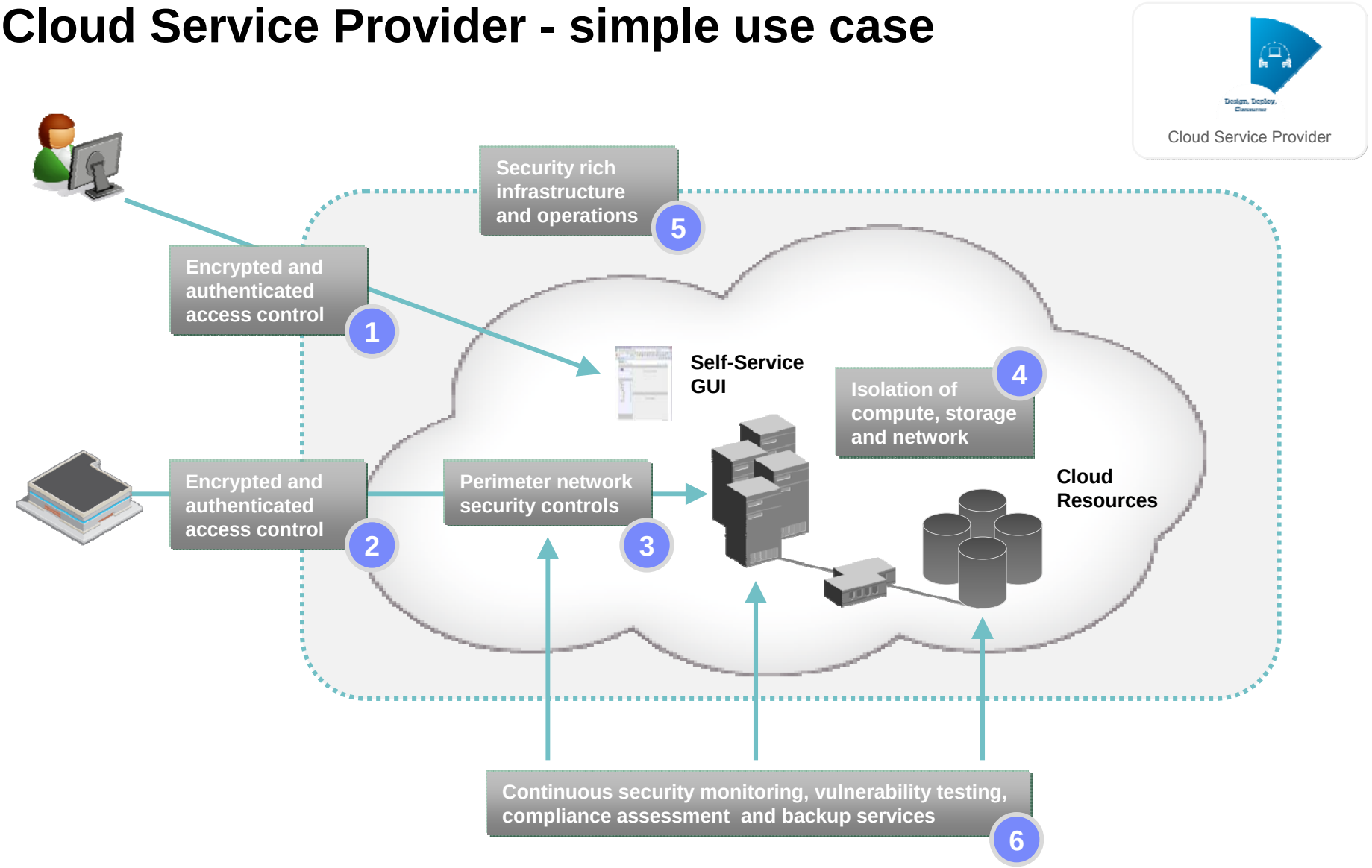
Key Business Drivers

- Protect PaaS infrastructure against threats and attacks
- Securely deploy Application workloads in PaaS environment
- Support regulatory compliance needs for the infrastructure, middleware & workload.

Use Cases / Key Security Requirements

- Manage Identities and Access
  - Including IT admin and end users for access to web applications deployed within the system
- Protect virtual servers, applications
  - against breaches, track and report (System and workload compliance)
  - against threats and attacks with intrusion prevention and detection including those tunneling through encrypted web transactions
- Provide secure platform and database services
  - Provide database-level activity monitoring and reporting for audit and compliance
- Provide threat Intelligence
  - Detect suspicious behavior in applications and demonstrate compliance
  - Internal & external threat detection in Middleware

Cloud Service Provider - simple use case



Cloud Service Provider – Business Drivers & Use Cases

Cloud Service Provider

Key Business Drivers

- Provide best-in-class security services for the cloud service consumer for the cloud hosted infrastructure and application.
- Shorten the deployment cycle for new customers
- Reduce hardware costs and energy use
- Increase the availability of information across the program and reduce the amount of effort spent maintaining existing security logic and infrastructure.

Use Cases / Key Security Requirements

Manage Identities and Access

- Role Based Access Control at various levels from tenants to individual categories
- Provide Single Sign On capability and federation of identities

Threat and Vulnerability Management

- Provide Intrusion detection and intrusion prevention capabilities
- Security Configuration and Patch Management
- Vulnerability and penetration testing

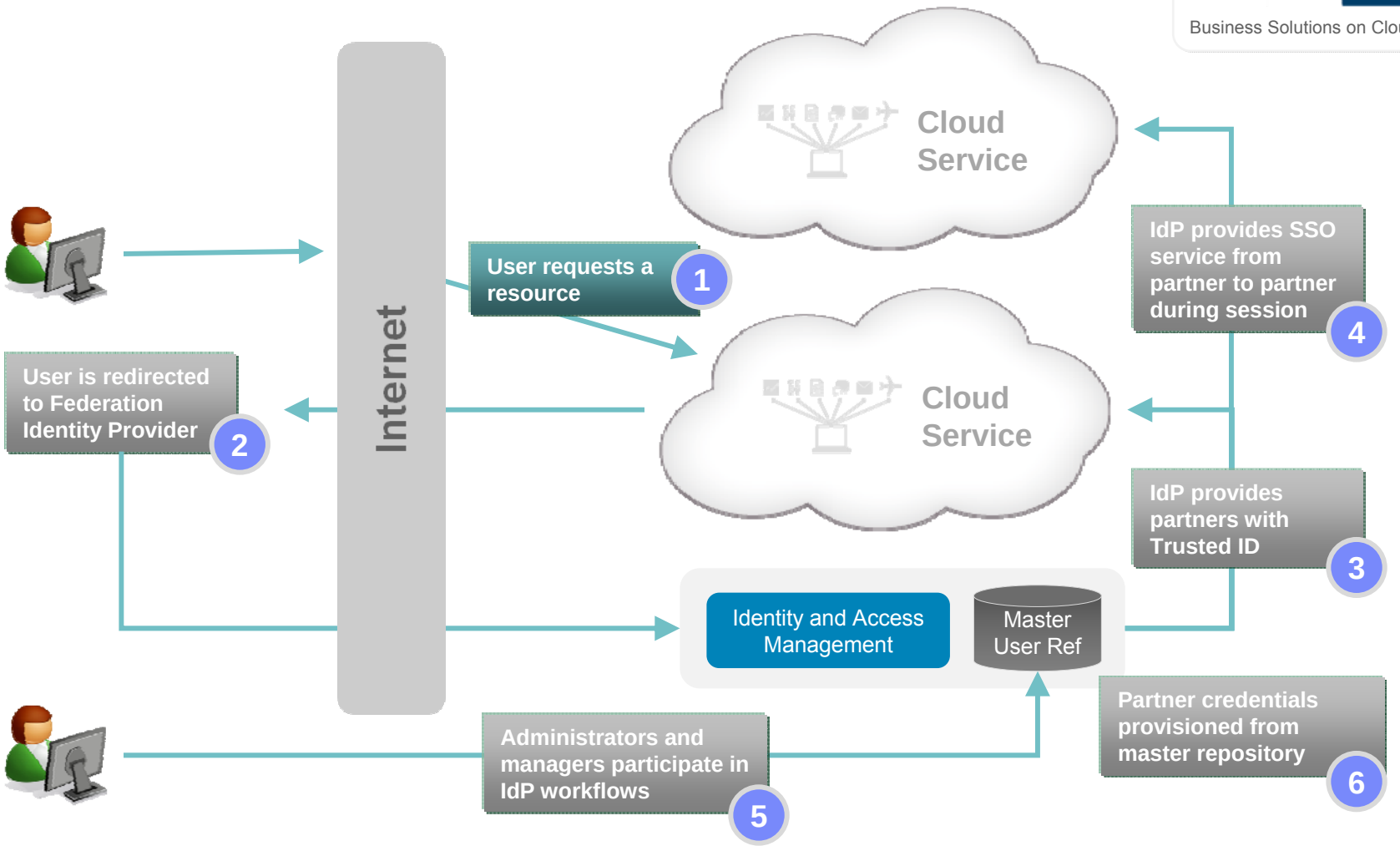
Visibility into the Cloud Infrastructure & Services

- Provide security in a shared tenant environment & security efforts for physical and virtual environments
- Provide tenant-specific visibility to the cloud through activity monitoring and reporting for audit and compliance
- enable eDiscovery, forensic analysis, auditability, and other similar governance requirements.

Security Governance and Standards

- Compliance to information security standards and IT governance frameworks like PCI, ISO/IEC 27001, SSAE16, COBIT, ITIL, BS 7799

Business Solutions on Cloud - simple use case



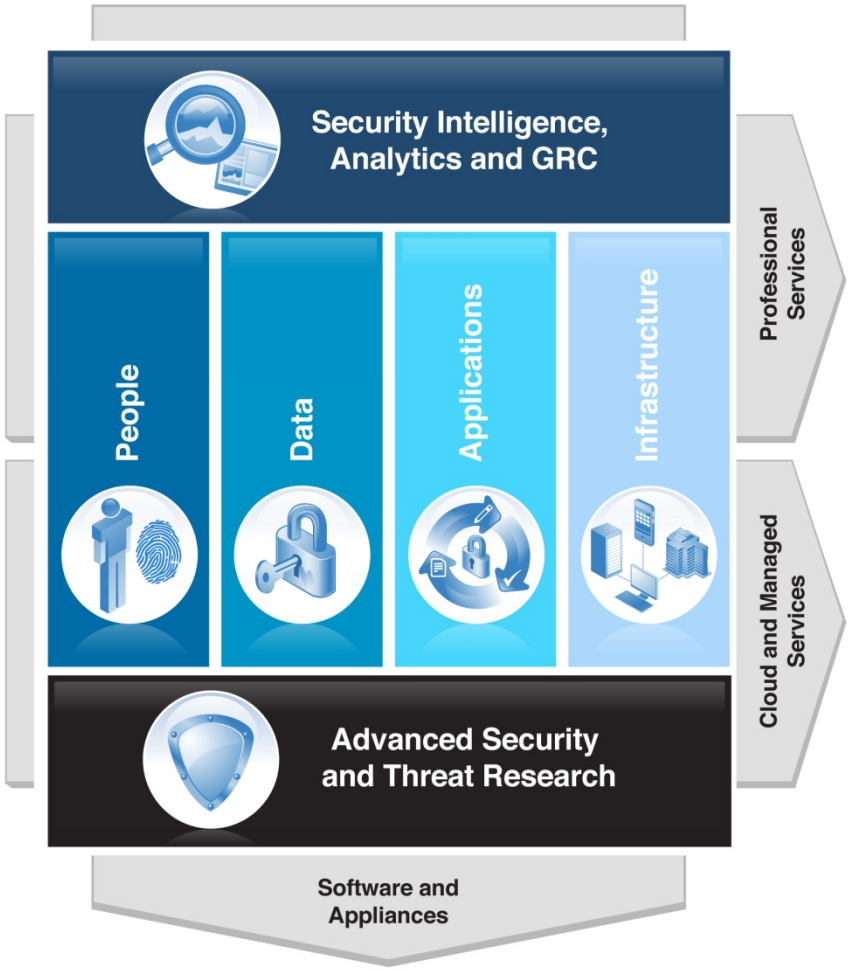
Securing Business Solutions on Cloud – Business Drivers & Use Cases

Key Business Drivers
▪ Enable new Business Model
▪ Increase cost efficiency & operational efficiency and mitigate security risks through automated Security Management.

Use Cases / Key Security Requirements
▪ Strong authentication solution for secure access to the cloud infrastructure
▪ Provide users with a seamless experience of accessing services through single sign-on.
▪ Enable secure means of integrating 3rd party services to the environment through API access.
▪ Enable service adoption through secure isolation of multi tenant data.
▪ Reduce risk & improve availability of services through prior security testing of content hosted on it.
▪ Provide ability to track & enforce in an automated way of who should have/has access to what services.
▪ Provide users with an ability to provide self service for automating business functions such as Password resets, service access etc.

IBM Security Framework &
IBM Cloud Security Foundation Controls

Using the Security Framework we articulate the way we address security in the Cloud in terms of Foundational Controls



Design

Cloud Governance
Cloud specific security governance including directory synchronization and geo locational support

Discover, Categorize, Protect Data & Information Assets
Strong focus on protection of data at rest or in transit

Deploy

Security Governance, Risk Management & Compliance
Security governance including maintaining security policy and audit and compliance measures

Information Systems Acquisition, Development, and Maintenance
Management of application and virtual Machine deployment

Problem & Information Security Incident Management
Management and responding to expected and unexpected events

Secure Infrastructure Against Threats and Vulnerabilities
Management of vulnerabilities and their associated mitigations with strong focus on network and endpoint protection

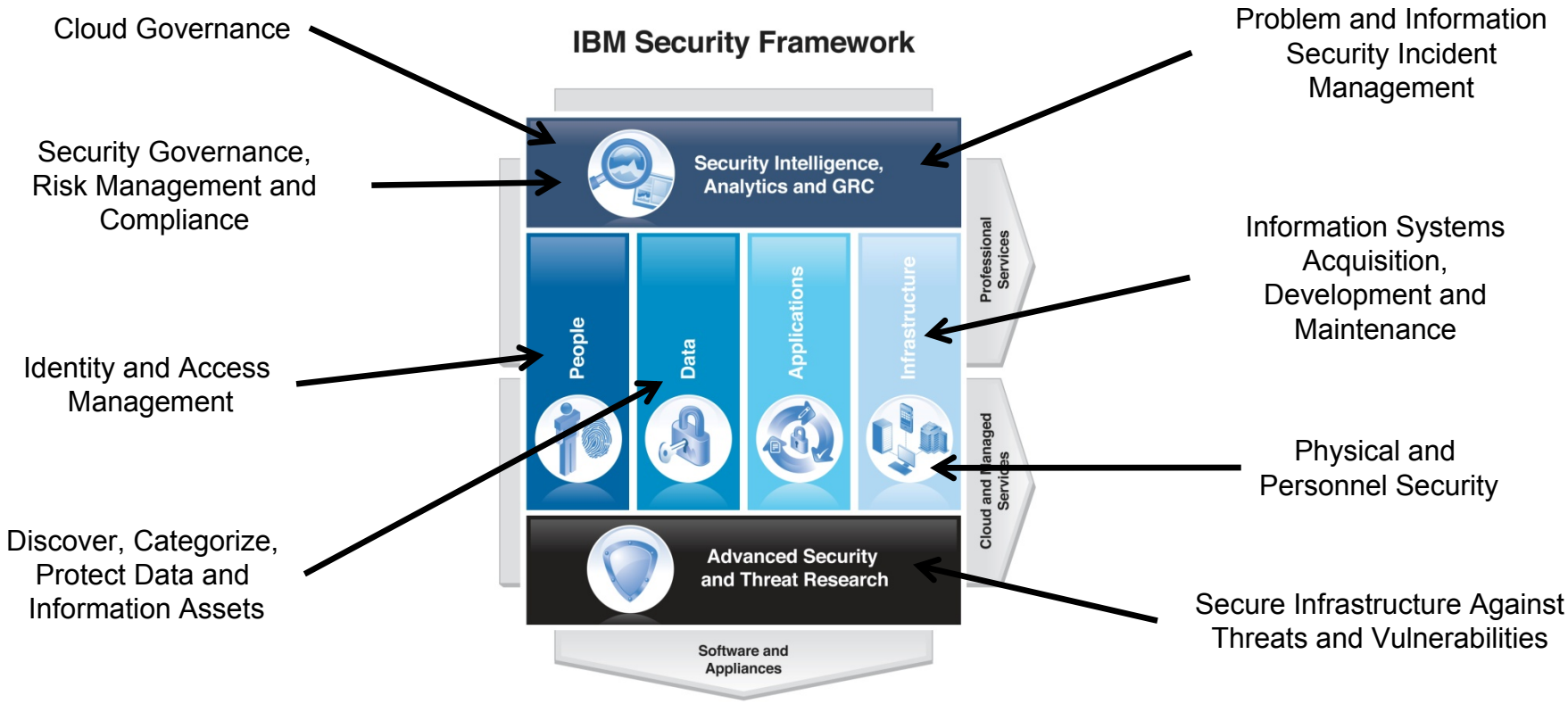
Consume

Identity and Access Management
Strong focus on authentication of users and management of identity

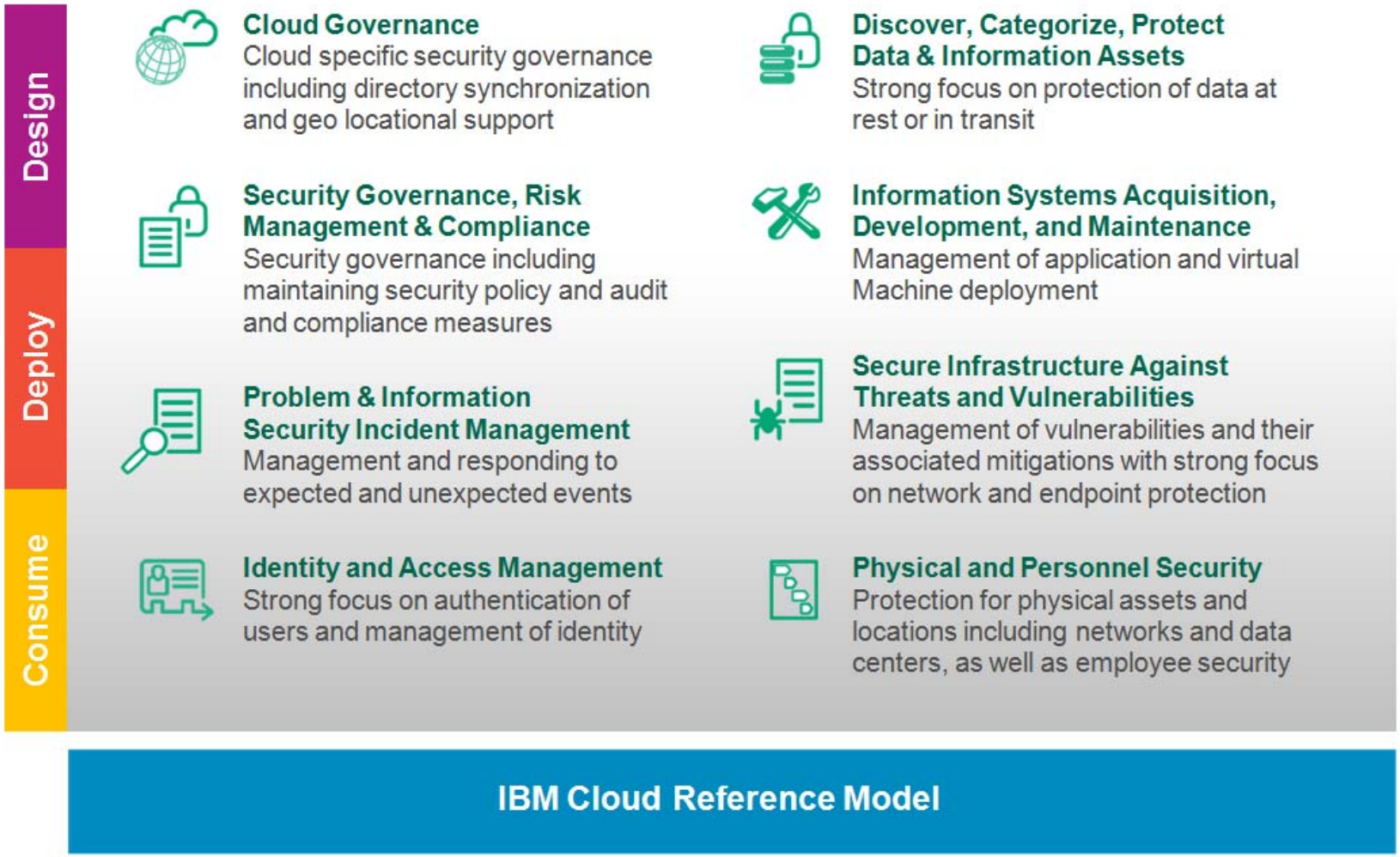
Physical and Personnel Security
Protection for physical assets and locations including networks and data centers, as well as employee security

Cloud Security Foundation Controls and the IBM Security Framework

- Cloud Security Foundation Controls provides the next level of detail within the IBM Security Framework for the Cloud



The IBM Cloud Security Foundation Controls provide a model for categorizing cloud security controls



Foundation Control 1: Cloud Governance

Cloud Governance: Cloud specific security governance including regional and industry support

Controls and IT Processes

•Policies for controlling the movement of tenant workloads between data-centers, countries or geographical regions

•Policies governing access to tenant workloads by third parties such as cloud service support vendors

•Governance of which cloud service providers (private and public) are used and under which conditions, e.g. based on the classification of data in the workload.

Examples

•SmartCloud Enterprise (SCE) and Enterprise+ (SCE+) provide multiple points of delivery globally.

•Customers choose the data center(s) in which to run their workloads. IBM does not move a customer's workloads between data centers.

•SCE+ Cloud ISeC and technical specifications govern security policy above the hypervisor.

•Many customers are making use of public clouds at the line of business level, with the IT Security team lacking visibility.

Foundation Control 2: Security Governance, Risk Management and Compliance

Security Governance, Risk Management & Compliance
including maintaining security policy and audit & compliance

Controls and IT Processes

•Necessary policy controls documented. Control mechanisms identified.
•Appropriate testing of controls. Internal review of operation of the control
•Inspection of the controls by internal and external parties
•Reporting on controls
•Executive and external notification of non-compliance
•Capture and reporting on risk management status
•Auditing cloud service provider and tenant activities
•Providing tenants with visibility of security policies and audit events related to their tenancy, but not those relating to other tenants

Examples

• Demonstration of good security governance through achieving industry certifications such as SSAE16 and ISO 27001, or regulatory regimes such as PCI-DSS.

• SCE has achieved ISO27001 compliance

• In SCE+, all security issues and exceptions are tracked using existing IBM tools.

• In SCE+, security data from sources such as health-check roll-up into existing organizational tooling for reporting and metrics.

Foundation Control 3: Problem and Information Security incident management

Problem & Information Security Incident Management

Management and responding to expected / unexpected events

Controls and IT Processes

- Problems documented and managed according to severity
- Logging maintained on critical systems
- Log retention period and periodic log reviews
- Identification and alerting of incidents
- Processes for response and reporting of incidents

Examples

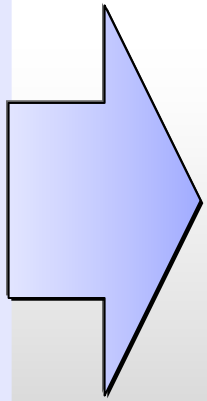
- SCE forwards all logs from critical systems to a central log repository.
- In a private cloud environment integration with existing logging and monitoring infra structure must be evaluated
- A public cloud service provider's security incident management processes need to plan for the potential cybersecurity implications of having unmanaged workloads running on their cloud

Foundation Control 4: Identity and Access Management

Identity and Access Management Strong focus on authentication of users and management of identity

Controls and IT Processes

- Initial identity verification, federated identity management
- Complexity rules, expiration period, password reuse
- User roles defined with access entitlements
- System access granted, periodically reviewed, and revoked based on business need
- Access is logged, accountability maintained
- Identify and resolve separation of duties conflicts
- Strong authentication and encryption of remote administration
- Monitor privileged access



Examples

- An organization consuming public cloud services, e.g. SaaS integrates their on-premise identity system with the SaaS identity system using federated identity management
- SCE leverages ibm.com's Web Identity service for portal authentication.
- Access to a cloud's managing environment (physical) may require strong authentication, e.g. certificate or token.

Foundation Control 5: Data classification and protection

Discover, Categorize, Protect Data & Information Assets

Strong focus on protection of data at rest or in transit

Controls and IT Processes

•Encrypt confidential and business critical data at rest, e.g. at application level or storage system level
•Encrypt confidential and business critical data in motion
•Management and protection for keys and certificates
•Managed backups implemented, encrypted and physically secured
•Inventory, periodic reconciliation, tracking of movement
•Expiration and data destruction; virtual system decommissioning
•Policies and logs regularly reviewed
•Isolation of tenant-specific data at rest from other tenants, e.g. discretionary access control (DAC)
•Policy based control of access to data at rest within a tenant, e.g. allowing sharing or otherwise as required
•Isolation of tenant-specific workloads from other tenants through network isolation
•Protection of tenant data from cloud service provider administrators

Examples

• Data encryption at rest can be achieved from within guest VMs, or through integration with the cloud storage infrastructure

• Private cloud may reduce data protection concerns but doesn't eliminate them. For example, isolating workloads and data from different business units to support conflict of interest or ethical wall objectives.

Foundation Control 6: Systems Acquisition and Maintenance

Information Systems Acquisition, Development, and Maintenance management of application /virtual Machine

Controls and IT Processes

- Documented deployment process
- Change control processes
- Administrative control and limits
- Vulnerability scanning
- Image hibernation and reactivation

Examples

- SCE+ provides a managed process for ensuring the security and compliance of instances after they are provisioned and before they are handed over to the cloud consumer.
- SCE and SCE+ periodically update images to ensure they include recent security patches and updates.

Foundation Control 7: Infrastructure protection

Secure Infrastructure Against Threats and Vulnerabilities

Management of vulnerabilities and their associated mitigations with strong focus on network and endpoint protection

Controls and IT Processes

- Well defined policy defined with required controls
- Encrypt confidential and business critical data
- Intrusion detection/prevention at network, host and hypervisor levels
- Vulnerability detection and remediation

Examples

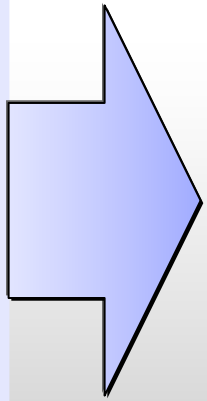
- SCE implements an IPS which checks both for inbound attacks against infrastructure and instances and for outbound attacks to proactively identify compromised instances
- SCE provides an optional VPN / VLAN service for secure access
- SCE/SCE+ managing infrastructure is routinely vulnerability scanned

Foundation Control 8: Physical and Personnel Security

Physical and Personnel Security Protection for physical assets and locations, as well as employee security

Controls and IT Processes

- Access granted, reviewed, and revoked
- Physical barriers, doors alarmed, and alarms tested
- Network cabling and infrastructure secured and caged
- Visitors escorted and logged, logs securely retained
- Personnel security background checks and ongoing monitoring
- Privileged access / reviewing personnel

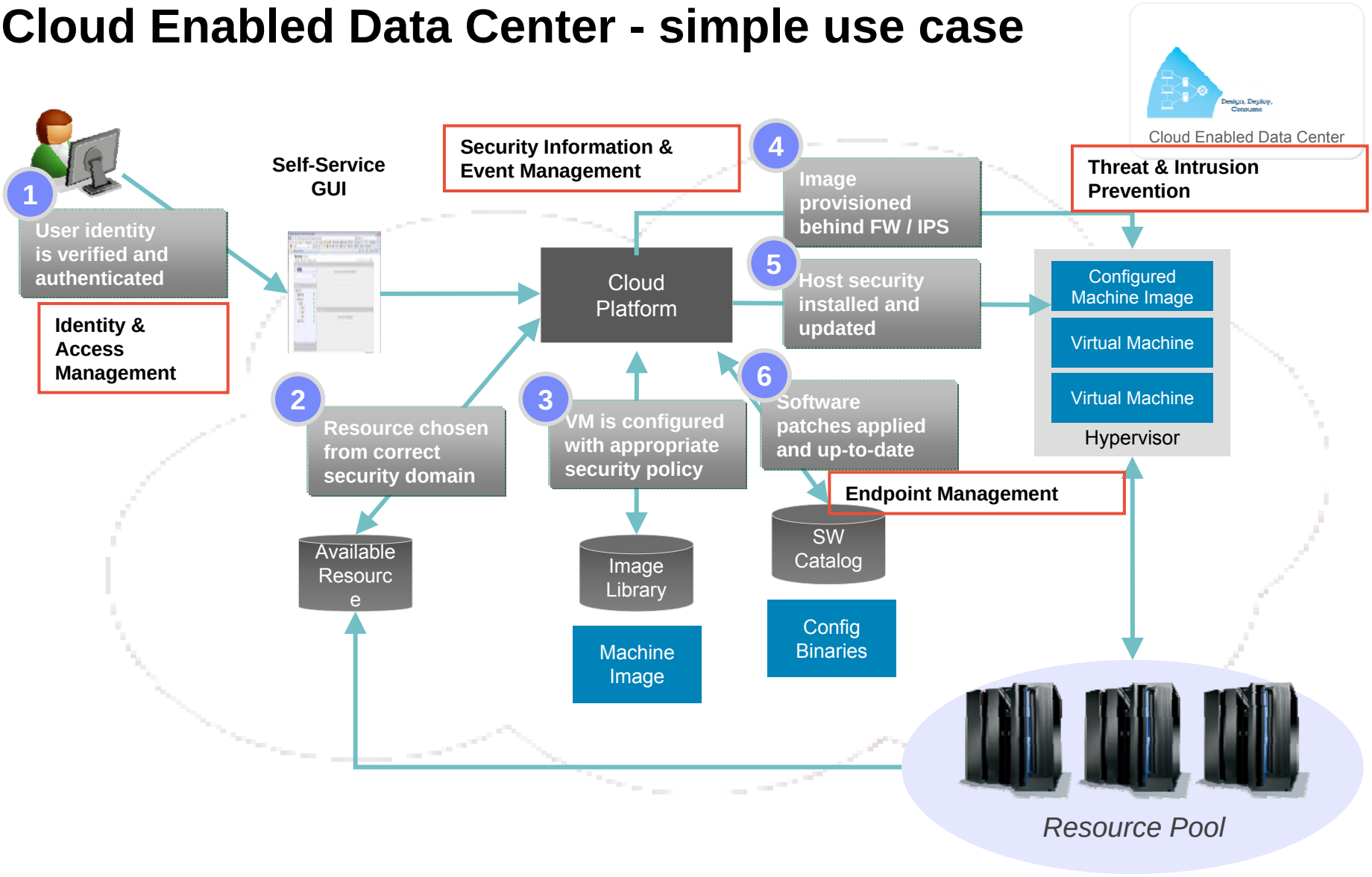


Examples

- SCE and SCE+ leverage IBM's existing rigorous data-center physical security processes
- Private clouds will integrate with a customer's existing procedures in this control category.
- All IBM personnel undergo background checks prior to being hired.
- IBM employees certify against IBM Business Conduct Guidelines on a yearly basis.

Cloud Security Solutions –
Cloud Enabled Data Center (IaaS)

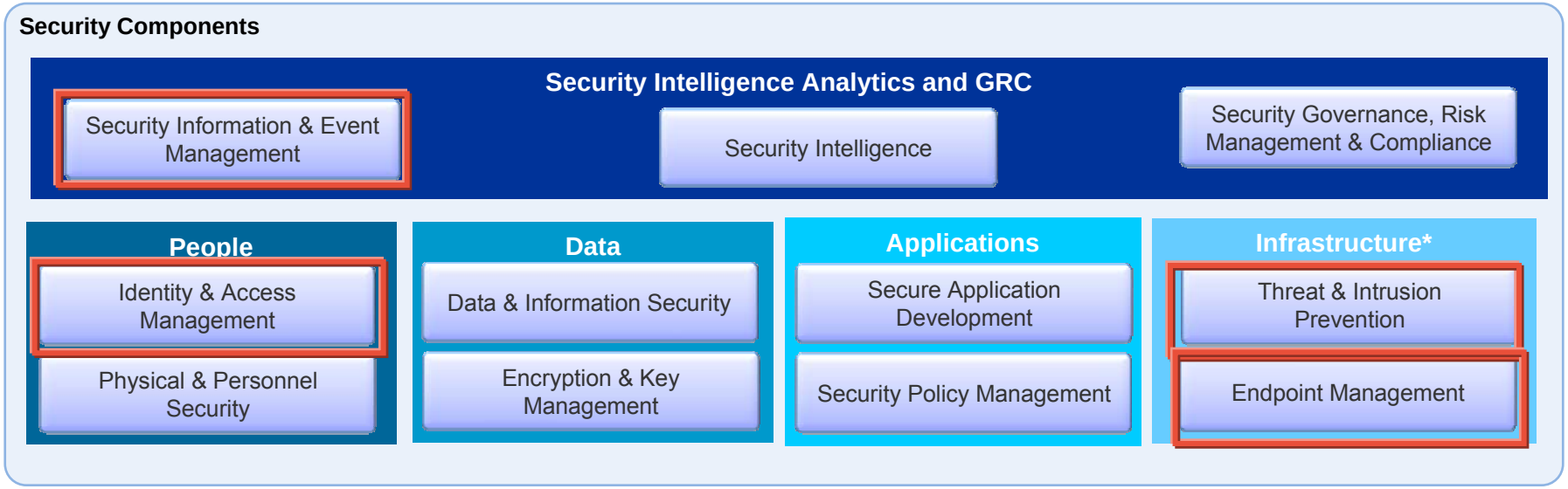
Cloud Enabled Data Center - simple use case



Micro-Pattern 12: Security Management – Use cases description

Micro-Pattern and Use Case Packages	Description
P11: Security Management *Provides* UCP12.1 – Identity and Access Mgmt UC12.2 Protect Virtual Infrastructure UCP12.3– Security info and Event Mgmt UCP12.4 – Automate Security tasks for complex services *Pre-reqs* P0 – Virtualization Management P1 – Monitoring and Events mgmt P5: Self-service automation of Compute Infrastructure P7: Self-service automation of Storage infrastructure P8: Self-service automation of Network P9: Self-Service automation of complex services	**Overview**: Use cases pertaining to securing the different levels of a cloud solution and infrastructure, from the security for the Virtualized infrastructure (e.g. Network, storage, hypervisors, etc..), to the security of VMs contents in a private environment, up to the security of complex services in a public or hybrid envirnments, (3) **Key business driver:** CDC-B5 **Provided use cases:** **CDC-UC12.1 Identity & Access management** ▪ CDC_UC 12.1.1 I want to manage datacenter identities and securely connect users to the cloud (Authentication & Authorization) through a Portal that supports User and Administrator Roles. User identity is verified typically through integration with an existing User Directory infrastructure (AD/LDAP/NIS) ▪ CDC_UC 12.1.2 I want to provide role based access to cloud resources - Image library, Storage ▪ CDC_UC 12.1.3 I want to provision user ids on the VM for access to the VM ▪ CDC_UC 12.1.4 I want to manage Confidentiality & integrity of storage, images and meta-data associated with master image. **CDC-UC12.2 Protect Virtual Infrastructure** •CDC_UC 12.2.1 I want to manage endpoints to secure and protect the virtual infrastructure (VM instances, hypervisors) as per IT Security Policy. •CDC_UC 12.2.2 I want to manage endpoints to ensure they are patched and kept up-to-date to meet compliance •CDC_UC 12.2.3 I want to provide protection, threat and vulnerability management for every layer of the virtual infrastructure **CDC-UC12.3 Security Information and Event management** •CDC-UC12.3.1 I want to maintain audit logs for virtual infrastructure and audit readiness/compliance reporting on User Activity •CDC-UC12.3.2 Provide visibility into virtual Infrastructure - **CDC-UC 12.4 Automate Security tasks for complex services** CDC-UC12.4.1 I want to automation to integrate with existing capabilities for identity and access management, end point management and log management and visibility into the cloud infrastructure that includes a. Provisioning of VM into a specific network/subnet as per the Security policy and behind FW / IPS rules. b. Provisioning of user ids on the VM for access to the VM c. Configuring the VM with appropriate security policy that implements specific OS resource settings and keeps the patched and kept up-to-date as per the security policy. d. Maintaining audit logs for virtual infrastructure compliance and audit readiness e. Provide visibility & monitoring for the virtual environment.

Security Component Model – Cloud Enabled Data Center

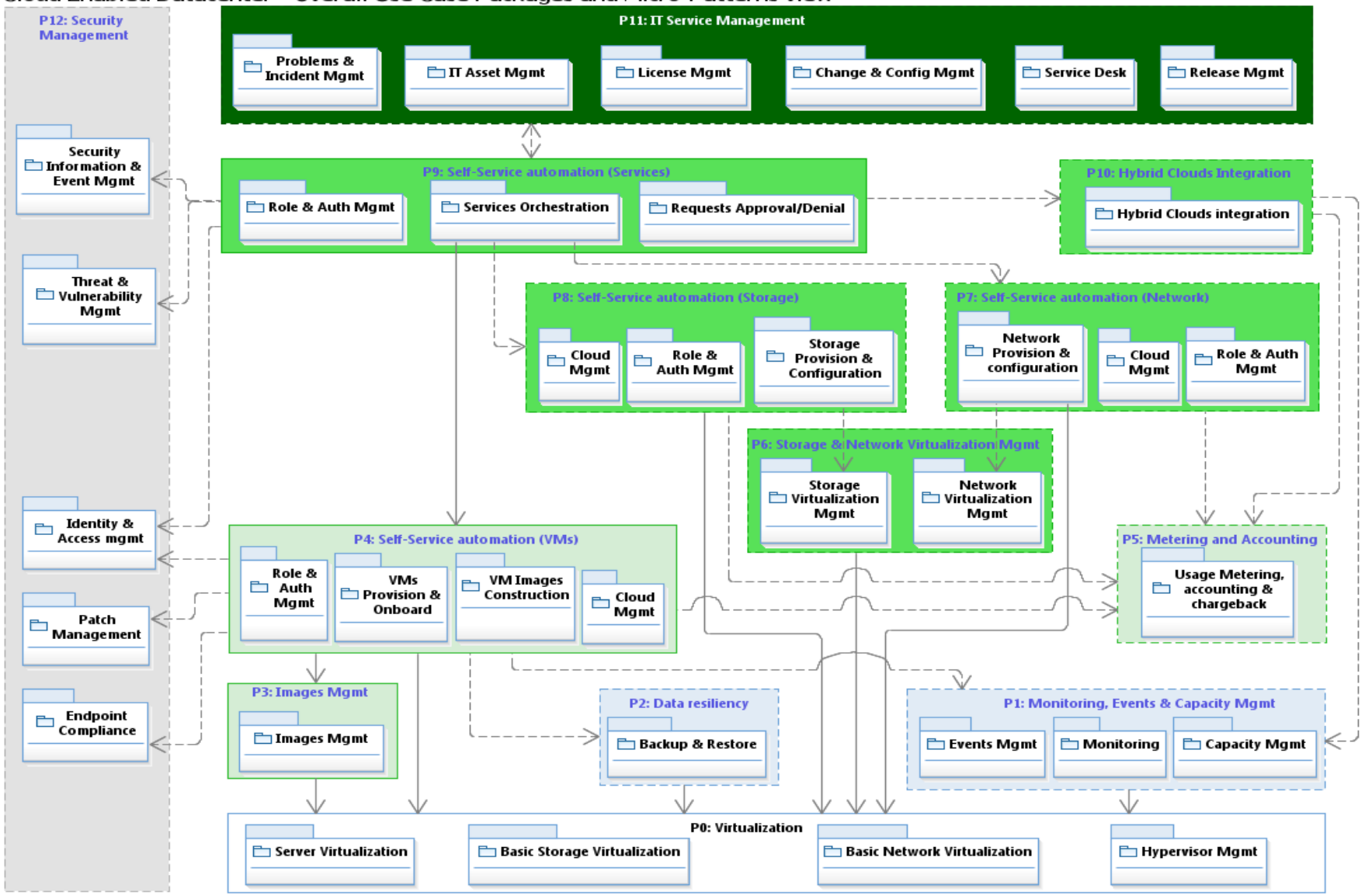


*Infrastructure Includes – Server, Network, Storage

These components are focus of present iteration of CCRA 3.x of Cloud Enabled Data Center Security pattern.

Legend:
→ "Use" relation
--→ "Optional use" relation

Cloud Enabled Datacenter - Overall Use Case Packages and Micro-Patterns view



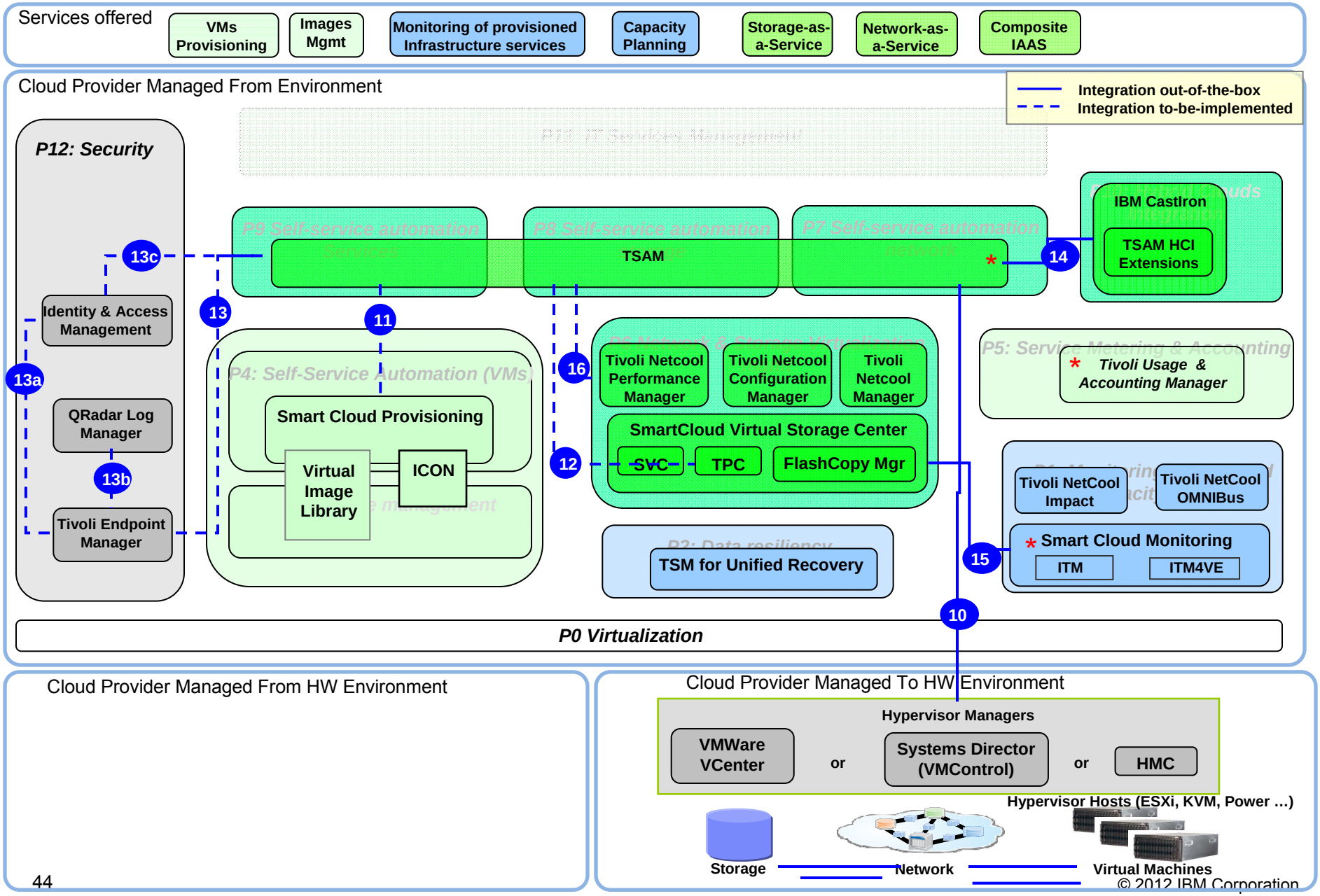
Security Architecture – Component Realization Guidance

Recommended Product	Capability Description	Selection Guidance
Identity & Access Management		
IBM Tivoli Identity Manager	Manages Identity Life Cycle & Provide Self service at Consumer/Provider	Recommended to have the master identities in TIM and replicated with the cloud platform (ISDM/TSAM)
IBM Tivoli Access Manager For e-Business	Reverse Proxy / Point of contact component to authenticate/authorize inbound web requests at Provider	To meet the requirement for single sign on to all cloud management tool console for the data centre management team and end users. Consider IBM Security Access Manager for Enterprise Single Sign-On if there are other third party non-web apps to provide SSO.
End Point Management		
IBM Tivoli Endpoint Manager for SC	Provides Patch management, Security configuration management	
Security Information and Event Management		
IBM Security QRadar SIEM	Provides extensive visibility and actionable insight to help protect networks and IT assets from a wide range of advanced threats. It helps detect and remediate breaches faster, address compliance, and improve the efficiency of security operations.	If only Log management use IBM Security QRadar Log management. SIEM provides advanced capabilities that includes integrated log management as well as detection of advanced threats and offenses.
Threat and Intrusion Prevention		
IBM Security Virtual Server Protection	Protects critical virtualized assets /virtual machines	Currently available only for VMWare hypervisors.
IBM Security Network Intrusion Prevention	Protects the network infrastructure from a wide range of attacks	SiteProtector recommended to provide centralized management of security intrusion prevention and single management point to control security policy

Note: Some IBM Security products are in the process of getting rebranded with IBM Security as the prefix. For instance IBM Tivoli Identity Manager may be referred as IBM Security Identity Manager in documents / websites.

Macro Pattern 2: Advanced IaaS Services (VMs, Storage, Network or their combinations) - AOD

Design Solution



(*) Included in ISDM

Cloud Security Solutions – Platform as a Service (PaaS)

Security Hardening of PaaS for Public Cloud

- Public cloud hosted service instances and application workload instances need to have their security hardened for public cloud use
  - Though security is very important for private cloud as well, public cloud security requirements are much more stringent
  - Public cloud instances are exposed to the internet and raise concerns of break-ins, denial of service attacks and privacy compromises
- The following are some examples of the security hardening requirements for public hosted multi-tenant services
  - No sharing of a service instance VM or an application workload instance VM between customers
  - SSH keys stored in the VMs are encrypted, and encryption keys are stored in a vault
  - Enforce use of strong passwords
  - Differentiate security policy between different types of customers
    - ✓For some customers, open SSH access to service instance VMs to enable implementation of their corporate security policies
    - ✓For other customers, lock SSH access to service instance VMs to provide a virtual appliance view of the service and to protect the internal metering & billing and IP artifacts

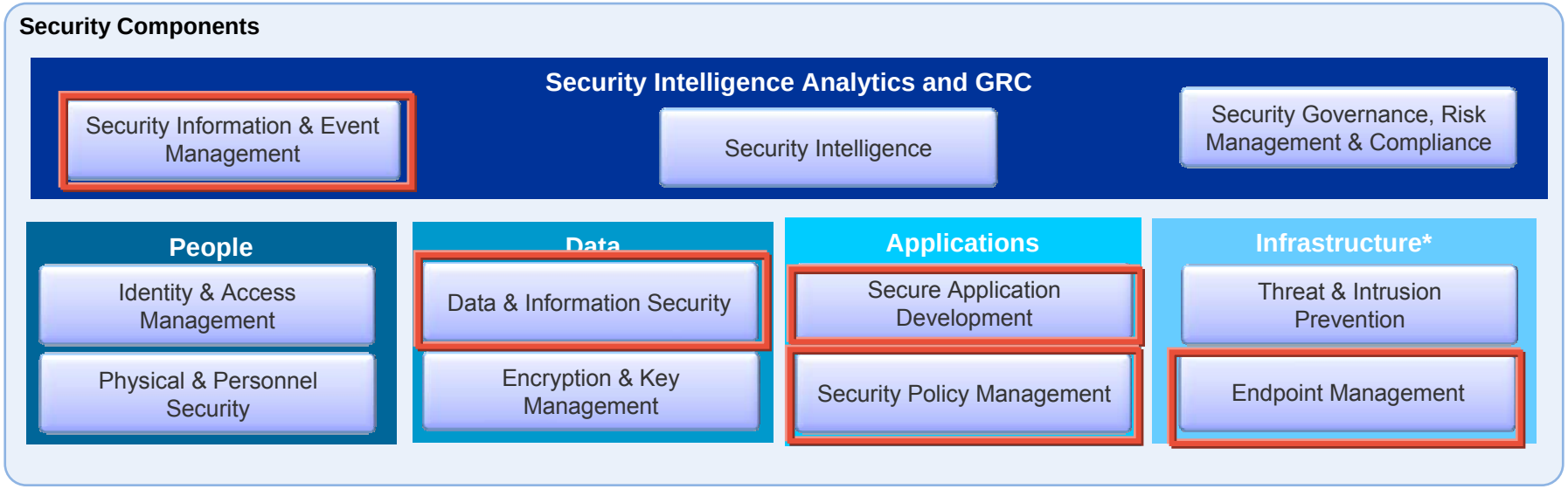
Patch Mgmt for PaaS Images and Virtual Machines

- There needs to be clearly defined and documented patch management policies to update the service instances and application workload instances with security patches and product updates
  - Consider these separately for managed services and unmanaged services

- Patch Management for Managed Services
  - Patch mgmt for images
    - ✓Update images in the public catalog on a regular basis with the latest security patches and product updates
    - ✓VMs created using a catalog image gets the patches & updates included in the most recent image update
  - Patch mgmt for VMs
    - ✓Since a VM is deployed from an image, newer security patches may have arrived and the VM may be out-of-sync
    - ✓Security rules may require strict adherence to patching schedules (e.g., apply critical patches within 3 days)

- Patch Management for Unmanaged Services
  - Patch mgmt for images
    - ✓It may be acceptable to just include the latest security patches and product updates with images produced for release refresh – with no further image patching outside of release refresh
    - ✓May require release refreshes to be fairly frequent (e.g., once every 4-6 weeks)
  - Patch mgmt for VMs
    - ✓Either no patching or at best manual patching for already deployed VMs
    - ✓It is desirable to provide an “update” facility that can update or replace an existing VM with code from latest image refresh so that the VM becomes current with all security patches that the image already has (this is better than no patching or manual patching)

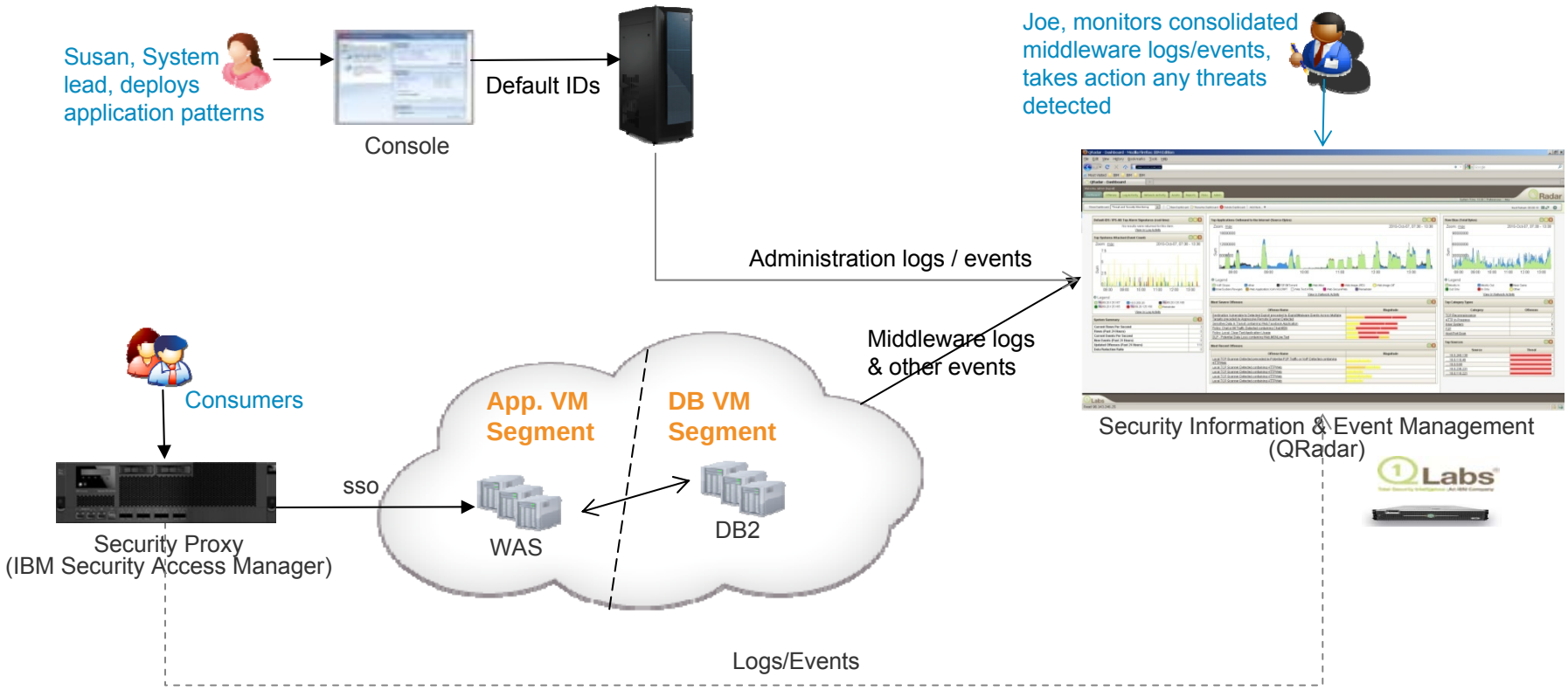
Security Component Model – Platform as a Service



*Infrastructure Includes – Server, Network, Storage

Focus Components

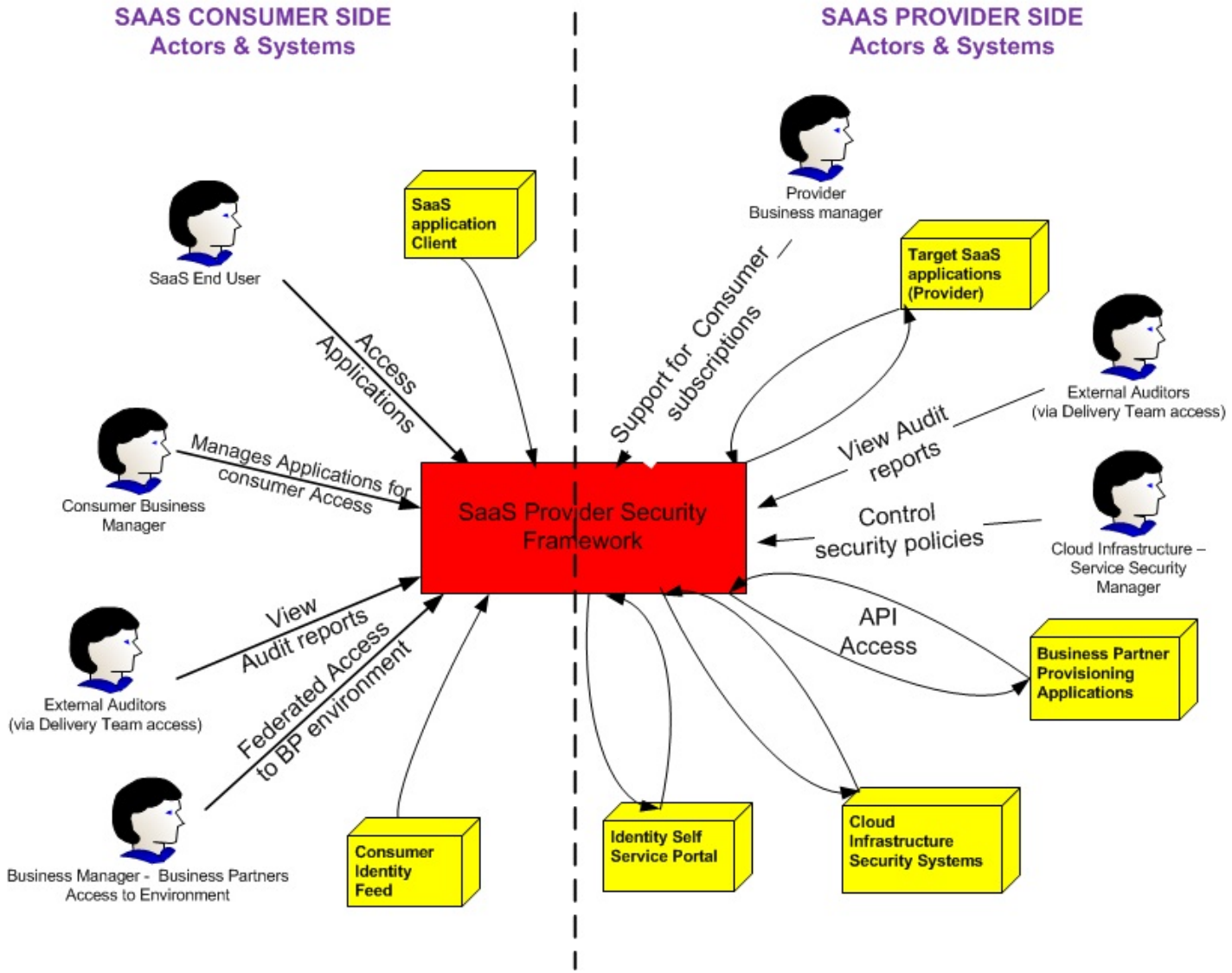
Scenario: Threat Detection in Virtual Application & System



- Centralized security log management and correlation
- Detect external threats e.g. SQL Injection, Brute force attacks, Login attempts, etc.
- Detect internal threats

Cloud Security Solutions – Software as a Service (SaaS)

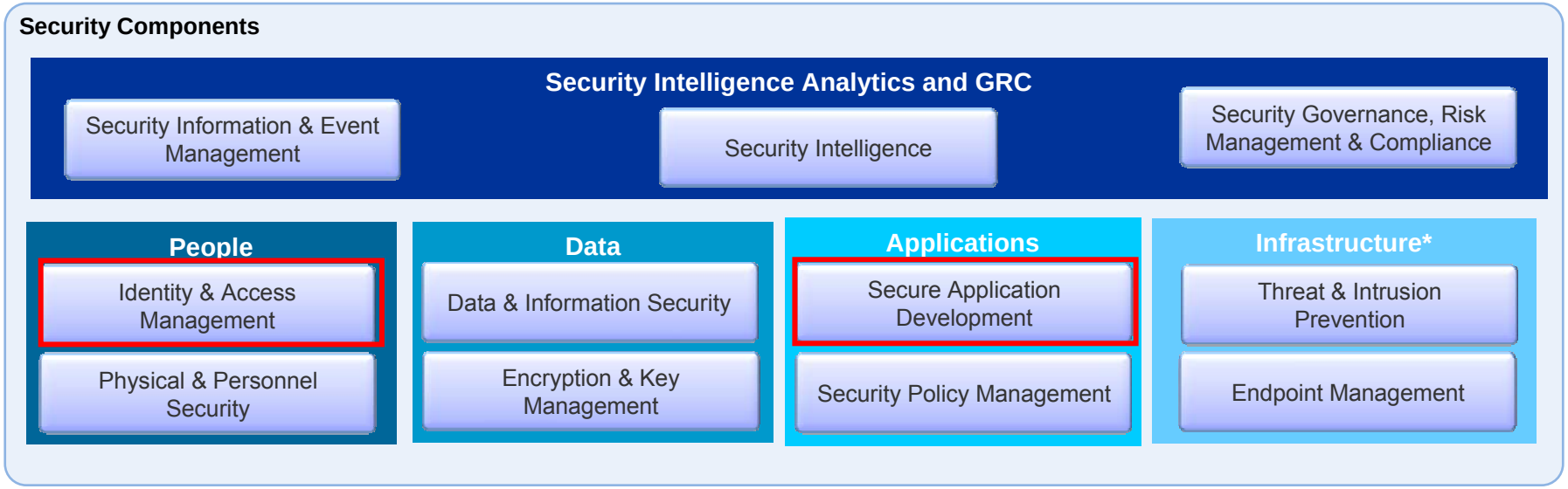
Business Solutions on Cloud - Security Management System Context



Business Solutions on Cloud - Security System Context Description

Cloud Boundary	Actor / System	Name	Description
Consumer	Actor	End User	Accesses the SaaS applications through the client
Consumer	Actor	Business Manager	Manages subscriptions for which users should have access to what applications
Consumer	Actor	External Auditors	Validate Consumer Infrastructure & processes for Security compliance.
Consumer	Actor	Business Manager – BP for SaaS Applications	Specify what consumer applications BP need integration with & federated access to.
Consumer	System	SaaS Application Client	Browser or application client to access the servers / Target SaaS applications on Provider
Consumer	System	Consumer Identity Feed	Provides list of identities to control access to external Saas provider applications as per consumer Identity Life cycle (new user/access, suspend, terminated user)
Provider	Actor	Business Manager	Provider side support to manage subscriptions for which users should have access to what applications
Provider	Actor	External Auditor	Validate Provider Infrastructure & processes for Security compliance.
Provider	Actor	Cloud – Security Service Manager	Manages Security operations of SaaS applications on Provider Cloud
Provider	System	Target SaaS applications	Applications from Provider that render the service to the consumers.
Provider	System	Partner Provisioning Applications	System to invoke provisioning mechanisms (through API) from Provider for 3rd Party access to SaaS applications potentially using standards such as OAuth.
Provider	System	Cloud Infrastructure Security Systems	Provides Security capabilities to provider environment. Can be either developed in house or outsourced through a Managed Security Services Provider (MSSP). Includes Vulnerability scanning
Provider	System	Identity Self Service Portal	Allows consumer / end users to perform self service of identity requests (password change/reset, request account access etc) for applications on Provider

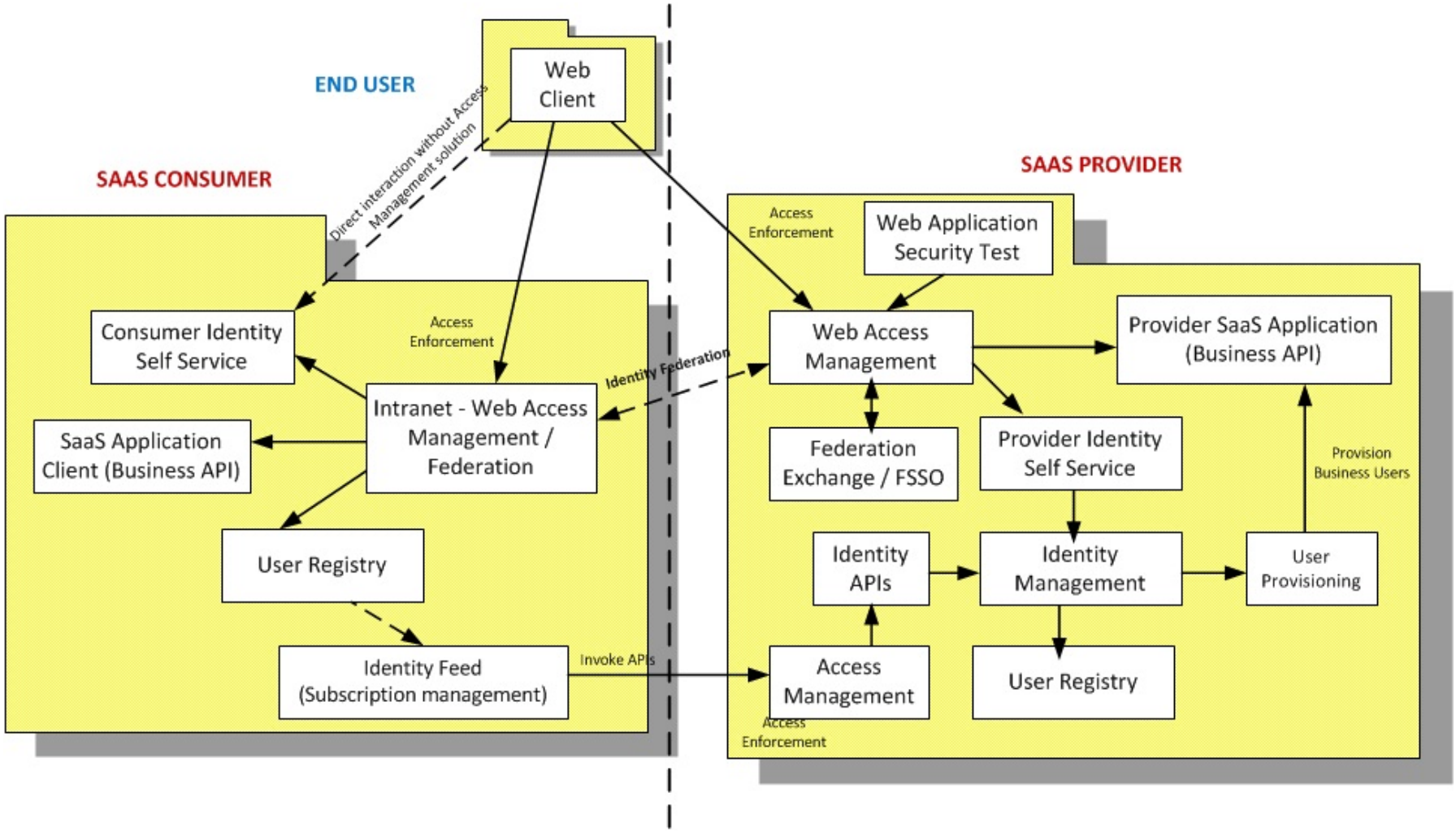
Security Component Model – Business Solution on Cloud



*Infrastructure Includes – Server, Network, Storage

These components are focus of present iteration of CCRA 3.x of Business Solution on Cloud

Business Solution on Cloud - Security Component Model

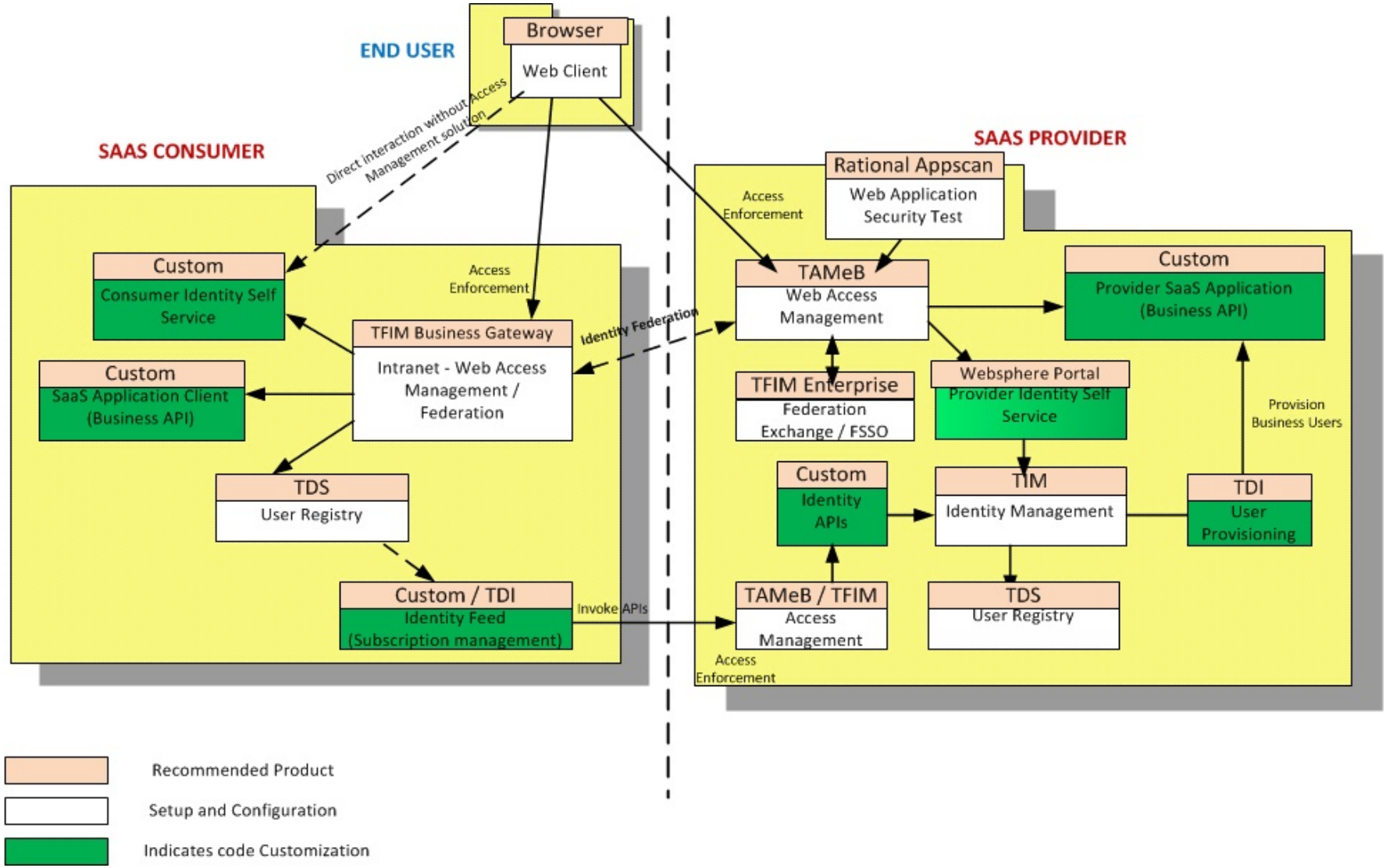


Security Architecture – Product Mappings

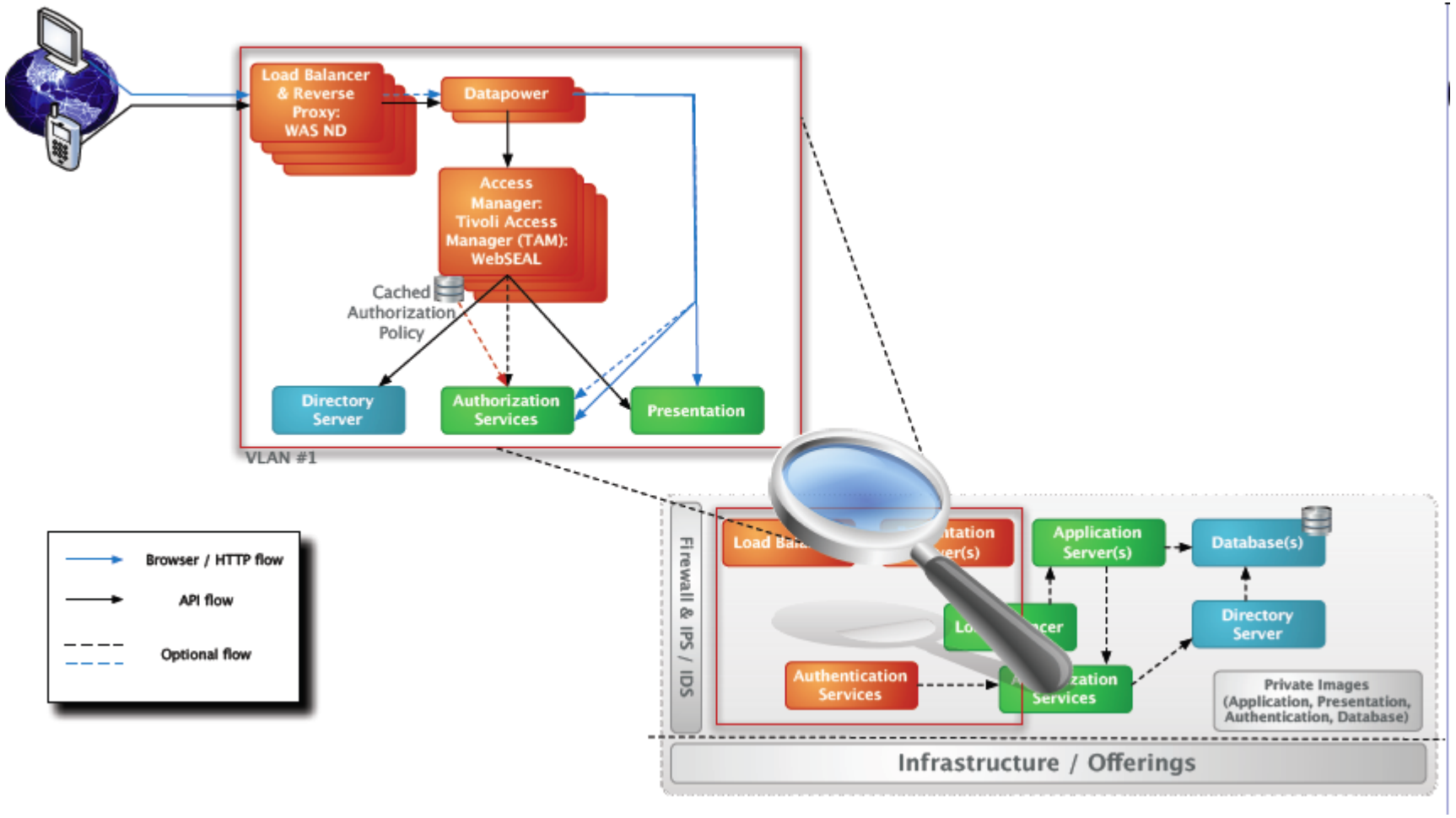
Recommended Product	Product Description	Selection Guidance
Identity & Access Management		
IBM Tivoli Directory Server	Helps Provider store User credentials in a registry with LDAP Protocol.	Recommended Identity Storage Platform for Provider. For small provider deployments (say <1K users), open Ldap as a registry could be an option.
IBM Tivoli Directory Integrator	Helps synchronize consumer id / passwords	As needed within Consumer / Provider environments.
IBM Tivoli Identity Manager	Manages Identity Life Cycle & Provide Self service at Consumer/Provider	Recommended in all deployments at Provider side. Consumer side optional
IBM Tivoli Access Manager For E-Business (TAMeB)	Reverse Proxy / Point of contact component to authenticate/authorize inbound web requests at Provider	Recommended in all deployments at Provider side.
IBM Tivoli Federated Identity Manager Enterprise (TFIM)	Web services Federated Sign On with multiple FSSO protocols support, point of contact to establish Federation. TFIM Enterprise Includes TAMeB and TDS in its bundle.	Recommended in all large deployments at Provider side. TFIM Primary role for SaaS adoption is FSSO. TFIM User selfcare may also be a consideration for provider side user management.
IBM Tivoli Federated Identity Manager Business Gateway (TFIM BG)	Web services Federated Sign On with FSSO protocol support, point of contact to establish Federation. TFIM Business Gateway does not include TAMeB/TDS in the bundle.	More suitable for consumer side. Especially Consumers that do not already have a viable federation mechanism.
IBM WebSphere Portal	Enriched User interface for Self care for Business transactions such as Reset Password, Request access etc.	TIM Self Service or TFIM User self care may not provide sufficiently customizable Self service UIs in a multi tenant environment. As a result a Presentation component such as Portal may be desirable. It is recommended to use TDS as registry for Portal.
Secure Application Development		
IBM Rational AppScan	Product to find application level vulnerabilities in Provider through black box or white box testing	1. Rational Appscan Standard for Black box testing, 2. Rational Appscan Source for White Box testing 3. Rational Appscan Enterprise for both black-box and white-box testing and web collaboration features for security testing.
IBM Application Security Assessment Services	GTS Services provides targeted code review and Vulnerability Assessment using tools such as Appscan, Nessus etc.	Use Application Security Assessment services for analyzing Provider applications as an opex model

Note: Some IBM Security products are in the process of getting rebranded with IBM Security as the prefix. For instance IBM Tivoli Identity Manager may be referred as IBM Security Identity Manager in documents / websites.

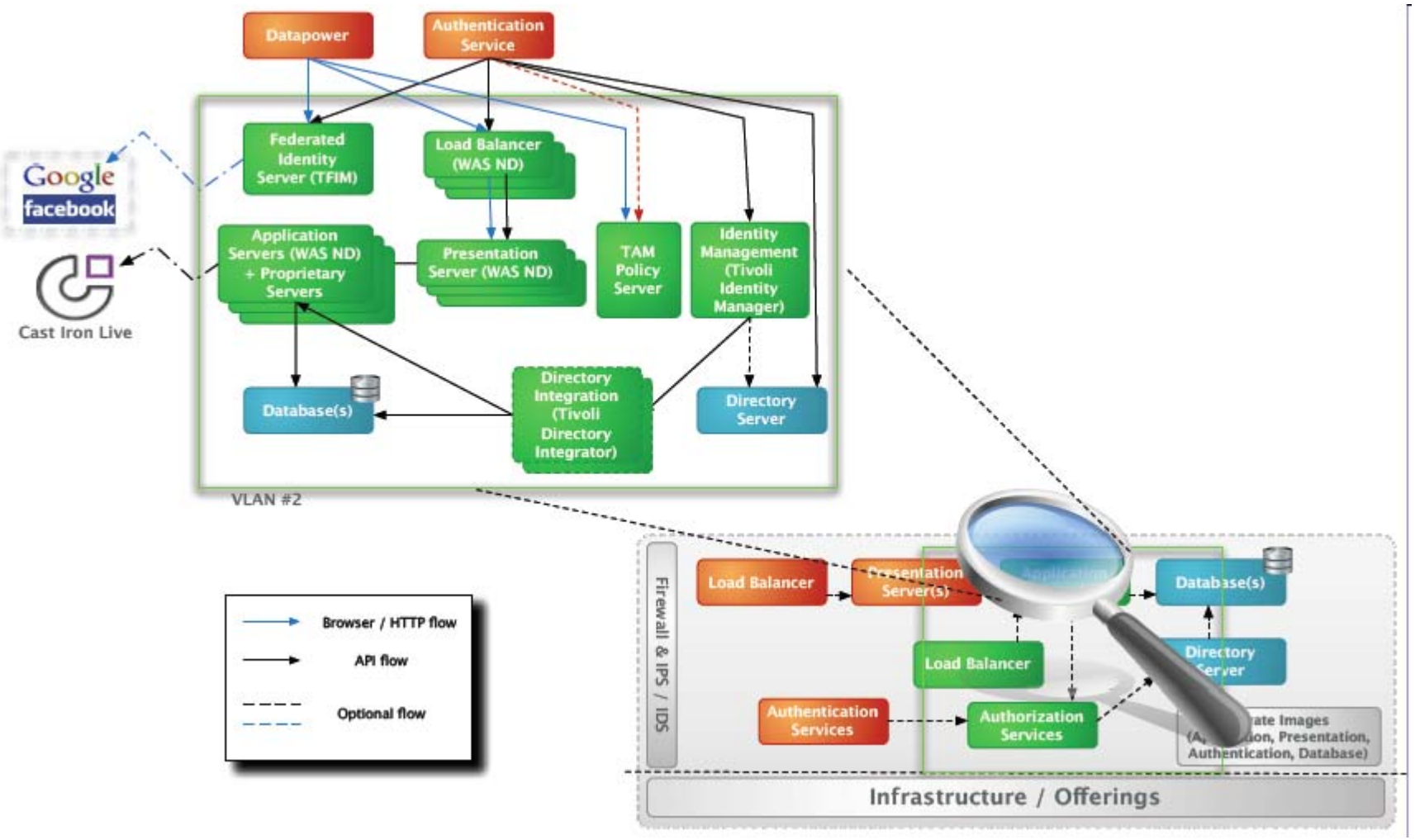
Security Component Realization – Operational Model



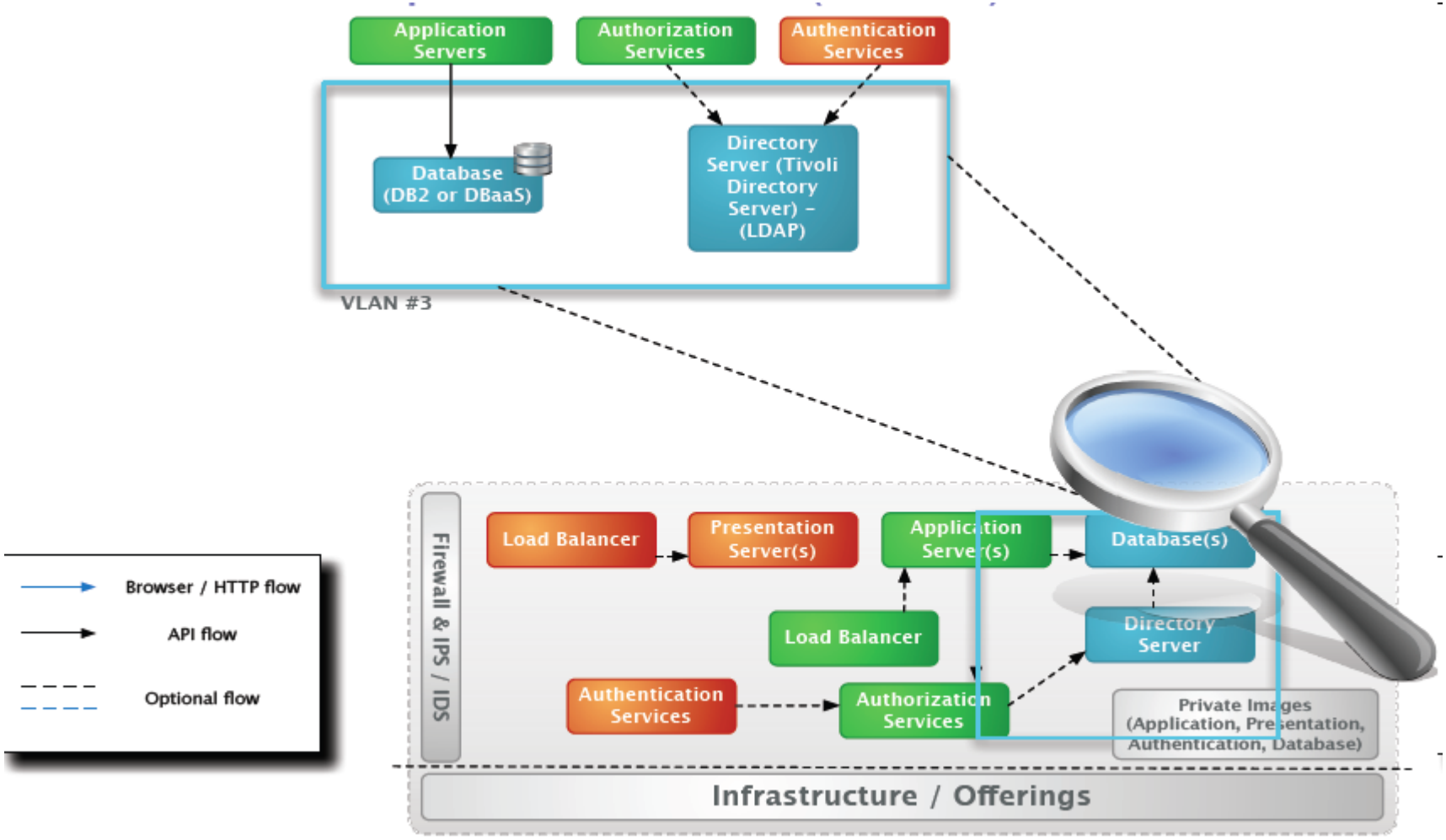
Architecture – Operational Model (Zone 1)



Architecture – Operational Model (Zone 2)



Architecture – Operational Model (Zone 3)



Cloud Security Solutions – Cloud Service Provider (CSP)

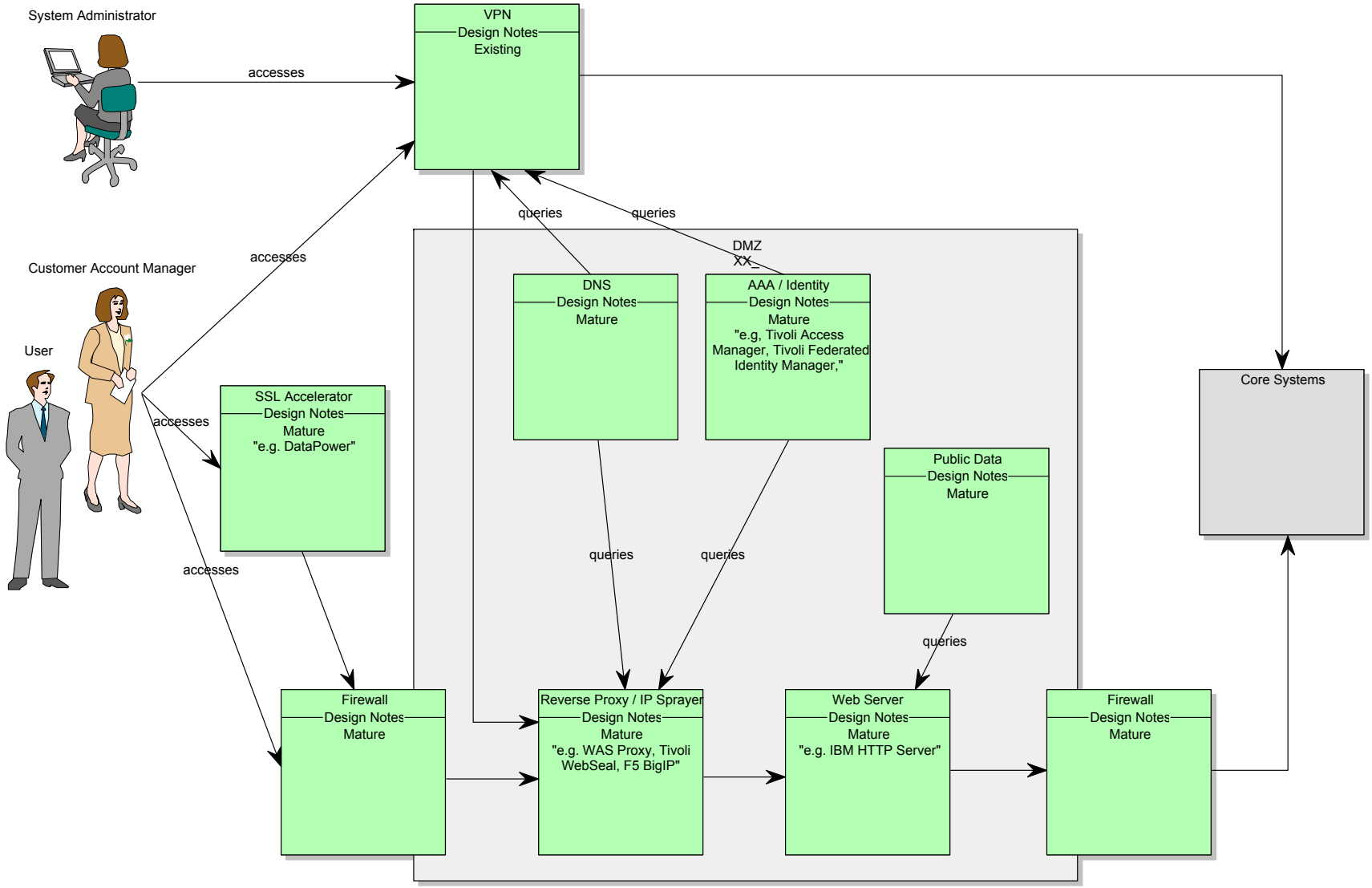
Access Domain

Pattern and Use Case Packages	Description
Access Domain	Install and configure access, presentation and service interface elements. Install Access Elements (Network security and routing elements) Configure Access Elements Install Presentation Elements (Elements that support visual interfaces provided by components, e.g. Web server, Web Portal) Configure Presentation Elements Install Service Interface Elements (Elements that support non-visual interface, e.g. Web Services endpoint server) Configure Service Interface Elements

Cloud Service Provider Non-Functional Requirements

Category	Description
Performance	Response time for administrative actions VM instance creation time VM instances created per hour Service Level Agreement measurement capability
Usability	Multi-lingual user interface User accessibility User Experience for Non-Administrators Interoperability – HTTP based interfaces Flexibility to support different types of workloads
Capacity	Capacity based on number of concurrent users Capacity based on number of concurrent VM instances Dynamic service scaling
Security	Network edge security compliance Interior Cloud security compliance
Availability	Redundancy within site Transparent failover and recovery to Consumer

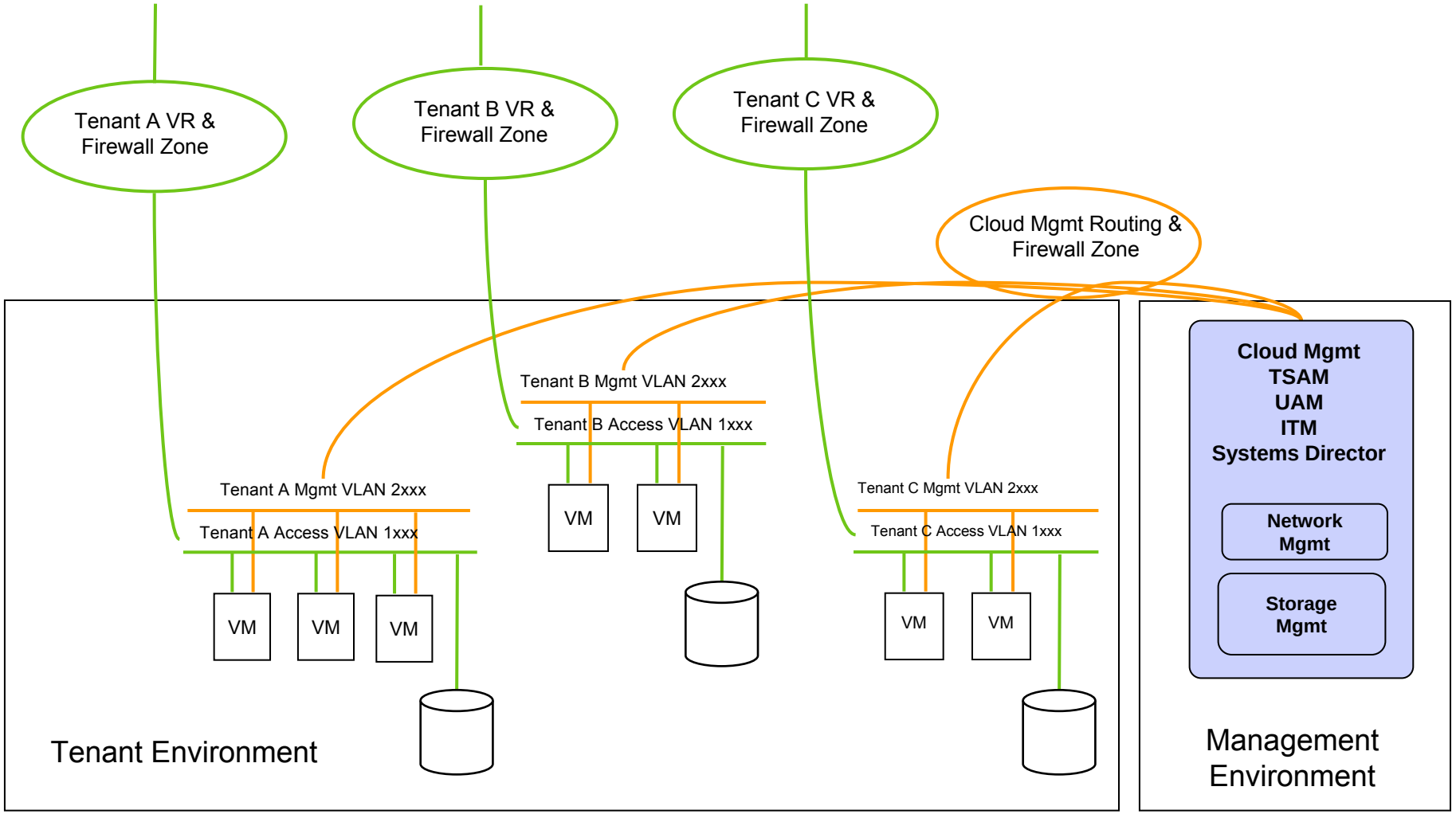
Access Domain



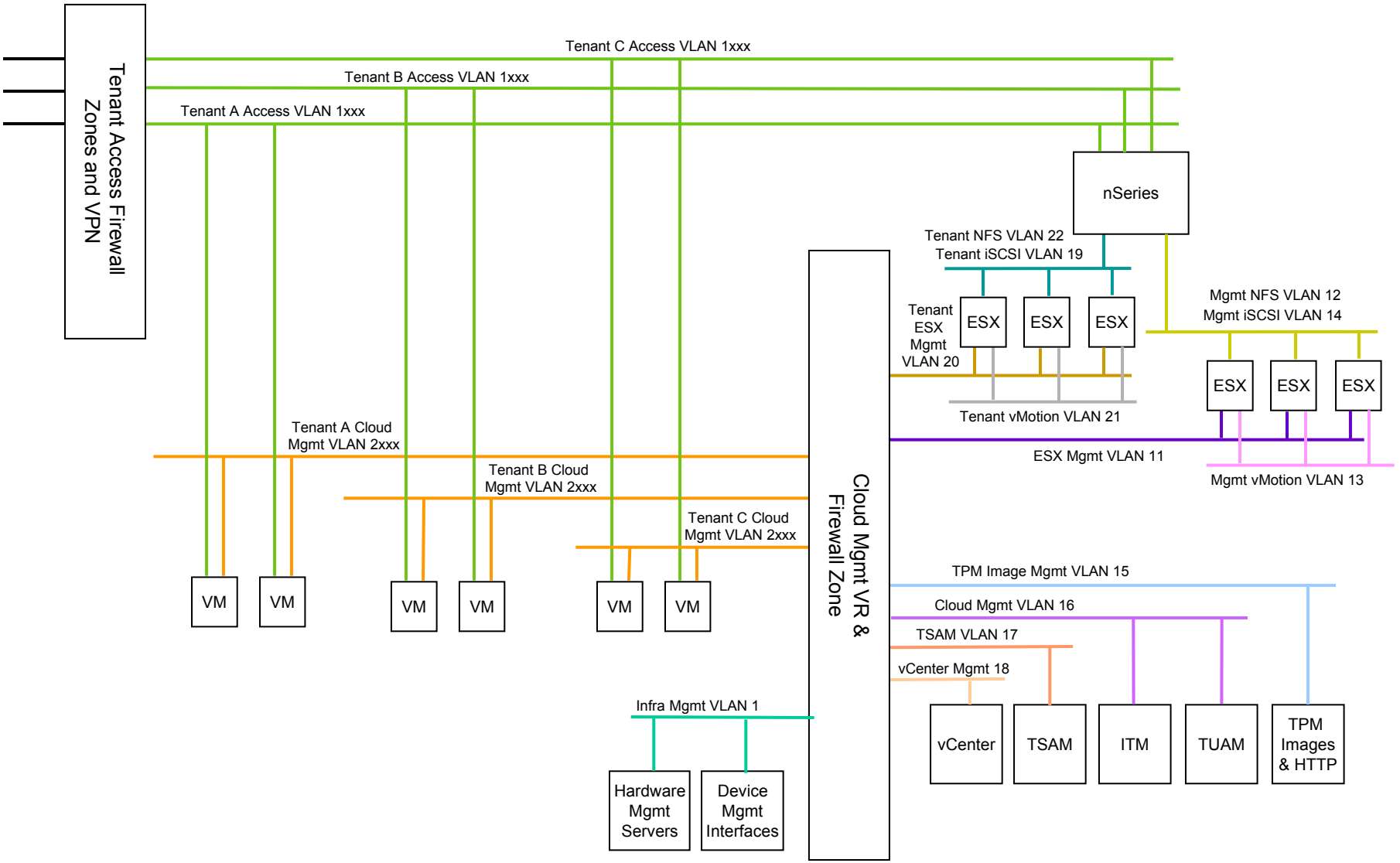
Security design

- LDAP based Authentication
  - Support for Support for LDAP solutions from IBM and other vendors, including Microsoft Active Directory
- Role Based Access Controls
  - Administrator Actors/Roles to segregate Customer and Cloud Administration
- Multi Customer Environment
  - Segregate the data by customer, so that each customer can only see data they are allowed to see
    - Teams, Users, Projects, Software, Images etc.
    - Segregation happens securely on the server side
  - Segregate virtual servers so that customers can only access their own systems
- Network Configuration
  - VLAN/Subnet management for customers/projects
    - Multiple subnets per customer (enabled by Cloud Administrator from loaded list of all VLANs)
    - Customer can select subnets (from list of subnets for that customer) for their own projects via Self-Service UI
  - Firewall configuration management
    - Customers can manage the firewall configuration for access to their subnets
    - VPN gateways to provide tenant specific access

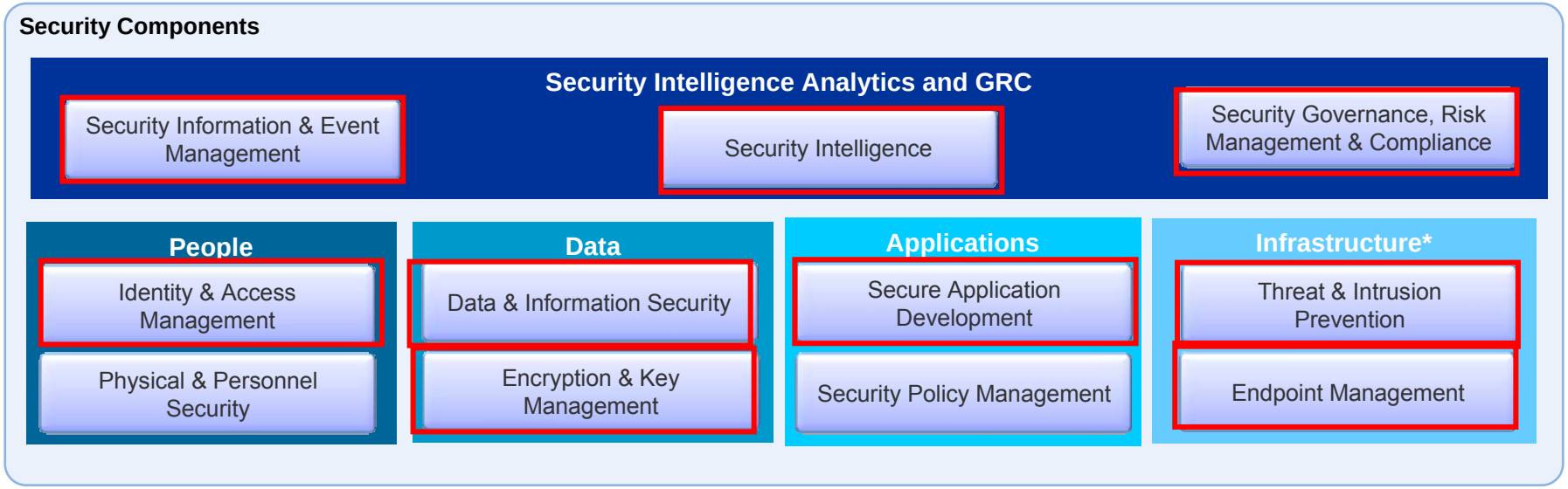
Secure tenant separation using VLANs and Virtual Routing



Logical VLAN network design for tenant separation



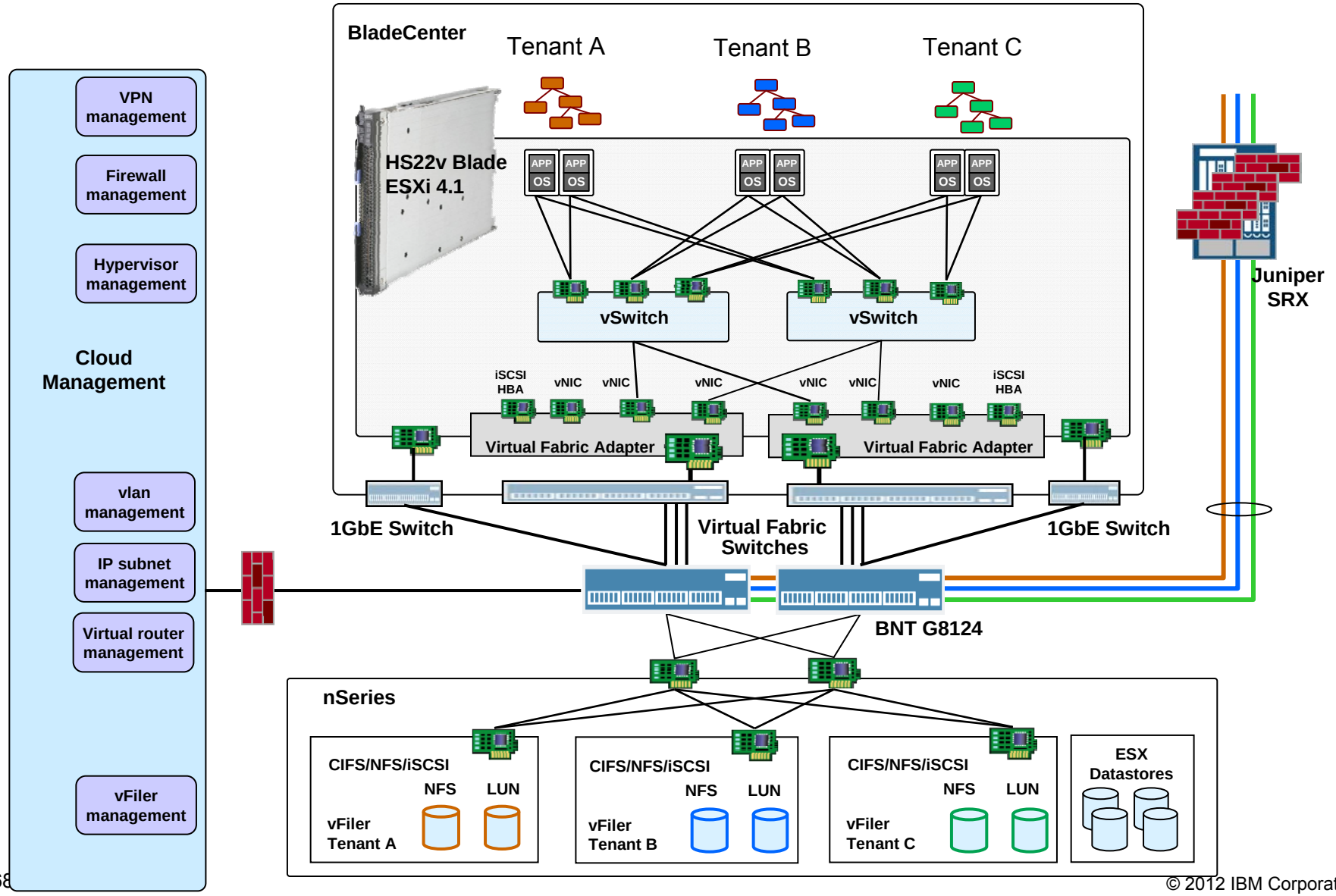
Security Component Model – Cloud Service Provider



*Infrastructure Includes – Server, Network, Storage

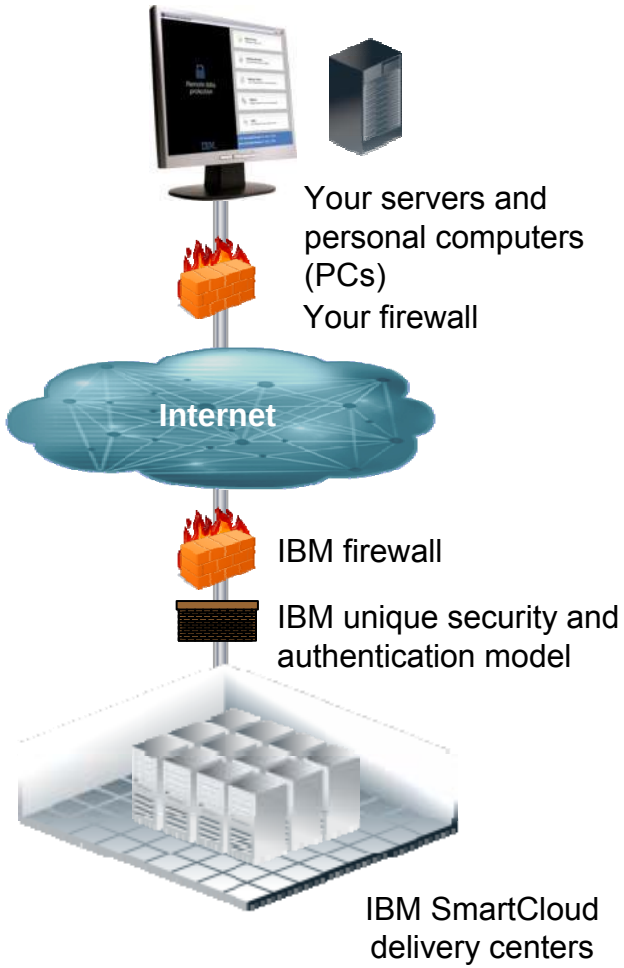
Focus Elements

Secure multi-tenancy component model



Cloud Security Solutions – SmartCloud Enterprise Security

What is IBM SmartCloud Enterprise?



Enterprise virtual IT infrastructure

- Helps provide more control, reliability and data security and can offer massive scalability in performance and capacity

IBM owned and managed

- Multi-tenant shared infrastructure
- Highly virtualized
- Multiple IBM delivery centers
- Preconfigured software images

Enhanced security

- Security-rich access through the Internet
- Virtual private network option
- Based on IBM security standards

Pay-per-use

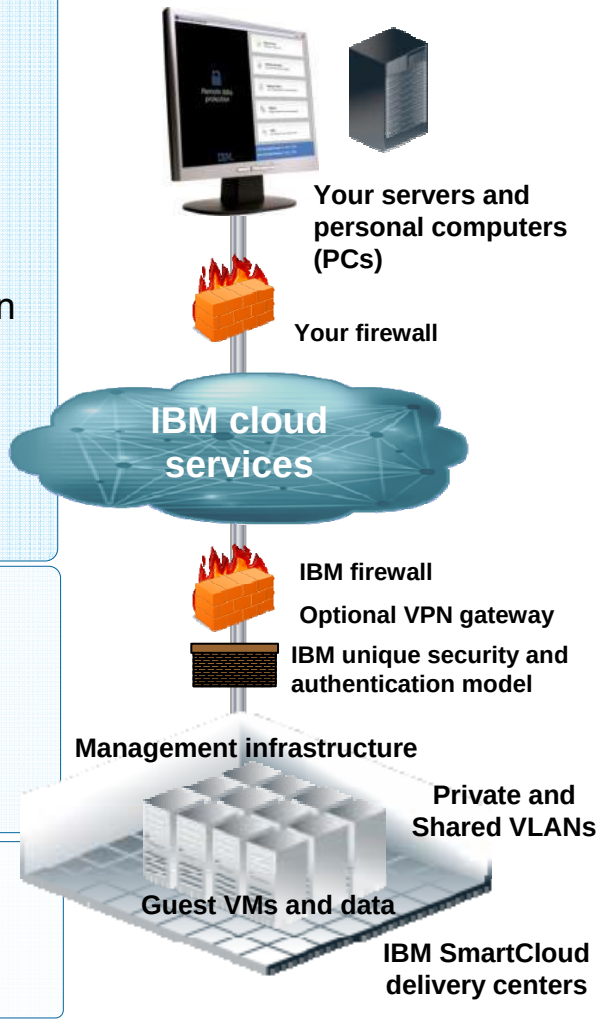
- Virtualized IT resources delivered on a usage-based billing model

Security is built into the IBM SmartCloud Enterprise offering

Virtual infrastructure
- Hypervisor-based isolation with customer configurable firewall rules
- Physical firewall and intrusion prevention service/intrusion detection service (IPS/IDS) between guest virtual machines (VMs) and Internet
- Multiple IP addresses per instance with which to enable security zones
- Optional virtual private network (VPN) and virtual local area network (VLAN) isolation of account instances
- Connections may be encrypted and IBM is isolated from VMs by design (using secure shell [SSH] keys in Linux® and Microsoft® Windows® Server user access control)
- Client has root access to guest virtual machines allowing further hardening of VMs, e.g. in-guest encryption
- Shared images patched and scanned regularly

Management infrastructure
- Access to the infrastructure is only enabled using web identity through the user interface portal or application programming interfaces [APIs]
- Complies with IBM security policies, including regular security scans
- Controlled and audited administrative actions and operations

Delivery centers
- Customer data and VMs are kept in the data center where provisioned
- Physical security is same as for IBM's internal data centers

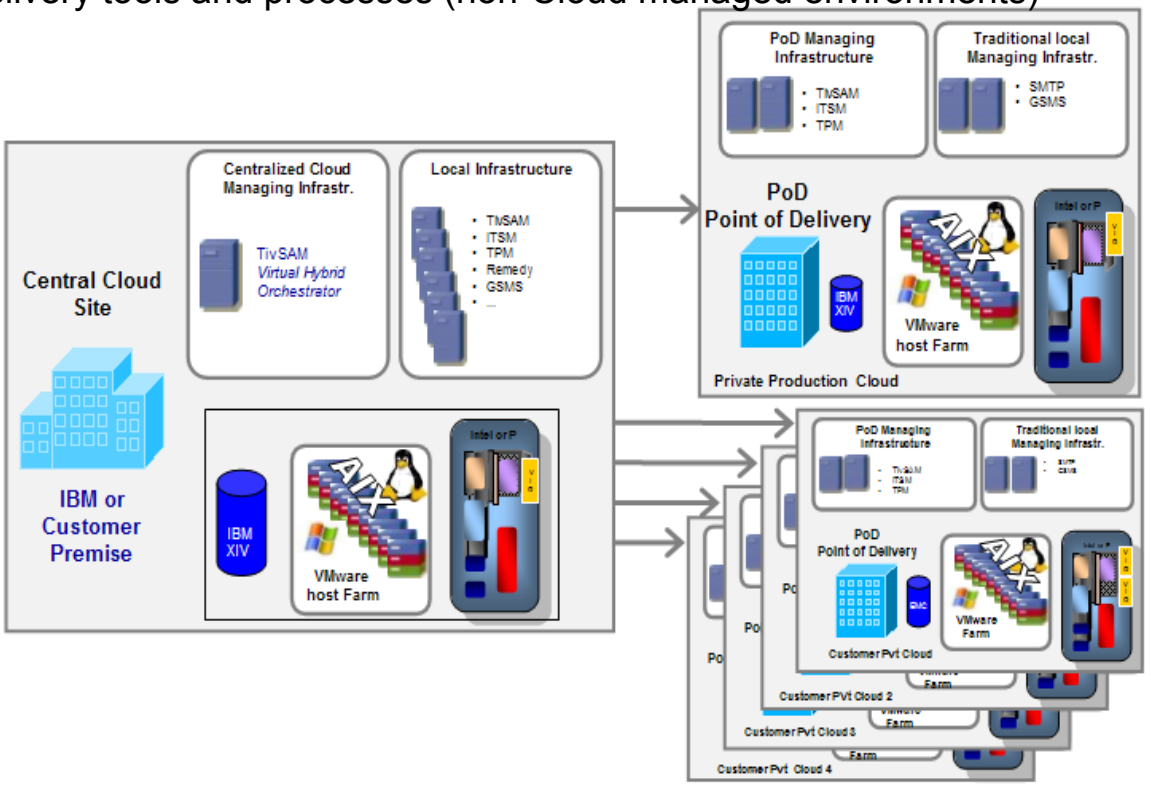


Cloud Security Solutions – SmartCloud Enterprise+ Security

SCE+ Overview

- Cloud hosting environment that supports workloads to committed SLAs; management above the hypervisor, with ITIL-based practices
- A shared layer provides economies of scale, speed of provisioning with shared cost, with a dedicated Managed environment for running client workloads with a high level of security isolation. On or off premise options
- Provides a wide choice of selected IBM hardware and software
- Integration with existing IBM SO delivery tools and processes (non-Cloud managed environments)

- Services included
  - Full service monitoring of instance
- Level of isolation and sharing
  - VPN/VLAN access
  - GSNI access
  - Dedicated physical layer optional
- Locations
  - Run environment on IBM or Customer premise (R1+)
- Architecture/Platform
  - Intel and Power architectures
  - OS options – Linux, Windows, AIX
  - Hypervisor – VMWare, PowerVM

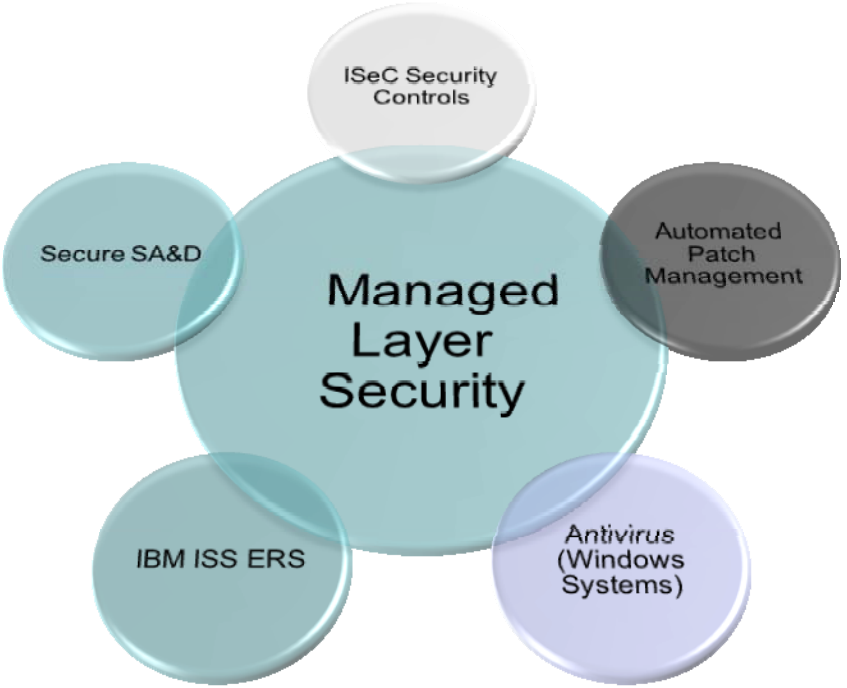


Our clouds implement security controls that meet or exceed industry best practices at the Management layer

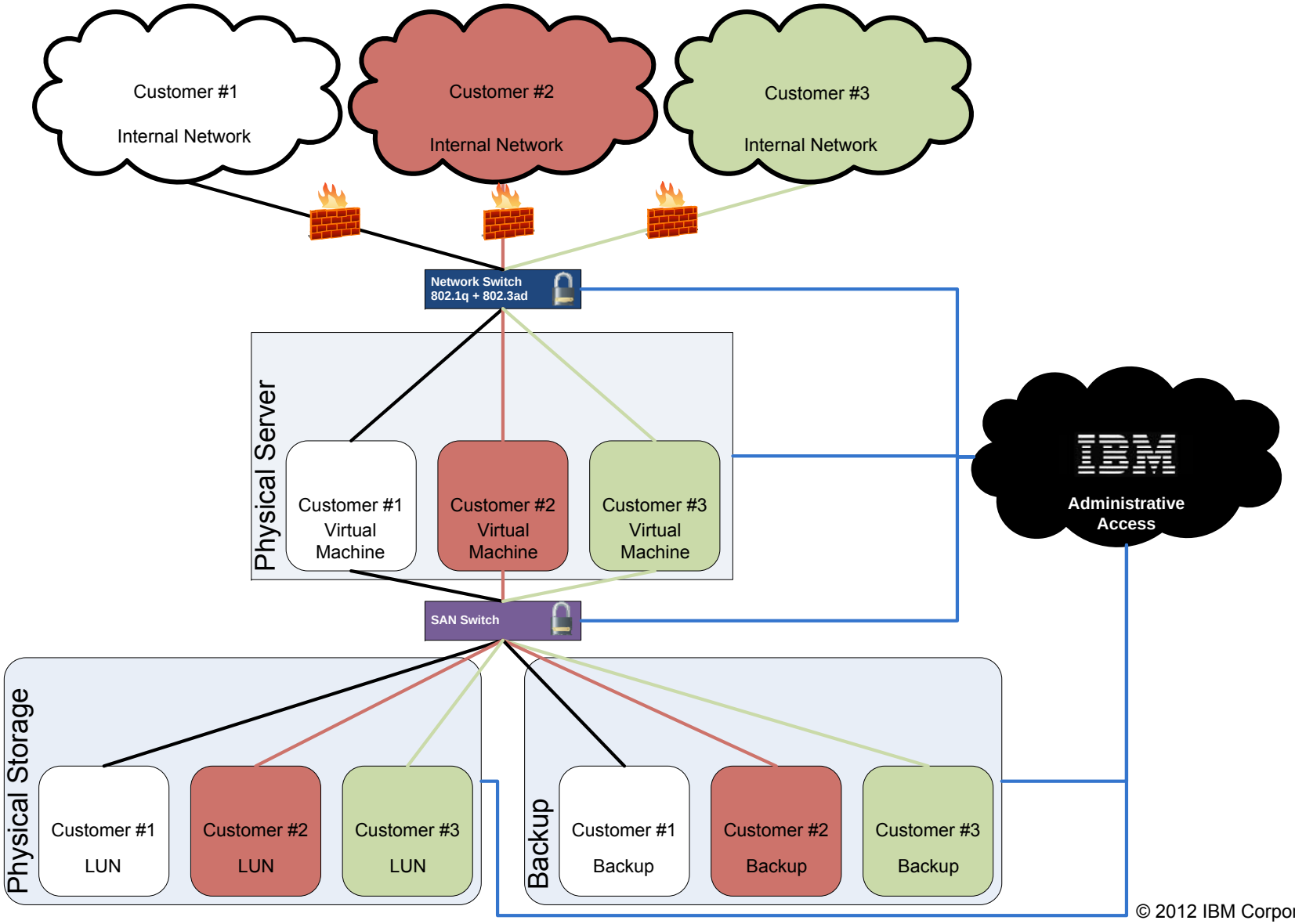
- Built on secure building blocks from IBM's experience in strategic outsourcing
- Network isolation using :
  - Physical and logic separation
  - Secure trunking and channeling
  - VLANs
- Out of band network for access to management infrastructure
  - Storage is separated using Zoning + Hypervisor isolation
- Regular validation of security parameters and policies using strategic IBM tools
- Strict adherence to IBM corporate patch and vulnerability scanning management practices
- Hosted in a Tier 3 (UTI-3) data center

The SCE+ managed environment adopts standard IBM security controls which have been used to secure thousands of customers across the globe

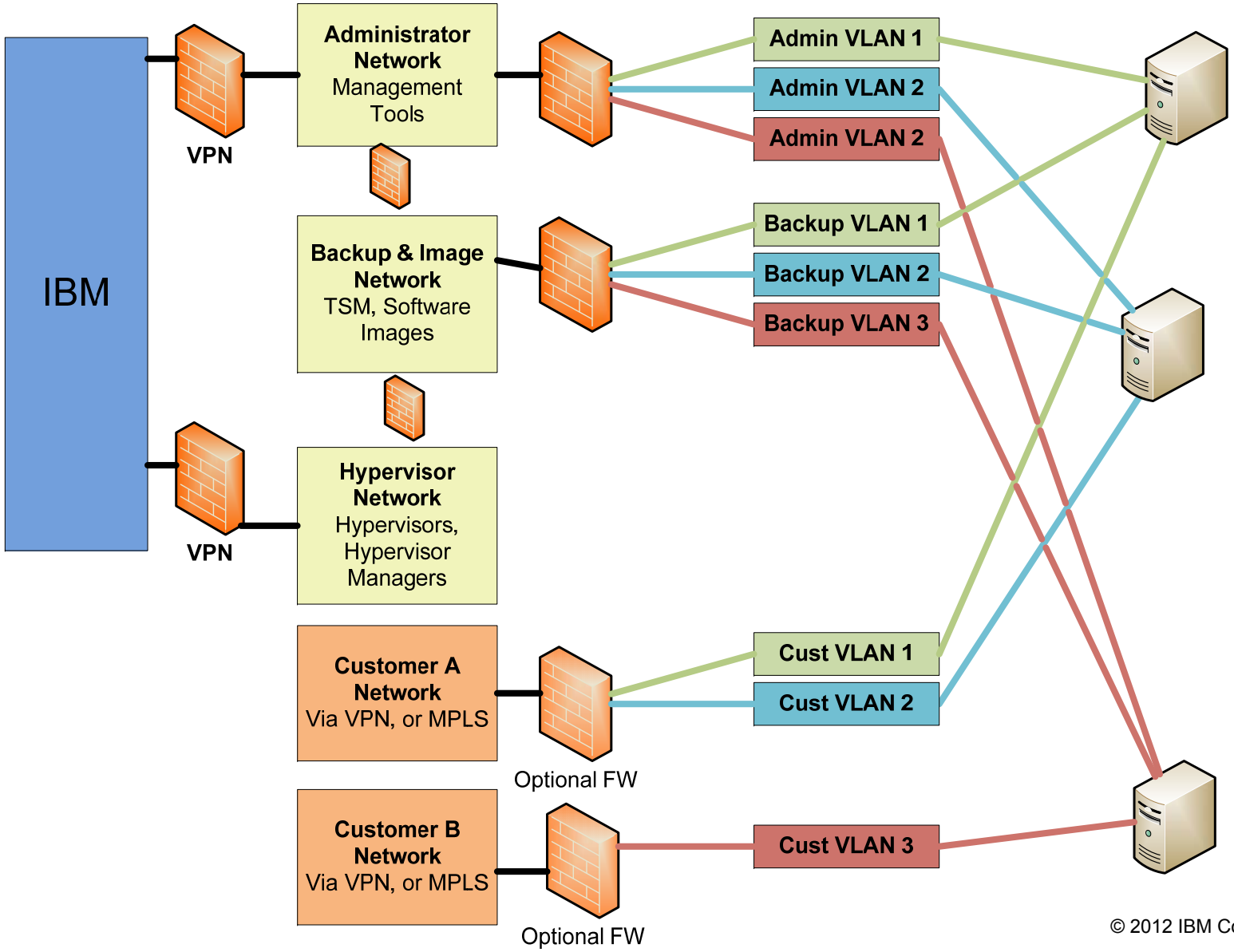
- ISO/IEC 27001/2 based security policy which supports industry and regulatory requirements
- Hardened OS images, validated using strategic IBM tools
- Securely configured middleware, based on security policy specifications
- Automated validation against ISeC security controls
- Automated processes for Service Activation and Deactivation (SA&D) and patch management
  - Activation
    - Patch installation
    - Security control applied
  - Deactivation
    - Zeroing of virtual disk
    - Invalidation of previous backups



Overview of multitenant separation and control



SCE+ Network Separation



Cloud Security Standards

IBM contributes to cloud security standards development to address customer barriers to cloud adoption

ISO JTC 1/SC 27 – IT Security Techniques

- ✓ Cloud security methodologies, procedures, guidelines, documentation and evaluation procedures

Identity in the Cloud TC (IDCloud)

- ✓ "Identity in the Cloud Use Cases Version 1.0" white paper
  - Covering 15 Identity Management categories
- ✓ "Cloud IdM Standards Gap Analysis" white paper

Cloud Auditing Data Federation (CADF) Working Group

- ✓ Standards for federation and classification of audit event data for activity reporting
- ✓ "Cloud Auditing Use Cases Whitepaper"
  - Including operational, business, security, SLA and SLM use cases

IETF OAuth 2.0

- ✓ A key security technology for the integration of REST APIs into the enterprise, whether inside or outside the firewall.
- ✓ IBM increasing support for OAuth 2 authentication across all brands

IBM Security Standards Participation

Driving client-focused open standards and interoperability

IBM engages customers on cloud security standards through the Cloud Standards Customer Council

- Formed April 2011, under OMG, to provide customer-lead guidance to the multiple cloud standards-defining bodies
- Establishing the criteria for open-standards-based cloud computing
  - ✓ Published “Practical Guide to Cloud Computing”, Sept. 2011
  - ✓ Published “Practical Guide to Cloud SLAs”, Feb. 2012

CSCC Security Working Group

- Formed February 2012, Co-chaired by The Kroger Co. & Boeing

- **Develop high priority use cases** for cloud security that reflect customer issues and pain points
- **Identify regulatory compliance capabilities** and options through security architecture standards
- **Identify “best-of-breed” security solutions** for Customers
  - ✓ Published “Security for Cloud Computing: 10 Steps to Ensure Success”, August 2012

Register & Download: http://www.cloud-council.org/security-pr

370+
companies are participating

50%
operate outside the IT realm

Membership:
http://www.cloud-council.org

80

CSCC Security WG – Whitepaper
"Security for Cloud Computing: 10 Steps to Ensure Success"

A reference to help enterprise IT & business decision makers as they analyze and consider the security implications of cloud computing on their business. (Published August, 2012)

10 Steps to Manage Cloud Security

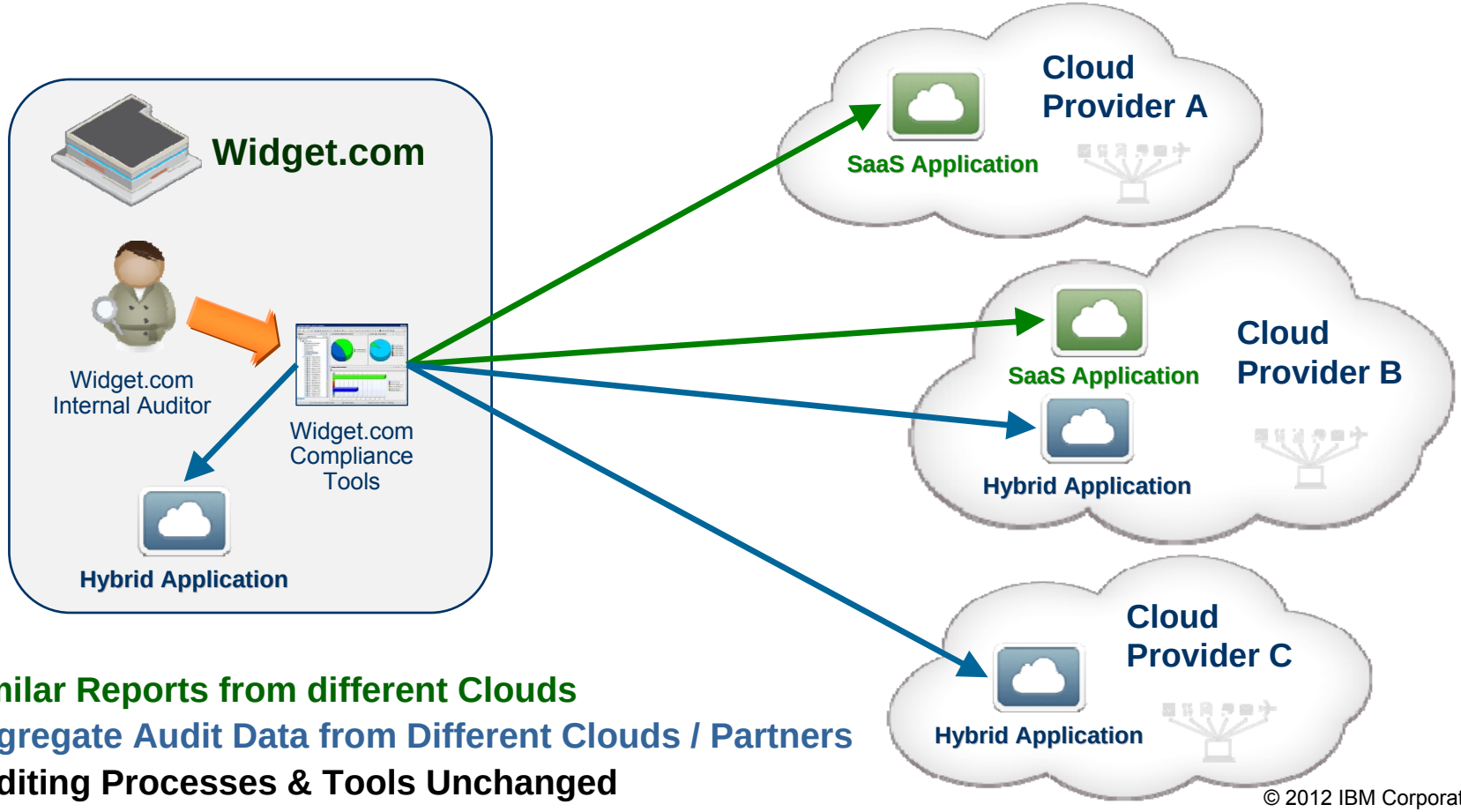
1. Ensure effective governance, risk & compliance
2. Audit operational & business processes
3. Manage people, roles & identities
4. Ensure proper protection of data & information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks & connections are secure
8. Evaluate security controls on physical infrastructure & facilities
9. Manage security terms in the cloud SLA
10. Understand the security requirements of the exit process

""The CSCC has created a practical guide to help those with information security expertise as well as those that don't have domain expertise. This work will help organizations step through ten areas to be cognizant of when evaluating cloud providers. The end effect is helping companies avoid decisions that put their data and service at risk." **Ryan Kean, Senior Director, Enterprise Architecture, The Kroger Company.**

Use Cases for DMTF Cloud Auditing Federation Standards

Standards for customers to request customized audit event information & activity reports for their cloud applications and data when they need it

- Standard **Prevents Cloud Provider "Lock In"** due to audit format dependencies
- Event Data is **Normalized** and **Categorized** to support auditing of Hybrid Cloud Applications
- Format is **Agnostic** to the underlying **Provider Infrastructure** and internal processes



✓ **Similar Reports from different Clouds**

✓ **Aggregate Audit Data from Different Clouds / Partners**

✓ **Auditing Processes & Tools Unchanged**

Market adoption accelerating

The OAuth 2.0 specification is developed by the OAuth Community and managed internationally through the IETF

What is it?

OAuth is an open protocol to allow authorized access in a simple and standard method from cloud, desktop, mobile and web applications to REST API endpoints. It provides a consistent model that bridges on-premise to cloud.

What is new?

OAuth 2.0 simplifies the process of developing a client, building on the lessons learned from previous versions. The latest version includes many new profiles, authorization flows, and support for web apps, desktop apps, mobile & living room devices.

Why is it important?

OAuth 2.0 is a key security technology for the integration of REST APIs into the enterprise, whether inside or outside the firewall. The additional capabilities (flows) have significantly increased market adoption. It is now an underlying security protocol in four other security standards.

✓**Current implementations include: Tivoli Federated Identity Manager 6.2.2, LotusLive**

✓**Planned implementations include: IBM Connections, IBM Lotus Notes/Domino, Rational Team Concert, WebSphere, Sterling**

Learn more about OAuth 2.0: http://oauth.net/

References

References

IBM Cloud Computing
IBM approaches cloud computing from the inside out, designing a cloud environment or providing cloud-based services for each organizations unique requirements.
Find out more at http://www.ibm.com/ibm/cloud/

IBM Enterprise Security
IBM business-driven approach to enterprise security helps you to address risk and reduce cost and complexity.
Find out more at http://www-03.ibm.com/security/