Key Concepts & Cloud Security Concerns

Introduction

- Cloud deployment is continuously increasing
  - Reduce cost and operational and maintenance overhead
- Cloud providers are investing heavily in security
- Security continues a big concern for enterprises
  - Lack of in-house control
  - Resource pooling by cloud providers
  - Shared responsibilities

Key Concepts

- Authentication
  - Refers to digitally confirming the identity of the entity
  - Determining “Who you are”
- Authorization
  - Check if user has permission to perform actions
  - “What you are allowed to do”
  - Access Control List is used

Key Concepts

- Confidentiality
  - Keeping the data secret from resources not authorized to access it.
  - While continue to provide access to “authorized” users
  - Loss of confidentiality
    - Fear of loss of control of data
    - Will the sensitive data stored on cloud remain confidential?
    - Will cloud provider have access to private data?

Key Concepts

- Integrity
  - Data does not get modified or corrupted
    - If data changes that you know that a change has taken place
  - Loss of Integrity
    - How to validate if Cloud provider is returning correct results
    - Could cloud provider temper with data?
- Availability
- Non-Repudiation

Key Concepts

- Availability
  - Will the service be available when I need it
  - Loss of availability
    - Can cloud provider prevent DOS attacks?
    - What happens if server goes down?

Security Concerns

Security Concerns

- Loss of Physical Control
  - One of the biggest concerns for enterprises
  - How do we make sure that our data an IP is in good hands
  - Raises important legal concerns as well.
  - Do cloud providers have access to our data?
  - Since we are sharing resources — what about competition?

Security Concerns

- Accountability
  - Who is accountable and liable?
  - Cloud provider employees can be phased, who is responsible for all compliance?
    - SOX, HIPAA, PCI?
- Data Residency
  - Do you know where the data is?
    - Can the data be moved without your knowledge
  - What are data residency requirements

Cloud Security Overview

Desired Functionality

- Customers want to have a trusted enterprise cloud:
    - They can run their mission critical workloads with more confidence.
    - What does it mean to be a “trusted” cloud vendor?
- Trust requires many capabilities in the following areas:
    - **Control**:
        - Want security mechanisms to control who can access their data under which conditions.
    - **Visibility**:
        - Need audit-quality logs to have more visibility into what is happening with their accounts and resources.

Desired Functionality

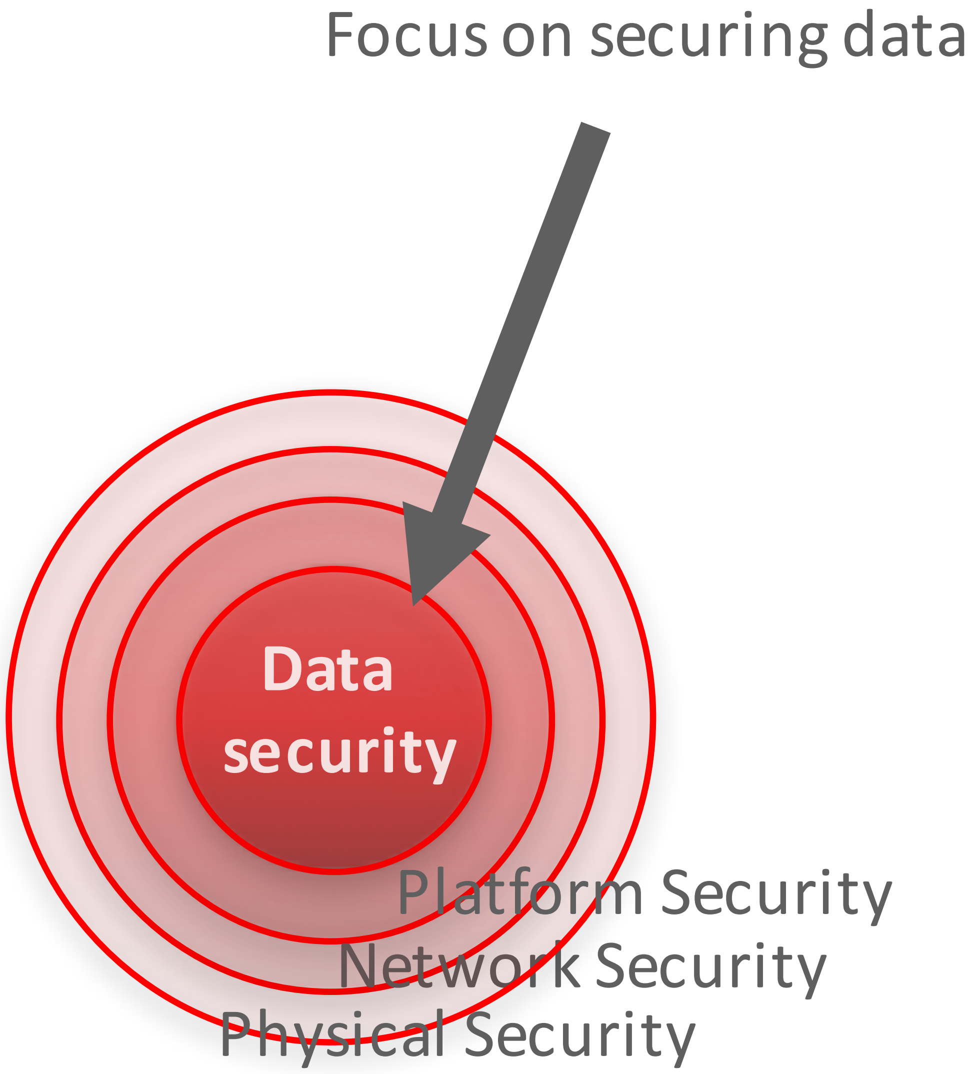
- **Auditability**:
  - ✓ Want auditability of their resources to make sure that their security configuration is flawless.
- **3rd Party Assurance**:
  - ✓ Want the ability to independently verify how their data is being stored, accessed and protected against unauthorized access and modification.
  - ✓ Want to know that the have the ability to implement their regulatory requirements in their cloud environment.

Desired Functionality

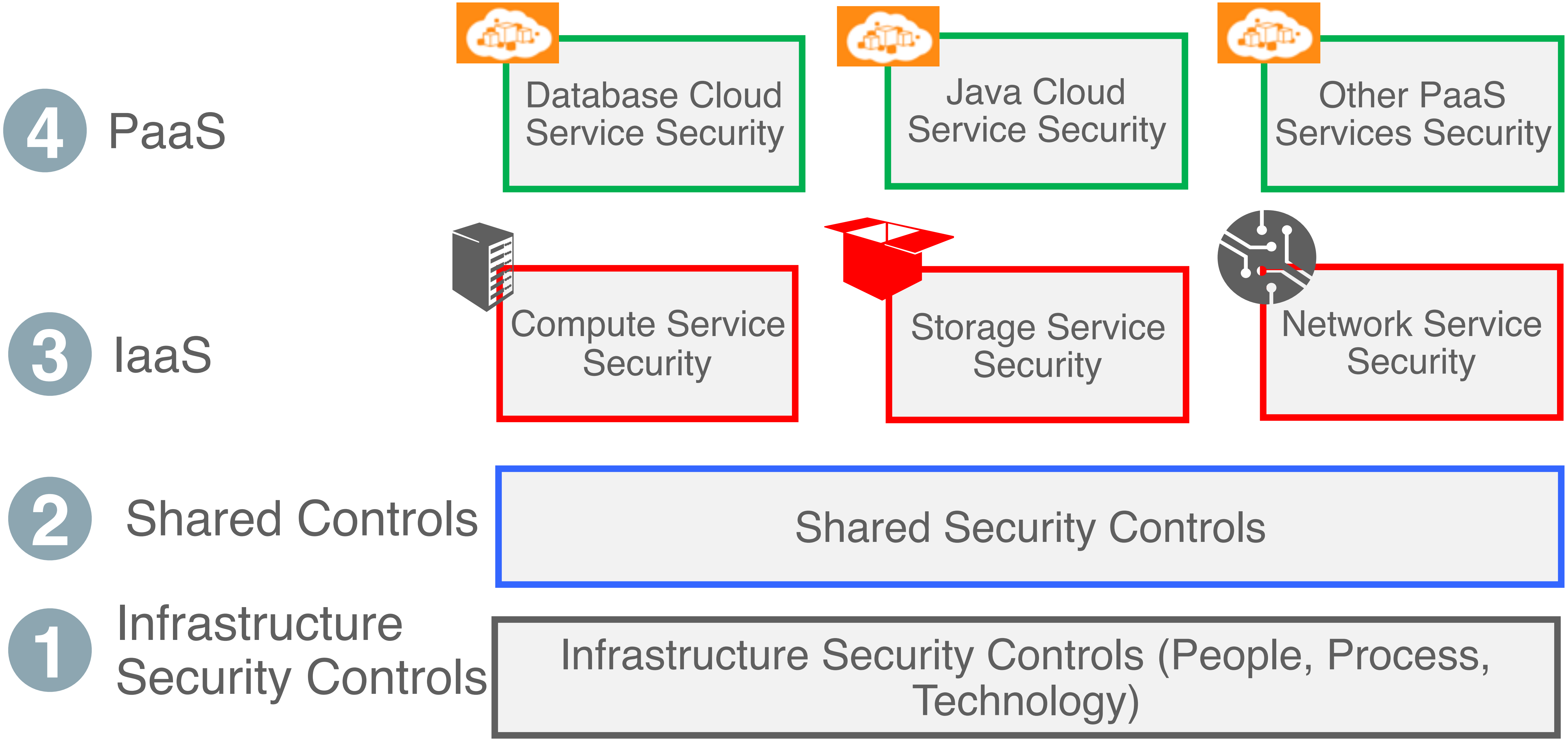
- **Out-of-the-box Integration with existing (security) technologies:**
  - ✓ They expect seamless integration with their existing security solutions such as Identity and Access Management.
- **Secure software and infrastructure:**
  - ✓ Last but not least, customers want cloud services that are architected, coded, tested, deployed and managed securely.

Security Philosophy

- Defense-in-depth
  - Multi-layer security approach
- Add security control closer to the data
- Breach are inevitable
  - Breach detection, incident response, and effective recovery



Security Control in all layers



4 PaaS

Database Cloud Service Security

Java Cloud Service Security

Other PaaS Services Security

3 IaaS

Compute Service Security

Storage Service Security

Network Service Security

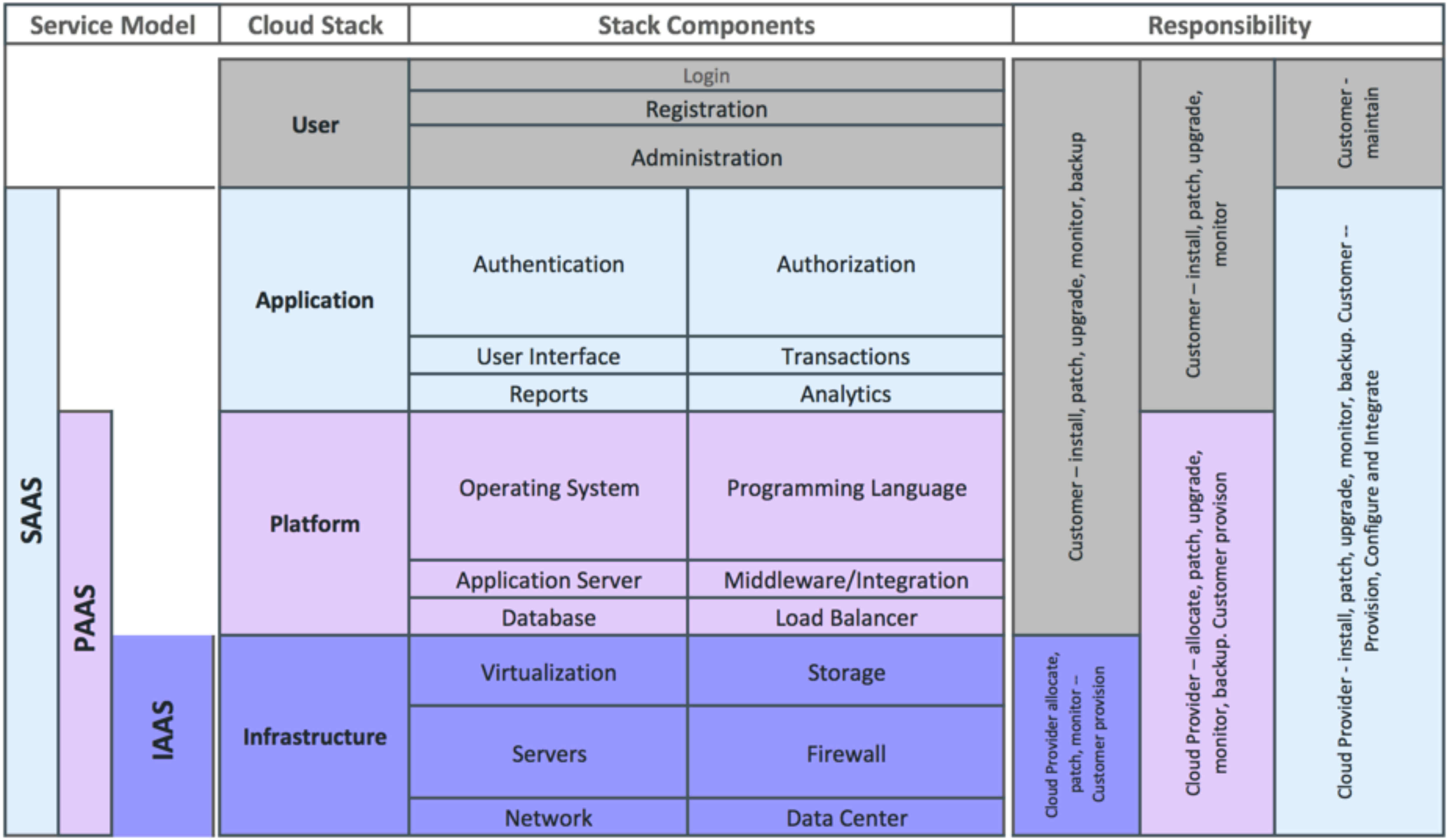
2 Shared Controls

Shared Security Controls

1 Infrastructure Security Controls

Infrastructure Security Controls (People, Process, Technology)

Shared Responsibility Model



Service Model			Cloud Stack	Stack Components		Responsibility		
			User	Login		Customer – install, patch, upgrade, monitor, backup	Customer – install, patch, upgrade, monitor	Customer - maintain
				Registration				
				Administration				
SAAS			Application	Authentication	Authorization			Cloud Provider - install, patch, upgrade, monitor, backup. Customer -- Provision, Configure and Integrate
				User Interface	Transactions			
				Reports	Analytics			
	PAAS		Platform	Operating System	Programming Language		Cloud Provider – allocate, patch, upgrade, monitor, backup. Customer provison	
				Application Server	Middleware/Integration			
				Database	Load Balancer			
		IAAS	Infrastructure	Virtualization	Storage	Cloud Provider allocate, patch, monitor -- Customer provision		
				Servers	Firewall			
				Network	Data Center			

IaaS Security Capabilities Fall in Two Buckets

- Cloud Operations Security
  - Physical access to data centers
  - Logical access to data centers
  - Network protection and monitoring
  - Incident response
  - Cloud governance (policies and procedures)
  - Auditing, certifications and attestations

- Cloud Service-Specific Security
  - Identity and access management
  - Data security
  - Virtualization (compute platform) security
  - Network security for instances
  - Security design
  - 3rd Party Certifications and attestations

Security Operations: Network

- Network
  - Multi-level Firewalling – Application, Middleware, Database
  - Shared Service Segmentation - Directory, Identity Manager, Access Manager
- Intrusion Detection
  - All infrastructure should be monitored 24x7x365
  - Security Information and Event Management
  - Servers, Switches, Firewalls, IDS, Anti-Virus/Malware,
  - Multi-factor Authentication Systems, Netflows, etc.

Security Operations: Incident Response

- Dedicated Cloud Security Teams Needed to Provide:
    - Detection
    - Mitigation
    - Forensics
    - Notification
- Incident Response Efforts Need to be Coordinated With:
    - Global Information Security
    - Global Product Security
    - Privacy & Security Legal

Data Disposal

- Upon termination of services or at Customer's request, will Provider delete environments?

- And delete data residing therein in a manner designed to ensure that they cannot reasonably be accessed or read?

Service-Specific Security

Compute Instance Security

- SSH based access to VMs:
  - Before creating a compute instance customers need to generate at least one SSH key pair and upload the SSH public key.
  - After adding an SSH public key, customers need to attach it to an instance.
  - Customers can update, disable, enable and delete an existing SSH public key.

Compute Instance Security

- Dynamic Firewall:
  - When you create an instance, by default, it shouldn’t allow any network traffic from and other instance or external host.
  - To allow communication among some of your instances, you should create a network security list and add the instances to that security list.
  - By default, the instances in a security list should b isolated from hosts outside the security list.
  - You should create “security rules” to enable communication with hosts
  - Each security rule should define a specific source, a destination, and a protocol-port combination over which communication is allowed.

Instance Isolation

- Virtualization is the foundation of Compute Cloud Service.
- Many security-related concerns about virtualization are unwarranted.
- Multiple hardware-supported and software-supported isolation techniques address the risks associated with virtualization.
- The first technique is instruction isolation.
    - Intel VT-x and AMD-V both enable a VMM to give the CPU to a virtual machine for direct execution until the time the virtual machine attempts to execute a privileged instruction.
    - At that point, the virtual machine execution is suspended, and the CPU is given back to the virtual machine monitor.

Instance Isolation

- In addition to CPU instruction isolation:
  - Hypervisor also provides memory and device isolation
  - By virtualization of physical memory and physical devices including disks.
  - This explicit virtualization of the physical resources leads to:
    - A clear separation between the guest OS and the hypervisor,
    - Resulting in a secure compute environment.
    - Thus, different customer instances running on the same physical machine are isolated from each other via the hypervisor.

Authentication

- The process of authentication involves:
  - Validating at least one factor of authentication
    - Factor can be something the entity or user knows (pw, pin)
    - Something that user has (smart card)
    - Something that can uniquely identify the user (fingerprints)
  - Multi-factor authentication
    - More than one factor is used for authentication

Single Sign On

- Enables users to access multiple systems after signing on once
- Since different systems or applications may be internally using different authentication mechanism
  - SSO upon receiving initial credentials translates for different systems
- Reduces human errors and aggravation
- Different implementations for SSO:

SSO: SAML-Token

- Security Assertion Markup Language (SAML)
  - XML based standard data format for exchanging security information between identify provider and service provider
- When user tries to access cloud app
  - SAML request is generated and user is predicted to the identity provider
  - The identity provider parses the request and authenticates the user
  - A SAML token is returned to the user who access the cloud app using the token

SSO: Kerberos

- Uses tickets for authenticating clients to a service
- Provides mutual authentication:
  - Both client and servers authenticate with each other
- Client authenticate itself to the Authentication Server
  - Client sends users ID to the AS
  - The AS checks if the client is in DB and generates a Client/TGS Session key
    - This is used by client and the remote

SSO: One Time Password

- Uses valid passwords for use only for a single session
- More secure — Not vulnerable to replay attacks
- Text message is the common delivery mode for OTP tokens
- The most common approach for generating OTP is time synchronization

IaaS: Storage Service Security

- Client-side customer controlled encryption
  - Customer can encrypt objects before sending to Storage Cloud Service
  - Unique symmetric key is generated for each object
  - Customer provides and manages an asymmetric key pair
- Availability via data replication across multiple storage nodes
  - Ensuring data will survive hardware failure
  - Yes they do happen in cloud as well.

IaaS: Storage Service Security

- Access control via roles and container based read/write ACLs
  - Access to stored objects is controlled by pre-defined groups
  - Customer can manage and define these roles, e.g.,:
    - Identity domain administrator
    - Storage Administrator

IaaS: Storage Service Security

- API Authentication
  - Most cloud provides offer access through RESTful APIs
  - API Calls to storage can be done using basic authentication
    - User name/password, token-based authentication
    - Grants token for 30-60 mins — refreshes after that time.
- Data Integrity checks
  - MD5 checks is periodically performed in multiple data copies

Shared Security Controls

- Shared identity and access management solution provided by Public Cloud Providers:
  - Including PaaS and IaaS services.
- Identity is a core feature that customers rely on to provide secure access to Providers' PaaS and IaaS services.
  - The Public Cloud feature that brings users, services, and applications together in a secure manner is **shared identity**.
- A tenant in Oracle Public Cloud represents a customer who has subscribed to one or more services from Public Cloud.
- Typically there is a one-to-one correspondence between a Public Cloud tenant and a customer.

Shared Security Controls

- An identity domain in the Public Cloud represents the namespace assigned for a tenant.

- An identity domain is used to identify and associate the assets of a tenant

  - Enable isolation of data assets and transactions of a tenant from that of other tenants.

- A tenant’s assets include subscribed services and data assets including security artifacts such as users, groups, tokens, cookies, and policies.

Shared Security Controls

- A customer can be associated with more than one Public Cloud identity domain.

- Corporate Identity Federation

  - Federate your corporate identity and your identity domain and thereby achieve single sign-on (SSO) between on-premises and the Public Cloud.

  - The SSO service enables users to log in to one domain and access another domain without logging in again.

Network Service Security

- Site-to-site VPN
  - Available with providers the offer dedicated compute
  - Customer establish a secure connection
    - IPSec tunnel between the VPN gateway and on-premise gateway
  - Customer can configure range of IP address for compute instances
  - Public IPs can be configured for internet access
  - 128-bit AES Symmetric key is used for encryption

Network Service Security

- Multitenant VPN
  - IPSec tunnel is established between customer gateway and provider gateway
  - Used for non-dedicated compute (multitenant)
- Direct Connect
  - Serves two purposes — Security and Performance
  - Applications sensitive to latency or require faster data movement.