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

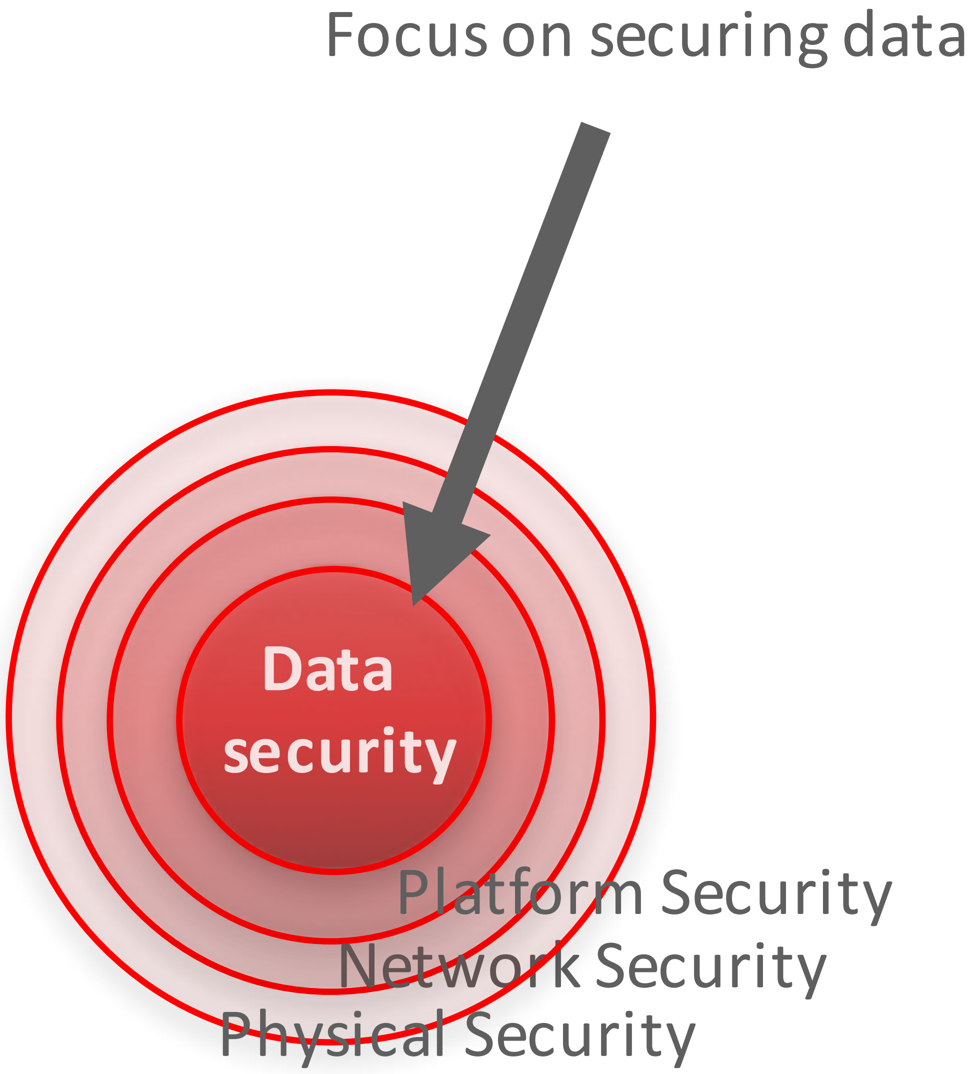
- **Auditability**:
  - ✓ Want auditability of their resources to make sure that their security configuration is flawless.
- **3rd Party Assurance**:
  - ✓ Want the ability to independently verify how their data is being stored, accessed and protected against unauthorized access and modification.
  -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

Desired Functionality

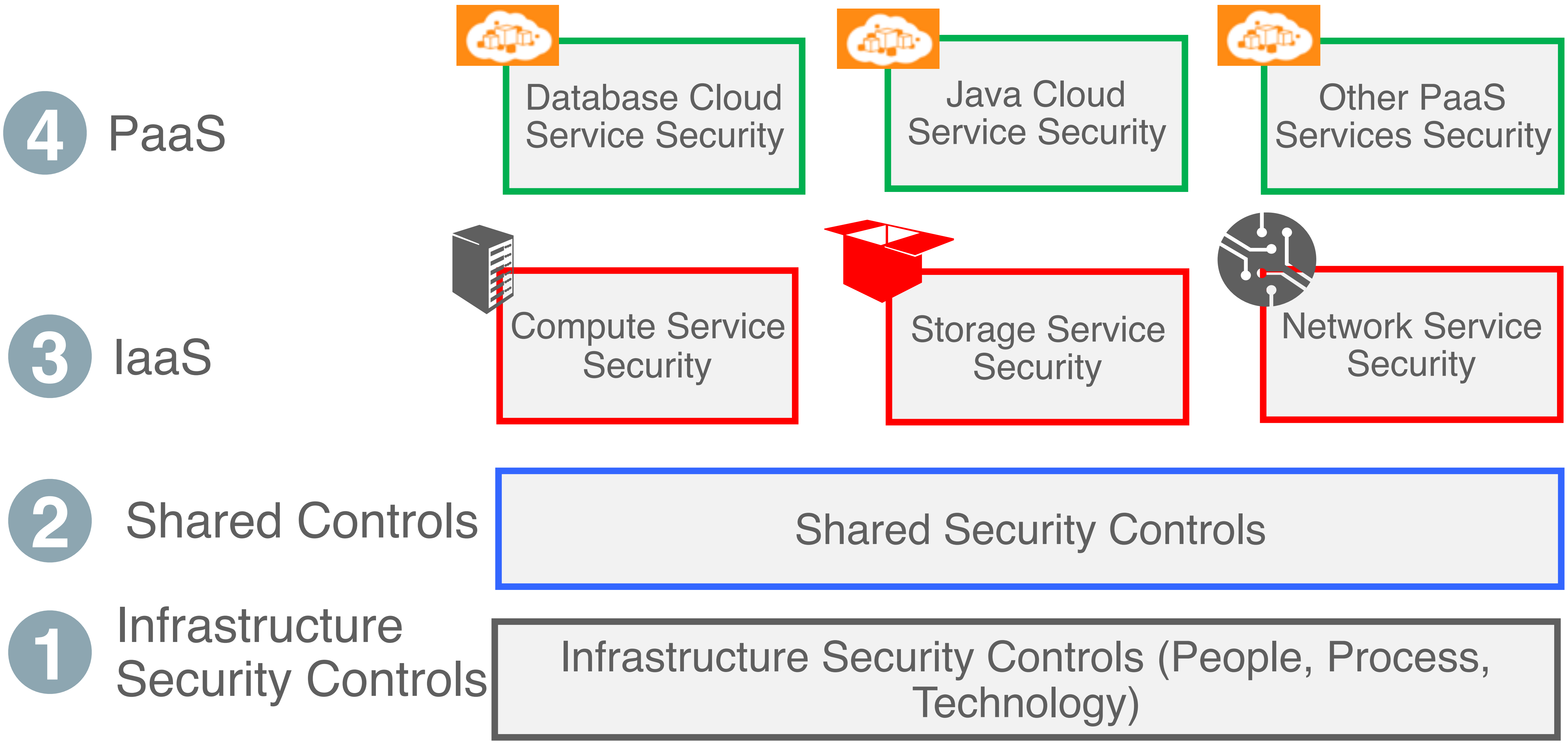
- **Out-of-the-box Integration with existing (security) technologies:**
  - ✓ They expect seamless integration with their existing security solutions such as Identity and Access Management.
- **Secure software and infrastructure:**
  - ✓ Last but not least, customers want cloud services that are architected,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

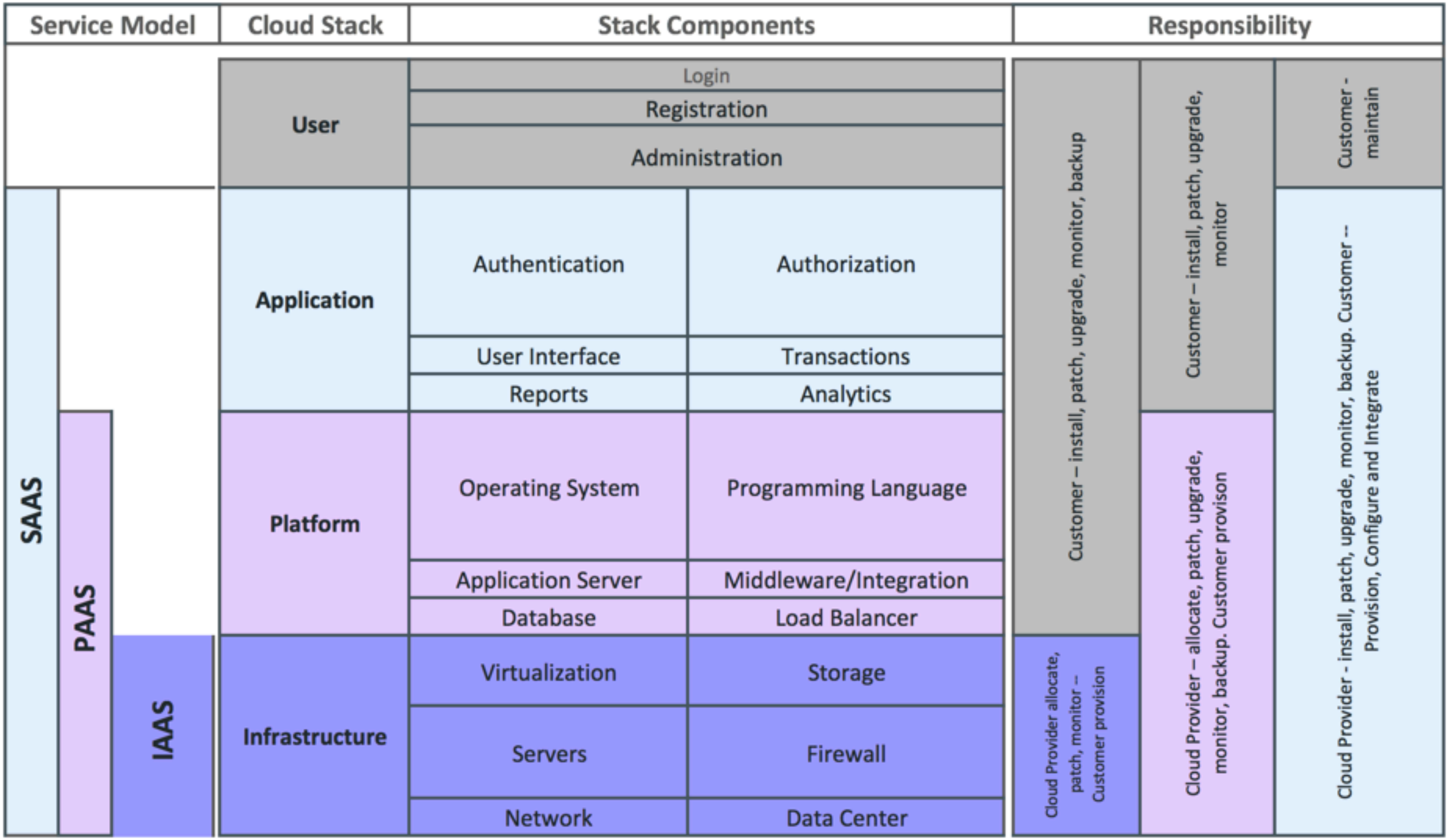
2 Shared Controls

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			

Sohail Rafiqi

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.

Cloud Access Security Broker

CASB

- So, what is CASB?,
  - CASB, stands for Cloud Access Security Broker, a term that has been coin by Gartner
  - According to Gartner, CASBs are security policy control points
    - Placed between users in your organization and the cloud.
- Gartner believes that there is 3 ways in which you can deploy CASB:
  - The first is a proxy like on-prem gateway.
  - The second a host-based agent.
  - And the third one, an API-centric, cloud solution.

CASB

- Current market trends shows a driving dissolution of the network perimeter.

- Users are everywhere,

  - Using unmanaged devices and connecting to on-premise and cloud applications

  - making network edge solutions such as FW, IPS/IDS, Network Proxies to become less than idea.

CASB

- Gartner classifies CASB functionality into four pillars.
- Visibility
  - Who is accessing what applications?
  - What are unmanaged users doing?
- So we can say that visibility in CASB provides:
  - Shadow IT discovery and sanctioned application control
  - Consolidated view of an organization's cloud service usage and the users who access data from any device or location.

CASB

- Compliance
  - Are there any over privileged users in my systems?
  - Are my access keys non-compliant?
  - Or is my DevOps practices compliant?
- CASB can assist with data residency and compliance with regulations and standards, as well as:
  - Identify cloud usage and the risks of specific cloud services.

CASB

- Data Security
  - For data security, CASB provides the ability to enforce data-centric security policies, things like:
    - Who is sharing data in the public cloud?
    - Am I fulfilling the shared security responsibility?
    - Are there any security holes in my DevOps?
- The idea is to prevent unwanted activity based on:
  - Data classification, discovery and user activity monitoring of access to sensitive data or privilege escalation.

CASB

- Threat Protection
  - Who are risky users in my systems?
  - How fast can I stop risky user activities?
  - or How fast can I stop risky applications?
- With threat protection, we try to prevent:
  - Unwanted devices, users and versions of applications from accessing cloud services.
  - Other examples in this category are user and entity behavior analytics (UEBA),
  - or the use of threat intelligence and malware identification.

Cloud Provider CASB

- Cloud Provider monitors:
  - Activity, configurations, transactions and content for IaaS, PaaS, and SaaS services.
- App-to-App and some are BYoD-ready.
- Full security automation:
  - including capabilities to Predict, Prevent, Detect and Respond.
- With secure provisioning:
  - Offer continuous protection of applications through its entire lifecycle.

Data Security

Introduce Risk

More risks concentrated in a single asset you need:

- Better Data Privacy protection
- Stronger Access Controls
- Improved Audit Management
-

More Sensitive Data outside of your control

- More people with potential to access your data
- Greater risk of sensitive data leakage

Database Cloud Service Security

- Dedicated database with full administrative control
  - Completely controlled by customer — (shared responsibility)
- Benefits from the compute and network security
- Upon creation — All access is set to disable by default
  - Appropriate security rules must be enabled.

Database Security

Objectives for Database Security

- Improve Regulatory Compliance
- Safeguard your Reputation/Brand
- Enhance Customer/ Employee Privacy/ Confidentiality
- Protect Intellectual Property
- Reduce risk and liability

Applications Impacted

- CRM
- ERP
- Financial
- HR
- POS
- Core Business

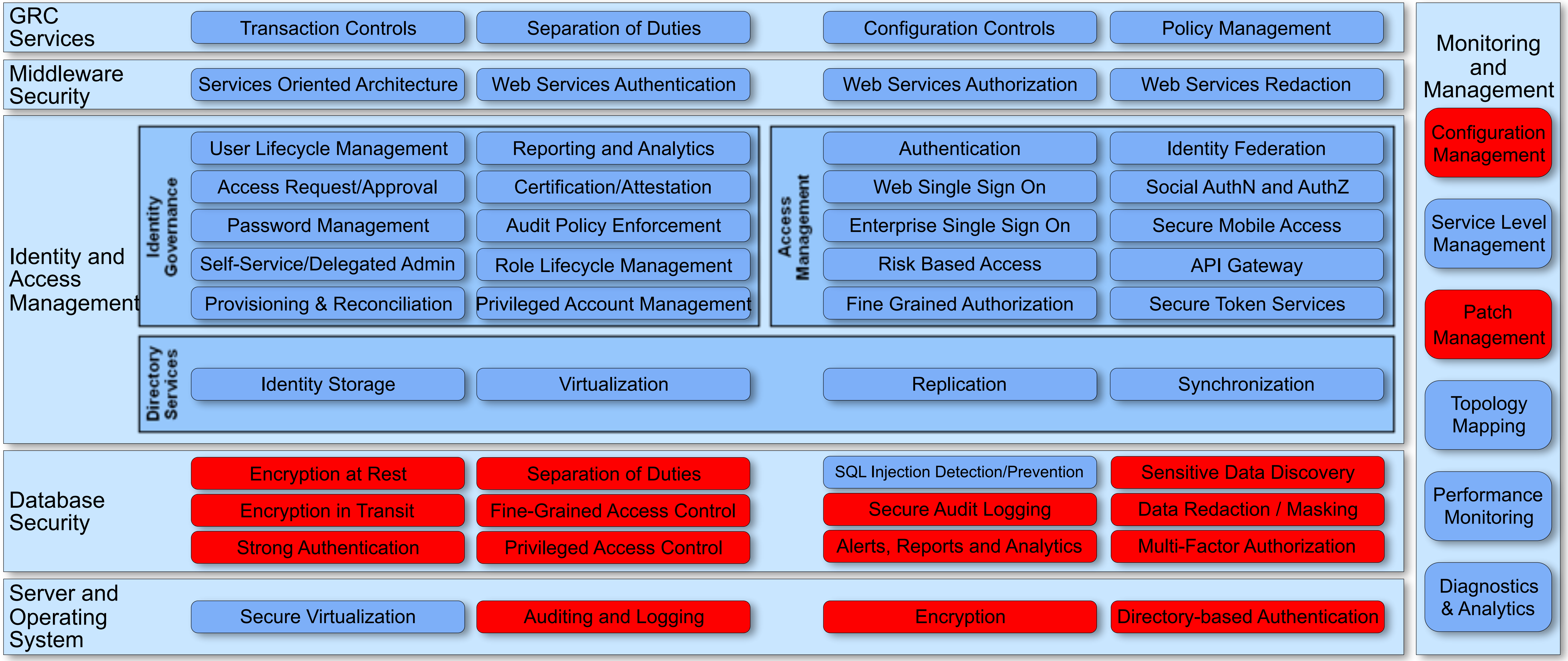
Key Data Affected

- Customer
- Employee
- Intellectual Property
- Partner/ Supplier
- Financial

Required Capabilities

- Row/Column Level Security
- Encryption & Secure Backup
- Privileged Access Controls
- SQL Injection Protection
- Audit, Alert & Monitoring
- Data Masking & Redaction
- Sensitive Data Discovery

DB Security in Cloud Deployment



GRC Services
- Transaction Controls
- Separation of Duties
- Configuration Controls
- Policy Management

Middleware Security
- Services Oriented Architecture
- Web Services Authentication
- Web Services Authorization
- Web Services Redaction

Identity and Access Management

Identity Governance
- User Lifecycle Management
- Reporting and Analytics
- Access Request/Approval
- Certification/Attestation
- Password Management
- Audit Policy Enforcement
- Self-Service/Delegated Admin
- Role Lifecycle Management
- Provisioning & Reconciliation
- Privileged Account Management

Access Management
- Authentication
- Identity Federation
- Web Single Sign On
- Social AuthN and AuthZ
- Enterprise Single Sign On
- Secure Mobile Access
- Risk Based Access
- API Gateway
- Fine Grained Authorization
- Secure Token Services

Directory Services
- Identity Storage
- Virtualization
- Replication
- Synchronization

Database Security
- Encryption at Rest
- Separation of Duties
- SQL Injection Detection/Prevention
- Sensitive Data Discovery
- Encryption in Transit
- Fine-Grained Access Control
- Secure Audit Logging
- Data Redaction / Masking
- Strong Authentication
- Privileged Access Control
- Alerts, Reports and Analytics
- Multi-Factor Authorization

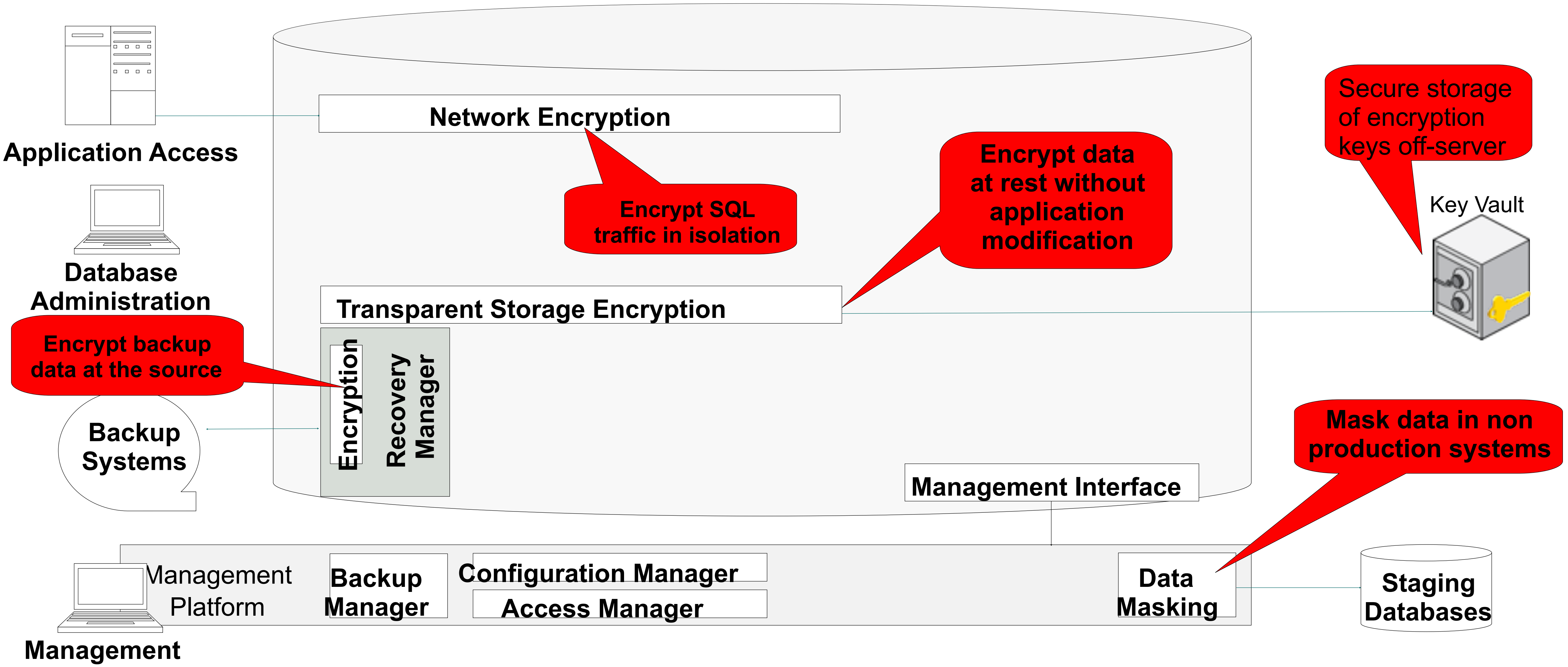
Server and Operating System
- Secure Virtualization
- Auditing and Logging
- Encryption
- Directory-based Authentication

Monitoring and Management
- Configuration Management
- Service Level Management
- Patch Management
- Topology Mapping
- Performance Monitoring
- Diagnostics & Analytics

Sohail Rafiqi

Logical View: Encryption and Masking

Objectives for Database Security	Improve Regulatory Compliance	Enhance Customer / Employee Privacy / Confidentiality	Reduce risk and liability



Application Access

Database Administration

Encrypt backup data at the source

Backup Systems

Network Encryption

Encrypt SQL traffic in isolation

Encrypt data at rest without application modification

Secure storage of encryption keys off-server

Key Vault

Transparent Storage Encryption

Encryption

Recovery Manager

Mask data in non production systems

Management Interface

Management Platform

Backup Manager

Configuration Manager

Access Manager

Data Masking

Staging Databases

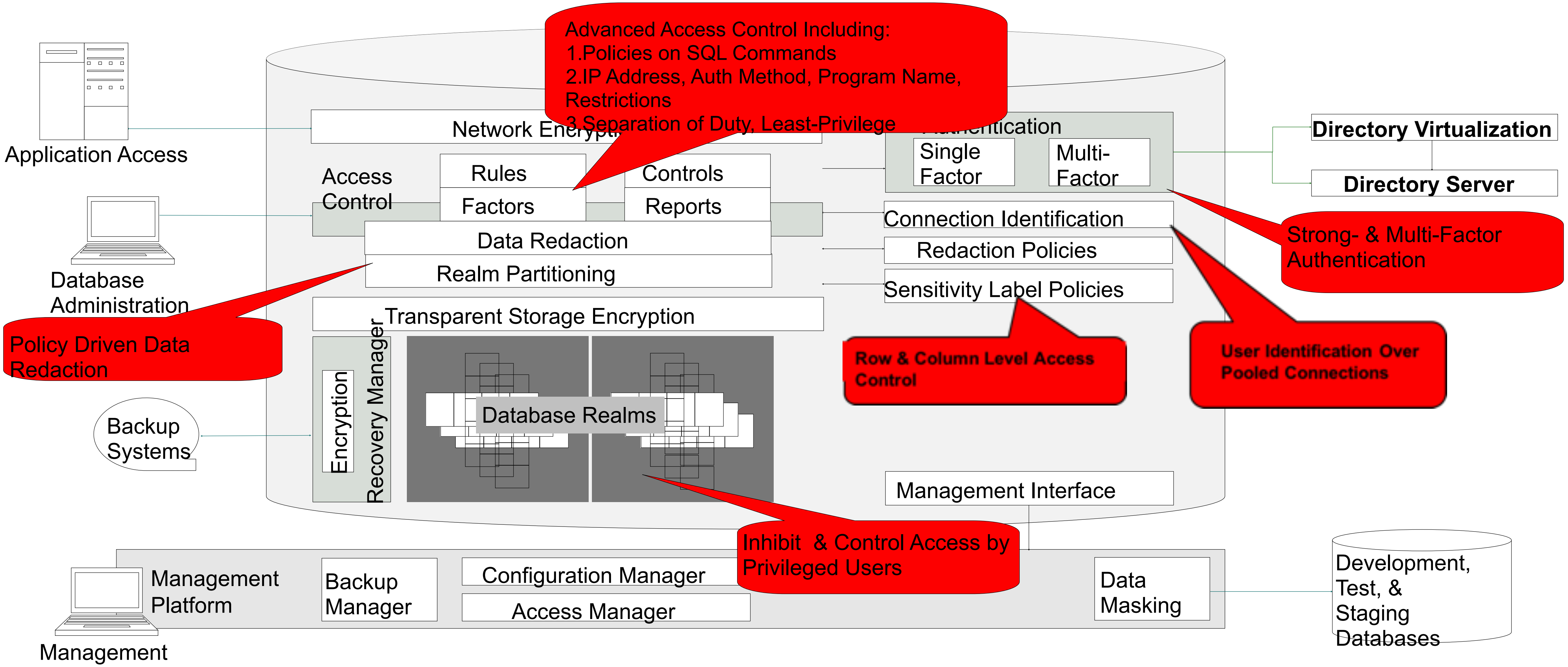
Management

Sohail Rafiqi

Logical View: Access Control

Objectives for Database Security

- Improve Regulatory Compliance
- Enhance Customer / Employee Privacy / Confidentiality
- Reduce risk and liability



Advanced Access Control Including:
1.Policies on SQL Commands
2.IP Address, Auth Method, Program Name, Restrictions
3.Separation of Duty, Least-Privilege

Policy Driven Data Redaction

Strong- & Multi-Factor Authentication

Row & Column Level Access Control

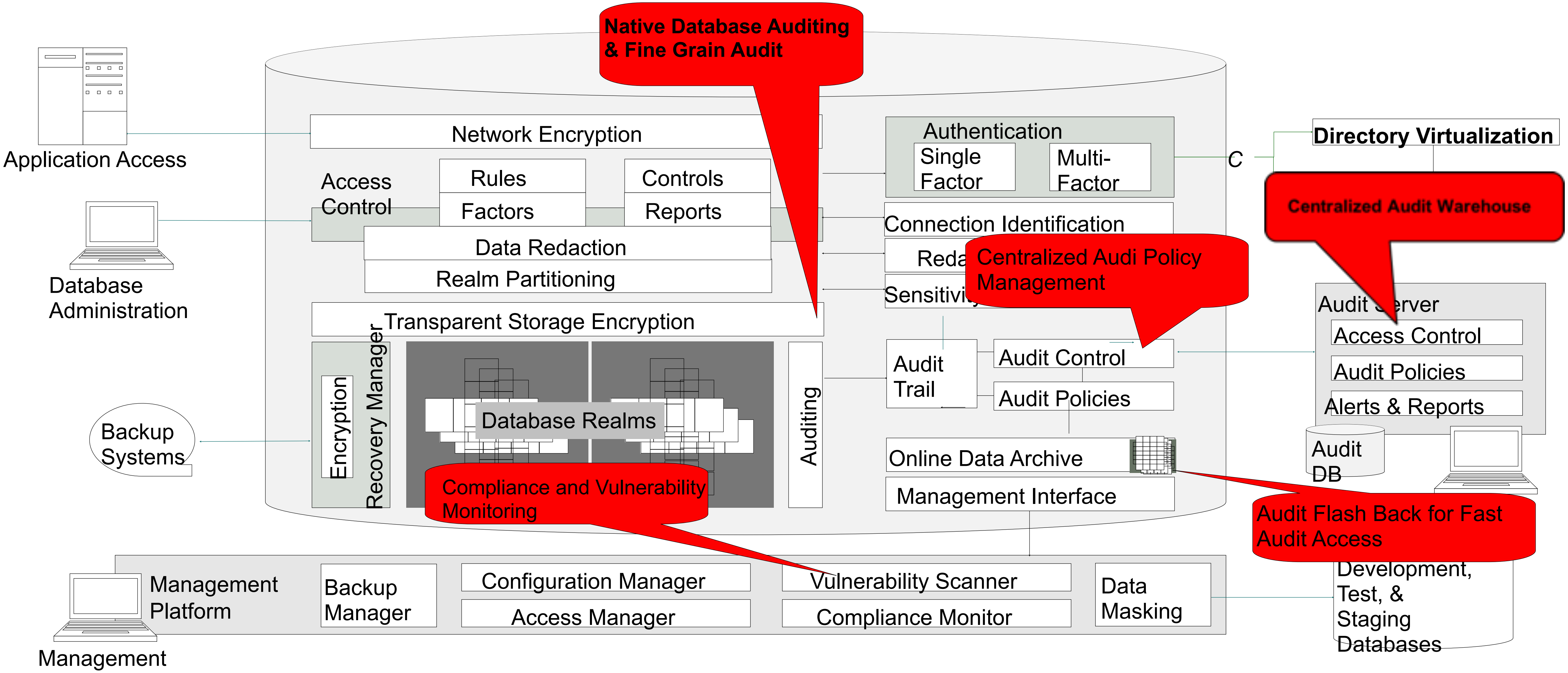
User Identification Over Pooled Connections

Inhibit & Control Access by Privileged Users

Logical View: Auditing and Monitoring

Objectives for Database Security

- Improve Regulatory Compliance
- Enhance Customer / Employee Privacy / Confidentiality
- Reduce risk and liability



Native Database Auditing & Fine Grain Audit

Centralized Audit Warehouse

Centralized Audi Policy Management

Compliance and Vulnerability Monitoring

Audit Flash Back for Fast Audit Access

Application Access

Database Administration

Backup Systems

Management

Network Encryption

Access Control

Rules

Factors

Controls

Reports

Data Redaction

Realm Partitioning

Transparent Storage Encryption

Encryption

Recovery Manager

Database Realms

Auditing

Authentication

Single Factor

Multi-Factor

C

Directory Virtualization

Connection Identification

Reda

Sensitivi

Audit Trail

Audit Control

Audit Policies

Online Data Archive

Management Interface

Audit Server

Access Control

Audit Policies

Alerts & Reports

Audit DB

Management Platform

Backup Manager

Configuration Manager

Access Manager

Vulnerability Scanner

Compliance Monitor

Data Masking

Development, Test, & Staging Databases

DoS/DDoS

DoS/DDoS

- Interruption causes in service (availability) to legitimate users
    - Using up all of the targets resources to accept network connections
        - Resulting in additional connections being denied
    - Sending a message that resets target host’s subnet mask
        - Causing a disruption of the target’s subnet routing
    - Filling up a target’s hard drive storage space

DoS/DDoS

- Cloud Provider network should offer protection against traditional network security issues such as:
  - Distributed denial of service (DDoS) attacks, man-in-the-middle attacks, IP spoofing, and port scanning.
- Network protection devices, including firewalls, needed:
  - To monitor and control network communications at the external boundary
  - and at internal boundaries within the network.
- These network boundary devices employ traffic flow policies, or access control lists (ACLs), that enforce the flow of traffic.
- Firewalls should be deployed in a layered approach to perform packet inspection with security policies configured to filter the packets based on:
  - Protocol, port, source, and destination IP address to identify authorized sources, destinations, and traffic types.

DoS/DDoS

- Vulnerability notification systems needed to monitor security incidents, advisories, and other related information.
- Scaled to support large amount of traffic
  - Wirespeed
- 3-7 layer attack prevention
- Load balancers can inspect traffic
- SYN encryption, support high capacity connection tables
- Pattern matching, flow validation, ICMP flood limitation, strict TCP forwarding
- NIDS — Monitors and block suspicious network traffic
  - NIDS sensors can be in Intrusion Prevention System (IPS) or Intrusion Detection System (IDS)