Cloud security

Joakim Persson

Outline

- Introduction to cloud security
- Cloud threats
- Securing the cloud
- Data center security
- Open Stack security
- Homomorphic encryption

Introduction to cloud security

Basic characteristics of information security

- **Privacy** - protecting access to individuals or resources
- **Confidentiality** - assuring that sensitive information is only disclosed with the expressed permission from the sponsor
- **Integrity** - maintaining and assuring the accuracy and consistency of data over its entire life-cycle
- **Availability** - securing that information is accessible when and where it is needed
- **Accountability** - specifying the duties and responsibilities in detail of individuals that work with information systems
- **Auditability** - facilitate the comparison of actual practices in an organisation with the policies and procedures that are defined for the activities
- **Authenticity/Trustworthiness** - ensuring data is genuine and validate that all parties involved are who they claim to be
- **Non-repudiation** - preventing participant from denying sending or receiving a transaction they participated in

Forums and Organisations

- NIST - National Institute of Standards and Technology
- CSA - The Cloud Security Alliance
- OCCI - Open Cloud Computing Interface
- ODCA - Open Data Center Alliance

CSA: Security guidance for cloud computing

1. Cloud computing architectural framework
2. Governance and Enterprise Risk Management
3. Legal Issues: Contracts and Electronic Discovery
4. Compliance and Audit
5. Information Management and Data Security
6. Portability and Interoperability
7. Traditional Security, Business Continuity and Disaster Recovery
8. Data Center Operations
9. Incident Response, Notification and Remediation
10. Application Security
11. Encryption and Key Management
12. Identity and Access Management
13. Virtualization
14. Security as a Service

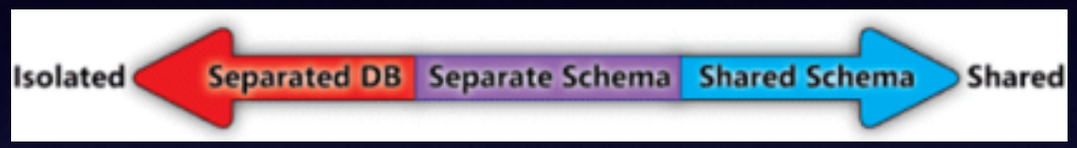
Cloud threats

CSA: The notorious nine: Cloud computing top threats 2013

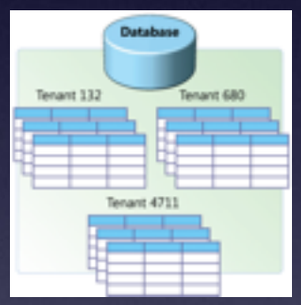
1. Data breaches
2. Data loss
3. Account or service traffic hijacking
4. Insecure interfaces and APIs
5. Denial of service
6. Malicious insiders
7. Abuse of cloud services
8. Insufficient due diligence
9. Shared technology vulnerabilities

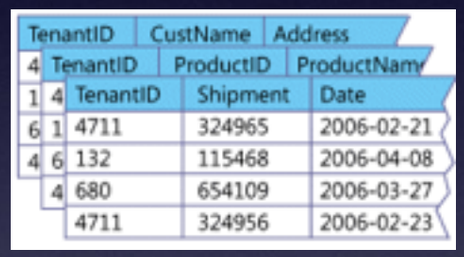
1. Data breaches

Multi-tenant SaaS



”Information leakage”





Cross-VM side channel attacks

- side channel attacks: time-driven, trace-driven, access-driven
- reconstruct private ElGamal key (457-bit exponent) using a 4096 bit modulo
- required a few hours of work

- Cross-VM Side Channels and Their Use to Extract Private Keys
- Multi-Tenant Data Architecture

2. Data loss

- Encrypt data, lose password => game over
- Attacks with data corruption as a goal
- Accidental deletion by cloud service provider
- Physical reason (fire, earthquake,…)
- Really painful…

3. Account or service traffic hijacking

- Phishing
- Fraud
- Zero-day attacks and other SW vulnerabilities
- Cross-site scripting
- Stealing credentials
- Eavesdropping
- Data manipulation, falsified information
- Client re-direction to falsified sites

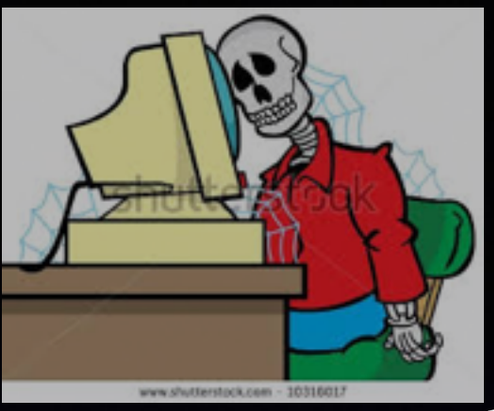
4. Insecure interfaces and APIs

- Used for provisioning, management, orchestration, and monitoring

- Control authentication, access control, encryption, activity monitoring using APIs

- Must be designed to protect against both accidental and malicious attempts to circumvent policy

- Third parties often build upon these interfaces to offer value-added services to their customers => Layered APIs



5. Denial of service

- Objective is to prevent users from accessing their data or applications
- Forces the cloud service to consume inordinate amounts of system resources (CPU, NW BW, memory, disk space,..)
- Results in intolerable slow-down, unresponsive service for legitimate users
- Distributed attacks (DDoS) especially hard to protect against
- Noisy-neighbours - workloads from other tenants gets more than a fair share (unintentionally) of system resources

6. Malicious insiders

- Current or former employee, contractor, or business partner with authorized access to the cloud provider's information system
- Intentionally exceeding and/or misusing the access to harm cloud tenants
- Increased level of user data access from IaaS < PaaS < SaaS

7. Abuse of cloud services

- The cloud is formidable compute platform
- Cost is low, computational power potentially enormous
- Can be used for unsolicited activities, e.g., cracking ecryption keys, DDoS attacks using array of cloud servers, etc.
- An issue for cloud providers rather than cloud customers
- Questions: how to detect, what is abuse, how to prevent

8. Insufficient due diligence

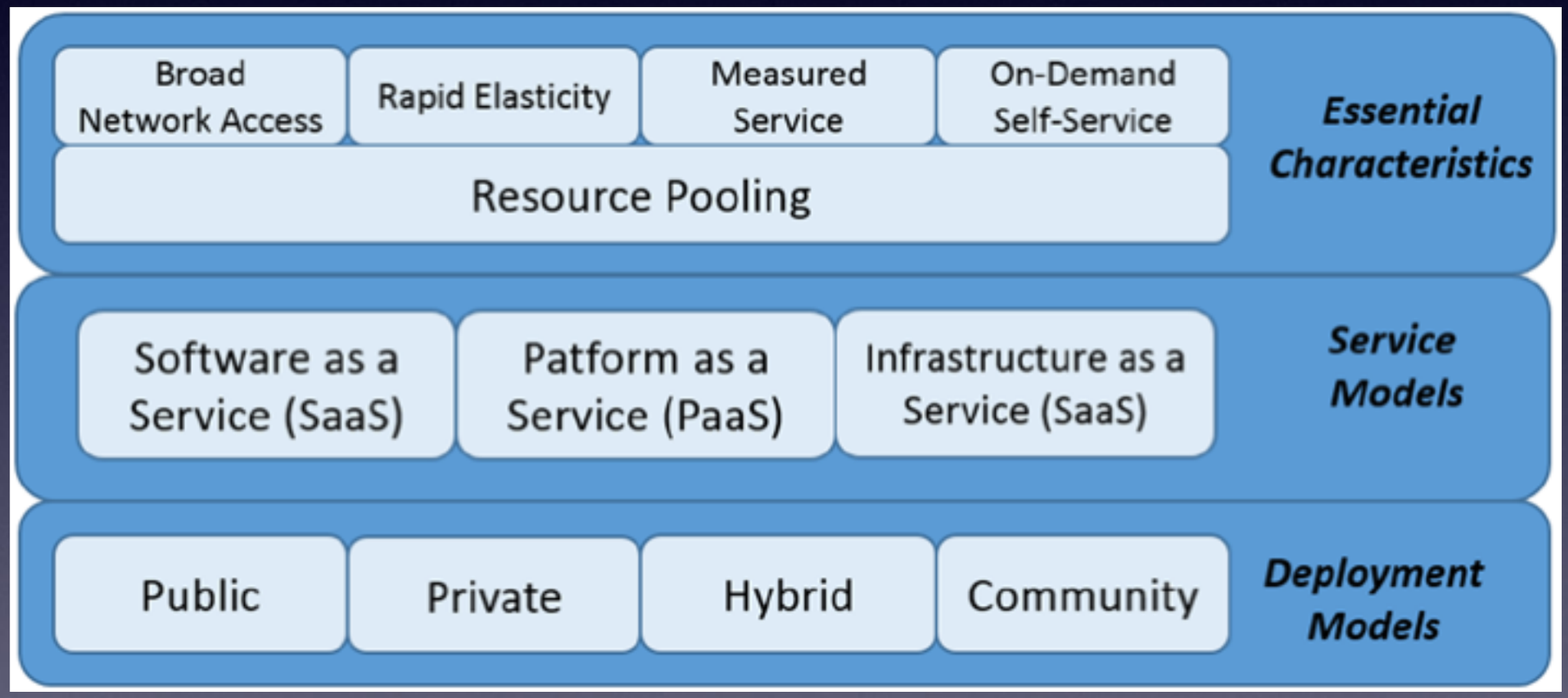
- Organzations move services to cloud without enough understandings of the security implications
- Incident response, encryption, security monitoring has to be handled
- Contractual issues arise over obligations on liability, response, or transparency by creating mismatched expectations between the CSP and the customer
- Pushing applications dependent on traditional enterprise security and control can be risky

9. Shared technology vulnerabilities

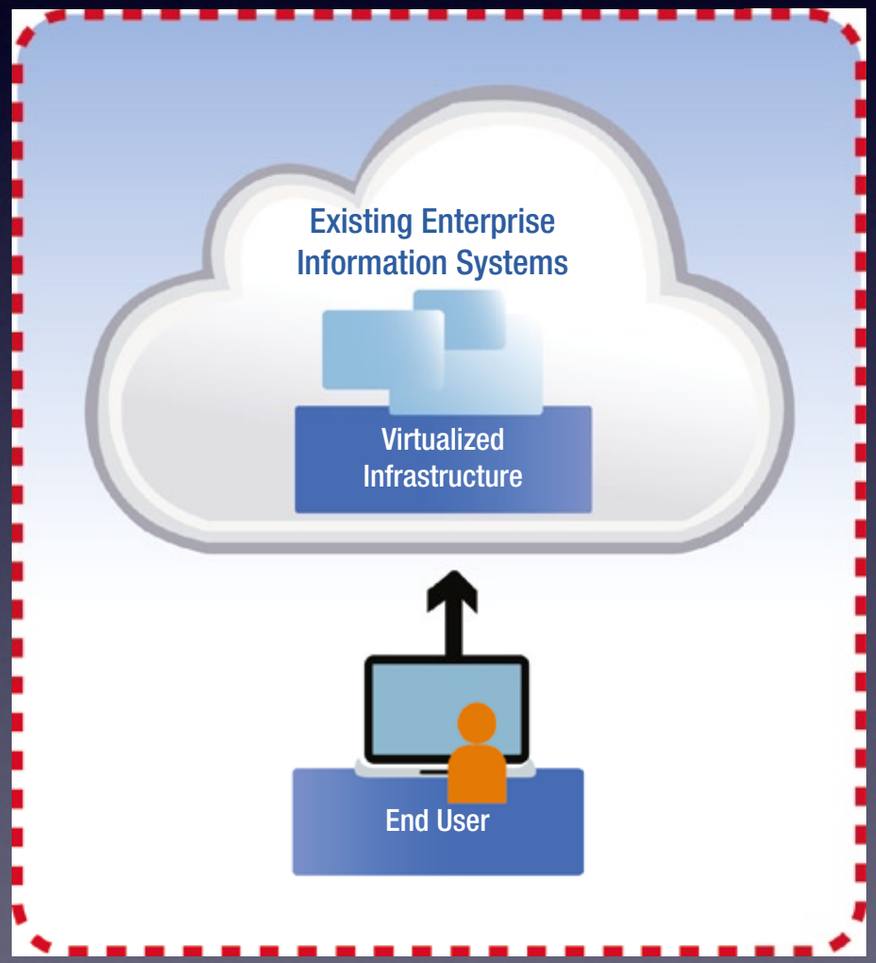
- Compromising one common component affects everything dependent on that component
  - hypervisor
  - shared plaform component
  - application in SaaS
- Break once, run everywhere

Securing the cloud

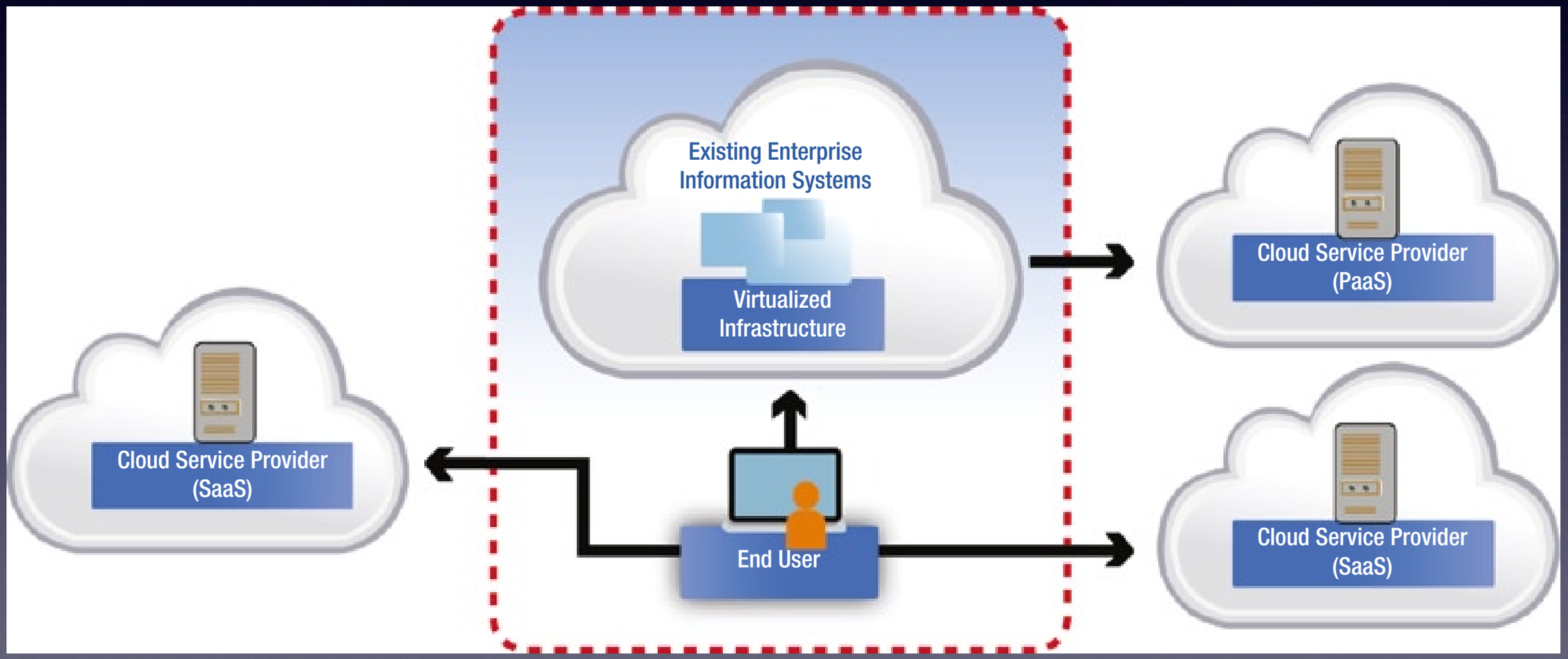
NIST definition of cloud computing



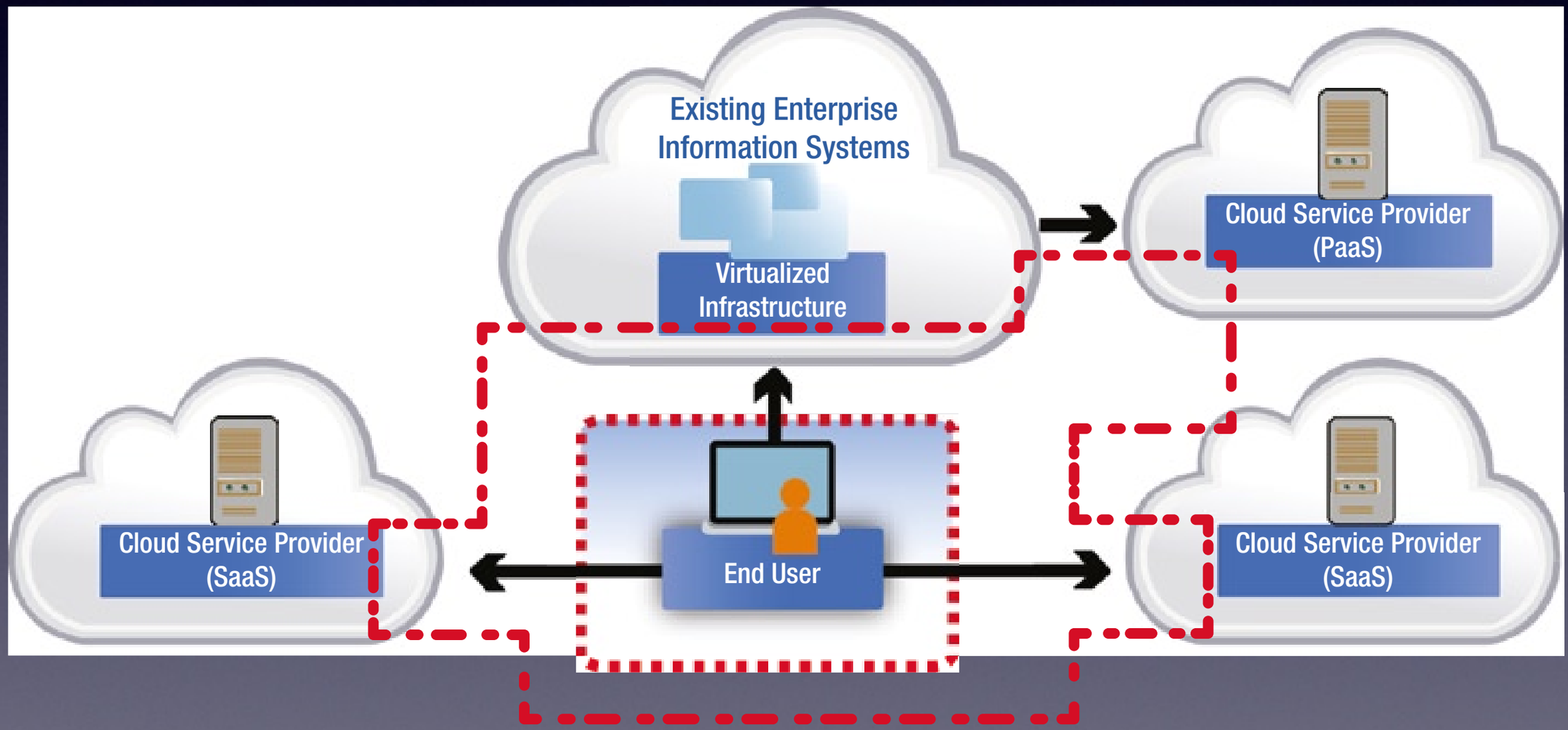
Traditional security perimeter



Hybrid cloud security perimeter



General cloud security perimeter



Trusted cloud

- A trusted computing infrastructure
- A trusted identity and access management
- Trusted software and applications
- Operations and risk management

What is ”trust”

- Assurance that people, data, entities, information, and processes function or behave as expected
- Machine-machine: handshake protocols
- Machine-human: certificate notifications
- Human-human: mutual confidence and faith

What is ”assurance”

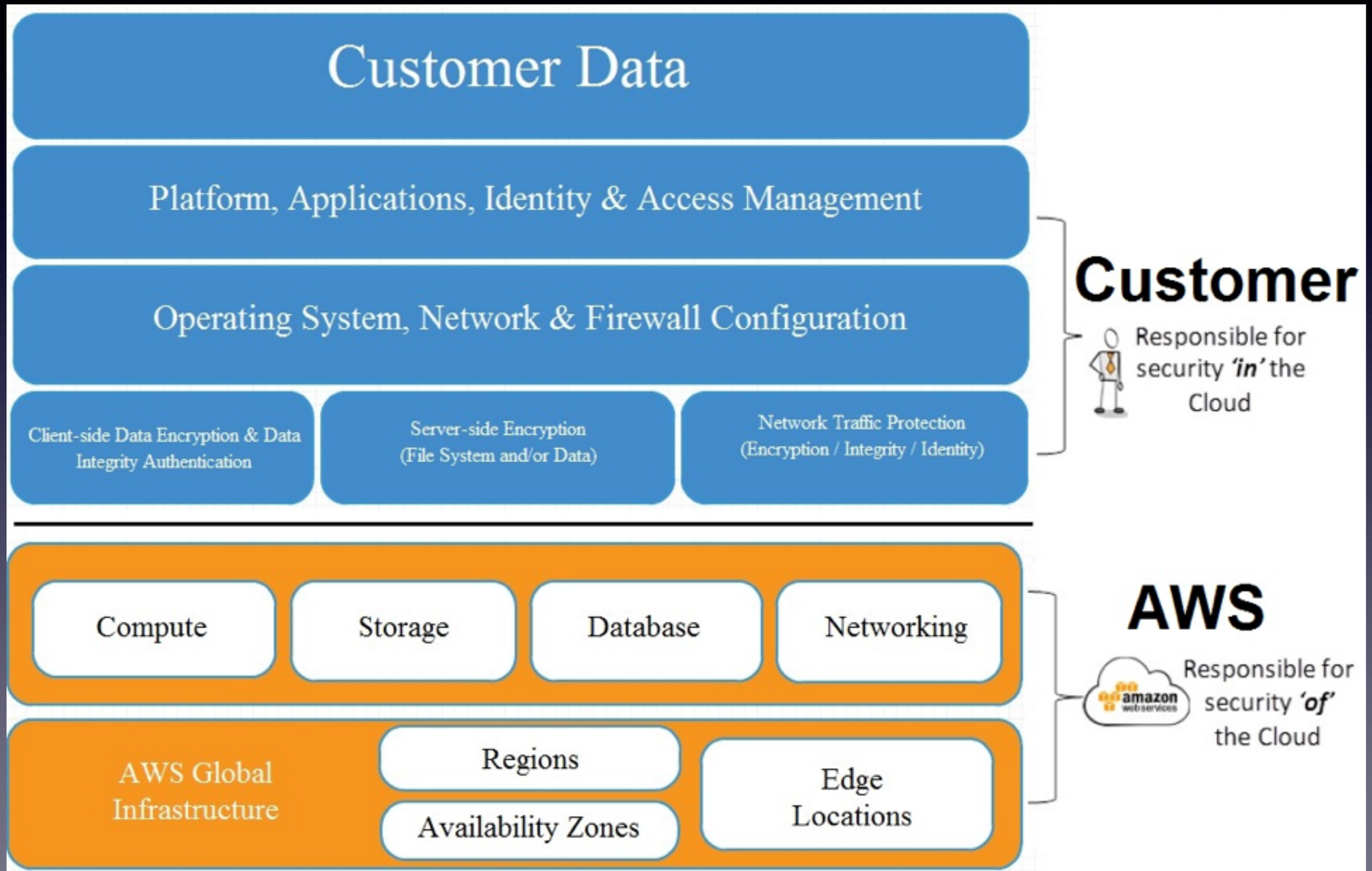
- Evidence of or confidence in that security controls are implemented and effective
- Shown by developers and operators through design, implementation, and maintenance of security measures
- Assessments of the implemented procedures and mechanisms relating to security

CSP compliance

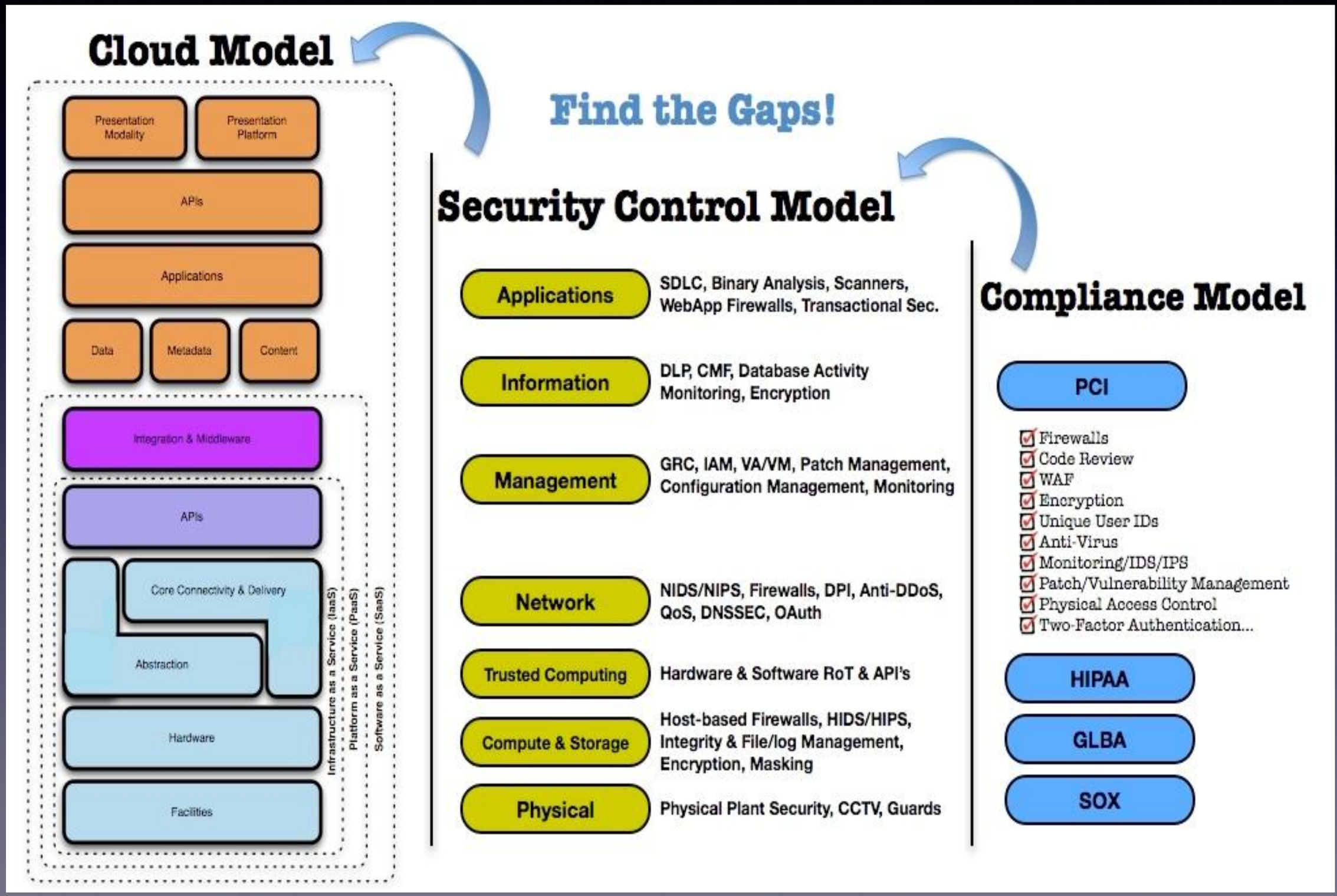
”Amazon Web Services Cloud Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As you build systems on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs; focusing on customer efforts for establishing and operating in an AWS security control environment.”

AWS assurance programs

AWS shared responsibility model



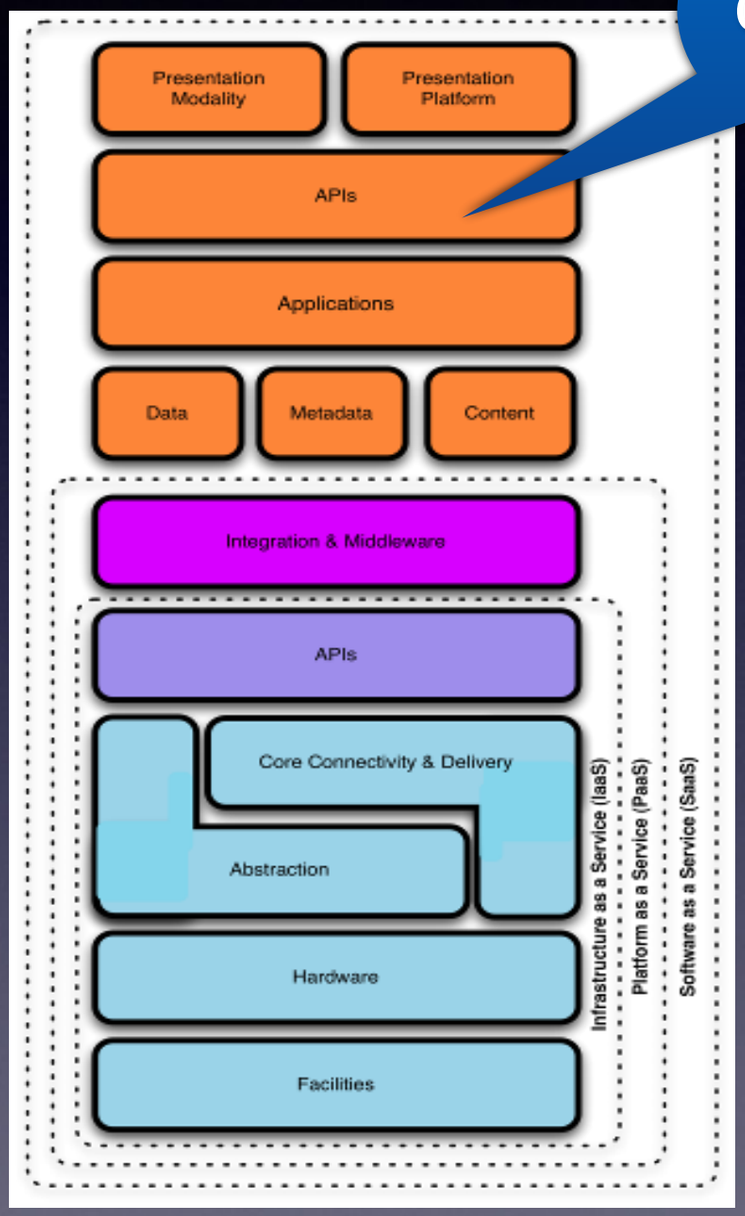
Integrating security (I)



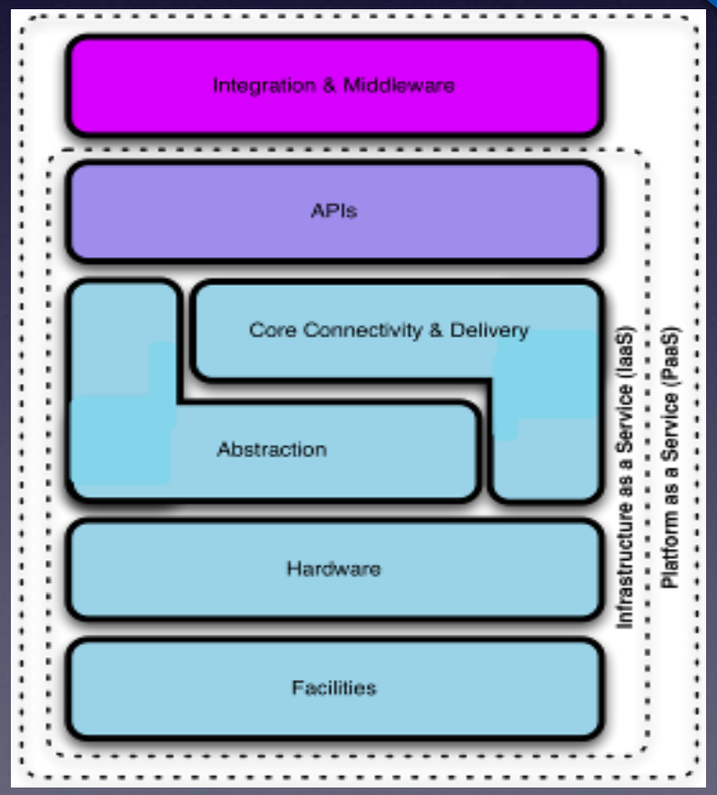
Integrating security (II)

SaaS

Contract it in

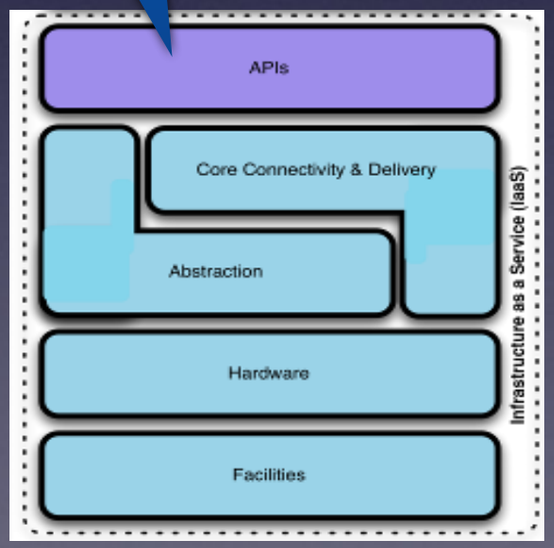


PaaS



You´re on your own

IaaS

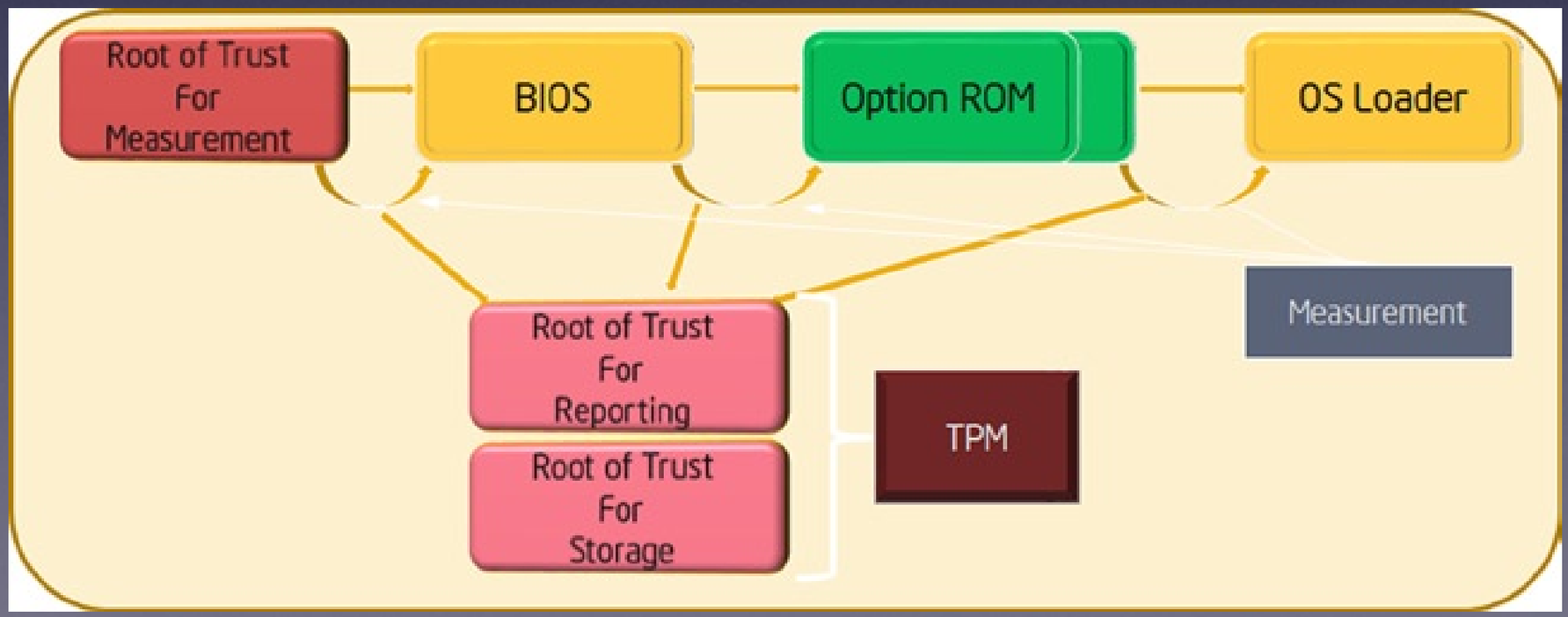


Data center security

A framework for trusted computing

Trusted boot

- Start with a hardware based root-of-trust
- Introduce a chain of trusts extending from boot to hypervisor
- Each piece of code in the boot sequence is verified before it runs



Attestation

- The act of guaranteeing that the launched components are trusted components
- Makes it possible for entities (e.g. resource scheduler of orchestrator) to check that the platform is in an secure state
- An attestation service enables a server to demonstrate its boot integrity
- The TPM computes a digital signature on platform configuration registers. The attestation service validates the signature and compares the values to a known-good reference

Trusted VM

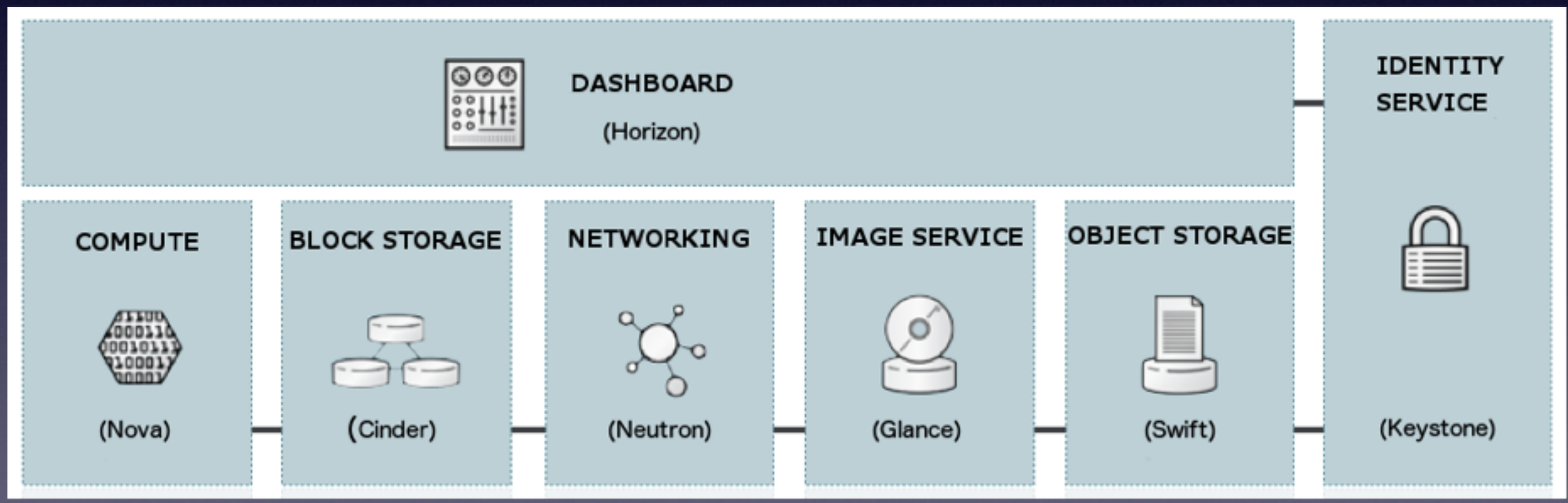
- Boot VM using trusted platform module to ensure integrity of its image
- Access management interface of hypervisor through reserved VLAN
- Isolate traffic to/from guest VMs using different VLANs
- Handle inter-VLAN routing through DC firewall, not using virtual switch in the hypervisor
- Lock down guest VM to only run needed protocols and restrict user privileges
- Secure storage - use encryption and access control

Software-defined security

- Built on top of SDN
- Provide IaaS tenants with means to define their own virtual networks
- No interference with NWs serving the cloud provider or other tenants
- Instantiate security on demand to fulfill specific needs of VM or group of VMs
- Deploy virtual network appliances (FWs, switches, intrusion detection/prevention etc.)
- APIs (to enable control of HW/SW) and Orchestration (invocate several APIs to accomplish a set of tasks)

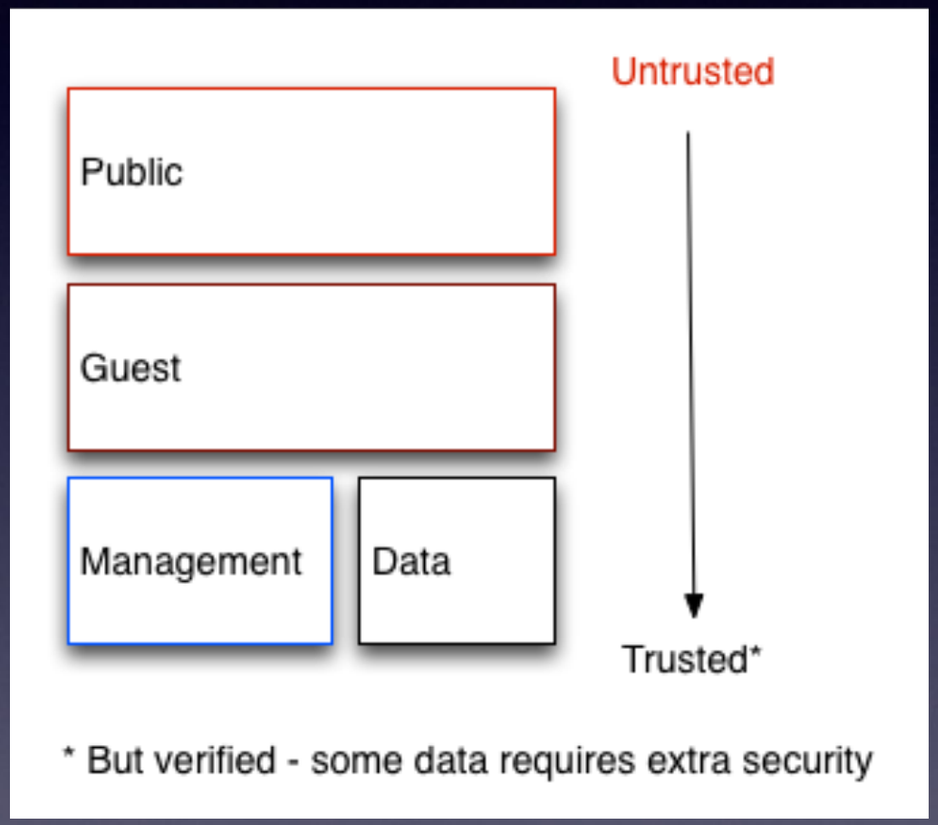
OpenStack security

OpenStack cloud service

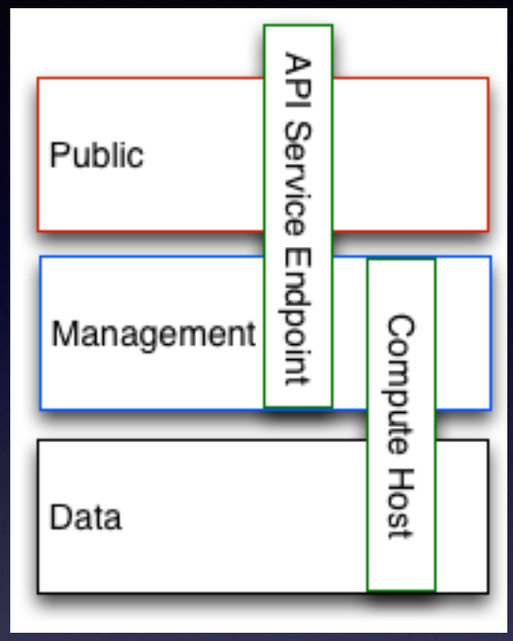


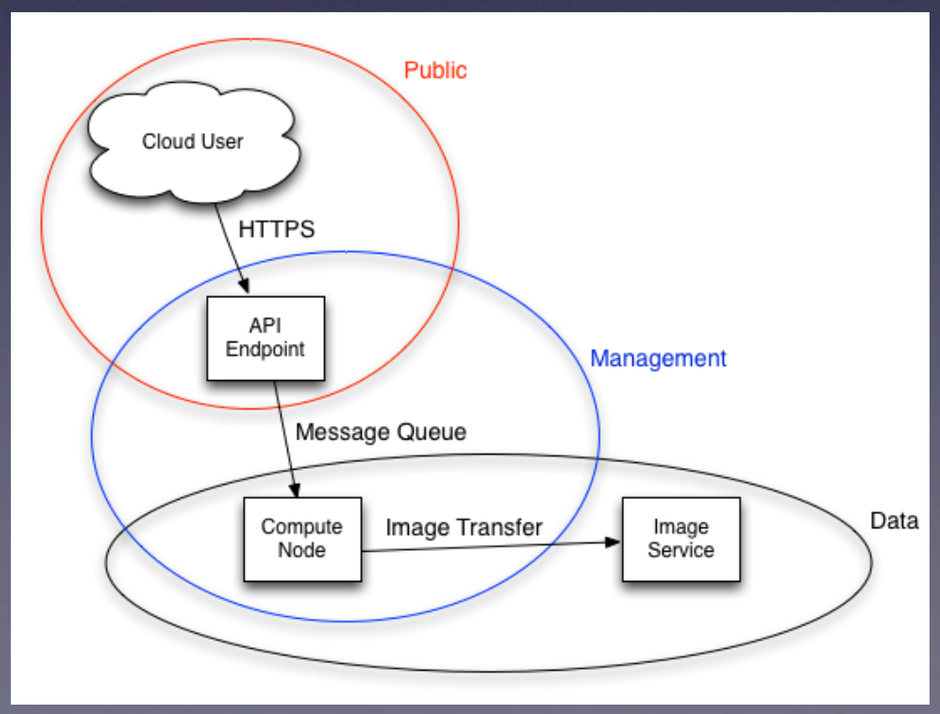
OpenStack security domains

Domains



Bridge





OpenStack network security

- **LB-aaS**: add VM instances to an application pool on a load balancer through API
- **VPN-aaS**: extend tenant's intranet with a virtual network segment from a remote cloud provider
- **FW-aaS**: customize FW rules to match corporate security and compliance requirements
- **VLAN-aaS**: expand the tenant's available cloud network resources

Homorphic encryption

Homomorphic encryption

- Computations carried out on ciphertext
- Deciphered result equivalent to the same computations applied to the plaintext
- Retaining confidentiality while processing data
- Facilitates service chaining without revealing information of the individual stages
- Perfect match for private data residing in public clouds

Partial homomorphic encryption (PHE)

Unpadded RSA: If the public key is (m, e), then the encryption of a message x is given by $E(x) \equiv x^e \pmod{m}$. The homomorphic property is then multiplication of plaintexts

$$E(x_1)E(x_2) \equiv x_1^e x_2^e \pmod{m} \equiv (x_1 x_2)^e \pmod{m} \equiv E(x_1 x_2)$$

Pailler cryptosystem: If the public key is (m, g), then the encryption of a message $x \in \mathbb{Z}_m$ is given by $E(x) \equiv g^x r^m \pmod{m^2}$, where $r \in \mathbb{Z}_m^*$ is a random integer. The homomorphic property is then addition of plaintexts

$$\begin{aligned} E(x_1)E(x_2) &\equiv (g^{x_1} r_1^m)(g^{x_2} r_2^m) \pmod{m^2} \equiv g^{x_1+x_2}(r_1 r_2)^m \pmod{m^2} \\ &\equiv E(x_1 + x_2 \pmod{m}) \end{aligned}$$

Fully homomorphic encryption (FHE)

- Arbitrary computations on the encrypted data is possible, thus any desired functionality can be accomplished working on the ciphertext
- Existence of a FHE scheme unknown for more than 30 years
- Craig Gentry proposed the first fully homomorphic encryption scheme in 2009 based on lattices
- The known FHE schemes are noisy, i.e., each operation on the ciphertext will detoriate it and eventually it cannot be decrypted anymore
- Periodically applying a certain ”bootstrapping” procedure to the ciphertext mitigates the noise problem
- FHE is SLOW!!!

HE malleable by design

Modifying the message is possible without the abiltity to read it:

m = "TRANSFER $0000100.00 TO ACCOUNT #199"

$x = E(m)$

$y = f(x)$, where f is chosen "wisely"

$m' = E^{-1}(y)$

m' = "TRANSFER $1000100.00 TO ACCOUNT #308"

THE END