(ISC)^2 Certified Cloud Security Professional (CCSP) Crash Course

Michael J. Shannon

CISSP, CCSP, CCSK
AWS Certified Security – Specialty,
Cisco CCNP-Security,
Palo Alto PCNSE7,
ITIL 4 Managing Professional

(ISC)² CCSP 2022 Exam

- The exam was “refreshed” in August
- Length of exam: 4 hours
- Number of items: 150
- Item format: Multiple choice
- Passing grade: 700 out of 1000 points
- Exam availability: English, Chinese, German, Japanese, Korean, Spanish
- Testing center: Pearson VUE Testing Center

@iconshock.com

Pearson

CCSP Examination Weights

Domains	Weight
1. Cloud Concepts, Architecture and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk and Compliance	13%
Total:	**100%**

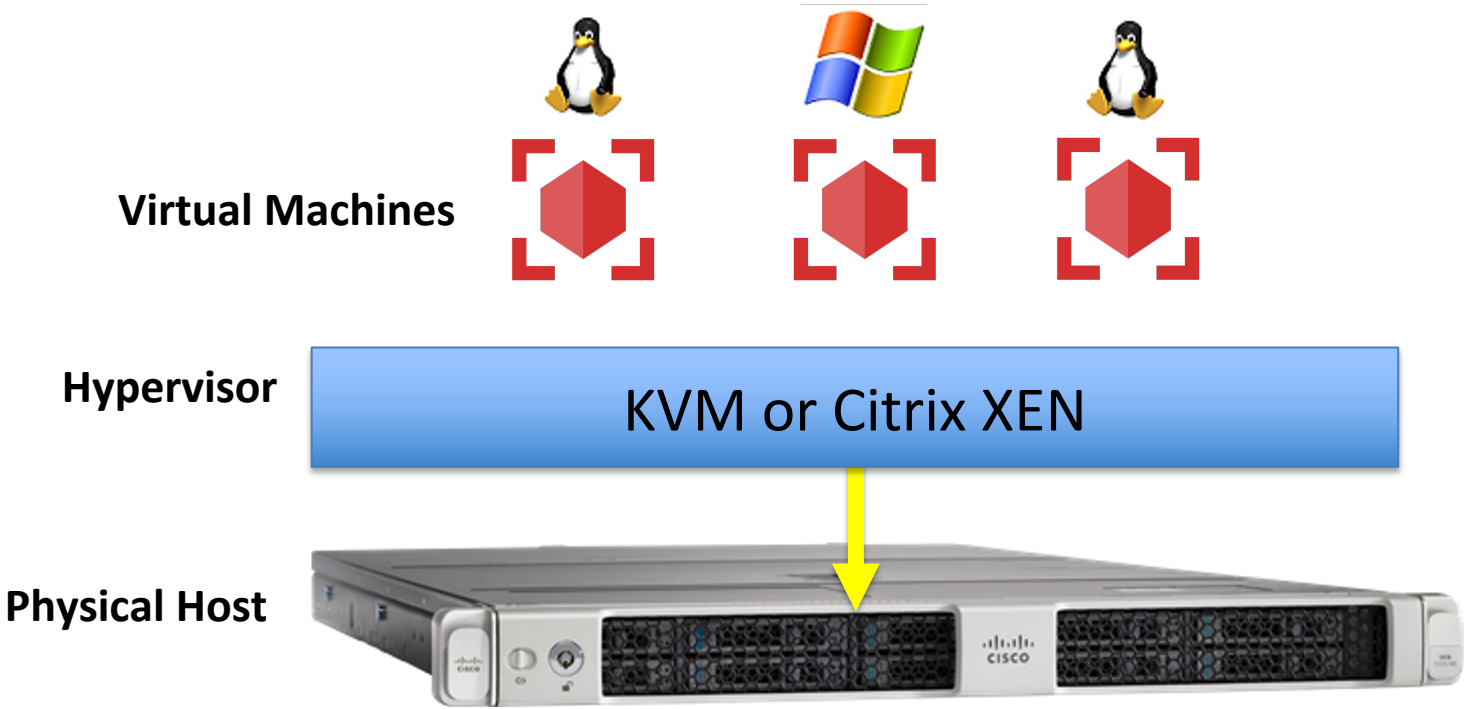
My Exam Insights

- This is an exam developed by CISSPs for CISSPs
- Many questions are simply “re-packaged” CISSP questions
- You must address this from 2 perspectives
  - A large customer (IT Manager) of a Cloud Service Provider
  - A highly privileged security manager of an on-premises private cloud or employee of a CSP
- Although vendor neutral – the exam slants towards AWS and GCP and away from Microsoft Azure
- There is a “best” answer, a close distracter, and two obvious wrong answers

Virtualization Components

- A **hypervisor** (Virtual Machine Manager – VMM) is the software that generates and controls a virtual infrastructure allowing multiple OSs to run simultaneously on a single physical machine
- The system running the hypervisor is called the “host”
- The virtual machines running on the host are “guests”
- Proprietary hypervisors: Hyper-V, vSphere/ESXi, OVM, and FusionSphere
- Open-source hypervisors: KVM, OpenVZ, Red Hat, Xen

Type 1 (Native or Bare Metal)

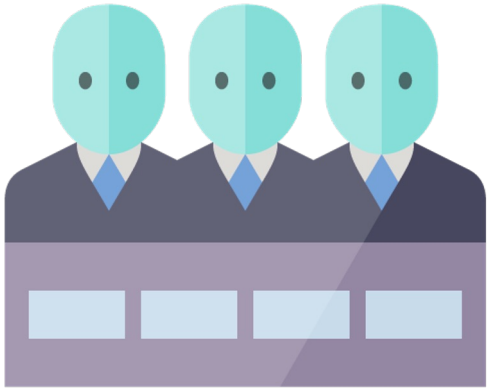


Cloud Computing Roles

- **Cloud Service Customer** (user) – the entity that is paying, leasing, renting, or trying cloud services. Also called the "consumer"
- **Cloud Service Provider** (CSP) – the vendor that is providing the services from their data center, zones, regions, and edge computing locations. Examples: AWS, Rackspace, IBM Cloud, Microsoft Azure, and Google Cloud Platform
- **Cloud Service Partner** – an entity with various partnership agreements with the CSP such as telecoms, broadband providers, Software-as-a-Service providers, and security solution vendors. Example AWS (GuardDuty) and Rapid7

Cloud Computing Roles

- **Cloud Service Broker** – an organization that buys hosting services from a CSP and then re-sells to their own consumers. Example: Direct Connect or ExpressRoute partners of AWS and Azure. Also "CASB"
- **Cloud Auditor** – Typically third-party regulators who are ensuring compliance with frameworks such as PCI-DSS

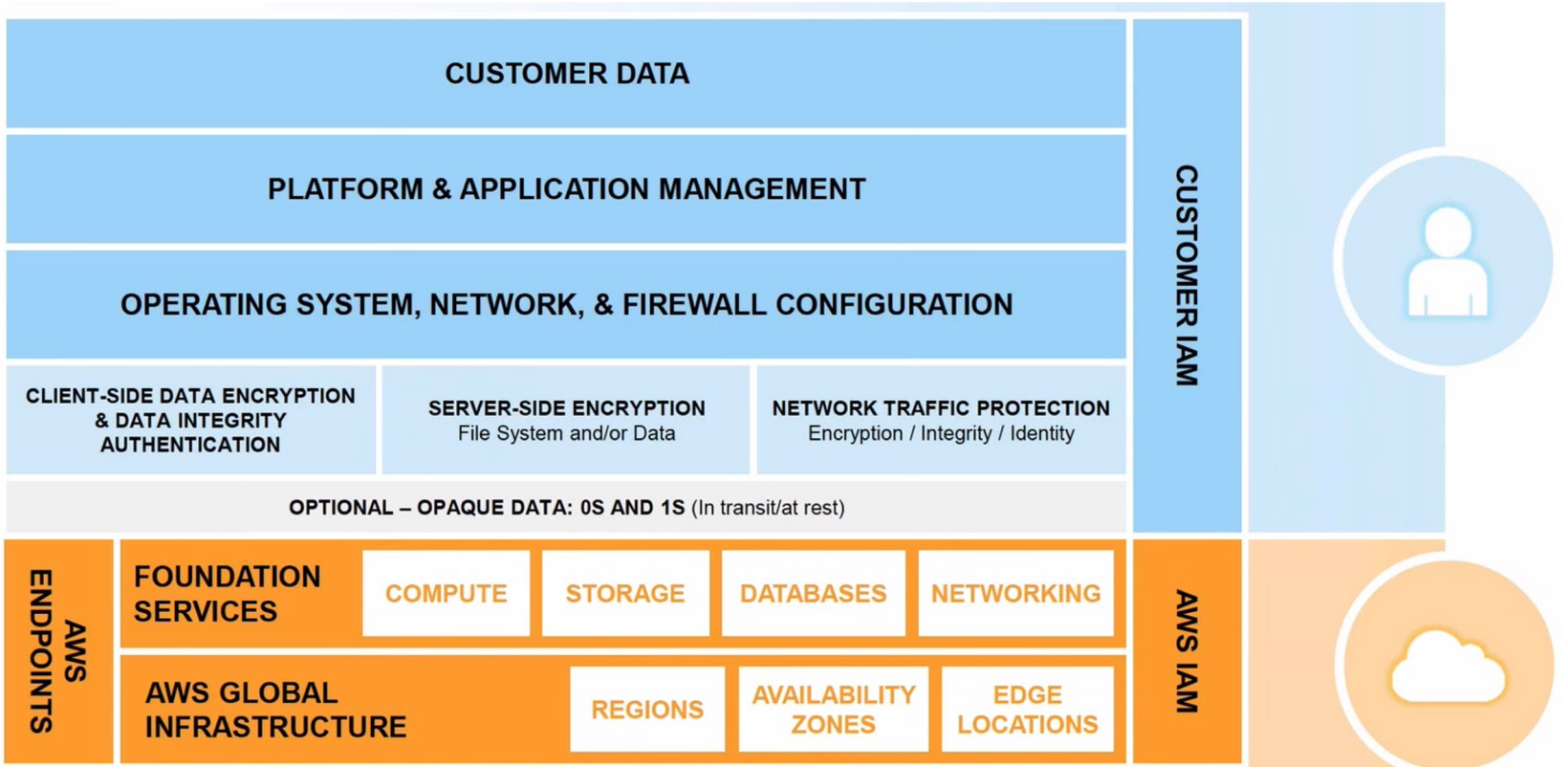


@iconshock.com

Infrastructure-as-a-Service (IaaS)

- **According to NIST**: “Infrastructure-as-a-service is where the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.
  The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)."

Infrastructure as a Service at AWS

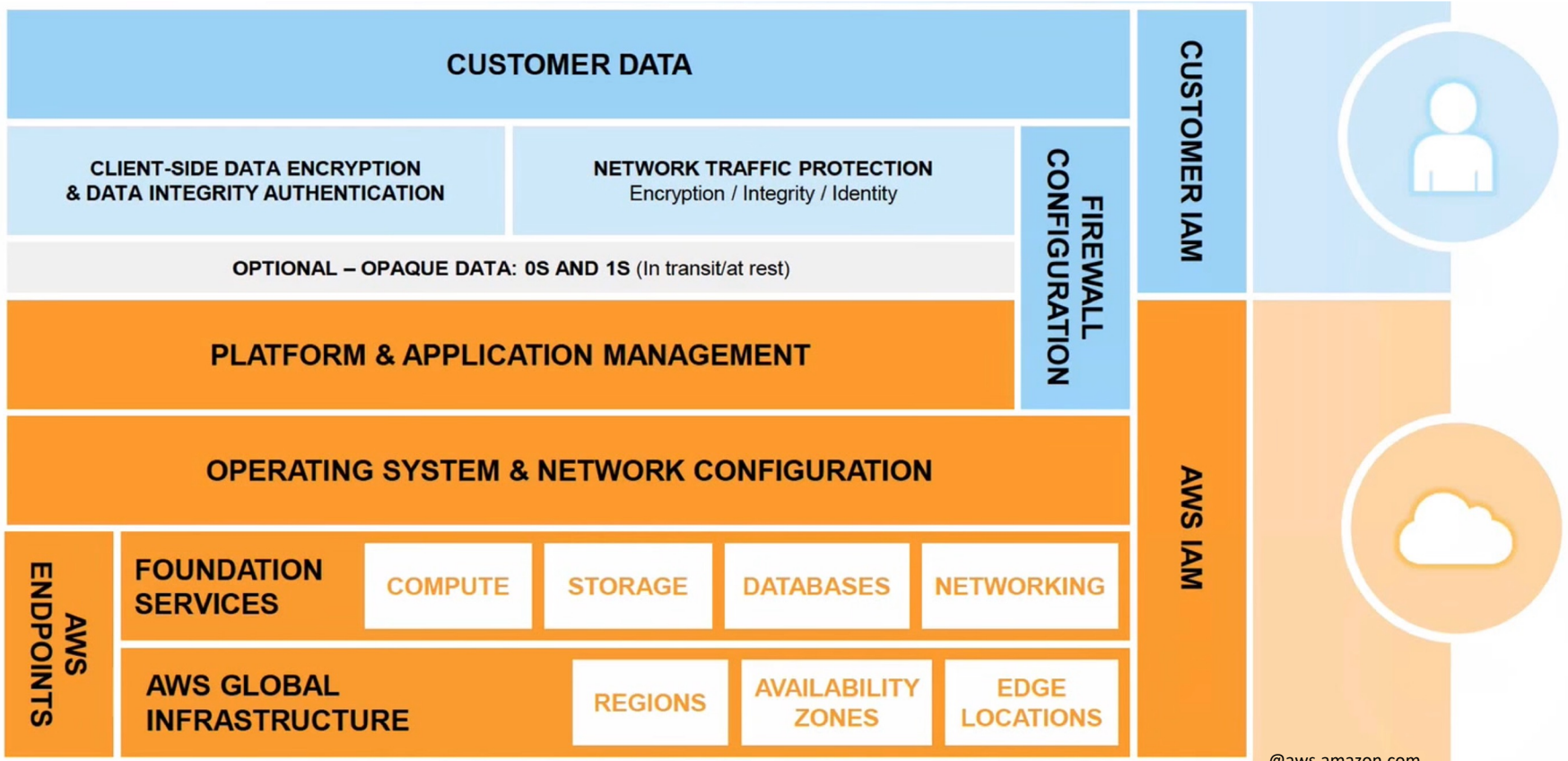


@aws.amazon.com

Platform-as-a-Service (PaaS)

- **According to NIST**: “Platform-as-a-service is the when the provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.
  The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations."

Platform-as-a-Service



Software-as-a-Service (SaaS)

- **According to NIST**: "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

  The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

SaaS Offerings

- Customer Relationship Management
- Enterprise Resource Planning (ERP)
- Community services
- Billing and taxation services
- Analytics services
- Personal storage services
- Security services
- Virtual help desk and call centers

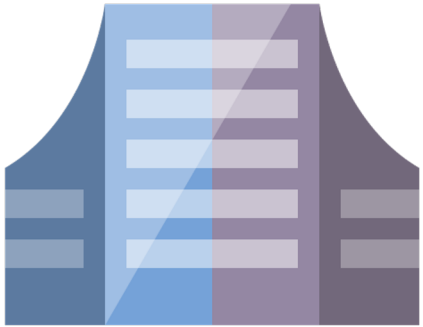
Exam Tip: Vendor Lock-in

- **Vendor lock-in** occurs when a cloud consumer is bound to a certain provider based on application environments, data, systems or other attributes that make portability or vendor changes
- **Software-as-a-Service is the most likely cloud type to suffer vendor lock-in**

@iconshock.com

Public Cloud Deployment Model

- A model where computing resources are owned and operated by a provider and shared across multiple tenants via the Internet or other public networks
- Public cloud makes computing resources available to consumers for purchase and users usually share the use of a public cloud
- Many businesses use a public cloud to scale existing IT resources on demand without having to commit to growing their physical IT infrastructure



@iconshock.com

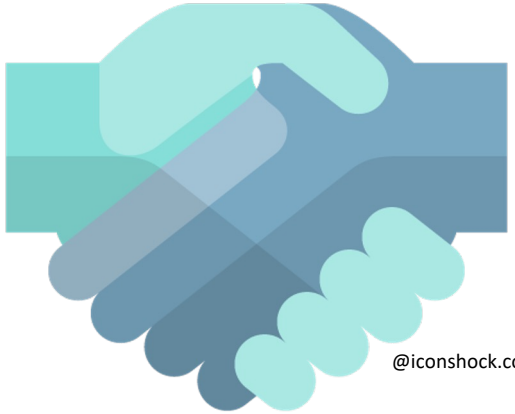
Private Cloud Deployment Model

- A model that is dedicated to a single customer with no other sharing of cloud resources – not a multi-tenant environment
- The private cloud can be a dedicated part of the Cloud Service Provider in a sandbox environment for an additional cost
- The private cloud can be an on-premises solution using virtualization and other cloud service and modern datacenter characteristics

@iconshock.com

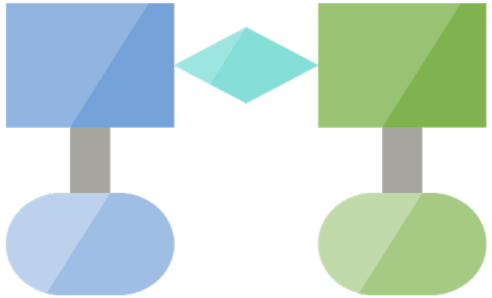
Community Cloud Deployment Model

- A method to connect infrastructure and applications between similar sector entities for public or private use
- Often used to share information and research among parties with various types of agreements and cooperative relationships
- Common examples are:
  - Government agencies and departments
  - Healthcare provider networks
  - Gaming communities
  - Insurance holding companies
  - Financial services companies



Hybrid Cloud Deployment Model

- Technically a combination of private, public, and/or community cloud deployments
- Can also be a method for connecting infrastructure and applications between cloud-based resources and other resources that are not placed in the cloud
- The most common type of hybrid deployment is between the provider's Public cloud and a standing on-premises enterprise Private cloud



Hybrid Cloud Deployment

- Example: suppose that an organization wants to use cloud services to automate batch data processing and analytics
- In a hybrid deployment, the company would be able to keep the legacy applications on premises while benefiting from the data and analytics services that run in the cloud
- Often involves “Bursting Up” to the cloud as needed
- **Exam Tip: Simply using SaaS solutions does not make it a hybrid.**

Multi-cloud Deployment

- Multi-cloud is a cloud computing model where an enterprise leverages a combination of clouds (two or more public clouds, two or more private clouds, or a combination of public, private and edge clouds) to distribute applications and services and:
  - Accelerate app transformation and the delivery of new apps
  - Avoid vendor lock-in and ensure enterprise sovereignty: Total cloud spend, data sovereignty, vendor dependencies and lock-in are increasing concerns

Multi-cloud Deployment (cont.)

- Distribute applications and services to the edge in industries such as logistics, retail and manufacturing, the next generation of gains in automation, efficiency and improved customer experiences require applications to be distributed to the edge, closer to physical devices and users
- Support the rise of the distributed workforce that secure and manage users and their devices in the new hybrid workforce challenge

Cloud Design Patterns

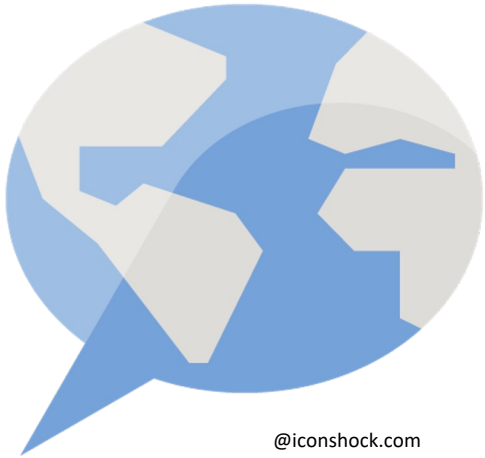
- SANS security principles
- AWS Well-Architected Framework
- Cloud Security Alliance (CSA) Enterprise Architecture

Example: AWS Global Infrastructure

The AWS Virginia Region has 6 Availability Zones – each with at least 2 datacenters - and there are 3 Edge Locations in Ashburn VA

Choosing the Right Region

- When selecting the proper Region for your services, data, and applications, consider the following 4 business factors:
  - Compliance with data governance and legal requirements
  - Proximity to your customers
  - Available services within a Region
  - Pricing



@iconshock.com

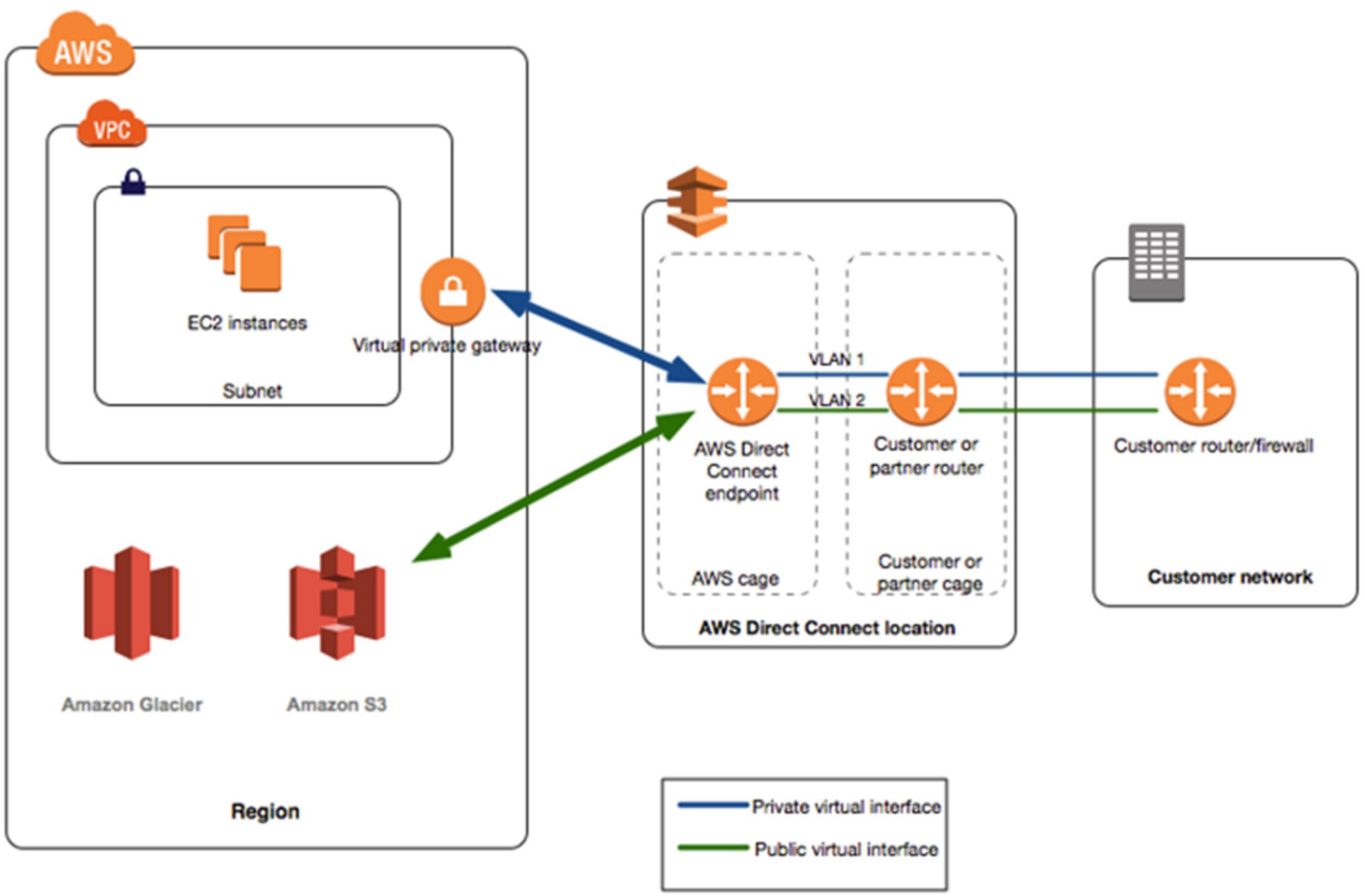
Impact of Related Technologies

- Data science
- Machine learning
- Artificial intelligence (AI)
- Blockchain
- Internet of Things (IoT)
- Containers
- Quantum computing
- Edge computing
- Confidential computing
- DevSecOps
- Ephemeral computing
- Serverless technology

Edge Computing

- Edge computing is a distributed computing standard that brings compute services and data storage close to the site where it is needed to speed up response times and preserve bandwidth
- CDN solutions place cached versions of content (often in elastic Redis in-memory storage clusters) at metro area edge locations
- Security is a shared responsibility model between customers, ISPs, and CDN providers
- **Edge computing can also be characterized by using direct solutions like AWS Direct Connect, Azure ExpressRoute, and Google Interconnect**

Edge Computing



Confidential Computing

- **Confidential Computing** is a Private Cloud built within a Public Cloud Infrastructure
- Applications, data, and workloads within a Confidential Cloud deployment are protected by a blend of hardware-grade encryption, memory isolation, and other services that assure workload, data, and platform integrity
- Confidential Clouds are typically created on-demand at runtime and the workloads and data function completely masked from insiders, bad actors, and malicious processes
- All aspects of a workload are secure even in the event of a physical host breach

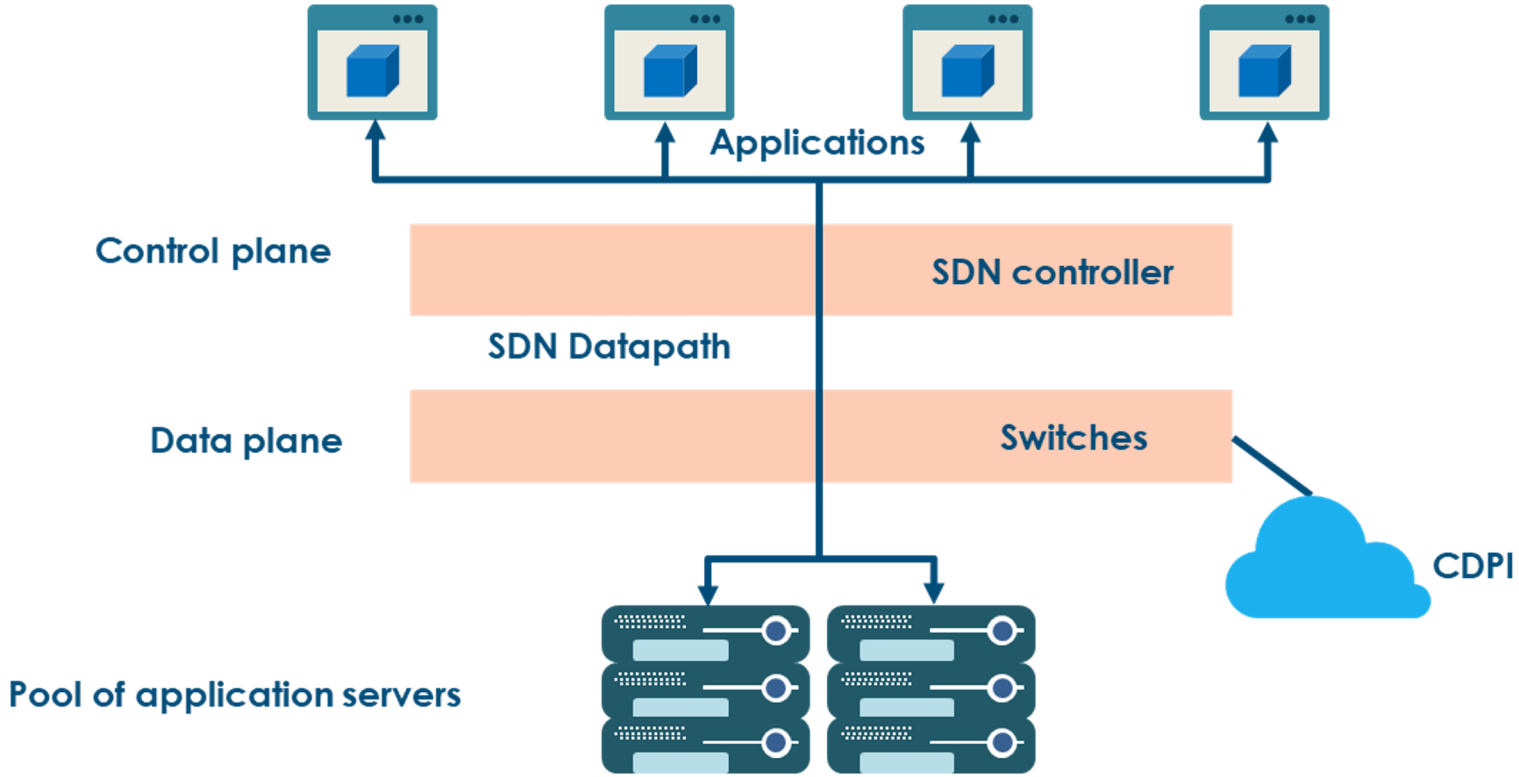
Ephemeral Computing

- Ephemeral computing is the process of creating a virtual computing environment on an ad-hoc temporary basis and then disposing of the environment when necessary or the resources are no longer in demand
- The consumer only pays for what is used
- Examples would be functions-as-a-service with AWS Lambda and Azure Functions

Serverless Technology

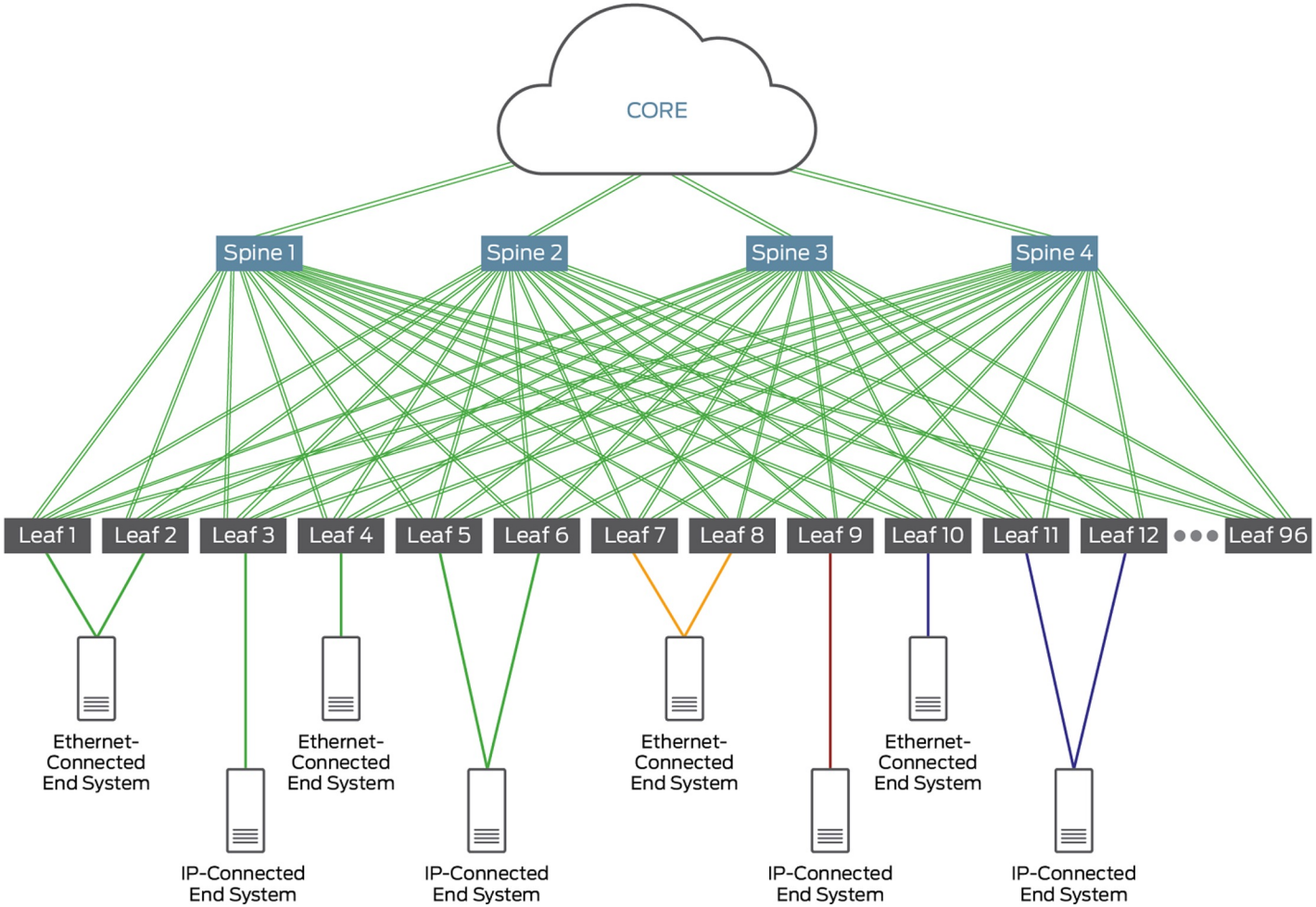
- Functions are a form of serverless technology
- These are technologies for running code, managing data, and integrating applications, all without managing Windows, Linux, and MacOS servers
- Serverless technologies feature automatic scaling, built-in high availability, and a pay-for-use billing model to increase agility and optimize costs

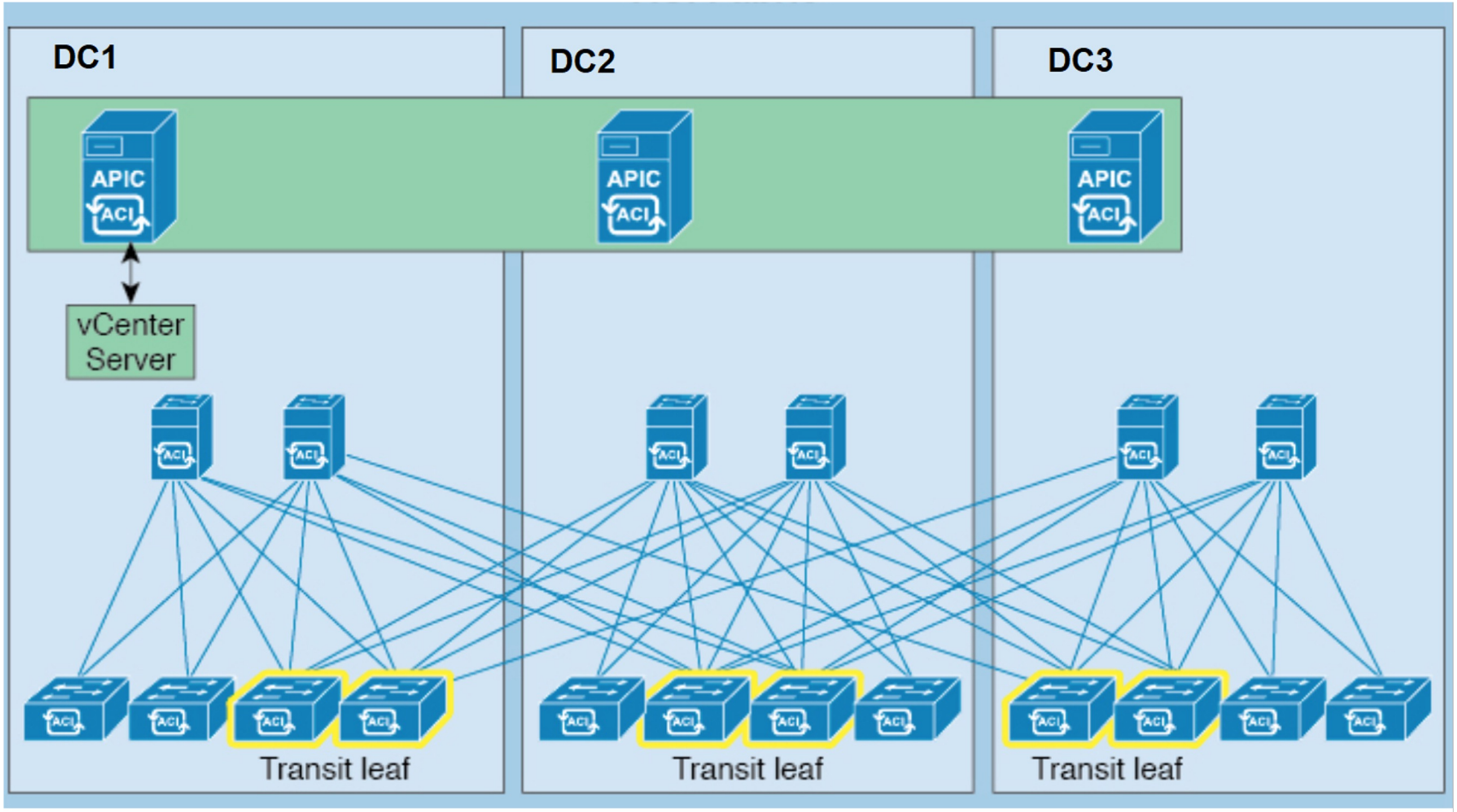
Software-Defined Networking (SDN)



VXLAN

- VXLAN can be described as an encapsulation protocol that connects the data center devices using tunneling to stretch Layer 2 connections over an underlying Layer 3 network
- VXLAN products come from a variety of vendors (Cisco is dominant) and decouples the physical hardware from the network map to support virtualization
  - The uncoupling allows the data center network to be deployed programmatically and fully separate planes
- VXLAN addresses the needs of multi-tenant data centers by offering the necessary scalable and secure segmentation


CORE
Spine 1
Spine 2
Spine 3
Spine 4
Leaf 1
Leaf 2
Leaf 3
Leaf 4
Leaf 5
Leaf 6
Leaf 7
Leaf 8
Leaf 9
Leaf 10
Leaf 11
Leaf 12
Leaf 96
Ethernet-Connected End System
IP-Connected End System
Ethernet-Connected End System
IP-Connected End System
Ethernet-Connected End System
IP-Connected End System
Ethernet-Connected End System
IP-Connected End System



CSP Availability Zone

Software-defined Security (SDS)

- SDS delivers highly controlled and secure environments often using virtualization
- Network security device functionality (next-gen firewalls, IDS/IPS, EDR, IdM) and segmentation are removed from hardware devices and moved to a software layer
  - IT infrastructure security services transition from hardware based to a software-defined solution
- SDS leverages the software-defined networking (SDN) initiative to enhance network security

Advantages of SDS

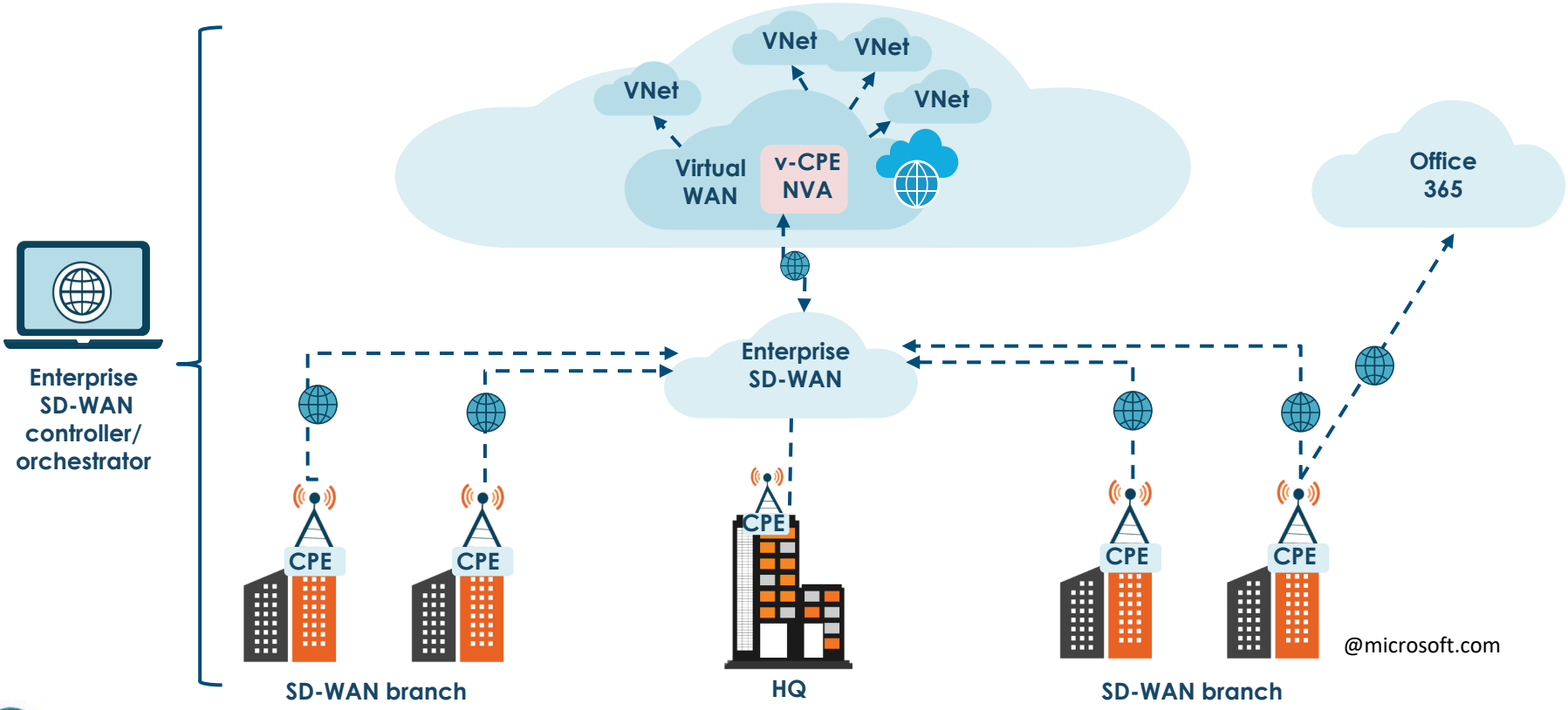
- Vigorous mitigation against security exploits
- Separates security from traditional hardware vulnerabilities
- Automated configuration allows for rapid countermeasures against zero-day attacks
- Provides a coordinated view of logical security policies that exist within the SDN controller model
- Integration with emerging technology to correlate events in a simpler way and respond more efficiently and intelligently to threats
- Facilitates Zero Trust for IoT & BYOD connectivity and security

SD-WAN (SD-MAN)

- An SDN approach that moves network traffic management away from the hardware and premises to next-generation software in the cloud for superior agility, control, and visibility
- Commonly used with Cloud Providers in metropolitan area solutions
- Incorporates a centralized control function with user-defined application and routing policies to deliver highly secure, robust, application-aware network traffic management

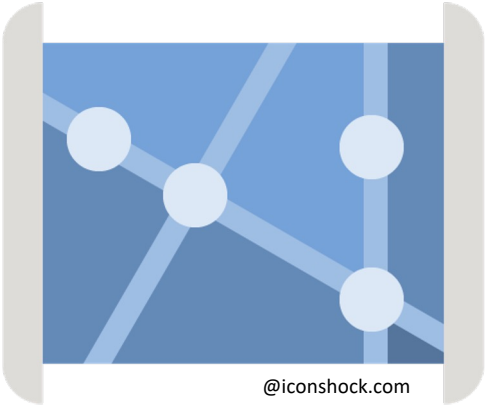
@iconshock.com

Microsoft Azure SD-WAN Solution



Securing Distributed Systems

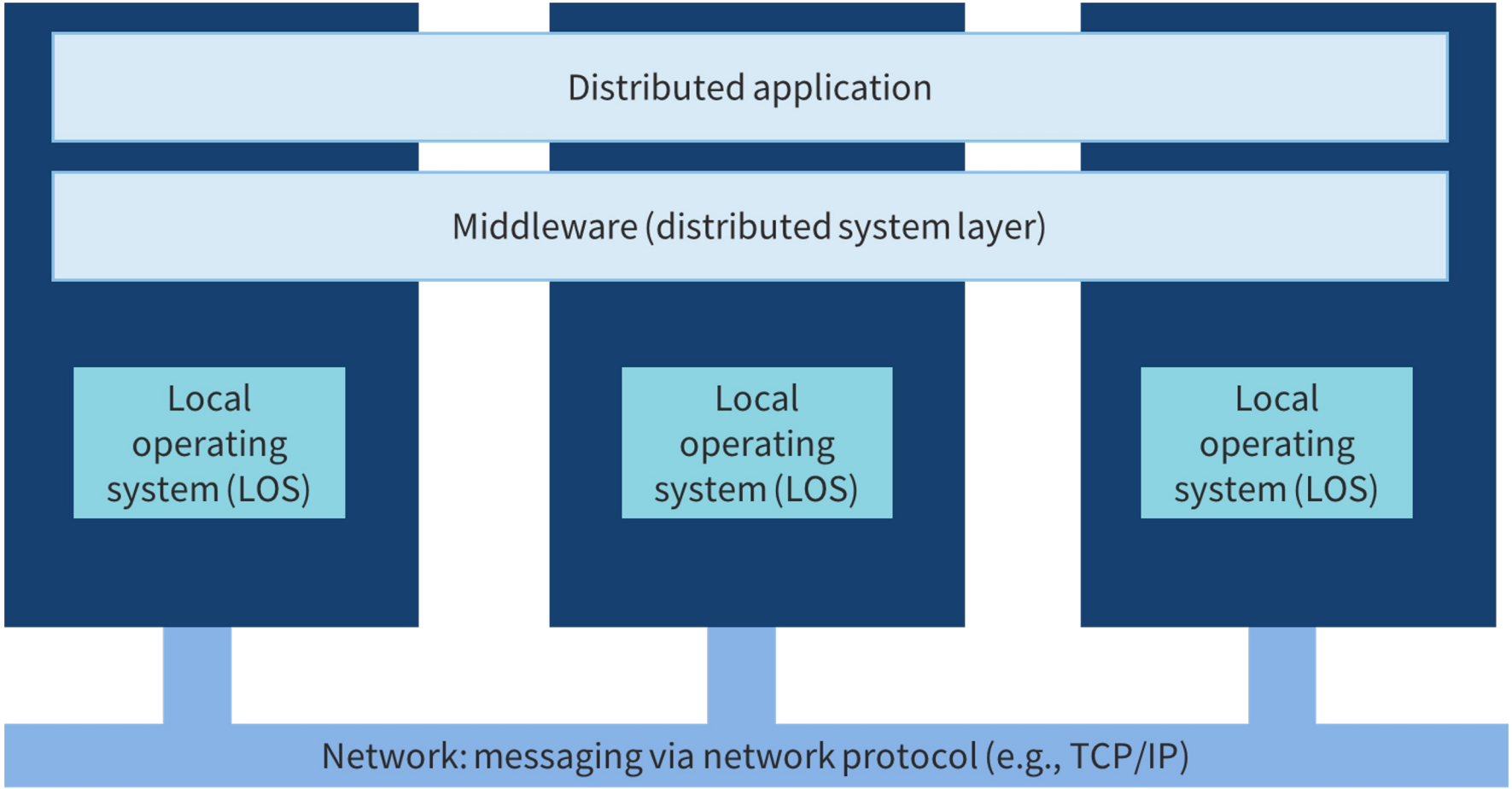
- Traditional distributed systems generally need more security actions than centralized systems, as there are many users, differentiated data, multiple sites, and distributed control
  - Blockchain would be an exception when implemented in a well-tested environment
- Security engineers must consider many permutations of failures and errors that can happen at any time, independently or in combination with other error conditions



Securing Distributed Systems

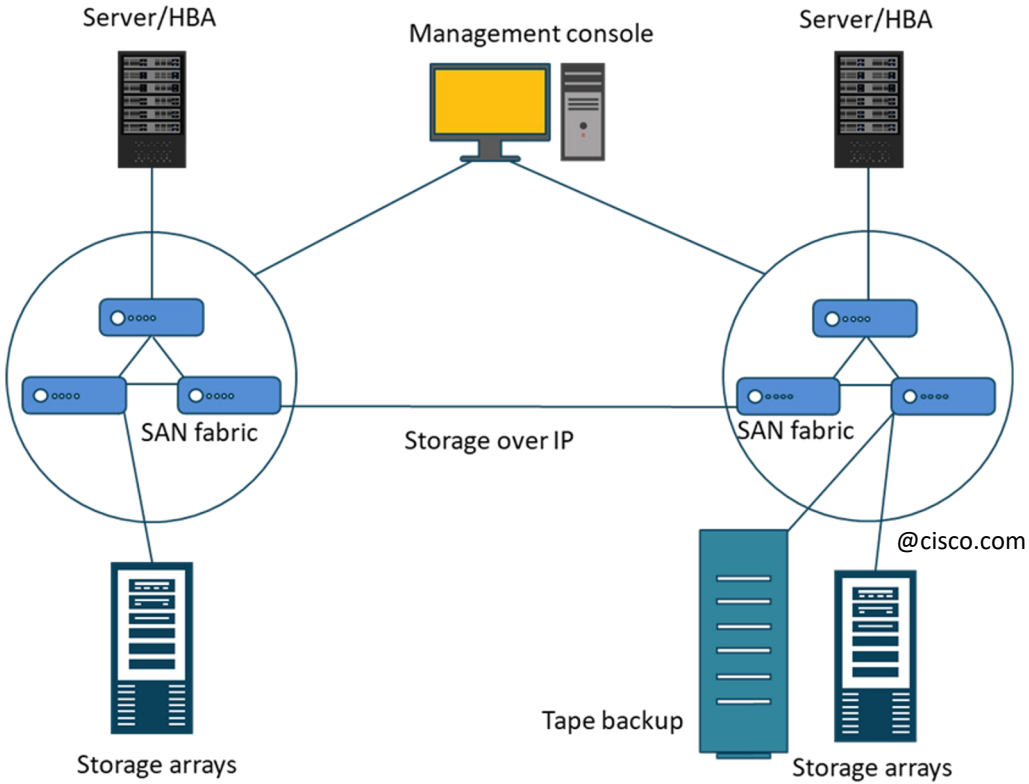
- Common exploits found in distributed communication systems:
  - Passive eavesdroppers monitor messages and gather private information (leakage)
  - Active attackers that further corrupt messages by inserting new data or modifying existing data
  - Distributed Denial of Service (DDoS) and botnets
  - Unauthorized access through poor access controls

@iconshock.com


Distributed application
Middleware (distributed system layer)
Local operating system (LOS)
Local operating system (LOS)
Local operating system (LOS)
Network: messaging via network protocol (e.g., TCP/IP)

Securing the Storage Area Network

- Zero Trust Architecture
- Consider IPsec AH for integrity and origin authentication
- 802.11AE (MACsec) can provide encryption and more on the SAN frames
- Use SDN controllers for management
- Harden all switches and servers
- Encrypt data at rest with AES-256-GCM



Availability vs. Durability

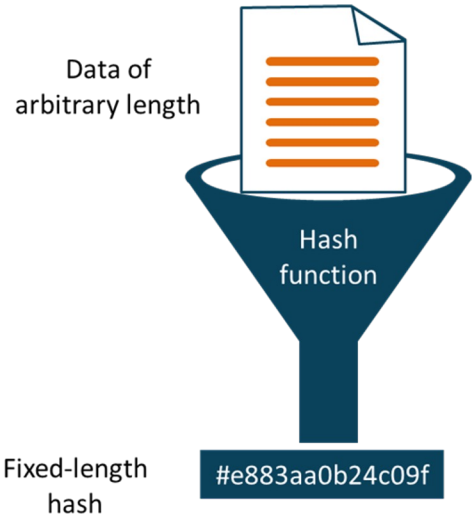
- **Availability** refers to system uptime (i.e., the storage system is operational and can deliver data upon request)
  - Historically, this has been achieved through hardware redundancy so that if any component fails, access to data will remain
- **Durability**, on the other hand, refers to long-term data protection (i.e., the stored data does not suffer from bit rot, degradation or other corruption)
  - Rather than focusing on hardware redundancy, it is concerned with data redundancy so that data is never lost or compromised

Cryptographic Services

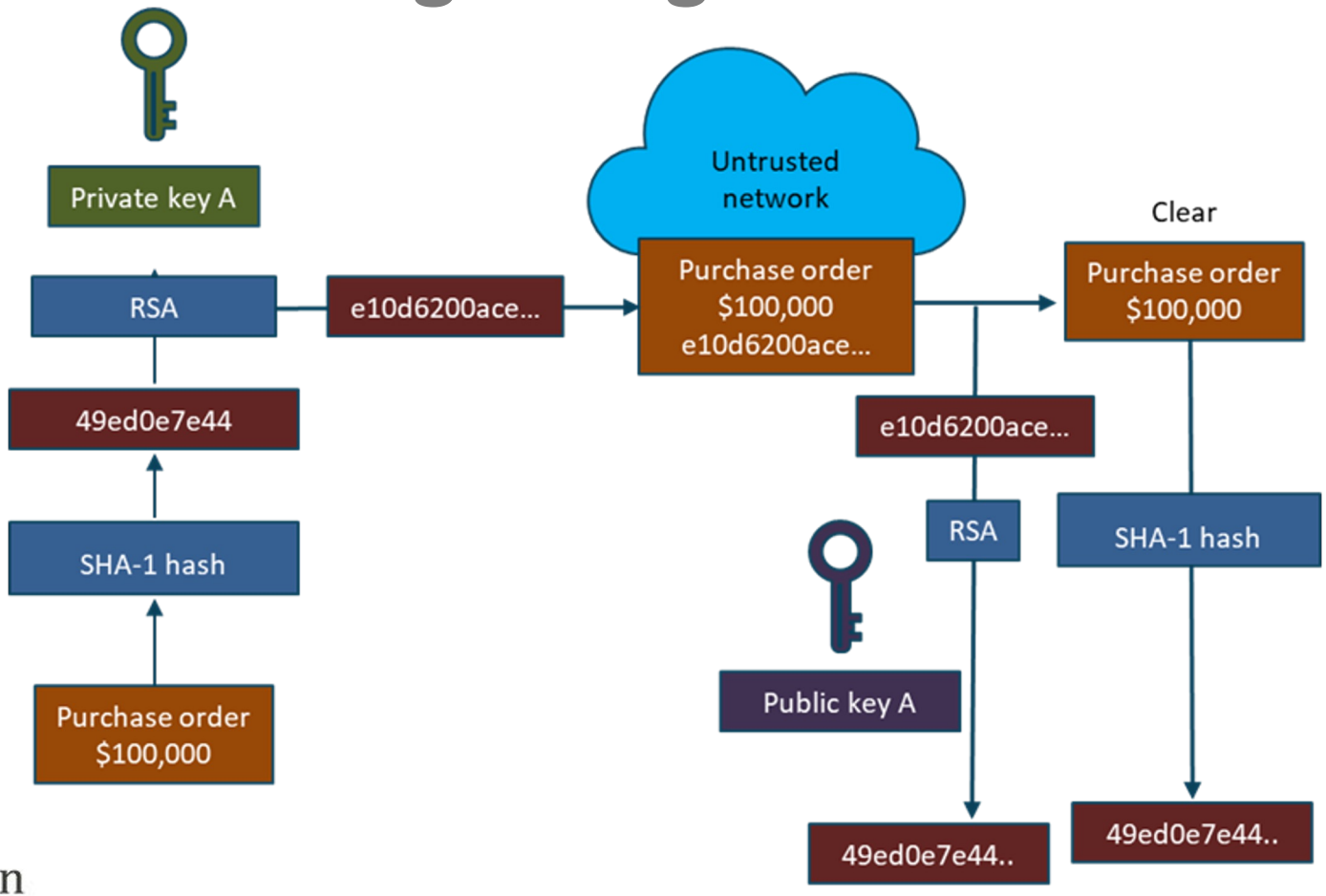
- Confidentiality
  - Hiding the data at rest, in transit, and in use from unauthorized entities
- Integrity
  - Ensures the data has not been altered while at rest or in transit
- Authenticity
  - Cryptographic controls that involve origin authentication and identity
- Non-repudiation
  - Ensures original sender cannot deny sending data or engaging in a digital transaction
  - Common to use digital certificates and digital signing

Cryptographic Services

- Symmetric key cryptosystems
  - For bulk data, 40 to 512-bit keys, protects data-at-rest at CSP, AES-CBC and AES-GCM
- Asymmetric key systems (public/private pairs)
  - Commonly RSA, DSA, ECDSA key pairs, 1026 to 4096-bit, highly scalable with PKI, used for privacy, origin authentication, digital signatures and key exchange
- Cryptographic hashing
  - fingerprinting, password storage, HMACs (origin authentication + integrity), non-repudiation with digital signatures (SHA-2, SHA-3, RIPEMD)



Digital Signatures



Cryptographic Best Practices

- Use elliptic curve (ECDSA) and ephemeral protocol suites (IKEv2) when protecting data in transit
- Digitally sign all external API calls to cloud resources
- Never embed cryptographic keys in the API or in a code repository
- Use the most recent TLS instead of SSL
- Use CloudHSM and Cloud Key management if compliant
- AES-GCM-256 is an Authenticated Encryptor Authenticated Decryptor (AEAD) that does not need a separate HMAC
- Consider DNSSEC and **HSTS** on web servers (Cisco Umbrella)

HTTP Strict-Transport-Security (HSTS)

- If a web site accepts an HTTP connection and redirects it to HTTPS, users may initially access the non-encrypted version of the site before being redirected
- This creates a vulnerability to man-in-the-middle attacks, as the redirect can be exploited to direct users to a malicious site instead of the secure version of the original site
- HTTP Strict-Transport-Security (HSTS) allows a TLS web site to instruct browsers that it should only be accessed using HTTPS, instead of using HTTP
- The web server employs the HTTP Strict-Transport-Security header

Key Management

- CSP key management is client-side, server-side, or KMS
- Removing keys from operation:
  - Destruction - removes an instance of a key in one of the permissible key forms at a specific location
  - Deletion – also removes an instance of a key, plus any data from which the key may be reconstructed
  - Termination - All instances and information of the key are completely removed from all locations, making it impossible to regenerate or reconstruct the key
  - **Crypto-shredding (cryptographic erasure) - is the singular pragmatic option for disposal of keys and data/media in the cloud**

Access Control

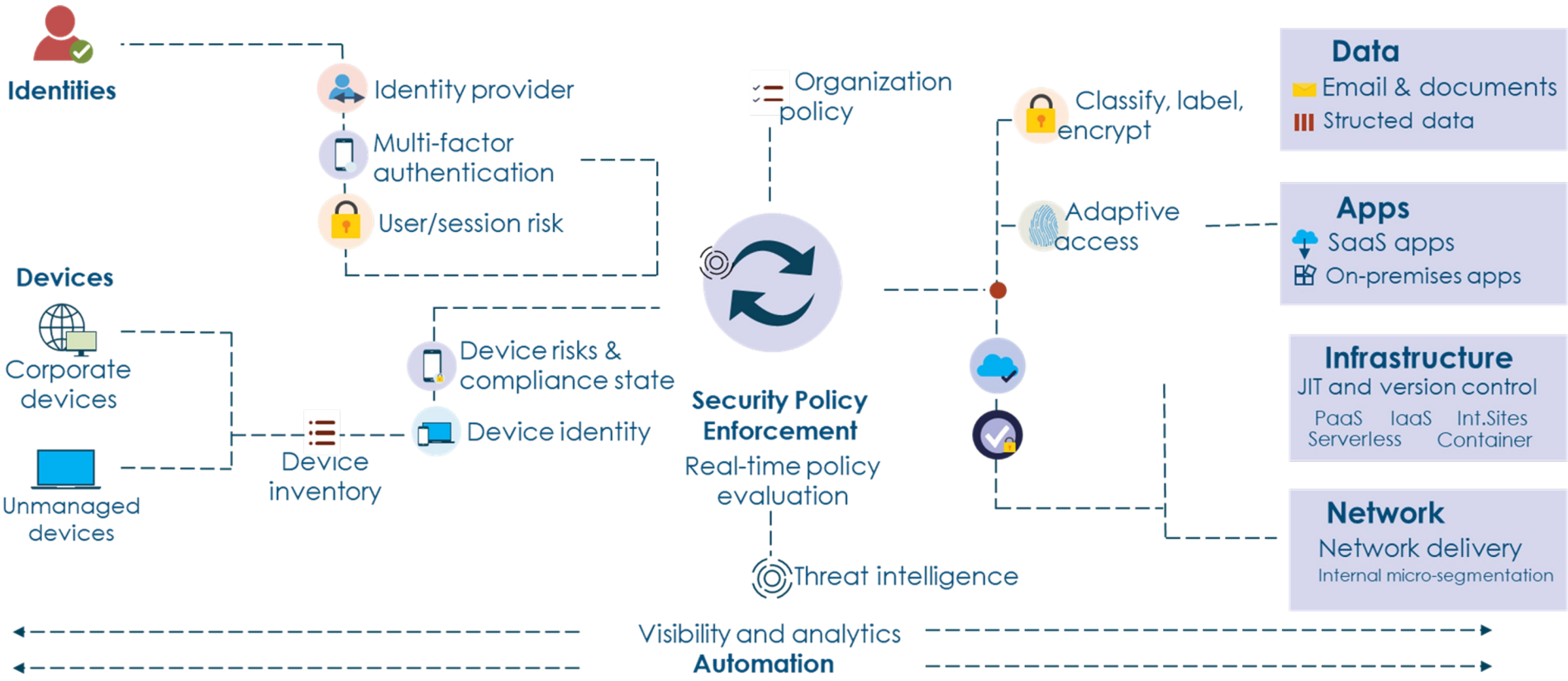
- Involves physical and logical access
- Basic credentials are usernames (username or email) and passwords
- Optional MFA highly recommended
  - Smart/OTP card, YubiKey, software authenticator
  - Biometric fingerprint or retinal scan
- Access key ID + access key for CSP access
- Federated access and single-sign-on
  - SAML.2.0, Oauth + OIDC, Shibboleth

@iconshock.com

Zero Trust

- Is an evolving paradigm moving focus to users, assets, and resources and away from a hardened corporate edge
- Uses zero trust principles to design industrial and enterprise infrastructure and workflows
- Assumes no implicit trust given to subjects based merely on their physical or network location – abandons “Trust but Verify”
- Performs authentication and authorization as distinct tasks before a session is established
- Performs authentication and authorization as distinct tasks before a session is established

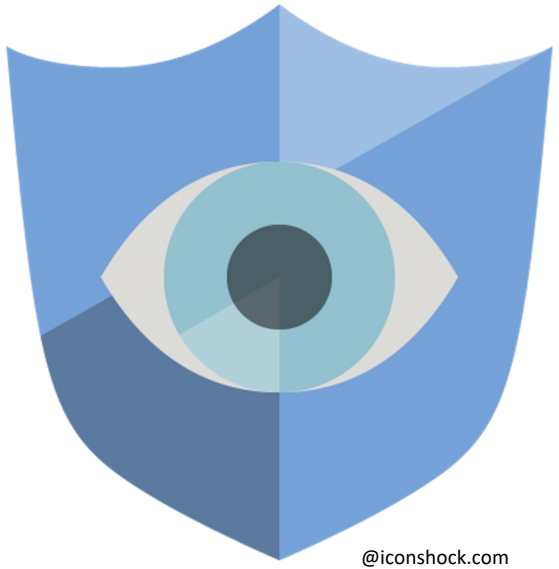
Zero Trust



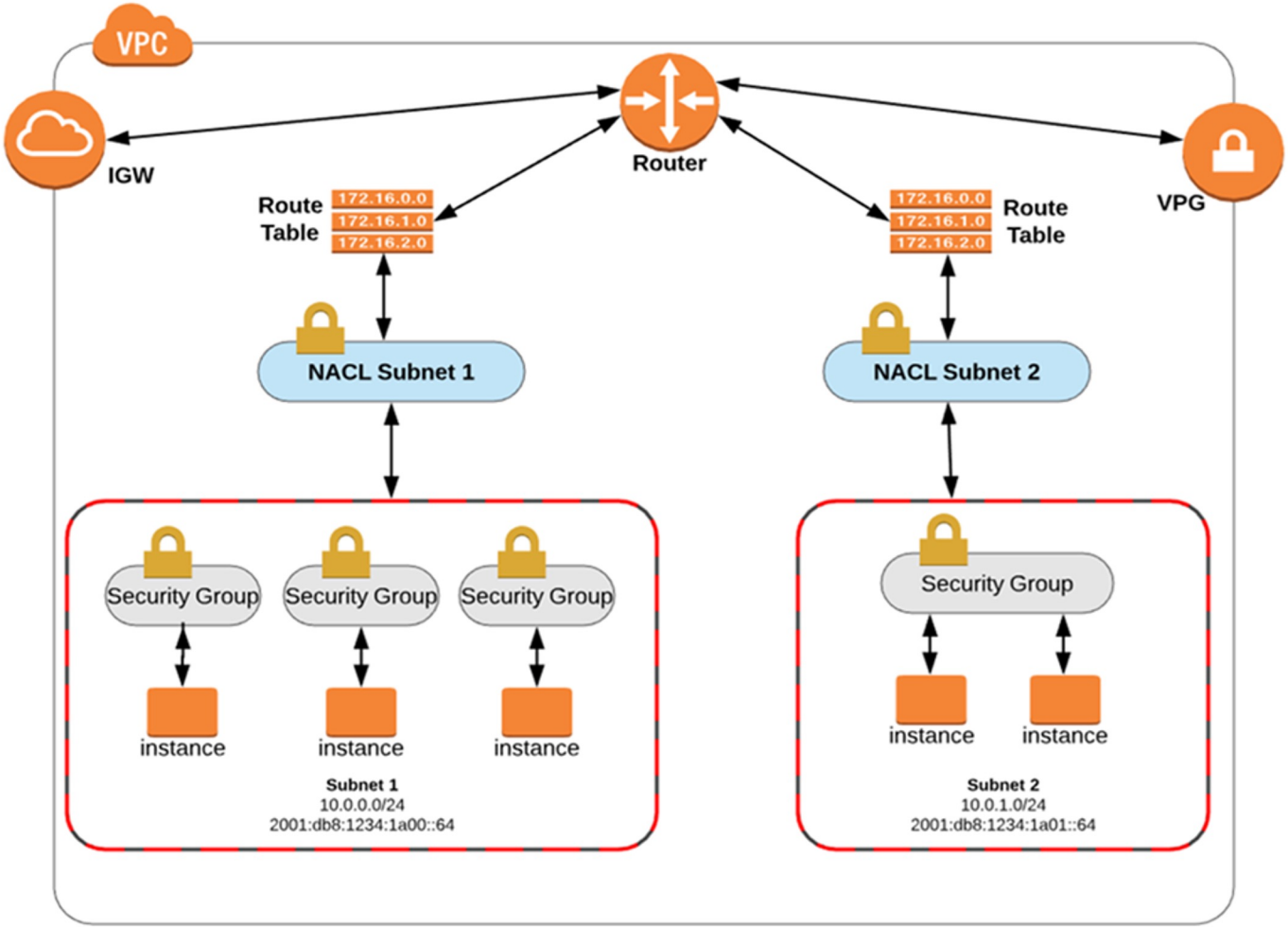
Pearson

Network Security

- Subnet design (public, private, vpn)
- Network ACLs (stateless L3/4)
- Security Group FW (stateful L3/4)
- Web Application Firewall (WebACL)
- Site-to-Site VPNs and Peer-to-Site VPNs
- Elastic Load Balancer Security
- Secure API endpoints
- TLS web management access
- Managed Threat Services



@iconshock.com

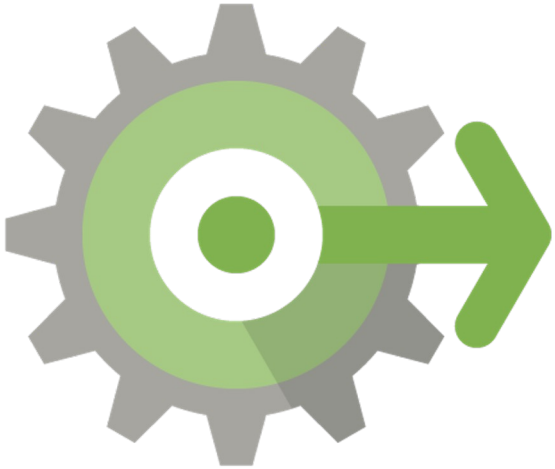

VPC
IGW
Router
VPG
Route Table
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
172.16.0.0
172.16.1.0
172.16.2.0
NACL Subnet 1
NACL Subnet 2
Security Group
Security Group
Security Group
Security Group
instance
instance
instance
instance
instance
Subnet 1
10.0.0.0/24
2001:db8:1234:1a00::64
Subnet 2
10.0.1.0/24
2001:db8:1234:1a01::64

Virtualization Vulnerabilities

- **VM sprawl**
  - When the number of VMs overtakes the administrator's ability to manage them and the available resources
  - Contributes to “ghost” or “shadow” IT
- VM sprawl avoidance
  - Enforce a strict process for deploying VMs with a library of standard VM images
  - Archive or recycle under-utilized VMs
  - Use a Virtual Machine lifecycle management tool or CSP

Virtualization Vulnerabilities

- **VM escape**
  - A serious threat where a process running in the guest VM interacts directly with the host OS
- VM escape protection
  - Patch VMs and VM software regularly
  - Only install what you need on the host and the VMs
  - Install verified and trusted applications only
  - Strong access control policies and passwords



@iconshock.com

Virtualization Vulnerabilities

- **Hyperjacking**
  - An attack that is targeted at exploiting a system from the outside to disrupt or inject a rogue module into the system
  - The attacker can control the virtual machines running on top of the same host and monitor their network traffic
  - Normal security controls are futile since the operating system will not be aware that the machine has been compromised
- Hyperjacking countermeasures
  - Hypervisor security management must be kept separate from regular traffic
  - Tested patch management

The CSA Treacherous 12

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders

@iconshock.com

The CSA Treacherous 12

7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues

@iconshock.com

Cloud Secure Data Lifecycle

Data Ownership

- **Owner** – is often the creator of the information/data
  - Can categorize and determines classification or sensitivity level
- **Custodian** – Is the keeper of the information from a technical perspective
  - Ensures that CIA is maintained
- **Steward** - Manages the data and metadata from a business perspective
  - Ensures compliance (standards/controls) and data quality
- **Processor** – performs data input and runs batch jobs
- **Chief Privacy Officer** - ensures privacy of entire organization

Phase 1: Create

- Data is either generated from scratch, inputted, or modified into another format either locally or in the cloud
- The data owner is often identified in the create phase
- Other key activities of phase one include:
  - Data discovery
  - Data categorization
  - Data classification
  - Data mapping
  - Data labeling (tagging)

@iconshock.com

Phase 2: Store

- After the Create phase, the data is put into a volume (block)/object storage system or into a database
- Relates to transactional, near-term usage data as opposed to long-term cold data storage
- Includes files and spreadsheets, typically done at during or at the end of the Create phase
- **Activities can also occur simultaneously when the data is generated in phase one**
- Protection of data at rest and data in transit will often occur here unless default encryption is implemented in the Create phase

Phase 3: Use

- Data is utilized by people, applications, and tools as well as being changed from the original state
- Raw data becomes information
- If data is used remotely then protection mechanisms must be in place (VPN, secure endpoints, digitally signed API calls)
- The systems that “use” the data must be secured as well
  - EDR Palo Alto Traps, VPN, Identity Rights Management (IRM), and Data Loss Prevention (DLP) engines, Device Inventory Service (Google), data warehousing

Phase 4: Share

- Data is visible, analyzed, and allocated among users, systems, and applications
- Global collaboration and sharing of data introduces obvious risks and lack of control
- Most of the control used in the previous phases will be implemented here in phase four (such as IRM and DLP services)
- Stringent Identity and Access Management (IAM/IdM) should be used to enforce the least privilege principle in line with access control model (ABAC, DAC, RBAC, MAC, etc.)

Phase 5: Archive

- Data is stored for long-term and removed from active usage
- It can be based on policy. Regulations, and governance
- Stringent cryptography (via KMS) will be used for data at rest
- Factors in choosing archival storage:
  - Location
  - Media format
  - Staffing
  - Cost
  - Operating procedures

@iconshock.com

Data Retention

- Data retention typically applies to production data in the Use and Share phases as it is kept for practical purposes as well as corporate utility policies and regulatory mandates
- The policy may also mandate formatting and storage of data as well
- A data retention policy may be closely aligned with the Archive phase of the cloud data lifecycle
- The retention period (usually several years) is an established amount of time that data remains in the archive phase before transitioning to the disposal or destruction phase

Data Archiving Decisions

- Archiving may be as an aspect of BCP/COOP backup and restore policy
  - CSPs offer a “deeper” cold storage
- There may be different data storage and archiving policies for volume (block) data and object data
  - **It is highly recommended that incremental and differential backups ALWAYS be programmed and automated**
- Cloud options involve retrieval plans:
  - Expedited – 1 to 5 minutes
  - Standard – 3 to 5 hours
  - Bulk – 5 to 12 hours

Phase 6: Destroy

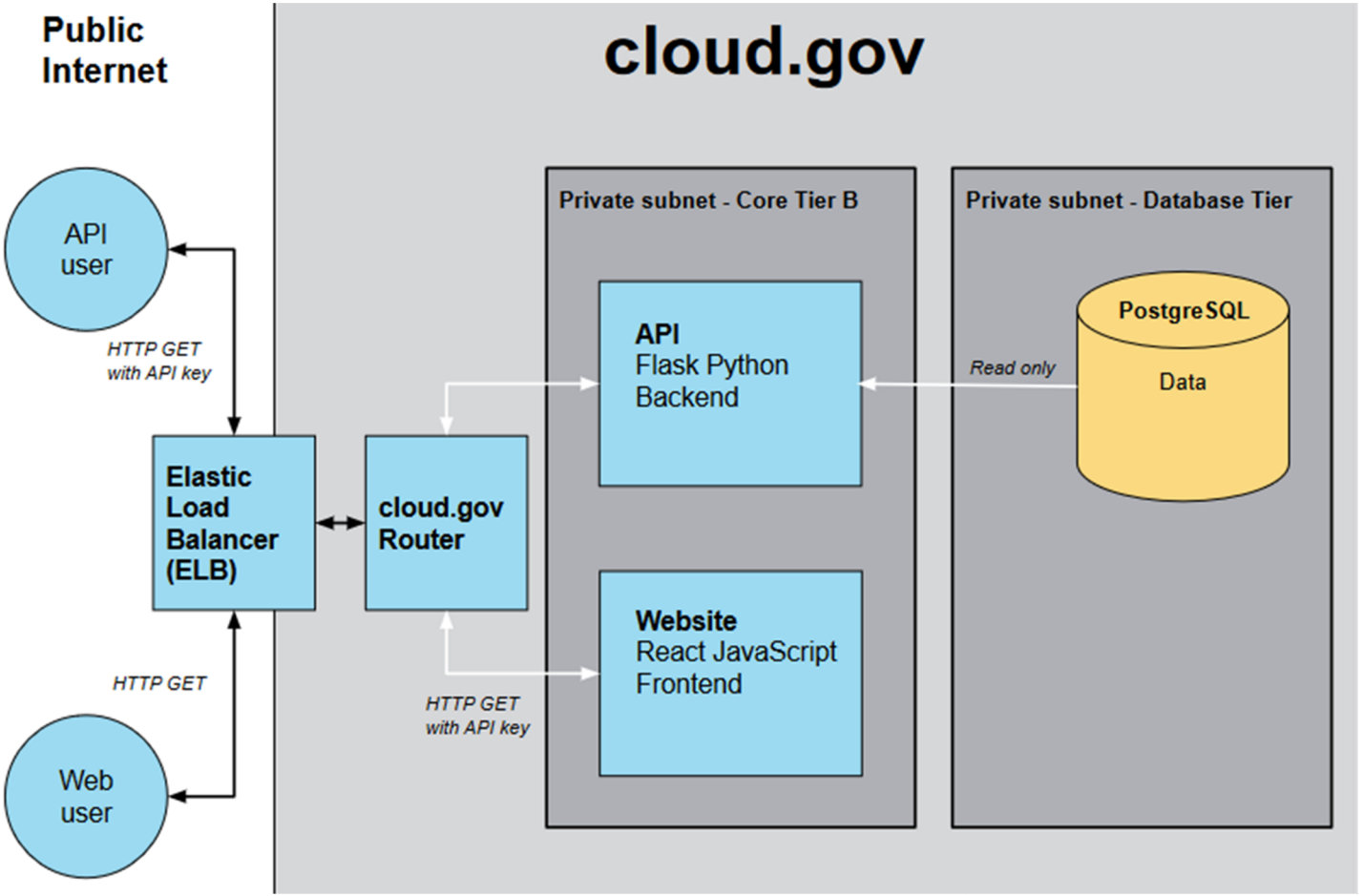
- Due to lifetime, utility, policy, governance, and/or regulations the data is no longer accessible or usable
- The service provider will have their own conventional methods for disposal of data and media, often using military grade programs or physical destruction

@iconshock.com

Data Deletion

- There are two main methods for customer data deletion as far as CSPs are concerned:
  - Using random data or null pointers to overwrite over data sectors that stored sensitive or proprietary intellectual property
    - The acceptable methods will be driven by regulatory standards and guidelines including the number of iterations
    - Not a practical method for confidence at a cloud provider
  - Cryptographic shredding or erasure which is the most effective and practical method in the cloud is

Cloud Data Flows

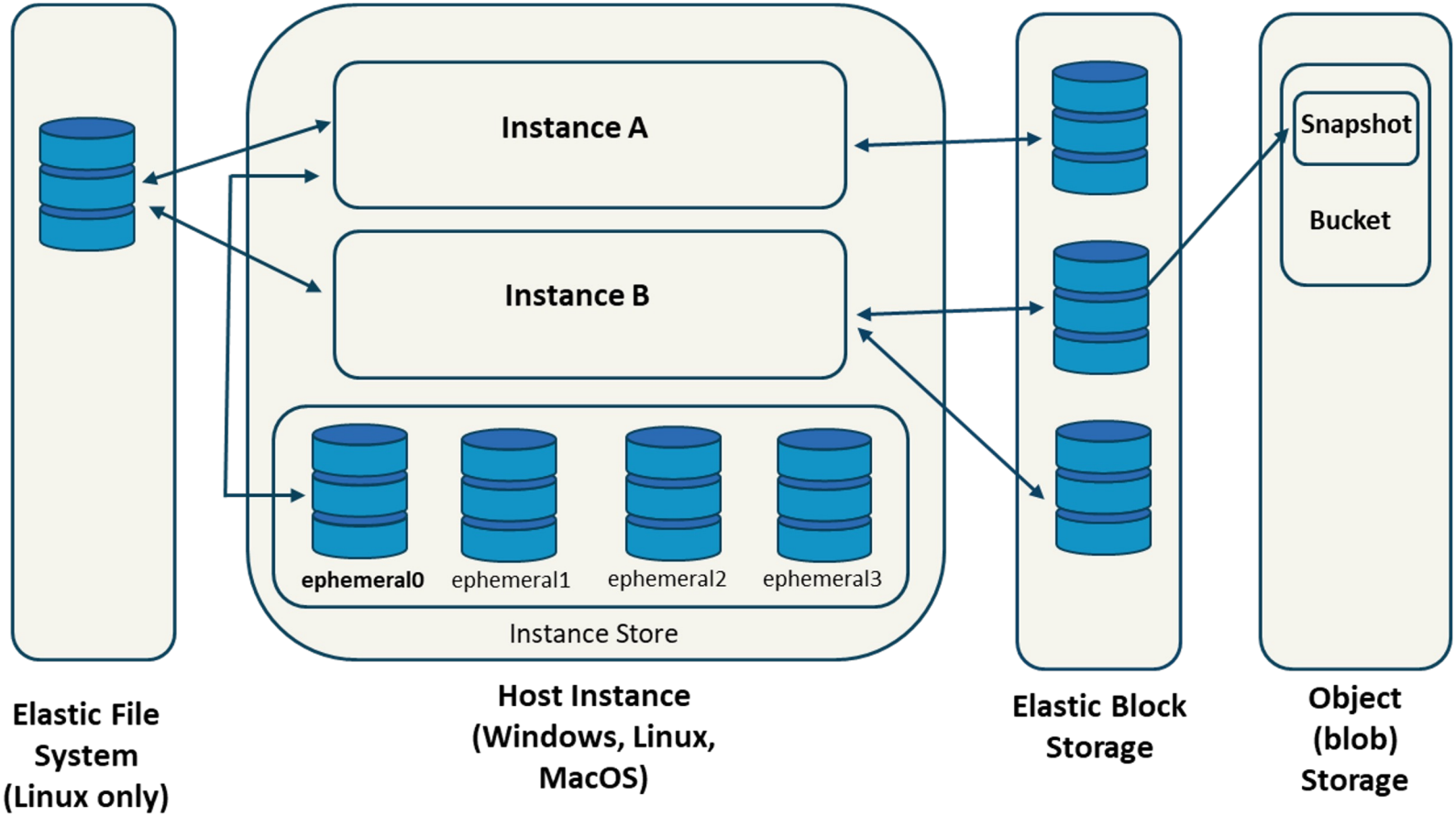


Data Structures

- **Structured** data follows a pre-defined data model and is therefore straightforward to analyze since it conforms to a tabular format with relationship between the different rows and columns (Excel files or SQL databases)
- **Unstructured data** – information that does not have a predefined data model or is not organized in a pre-defined way (audio, video files or No-SQL databases)

Data Structures

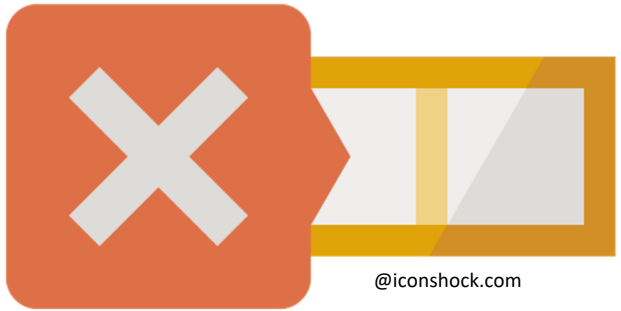
- **Semi-structured data** - does not conform with the formal structure of data models associated with relational databases or other forms of data tables, but nonetheless contain tags or other markers to separate semantic elements and enforce hierarchies of records and fields within the data (JSON, YAML, XML)
- **Metadata** – data about data that supports Big Data analysis and big data solutions to provides deeper analysis regarding a specific set of data



@aws.amazon.com

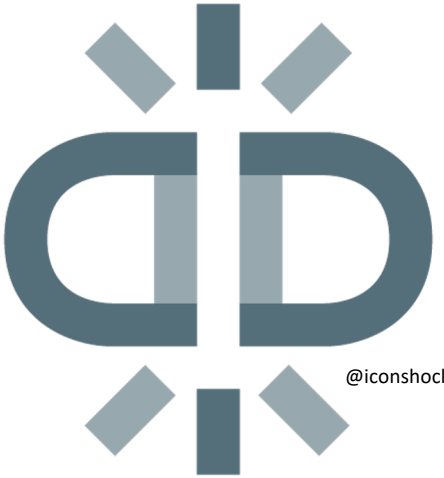
Threats to Storage Types

- Unauthorized access to data in storage in order to modify, exfiltrate, or delete
- DDoS botnet attacks on storage systems
- API requests or URLs which both have their own list of vulnerabilities
- Bit rot, degradation or other corruption



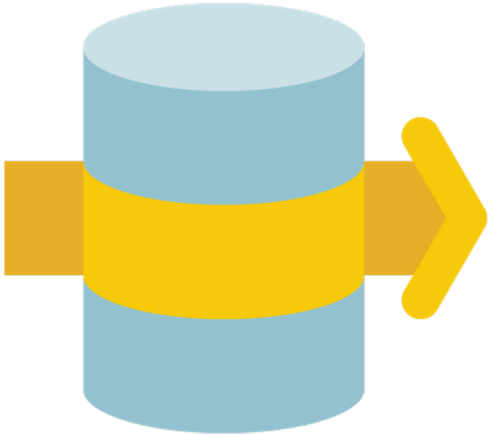
Threats to Storage Types (cont.)

- Data containing PHI, PII, IP, and other sensitive data is a prime target for advanced persistent threats (APT) and data remanence attacks
- Physical disk failure vulnerability in the cloud datacenter remains regardless of the storage or database type
- Ransomware attacks are becoming more common against data stored as objects or blobs at the CSP (S3, Azure Blob, GCS)



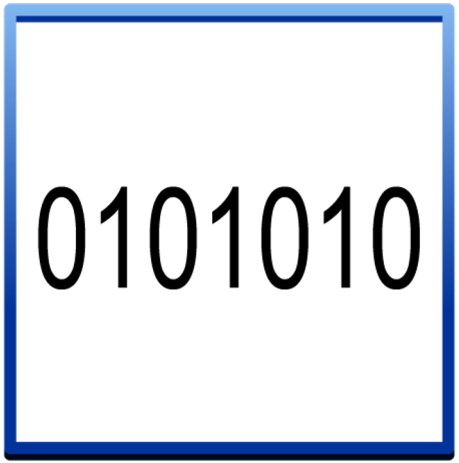
Data Dispersion

- Data dispersion is a technique that is often used to enhance data security, but **without the use of encryption**
- Dispersion is like legacy RAID in that data is spread across different storage areas and even different cloud providers in disparate geographic locations
- However, if data is spread across multiple cloud providers, an outage at one could make the dataset unavailable to users, regardless of location



Bit Splitting and Erasure Coding

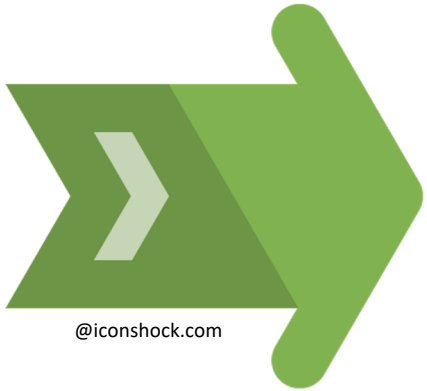
- Bit splitting is similar to adding encryption to RAID where the data is first encrypted, then divided into chunks, and the pieces are distributed across several storage data centers or zones
- Erasure coding is like using parity bits for RAID striping and helps you recover missing data if cloud data is unavailable/lost while your data is dispersed

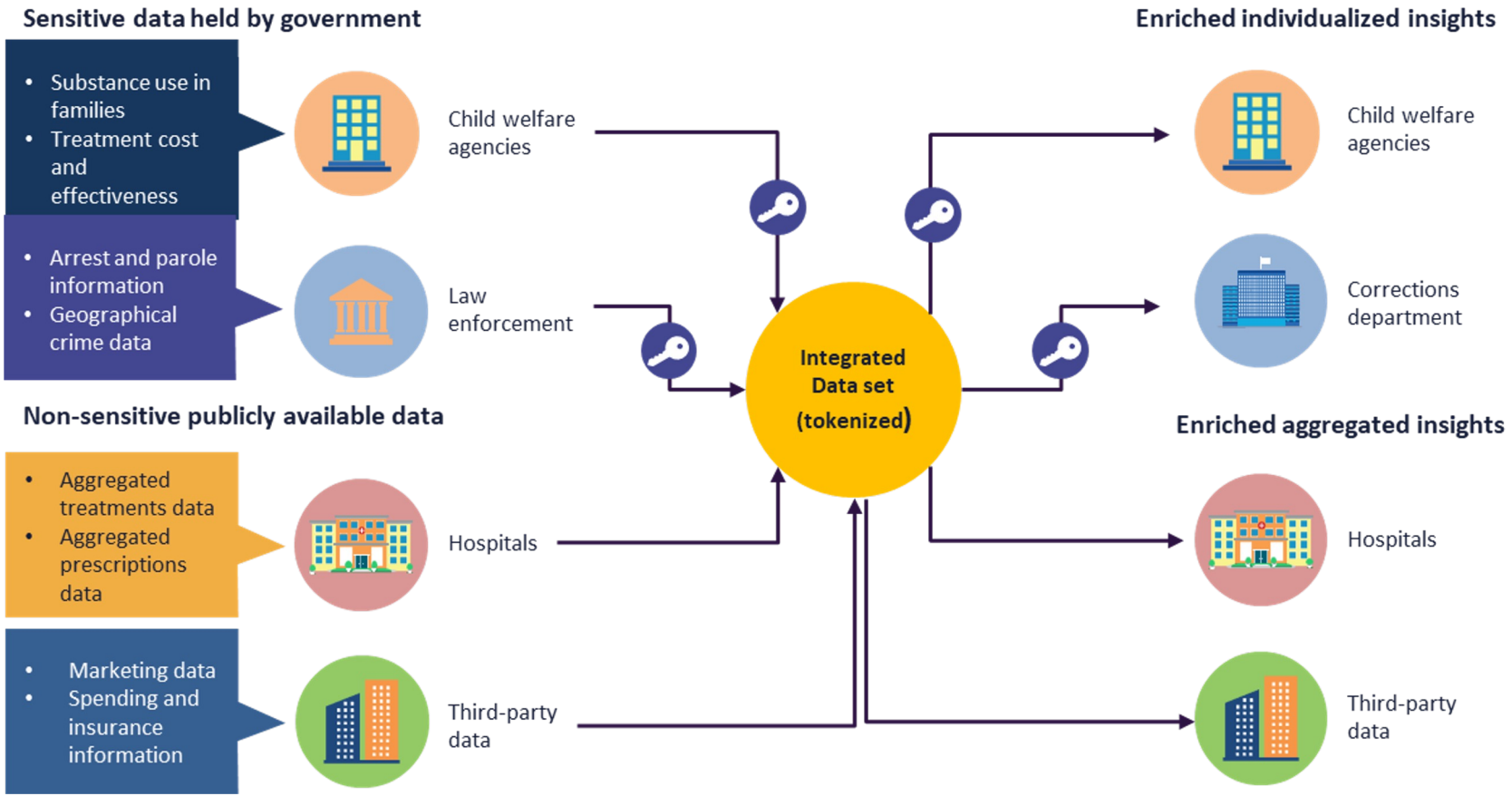


@iconshock.com

Tokenization

- The process of sending sensitive data through an API call (or batch file) to an entity that substitutes the data with non-sensitive placeholders called **tokens**
- Tokenization comprises two distinct databases
  - One with the actual sensitive data
  - One with tokens mapped to each chunk of data
- Unlike encrypted data, the tokenized data is irreversible and unintelligible
  - No math relationship between data and token

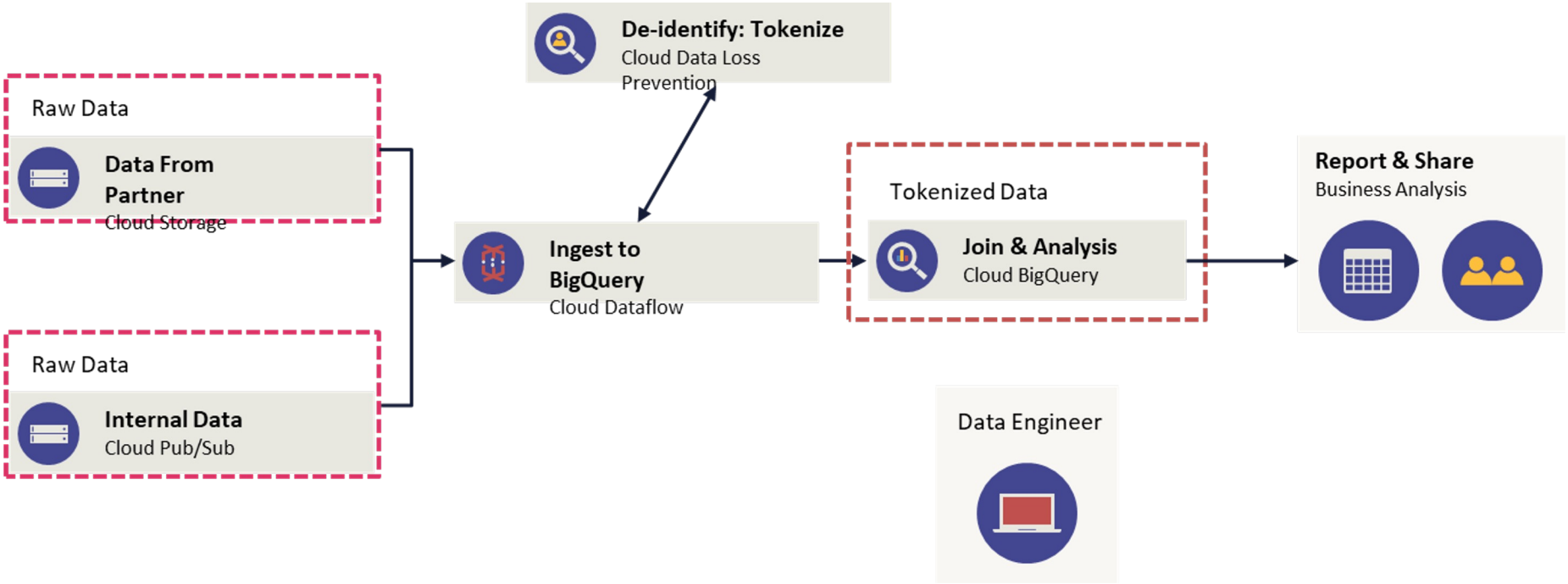




@microsoft.com

Pearson

Data Tokenization on Google Cloud Platform



Source: https://cloud.google.com/blog/products/identity-security/take-charge-of-your-data-how-tokenization-makes-data-usable-without-sacrificing-privacy

Anonymization

- A method of de-identification that consists of eliminating personally identifiable information from a data set that may be used for:
  - Medical research
  - Auditing and testing
  - Financial inquiry
  - Statistical analysis
  - Forensic investigations

@iconshock.com

Masking

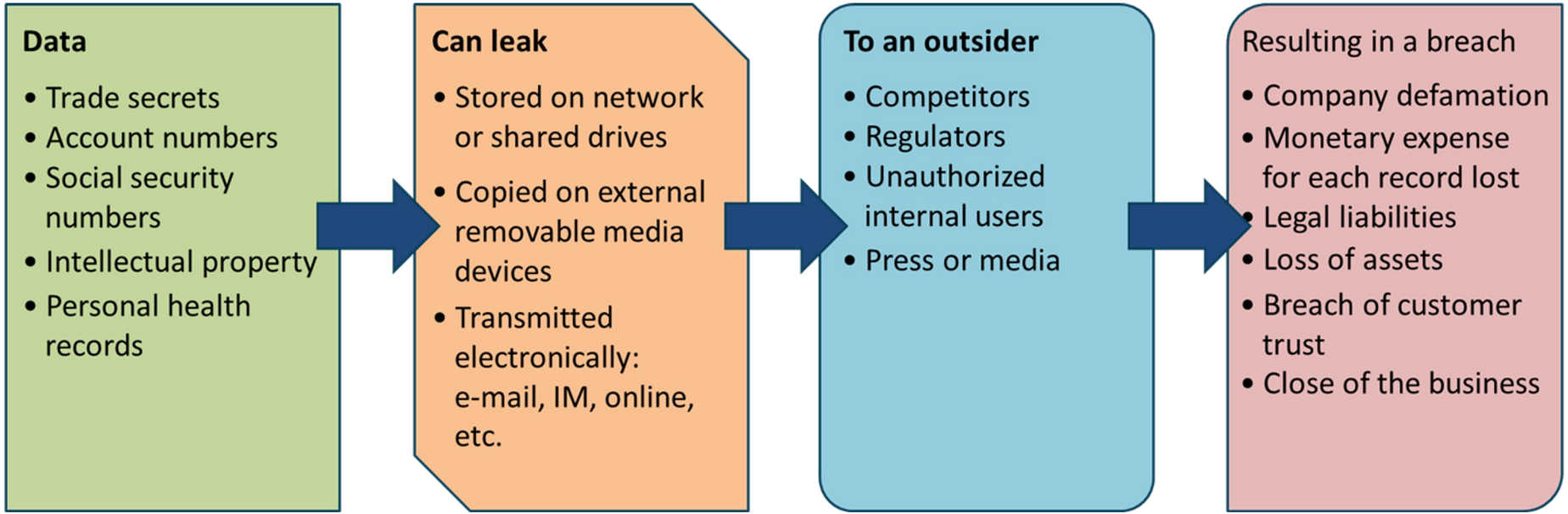
- Hiding the data using arbitrary or unusable characters
- Often involves using characters like “X” to hide some or all data
- Example is to display the last 4 digits of:
  - Social Security number
  - Credit card number
  - National ID number
  - Bank account number
  - Username or email address

@iconshock.com

Obfuscation

- To reduce data to an illegible state or to hide characteristics of PII, PHI and IP
  - "**Obscuring**" is a similar concept where static or dynamic techniques are used on the original data or a representational data set
  - "**Shuffling**" is a term that describes utilizing characters from the same data set to further present the data
  - "**Randomization**" is when all or some of the data is replaced with indiscriminate characters
- **It is critical that the chosen method prevent inference whereby one could extrapolate the original data set - additional abstraction may be necessary**

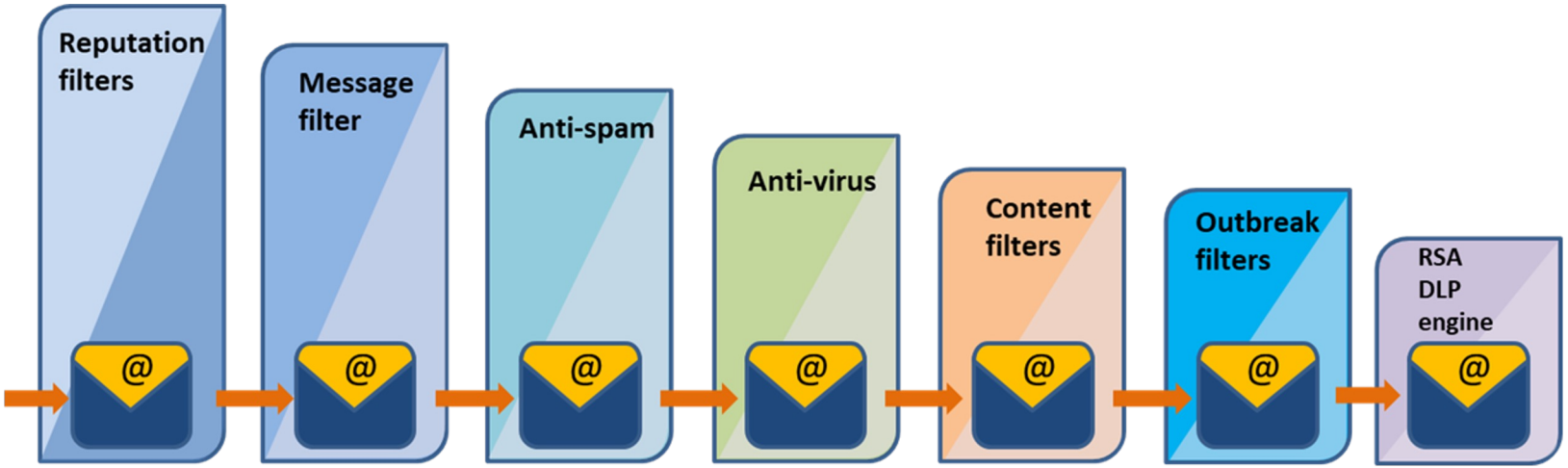
Data Loss Prevention (DLP)



@dhs.gov

Data Loss Prevention (DLP)

- Enhanced security controls as part of layered defense-in-depth
- Enforcement of corporate security policy to accompany the AUP
- Heightening the visibility of egress data and information flow
- Adherence to governance and regulatory compliance (PCI, GDPR)



Data Discovery

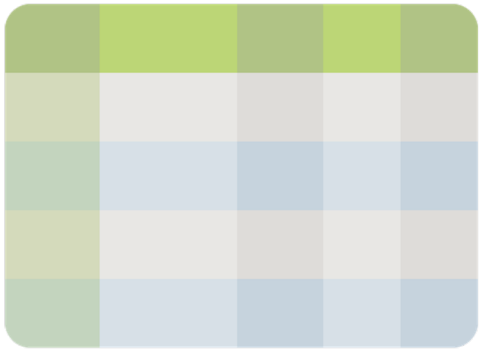
- The enterprise is performing an initial asset assessment and inventory of data ownership OR
- The organization is performing e-discovery as part of a digital forensic investigation
- 3 main forms of structured or unstructured data discovery
  - **Content-based** – dataset contents such as terms and pattern-matching
  - **Label-based** – discovery is based on existing labels an/or tagging that is applied to physical and logical assets both on-prem and in the cloud
  - **Metadata-based** – leveraging the extensible metadata available on data stored as objects – using APIs against data at CSPs

Implementing Data Classification

- The early phases of information security life cycles consist of identification, assessment (valuation), and classification of data assets
- Labeling and tagging (logical) is used to classify assets and information
  - Can be used to determine the level of protection and how the asset should be handled
  - Handling controls who has access to information and is based on labeling – how it has been classified
- Classification can be based on location, value, age, utility, useful lifetime, personal association, or a sensitivity label for a mandatory access control (MAC Bell-LaPadula or Biba) model

Classification or Sensitivity Levels

- **Government/military:**
  - Top Secret
  - Secret
  - Confidential
  - Sensitive But Unclassified (SBU)
  - Unclassified
- **Commercial/private sector:**
  - Confidential
  - Private
  - Sensitive
  - Public



@iconshock.com

Information Rights Management (IRM)

- Also called DRM and E-DRM
- The goals are to implement controls that work with access controls to protect data and file-level assets
  - Example: Must control copying, deleting, and modifying certain PDF documents to protect intellectual property (IP) and copyrights
- DRM is used by publishers, manufacturers, and IP owners for digital content and device monitoring
- Since digital signing and certificates are often used, an enterprise PKI may be part of the policy

AZURE RIGHTS MANAGEMENT

Rights Management

Authentication and authorization

Content key and rights

Policy, which contains usage rights and the content key, is added to document

Secret cola formula:

- Water
- HFCS
- Brown #16

Document is unprotected

Protect

Policy

#!@#!#!@#♭
()&)(*&)(@#!
#!@#!#!@#♭
()&)(*&)(@#!
#!@#!#!@#♭
()&)(*&)(@#!

Content is protected by a symmetric key, which is encrypted with the organization's root key

Secret cola formula:

- Water
- HFCS
- Brown #16

Document remains protected but decrypted with usage rights enforced for authenticated user

@microsoft.com

Pearson

Digital Rights Management for PDF Files

Manage document usage	Deny unauthorized sharing	Stop screen captures or printing to files	Enforce expiration	Revoke access based on least privilege
Restrict to specific IP CIDR ranges	Watermark PDF files	Track document usage	Integrate with CLI for automation	Integrate with e-commerce solutions

Business Continuity and Disaster Recovery Planning

@iconshock.com

- **There are two aspects to consider with BCP and DR:**
  - The continuity of operations and disaster recovery responsibilities **of the cloud provider** and
  - The customer using the Cloud Service Provider for their own business continuity, site resiliency, and/or disaster recovery solutions
  - This may also include Backup and Restore practices

Cost Benefit Analysis

- Cost-Benefit Analysis (CBA) should be performed early in the security management lifecycle
- After identifying all possible controls and evaluating their feasibility and effectiveness, enterprises should allocate resources and implement cost-effective controls based on qualitative or quantitative risk management methodologies
- The goal is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk
- **Security architects may need to justify decision to C-suite, steering committees, or other boards of decision makers**

Cost Benefit Analysis

- **NIST SP 800-30 Risk Management Guide for Information Technology Systems states:**
  - If control would reduce risk more than needed, then see whether a less expensive alternative exists
  - If control would cost more than the risk reduction provided, then find something else
  - If control does not reduce risk sufficiently, then look for more controls or a different control
  - If control provides enough risk reduction and is cost-effective, then use it

@iconshock.com

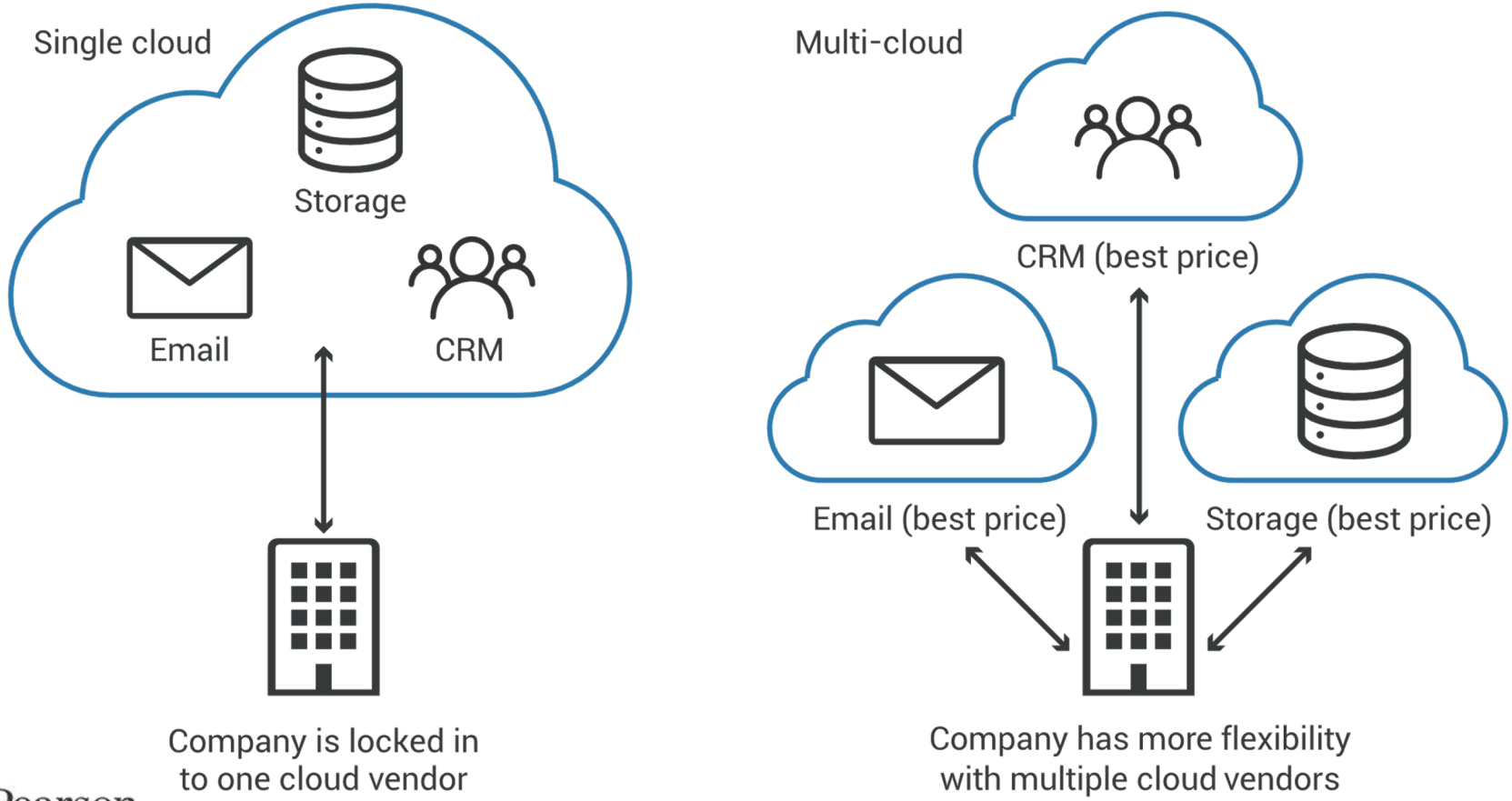
Cloud ROI Critical Factors

- Critical factors when calculating ROI according to VMware:
  - Productivity
  - Leverage
  - Pay as you go and need
  - Provisioning time
  - Reduction of capital spending
  - Access to new markets and regions
  - Cloud risk management

Functional Security Requirements

- **Portability** - the ability to move applications, containers, code, and associated data from one CSP to another or between legacy on-prem environments and the cloud
- **Interoperability** – when the customer app does not function properly when changes are made to an environment; more common in a PaaS scenario since the O/S is managed and updated by the provider
- **Vendor lock-in** –when the consumer is unable to retain, migrate, or transfer to another based on technical or non-technical restrictions
- **Vendor lock-out** – A situation where the customer is not able to recover or access their own data due to a vendor going out of business, going bankrupt, or legal holds are implemented

Vendor Lock-in

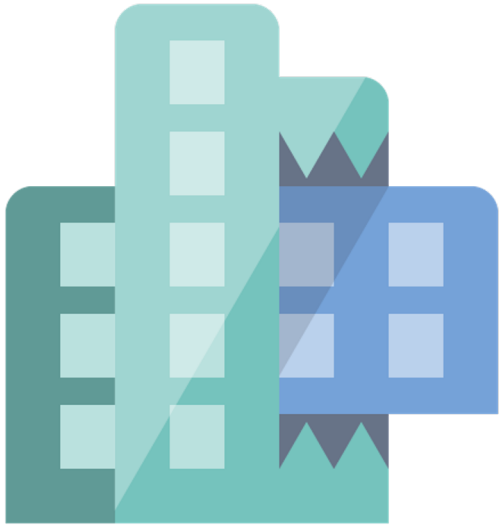


Pearson

https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/

Security Considerations for IaaS

- The cloud customer has the highest degree of responsibility for security:
  - Network design and firewalls
  - Operating system and applications
  - Data encryption (client-side vs. server-side)
  - Data protection
- CSP will secure the facility and datacenter – everything at Layers 1 and 2 of the OSI model including the hypervisors



@iconshock.com

Security Considerations for IaaS

- Customer has limited visibility and monitoring of the provider site and datacenter which makes audits challenging – must rely on third-parties
- Must be negotiated in early negotiations
- **Some activities may be prohibited by regulations such as Cloud-based HSM instead of on-prem HSM**

@iconshock.com

Security Considerations for PaaS

- The customer loses additional control/responsibility when using platform-as-a-service since the provider installs, manages, upgrades, updates the operating systems, database systems, and even some applications
- There is more gray area with managed and “fully-managed” services (example: AWS Aurora vs. RDS MySQL)
- SLA’s and policies must be more structured and customized, especially when regulatory compliance is involved
- Customer should have adequate monitoring and metering when using PaaS

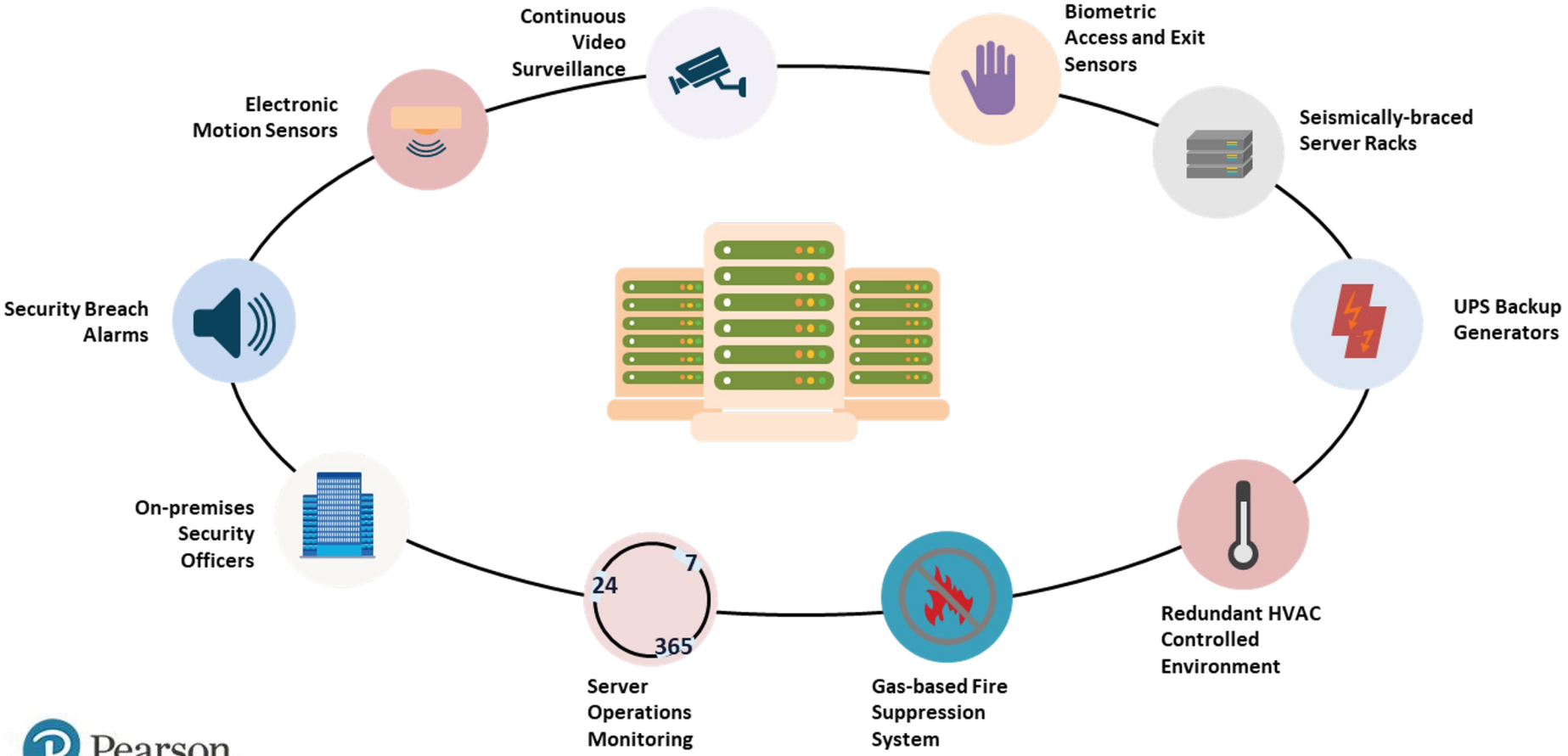
Security Considerations for SaaS

- **Practically all control is assumed by the service provider**
- The consumer will only create, deliver, and modify data delivered to the cloud system
- Often, the applications are being rendered via XML or web-based tools on the client system or VDI environment
- Customer has limited administrative rights, elevated privileges, permissions, and authorization
- **Consumer may still have contractual responsibilities for safeguarding data and federated access therefore a Cloud Access Security Broker (CASB) is often employed to assist SaaS solutions**

Legal Holds

- This term denotes a process that an enterprise uses to retain all forms of pertinent data and information when it realistically anticipates some form of litigation against it, or some need for future utility in a court of law
- A legal hold can be a restriction placed on a database or set of records that exists as a result of existing or anticipated litigation, audit, government investigation or other such activity that suspends the regular usage, processing, or destruction of data

Cloud Datacenter Physical Security

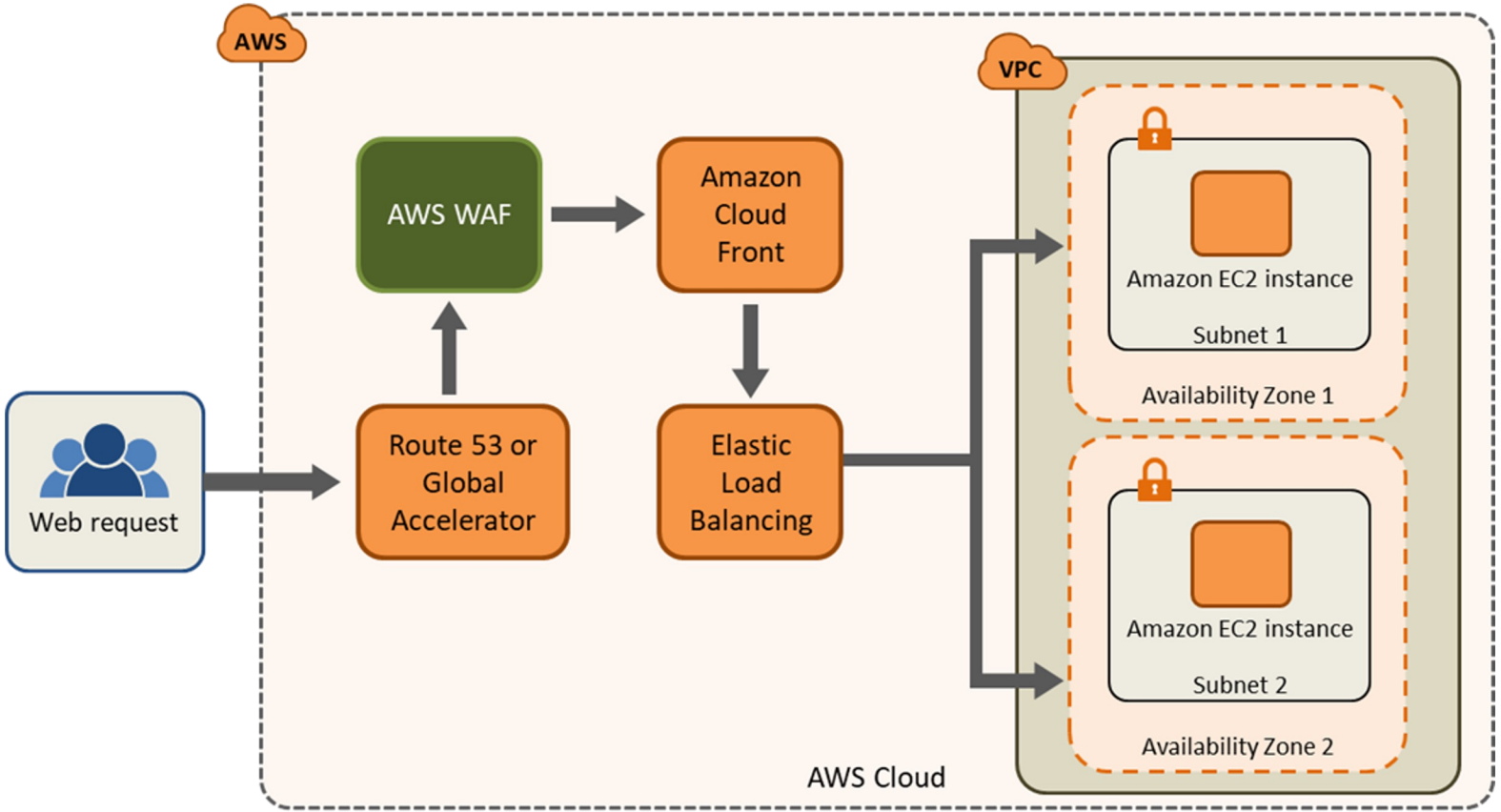


Pearson

Content Distribution (Delivery) Networks

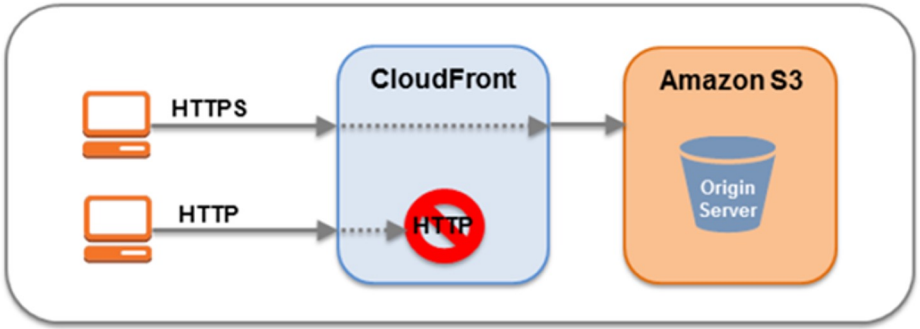
- A widely distributed platform that lessens delays in loading web page or other streaming content by reducing the physical distance between the server and the users around the world
- Without a CDN, origin servers would have to respond to every end user request, resulting in substantial traffic to the origin and subsequent load – as in the early “dotcom” era
- By responding to end user requests using modern edge computing and elastic caching (usually Redis clusters), the CDN offloads traffic from content servers to metro edge locations
- Examples are Cloudflare, Akamai, Fastly, and AWS CloudFront

CloudFront at Amazon Web Services

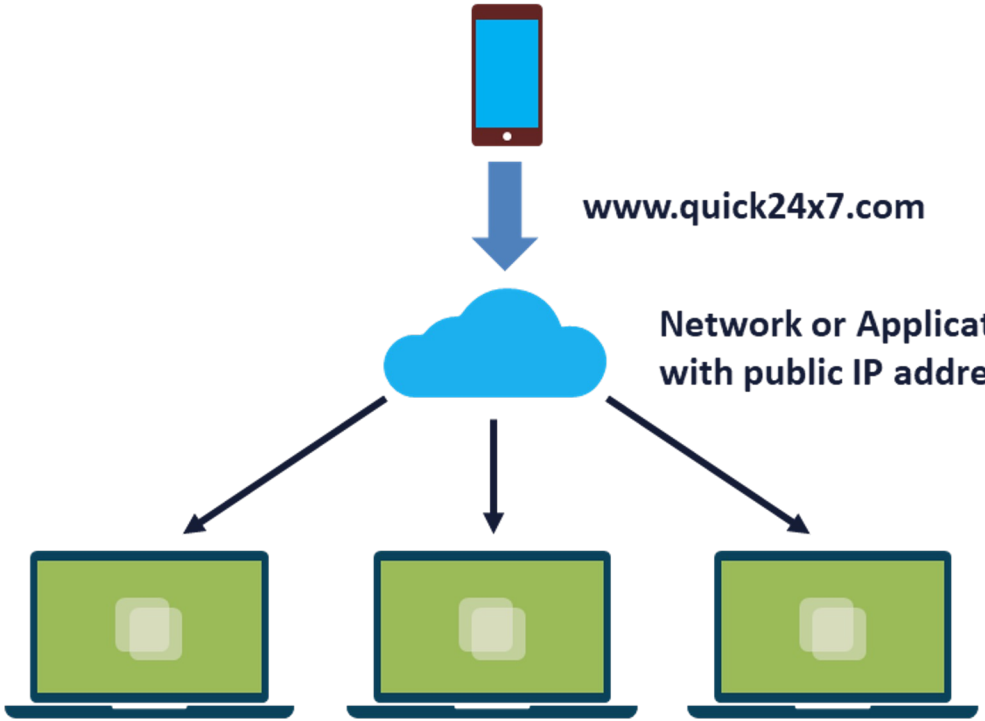


AWS CloudFront Security

- High-level data center physical security is in place
- Uses TLSv1.1 and TLSv1.2 protocols for HTTPS connections between CloudFront and the custom origin web server
- Cipher suites use the ECDHE protocol on all connections
- Private Content Feature controls who can download content
- Origin Access Identities can control access to original copies of objects



Cloud Elastic Load Balancers



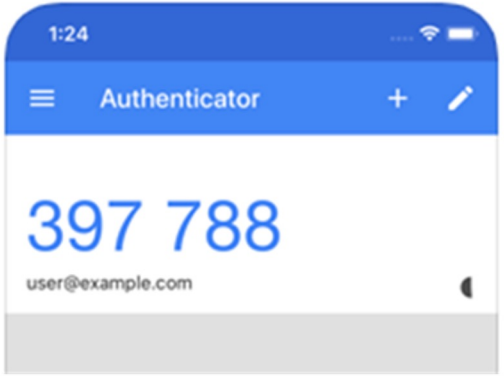
Secure Elastic Load Balancers

- Network (TCP, UDP, TLS) or Application (HTTPS/S) elastic load balancers are used at CSPs
- They can represent the virtual networks and resources to the public on the Internet
- Performs health checks on target instances
- Produces flow logs and DNS reports for visibility and Active Defense security
- Runs the TLS listener on Application LB to decrypt
- Can also have layer 3/4 and web application firewall (WebACL) applied

CSP Management Plane Protection

- All CSPs have systems management tools for managing the infrastructure using a graphical portals and IAM
- Can be used with IaaS and SaaS solutions
  - Agent software is provided to install on Windows, Linux, and MacOS systems
  - SSH2 sessions are setup initially then subsequent management sessions are protected with keys
- Managed services can setup ad hoc management sessions when federated SSO using SAML 2.0 is used
- CLI, SDK, and other console-based access must be digitally signed

Use MFA on all root and service accounts

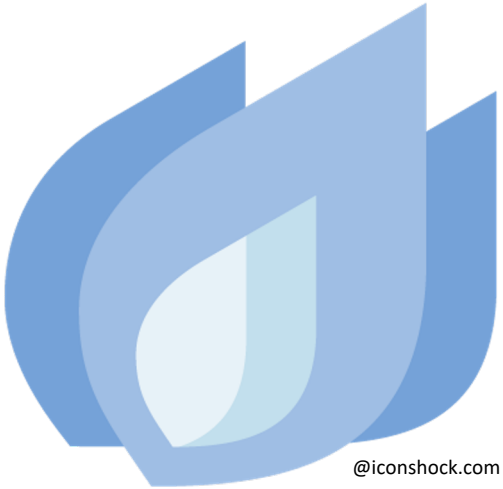


HVAC Design Considerations

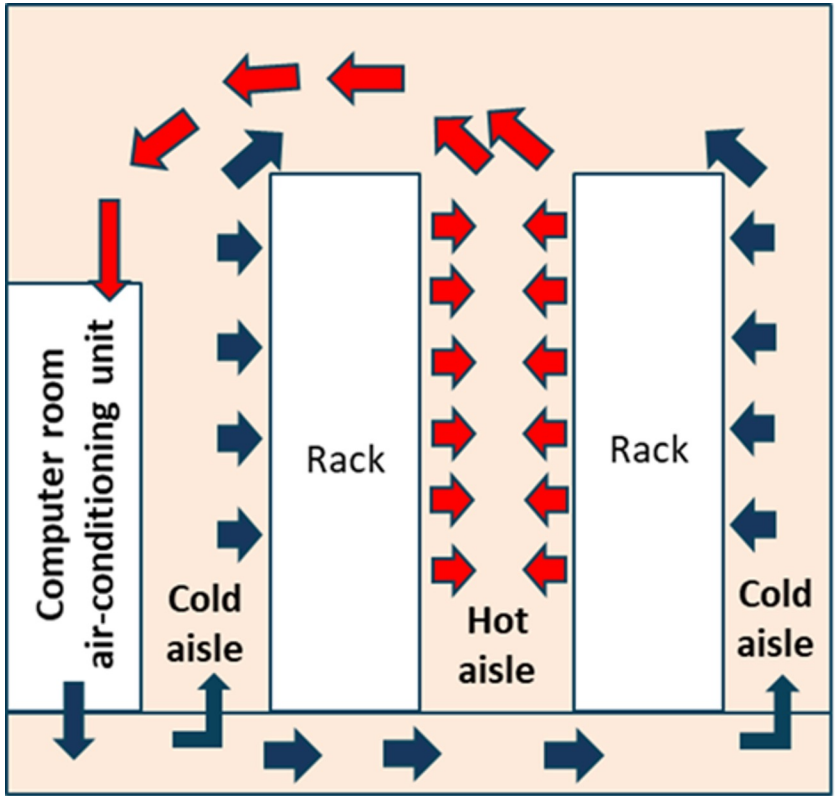
- HVAC systems should provide air management that separates the cool air from the heat exhaust of the servers
- Local climate will impact the HVAC design requirements
- Redundant HVAC systems should be part of the design
- There are racks with built-in ventilation or alternating cold/hot aisles
- The best design choice will depend on space and building design constraints

HVAC Design Considerations

- Consider energy efficient systems when feasible
- **Recommended temp: 72 to 76 degrees**
- **Recommended humidity: 40-60%**
- **Backup power supplies should be available to the HVAC system based on business impact analysis (BIA)**
- The HVAC system should filter contaminants and dust

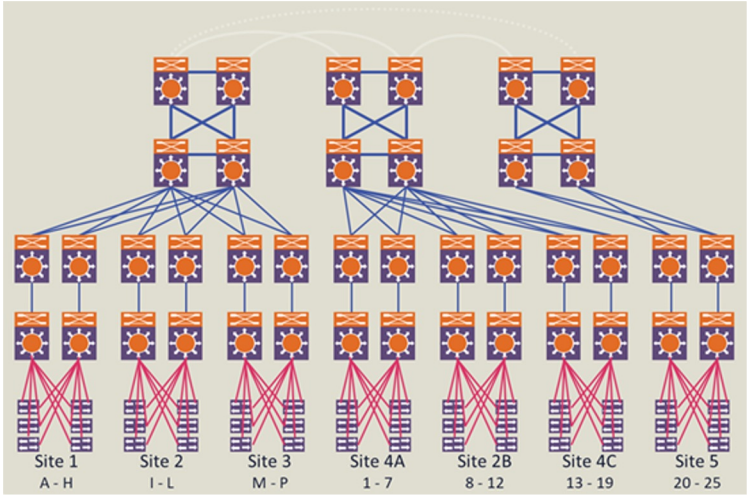


Cold/Hot Aisles and Chillers



Distribution Frames and Wiring Closets

- Gain visibility into all ethernet and fiber cable runs as well as the security of distribution frame (MDF rooms) rooms and closets
  - Under the floor, above ceiling panels, in the walls
- Lock all doors to server rooms and frame rooms and no window access (or use security windows with wire mesh)
- Use hardened management stations

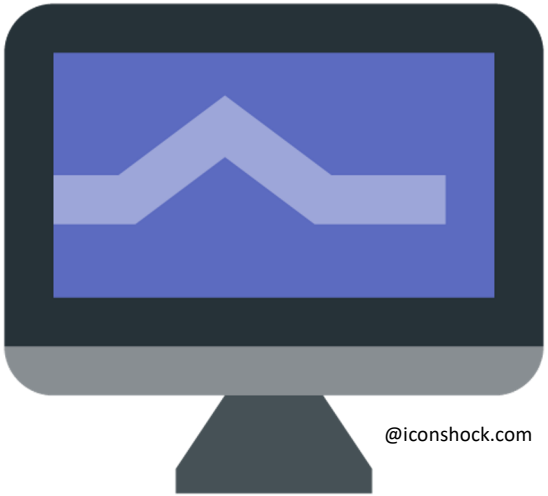


Server Rooms and Data Centers

- Access control both at the perimeter and at room ingress points by professional security staff using video surveillance, intrusion detection systems, and more
- Authorized staff should pass biometric dual-factor authentication a minimum of two times to access data center floors
- Implement protective barriers
- Have visibility into high-security compartmentalized areas including all power conduits and water lines
- **Have redundant and monitored support systems with secure KVM systems**

Secure KVM

- According to the Common Criteria, a secure KVM will do the following:
  - Isolated data channels
  - Tamper-warning labels on each side of the KVM
  - Housing intrusion detection
  - Fixed firmware
  - Tamper-proof circuit board
  - Safe buffer design
  - Selective USB access
  - Push-button control



Server Rooms and Data Centers (cont.)

- Airgap is the physical separation of the control network and other networks
- Implement Separation of Duties (SoD) initiatives
- Separate the highly secure networks from the unsecured networks with physical or logical compartmentalization
- Log and audit all devices and objects entering and exiting facility
- Work with facilities management to integrate blueprints and topological diagrams into IT services

Server Rooms and Data Centers (cont.)

- When an employee no longer has a business need for data center privileges, access must be immediately revoked, even if they continue to be an employee
- Automatic fire detection and suppression equipment must be used
- The electrical power systems should be fully redundant and maintainable without impact to operations 24/7
- Uninterruptible power supply (UPS) units can provide back-up power for critical and essential loads in the facility in the event of an electrical failure
- Data centers often use generators to provide back-up power for the entire facility

Multi-vendor Pathway Connectivity

- Uninterrupted service and constant access are critical to the daily operation and productivity of the enterprise
- Since downtime leads directly to loss of income, datacenters must be designed for redundant, fail-safe reliability and availability
  - Datacenter reliability is also defined by the performance of the infrastructure
- There should be redundant connectivity from multiple providers into the datacenter
  - This will help prevent a single point of failure for network connectivity
  - The redundant paths should deliver the minimum expected connection speeds (10GB/100GB) for datacenter operations

CSA Virtualization Risk Mitigation

- Risk #1 – VM Sprawl
- Risk #2 – Sensitive Data Within a VM
  - Passwords, personal data, bash profiles, bash history files, encryption keys, license keys, data and image captures
- Risk #3 – Security of Offline and Dormant VM
- Risk #4 – Security of Pre-Configured (Golden Image) VM / Active VMs
- Risk #5 – Lack of Visibility Into and Controls Over Virtual Networks
  - Hinders existing security policy enforcement in most organizations
  - Traffic over virtual networks may not be visible to physical network security protection devices, such as NIDS/NIPS

VM Sprawl Mitigation

- Implement policies, guidelines, and processes to govern and control VM lifecycle management
- Control the creation, storage, and use of VM images with a formal change management process and tools
- Retain known-good—and timely patched—images of a guest OS separately
- Utilize virtualization management solutions to examine, patch, and apply security configuration changes to VMs

@iconshock.com

Securing Offline/Dormant VMs and Golden Images

- Make certain appropriate hardening and protection techniques are deployed for VM instances using VM guest hardening
- Supplement VM operating systems with built-in security measures, leveraging third-party security technology like visibility and monitoring tools
- Implementing integrity checksums for all VM images
- Encrypt VM images to counter unauthorized alteration
- Introduce strict controls for access, generation, and deployment of VM images/instances

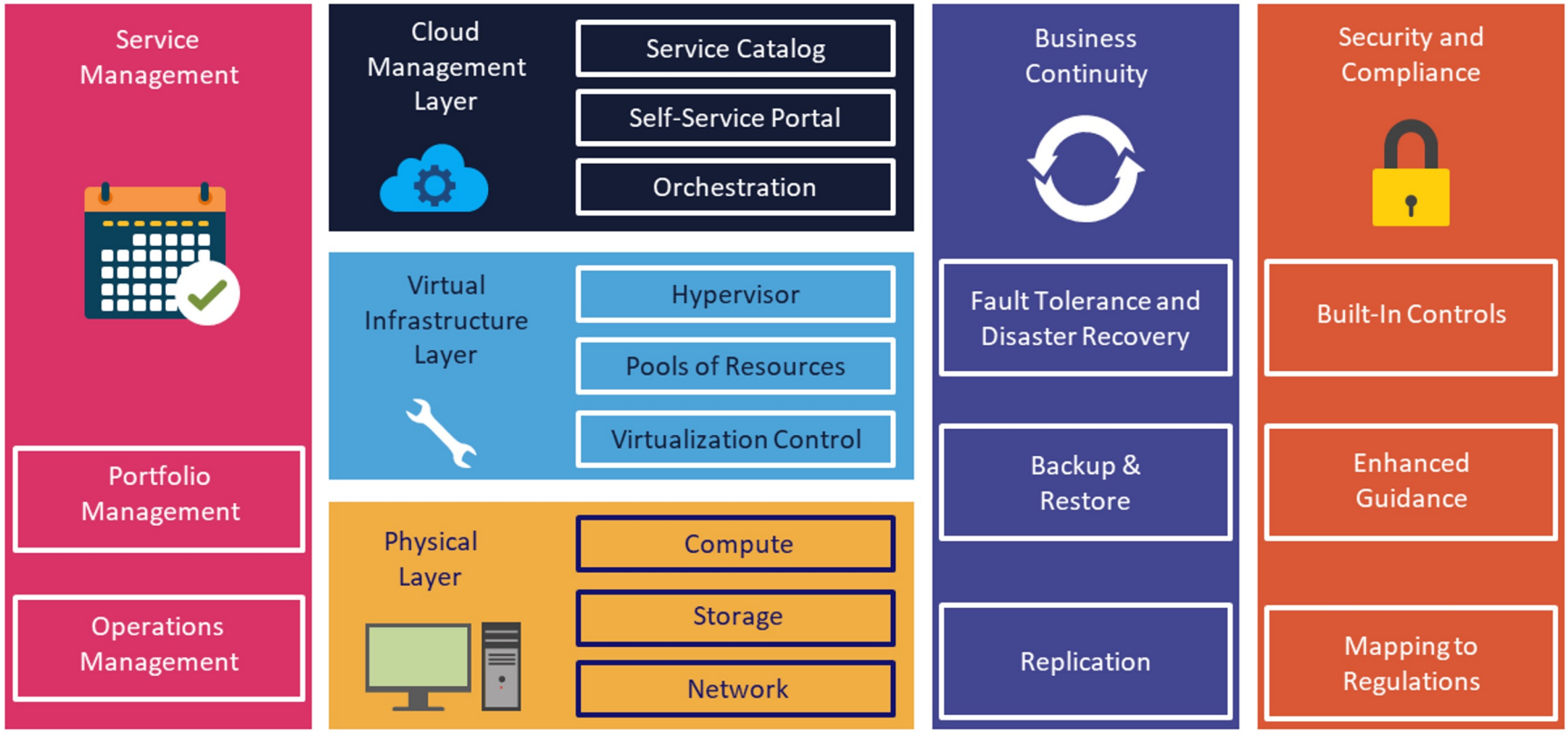
CSA Virtualization Risk Mitigation

- Risk #6 – **Resource Exhaustion**
  - Resource-intensive software can consume resources in a physical server when it is deployed in multiple VMs. For instance, anti-virus and other security software interrupt every call to disk or memory in order to monitor and prevent security incidents such as cracking or viruses
- Risk #7 – Hypervisor Security
- Risk #8 – Unauthorized Access to Hypervisor

CSA Virtualization Risk Mitigation

- Risk #9 – Account or Service Hijacking Through the Self-Service Portal
  - A self-service portal is often used to delegate specific parts of virtual infrastructure provisioning and management to assigned self-service administrators
  - Generous use of self-service portals in cloud computing services will increase susceptibility to security risks, including account or service hijacking
- Risk #10 – Workload of Different Trust Levels Located on the Same Server
- Risk #11 – Risk Due to Cloud Service Provider API

VMWARE SECURITY DESIGN



Risk Treatment (Handling)

- Risk acceptance
  - Do not implement any safeguards
  - Justification in writing is often required
- Risk avoidance
  - Choose not to undertake actions that introduce risk
- Risk transference/sharing
  - Pass the risk to a third-party, such as an insurance company or a cloud service provider
- Risk mitigation
  - Implement safeguards that will eliminate or reduce risk exposure - risk may exist, but impact is reduced

Risk Assessment

	Event type								
	Accidental Leak	**Espionage**	**Financial fraud**	**Misuse**	**Opportunistic data theft**	**Physical theft**	**Product alteration**	**Sabotage**	**Violence**
Nonhostile									
Reckless insider	X			X			X		
Untrained/distracted insider	X			X			X		
Outward sympathizer	X			X					
Unknown (nonhostile or hostile)									
Supplier	X	X	X	X	X		X		
Partner	X	X	X	X	X		X		
Hostile									
Irrational individual	X			X		X		X	X
Thief		X	X		X	X			
Disgruntled insider	X	X	X	X	X	X	X	X	X
Activist		X		X	X	X	X	X	
Terrorist						X		X	X
Organized crime		X	X		X	X	X		
Competitor		X			X		X	X	
Nation state		X			X		X	X	

Tim Casey et al., "A Field Guide To Insider Threat," PDF file, https://www.nationalinsiderthreatsig.org (IT@Intel, Intel Corporation, October 2015), https://www.nationalinsiderthreatsig.org/itrmresources/Intel%20Insider%20Threat%20Field%20Guide.pdf.

Risk Ledger (Register or Log)

- Often represented as a scatter plot/table from a database
- Fulfills regulatory compliance
- Repository of identified risks, impact, scenarios, and potential responses

Identified Risks	Root Causes	Probability and Impact	Ranking	Categories	Priorities	Time and Cost Objectives	Potential Responses	Risk Owners	Assumptions

Qualitative Risk Analysis

- Subjective tactic using opinions, estimation, and experienced scenarios to determine risk levels
  - Real-world experiences
  - Expert judgement
  - Case studies
  - Best practices
  - Intuition

@iconshock.com

- Often involves interviewing people (Delphi) regarding assets, known risks, known vulnerabilities, common threats, and historical impacts

Qualitative Heat Map

			Impact				
Likelihood			Negligible	Minor	Moderate	Critical	Disastrous
			1	2	3	4	5
	Frequent	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

Quantitative Analysis

- Mathematical methodology for obtaining monetary and numeric outputs based on the following:
  - Asset values
  - Impact and magnitude
    - Severity of incident
  - Probability and likelihood of occurrence
    - Threat frequency
  - Costs and effectiveness of safeguards
  - **Probabilities based on percentages and calibrated estimation using OpenFAIR is popular**

Classic Whitman Analysis

- AV (asset value)
  - Value of the asset according to the organization
- EF (exposure factor)
  - Percentage of asset loss caused by identified threat
- SLE (single loss expectancy)
  - Potential loss if attack occurs
  - (Asset value * exposure factor)
- ARO (annualized rate of occurrence)
  - Estimated frequency the threat will occur within a single year
- ALE (annualized loss expectancy) = (SLE * ARO)

Classic Whitman Analysis

Risk analysis						
Asset	**Threat**	**Asset value**	**Exposure factor**	**Single loss expectancy**	**Annualized rate of occurrence**	**Annualized loss expectancy**
SRV_1	Fire	$15000	100%	$15000	0.1	$1500
SRV_2	Fire	$20000	100%	$20000	0.1	$2000
SRV_1	Flood	$15000	100%	$15000	0.0001	$1.5
SRV_2	Flood	$20000	100%	$20000	0.0001	$2.0
SRV_1	Virus (no AV software)	$15000	10%	$1500	365	$547,500
SRV_1	Virus (with AV software)	$15000	10%	$1500	1	$1500

AWS Cloud Practitioner

Michael J. Shannon

See You Tomorrow!