Basics of cloud computing:

- Cloud Computing is an emerging style of IT delivery in which applications, data and IT resources rapidly provisioned and provided as standardized offerings to users over the web in a flexible pricing model.
- "The National Institute of Standards and Technology (NIST) defines cloud computing as a "pay-per-use model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- "The National Institute of Standards and Technology (NIST) defines cloud computing as a "pay-per-use model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Why is cloud computing necessary?

- Cost Reduction
- Universal Access
- Software Updates
- Application Alternatives
- Potential and cost Effective
- Flexibility

- Users can scale services to fit their needs, customize applications and access cloud services from anywhere with an internet connection.

Introduction to key cloud services (Compute, storage, networking):

- Fundamentally the term "compute" refers to physical servers comprised of the processing, memory, and storage required to run an operating system such as Microsoft Windows or Linux, and some virtualized networking capability.

Compute Services

The components of a compute server include the following:

- **Processor or Central Processing Unit (CPU)** – the CPU is the brains of the computer and carries out the instructions of computer programs
- **Memory or Random Access Memory (RAM)** – within a computer memory is very high-speed storage for data stored on an integrated circuit chip
- **Storage** – the storage location for the operating system files (and optionally data). This is typically a local disk stored within the computer or a network disk attached using a block protocol such as iSCSI
- **Network** – physical network interface cards (NICs) to support connectivity with other servers

- When used in cloud computing, the operating system software that is installed directly on the server is generally a hypervisor that provides a hardware abstraction layer onto which additional operating systems can be run as virtual machines (VMs) or "instances". This technique is known as hardware virtualization.

Storage as a Services(Staas)

- Storage as a service defines a business model where a large company will rent spaceon their storage infrastructure to a small company or an individual who lack thebudget to compensate for it on their own.
- The main advantage of StaaS is an enterprise in cost savings.
- The storage is rented by the provider using either accost -per-data-transferred or cost-per-gigabyte-stored model.
- The users need not to compensate for infrastructure, they just pay for how much data they transferred and saved on the server of the provider.

- If there is any loss of data, the client can get the lost data from provider of the service.
- Examples: web e-mail providers such as yahoo, Gmail, hot mail, sites like flickr, Picasa,YouTube, facebook.

Network as a service

What is cloud networking?

- **Cloud networking** is a type of IT infrastructure in which some or all of an organization's network capabilities and resources are hosted in a public or private cloud platform, managed in-house or by a service provider, and available on demand.
- Companies can either use on-premises cloud networking resources to build a private cloud network or use cloud-based networking resources in the public cloud, or a hybrid cloud combination of both. These network resources can include virtual routers, firewalls, and bandwidth and network management software, with other tools and functions available as required.

Why cloud networking?

- Businesses today turn to the cloud to drive agility, deliver differentiation, accelerate time-to-market, and increase scale. The cloud model has become the standard approach to build and deliver applications for the modern enterprise.
- Cloud networking has also played a critical role in the way organizations address their growing infrastructure needs, regional expansions, and redundancy plans. Many organizations are adopting a multi-data center strategy and leveraging multiple clouds from multiple cloud service providers (CSPs).

Benefits of cloud networking

- Most organizations have become a patchwork of on-premises technologies, public cloud services, legacy applications and systems, and emerging technologies — a complex situation that contributes to a weak security posture and results in inadequate governance, visibility, and manageability across fragmented networks.
- A **Virtual Cloud Network is VMware's vision of the future of networking**. It is an architectural approach (not a product) built in software at global scale from **edge-to-edge**, that's able to deliver consistent, pervasive connectivity and security for apps and data wherever they reside, independent of underlying physical infrastructure.
- Whether your workloads are on premises or in the cloud, the same network and security stack can be used to provide connectivity, security, and visibility
- It is also the kind of next-generation networking service consumption technology that IT is increasingly adopting to provide the digital fabric that helps unify a hyper-distributed world.

What is network virtualization?

- Network Virtualization (NV) refers to abstracting network resources that were traditionally delivered in hardware to software. NV can combine multiple physical networks to one virtual, software-based network, or it can divide one physical network into separate, independent virtual networks.
- Network virtualization software allows network administrators to move virtual machines across different domains without reconfiguring the network. The software creates a network overlay that can run separate virtual network layers on top of the same physical network fabric.

Why network virtualization?

- Network virtualization is rewriting the rules for the way services are delivered, from the software-defined data center (SDDC), to the cloud, to the edge. This approach moves networks from static, inflexible, and inefficient to dynamic, agile, and optimized. Modern networks must keep up with the demands for cloud-hosted, distributed apps, and the increasing threats of cybercriminals while delivering the speed and agility you need for faster time to market for your applications. With network virtualization, you can forget about spending days or weeks provisioning the infrastructure to support a new application. Apps can be deployed or updated in minutes for rapid time to value.

How does network virtualization work?

- Network virtualization decouples network services from the underlying hardware and allows virtual provisioning of an entire network. It makes it possible to programmatically create, provision, and manage networks all in software, while continuing to leverage the underlying physical network as the packet-forwarding backplane. Physical network resources, such as switching, routing, firewalling, load balancing, virtual private networks (VPNs), and more, are pooled, delivered in software, and require only Internet Protocol (IP) packet forwarding from the underlying physical network.
- Network and security services in software are distributed to a virtual layer (hypervisors, in the data center) and "attached" to individual workloads, such as your virtual machines (VMs) or containers, in accordance with networking and security policies defined for each connected application. When a workload is moved to another host, network services and security policies move with it. And when new workloads are created to scale an application, necessary policies are dynamically applied to these new workloads, providing greater policy consistency and network agility.

Benefits of network virtualization

- Network virtualization helps organizations achieve major advances in speed, agility, and security by automating and simplifying many of the processes that go into running a data center network and managing networking and security in the cloud. Here are some of the key benefits of network virtualization:
  - Reduce network provisioning time from weeks to minutes
  - Achieve greater operational efficiency by automating manual processes
  - Place and move workloads independently of physical topology
  - Improve network security within the data center

Network Virtualization Example

- One example of network virtualization is virtual LAN (VLAN). A VLAN is a subsection of a local area network (LAN) created with software that combines network devices into one group, regardless of physical location. VLANs can improve the speed and performance of busy networks and simplify changes or additions to the network.
- Another example is network overlays. There are various overlay technologies. One industry-standard technology is called virtual extensible local area network (VXLAN). VXLAN provides a framework for overlaying virtualized layer 2 networks over layer 3 networks, defining both an encapsulation mechanism and a control plane. Another is generic network virtualization encapsulation (GENEVE), which takes the same concepts but makes them more extensible by being flexible to multiple control plane mechanisms.
- VMware NSX Data Center – Network Virtualization Platform
- VMware NSX Data Center is a network virtualization platform that delivers networking and security components like firewalling, switching, and routing that are defined and consumed in software. NSX takes an architectural approach built on scale-out network virtualization that delivers consistent, pervasive connectivity and security for apps and data wherever they reside, independent of underlying physical infrastructure.

Cloud delivery models

List and explain various types of cloud.

Types of Clouds: Basic Cloud Types

i. Public Clouds

ii. Private Clouds

iii. Hybrid Clouds

i) Public Clouds:

Figure 2: Public Cloud

- Public clouds are open to use by the general users.
- Public clouds survive ahead of the firewall of an industry, entirely hosted and supervised by vendors such as Amazon, MS and Google.
- Works on Pay-as-you-go criterion.
- Users do not have the power of resources management.
- Every task is supervised, software updated, and security patches installed by the third party.

Private Clouds:

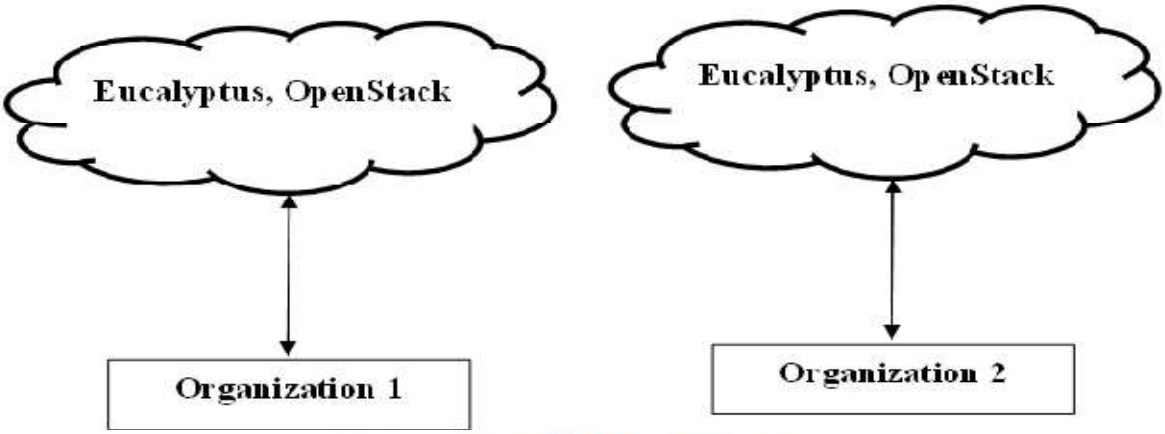


Figure 3: Private Cloud

- Private clouds exist within the firewall of an organization.
- Private clouds are entirely supervised by an enterprise.
- Possess all qualities of a public cloud with the additional responsibility of managing underlying IT infrastructure.
- It is used by the industries who have invested in their IT infrastructure massively.
- It is most suited for applications with strict security need, follow some rules or designed for regulatory tasks.

Hybrid Clouds:

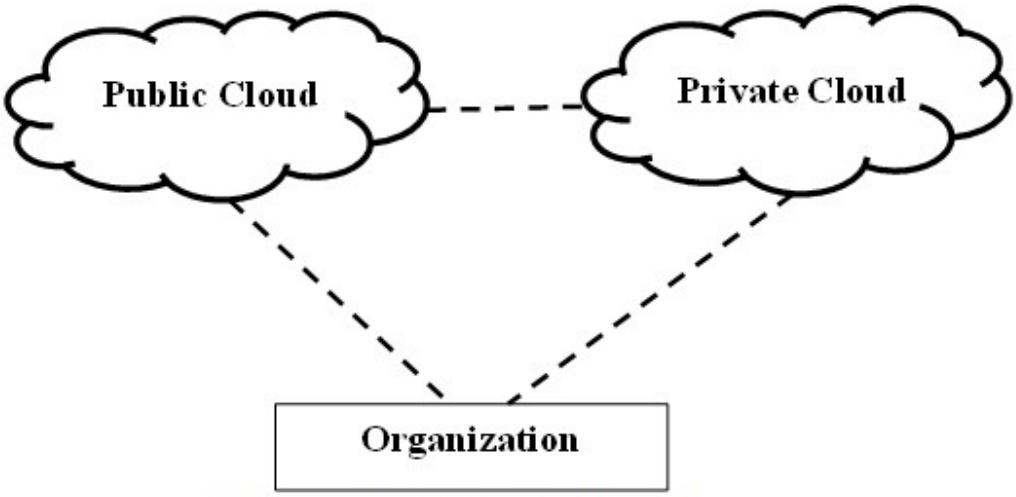


Figure 4: Hybrid Cloud

- Hybrid clouds consists of external as well as internal providers.
- It is a blend of Public as well as Private Clouds.
- Here, secure and complex applications are supervised by an organization and unsecured apps are managed by the third party vendors.
- They have distinct identity and are surrounded by standard technology.
- It enables data and application portability.
- Hybrid clouds are mainly used in Cloud bursting.

IV. Community Cloud:

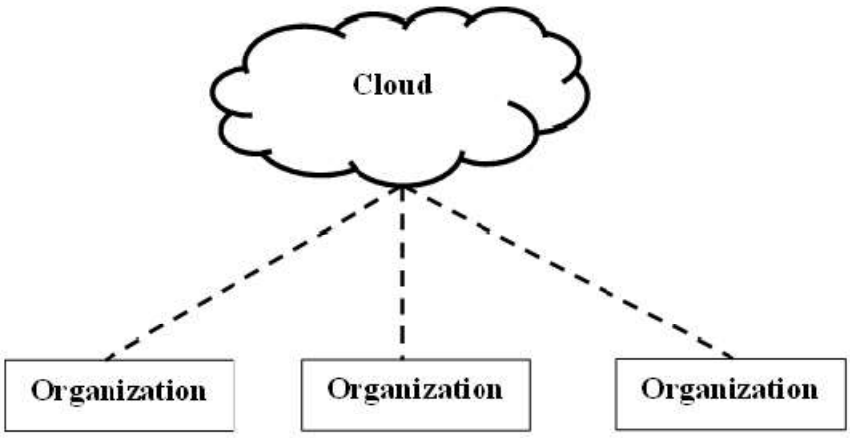


Figure 5: Community Cloud

- Community Cloud is implemented when several businesses have similar requirements and perspectives to share. These are accessible to members of a particular community, but are not available to the general public. Examples include branches of the educational organizations and government, military and industry suppliers and partners.
- These are mainly useful when the customers distribute special needs or there is a necessity for general services. By creating the virtual data centre from instances of virtual machines deployed on user machines (which are underutilized), another form of Community Cloud can be established. Thus, a Community Cloud is a kind of Private Cloud, but goes beyond a business or an organization.

Compare public cloud verses private cloud.

Sl. No.	Type	Public Cloud	Private Cloud
1	**Infrastructure Owner**	The owner of the infrastructure is the cloud provider or third party.	The owner of the infrastructure is an enterprise
2	**Cost**	The cost is less.	The cost is high.
3	**Scalability**	Scalability is on demand and unlimited.	Scalability is limited to the infrastructure installed.
4	**Security**	Concern regarding data security.	Security is high.
5	**Performance**	The performance is hard to attain for unpredictable environments.	The performance is guaranteed.
6	**Control and Management**	The public cloud manipulates the virtual machines which result in less management burden.	The private cloud has a high level of control over the resources which requires extra expertise to manage them.

IaaS v/s PaaS v/s SaaS

Explain application as a Service (SaaS) with a neat diagram and also list its isadvantages.

- Application as a Service can also be called as Software as a Service, which is simply written SaaS. In SaaS, customers rent software hosted by the vendor. This service is defined as a distribution model where the applications are hosted by a service provider or a vendor and made accessible to users over the internet. Software as a Service is similar to Application Service Provider (ASP) where a provider hosts available applications or software for the users and delivers those over the web.
- The merits of the model which includes this service are global accessibility, easy administration, compatibility, that is, all customers can use the same software version. With SaaS, tasks such as application or software deployment, maintenance, and keeping it working correctly from testing, managing patches, observing performance, etc., will be managed by the provider.
- In simple words, it can be understood as a provider hosts software or centrally located application, and can be made available for easy access to customers over the network, that is, internet on the basis of payment.

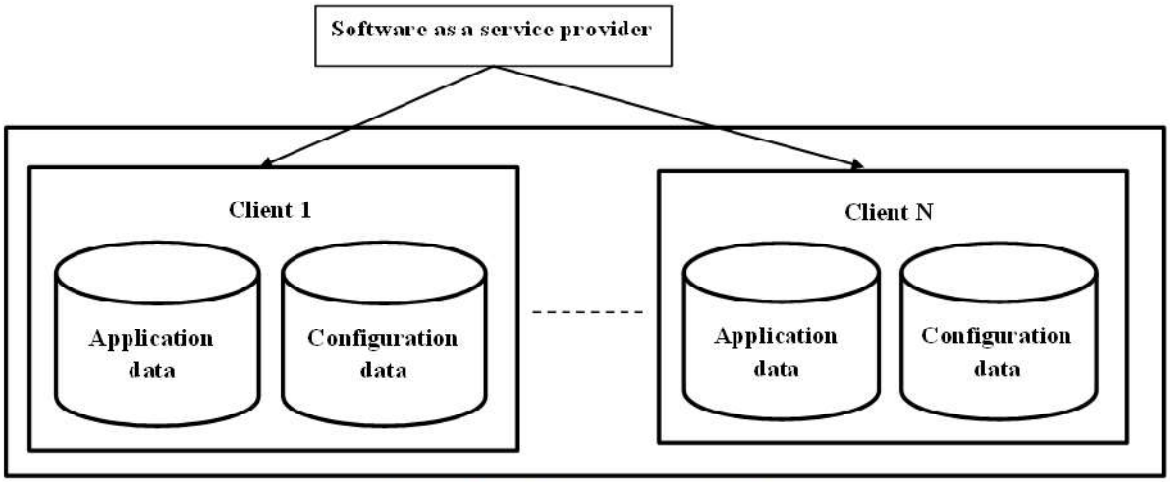


Figure 8: Software as a Service

Disadvantages of SaaS

1. Security is a major concern since the whole data will be in Cloud.
2. Switching between different SaaS vendors is a little bit challenging as it may involve a slow and difficult process of transferring very big data files through the internet.
3. Internet connection is mandatory.
4. Software as a Service model is not apt for the applications which demand response time in milliseconds.

12. (a) Explain Application /Software as a Service.

(b) What are the advantages and disadvantages of SaaS?

(a) Application as a service is also called as Software as a service(SaaS).

- In SaaS Customers rent s/w hosted by the vendors. This is defined as a software distribution model where the applications arehosted by a service provider and made accessible to the users over the internet.

(b) Advantages of SaaS:

- The service model SaaS facilitates the enterprises that all locations are using the application of the correct version.
- SaaS also increases the accessibility of application to global localities.
  - customization
  - security
  - web reliability
  - more bandwidth
- SaaS involves less maintenance of set-up, installation, monitoring of software.

Disadvantages of SaaS:

- Security is a major concern since the whole data will be in the cloud Internet connection is mandatory
- Switching different SaaS vendors is a little bit challenging as it may involve a slow and difficult process of transferring very big data files through internet
- Software as a service (SaaS) model is not apt for applications which demand for response time in milliseconds

Describe the importance of Platform as a service (PaaS).

- Paas provides hardware,storage,operating systems & network capacity on a charge basis over the network internet.
- It includes services for application development and deployment.
- PaaS is a verified model for running applications without the difficulty of maintaining software and hardware infrastructure at your own company.
- It allows users to create web applications very quickly, without bothering about the cost and complexity of buying and also managing the related hardware/software.
- PaaS is used to build multi-tenant applications.
- The developer's duty is simply to write the code by using the services provided by PaaS and the PaaS provider will take care of uploading that code and making it available to the users through the internet.

Advantages of IaaS cloud computing layer

There are the following advantages of IaaS computing layer -

1. Shared infrastructure

- IaaS allows multiple users to share the same physical infrastructure.

2. Web access to the resources

- Iaas allows IT users to access resources over the internet.

3. Pay-as-per-use model

- IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.

4. Focus on the core business

- IaaS providers focus on the organization's core business rather than on IT infrastructure.

5. On-demand scalability

- On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

Disadvantages of IaaS cloud computing layer

1. Security

- Security is one of the biggest issues in IaaS. Most of the IaaS providers are not able to provide 100% security.

2. Maintenance & Upgrade

- Although IaaS service providers maintain the software, but they do not upgrade the software for some organizations.

3. Interoperability issues

- It is difficult to migrate VM from one IaaS provider to the other, so the customers might face problem related to vendor lock-in.

Some important point about IaaS cloud computing layer

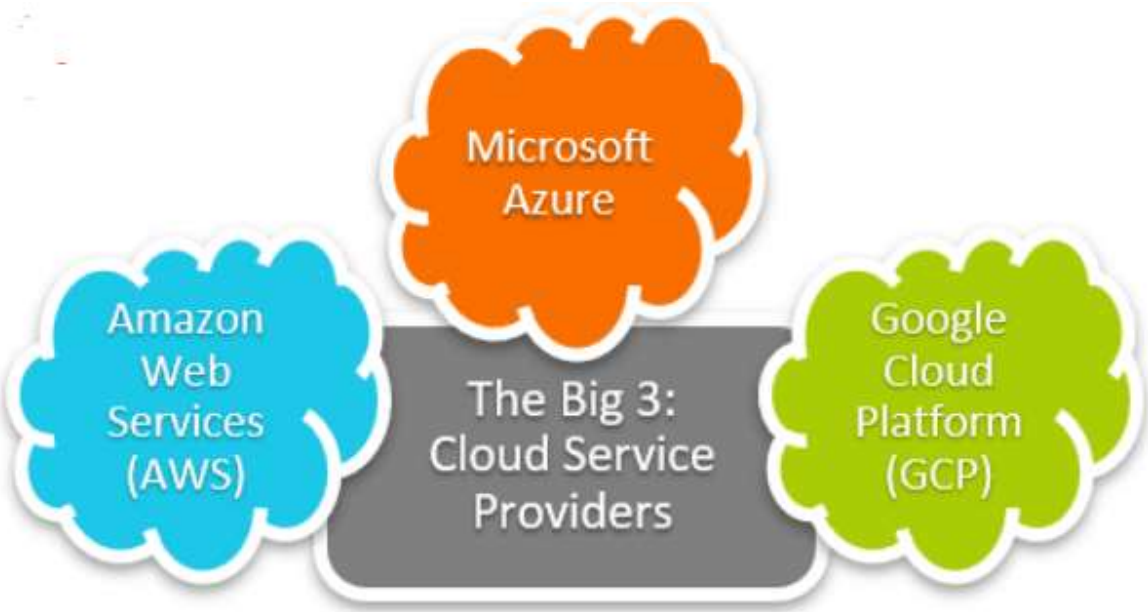
- IaaS cloud computing platform cannot replace the traditional hosting method, but it provides more than that, and each resource which are used are predictable as per the usage.
- IaaS cloud computing platform may not eliminate the need for an in-house IT department. It will be needed to monitor or control the IaaS setup. IT salary expenditure might not reduce significantly, but other IT expenses can be reduced.
- Breakdowns at the IaaS cloud computing platform vendor's can bring your business to the halt stage. Assess the IaaS cloud computing platform vendor's stability and finances. Make sure that SLAs (i.e., Service Level Agreement) provide backups for data, hardware, network, and application failures. Image portability and third-party support is a plus point.
- The IaaS cloud computing platform vendor can get access to your sensitive data. So, engage with credible companies or organizations. Study their security policies and precautions.

Introduction to cloud vendors(Azure,AWS, GCP)

- A cloud service provider is an information technology (IT) company that provides its customers with computing resources over the internet and delivers them on-demand.
- Cloud computing is like your water/ electricity bill; you **only pay for what you use**. In this way cloud vendors provide Pay-as-you-go Model for cloud users.
- Cloud Service providers (CSP) offers various services such as Software as a Service**,** Platform as a service**,** Infrastructure as a service**,** network services**,** business applications**,** mobile applications**,** and infrastructure in the cloud.
- The cloud service providers host these services in a data center, and users can access these services through cloud provider companies using an Internet connection.
- CSPs are well-suited for organizations and individuals who don't want the responsibility of installing software, hardware or network resources and maintaining them until the end of their life cycles.

There are the following Cloud Service Providers Companies –

1.Amazon Web Services (AWS)
2. Microsoft Azure
3. Google Cloud Platform (GCP)
4. IBM Cloud Services
5. VMware Cloud
6. Oracle cloud
7. Red Hat
8. DigitalOcean
9. Rackspace
10. Alibaba Cloud



Amazon Web Services (AWS)

- Amazon Web Services is a **secure cloud service platform** provided by **Amazon** company.
- AWS started its life as an internal cloud offering by 2006,
- AWS is the most mature cloud platform offering a wide range of services to practically everyone: individual developers, large enterprises, and even governments.
- It offers various services such as database storage, computing power, content delivery, Relational Database, Simple Email, Simple Queue, and other functionality to increase the organization's growth.
- It had evolved into a publicly available cloud platform with services like Amazon S3 cloud storage and elastic compute cloud (EC2). serve millions of users.
- **Features of AWS**
- AWS provides various powerful features for building scalable, cost-effective, enterprise applications. Some important features of AWSis given below-
- AWS is **scalable** because it has an ability to scale the computing resources up or down according to the organization's demand.

- AWS is cost-effective as it works on a pay-as-you-go pricing model.
- It provides various flexible storage options.
- It offers various security services such as infrastructure security, data encryption, monitoring & logging, identity & access control, penetration testing, and DDoS attacks.
- It can efficiently manage and secure Windows workloads.

Prominent AWS customers include:

- Expedia
- Netflix
- Coinbase
- Formula 1
- Coca Cola
- Intuit
- Airbnb
- Lyft
- Coursera
- Food and Drug Administration (FDA)

2. Microsoft Azure

- Microsoft Azureis also known as **Windows Azure**. It supports various operating systems, databases, programming languages, frameworks that allow IT professionals to easily build, deploy, and manage applications through a worldwide network. It also allows users to create different groups for related utilities.

- Microsoft Azure is the second-largest cloud platform. Debuting in 2010, Azure has evolved into a cloud platform with more than 200 products and services. Today, it is among the fastest-growing cloud platforms.
- As Microsoft offers Azure, it provides a wide array of services tailored particularly for Microsoft-centric enterprises—making the switch to a cloud or a hybrid-cloud environment smooth for many organizations.
- In use by more than 95% of Fortune 500 companies, Microsoft Azure has a proven track record in catering to enterprise users.
- Importantly, Azure is not limited to Windows-based services. It also supports open-source languages, technologies, and platforms, giving anyone the freedom to build and support any application.

Features of Microsoft Azure

- Microsoft Azure provides **scalable**, **flexible**, and **cost-effective**
- It allows developers to quickly manage applications and websites.
- It managed each resource individually.

- Its IaaS infrastructure allows us to launch a general-purpose virtual machine in different platforms such as Windows and Linux.
- It offers a **Content Delivery System (CDS)** for delivering the Images, videos, audios, and applications.

Well-known Azure customers include:

- DAIMLER AG
- McKesson Group
- Asos
- Center of Disease Control (CDC) – US
- National Health Service (NHS) – UK
- HSBC
- Starbucks
- Walgreens
- 3M
- HP
- Mitsubishi Electric
- Renault
- eBay, Samsung, Rolls-Royce

3. Google Cloud Platform(GCP)

- Google cloud platform is a product of **Google**. It consists of a set of physical devices, such as computers, hard disk drives, and virtual machines. It also helps organizations to simplify the migration process.

- Available to the general public beginning in 2010, the Google Cloud Platform currently offers over 100 services spanning computing, networking, big data, and more. Today GCP consists of services including Google Workspace, enterprise Android, and Chrome OS.

- Compared to AWS and Azure, GCP is the smallest of the Big 3 cloud providers. Yet it offers a robust set of cloud services to power and support any kind of application.
- Notable GCP customers include:
  - Toyota
  - Unilever
  - Nintendo
  - Spotify
  - The Home Depot
  - Target

- Twitter
- Paypal
- UPS

Features of Google Cloud

- Google cloud includes various **big data services** such as Google BigQuery, Google CloudDataproc, Google CloudDatalab, and Google Cloud Pub/Sub.
- It provides various services related to **networking**, including Google Virtual Private Cloud (VPC), Content Delivery Network, Google Cloud Load Balancing, Google Cloud Interconnect, and Google Cloud DNS.
- It offers various **scalable** and **high-performance**
- GCP provides various **serverless services** such as Messaging, Data Warehouse, Database, Compute, Storage, Data Processing, and Machine learning (ML)
- It provides a free cloud shell environment with Boost Mode.

How to choose a cloud service provider

Organizations evaluating potential cloud partners should consider the following factors:

- **Cost.** The cost is usually based on a per-use utility model, but all subscription details and provider-specific variations must be reviewed. Cost is often considered one of the main reasons to adopt a cloud service platform.
- **Tools and features.** An overall assessment of a provider's features, including data management and security features, is important to ensure it meets current and future IT needs.
- **Physical location of the servers**. Server location may be an important factor for sensitive data, which must meet data storage regulations.
- **Reliability.** Reliability is crucial if customers' data must be accessible. For example, a typical cloud storage provider's SLA specifies precise levels of service -- such as 99.9% uptime -- and the recourse or compensation the user is entitled to should the provider fail to deliver the service as described. However, it's important to understand the fine print in SLAs, because some providers discount outages of less than 10 minutes, which may be too long for some businesses.
- **Security.**Cloud security should top the list of cloud service provider considerations. Organizations such as the Cloud Security Alliance offer certification to cloud providers that meet its criteria.
- **Business strategy.** An organization's business requirements should align with the offerings and technical capabilities of a potential cloud provider to meet both current and long-term enterprise goals.

How to choose a cloud service provider

- There are many factors to consider when choosing a CSP. Let’s take a look at the most common angles.
- **Regions and availability**
- When choosing a cloud provider, the first thing to consider is its supported regions and availability. These directly impact the performance of your cloud, due to factors like latency and compliance requirements, especially when dealing with data.
- As of September 2021, here’s where the Big 3 stand:
- **Amazon Web Service** has 25 geographic regions with 81 availability zones. 218+ edge locations, and 12 Regional Edge Caches.
- **Microsoft Azure** runs 60+ regions with a minimum of three availability zones in each region with more than 116 edge locations (Points of Presence).
- **Google Cloud Platform** has 27 cloud regions with 82 zones and 146 edge locations.

- Common services
- AWS and Azure have the largest service catalogs by offering more than 200+ services. GCP currently offers around 100+ services. A general breakdown of services is:
- AWS has the largest catalog of services.
- Azure is a close second with an impressive set of AI, ML, and analytics services.
- Google Cloud Platform comes in third place for the number of services offered.
- In this section, let's take a look at the common service offerings of each cloud platform.
- **Compute Services**

SERVICE	AWS	AZURE	GCP
VM (Compute Instance)	EC2 (Elastic Compute)	Azure Virtual Machine	Google Compute Engine

Database & Storage Services

SERVICE	AWS	AZURE	GCP
RDBMS (Multiple Database Types – SQL, MySQL, etc..)	AWS RDS	Azure SQL/ Database for MySQL/PostgreSQL	Cloud SQL
File Storage	Elastic File System	Azure File Storage	Google Filestore

Networking

SERVICE	AWS	AZURE	GCP
Virtual Network	Virtual Private Cloud (VPC)	Virtual Network (Vnet)	Virtual Private Cloud (VPC)
Load Balancing	Elastic Load Balancer	Azure Load Balancer	Google Cloud Load Balancing

Pricing

The pricing of the cloud platform depends on many factors:

- Customer requirements
- Usage
- The services used

AWS vs Azure vs GCP: pros & cons

AWS	
Pros	**Cons**
• Most services available, from networking to robotics • Most mature • Considered the gold standard in cloud reliability and security • More compute capacity vs Azure & GCP • All major software vendors make their programs available on AWS	• Dev/Enterprise support must be purchased • Can overwhelm newcomers with the sheer number of services and options • Comparatively limited options for hybrid cloud
MICROSOFT AZURE	
Pros	**Cons**
• Easy integration and migrations for existing Microsoft services • Many services available, including best-in-class AI, ML, and analytics services • Relatively cheaper for most services vs AWS & GCP • Great support for hybrid cloud strategies	• Fewer service offerings vs AWS • Particularly geared towards enterprise customers
GCP	
Pros	**Cons**
• Plays nicely with other Google service and products • Excellent support for containerized workloads • Global fiber network	• Limited services vs AWS & Azure • Limited support for enterprise use cases

- All three platforms offer competitive pricing plans with additional cost management options—reserved instances, budgets, and resource optimization—available to all users.
- The consensus in the IT community is that Microsoft Azure has the lowest on-demand pricing while Amazon tends to come somewhere around the middle.
- However, there is a clear advantage when enterprise customers already using Microsoft services (Windows, active directory, MS SQL, etc.) move to Azure as it is significantly cheaper than other cloud providers.

The 14 Cloud Security Principles explained

- Cloud security is an essential part of today's cyber security landscape. With hybrid working now the norm, many organisations are relying on Cloud services to access data from home or the office.
- But whenever organisations adopt technological solutions such as this, they must acknowledge the risks that come with it. Indeed, Cloud computing can increase the risk of data breaches and regulatory non-compliance, as well as introducing other vulnerabilities.
- To mitigate these risks, the NCSC (National Cyber Security Centre) created the Cloud Security Principles, which outline 14 guidelines for protecting information stored online.

1. Data in transit protection

- **What the NCSC says**: User data transiting networks should be adequately protected against tampering and eavesdropping.
- **How you can achieve it**: There are many ways you can bolster your network security, such as auditing and mapping your infrastructure to look for vulnerabilities. This might include spotting misconfigured firewalls or physical security threats.
- You should also make sure firmware and software are up to date, check that default passwords have been changed and secure your physical premises.
- Additionally, you should consider encrypting data or using VPNs where possible. Encryption can greatly reduce the risk of data being compromised in transit, but it will also make sharing data more complex and will require significant resources.
- Meanwhile, VPNs protect remote users by extending your organisation's private network across a public network. This enables employees to send and receive data as if their computer was directly connected to your organisation's network.

2. Asset protection and resilience

- **What the NCSC says**: User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
- **How you can achieve it**: The NCSC breaks down this principle into six parts: physical location and legal jurisdiction, data centre security, data at rest protection, data sanitisation, equipment disposal, and physical resilience and availability.
- Physical location and legal jurisdiction is relevant if you are subject to laws such as the GDPR (General Data Protection Regulation), which contain strict rules on data depending on its location.
- To determine this, you must identify the locations at which your data is stored, processed and managed, and consider how this affects your compliance with relevant legislation.
- Similarly, you should consider whether the legal jurisdiction within which the Cloud service provider operates applies to you.
- Data centre security refers to the controls you have implemented to protect the physical locations in which data is stored. This should cover the threat of unauthorised access, tampering, theft and reconfiguration of systems.
- Data at rest protection refers to the security of information stored in the Cloud, and data sanitation refers to the process of supplying resources, transferring them and having users return them when no longer needed.
- Equipment disposal requires organisations to securely delete or discard information at the end of its lifecycle. Physical records should be shredded, while digital documents and other relevant information – such as credentials and configuring information – should be wiped from hard drives.
- Finally, physical resilience and availability refers to an organisation's ability to function in the event of failures, security incidents and cyber attacks.

3. Separation between users

- **What the NCSC says**: A malicious or compromised user of the service should not be able to affect the service or data of another.
- **How you can achieve it**: Factors that affect user separation include where the separation controls are implemented, who the organisation shares the service with and the level of assurance available in the implementation of separation controls.
- As such, organisations must understand the types of user that they share the Cloud service with and implement appropriate tools. This might include virtualisation technologies or other software that can separate users.
- Whenever organisations use such tools, they must also conduct regular penetration tests on their infrastructure and web applications to look for vulnerabilities.

4. Governance framework

- **What the NCSC says**: The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.
- **How you can achieve it**: Organisations should begin by appointing a board representative (or a person with the direct delegated authority) to take responsibility for the security of the Cloud service. This will typically be the chief information officer, chief security officer or someone with a similar title.
- Next, they should document a framework for security governance containing policies addressing key aspects of information security.
- The organisation must also implement processes to identify and ensure compliance with relevant legal and regulatory requirements.

5. Operational security

- **What the NCSC says**: The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.
- **How you can achieve it**: There are four things to consider here, the first of which is configuration and change management. This means ensuring that changes to the system have been properly tested and authorised.
- The second thing to consider is vulnerability management, which involves identifying and mitigating security issues in constituent components.
- Third, you must implement protective monitoring, which enables you to detect cyber attacks and unauthorised activity on the service.
- Finally, you must create an incident management system to ensure that you can respond to incidents and recover a secure, available service.

6. Personnel security

- **What the NCSC says**: Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.
- **How you can achieve it**: Service providers must conduct security screening for employees and provide regular security training.
- This should include explanations of the security responsibilities associated with specific roles and the ways in which the organisation screens and manages personnel within privileged roles.
- BS7858 outlines a basic standard for personnel screening, and organisations are advised to follow its guidelines.

7. Secure development

- **What the NCSC says**: Services should be designed and developed to identify and mitigate threats to their security. Those that aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.
- **How you can achieve it**: Organisations must create an ISO 27001 secure development policy to ensure that development is carried out in line with industry good practice.
- They should also regularly monitor new and evolving threats, taking appropriate steps to adjust their service accordingly.
- Additionally, organisations should implement configuration management processes to guarantee the integrity of the solution through development, testing and deployment.

8. Supply chain security

- **What the NCSC says**: The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.
- **How you can achieve it**: If your organisation relies on third-party products and services, you must understand how your information is shared with and accessible to those partners and how it flows through their supply chain.
- You must also review the service provider's procurement processes, looking at the security requirements it places on third-party suppliers. Similarly, you must understand how the service provider manages third-party security risks and the ways it enforces the security requirements of its suppliers.
- Finally, you should review how the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.

9. Secure user management

- **What the NCSC says**: Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.
- **How you can achieve it**: There are two things you must address here. First, users must be properly authenticated before they are allowed to perform management activities, report faults or request changes to the service.
- These changes can be performed through a service management web portal or by telephone/email.
- Second, you must implement role-based access controls within management interfaces to prevent users from making unauthorised changes that could affect the service.
- This step also protects management interfaces in the event that an employee's account is compromised by criminal hackers.

10. Identity and authentication

- **What the NCSC says**: All access to service interfaces should be constrained to authenticated and authorised individuals.
- **How you can achieve it**: This principle requires a series of technical solutions. First, you should implement two-factor authentication to strengthen the login process.
- By doing this, you protect employees' accounts in the event that their password is compromised, because an attacker will still need the hardware or software token.
- You should also obtain a TLS client certificate, which will provide strong cryptographic protection, and implement identity federation with your existing identity provider.

11. External interface protection

- **What the NCSC says**: All external or less trusted interfaces of the service should be identified and

appropriately defended.

- **How you can achieve it**: You must first understand the physical and logical interfaces from which your information is available and how access to your data is controlled.
- Once you have this information, you must implement measures to ensure that the service identifies and authenticates users to an appropriate level over those interfaces. This includes the Internet, community networks and private networks.

12. Secure service administration

- **What the NCSC says**: Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.
- **How you can achieve it**: To begin, you must understand which service administration model is being used by.
- Next, you should assess the risks associated with that administration model. The NCSC outlines those risks on its website. If you cannot determine which service administration model is used, you should refer to the risks associated with the *Direct service administration* approach.

13. Audit information for users

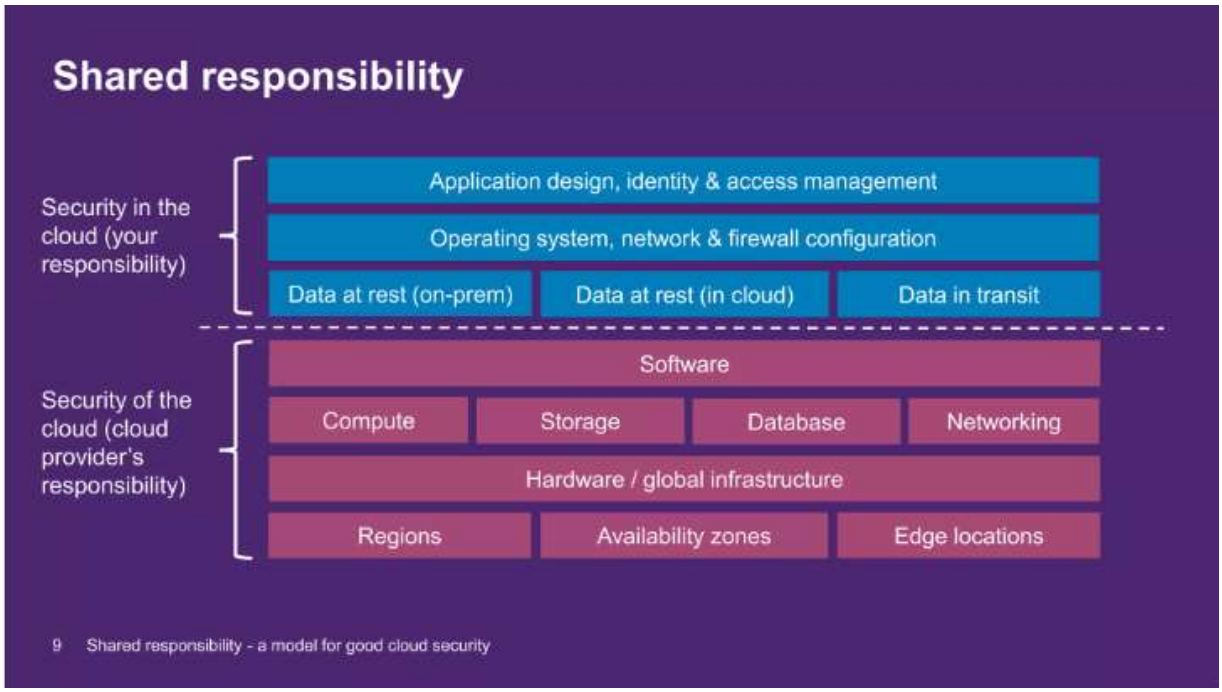
- **What the NCSC says**: You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.
- **How you can achieve it**: This principle refers to the way in which you will receive audit information rather than what you will do with it.
- As such, your requirements relate to the processes related to receiving the information. This means establishing how and when audit information will be provided, including the format of the data, and the data retention period associated with it.
- The NCSC splits this into three potential scenarios: the service provider might not offer any audit information, it might provide some information (perhaps as a result of negotiation) or it might make specific information available.
- For the audit information to be useful, you must insist on receiving complete, specific details. If you don't, you will face regulatory compliance issues and could be at greater risk of security incidents.

14. Secure use of the service

- **What the NCSC says**: The security of Cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.
- **How you can achieve it**: Your responsibilities here are subject to the deployment models you use, the features of those services and the scenario in which you intend to use the service.
- For example, with infrastructure- and platform-as-a-service offerings, the organisation is responsible for significant aspects of their security, including the installation and configuration of an operating system, the deployment of applications and their maintenance.
- The NCSC provides a guide for organisations configuring infrastructure-as-a-service securely.
- Separately, it recommends that organisations identify the security requirements related to its use of service and educate staff on how to use and manage that service securely.

Shared Responsibility Model:

- The **Shared Responsibility Model** is a security and compliance framework that outlines the responsibilities of **cloud service providers (CSPs)** and **customers** for securing every aspect of the cloud environment, including hardware, infrastructure, endpoints, data, configurations, settings, operating system (OS), network controls and access rights.
- In its simplest terms, the Shared Responsibility Model dictates that the cloud provider—such as Amazon Web Service (AWS), Microsoft Azure, or Google Cloud Platform (GCP)—must monitor and respond to security threats related to the cloud itself and its underlying infrastructure. Meanwhile, end users, including individuals and companies, are responsible for protecting data and other assets they store in any cloud environment.



- When an enterprise runs and manages its own IT infrastructure on premises, within its own data center, the enterprise -- and its IT staff, managers and employees -- is responsible for the security of that infrastructure, as well as the applications and data that run on it. When an organization moves to a public cloud computing model, it hands off some, but not all, of these IT security responsibilities to its cloud provider. Each party -- the cloud provider and cloud user -- is accountable for different aspects of security and must work together to ensure full coverage.
- While the responsibility for security in a public cloud is shared between the provider and the customer, it's important to understand how the responsibilities are distributed depending on the provider and the specific cloud model.
- The type of cloud service model -- infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) -- dictates who is responsible for which security tasks. According to the Cloud Standards Customer Council, an advocacy group for cloud users, users' responsibilities generally increase as they move from SaaS to PaaS to IaaS.

Amaznon's AWS Shared Responsibility Model

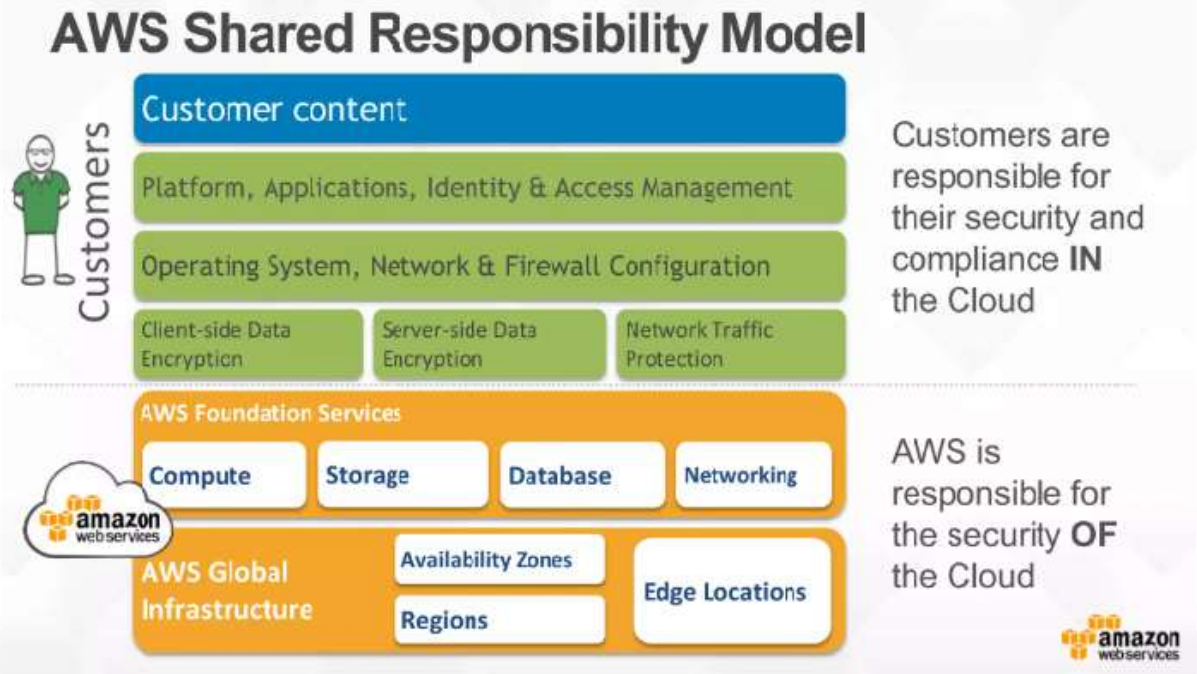


Fig:The cloud service provider's and user's security responsibilities vary depending on whether they're using the IaaS, PaaS or SaaS model.

The cloud service provider's and user's security responsibilities vary depending on whether they're using the IaaS, PaaS or SaaS model.

- **IaaS.** The cloud provider is responsible for services and storage -- the basic cloud infrastructure components such as virtualization layer, disks and networks.
- The provider is also responsible for the physical security of the data centers that house its infrastructure. IaaS users, on the other hand, are generally responsible for the security of the OS and software stack required to run their applications, as well as their data.
- **PaaS.** When the provider supplies a more comprehensive platform, the provider assumes greater responsibility that extends to the platform applications and OSes.

- For example, the provider ensures that user subscriptions and login credentials are secure, but the user is still responsible for the security of any code or data -- or other content -- produced on the platform.
- **SaaS.** The provider is responsible for almost every aspect of security, from the underlying infrastructure to the service application, such as an HR or finance tool, to the data the application produces.
- Users still bear some security responsibilities such as protecting login credentials from phishing or social engineering attacks.

The customer's typical cloud security responsibilities

In general terms, a cloud customer is always responsible for configurations and settings that are under their direct control, including the following:

- **Data.** A user must ensure that any data created on or uploaded to the cloud is properly secured. This can include the user's creation of authorizations to access the data, as well as the use of encryption to protect the data from unauthorized access.
- **Applications.** If a user placed a workload into a cloud VM, the user is still fully responsible for securing that workload. This can include creating secure (hardened) code through proper design, testing and patching; configuring and maintaining proper identity and access management (IAM); and securing any integrations -- the security of connected systems such as local databases or other workloads.
- **Credentials.** Users control the IAM environment such as login mechanisms, single sign-on, certificates, encryption keys, passwords and any multifactor authentication items.
- **Configurations.** The process of provisioning a cloud environment includes a significant amount of user control through configuration settings. Any cloud instances must be configured in a secure manner using the provider's tools and options.
- **Outside connections.** Beyond the cloud, the user is still responsible for anything in the business that connects to the cloud such as traditional local data center infrastructure and applications.

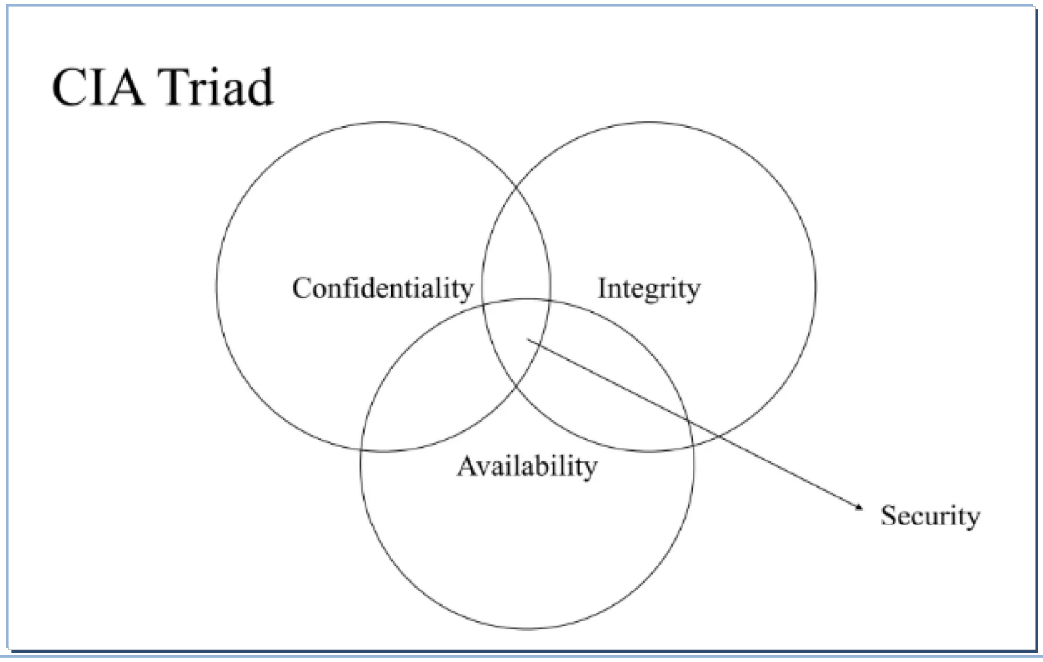
The provider's typical cloud security responsibilities

Public clouds present a vast and complex infrastructure, and cloud providers will always be completely responsible for that infrastructure, including the following components:

- **Physical layer.** The provider manages and protects the elements of its physical infrastructure. This includes servers, storage, network gear and other hardware as well as facilities. An infrastructure typically includes various resilient architectures such as redundancy and failover, as well as redundant power and network carrier connectivity. Infrastructure management also frequently includes backup, restoration and disaster recovery implementations.
- **Virtualization layer.** Public clouds are fundamentally do-it-yourself environments where users can provision and use as many resources and services as they wish. But such flexibility demands a high level of virtualization, automation and orchestration within the provider's infrastructure. The provider is responsible for implementing and maintaining this virtualization/abstraction layer as well as its various APIs, which serve as the means of user access and interaction with the infrastructure.
- **Provider services.** Cloud providers typically offer a range of dedicated or pre-built services such as databases, caches, firewalls, serverless computing, machine learning and big data processing. These pre-built services can be provisioned and used by customers but are completely implemented and managed by the cloud providers -- including any OSes and applications needed to run those services.

Principle of least privilege :

- The principle of least privilege (PoLP) stipulates that users should be granted the least privileges they need to carry out their role, and is arguably one of the most important principals of data security.
- PoLP helps to minimize the attack surface – limiting the amount of damage that can be caused were an attacker to gain access to a set of credentials. Likewise, PoLP helps to protect against both negligent and malicious insiders.
- As Governments across the globe introduce their own stringent data privacy regulations, a failure to adequately restrict access to personal data could result in costly lawsuits and fines.



Security Goals (general)

- *Confidentiality (Secrecy or Privacy)* – Resources can be accessed only by authorized parties
- *Integrity* – Resources can be modified only by authorized parties
- *Availability* – Resources should be accessible to authorized parties at appropriate times.

Tips for implementing Least Privilege in the cloud

Assigning the appropriate access controls requires some initial housekeeping, which includes locating your critical assets, and removing any redundant data and accounts. When implementing the principal of least privilege in the cloud, ideally, you should use a single Identify Access Management (IAM) solution, and a single solution for monitoring permissions. Your chosen auditing solution should be able to aggregate and correlate event logs from multiple cloud platforms, as well as hybrid environments.

1. Discover & classify your sensitive data

- Perhaps the best place to start would be to ensure that we know exactly what sensitive data we have, and where it is located. Most popular cloud platforms provide data classification capabilities out-of-the-box, including AWS, Azure and Google Cloud. However, for multi-cloud or hybrid environments, there are third-party solutions which will scan your local and remote repositories and automatically discover and classify sensitive data as it is found. Some solutions can also classify sensitive data at the point of creation. It's always good practice you make sure that any redundant data is removed before attempting to implement PoLP. Establishing a profound understanding of what data you have makes the process of assigning access rights considerably easier.

2. Implement Role-Based Access Control (RBAC)

- A common technique that is used to simplify the process of setting up PoLP is Role-Based Access Control (RBAC). As opposed to trying to assign access rights to specific individuals, you can define a comprehensive set of roles, each with their respective privileges, and assign users to these roles on an ad-hoc basis. While RBAC is arguably less granular than assigning access rights on a per-user basis, it is generally more secure as it is less prone to error. Most popular cloud platforms provide role-based access control, including AWS, Azure and Google Cloud.

3. Identify and remove inactive user accounts

- You will need to ensure that any inactive user accounts are identified and removed before implementing PoLP. Since inactive user accounts are rarely monitored, hackers often target them as it enables them to gain persistent access to the network with less risk of getting caught.

4. Monitor privileged accounts in real-time

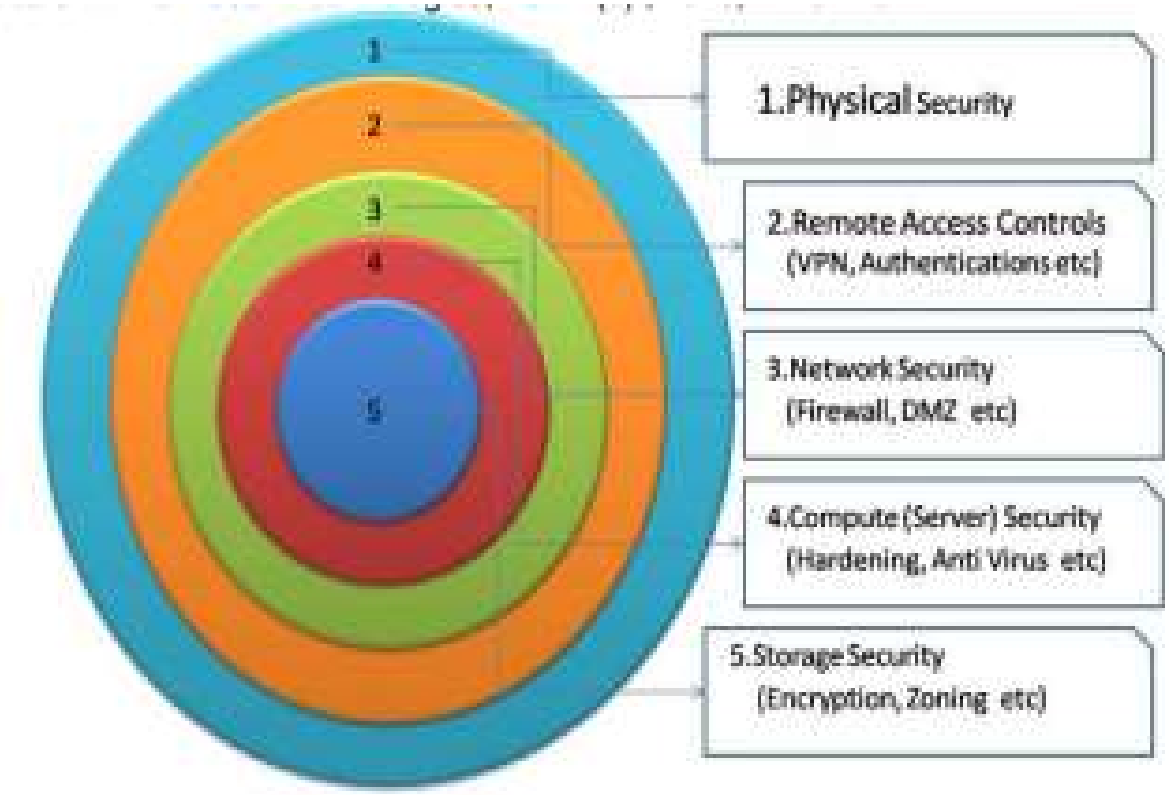
- You will need to ensure that you have as much visibility as possible into who is already accessing what data, and when. Most real-time auditing solutions use machine learning techniques to monitor user behavior and establish usage patterns which can be tested against in order to identify anomalies. Once you have an understanding of each user's behavioral patterns, you can use this information as a guide to determine what data each user should have access to.

5. Implement dynamic access controls and Just In Time (JIT) access

- Of course, there are times when a user may need access to assets which they don't normally need access to. For obvious reasons, we cannot simply grant access to a user just because they ask for it. There needs to be a formal process to determine the legitimacy of their request.

Defense in depth

- Defense-in-depth represents the use of multiplesecurity defenses to help mitigate the risk of security threats, if one component of the defense is being compromised.
- An example, could be an antivirus software installed on individual VM when there is already a virus protection on the firewalls within the same environment.
- Different security products from multiple vendors may be deployed to defend different potential vulnerable resources within the network.



ADVANTAGES OF APPROACH

- Multilayered cloud security approach
- Minimizes the risk of security breach even other components of the system get compromised.
- Compete CIA triad assurance for critical enterprise business information and applications.
- Provides additional time to detect and respond to the attacks.
- Can handle higher velocity and different varieties of attacks.
- Crucial data storage is at the deepest layer to provide stronger protection.
- Includes all the areas of possible security vulnerabilities even with the virtualized components.
- Complete security solution for cloud computing, well suited for all types of deployment models of cloud.
- Use of best practice security mechanisms in the different areas of concerns.
- Meets all the requirements of the SLAs and other legal issues.
- Performance management and focus on the availability of the cloud resources and services.
- Less overheads on the client sites so to avoid throughput issues.
- The overall cost of the approach is higher, but can be optimized.

Defense in Depth (DiD) refers to an information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data within.

Threat actors, diagrams & trust boundaries

- **Threat Actor:** "A **threat actor**, also called a **malicious actor**, is an entity that is partially or wholly responsible for a security incident that impacts – or has the potential to impact – an organization's security."
- A threat actor – compared to a hacker or attacker – does not necessarily have any technical skill sets.
- They are a person or organization with malicious intent and a mission to compromise an organization's security or data. This could be anything from physical destruction to simply copying sensitive information.
- **Hacker:** A hacker can "hack" his or her way through the security levels of a computer system or network.
- **Attacker:**A **cyberattack** is any offensive maneuver that targets computer information systems, computer networks, infrastructures, or personal computer devices.

- A Hackers and attackers are technical personas or organizations intentionally targeting technology to create an incident and, hopefully (for them, not you), a breach. They can be solo individuals, groups, or even nation-states with goals and missions to destabilize a business, government, to disseminate information, or for financial gain.
- **Assets** – a resource of value. May be tangible or intangible. Usually referred to a 'Object'.
- **Threat** – Undesired act that potentially occurs causing compromise or damage of an asset.
- **Threat Agent** – Something/someone that makes the threat materialize. Usually referred to as 'Subject'
- Vulnerability – Weakness that makes an attack possible.
- **Attack –** Act of malicious threat agent. Also known as Exploit.
- **Safeguard (Countermeasure)** – address vulnerabilities (not threats directly);
- For example – Application Design, Writing Secure Code, deploy with least privilege
- Probability – the potential chance of a threat being realized by an attack on an asset
- Impact – Outcome of the materialized threat.

Four main types of threat actors that you may need to worry about:

- Organized crime or independent criminals, interested primarily in making money.
- Hacktivists, interested primarily in discrediting you by releasing stolen data, committing acts of vandalism, or disrupting your business.
- Inside attackers, usually interested in discrediting you or making money.
- State actors, who may be interested in stealing secrets or disrupting your business.

Cloud asset management

- Cloud asset management is the process used to control an organization's cloud infrastructure and the application data within the cloud.
- Many organizations use a variety of cloud-based applications to store and manage their digital assets.
- With a collection of cloud-based asset sources, CAM helps organize assets to avoid operational hiccups and security concerns.
- Incorporating the use of cloud asset management practices provides an organization with visibility and easy control over the digital assets within the company cloud.
- Optimizing an organization's asset cloud allows users to efficiently access company data when necessary and provides a method to effectively monitor internal assets and maintain data security.

Why is asset management important?

- From physical products to digital company data, asset management is a critical component of any organization.
- For one, asset management is necessary for complete visibility and control over various assets.
- Fully comprehending the who, what, and where's of an asset inventory helps streamline operations and allows multiple users to access data whenever and wherever.
- Not to mention, it's easy to mishandle company assets without proper management, allowing data to fall into the wrong hands or become swept under the rug. Assets that fall into the wrong hands, especially digital ones, can also cause costly customer debacles and security concerns that can significantly impact overall operations — or invite cybercriminals to your virtual front door.

The Key Benefits of Cloud Asset Management

- Cloud asset management provides businesses with the ability to make better decisions, supported by valuable data.
- When you align the long-term integrity of your cloud infrastructure (visibility, accuracy, and reliability) with your cloud management objectives, you build a stronger cloud framework, with minimized risks.
- Here are three of the main benefits of cloud asset management:

1. Cloud Inventory Accuracy

- A key advantage of cloud asset management is the ability to gain greater visibility over your cloud asset inventory. Cloud asset management systems can gather in-depth inventory information that can be used to make educated decisions about managing your assets in the most cost-effective manner possible.
- Not only does this encourage your enterprise to make the most of your existing infrastructure, but it also targets extra or unnecessary spending. By minimizing risk, and steering clear of cloud projects that would prove fruitless, you can avoid wasting valuable finances. Similarly, greater visibility of your inventory can help you target exactly where improvements can be made.
- An accurate cloud asset inventory ensures your enterprise can optimize these measures with confidence, based on reliable data instead of guesswork.

2. Automation

- Cloud asset management uses automated processing to instantly manage the discovery of your assets and provides real-time, up-to-date inventory information. Not only can automation reduce the time-consuming process of trawling through large amounts of data, but it also removes human error from cloud asset management – boosting the accuracy of your cloud management processes.
- Additionally, automation enables your enterprise to become self-serving, placing control of your cloud estate

back in your hands. By using a system that enables your employees to service your cloud infrastructure, you remove the unnecessary interference of your cloud provider. This provides you with greater transparency and visibility over your cloud expenses. For example, it can help you automatically track your cloud costs, and identify extraneous or unnecessary cloud spending that can be changed as required.

3. Security Assurance

- Cloud asset management firms up your cloud security package – enabling you to keep track of your critical security measures with actionable assessments of potential risks and threats to your cloud infrastructure. Automated systems can fix vulnerabilities upon detection, without human intervention – ensuring your business is not left with critical security gaps.
- Additionally, cloud asset management systems identify non-compliant cloud resources and shift them back into compliance immediately. Considering cloud compliance is one of the most vital legal requirements of cloud technology, it's important to have rigorous security and compliance checkpoints in place. Cloud asset management enables this, by automatically processing regulatory reviews of your cloud estate.

Identity & Access management in the cloud

- Identity and Access Management (IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage Google Cloud resources centrally. For enterprises with complex organizational structures, hundreds of workgroups, and many projects, IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes.

Simplicity first

- We recognize that an organization's internal structure and policies can get complex fast. Projects, workgroups, and managing who has authorization to do what all change dynamically. IAM is designed with simplicity in mind: a clean, universal interface lets you manage access control across all Google Cloud resources consistently. So you learn it once, then apply everywhere.

The right roles

- IAM provides tools to manage resource permissions with minimum fuss and high automation. Map job functions within your company to groups and roles. Users get access only to what they need to get the job done, and admins can easily grant default permissions to entire groups of users.

Smart access control

- Permissions management can be a time-consuming task. Recommender helps admins remove unwanted access to Google Cloud resources by using machine learning to make smart access control recommendations. With Recommender, security teams can automatically detect overly permissive access and rightsize them based on similar users in the organization and their access patterns.

Get granular with context-aware access

- IAM enables you to grant access to cloud resources at fine-grained levels, well beyond project-level access. Create more granular access control policies to resources based on attributes like device security status, IP address, resource type, and date/time. These policies help ensure that the appropriate security controls are in place when granting access to cloud resources.

Streamline compliance with a built-in audit trail

- A full audit trail history of permissions authorization, removal, and delegation gets surfaced automatically for your admins. IAM lets you focus on business policies around your resources and makes compliance easy.

Enterprise identity made easy

- Leverage Cloud Identity, Google Cloud's built-in managed identity to easily create or sync user accounts across applications and projects. It's easy to provision and manage users and groups, set up single sign-on, and configure two-factor authentication (2FA) directly from the Google Admin Console. You also get access to the Google Cloud Organization, which enables you to centrally manage projects via Resource Manager.

Workforce Identity Federation

- Workforce Identity Federation lets you use an external identity provider (IdP) to authenticate and authorize a workforce—a group of users, such as employees, partners, and contractors—using IAM, so that the users can access Google Cloud services. Workforce Identity Federation uses an identity federation approach instead of directory synchronization, eliminating the need to maintain separate identities across multiple platforms.

Introduction to IAM

- Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations.
- Systems used for IAM include single sign-on systems, two-factor authentication, multifactor authentication and privileged access management.
- These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared.
- IAM systems can be deployed on premises, provided by a third-party vendor through a cloud-based subscription model or deployed in a hybrid model.
- On a fundamental level, IAM encompasses the following components:
  - how individuals are identified in a system (understand the difference between identity management and authentication);
  - how roles are identified in a system and how they are assigned to individuals;
  - adding, removing and updating individuals and their roles in a system;
  - assigning levels of access to individuals or groups of individuals; and
  - protecting the sensitive data within the system and securing the system itself.

Why is IAM important?

- Businesses leaders and IT departments are under increased regulatory and organizational pressure to protect access to corporate resources. As a result, they can no longer rely on manual and error-prone processes to assign and track user privileges. IAM automates these tasks and enables granular access control and auditing of all corporate assets on premises and in the cloud.
- IAM, which has an ever-increasing list of features
- Including biometrics,
- behaviour analytics and AI is well suited to the rigors of the new security landscape.
- For example, IAM's tight control of resource access in highly distributed and dynamic environments aligns with the industry's transition from firewalls to zero-trust models and with the security requirements of IoT.
- For more information on the future of IoT security, check out this video.
- While IT professionals might think IAM is for larger organizations with bigger budgets, in reality, the technology is accessible for companies of all sizes.

Basic components of IAM

- An IAM framework enables IT to control user access to critical information within their organizations. IAM products offer role-based access control, which lets system administrators regulate access to systems or networks based on the roles of individual users within the enterprise.
- In this context, access is the ability of an individual user to perform a specific task, such as view, create or modify a file. Roles are defined according to job, authority and responsibility within the enterprise.
- IAM systems should do the following: capture and record user login information, manage the enterprise database of user identities, and orchestrate the assignment and removal of access privileges.
- That means systems used for IAM should provide a centralized directory service with oversight and visibility into all aspects of the company user base.
- Digital identities are not just for humans; IAM can manage the digital identities of devices and applications to help establish trust.
- In the cloud, IAM can be handled by authentication as a service or identity as a service (IDaaS). In both cases, a third-party service provider takes on the burden of authenticating and registering users, as well as managing their information. Read more about these cloud-based IAM options.

Benefits of IAM

IAM technologies can be used to initiate, capture, record and manage user identities and their related access permissions in an automated manner. An organization gains the following IAM benefits:

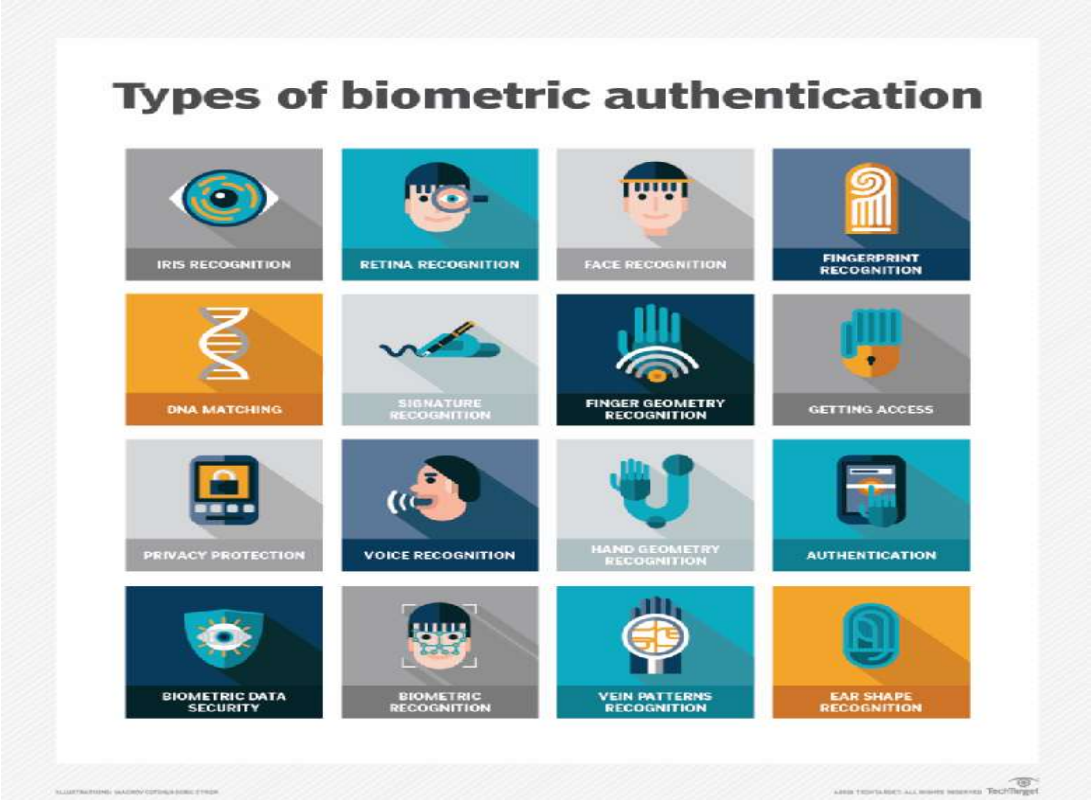
- Access privileges are granted according to policy, and all individuals and services are properly authenticated, authorized and audited.
- Companies that properly manage identities have greater control of user access, which reduces the risk of internal and external data breaches.
- Automating IAM systems allows businesses to operate more efficiently by decreasing the effort, time and money that would be required to manually manage access to their networks.
- In terms of security, the use of an IAM framework can make it easier to enforce policies around user authentication, validation and privileges, and address issues regarding privilege creep.
- IAM systems help companies better comply with government regulations by allowing

Types of digital authentication

- With IAM, enterprises can implement a range of digital authentication methods to prove digital identity and authorize access to corporate resources.
- **Unique passwords.** The most common type of digital authentication is the unique password. To make passwords more secure, some organizations require longer or complex passwords that require a combination of letters, symbols and numbers. Unless users can automatically gather their collection of passwords behind a single sign-on entry point, they typically find remembering unique passwords onerous.
- **Pre-shared key (PSK).** PSK is another type of digital authentication where the password is shared among users authorized to access the same resources -- think of a branch office Wi-Fi password. This type of authentication is less secure than individual passwords.
- A concern with shared passwords like PSK is that frequently changing them can be cumbersome.
- **Behavioral authentication.** When dealing with highly sensitive information and systems, organizations can use behavioral authentication to get far more granular and analyze keystroke dynamics or mouse-use characteristics. By applying artificial intelligence, a trend in IAM systems, organizations can quickly recognize if user or machine behavior falls outside of the norm and can automatically lock down systems.
- **Biometrics.** Modern IAM systems use biometrics for more precise authentication. For instance, they collect a

range of biometric characteristics, including fingerprints, irises, faces, palms, gaits, voices and, in some cases, DNA. Biometrics and behavior-based analytics have been found to be more effective than passwords.

- When collecting and using biometric characteristics, companies must consider the ethics in the following areas:
  - data security (accessing, using and storing biometric data);
  - transparency (implementing easy-to-understand disclosures);
  - optionality (providing customers a choice to opt in or out); and
  - biometric data privacy (understanding what constitutes private data and having rules around sharing with partners.
- One danger in relying heavily on biometrics is if a company's biometric data is hacked, then recovery is difficult, as users can't swap out facial recognition or fingerprints like they can passwords or other non-biometric information.
- Another critical technical challenge of biometrics is that it can be expensive to implement at scale, with software, hardware and training costs to consider.



Implementing IAM in the enterprise

- Before any IAM system is rolled out into the enterprise, businesses need to identify who within the organization will play a lead role in developing, enacting and enforcing identity and access policies. IAM impacts every department and every type of user (employee, contractor, partner, supplier, customer, etc.), so it's essential the IAM team comprises a mix of corporate functions.
- IT professionals implementing an IAM system largely on-premises and largely for employees should become familiar with the OSA IAM design pattern for identity management, SP-010. The pattern lays out the architecture of how various roles interact with IAM components as well as the systems that rely on IAM. Policy enforcement and policy decisions are separated from one another, as they are dealt with by different elements within the IAM framework.

1. Make a list of usage, including applications, services, components and other elements users will interact with. This list will help validate that usage assumptions are correct and will be instrumental in selecting the features needed from an IAM product or service.
2. Understand how the organization's environments, such as cloud-based applications and on-premises applications, link together. These systems might need a specific type of federation (Security Assertion Markup Language OpenID Connect, for instance).
3. Know the specific areas of IAM most important to the business. Answering the following questions will help:
    a. Is multifactor authentication needed?
    b. Do customers and employees need to be supported in the same system?
    c. Are automated provisioning and deprovisioning required?
    d. What standards need to be supported?

Implementations should be carried out with IAM best practices in mind, including documenting expectations and responsibilities for IAM success. Businesses also should make sure to centralize security and critical systems around identity. Perhaps most important, organizations should create a process they can use to evaluate the efficacy of current IAM controls.

Introduction to Federal Identity Management

- The term "identity management" is relatively new, the concept is not. In fact, the underlying processes have been in use for many generations in an offline environment. Passports, driver's licenses, and employee ID cards are all components of what might be referred to as identity management systems – i.e., they are credentials issued by an entity for the purpose of identifying individuals, and they are used by such individuals to validate their identity in order to enter into a transaction with a third party.
- While there are many different approaches to identity management, it essentially involves two fundamental processes:
- the process of identifying a person and issuing an identity credential to reflect that identity ("identification"), and
- the process of later verifying that a particular person presenting that credential and claiming to be that previously identified person is, in fact, such person ("authentication").
- Once an individual's identity is successfully authenticated, a third process, referred to as "authorization," is used by the business relying on the authenticated identity to determine what rights and privileges are accorded to such person – e.g., whether such person should be granted access to a website, a database, a bar, an airport boarding area, etc.
- A simple and familiar example of these processes can be seen in the case of an employee who logs into his or her employer's network using a user ID and password.
- Before a company allows a person to access its internal network, that person must be properly identified in a manner appropriate for the transaction (e.g., as an employee with certain authority), and then that identity must be authenticated at the time of each transaction. Employees are identified by their employer, and issued an identity credential consisting of a unique identifier (typically a User ID) which is linked to other relevant information attributes stored on the company's computer system. A secret (in this case, a password), is then used to link the employee to the identity credential. Thereafter, when the employee wants to remotely access the company's network, he or she can be authenticated by using the password in an authentication protocol. The authentication protocol allows the employee to demonstrate to the employer that he or she has or knows the secret, and thus, is the person previously identified
- A key characteristic of some existing offline identity documents (such as a passport or driver's license) is that

their use is not limited to transactions with the entities that issued them. Rather, they are often accepted by third parties (such as airport security, a bank, or a bartender) when proof of certain aspects of one's identity is required. This characteristic is critical for the identity credentials needed for e-commerce. Such an approach, whereby a business or government agency relies on an identification process performed, and identity information provided, by one of several possible unrelated third parties is sometimes referred to as a federated identity model. Under such a model, a single identity credential can be used with numerous organizations that had no involvement with the original issuance of the credential. The challenge is to import a similar approach to the digital online environment. That is, to create secure, reliable and trustworthy digital identity credentials that can be used across different ecosystems and entities. This allows individuals to use the same identity credential to sign on to the networks of more than one business in order to conduct transactions.

IAM Best Practices

Identity and Access Management (IAM) has become an essential element of security plans for many organizations. To reap the most security benefits, it is imperative that companies ensure that their IAM tools and processes are set up correctly. In this article, we will share 11 identity and access management best practices your company should adopt to establish a strong security posture. By the end of this article, you'll know the next steps to take to incorporate **IAM best practices** into your security strategy.

1. Adopt a Zero Trust Approach to Security

Many companies have applications, platforms, and tools that are designed with implicit trust features. Implicit trust means that if users have access to your network or log in to a tool, the system "remembers" them and doesn't always prompt the user to verify their identity again. These lax access permissions can pose a major risk to your organization's security stance if an unauthorized entity gains access to your system via a remembered credential.

2. Identify and Protect High-Value Data

Protecting your most valuable data involves limiting who can access it as much as possible—but, to limit access, you first need to know where your most valuable data is stored and how it is used.

3. Enforce a Strong Password Policy

Your IAM technologies are only as strong as the identity management best practices and policies that support them. If your team is leveraging single sign-on (SSO) tools, it's critical that each user's password is strong, unique, and difficult to guess to support password and IAM best practices. Passwords must be complex enough to deter cyberattacks, frequently changed, and not used for multiple sign-on requirements.

4. Use Multi-Factor Authentication (MFA)

User authentication is an essential component of effective identity and access management best practices. After all, if you can't guarantee a user is who they claim to be, you may be putting your data at risk and unintentionally allowing access to an unauthorized user.

MFA tools often use a combination of these methods to authenticate identity:

- Biometric authentication (e.g., fingerprints or facial recognition)
- Possession authentication (e.g., sending a one-time password to a user's personal device)
- Knowledge authentication (e.g., answering security questions)
- User location or time data

5. Automate Workflows

IAM tools offer IT teams many opportunities to use automation to make your organization more secure. Automation reduces manual errors, streamlines workflows, and supports compliance and governance needs.

6. Adopt The Principle of Least Privilege

One of the most common roles and permissions best practices is applying the principle of least privilege. IAM least privilege encourages organizations to restrict access and permissions as much as possible, without interfering with

users' daily workflows.

7. Enforce Just-in-Time Access Where Appropriate

In some circumstances, the principle of least privilege doesn't provide the necessary flexibility that certain situations require. For instance, a help desk associate may need temporary elevation of privileges to troubleshoot a customer's urgent ticket. One way to enforce identity and access management best practices, yet still support the principle of least privilege without compromising user experience, is by leveraging just-in-time access.

8. Leverage Both Role-Based Access Control and Attribute-Based Access Control Policies

Using role-based access control (RBAC) and attribute-based access control (ABAC) together can facilitate robust user access management best practices.

9. Regularly Audit Access to Resources

Even with strong policies around access control, over-provisioning remains a problem for many organizations. Auditing is one of the fundamental IAM best practices to build into your overall IAM strategy to maintain the principle of least privilege.

10. Centralize Log Collection

Many IAM tools automatically generate logs, and these logs are valuable tools to help your team meet compliance requirements, audit usage, and strengthen IAM policies. However, not all teams think to centralize where they store their logs.

11. Adopt IAM Solutions That Work With Existing Tools Using the right tools can make applying identity and access management industry best practices much easier for your organization. There's no need to force a round peg into a square hole; instead of making IAM solutions fit your existing tech stack, search for the right solutions that already support your existing tools and applications.

IAM ADUIT LOGS

1) Create an IAM Policy

Make sure the IAM process is clearly defined and a crucial part of your organizational security policy. Creating an IAM policy document is strongly recommended for the following reasons:

- Meet compliance requirements
- Manage user access and authorization
- Define access to stakeholders who can help make a robust IAM policy
- Robust incident response

Moreover, it's more important to review the policy document at regular intervals to ensure that the right practices are updated and followed on time.

2) Develop and Streamline Procedure

It's not done with creating a policy, and you see desired results only if implemented properly. For that, you need to develop a procedure involving all stakeholders in the IAM process and define roles.

The streamlined procedure should have the list of stakeholders with assigned responsibilities and actions they are accountable for.

3) Access Review

In any organization, users, roles, and responsibilities keep changing. In such a scenario, it's important to review access and authorizations given to different users. To ensure the right access is given, formulate a user access review process.

Keep reviewing that at different intervals to avoid discrepancies. Policy-Based Access Control (PBAC) is one means to execute the user access review process.

4) Appropriate Privileges

This is the crucial point that defines the robustness of an IAM system. Despite being known, this is often ignored. It's very important to see the user access remains limited to 'particular' job requirements and not further. It's recommended to follow the Least Privileged Account principle, which calls for setting maximum limitations possible to the resources.

If special privileges have to be given, make sure to revoke them immediately after the temporary period set for its usage ends.

5) Segregating Responsibilities

This is one crucial aspect that can avoid possible risks in the very first step. Segregating duties among people keeps them limited to their respective functions, and none gets complete access. In case of critical tasks, break them into smaller ones and assign them to multiple people. This keeps every process and its associated security functions independent from others.

In case one of any breach to a process, the threat scope remains limited to that particular process, leaving the rest of the system.

6) Generic Accounts

Generic accounts are required in every organization to execute regular and common activities like training and testing. But keeping them idle can lead to security risks. Never assign admin rights to generic accounts and make sure to delete the unused ones.

It's important to see they are bound by strong passwords to avoid breaches through default settings. Privileged Access Management (PAM) and PBAC can offer full control over generic accounts.

7) Delete/Disable Idle Accounts

It's important to keep your IAM system clean, secure and updated. Delete any unused user account (generic or important ones) lying idle. Leaving them is like allowing them to grow further and welcome threats through them.

Delete inactive users lying individually and in groups. Make sure users are only present in their relevant groups. Conduct a regular review of group policies and delete exposed login details.

8) Document Everything

Back to where we started. We started with documenting policy for its effective implementation. But it's important to document everything in implementation too. This forms as a trial for future implementations and helps comply with rules every time.

Documentation is key to the IAM audit process, where you need to share administration activities, policies, and usage documented. Moreover, the documentation process gives a better understanding of the entire IAM system, helping you find ways to improve it further.

Intro to AWS/Azure clint and Web Portal

What is AWS client?

- AWS Client VPN is **a fully-managed remote access VPN solution used by your remote workforce to securely access resources within both AWS and your on-premises network**. Fully elastic, it automatically scales up, or down, based on demand.

- When migrating applications to AWS, your users access them the same way before, during, and after the move. AWS Client VPN, including the software client, supports the OpenVPN protocol.

Benefits

Advanced authentication

- Many organizations require multi-factor authentication (MFA) and federated authentication from their VPN solution. AWS Client VPN supports these and other authentication methods.

Elastic

- Traditional on-premises VPN services are limited by the capacity of the hardware that runs them. AWS Client VPN is a pay-as-you-go cloud VPN service that elastically scales up or down based on user demand.

Remote access

- Unlike on-premises VPN services, AWS Client VPN allows users to connect to AWS and on-premises networks using a single VPN connection

Fully managed

- AWS Client VPN automatically takes care of deployment, capacity provisioning, and service updates — while you monitor all connections from a single console.

AWS Client VPN use cases

Quickly scale remote access

- Unexpected events can require many of your employees to work remotely. This creates a spike in VPN connections and traffic that can reduce performance or availability for your users. AWS Client VPN is elastic, and automatically scales up to handle peak demand. When the spike has passed, it scales down so you are not paying for unused capacity.

Access applications during migration

- AWS Client VPN provides users with secure access to applications both on premises and in AWS. This is helpful during a cloud migration when applications move from on-premises locations to the cloud. With AWS Client VPN, users don't have to change the way they access their applications during or after migration.

Integrate with your authentication and MDM systems

- AWS Client VPN supports authentication with Microsoft Active Directory using AWS Directory Services, Certificate-based authentication, and Federated Authentication using SAML-2.0 to facilitate these scenarios when using the AWS provided OpenVPN Client software. AWS Client VPN works with Mobile Device Management (MDM) solutions to reject devices that do not comply with the your policies.

Securely connecting IoT devices

Create encrypted connections between IoT devices and Amazon Virtual Private Cloud (VPC) resources using certificate-based authentication.

In this tutorial you will create a Client VPN endpoint that does the following:

- Provides all clients with access to a single VPC.
- Provides all clients with access to the internet.
- Uses mutual authentication.

The following diagram represents the configuration of your VPC and Client VPN endpoint after you've completed this tutorial.

Steps

- Prerequisites
- Step 1: Generate server and client certificates and keys
- Step 2: Create a Client VPN endpoint
- Step 3: Associate a target network
- Step 4: Add an authorization rule for the VPC
- Step 5: Provide access to the internet
- Step 6: Verify security group requirements
- Step 7: Download the Client VPN endpoint configuration file
- Step 8: Connect to the Client VPN endpoint

What is Azure?

Azure Cloud is an ever-expanding set of services that help your organization meet your current and future business challenges. Azure gives you the freedom to build, manage and deploy applications across a vast global network using the tools and frameworks of your choice.

What does Azure provide?

With Azure, you have everything you need to build your next great solution. The following table lists the many benefits that Azure provides for ease of invoicing with Objective.

Be ready for the future: Microsoft's constant innovation supports your growth today and your product vision for tomorrow.

Build on Your Terms: You have options. With a commitment to open-source and support for all languages and frameworks, you can build as you wish and deploy wherever you want.

Operate the hybrid seamlessly: on-premises, in the cloud, and on edge--we'll meet you where you are. Integrate and manage your environment with tools and services designed for hybrid cloud solutions.

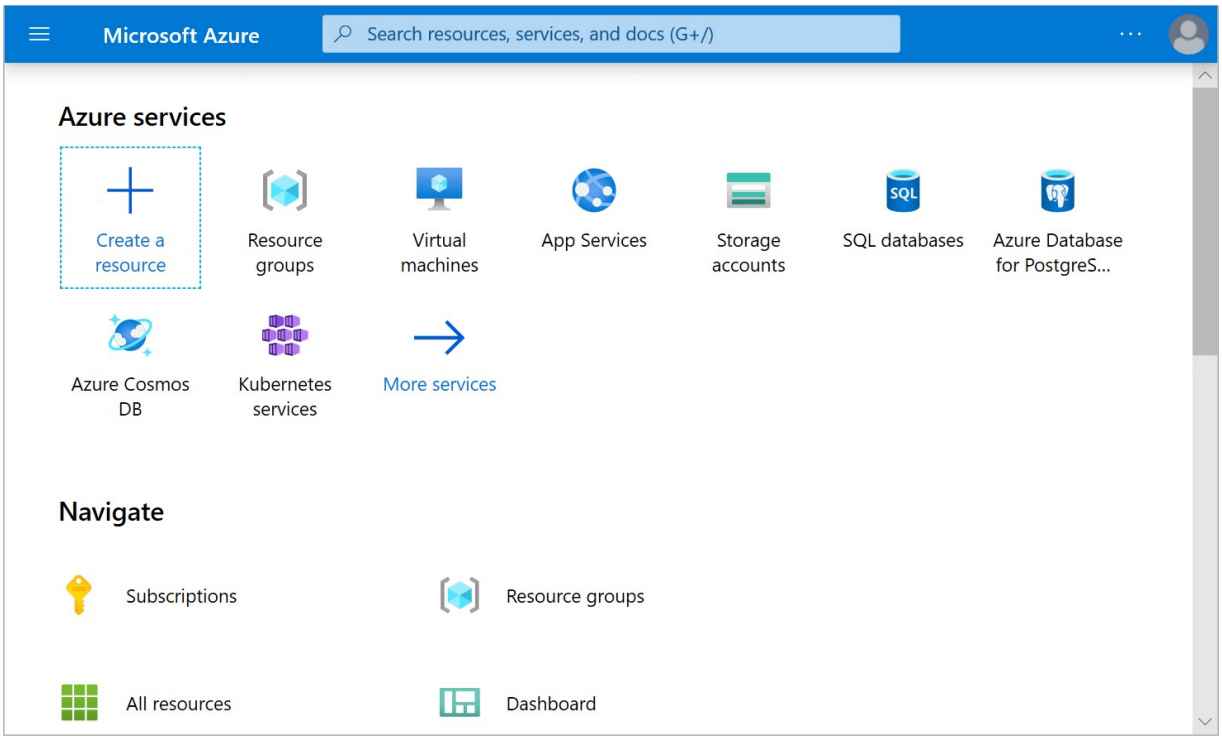
Trust your cloud: Get security from the ground up, backed by a team of experts, and proactive compliance trusted by enterprises, governments, and startups.

What is Azure Portal?

Azure Portal is a web-based, integrated console that provides an alternative to command-line tools. With the Azure Portal, you can manage your Azure subscription using the graphical user interface. You can do this:

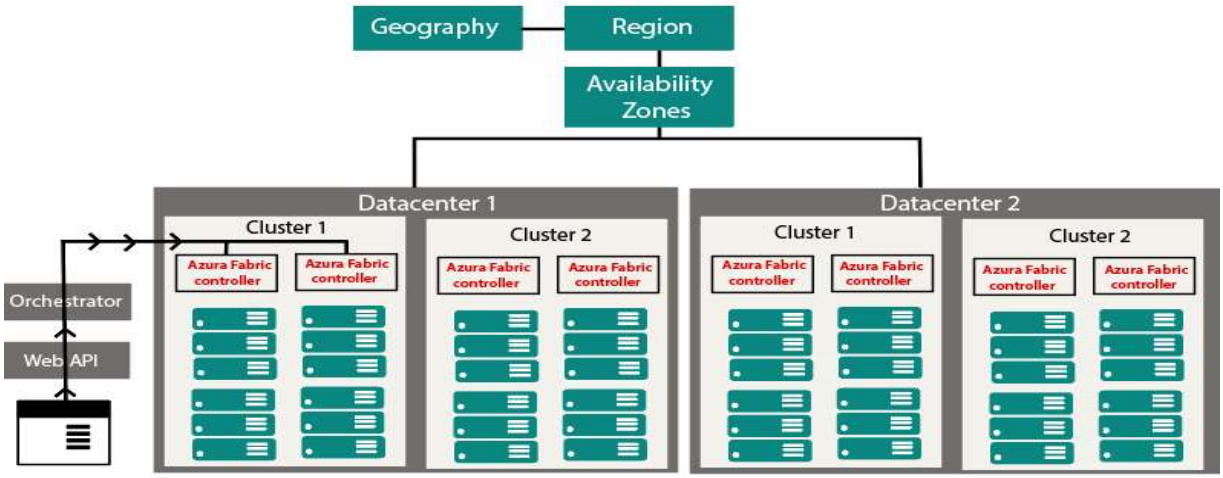
- Build, manage and monitor everything from simple web apps to complex cloud deployments.
- Create custom dashboards for an organized view of resources.
- Configure accessibility options for the optimum experience.

The Azure Portal is designed for flexibility and constant availability. It maintains a presence in each Azure datacenter. This configuration makes the Azure portal resilient to isolated datacenter failures and prevents network slowdowns by being closer to users. The Azure Portal is constantly updated, and maintenance activities do not require any downtime.



How Azure works

It is essential to understand the internal workings of Azure so that we can design our applications on Azure effectively with high availability, data residency, resilience, etc.



Microsoft Azure is completely based on the concept of virtualization. So, similar to other virtualized data center, it also contains *racks*. Each rack has a separate power unit and network switch, and also each rack is integrated with a software called *Fabric-Controller*. This *Fabric-controller* is a distributed application, which is responsible for managing and monitoring servers within the rack. In case of any server failure, the Fabric-controller recognizes it and recovers it. And Each of these Fabric-Controller is, in turn, connected to a piece of software called *Orchestrator*. This *Orchestrator* includes web-services, Rest API to create, update, and delete resources.

When a request is made by the user either using PowerShell or Azure portal. First, it will go to the Orchestrator, where it will fundamentally do three things:

1. Authenticate the User
2. It will Authorize the user, i.e., it will check whether the user is allowed to do the requested task.
3. It will look into the database for the availability of space based on the resources and pass the request to an appropriate Azure Fabric controller to execute the request.

Combinations of racks form a cluster. We have multiple clusters within a data center, and we can have multiple Data Centers within an Availability zone, multiple Availability zones within a Region, and multiple Regions within a Geography.

- **Geographies:** It is a discrete market, typically contains two or more regions, that preserves data residency and compliance boundaries.
- **Azure regions:** A region is a collection of data centers deployed within a defined perimeter and interconnected through a dedicated regional low-latency network.
- **Availability Zones:** These are the physically separated location within an Azure region. Each one of them is made up of one or more data centers, independent configuration.

Azure covers more global regions than any other cloud provider, which offers the scalability needed to bring applications and users closer around the world. It is globally available in 50 regions around the world. Due to its availability over many regions, it helps in preserving data residency and offers comprehensive compliance and flexible options to the customers.

Vulnerability management:

- It is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimizing their "attack surface."

Vulnerability management process:

Every new vulnerability introduces risk to the organization. So, a defined process is often used to provide organizations with a way to identify and address vulnerabilities quickly and continually. At a high level, 6 processes make up vulnerability management—each with their own subprocesses and tasks.

- Discover: You can't secure what you're unaware of. The first process involves taking an inventory of all assets across the environment, identifying details including operating system, services, applications, and configurations to identify vulnerabilities. This usually includes both a network scan and an authenticated agent-based system scan. Discovery should be performed regularly on an automated schedule.
- Prioritize: Second, discovered assets need to be categorized into groups and assigned a risk-based prioritization based on criticality to the organization.
- Assess: Third is establishing a risk baseline for your point of reference as vulnerabilities are remediated and risk is eliminated. Assessments provide an ongoing baseline over time.
- Remediate: Fourth, based on risk prioritization, vulnerabilities should be fixed (whether via patching or reconfiguration). Controls should be in place so that that remediation is completed successfully and progress can be documented.
- Verify: Fifth, validation of remediation is accomplished through additional scans and/or IT reporting.
- Report: Finally, IT, executives, and the C-suite all have need to understand the current state of risk around vulnerabilities. IT needs tactical reporting on vulnerabilities identified and remediated (by comparing the most recent scan with the previous one), executives need a summary of the current state of vulnerability (think red/yellow/green type reporting), and the C-suite needs something high-level like simple risk scores across parts of the business.

Discovering cloud misconfigurations:

- Companies are increasingly moving their IT operations to IaaS (infrastructure-as-a-service) solutions. Gartner estimates that by 2022, about 60% of business entities will be leveraging cloud-managed offerings, doubling the recorded use in 2018.
- Cloud offerings like Amazon Web Services (AWS) are generally secure. But since IaaS uses a shared security model, there's a great chance of data security issues, including cybersecurity and workload concerns. Misconfigurations when migrating to cloud-native environments can inadvertently lead to cybersecurity loopholes.
- Misconfiguration isn't just a theoretical cloud computing concern. McAfee's enterprise security research shows that the typical enterprise experiences approximately 3,500 incidents monthly. From the study, 90% of businesses reported that they'd experienced IaaS security issues.
- Therefore, getting it right with cloud migration configuration can significantly reduce future IaaS security issues and boost your digital transformation.

Cloud Misconfiguration – A Major Security Threat

- Cloud misconfiguration refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption. These cyber threats come in the form of security breaches, external hackers, ransomware, malware, or insider threats that use vulnerabilities to access your network.

- The NSA considers cloud misconfiguration a leading vulnerability in a cloud environment. While these risks are often less sophisticated, the issues' prevalence is generally through the roof.
- Misconfiguration is a cloud computing problem because multi-cloud environments can be quite complicated, and it can be tough to detect and manually remediate mistakes. According to a Gartner survey, these issues cause 80% of all data security breaches, and until 2025, up to 99% of cloud environment failures will be attributed to human errors.
- This is tricky, considering there's no one-time remedy for cloud misconfiguration issues like cloud leaks. However, it would help to implement security procedures at the build stage. So, DevOps and security teams must work collaboratively.

Common Cloud Misconfigurations and Their Solutions

- Let's take a deep dive into the most common cloud misconfigurations that you'll likely have to deal with when migrating to a cloud environment.

1. Unrestricted Inbound Ports

- All ports open to the internet can be potentially problematic. Cloud services mostly use high-number UDP or TCP ports to prevent exposure risks, but determined hackers can still sniff them out. Obfuscation can be helpful, but it's insufficient by itself.
- When migrating to a multi-cloud environment, make sure you know the full range of open ports and then restrict or lock down those that aren't strictly necessary.

2. Unrestricted Outbound Ports

- These ports create opportunities for security events like data exfiltration, lateral movement, and internal network scans once there's a system compromise. Granting outbound access to RDP or SSH is a common cloud misconfiguration. Application servers seldom have to SSH to other network servers, so it's unnecessary to use open outbound ports for SSH.
- Make sure you limit the outbound port access and use the least privilege principle to restrict outbound communications.

3. "Secrets" Management

- This configuration issue can be damaging to your organization. Securing secrets like API keys, passwords, encryption keys, and admin credentials is essential. But most companies openly avail these through compromised servers, poorly configured cloud buckets, HTML code, and GitHub repositories. This is as risky as leaving your home’s deadbolt key taped to your front door.
- You can beat this by maintaining an inventory of all your company secrets in the cloud and regularly evaluating how they're secured. Otherwise, threat actors could easily breach your systems, access your data, and overrun your cloud resources to effect irreversible damage.
- You may also use secret management solutions and services like Hashicorp Vault, AWS Secrets Manager, Azure Key Vault, and AWS Parameter Store.

4. Disabled Monitoring and Logging

- Surprisingly, most organizations fail to configure, enable, or review the telemetry data and logs offered by public clouds, which can be sophisticated. It would help to have someone responsible for regular reviews and flagging security-related incidents.
- This valuable tip isn't only limited to IaaS public clouds. You'll also get the same information from storage-as-a-service vendors, which you must also review regularly. A maintenance alert or update bulletin could leave your organization with profound security implications, but it won't help if there's no one paying attention.

5. ICMP Left Open

- The ICMP (Internet Control Message Protocol) reports network device errors, but it's a common target for threat actors. This happens because while the protocol can display if your server is responsive and online, cybercriminals can also use it to pinpoint an attack.
- Furthermore, it's also an attack vector for denial-of-service (DDoS) and many types of malware. A ping flood or ping sweep can overwhelm your servers with ICMP messages. While it's a dated attack strategy, it's still effective. So make sure your cloud configuration blocks ICMP.

6. Insecure Automated Backups

- Insider threats to your cloud environment are an ever-present cybersecurity risk. According to McAfee, about 92% of business organizations have workers' credentials being sold on the darknet. One section where insider threats can be particularly damaging is when you fail to secure automated cloud data backup properly.
- You may have protected your master data, but poorly configured backups will inadvertently remain vulnerable and exposed to insider threats.
- When migrating to the cloud, ensure your backups are encrypted whether at rest or in transit. Also, verify the permissions to restrict access to the backups.

7. Storage Access

- Most cloud users believe that "authenticated users" only cover those already authenticated within the relevant apps or organizations regarding storage buckets. Unfortunately, this isn't the case.
- "Authenticated users" refers to any person with AWS authentication, essentially any AWS client. Due to this misunderstanding, alongside the resulting control settings misconfiguration, you may have your storage objects wholly exposed to public access. Be especially cautious when setting storage object access to grant it to only the people within your organization.

8. Lack of Validation

- This cloud configuration error is a meta-issue: most organizations don't create and implement systems for identifying misconfigurations whenever they occur. Whether an outside auditor or internal resource, you need someone to verify that permissions and services are correctly configured and deployed.
- Create a schedule that ensures validation occurs like clockwork because mistakes are inevitable as the cloud environment evolves. You also need a rigorous process of auditing cloud configurations periodically. Otherwise, you may leave a security loophole that cybercriminals can exploit.

9. Unlimited Access to Non-HTTPS/HTTP Ports

- Web servers are made to host web services and websites to the internet, alongside other services like RDP or SSH for databases or management. However, you must block these from accessing every part of the internet.
- Improperly configured ports can open your cloud infrastructure up to malicious actors looking to brute force or exploit the authentication. When opening these ports to the web, ensure you limit them to accept traffic from specific addresses, such as your office.

10. Overly Permissive Access to Virtual Machines, Containers, and Hosts

- Would you connect a virtual or physical server in your data center directly to the internet without protecting it using a firewall or filter? You likely wouldn't, but people do exactly this in their cloud infrastructures all the time.
- Some of the most common examples include:
  - Enabling legacy protocols and ports like FTP on cloud hosts

- Legacy protocols and ports like rexec, rsh, and telnet in physical serves that have been made virtual and moved to the cloud
- Exposing etcd (port 2379) for Kubernetes clusters to the public internet

- You can avoid this cloud configuration mistake by securing important ports and disabling (or at the very least locking down) legacy, insecure protocols in your cloud environment the same way you would treat your on-premise data center.

11. Enabling Too Many Cloud Access Permissions

- A major benefit of cloud computing is its ease of scalability. However, this simplicity of expansion is not without its downsides. As cloud environments grow larger and more complex, administrators rapidly lose oversight of system controls.
- Lack of visibility makes it harder for admins to review permissions and restrict access. They may also find it easier to enable default permission settings for all users to avoid dealing with an influx of access requests.
- Unnecessary permissions greatly increase the risk of insider threats, which could result in cloud leaks and data breaches.
- Organizations should seek to adopt the emerging Secure Access Service Edge (SASE) architecture, which enables more efficient cloud security, including the use of Cloud Access Service Brokers (CASBs) and Cloud Security Posture Management (CSPM) solutions to manage user permissions in multi-cloud environments.

12. Subdomain Hijacking (AKA Dangling DNS)

- A common cause of this type of cyberattack is when an organization deletes a subdomain from its virtual host (e.g. AWS, Azure, Github, etc.) but forgets to delete the its associated records from the Domain Name System (DNS).
- Once the attacker discovers the unused subdomain, they can re-register it via the hosting platform and route users to their own malicious web pages.
- Such hijacking could result in malware injections or phishing attacks to unsuspecting users and can cause severe reputational damage to the original subdomain owner.
- To avoid subdomain hijacking, organizations should always remember to delete DNS records for all domains and subdomains that are no longer in use.
- 13. Misconfigurations Specific to Your Cloud Provider(s)
- While misconfigurations like open ports and overly permissive access are applicable to all cloud providers, many misconfigurations exist that are more specific to the service(s) you're using. For example, default public access settings for S3 buckets is a well-known AWS flaw.
- Organizations should research cloud misconfigurations specific to their cloud service provider(s).

Remediating vulnerabilities:

- It is always important to remember that the end-game of vulnerability management is remediation. One of the important KPIs of a vulnerability management program is how many high-risk vulnerabilities are removed or neutralized before critical systems and assets are compromised.

Why is Vulnerability Remediation Important?

- Customers, partners, employees and regulators expect companies to put in place policies and processes that continuously and effectively protect data from accidental or malicious loss and exposure. There is also zero tolerance for system disruptions or slowdowns. In short, meeting vulnerability

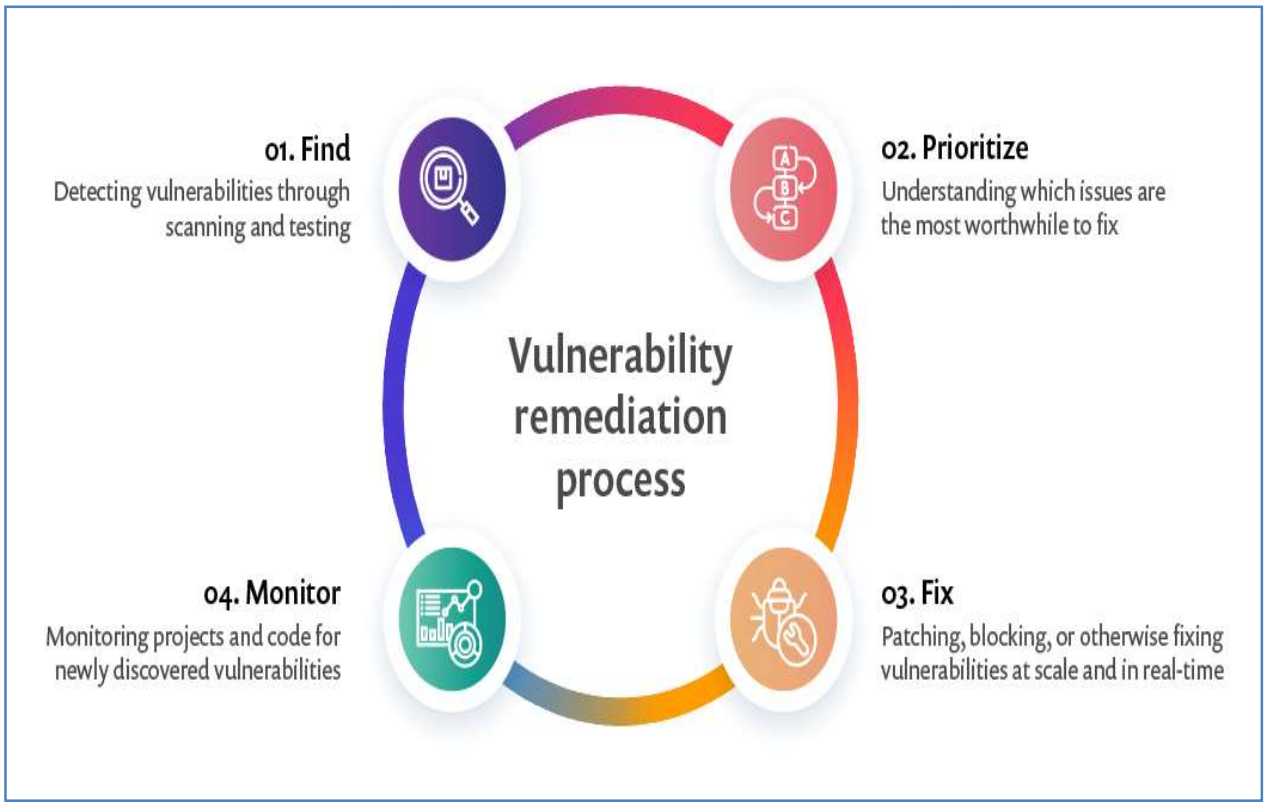
remediation challenges has become a business-critical activity.

What is the Vulnerability Remediation Process?

- The vulnerability remediation process is a workflow that fixes or neutralizes detected weaknesses. It includes 4 steps: finding vulnerabilities through scanning and testing, prioritising, fixing and monitoring vulnerabilities.

4 steps of vulnerability remediation process

1. **Find:** Detecting vulnerabilities through scanning and testing
2. **Prioritize:** Understanding which vulnerabilities pose a real and significant risk
3. **Fix:** Patching, blocking, or otherwise fixing vulnerabilities at scale and in real-time
4. **Monitor:** Automatically monitor projects and code for newly discovered vulnerabilities, with real-time alerts and notifications via all the relevant channels



1. Finding Vulnerabilities

- Security vulnerabilities are known coding flaws or system misconfigurations that can be exploited to compromise an application, service, library, container, or function and all its related assets. The active exploit seeks to shut down or disrupt performance, exfiltrate data, hijack compute resources, and so on. Systems and assets that are laterally accessible to the compromised component are also at risk.
- The first step of the vulnerability remediation process, therefore, is to scan for and find security vulnerabilities. Mature vulnerability management programs implement a shift-left DevSecOps approach in which vulnerability scanning takes place throughout a secure SDLC (software development life cycle). In order not to slow down the CI/CD pipeline, automated vulnerability testing tools are deployed in development, testing, and production environments. These may include:
  - **Software Composition Analysis** (SCA) tools
  - **Open source vulnerability scanners**
  - White-box static application security (**SAST**) tools

- Black-box dynamic application security tools (**DAST**)

- Special attention needs to be paid to **container security**. It is important to scan for security vulnerabilities in container images as well as in running container instances, with all their linkages. It is also important to ensure that third-party container images are from trusted sources only. **Kubernetes security** also raises a unique set of vulnerability scanning challenges. If a cluster is breached, every service and machine in the network is at risk.

2. Prioritizing Vulnerabilities

- The next step in the vulnerability remediation process is prioritizing vulnerability remediation.
- No matter which approach your company takes to security risk management, not every detected vulnerability poses the same level of risk. It is always a tradeoff among a variety of considerations such as severity, fixability, coverage, and compliance. With risk-based, context-aware prioritization, the vulnerability remediation team can focus its limited resources on the issues that matter the most.
- Good likelihood that 80% plus of discovered vulnerabilities are false-positives, another 18% are low-risk and then the last 2% are really things that you need to fix.

3. Fixing Vulnerabilities

- The third step in the vulnerability remediation process is to fix the weakness.
- In many cases, removing vulnerable software involves deploying an upgrade or a patch, as recommended by the vendor of the affected software. However, patch deployment can be challenging in and of itself. Testing and rolling out patches and upgrades can consume considerable time and resources. Business-critical systems may have to be shut down during the deployment process. And there is always the risk that the patch will have unforeseen impact on the application itself or its dependencies.
- There may be less risky ways to fix a weakness, or to at least buy time while a patch is being prepared for deployments. For example, you can update risky system, platform, or service configurations. Similarly, you can disable a vulnerable process or function, or remove a vulnerable component, that is not actually in use.

4. Monitoring Vulnerabilities

- Just like the rest of the SDLC, the security vulnerability remediation process is continuous. To facilitate this loop, you need to have monitoring in place. The tool(s) you use to do this need to automatically monitor projects and code for newly discovered vulnerabilities, with real-time alerts and notifications via all the relevant channels.
- Ideally, the monitoring tool will also provide contextualized prioritization, helping with both steps 1 and 2 of the vulnerability remediation process (**find** and **prioritize**). Otherwise, developers or AppSec teams receiving notifications will quickly become burned out by an influx of low-priority vulnerabilities. It's important that teams are not overwhelmed by noise, which can delay them from handling important, high-priority vulnerabilities that need prompt remediation.

Tracking open vulnerabilities using cloud native tools:

- All three of the major cloud providers offer a vulnerability scanning solution as part of their cloud services. Let's see what is provided by these first-party solutions.

AWS Vulnerability Scanning

- Amazon Inspector is a vulnerability management service that continuously scans AWS workloads for vulnerabilities. It automatically detects and scans Amazon EC2 instances and container images in Amazon Elastic Container Registry (Amazon ECR), identifying software vulnerabilities and accidental network exposure.
- Amazon Inspector creates a "finding" when it identifies software vulnerabilities or network issues. These

findings describe the vulnerability, identify affected resources, assess the severity of the vulnerability, and provide remediation guidance. You can use the Amazon Inspector console to review findings in your Amazon account, or view findings within other AWS services.

Azure Vulnerability Scanning

- Microsoft provides Defender Vulnerability Management, a solution that provides asset visibility, assessment, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and networked devices. It can be used to secure resources in the Azure cloud and elsewhere.
- By leveraging Microsoft's extensive threat intelligence database, Defender Vulnerability Management automatically assesses the business and device environment and performs breach forecasting. It can quickly and consistently prioritize and assign risk scores to vulnerabilities in a company's most valuable assets, including both software vulnerabilities and misconfigurations, and provides actionable remediation advice to mitigate the impact.

Google Cloud Platform (GCP) Vulnerability Scanning

Google provides the Security Command Center, which offers three key vulnerability scanning features:

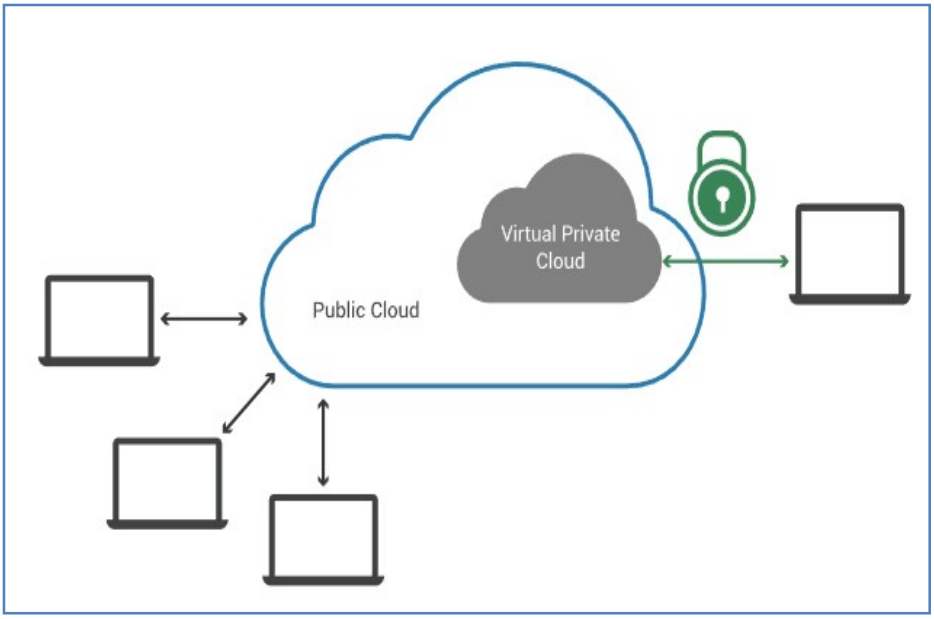
- Continuously monitors container images to identify suspicious changes and remote access attempts. The service can detect common container runtime attacks.
- Monitors cloud logs for your organization's Google services and detects threats using detection logic and threat intelligence feeds from Google.
- Scans web applications running on Google App Engine, Google Compute Engine, or Google Kubernetes Engine (GKE). The service can scrape application URLs, execute user input, and test for vulnerabilities such as legacy libraries, mixed content, and cross-site scripting (XSS).

Network security and Security groups:

- Cloud-based infrastructure requires a similar level of security as an organization's on-prem environment. Cloud network security is a foundational layer of cloud security and is vital to protecting the data, applications, and IT resources deployed within enterprise cloud environments as well as the traffic flowing between cloud deployments and the enterprise's intranet and on-prem data centers.
- On-prem enterprise networks use network security solutions for advanced threat prevention, to restrict access to corporate systems, enforce security policies, and perform internal segmentation of corporate networks. Cloud network security provides similar enterprise-grade protection to cloud infrastructure and networks.
- Network Security Groups(NSGs)
- Network security groups (NSGs) determine the inbound and outbound traffic to and from your CDP environment. That is, you should use security group settings to allow users from your organization access to CDP(Cloudera Data Platform) resources.
- You have two options:
  - Use your existing security groups (recommended for production)
  - Have CDP create new security groups
- You should verify the security group limits in your Azure account to ensure that you can create security groups for CDP.

Virtual Private Clouds (VPC):

- A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud. VPC customers can run code, store data, host websites, and do anything else they could do in an ordinary private cloud, but the private cloud is hosted remotely by a public cloud provider.
- VPCs combine the scalability and convenience of public cloud computing with the data isolation of private cloud computing.
- Imagine a public cloud as a crowded restaurant, and a virtual private cloud as a reserved table in that crowded restaurant. Even though the restaurant is full of people, a table with a "Reserved" sign on it can only be accessed by the party who made the reservation. Similarly, a public cloud is crowded with various cloud customers accessing computing resources – but a VPC reserves some of those resources for use by only one customer.



How a virtual private cloud works

- In a virtual private cloud model, the public infrastructure-as-a-service (IaaS) provider is responsible for ensuring that each private cloud customer's data remains isolated from every other customer's data both in transit and inside the cloud provider's network. This can be accomplished through the use of security policies requiring some -- or all -- of the following elements: encryption, tunneling, private IP addressing or allocating a unique virtual local area network (VLAN) to each customer.
- A virtual private cloud user can define and directly manage network components, including IP addresses, subnets, network gateways and access control policies.

Benefits and challenges of virtual private clouds

- As mentioned above, one of the biggest benefits of VPCs is that they enable an enterprise to tap into some of the benefits of private clouds, such as more granular network control, while still using off-premises, public cloud resources in a highly scalable, pay-as-you-go model.
- Another benefit of VPCs is enabling a hybrid cloud deployment. An enterprise can use a VPC as an extension of its own data center without dealing with the complexities of building an on-premises private cloud.
- Despite the benefits of VPCs, they can also introduce some challenges. For example, an enterprise might face some complexity when configuring, managing and monitoring its virtual private network (VPN).

- In addition, while VPCs offer an isolated environment within a public cloud in which workloads can run, they are still hosted outside an enterprise's own data center. This means that businesses in highly regulated industries with strict compliance requirements might face limitations on which kinds of applications and data they can place in a VPC.
- Before it commits to a VPC, an enterprise should also verify that all of the resources and services it wants to use from its chosen public cloud provider are available via that provider's VPC.

Virtual private cloud providers

- Most leading public IaaS providers, including Amazon Web Services (AWS), Microsoft Azure and Google, offer VPC and virtual network services.

WAF in Cloud:

- A regular **web application firewall (WAF)** provides security by operating through an application or service, blocking service calls, inputs and outputs that do not meet the policy of a firewall, i.e. set of rules to a HTTP conversation. WAFs do not require modification of application source code.
- The rules to blocking an attack can be customized depending on the role in protecting websites that WAFs need to have. This is considered an evolving information security technology, more powerful than a standard network firewall, or a regular intrusion detection system.

- Today, WAF products are deeply integrated with network technologies such as load balancing and — cloud.
- Cloud-based WAFs, thus, utilize all advantages of WAFs and share that threat detection information among all tenants of the service, which improves results and speeds up detection rates.
- The whole community learns from an attack to any website sharing a single cloud-based WAF service. Plus, cloud based WAF technology is:
    - elastic
    - scalable
    - fast
    - easy to set-up
    - offered as pay-as-you-grow service

- sharing back reports

- **By using cloud-based WAFs, clients need not make any software or hardware changes and tunings to their system**, and can successfully protect their websites from threats, by applying custom rules and deciding on the aggressiveness of the protection.
- This service is used and considered ideal by anyone from financial institutions to mid-sized businesses and trading platforms, to government bodies, e-commerce vendors, and so on. They all pick WAF as protection against top vulnerabilities such as:
  - identity theft
  - access to confidential/unauthorized data
  - falsified transactions
  - injection flaws (such as SQL injection)
  - broken authentication session
  - cross-site scripting (XSS flaws)
  - sensitive data exposure
  - forged requests to access functionality
  - forged HTTP requests to a vulnerable web application
  - vulnerable component exploit
  - unvalidated redirects and forwards
- With cloud space opening up and bringing full virtualization of OS, of storage, of software, platform, and infrastructure, more applications need to be developed for the cloud (while most are not) and remain secure on the cloud.
- With WAF in the cloud, traffic is being redirected to traffic scrubbing and protecting proxy farm of WAFs. Cloud-based WAF service providers will often include a full threat analysis, exception handling policies, as well as continuous monitoring of their service.

Incident Response

- An **event** is an observed change to the normal behavior of a system, environment, process, workflow or person. Examples: router ACLs were updated, firewall policy was pushed.
-
- An **alert** is a notification that a particular event (or series of events) has occurred, which is sent to responsible parties for the purpose of spawning action. Examples: the events above sent to on-call personnel.
-
- An **incident** is an event that negatively affects the confidentiality, integrity, and/or availability (CIA) at an organization in a way that impacts the business. Examples: attacker posts company credentials online, attacker steals customer credit card database, worm spreads through network.

What is Incident Response?

- Incident response (IR) is the steps used to prepare for, detect, contain, and recover from a data breach.Incident response is the methodology an organization uses to respond to and manage a cyber-attack.
- An incident response aims to reduce this damage and recover as quickly as possible.

- An incident response plan is a document that outlines an organization's procedures, steps, and responsibilities of its incident response program.
- It is a document that spells out the actions that need to be taken to minimise the damage and protect your business data during the attack.

Why is Incident Response Important?

- As the cyberattacks increase in scale and frequency, incident response plans become more vital to a company's cyber defenses.

Who is the Incident Response Team?

- The company should look to their "Computer Incident Response Team (CIRT)" to lead incident response efforts. This team is comprised of experts from upper-level management. Incident response should also be supported by HR, legal, and PR or communications.

Six key steps to a response plan:

1,Preparation:

- Developing policies and procedures to follow in the event of a cyber-breach.
- This will include determining the exact composition of the response team and the triggers to alert internal partners.
- Key to this process is effective training to respond to a breach and documentation to record actions taken for later review.

2.Identification:

- This is the process of detecting a breach and enabling a quick, focused response. IT security teams identify breaches using various threat intelligence streams, intrusion detection systems, and firewalls.
- Some people don't understand what threat intelligence is but it's critical to protecting your company.
- Threat intelligence professionals analyze current cyber threat trends, common tactics used by specific groups, and keep your company one step ahead.

3.Containment:

- One of the first steps after identification is to contain the damage and prevent further penetration.
- This can be accomplished by taking specific sub-networks offline and relying on system backups to maintain operations.
- Your company will likely remain in a state of emergency until the breach is contained.

4.Eradication:

- This stage involves neutralizing the threat and restoring internal systems to as close to their previous state as possible.
- This can involve secondary monitoring to ensure that affected systems are no longer vulnerable to subsequent attack.

5.Recovery:

- Security teams need to validate that all affected systems are no longer compromised and can be returned to working condition.
- This also requires setting timelines to fully restore operations and continued monitoring for any abnormal network activity.
- At this stage, it becomes possible to calculate the cost of the breach and subsequent damage.

6.Lessons Learned:

- One of the most important and often overlooked stages.

- During this stage, the incident response team and partners meet to determine how to improve future efforts.
- This can involve evaluating current policies and procedures, as well specific decisions the team made during the incident.
- Final analysis should be condensed into a report and used for future training.
- Forcepoint can help your team analyze previous incidents and help improve your response procedures.
- Protecting your organization requires a determined effort to constantly learn and harden your network against malicious actors.

A Cyber Incident Response Plan is important because it helps the business to:

1. Identify the breach correctly.
2. Contain the attack, control the damage and perhaps thwart the cyber criminals in their attempt to steal data.
3. Protect customer data and other sensitive information as far as possible.
4. Patch the vulnerabilities that allowed the attack to happen in the first place.
5. Recover from the attack with minimal damage and/or regulatory implications.
6. Assess the lessons learned and implement them to enhance/improve the Cyber Incident Response Plan further.

What Does a Cyber Incident Response Plan Include?

A cyber incident response plan example should outline (amongst other things depending on the organisational context) the key steps your company will take in the event of a cyberattack. Your plan should include the following:

- A description of your company's incident response team and their roles and responsibilities.
- An overview of the company's incident response process.
- The steps that will be taken to contain the attack and prevent it from spreading.
- How information will be shared within the company and with external parties.
- The procedures for restoring systems and data.
- The contact information for key personnel.

Log Analysis

What is log analysis?

Log analysis is the process of reviewing, interpreting and understanding computer-generated records called logs.

Key takeaways

- Log analysis functions manipulate data to help users organize and extract information from the logs.
- Organizations that effectively monitor their cyber security with log analysis can make their network assets more difficult to attack.
- Log analysis is a crucial activity for server administrators who value a proactive approach to IT.
- With Sumo Logic's cloud-native platform, organizations and DevOps teams can aggregate and centralize event logs from applications and their infrastructure components throughout private, public and hybrid cloud environments.

What is a log analyzer?

- Log analyzers provide functionality that helps developers and operations personnel monitor their applications as well as visualize log data in formats that help contextualize the data. This, in turn, enables the development team to gain insight into issues within their applications and identify opportunities for improvement. When referencing a log analyzer, we're referring to software designed for use in log management and log analysis.

Log analysis offers many benefits, but these benefits cannot be realized if the processes for log management and log file analysis are not optimized for the task. Development teams can achieve this level of optimization through the use of log analyzers.

How do you analyze logs?

- One of the traditional ways to analyze logs was to export the files and open them in Microsoft Excel. This time-consuming process has been abandoned, as tools like **Sumo Logic** have entered the market. With Sumo Logic, you can integrate with several different environments using IIS web servers, NGINX, and others. With free trials available to test out their log analysis tooling at no risk, the time has never been better to see how log analyzers can help improve your strategies for log analysis and the processes described above.

Log analysis functions and methods

- Log analysis functions manipulate data to help users organize and extract information from the logs. Here are just a few of the most common methodologies for log analysis.
- **Normalization**
  Normalization is a data management technique wherein parts of a message are converted to the same format. The process of centralizing and indexing log data should include a normalization step where attributes from log entries across applications are standardized and expressed in the same format.
- **Pattern recognition**
  Machine learning applications can now be implemented with log analysis software to compare incoming messages with a pattern book and distinguish between "interesting" and "uninteresting" log messages. Such a system might discard routine log entries, but send an alert when an abnormal entry is detected.
- **Classification and tagging**
  As part of our log analysis, we may want to group log entries that are of the same type. We may want to track all of the errors of a certain type across applications, or we may want to filter the data in different ways.
- **Correlation analysis**
  When an event happens, it is likely to be reflected in logs from several different sources. Correlation analysis is the analytical process of gathering log information from a variety of systems and discovering the log entries from each system that connects to the known event.

How to perform log analysis

- Logs provide visibility into the health and performance of an application and infrastructure stack, enabling developer teams and system administrators to easily diagnose and rectify issues. Here's our basic five-step process for managing logs with log analysis software:

1. **Instrument and collect** - install a collector to collect data from any part of your stack. Log files may be streamed to a log collector through an active network, or they may be stored in files for later review.
2. **Centralize and index** - integrate data from all log sources into a centralized platform to streamline the search and analysis process. Indexing makes logs searchable, so security and IT personnel can quickly find the information they need.
3. **Search and analyze** - Analysis techniques such as pattern recognition, normalization, tagging, and correlation analysis can be implemented either manually or using native machine learning.
4. **Monitor and alert** - With machine learning and analytics, IT organizations can implement real-time, automated log monitoring that generates alerts when certain conditions are met. Automation can enable the continuous monitoring of large volumes of logs that cover a variety of systems and applications.
5. **Report and dashboard** - Streamlined reports and dashboarding are key features of log analysis software. Customized reusable dashboards can also be used to ensure that access to confidential security logs and metrics is provided to employees on a need-to-know basis.

Log analysis in cyber security

- Organizations that wish to enhance their capabilities in cyber security must develop capabilities in log analysis that can help them actively identify and respond to cyber threats. Organizations that effectively monitor their cyber security with log analysis can make their network assets more difficult to attack. Cyber security monitoring can also reduce the frequency and severity of cyber-attacks, promote earlier response to threats and help organizations meet compliance requirements for cyber security, including:
- The first step to an effective cyber security monitoring program is to identify business applications and technical infrastructure where event logging should be enabled. Use this list as a starting point for determining what types of logs your organization should be monitoring:
- System logs
    - System activity logs
    - Endpoint logs
    - Application logs
    - Authentication logs
    - Physical security logs
- Networking logs
    - Email logs
    - Firewall logs
    - VPN logs
    - Netflow logs
- Technical logs
    - HTTP proxy logs
    - DNS, DHCP and FTP logs
    - AppFlow logs
    - Web and SQL server logs
- Cyber security monitoring logs
    - Malware protection software logs
    - Network intrusion detection system (NIDS) logs
    - Network intrusion prevention system (NIPS) logs
    - Data loss protection (DLP) logs

Centralized log collection & analysis

- Log events are generated all the time in any application built with visibility and observability in mind. As end users utilize the application, they are creating log events that need to be captured and evaluated for the DevOps team to understand how their application is being used and the
- In addition, it's important to know that the analysis of log events isn't just useful for responding to incidents that are detrimental to the health of the application. It can also help organizations keep tabs on how customers are interacting with their applications. For example, you can track which sources refer to the most users and which browsers and devices are used most frequently. This information can help organizations fine-tune their applications to help provide end users with the greatest value and user experience moving forward. It is much easier to gather this information when log data is contextualized through centralized log collections and intuitive visualizations – and the easiest way to do this is to use log analysis tools such as the one provided by Sumo Logic.

Key metrics (MTTD & MTTR)

- While there are dozens of metrics available to determine success, here are two key cybersecurity performance indicators every organization should monitor MTTD & MTTR.

What is MTTD and MTTR?

- The two measurements and their role in the cyber security industry:
  - Mean Time to Detect (MTTD): Your MTTD is the average time it takes to discover a security threat or incident.
  - Mean Time to Respond (MTTR): Your MTTR measures the average time it takes to control and remediate a threat.
- Your MTTD and MTTR depend on a number of factors, including the size and complexity of your network, the size and expertise of your IT staff, your industry, and more. And different companies measure things in different ways. There are no industry-standard approaches to measuring MTTD and MTTR, so granular comparisons between organizations can be problematic apples-vs-oranges affairs.

Why is it important to measure your security operations effectiveness?

- As they say, what gets measured gets managed, which is why security teams are very well aware that MTTD and MTTR are some of the most important metrics to follow.
- Measuring the effectiveness of your security operations will help you focus your efforts on areas where improvements will provide the highest gains.
- Last but not least, displaying your progress can help you prove the value of your program to your board.
- Best strategies to drive down your MTTD and MTTR
- Reducing MTTD and MTTR is the primary goal of a resilient security operations program, which starts with applying a series of techniques, including:

• Understanding cyber attacks

- TTPs is an acronym that everyone in the industry should be familiar with – tactics, techniques and procedures – but not everyone understands how they aid counterintelligence and cyber security operations. TTPs define how threat actors orchestrate and manage attacks. Knowing these patterns and behaviours allows Analysts to strengthen alerting, identify additional vectors of attack, and provide invaluable support to the investigative process by understanding likely compromised hosts, contextualising events and aiding in the identification of appropriate mitigation processes.

• Optimising your incident response plan

- The key to success in a cyber security incident extends beyond the tools you leverage in your environment. Having a solid IR plan will ensure your business is prepared to respond in the event of an incident. Go beyond the implementation of policy and identify your most sensitive assets, define which critical security events your teams should focus on and get buy-in from management to ensure you are prepared for security breaches.

- Implementation of policy and identify your most sensitive assets, define which critical security events your teams should focus on and get buy-in from management to ensure you are prepared for security breaches.

• Know normal

- Taking the time to understand what is normal will make the abnormal stick out. This will enable Analysts to catch changes in network and endpoint activity that could indicate a security breach. It has the added benefit of allowing Analysts to fine-tune technologies and decrease alert fatigue.

• Streamlining decision making

- Security Orchestration, Automation and Response (SOAR) tools allow security teams to connect disparate systems into one centralised point of authority. This enables security teams to make faster and more efficient decisions. SOAR can be used to escalate alerts, provide additional context and notify the right people and tools to neutralise and remediate incidents.

• Use machine learning to enhance threat hunting

- Develop a comprehensive methodology to simulate threat actor activity within your environment. Test these hypotheses against collected data and leverage technology to automate those searches.

• Conducting regular Offensive Security assessments

- From vulnerability scanning to Penetration Testing, these tests are designed to simulate threat actors breaching an environment. Frequent testing results in a stronger security posture, as Incident Response plans and technologies are further refined and improved.

• Performing regular Security Awareness Training (SAT and Phishing Campaigns)

- People are frequently the weakest security link and the biggest factor in driving down your MTTD and MTTR. Security Awareness Training can never be a "one and done", to be successful it needs to be an ongoing process.

- For any organization to protect itself from cyberattacks and data breaches, it's critical to discover and respond to cyber threats as quickly as possible.
- According to the SANS 2019 Incident Response survey, 52.6% of organizations had an MTTD of less than 24 hours, while 81.4% had an MTTD of 30 days or less.

- Once an incident is detected, 67% of organizations report an MTTR of less than 24 hours, with that number increasing to 95.8% when measuring an MTTR of less than 30 days. However, according to the Verizon Data Breach Investigations Report, 56% of breaches took months or longer to discover at all. That's an incredible amount of time for the bad guys to be inside of your perimeter while preparing to exfiltrate your data.

How to Improve MTTD and MTTR

- Measuring and improving MTTD and MTTR is easier said than done. The fact is that many businesses work with IT teams that are stretched thin and often lack cybersecurity expertise. Meanwhile, they face ever-more

sophisticated attacks stemming from well-funded criminal networks or malicious nation-state actors. That said, there are a number of things every organization can do to drive down its MTTD and MTTR.

Start with a plan: Create an incident response plan in advance of potential attacks to identify and define stakeholder responsibilities so the entire team knows what to do when an attack occurs. This plan can define your processes and services used to detect these threats. As you get a few incidents under your belt, review your plan to look for areas for improvement that can reduce MTTD and MTTR.

Conduct regular cybersecurity training: Cybersecurity isn't simply an IT issue—people are frequently the weakest link. Employees may facilitate a compromise by clicking malicious emails or links that install ransomware, viruses, and other malware. In addition, non-technical company leaders may not grasp the risk of cyberattacks, which keeps them from providing sufficient budget and resources IT needs to be effective. The more educated the entire company becomes about cybersecurity, the more prepared it will be to both prevent and respond to attacks. To be effective, education is an ongoing process rather than "one and done."

Level up to Reduce MTTD and MTTR

A security operations center (SOC) such as the Arctic Wolf SOC-as-a-service can extend the capabilities of your IT team by providing 24/7, real-time monitoring of your on-premise and cloud resources. This will help you see if, when, and where an attack occurs, vastly reducing your MTTD. Meanwhile, Arctic Wolf's Concierge Security™ Team can help reduce MTTR by providing expert advice to help navigate incident response.

Data protection in the cloud

Data In Transit vs. Data At Rest

Definition of Data In Transit vs. Data At Rest

- Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network. Data protection in transit is the protection of this data while it's traveling from network to network or being transferred from a local storage device to a cloud storage device – wherever data is moving, effective data protection measures for in transit data are critical as data is often considered less secure while in motion.
- Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network. While data at rest is sometimes considered to be less vulnerable than data in transit, attackers often find data at rest a more valuable target than data in motion. The risk profile for data in transit or data at rest depends on the security measures that are in place to secure data in either state.
- Protecting sensitive data both in transit and at rest is imperative for modern enterprises as attackers find increasingly innovative ways to compromise systems and steal data.

The Role of Encryption In Data Protection In Transit and At Rest

- Data can be exposed to risks both in transit and at rest and requires protection in both states. As such, there are multiple different approaches to protecting data in transit and at rest. Encryption plays a major role in data protection and is a popular tool for securing data both in transit and at rest. For protecting data in transit, enterprises often choose to encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc) to protect the contents of data in transit. For protecting data at rest, enterprises can simply encrypt sensitive files prior to storing them and/or choose to encrypt the storage drive itself.

Best Practices for Data Protection In Transit and At Rest

Unprotected data, whether in transit or at rest, leaves enterprises vulnerable to attack, but there are effective security measures that offer robust data protection across endpoints and networks to protect data in both states. As mentioned above, one of the most effective data protection methods for both data in transit and data at rest is data encryption.

In addition to encryption, best practices for robust data protection for data in transit and data at rest include:

- Implement robust network security controls to help protect data in transit. Network security solutions like firewalls and network access control will help secure the networks used to transmit data against malware attacks or intrusions.
- Don't rely on reactive security to protect your valuable company data. Instead, use proactive security measures that identify at-risk data and implement effective data protection for data in transit and at rest.
- Choose data protection solutions with policies that enable user prompting, blocking, or automatic encryption for sensitive data in transit, such as when files are attached to an email message or moved to cloud storage, removable drives, or transferred elsewhere.
- Create policies for systematically categorizing and classifying all company data, no matter where it resides, in order to ensure that the appropriate data protection measures are applied while data remains at rest and triggered when data classified as at-risk is accessed, used, or transferred.

Finally, if you utilize a public, private, or hybrid cloud provider for storing data or applications, carefully evaluate cloud vendors based on the security measures they offer – but don't rely on the cloud service to secure your data. Who has access to your data, how is it encrypted, and how often your data is backed up are all imperative questions to ask.

While data in transit and data at rest may have slightly different risk profiles, the inherent risk hinges primarily on the sensitivity and value of your data; attackers will attempt to gain access to valuable data whether it's in motion, at rest, or actively in use, depending on which state is easiest to breach. That's why a proactive approach including classifying and categorizing data coupled with content, user, and context-aware security protocols is the safest and most effective way to protect your most sensitive data in every state.

Frequently Asked Questions

What is the difference between data at rest and data in transit?

- The difference between data at rest and data in transit is simply whether the data is currently stationary or moving to a new location. Data at rest is safely stored on an internal or external storage device.
- Data in transit, also known as data in motion, is data that is being transferred between locations over a private network or the Internet. The data is vulnerable while it is being transmitted. Data can be intercepted and compromised as it travels across the network where it is out of a user's direct control. For this reason, data should be encrypted when in transit. Encryption makes the data unreadable if it falls into the hands of unauthorized users.

What is an example of data in transit?

- An example of data in transit is information transferred between a remote user's mobile device and a cloud-based application. If the data is transmitted in plaintext and not encrypted, it can be compromised by malicious actors. Valuable or sensitive in-transit data should always be encrypted.

Is data encrypted in transit and at rest?

- Data may or may not be encrypted when it is in transit and at rest. Encryption is not a native characteristic of data in either an in-transit or at-rest state. Encryption protects data from unauthorized use and can be implemented on data in transit or at rest. Affording valuable data extra protection through encryption is always a good idea, whether it's at rest or in transit. It is critically important to encrypt sensitive data in transit when it is potentially exposed to unknown entities.

What are some data at rest examples?

Data at rest is information that is currently not moving between two points and is safely stored on a computer or device. As soon as a user attempts to transfer any of these items over the network, they become data in transit. Examples of data at rest include:

- Spreadsheet files stored on your laptop's hard drive
- Videos stored on your iPhone or Android device
- Employment records stored in corporate HR applications
- Sales information that is stored in company databases

Cloud data storage - AWS EBS, S3 / Azure SAS

- Cloud data storage - AWS EBS, S3 / Azure SAS
- **Cloud data storage - AWS EBS**
- Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.
- You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage.
- Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.
- Amazon EBS allows you to create storage volumes and attach them to Amazon EC2 instances.
- Once attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use block storage.
- Amazon EBS volumes are placed in a specific Availability Zone where they are automatically replicated to protect you from the failure of a single component.
- All EBS volume types offer durable snapshot capabilities and are designed for 99.999% availability.

- Amazon EBS provides a range of options that allow you to optimize storage performance and cost for your workload.
- These options are divided into two major categories:
- **SSD-backed storage for transactional workloads**, such as databases and boot volumes (performance depends primarily on IOPS).
- **HDD-backed storage for throughput intensive workloads**, such as MapReduce and log processing (performance depends primarily on MB/s).
- We recommend Amazon EBS for data that must be quickly accessible and requires long-term persistence.
- **Cloud data storage - AWS S3**

- Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance.
- Customers of all sizes and industries can store and protect any amount of data for virtually any use case, such as data lakes, cloud-native applications, and mobile apps. With cost-effective storage classes and easy-to-use management features, you can optimize costs, organize data, and configure fine-tuned access controls to meet specific business, organizational, and compliance requirements.

Azure SAS

Azure shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example:

- What resources the client may access.
- What permissions they have to those resources.
- How long the SAS is valid.

Types of shared access signatures

Azure Storage supports three types of shared access signatures:

- User delegation SAS
- Service SAS
- Account SAS

User delegation SAS

A user delegation SAS is secured with Azure Active Directory (Azure AD) credentials and also by the permissions specified for the SAS. A user delegation SAS applies to Blob storage only.

For more information about the user delegation SAS, see Create a user delegation SAS (REST API).

Service SAS

A service SAS is secured with the storage account key. A service SAS delegates access to a resource in only one of the Azure Storage services: Blob storage, Queue storage, Table storage, or Azure Files.

For more information about the service SAS, see Create a service SAS (REST API).

Account SAS

An account SAS is secured with the storage account key. An account SAS delegates access to resources in one or more of the storage services. All of the operations available via a service or user delegation SAS are also available via an account SAS.

You can also delegate access to the following:

- Service-level operations (For example, the **Get/Set Service Properties** and **Get Service Stats** operations).

- Read, write, and delete operations that aren't permitted with a service SAS.

A shared access signature can take one of the following two forms:

- **Ad hoc SAS**. When you create an ad hoc SAS, the start time, expiry time, and permissions are specified in the SAS URI. Any type of SAS can be an ad hoc SAS.

- **Service SAS with stored access policy**. A stored access policy is defined on a resource container, which can be a blob container, table, queue, or file share. The stored access policy can be used to manage constraints for one or more service shared access signatures. When you associate a service SAS with a stored access policy, the SAS inherits the constraints—the start time, expiry time, and permissions—defined for the stored access policy.

How a shared access signature works

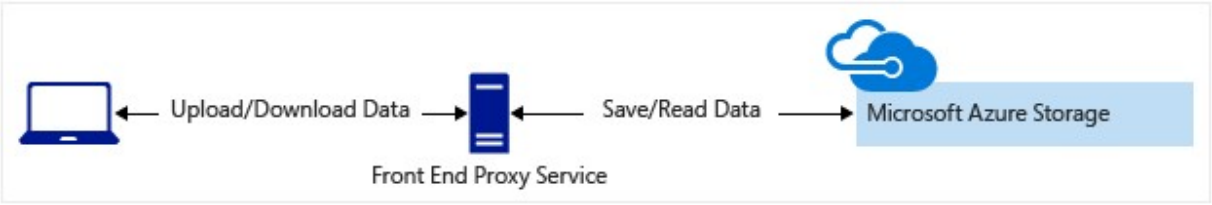
- A shared access signature is a signed URI that points to one or more storage resources. The URI includes a token that contains a special set of query parameters. The token indicates how the resources may be accessed by the client. One of the query parameters, the signature, is constructed from the SAS parameters and signed with the key that was used to create the SAS. This signature is used by Azure Storage to authorize access to the storage resource.
- **Note**
- It's not possible to audit the generation of SAS tokens. Any user that has privileges to generate a SAS token, either by using the account key, or via an Azure role assignment, can do so without the knowledge of the owner of the storage account. Be careful to restrict permissions that allow users to generate SAS tokens. To prevent users from generating a SAS that is signed with the account key for blob and queue workloads, you can disallow Shared Key access to the storage account. For more information, see Prevent authorization with Shared Key.
- **SAS signature and authorization**
- You can sign a SAS token with a user delegation key or with a storage account key (Shared Key).
- ***Signing a SAS token with a user delegation key***
- You can sign a SAS token by using a *user delegation key* that was created using Azure Active Directory (Azure AD) credentials. A user delegation SAS is signed with the user delegation key.
- To get the key, and then create the SAS, an Azure AD security principal must be assigned an Azure role that includes the Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey action. For more information, see Create a user delegation SAS (REST API).

When to use a shared access signature

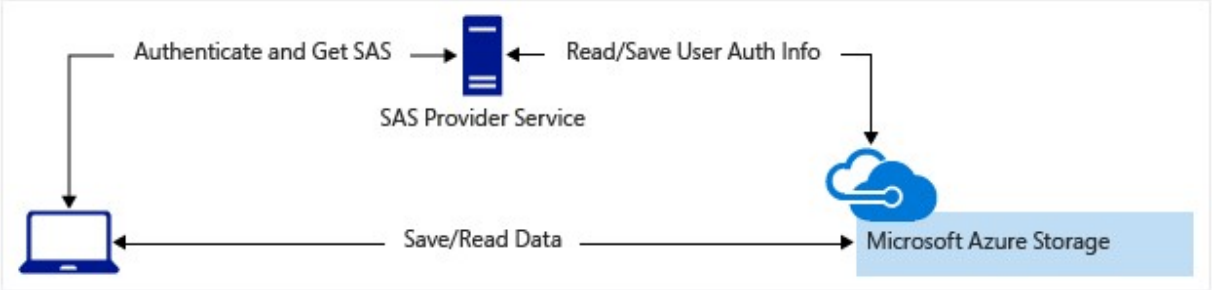
Use a SAS to give secure access to resources in your storage account to any client who does not otherwise have permissions to those resources.

A common scenario where a SAS is useful is a service where users read and write their own data to your storage account. In a scenario where a storage account stores user data, there are two typical design patterns:

1. Clients upload and download data via a front-end proxy service, which performs authentication. This front-end proxy service allows the validation of business rules. But for large amounts of data, or high-volume transactions, creating a service that can scale to match demand may be expensive or difficult.



2. A lightweight service authenticates the client as needed and then generates a SAS. Once the client application receives the SAS, it can access storage account resources directly. Access permissions are defined by the SAS and for the interval allowed by the SAS. The SAS mitigates the need for routing all data through the front-end proxy service.



Many real-world services may use a hybrid of these two approaches. For example, some data might be processed and validated via the front-end proxy. Other data is saved and/or read directly using SAS.

Additionally, a SAS is required to authorize access to the source object in a copy operation in certain scenarios:

- When you copy a blob to another blob that resides in a different storage account.
  You can optionally use a SAS to authorize access to the destination blob as well.
- When you copy a file to another file that resides in a different storage account.
  You can optionally use a SAS to authorize access to the destination file as well.
- When you copy a blob to a file, or a file to a blob.
  You must use a SAS even if the source and destination objects reside within the same storage account.

Secrets Management

Why Secrets Management is Important

Passwords and keys are some of the most broadly used and important tools your organization has for authenticating applications and users and providing them with access to sensitive systems, services, and information. Because secrets have to be transmitted securely, secrets management must account for and mitigate the risks to these secrets, both in transit and at rest.

Secrets can include:

- User or auto-generated passwords
- API and other application keys/credentials (including within containers)
- SSH Keys
- Database and other system-to-system passwords.
- Private certificates for secure communication, transmitting and receiving of data (TLS, SSL etc.)
- Private encryption keys for systems like PGP
- RSA and other one-time password devices

Challenges to Secrets Management

As the IT ecosystem increases in complexity and the number and diversity of secrets explodes, it becomes increasingly difficult to securely store, transmit, and audit secrets.

Common risks to secrets and some considerations include:

- Incomplete visibility and awareness:
- Hardcoded/embedded credentials
- Privileged credentials and the cloud
- DevOps tools
- Third-party vendor accounts/remote access solutions
- Manual secrets management processes
- Best Practices & Solutions for Secrets Management