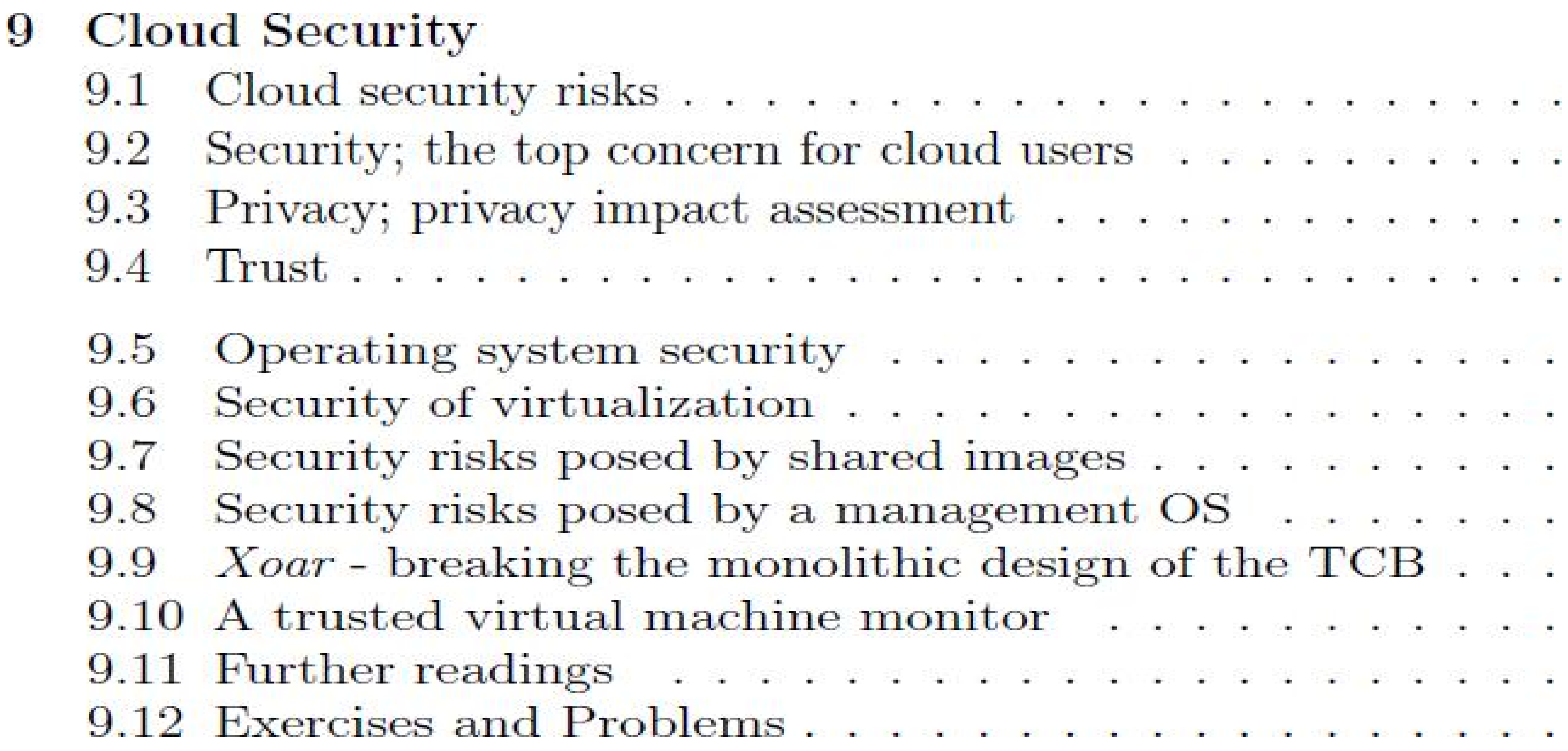
Cloud Security

Prof. Hemant Kumar Apat

Cloud Security



9 Cloud Security

Introduction

- Cloud computing continues to transform the way organizations use, store, and share data, applications, and workloads.
- In Cloud platform, as more data and applications are moving to the cloud, the security threat also increases.
- Cloud technology turned cybersecurity on its head. The availability and scope of data, and its interconnectedness, also made it extremely vulnerable from many threats.

Importance of cloud security

- According to recent research, 1 in 4 companies using public cloud services have experienced data theft by a malicious actor.
- An additional 1 in 5 has experienced an advanced attack against their public cloud infrastructure.
- In the same study, 83% of organizations indicated that they store sensitive information in the cloud. With 97% of organizations worldwide using cloud services today, it is essential that everyone evaluates their cloud security and develops a strategy to protect their data.

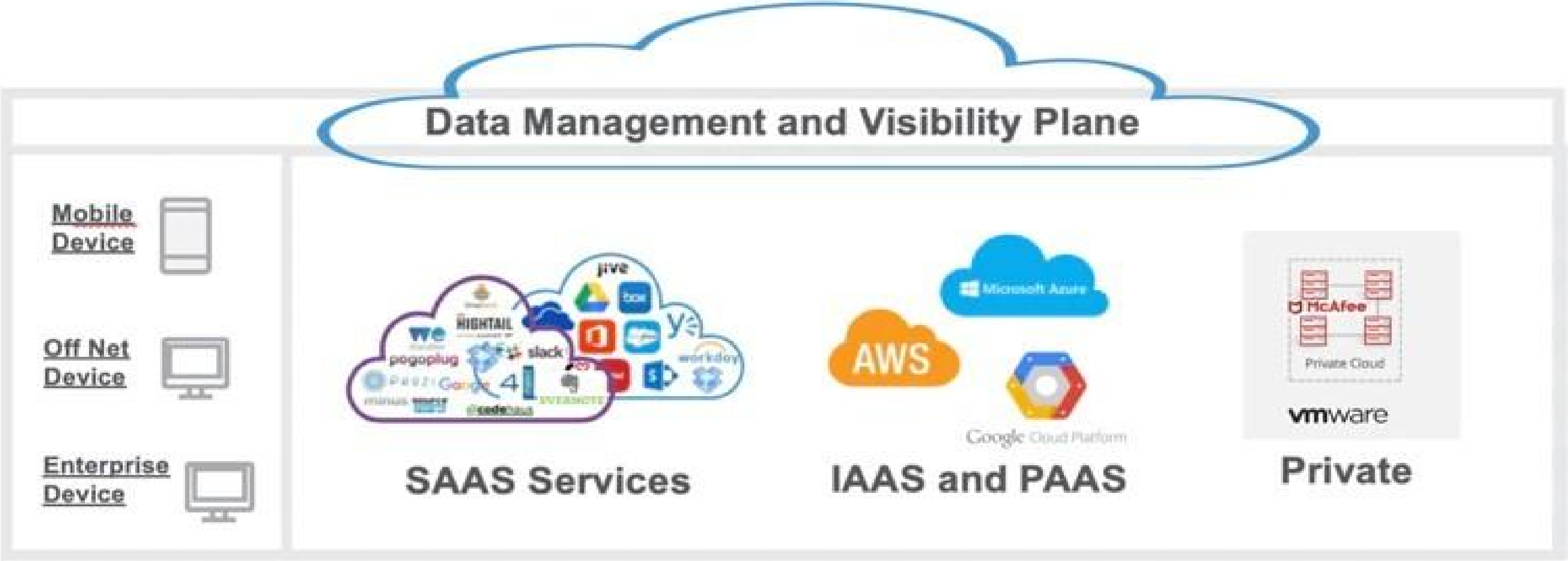
Cloud computing categories

Cloud security differs based on the category of cloud computing being used.

1. **Public cloud services, operated by a public cloud provider** — These include software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).
2. **Private cloud services, operated by a public cloud provider** — These services provide a computing environment dedicated to one customer, operated by a third party.
3. **Private cloud services, operated by internal staff** — These services are an evolution of the traditional data center, where internal staff operates a virtual environment they control.
4. **Hybrid cloud services** — Private and public cloud computing configurations can be combined, hosting workloads and data based on optimizing factors such as cost, security, operations and access. Operation will involve internal staff, and optionally the public cloud provider.

Common control plane across cloud models:

- When using a cloud computing service provided by a public cloud provider, data and applications are hosted with a third party, which marks a fundamental difference between **cloud computing** and **traditional IT**, where most data was held within a self-controlled network.



Challenges in Cloud Computing

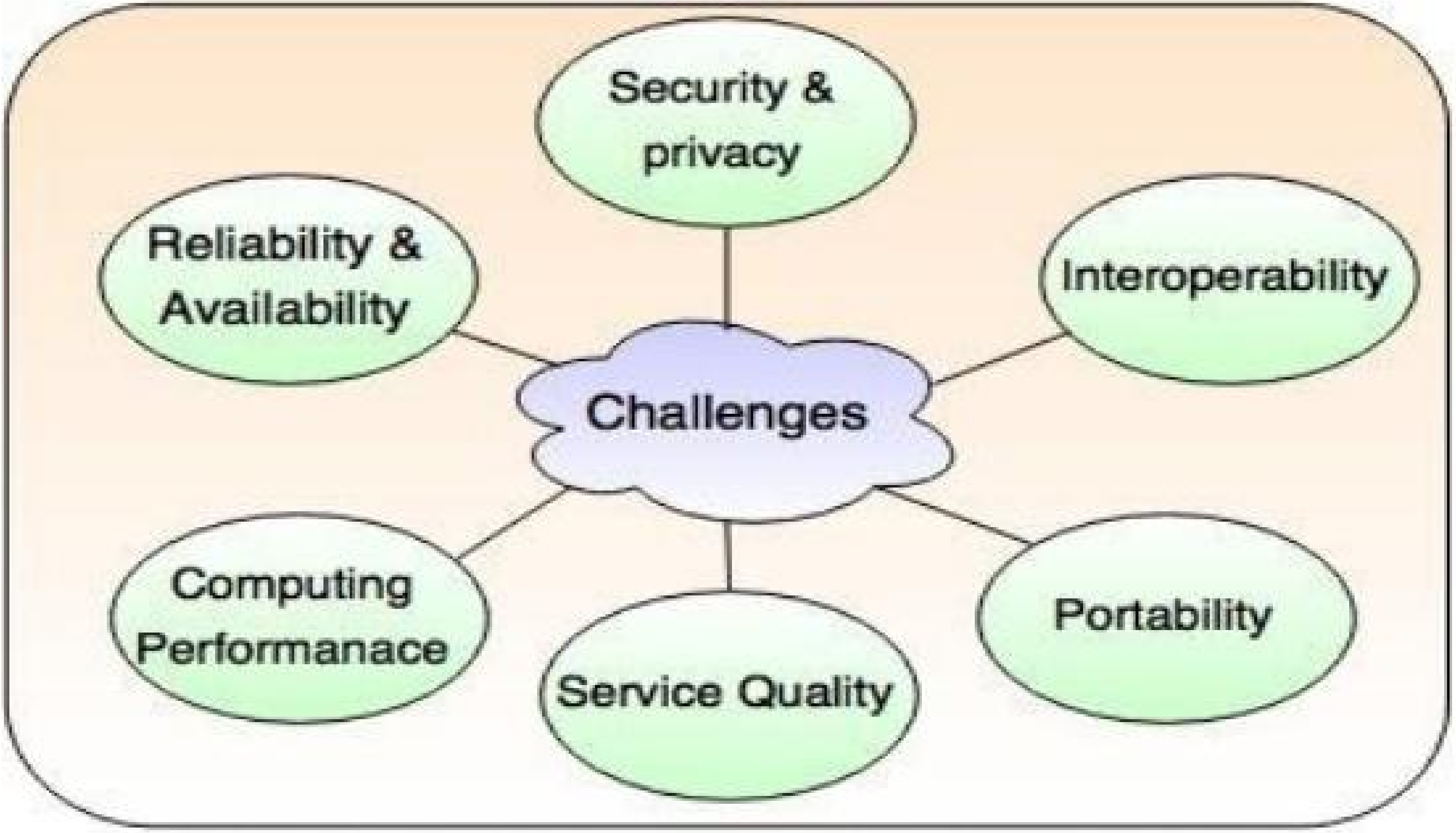


Fig. - Challenges in Cloud Computing

Challenges in Cloud Computing

- **Security and Privacy:** Security and privacy are the main challenge in cloud computing. These challenges can reduced by using security applications, encrypted file systems, data loss software.
- **Interoperability:** The application on one platform should be able to incorporate services from the other platform. This is known as **Interoperability.** It is becoming possible through web services, but to develop such web services is complex.
- **Portability:** The applications running on one cloud platform can be moved to new cloud platform and it should operate correctly without making any changes in design, coding. The portability is not possible, because each of the cloud providers uses different standard languages for their platform.
- **Service Quality:** The Service-Level Agreements (SLAs) of the providers are not enough to guarantee the availability and scalability. The businesses disinclined to switch to cloud without a strong service quality guarantee.
- **Computing Performance:** High network bandwidth is needed for data intensive applications on cloud, this results in high cost. In cloud computing, low bandwidth does not meet the desired computing performance.
- **Reliability and Availability:** Most of the businesses are dependent on services provided by third-party, hence it is mandatory for the cloud systems to be reliable and robust.

Four main categories of cloud computing:

Cloud security differs based on the category of cloud computing being used.

- **Public cloud services, operated by a public cloud provider** — These include software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).
- **Private cloud services, operated by a public cloud provider** — These services provide a computing environment dedicated to one customer, operated by a third party.
- **Private cloud services, operated by internal staff** — These services are an evolution of the traditional data center, where internal staff operates a virtual environment they control.
- **Hybrid cloud services** — Private and public cloud computing configurations can be combined, hosting workloads and data based on optimizing factors such as cost, security, operations and access. Operation will involve internal staff, and optionally the public cloud provider.

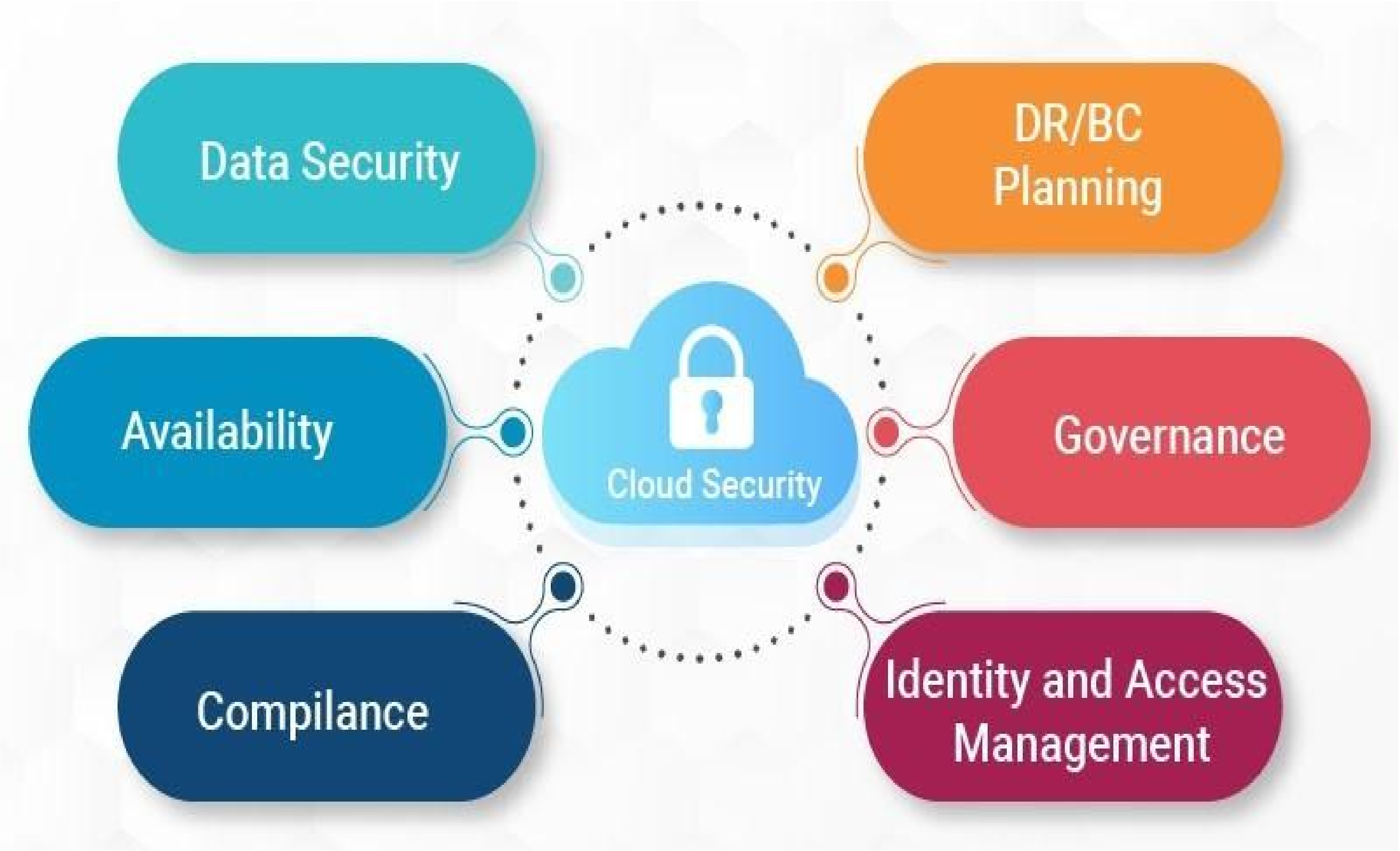
Cloud security

- Cloud security, also known as **cloud computing security**, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure.
- These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices.
- The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place.
- The implementation of cloud security processes is a joint responsibility between the business owner and solution provider.
- Cloud security is a set of policies and procedures which work together to protect data on the remote servers from data corruption, theft, leakage or data loss. The security measures protect cloud data and customers' privacy by setting authentication rules for an individual.

Cloud Security

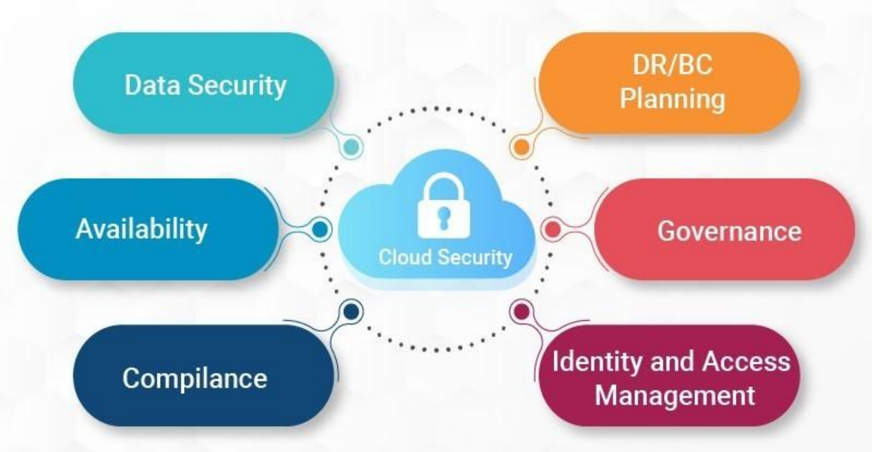
- Cloud security, also known as cloud computing security, consists of a set of **policies**, **controls**, **procedures** and **technologies** that work together to protect cloud-based systems, data, and infrastructure.
- These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices.
- Cloud service authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business.
- Security service rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.
- The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place and the implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

Component of Cloud Security



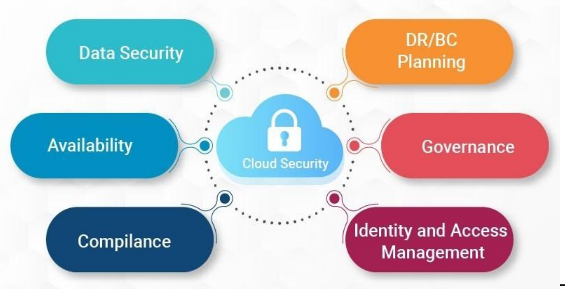
Component of Cloud Security

- **Data Security:** Several data threats are associated with cloud data services which generally includes, Denial of service attacks, side-channel attacks, Data breaches, insider threats, Malware injection, Insecure APIs, virtualisation threats and Abuse of Cloud services. Data security ensures protection from these vulnerabilities.
- **Availability:** This expresses the context of data and services are available. And that will be transmitted to your location encrypted and secured.
- **Compliance:** Cloud compliance specifies the laws and regulations that apply while working. It also includes access to information laws which may enable governance.



Component of Cloud Security

- **DR/BC Planning:** Cloud Disaster Recovery and Business Continuity refers to the planning of technologies and services which can be applied at the time of mishappening or unplanned events with minimum delay in Business.
- **Governance:** Cloud Security governance is a management model to conduct security management and operations in the cloud to ease the business targets to achieve. It explains the methodology of structures, operational practices, performance expectations and metrics for optimising Business value.
- **Identity and Access Management (IAM):** This covers products, processes and policies (3Ps). Companies use the set of 3Ps to manage user identities within an organisation. Also, it is used to validate user access.These components come under cloud security and protection.



Attacks in a cloud computing environment

Three actors involved; six types of attacks possible.

The user can be attacked by:

- Service → SSL certificate spoofing, attacks on browser caches, or phishing attacks.
- The cloud infrastructure → attacks that either originates at the cloud or spoofs to originate from the cloud infrastructure.

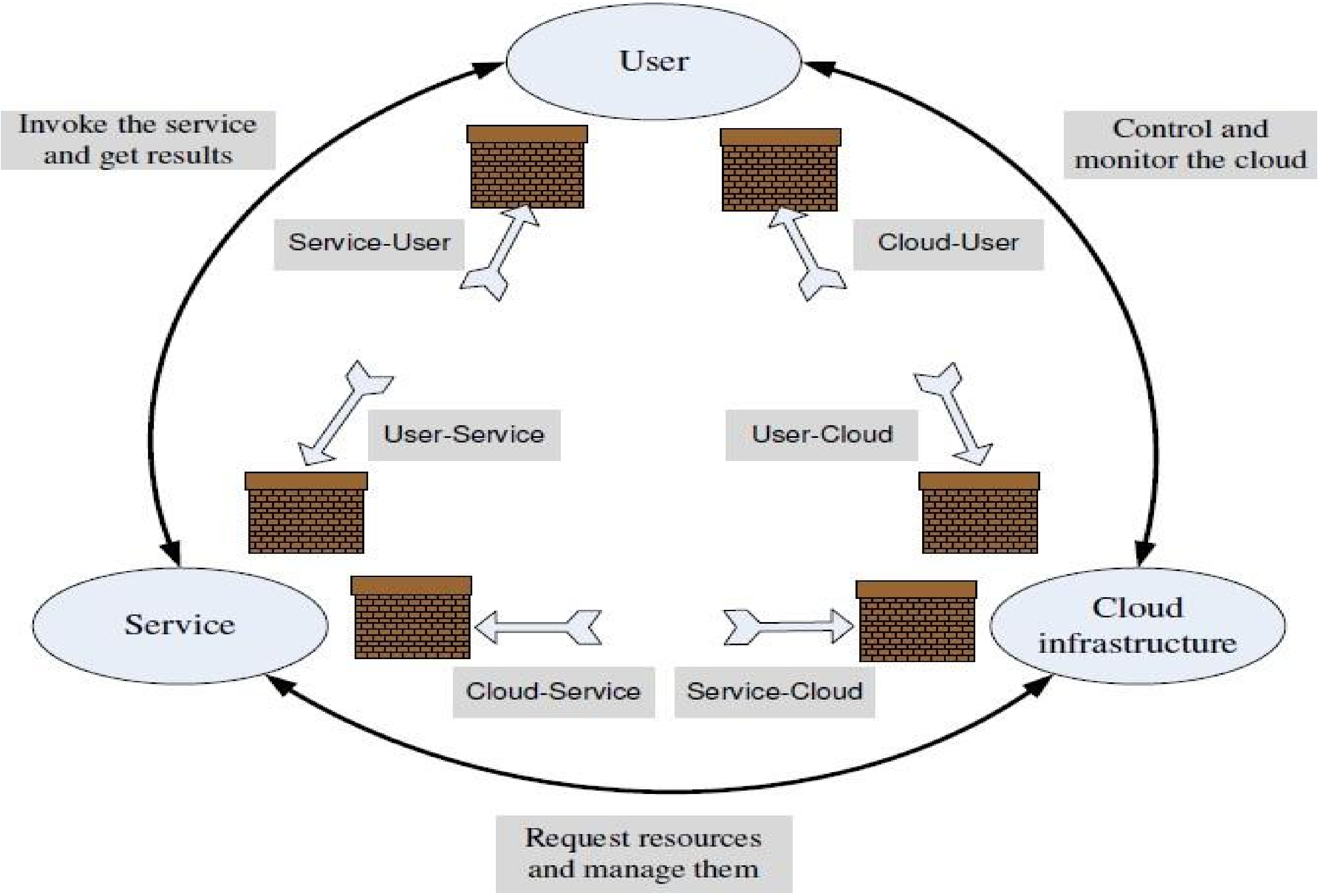
The service can be attacked by:

- A user→ buffer overflow, SQL injection, and privilege escalation are the common types of attacks.
- The cloud infrastructure → the most serious line of attack. Limiting access to resources, privilege-related attacks, data distortion, injecting additional operations.

The cloud infrastructure can be attacked by:

- A user → targets the cloud control system.
- A service → requesting an excessive amount of resources and causing the exhaustion of the resources.

Surfaces of attacks in a cloud computing environment



Top threats to cloud computing

- **Sept. 23, 2020** – The Cloud Security Alliance (CSA), the world's leading organization dedicated to defining standards, certifications and best practices to help ensure a secure cloud computing environment, today released Top Threats to Cloud Computing: Egregious 11 Deep Dive.

11 Top Threats to Cloud Computing

1. Data Breach;
2. Misconfiguration and Inadequate Change Control;
3. Insufficient Identity, Credential, Access, and Key Management;
4. Insufficient Identity and Credential Management;
5. Account Hijacking;
6. Insider Threat;
7. Insecure Interfaces and Application Programming Interfaces;
8. Weak Control Plane;
9. Metastructure and Applistructure Failures;
10. Limited Cloud Usage Visibility;
11. Abuse and Nefarious Use of Cloud Services.

Top Threats to Cloud Computing:[1]

1 **Data breaches :** A data breach can be any cybersecurity incident or attack in which sensitive or confidential information is viewed, stolen, or used by an unauthorized individual.

Business Impact

- Data breaches can damage a company's reputation and foster mistrust from customers and partners.
- A breach can lead to the loss of intellectual property (IP) to competitors, impacting the release of a new product.
- Regulatory implications many result in financial loss.
- Impact to a company's brand could affect its market value.
- Legal and contractual liabilities may arise.
- Financial expenses may occur as a result of incident response and forensics.

Top Threats to Cloud Computing:[1] Data breaches

1 **Data breaches :** A data breach can be any cybersecurity incident or attack in which sensitive or confidential information is viewed, stolen, or used by an unauthorized individual.

Key Takeaways and Recommendations

- Defining the business value of data and the impact of its loss is essential for organizations that own or process data.
- Protecting data is evolving into a question of who has access to it.
- Data accessiblevia the Internet is the most vulnerable asset for misconfiguration or exploitation.
- Encryption techniques can protect data but can also hamper system performance and make applications less user-friendly.
- A robust and well-tested incident response plan that considers the cloud provider and data privacy laws can help data breach victims recover.

11 Top Threats to Cloud Computing: [2]

[2] Misconfiguration and inadequate change control

- Misconfiguration occurs when computing assets are set up incorrectly, leaving them vulnerable to malicious activity.
- Some examples of misconfiguration include: Unsecured data storage elements or containers, excessive permissions, unchanged default credentials and configuration settings, standard security controls left disabled, unpatched systems and logging or monitoring left disabled, and unrestricted access to ports and services.

Business Impact

- The business impact depends on the nature of the misconfiguration, and how quickly it is detected and resolve. The most common issue is the exposure of data stored in cloud repositories

11 Top Threats to Cloud Computing: [2]

[2] Misconfiguration and inadequate change control

- Misconfiguration occurs when computing assets are set up incorrectly, leaving them vulnerable to malicious activity.

Key Takeaways and Recommendations

- As cloud-based resources can be complex and dynamic, they can prove challenging to configure.
- Traditional controls and approaches for change management are not effective in the cloud.
- Companies should embrace automation and use technologies that continuously scan for misconfigured resources and remediate problems in real time.

11 Top Threats to Cloud Computing: [3]

[3] Insufficient identity, credential, access and key management

- Security incidents and breaches can occur due to the inadequate protection of credentials, a lack of regular automated rotation of cryptographic keys and passwords, a lack of scalable identity and credential management systems, a failure to use multifactor authentication , and a failure to use strong passwords.

Business Impact

- Insufficient identity, credential, or key management can enable unauthorized access to data. As a result, malicious actors masquerading as legitimate users can read, modify, and delete data. Hackers can also issue control plane and management functions, snoop on data in transit, and release malware that appears to come from a legitimate source.

Key Takeaways and Recommendations

- Secure accounts that are inclusive to two-factor authentication and limit the use of root accounts.
- Practice the strictest identity and access controls for cloud users and identities.
- Segregate and segment accounts, virtual private clouds (VPCs), and identity groups based on business needs and the principle of least privilege.
- Rotate keys, remove unused credentials and privileges, employ central and programmatic
  key management.

11 Top Threats to Cloud Computing: [4]

[4] Lack of cloud security architecture and strategy

- As companies migrate parts of their IT infrastructure to the public cloud, one of the largest challenges is implementing the proper security to guard against cyber attacks. Assuming that you can just "lift and shift' your existing, internal IT stack and security controls to the cloud can be a mistake.

Business Impact

- Proper security architecture and strategy are required for securely moving, deploying, and operating in the cloud. Successful cyberattacks due to weak security can lead to financial loss, reputational damage, legal repercussions, and fines.

Key Takeaways and Recommendations

- Make sure that security architecture aligns with your business goals and objectives.
- Develop and implement a security architecture framework.
- Ensure that the threat model is kept up to date.
- Bring continuous visibility into the actual security posture.

11 Top Threats to Cloud Computing: [5]

[5] Account hijacking

- Through account hijacking, attackers gain access to and abuse accounts that are highly privileged or sensitive. In cloud environments, the accounts at greatest risk are cloud service accounts or subscriptions.

Business Impact

- As account hijacking implies full compromise and control of an account, business logic, function, data, and applications reliant on the account can all be at risk.
- The fallout from account hijacking can be severe. Some recent breach cases lead to significant operational and business disruptions, including the complete elimination of assets, data, and capabilities.
- Account hijacking can trigger data leaks that lead to reputational damage, brand value degradation, legal liability exposure, and sensitive personal and business information disclosures.

Key Takeaways and Recommendations

- Account hijacking is a threat that must be taken seriously.
- Defense-in-depth and IAM controls are key in mitigating account hijacking.

11 Top Threats to Cloud Computing: [6]

[6] Insider threats

- Insiders don't have to break through firewalls, virtual private networks (VPNs), and other security defenses and instead operate on a trusted level where they can directly access networks, computer systems, and sensitive data.

Business Impact

- Insider threats can result in the loss of proprietary information and intellectual property.
- System downtime associated with insider attacks can impact company productivity.
- Data loss can reduce confidence in company services.
- Dealing with insider security incidents requires containment, remediation, incident response, investigation, post-incidence analysis, escalation, monitoring, and surveillance, all of which can add to a company's workload and security budget.

11 Top Threats to Cloud Computing: [6]

[6] Insider threats …

Key Takeaways and Recommendations

- Take measures to minimize insider negligence to mitigate the consequences of insider threats.
- Provide training to your security teams to properly install, configure, and monitor your computer systems, networks, mobile devices, and backup devices.
- Provide training to your regular employees to inform them how to handle security risks, such as phishing and protecting corporate data they carry outside the company on laptops and mobile devices.
- Require strong passwords and frequent password updates.
- Inform employees of repercussions related to engaging in malicious activity.
- Routinely audit servers in the cloud and on-premises, and then correct any changes from the secure baseline set across the organization.
- Make sure that privileged access security systems and central servers are limited to a minimum number of employees, and that these individuals include only those with the training to handle the administration of mission-critical computer servers.
- Monitor access to all computer servers at any privilege level.

11 Top Threats to Cloud Computing: [7]

[7] Insecure interfaces and APIs

- APIs (Application Programming Interfaces) and UIs (User Interfaces) are typically the most exposed parts of a system, often the only asset with a public IP address available outside the trusted boundary. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent security.

Business Impact

- Though most cloud providers try to integrate security into their models, cloud customers must also understand the security implications. A weak set of interfaces and APIs exposes organizations to various security issues related to confidentiality, integrity, availability, and accountability.

Key Takeaways and Recommendations

- Practice good API hygiene. This includes the diligent oversight of items such as inventory, testing, auditing, and abnormal activity protections.
- Ensure the proper protection of API keys and avoid reuse.
- Consider using standard and open API frameworks (e.g., Open Cloud Computing Interface (OCCI) and Cloud Infrastructure Management Interface (CIMI)).

11 Top Threats to Cloud Computing: [8]

[8] Weak control plane

- The control plane enables the security and integrity to complement the data plane, which provides the stability of the data. A weak control plane means the person in charge is not in full control of the data infrastructure's logic, security, and verification.

Business Impact

- A weak control plane could result in data loss, either by theft or corruption. Regulatory punishment for data loss may be incurred as well.
- With a weak control plane, users may also be unable to protect their cloud-based business data and applications.

Key Takeaways and Recommendations

- Adequate security controls provided through a cloud provider are necessary so that cloud customers can fulfill their legal and statutory obligations.
- Cloud customers should perform due diligence and determine if the cloud service they intend to use possesses an adequate control plane.

11 Top Threats to Cloud Computing: [9]

[9] Metastructure and applistructure failures

- Potential failures exist at multiple levels in the metastructure and applistructure model. For example, poor API implementation by the cloud provider offers attackers an opportunity to disrupt cloud customers by interrupting confidentiality, integrity, or availability of the service.

Business Impact

- Metastructure and applistructure are critical components of a cloud service. Failures involving these features at the cloud provider level can severely impact all service consumers. At the same time, misconfigurations by the customer could disrupt the user financially and operationally.

Key Takeaways and Recommendations

- Cloud providers must offer visibility and expose mitigations to counteract the cloud's inherent lack of transparency for customers.
- Cloud customers should implement appropriate features and controls in cloud native designs.
- All cloud providers should conduct penetration testing and provide findings to customers.

11 Top Threats to Cloud Computing: [10]

[10] Limited cloud usage visibility

- Limited cloud usage visibility occurs when an organization does not have the ability to visualize and analyze whether cloud service use within the organization is safe or malicious.

Business Impact

- Lack of governance. When employees are unfamiliar with proper access and governance controls, sensitive corporate data can be placed in public access locations vs. private access locations.
- Lack of awareness. When data and services are in use without the knowledge of the company, they are unable to control their IP. That means the employee has the data, not the company.
- Lack of security. When an employee incorrectly sets up a cloud service, it can become exploitable not only for the data that resides on it but for future data. Malware, botnets, cryptocurrency mining malware, and more can compromise cloud containers, putting organizational data, services, and finances at risk.

11 Top Threats to Cloud Computing: [10]

[10] Limited cloud usage visibility

Key Takeaways and Recommendations

- Mitigating these risks starts with the development of a complete cloud visibility effort from the top down. This process usually starts with creating a comprehensive solution that ties into people, process, and technology.
- Mandate company-wide training on accepted cloud usage policies and enforcement.
- All non-approved cloud services should be reviewed and approved by the cloud security architect or third-party risk management.
- Invest in solutions like cloud access security brokers (CASB) or software defined gateway (SDG) to analyze outbound activities and help discover cloud usage, at-risk users, and to follow the behavior of credentialed employees to identify anomalies.
- Invest in a web application firewall (WAF) to analyze all inbound connections to your cloud services for suspicious trends, malware, distributed denial-of-service (DDoS), and Botnet risks.
- Select solutions that are specifically designed to monitor and control all of your key enterprise cloud applications (enterprise resource planning, human capital management, commerce experience, and supply chain management) and ensure suspicious behaviors can be mitigated.
- Implement a zero-trust model across your organization.

11 Top Threats to Cloud Computing: [11]

[11] Abuse and nefarious use of cloud services

- Malicious actors may leverage cloud computing resources to target users, organizations, or other cloud providers, and can also host malware on cloud services. Some examples of the misuse of cloud resources include: launching DDoS attacks, email spam and phishing campaigns, "mining" for digital currency, large-scale automated click fraud, brute-force attacks of stolen credential databases, and hosting of malicious or pirated content.

Business Impact

- If an attacker has compromised the management plane of a customer's cloud infrastructure, the attacker can use the cloud service for illicit purposes while the customer foots the bill. The bill could be substantial if the attacker consumed substantial resources, such as mining cryptocurrency.
- Attackers can also use the cloud to store and propagate malware. Enterprises must have controls in place to deal with these new attack vectors. This may mean procuring security technology that can monitor cloud infrastructure or API calls from and to the cloud service.

Key Takeaways and Recommendations

- Enterprises should monitor their employees in the cloud, as traditional mechanisms are unable to mitigate the risks posed by cloud service usage.
- Employ cloud data loss prevention (DLP) technologies to monitor and stop any unauthorized data exfiltration.

The benefits of a top cloud computing security solution:

1. **Protection against DDoS**. Distributed denial of service attacks are on the rise, and a top cloud computing security solution focuses on measures to stop huge amounts of traffic aimed at a company's cloud servers. This entails monitoring, absorbing and dispersing DDoS attacks to minimize risk.
2. **Data security**. In the ever-increasing era of data breaches, a top cloud computing security solution has security protocols in place to protect sensitive information and transactions. This prevents a third party from eavesdropping or tampering with data being transmitted.
3. **Regulatory compliance**. Top cloud computing security solutions help companies in regulated industries by managing and maintaining enhanced infrastructures for compliance and to protect personal and financial data.

The benefits of a top cloud computing security solution:

4. **Flexibility**. A cloud computing solution provides you with the security you need whether you're turning up or down capacity. You have the flexibility to avoid server crashes during high traffic periods by scaling up your cloud solution. Then when the high traffic is over, you can scale back down to reduce costs.
5. **High availability and support**. A best-practices cloud computing security solution offers constant support for a company's assets. This includes live monitoring 24 hours a day, 7 days a week, and every day of the year. Redundancies are built-in to ensure your company's website and applications are always online.

Segmentation of cloud security responsibilities

- In each public cloud service type, the cloud provider and cloud customer share different levels of responsibility for security. By service type, these are:

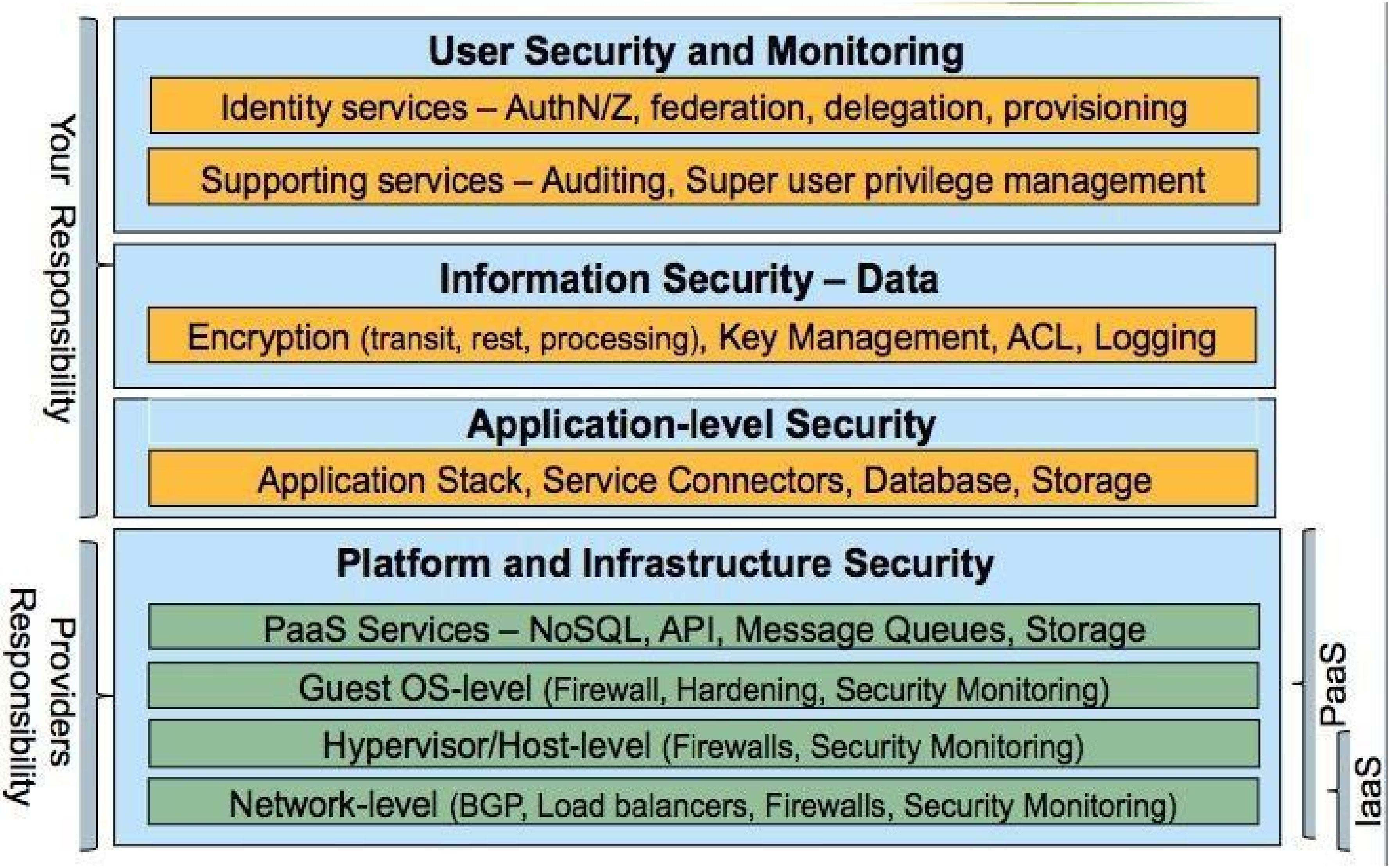
- **Software-as-a-service (SaaS)** — Customers are responsible for securing their data and user access.
- **Platform-as-a-service (PaaS)** — Customers are responsible for securing their data, user access, and applications.
- **Infrastructure-as-a-service (IaaS)** — Customers are responsible for securing their data, user access, applications, operating systems, and virtual network traffic.

What Is Cloud Security Architecture?

- Cloud security architecture is a strategy designed to secure and view an enterprise's data and collaboration applications in the cloud through the lens of shared responsibility with cloud providers.
- Cloud-enabled innovation is becoming a competitive requirement. As more enterprises seek to accelerate their business by shifting data and infrastructure to the cloud, security has become a higher priority. Operations and development teams are finding new uses for cloud services, and companies are searching for strategies to gain speed and agility. Enterprises must remain competitive by adding new collaborative capabilities and increasing operational efficiency in the cloud – while also saving money and resources.

Cloud Security Architecture is a shared responsibility

- Cloud security is based on a shared cloud responsibility model in which both the provider and the customer possess responsibility in securing the cloud.
- Shared responsibility does not mean less responsibility. Cloud providers will cover many aspects of physical, infrastructure, and application security while cloud customers remain responsible for certain areas of security and control, depending on the cloud environment.



User Security and Monitoring

Identity services – AuthN/Z, federation, delegation, provisioning

Supporting services – Auditing, Super user privilege management

Information Security – Data

Encryption (transit, rest, processing), Key Management, ACL, Logging

Application-level Security

Application Stack, Service Connectors, Database, Storage

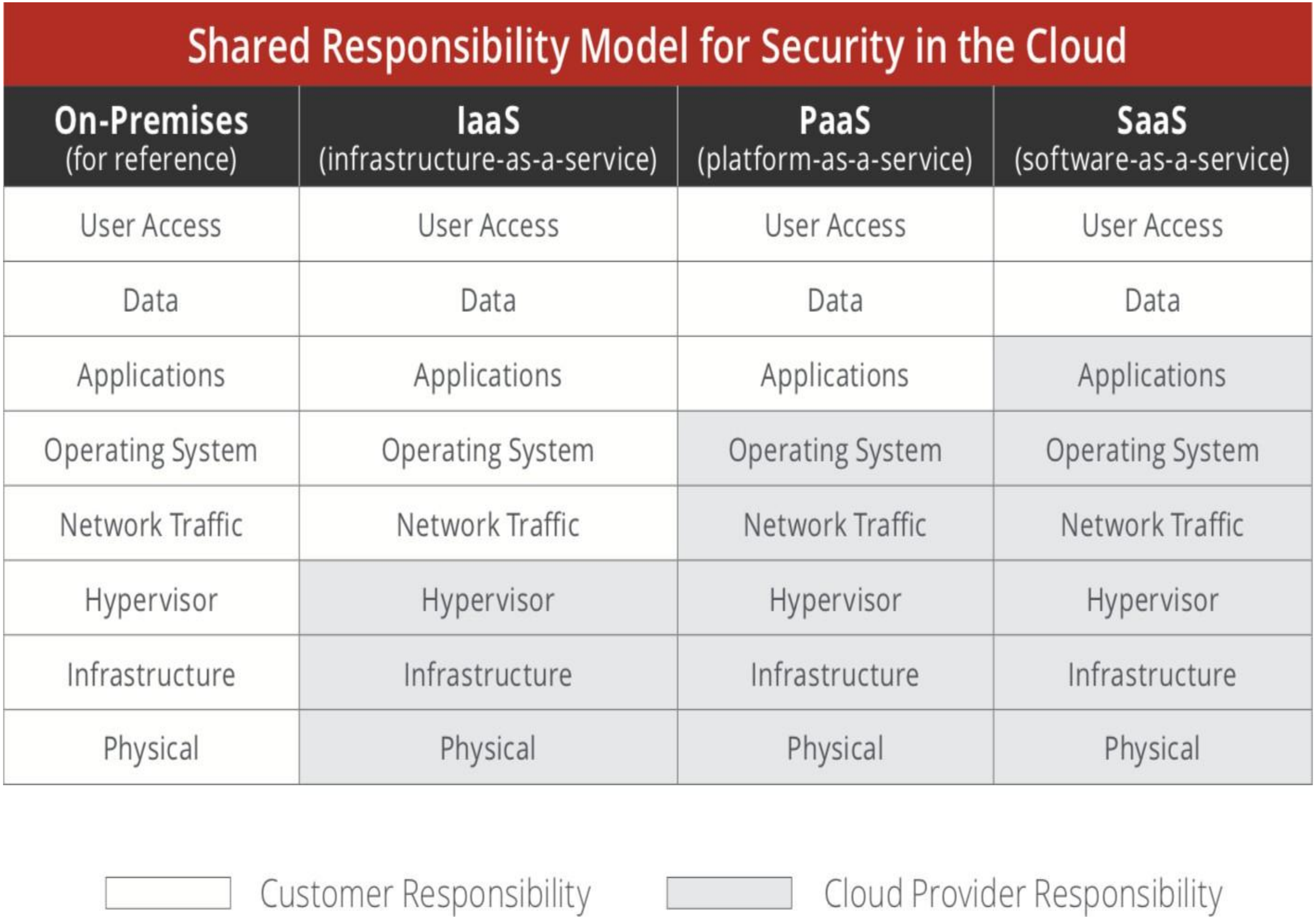
Platform and Infrastructure Security

PaaS Services – NoSQL, API, Message Queues, Storage

Guest OS-level (Firewall, Hardening, Security Monitoring)

Hypervisor/Host-level (Firewalls, Security Monitoring)

Network-level (BGP, Load balancers, Firewalls, Security Monitoring)

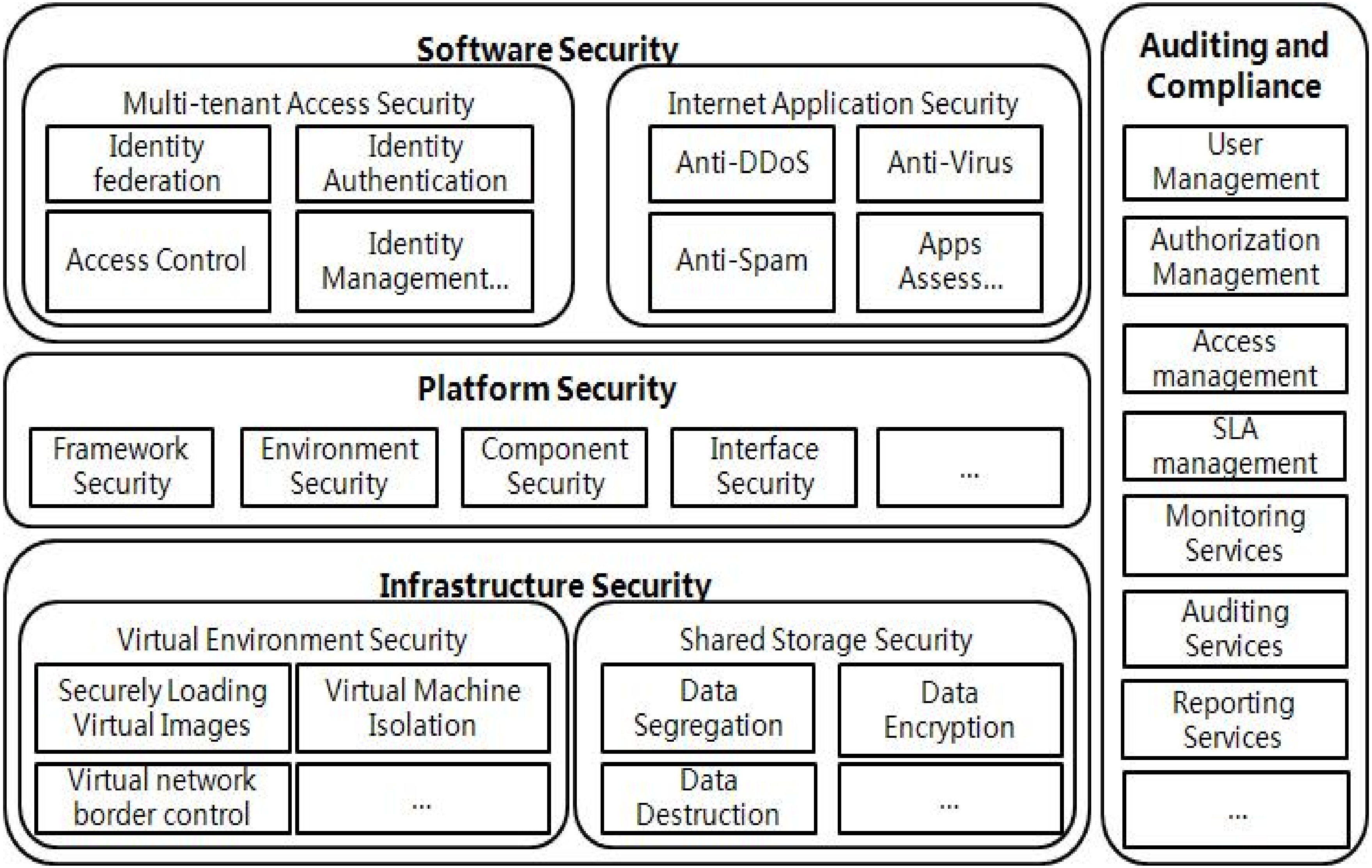


Shared Responsibility Model for Security in the Cloud

On-Premises (for reference)	**IaaS** (infrastructure-as-a-service)	**PaaS** (platform-as-a-service)	**SaaS** (software-as-a-service)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	▨ Applications
Operating System	Operating System	▨ Operating System	▨ Operating System
Network Traffic	Network Traffic	▨ Network Traffic	▨ Network Traffic
Hypervisor	▨ Hypervisor	▨ Hypervisor	▨ Hypervisor
Infrastructure	▨ Infrastructure	▨ Infrastructure	▨ Infrastructure
Physical	▨ Physical	▨ Physical	▨ Physical

□ Customer Responsibility ▨ Cloud Provider Responsibility

Cloud Computing Security Architecture



Software Security

Multi-tenant Access Security

- Identity federation
- Identity Authentication
- Access Control
- Identity Management...

Internet Application Security

- Anti-DDoS
- Anti-Virus
- Anti-Spam
- Apps Assess...

Platform Security

- Framework Security
- Environment Security
- Component Security
- Interface Security
- ...

Infrastructure Security

Virtual Environment Security

- Securely Loading Virtual Images
- Virtual Machine Isolation
- Virtual network border control
- ...

Shared Storage Security

- Data Segregation
- Data Encryption
- Data Destruction
- ...

Auditing and Compliance

- User Management
- Authorization Management
- Access management
- SLA management
- Monitoring Services
- Auditing Services
- Reporting Services
- ...

Cloud Security responsibility: Infrastructure-as-a-Service (IaaS)

- IaaS is a cloud computing model that provides virtualized computing resources including networking, storage, and machines accessible through the internet. In IaaS, the Cloud Service Provider (CSP) is responsible for the controls that protect their underlying servers and data including security of servers, storage and networking hardware, virtualization, and the hypervisor. The enterprise's security responsibilities include user access, data, applications, operating systems, and network traffic.
- **According to Gartner**, by 2021, 50% of enterprises will unknowingly and mistakenly have exposed some IaaS storage services, network segments, applications, or APIs directly to the public internet, up from 25% atYE18 (year-end 2018).
- Through 2023— at least 99% of cloud security failures will be the customer's fault."

IaaS cloud security models require these security features

- Audit and monitor resources for misconfiguration
- Automate policy corrections
- Prevent data loss with DLP
- Capture custom app activity and enforce controls
- Detect malicious user activity and behavior
- Detect and remove malware
- Discover rouge IaaS services and accounts
- Identify provisioned user risk
- Enrich native cloud platform forensics
- Manage multiple IaaS provider

Cloud Security responsibility:

- According to Gartner, through 2023, at least 99% of cloud security failures will be the customer’s fault.Through 2024, workloads that leverage the programmability of cloud infrastructure to improve security protection will demonstrate improved compliance and at least 60% fewer security incidents than those in traditional data centers. As with on-premises data centers, the majority of successful cloud attacks are caused by mistakes, such as misconfiguration, missing patches, or mismanaged credentials.To achieve more secure cloud-based infrastructure and platform services, Gartner recommends a systematic and risk-based approach for IaaS/PaaS security using a set of layered capabilities.

Cloud Security responsibility: Platform-as-a-Service (PaaS)

- The CSP secures a majority of a PaaS cloud service model, however, the enterprise is responsible for the security of its applications. PaaS builds upon IaaS deploying applications without taking on the cost and resources required to buy and manage hardware, software, and hosting capabilities.These features can include:

1. Cloud Access Security Brokers (CASB)
2. Cloud workload protection platforms (CWPP)
3. Cloud security posture management (CSPM)
4. Business analytics/intelligence
5. Logs
6. IP restrictions
7. API gateways
8. Internet of Things (IoT)

Cloud Security responsibility: Software-as-a-Service (SaaS)

- **Software-as-a-Service (SaaS)** – Terms of security ownership within SaaS are negotiated with the CSP as part of their service contract. SaaS often hosts an enterprise's physical, infrastructure, hypervisor, network traffic, and operating system.
- SaaS apps and infrastructure controls can include:

1. Enforce data loss prevention (DLP)
2. Prevent unauthorized sharing of sensitive data to wrong people
3. Block sync/download of corporate data to personal devices
4. Detect compromised account, insider threats, and malware
5. Gain visibility into unsanctioned applications
6. Audit for misconfiguration

A set of principles you can apply when evaluating a cloud service provider's security maturity:

- **Disclosure of security policies, compliance and practices**: The cloud service provider should demonstrate compliance with industry standard frameworks such as ISO 27001, SS 16 and CSA Cloud controls matrix.
- Controls certified by the provider should match control expectations from your enterprise data protection standard standpoint. When cloud services are certified for ISO 27001 or SSAE 16, the scope of controls should be disclosed. Clouds that host regulated data must meet compliance requirements such as PCI DSS, Sarbanes-Oxley and HIPAA.
- **Disclosure when mandated:** The cloud service provider should disclose relevant data when disclosure is imperative due to legal or regulatory needs.

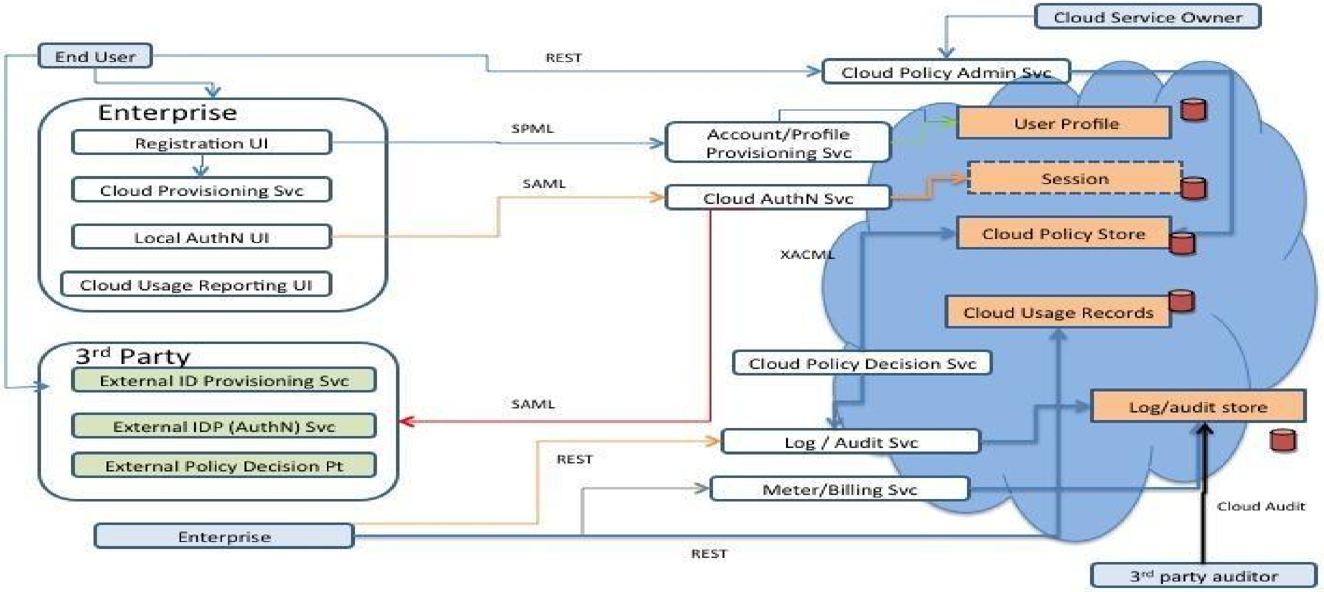
A set of principles you can apply when evaluating a cloud service provider's security maturity:

- **Security architecture:** The cloud service provider should disclose security architectural details that either help or hinder security management as per the enterprise standard. For example, the architecture of virtualization that guarantees isolation between tenants should be disclosed.
- **Security Automation –** The cloud service provider should support security automation by publishing API(s) (HTTP/SOAP) that support:
  - Export and import of security event logs, change management logs, user entitlements (privileges), user profiles, firewall policies, access logs in a XML or enterprise log standard format.
  - Continuous security monitoring including support for emerging standards such as Cloud Audit.
- **Governance and Security responsibility:** Governance and security management responsibilities of the customer versus those of the cloud provider should be clearly articulated.

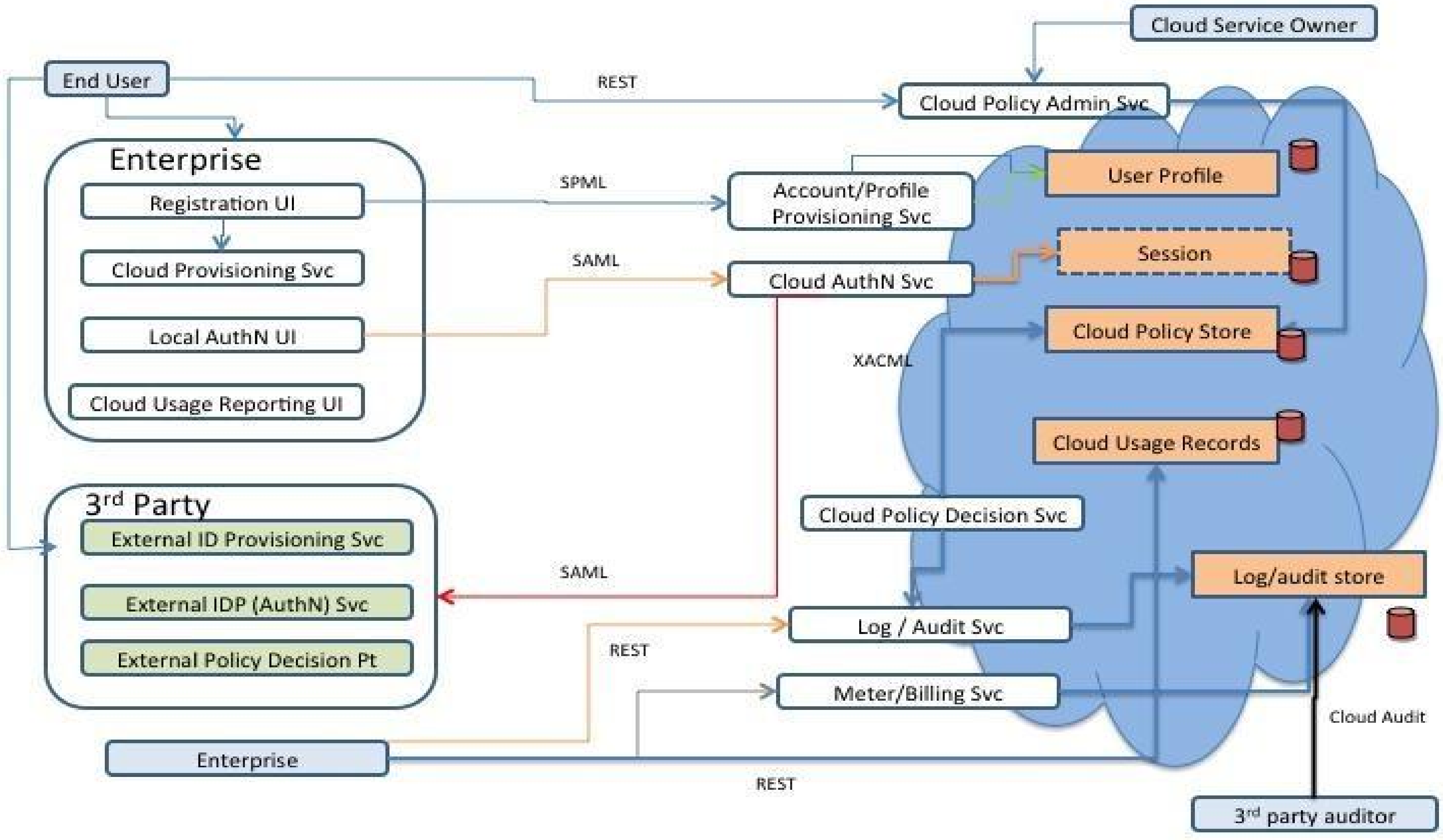
Application Security Services (in-house or cloud service provider)

- Security services such as user identification, authentication, access enforcement, device identification, cryptographic services and key management can be located either with the cloud service provider, within the enterprise data center or some combination of the two.
- The second pattern illustrated below is the identity and access pattern derived from the CSA identity domain.

Cloud Identity/Access Architecture Pattern

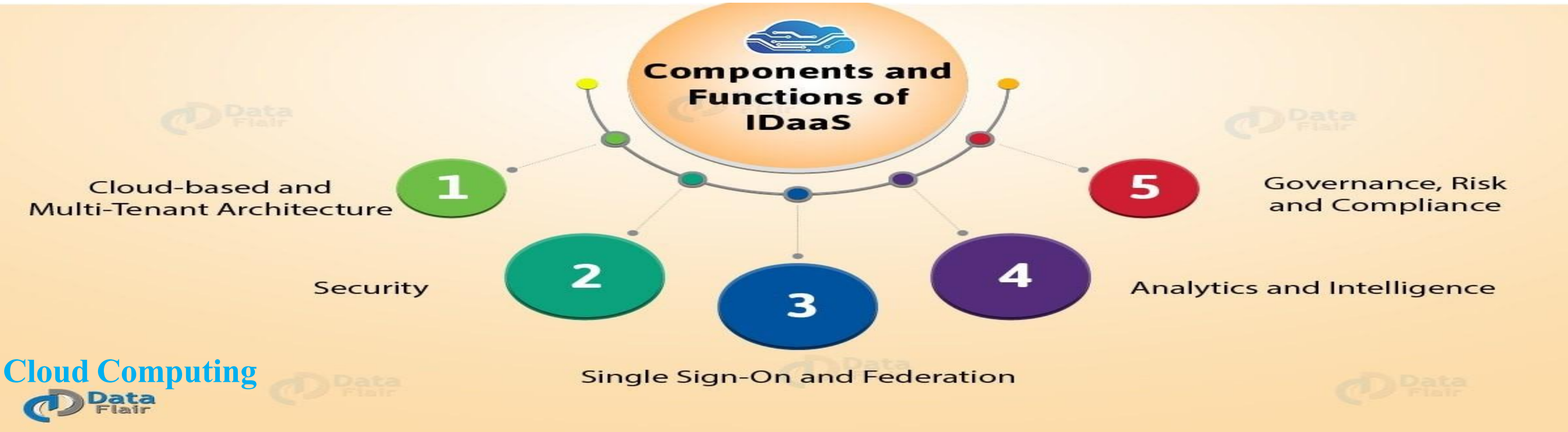


Cloud Identity/Access Architecture Pattern



What is Cloud Identity?

- Cloud Identity is an Identity as a Service (IDaaS) and enterprise mobility management (EMM) product.
- It offers the identity services and endpoint administration. As an administrator, you can use Cloud Identity to manage your users, apps, and devices from a central location.
- Example: G Suite as a stand-alone product with "Identity as a Service" (IDaaS) . As an administrator, you can use Cloud Identity to manage your users, apps, and devices from a central location—the Google Admin console.


Components and Functions of IDaaS
1
Cloud-based and Multi-Tenant Architecture
2
Security
3
Single Sign-On and Federation
4
Analytics and Intelligence
5
Governance, Risk and Compliance
Data Flair

Identity Security services (controls) at cloud service providers

The cloud hosts the following services:

- **Authentication service** that supports user authentication originating from an enterprise portal (Local AuthN UI) and typically delivered using SAML protocol. The authenticated session state is maintained in a cloud session store.
- **Account and profile provisioning service** supports the provisioning of new accounts and user profiles, typically invoked via SPML (Service Provisioning Markup Language) or a cloud service provider specific API. Profiles are stored in the user profile store.
- **Cloud policy admin service** is used for managing policies that dictate which resources in the cloud can be accessed by end users. Using this service, cloud service owners (enterprise) can perform administrative functions and end users can request for access to cloud resources. Cloud policies are stored in the cloud policy store.
- **Logging and auditing service** supports dual functions. The first function is event logging, including security events, in the cloud and the second is for audit purposes. Cloud Audit protocols and APIs can be employed to access this service.
- **Metering service** keeps track of cloud resource usage. Finance departments can use this service for charge-back as well as for billing reconciliation.

Identity as a service (IDaaS)

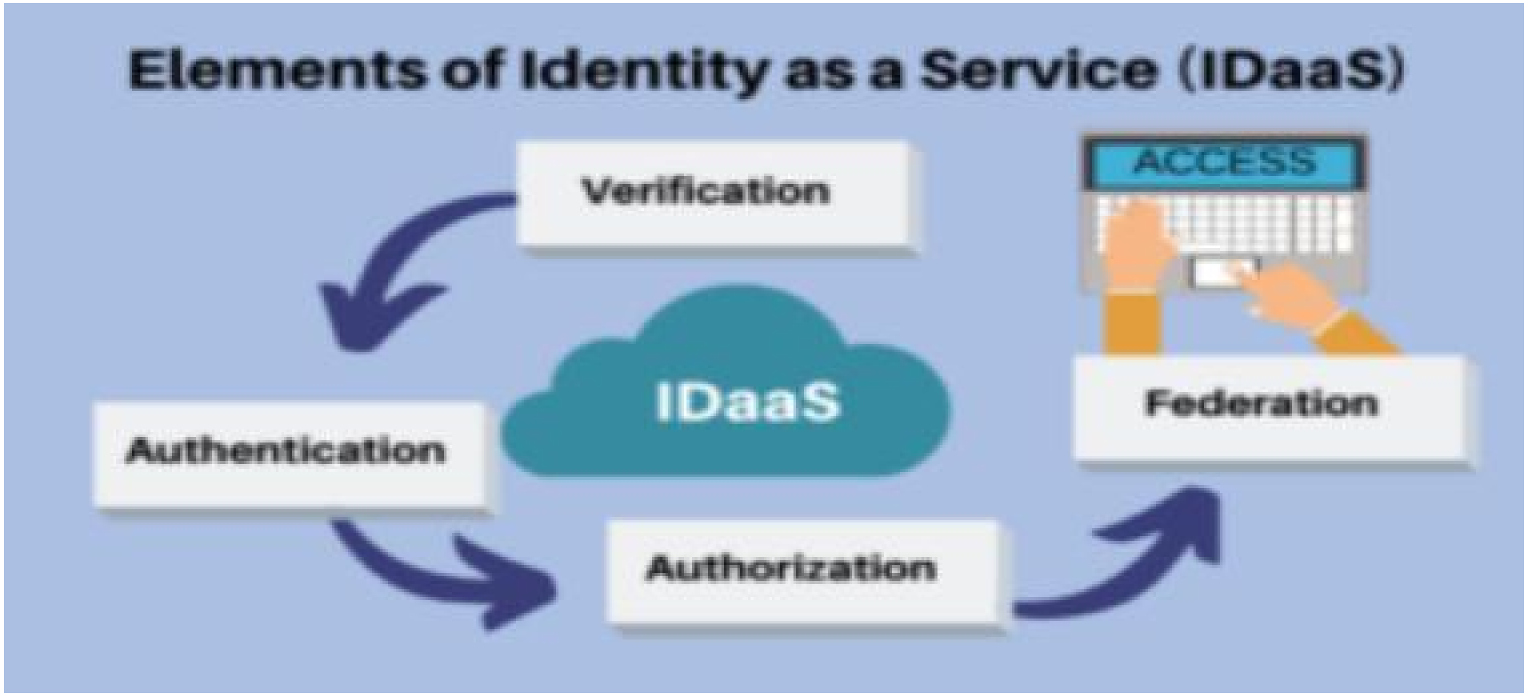
- **Identity as a service (IDaaS)** is a SaaS-based IAM offering that allows organizations to use single sign-on (SSO using SAML or OIDC), authentication and access controls to provide secure access to their growing number of software and SaaS applications.
- Gartner defines IDaaS as, "a predominantly cloud-based service in a multi-tenant or dedicated and hosted delivery model that brokers core identity governance and administration (IGA), access and intelligence functions to target systems on customers' premises and in the cloud."

Gartner states that the core aspects of IDaaS are:

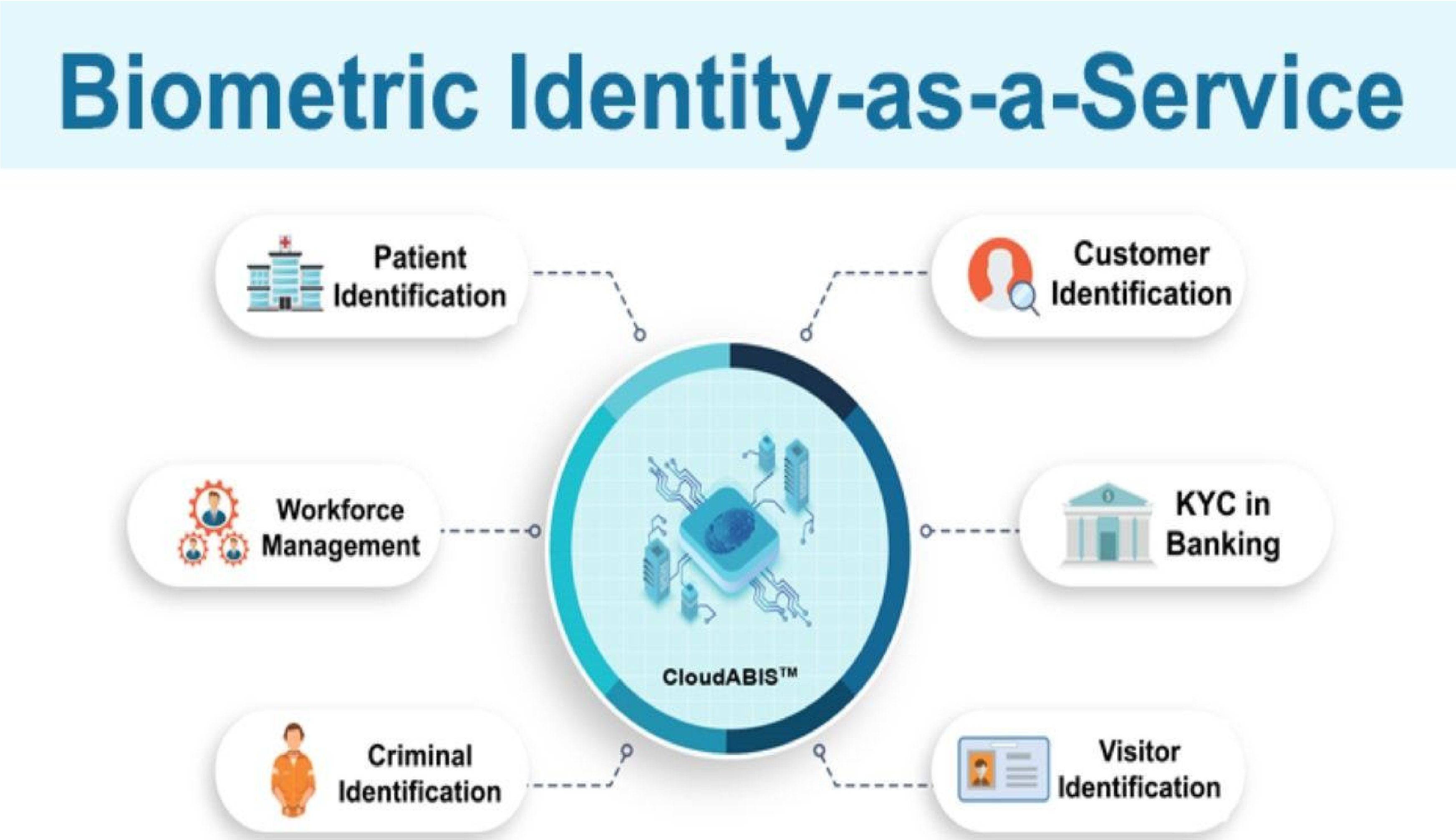
- **IGA:** Provisioning of users to cloud applications and password reset functionality.
- **Access:** User authentication, SSO and authorization supporting federation standards such as SAML.
- **Intelligence:** Identity access log monitoring and reporting

Identity as a service (IDaaS)

IDentity as a service (IDaaS) is an authentication infrastructure [IDA 14] that is built, hosted and managed by a **cloud** provider or a **cloud** broker. IDaaS is based on single sign-on (SSO) authentication and user authorization for access to the **cloud**.



Example:



Biometric Identity-as-a-Service

Cloud security challenges

1. **Visibility into cloud data** — In many cases, cloud services are accessed outside of the corporate network and from devices not managed by IT. This means that the IT team needs the ability to see into the cloud service itself to have full visibility over data, as opposed to traditional means of monitoring network traffic.
2. **Control over cloud data** — In a third-party cloud service provider's environment, IT teams have less access to data than when they controlled servers and applications on their own premises. Cloud customers are given limited control by default, and access to underlying physical infrastructure is unavailable.
3. **Access to cloud data and applications** —Users may access cloud applications and data over the internet, making access controls based on the traditional data center network perimeter no longer effective. User access can be from any location or device, including bring-your-own-device (BYOD) technology. In addition, privileged access by cloud provider personnel could bypass your own security controls.

Cloud security challenges

4. **Compliance** — Use of cloud computing services adds another dimension to regulatory and internal compliance. Your cloud environment may need to adhere to regulatory requirements such as HIPAA, PCI and Sarbanes-Oxley, as well as requirements from internal teams, partners and customers. Cloud provider infrastructure, as well as interfaces between in-house systems and the cloud are also included in compliance and risk management processes.
5. **Cloud-native breaches** – Data breaches in the cloud are unlike on-premises breaches, in that data theft often occurs using native functions of the cloud. A Cloud-native breach is a series of actions by an adversarial actor in which they "land" their attack by exploiting errors or vulnerabilities in a cloud deployment without using malware, "expand" their access through weakly configured or protected interfaces to locate valuable data, and "exfiltrate" that data to their own storage location.

Cloud security challenges

6. **Misconfiguration** – Cloud-native breaches often fall to a cloud customer's responsibility for security, which includes the configuration of the cloud service. Research shows that just 26% of companies can currently audit their IaaS environments for configuration errors. Misconfiguration of IaaS often acts as the front door to a Cloud-native breach, allowing the attacker to successfully land and then move on to expand and exfiltrate data. Research also shows 99% of misconfigurations go unnoticed in IaaS by cloud customers.
7. **Disaster recovery** – Cybersecurity planning is needed to protect the effects of significant negative breaches. A disaster recovery plan includes policies, procedures, and tools designed to enable the recovery of data and allow an organization to continue operations and business.
8. **Insider threats** – A rogue employee is capable of using cloud services to expose an organization to a cybersecurity breach.

Cloud security solutions

Cloud security solutions

Criteria to solve the primary cloud security challenges of visibility and control over cloud data.

[1] **Visibility into cloud data** — A complete view of cloud data requires direct access to the cloud service. Cloud security solutions accomplish this through an application programming interface (API) connection to the cloud service. With an API connection it is possible to view:

- What data is stored in the cloud.
- Who is using cloud data?
- The roles of users with access to cloud data.
- Who cloud users are sharing data with.
- Where cloud data is located.
- Where cloud data is being accessed and downloaded from, including from which device.

Cloud security solutions

[2] **Control over cloud data** — Once you have visibility into cloud data, apply the controls that best suit your organization. These controls include:

- **Data classification** — Classify data on multiple levels, such as sensitive, regulated, or public, as it is created in the cloud. Once classified, data can be stopped from entering or leaving the cloud service.
- **Data Loss Prevention (DLP)** — Implement a cloud DLP solution to protect data from unauthorized access and automatically disable access and transport of data when suspicious activity is detected.
- **Collaboration controls** — Manage controls within the cloud service, such as downgrading file and folder permissions for specified users to editor or viewer, removing permissions, and revoking shared links.
- **Encryption** — Cloud data encryption can be used to prevent unauthorized access to data, even if that data is exfiltrated or stolen.

Cloud security solutions

3 **Access to cloud data and applications**— As with in-house security, access control is a vital component of cloud security. Typical controls include:

- **User access control** — Implement system and application access controls that ensure only authorized users access cloud data and applications. A Cloud Access Security Broker (CASB) can be used to enforce access controls
- **Device access control** — Block access when a personal, unauthorized device tries to access cloud data.
- **Malicious behavior identification** — Detect compromised accounts and insider threats with user behavior analytics (UBA) so that malicious data exfiltration does not occur.
- **Malware prevention** — Prevent malware from entering cloud services using techniques such as file-scanning, application whitelisting, machine learning-based malware detection, and network traffic analysis.
- **Privileged access** — Identify all possible forms of access that privileged accounts may have to your data and applications, and put in place controls to mitigate exposure.

Cloud security solutions

4 **Compliance** — Existing compliance requirements and practices should be augmented to include data and applications residing in the cloud.

- **Risk assessment** — Review and update risk assessments to include cloud services. Identify and address risk factors introduced by cloud environments and providers. Risk databases for cloud providers are available to expedite the assessment process.
- **Compliance Assessments** — Review and update compliance assessments for PCI, HIPAA, Sarbanes-Oxley and other application regulatory requirements.

Cloud Security Gateway (CSG)

Cloud Security Gateway (CSG)

- Cloud security gateways (CSGs), also known as **cloud access security brokers (CASB)**, are on-premises or cloud-hosted security software that act as a policy enforcement point between an enterprise and cloud applications that employees use.
- CSGs provide IT security teams visibility into cloud service usage and cloud-centric security capabilities that mirror the controls enterprises deployed to protect their data in on-premises applications including data loss prevention, user and entity behavior analytics (UEBA), encryption, access control, and more.

Key Requirements of Cloud Security Gateways

1. Visibility:

- While cloud adoption continues to rise, enterprises are finding that simply blocking cloud services from being used isn’t sufficient. With the explosive growth of available cloud services, when an organization blocks one cloud service, employees frequently respond by seeking out lesser-known, potentially riskier alternatives that can end up exacerbating the problem.
- And while the IT department may have visibility into sanctioned/permitted cloud services, they lack the needed visibility into the scope of shadow IT cloud service use. They often do not know, for example, who is using which cloud services, what kind of data is going to each cloud service in use, with whom that data is being shared with, and which devices are accessing it and from where.
- These organizations turn to CSGs to solve this problem. CSGs provide continuous visibility into both sanctioned and unsanctioned (shadow IT) cloud usage. This visibility extends to the data retention policies of each unsanctioned cloud service, how much data is being uploaded/downloaded to a cloud service, whether the service provider can encrypt data at rest or in transit, and an overall security risk score for each cloud service in use. Enterprises use the cloud service risk score to evaluate and select cloud services that meet their security and compliance requirements, thereby streamlining the process of cloud service adoption.

Key Requirements of Cloud Security Gateways

2. Compliance

- Employees routinely upload sensitive and regulated data to the cloud. In the past, organizations relied on on-premises data loss prevention (DLP) solutions to protect that data from leakage via email and ensure they remained compliant with internal policies and external regulations. CSGs extend these on-premises DLP controls to the cloud so that enterprises can prevent certain types of sensitive data from being uploaded to high-risk cloud services or being shared from trusted cloud services to third parties.
- CSGs also provide a unified, cross-cloud DLP policy engine, incident reporting, and remediation workflow that ensure a consistent set of controls across cloud services. The cloud DLP capabilities of CSG can protect a broad range of sensitive and regulated data including payment card data (PCI-DSS), protected health information (HIPAA-HITECH), intellectual property, and personally identifiable information.

Key Requirements of Cloud Security Gateways

3. Threat Protection

- One of the core capabilities of a CSG is threat protection. This capability is essential because cloud usage occurs outside the scope of conventional enterprise threat protection solutions, such as intrusion prevention solutions (IPS) and security information and event management (SIEM) systems. Additionally, the rise of social engineering and the resulting compromised accounts have become one of the leading causes of security failures.
- CSGs analyze cross-cloud user behavior patterns to identify both malicious and negligent insider threats, as well as external threats such as compromised accounts. Effective threat protection uses machine learning to build behavior models for all employees and create baselines for each. Any activity that deviates from this baseline is then flagged as a threat if it reaches a certain threshold.
- There are four primary CSG deployment modes that provide coverage for different users, devices, and access scenarios:
- **Log collection** – consuming event logs from existing infrastructure such as firewalls, secure web gateways, and SIEMs.
- **Forward Proxy** – inline deployment between the endpoint and cloud service in which the device or network routes traffic to the CSG proxy.
- **Reverse proxy** – inline deployment between the endpoint and cloud service in which the cloud service or identity provider routes traffic to the CSG proxy.
- **API** – direct integration of the CSG and cloud service. Depending on cloud provider APIs, the CSG can view activity, content, and take enforcement action.

Key Requirements of Cloud Security Gateways

4. Data Security

- As enterprise data is transferred to the cloud and employees access data from off-network locations and unmanaged devices, they circumvent existing security technologies. CSGs provide an additional layer of security such as encryption, access control, etc.
- Mature CSGs can provide end-to-end structured and unstructured data encryption to data being uploaded to a cloud service and data already in a cloud service. These solutions also allow the enterprise to control the encryption keys used to protect data in the cloud and integrate with KMIP-compliant key management solutions to broker the use of enterprise keys.

References

- https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html
- https://www.akamai.com/us/en/resources/data-security-in-cloud-computing.jsp
- https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-18762013000300005
- https://www.mcafee.com/enterprise/en-us/security-awareness/cloud.html
- https://www.infoq.com/articles/cloud-security-architecture-intro/
- https://www.techrepublic.com/article/how-to-prevent-the-top-11-threats-in-cloud-computing/