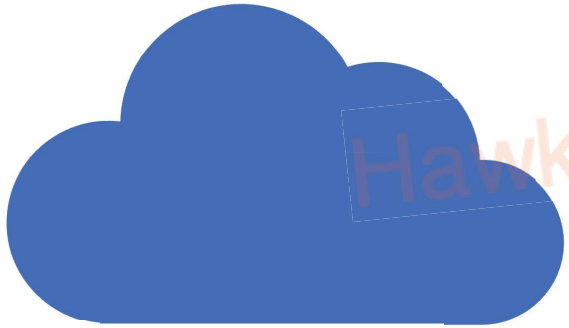
AZ-900: Microsoft Azure Fundamentals

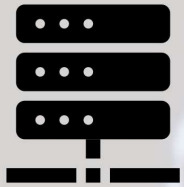


Exam Syllabus

- Describe Cloud Concepts (25-30%)
- Describe Azure Architecture and Services (35-40%)
- Describe Azure Management and Governance (30-35%)

What is Cloud Computing?

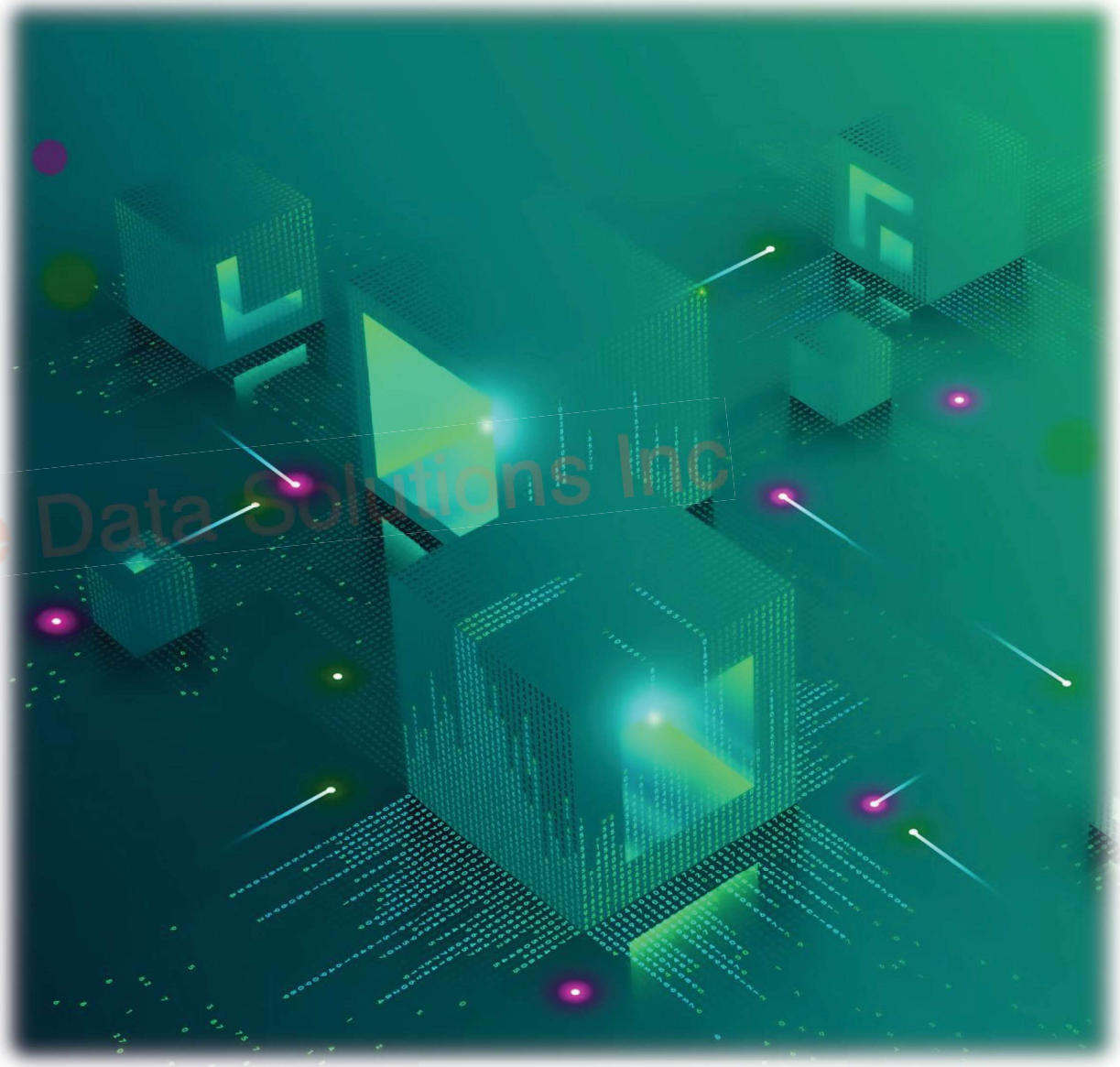
- Cloud Computing is the on-demand delivery of IT resources over the internet.
- In essence, instead of buying physical infrastructure like servers, computers, managing a physical area to protect & manage this infrastructure – we simply rent & access these.
- Examples of IT Resources are Virtual Machines, Databases, Networking. The cloud services go one step beyond and include Internet of Things (IoT), Machine Learning (ML) and Artificial Intelligence (AI).

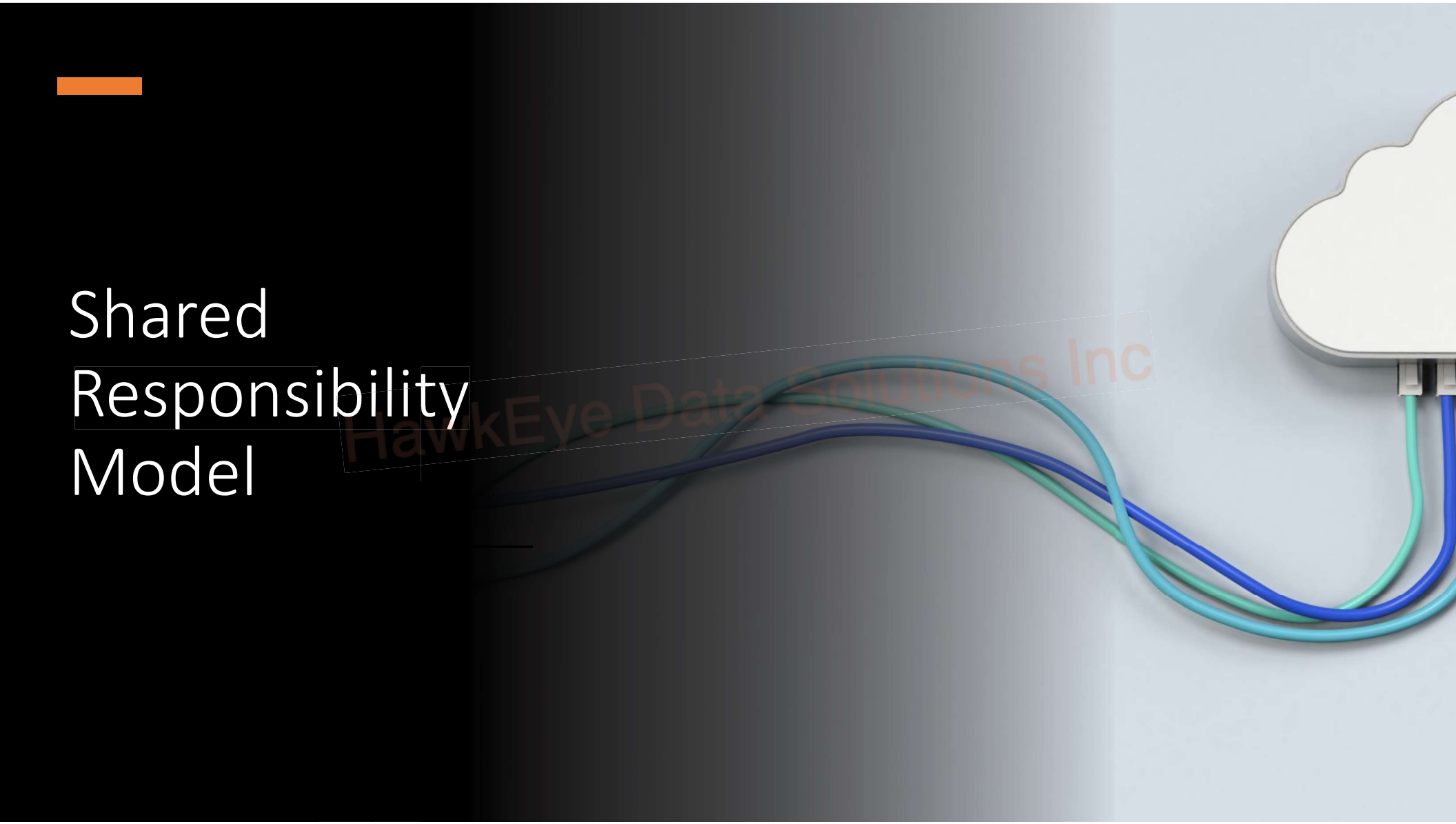

- Using someone else's infrastructure. They have the headache of managing and maintaining it.

- The power to deploy databases, virtual machines, networks etc. at the click of a button!

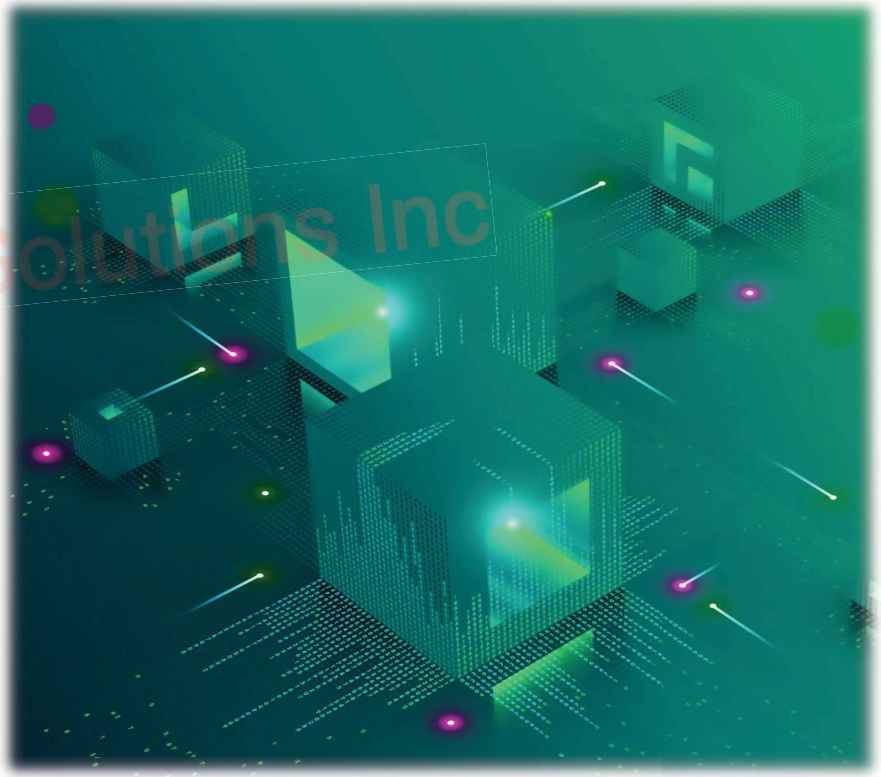
- You lower your upfront costs, the infrastructure runs more efficiently, and can scale as per your need!



Shared Responsibility Model



The Shared Responsibility Model outlines the division of security tasks and obligations between cloud service providers (CSPs) and cloud users.



As more organizations move their operations to the cloud, this model clarifies who is responsible for securing various layers of the infrastructure, ensuring a secure environment for data and applications.

- Information and Data
- Devices (Mobile & PC)
- Accounts & Identities
- Identity and Directory Infrastructure
- Applications
- Network Controls
- Operating System
- Physical Hosts
- Physical Network
- Physical Datacenter

On – Prem?

EVERYTHING!

Cloud Service Provider (CSP)

- **Physical Security:** Cloud providers are responsible for securing their data centers, including physical access controls, surveillance, and environmental protections.
- **Network Infrastructure:** The underlying network infrastructure, such as routers and switches, is managed and secured by the CSP.
- **Host Infrastructure:** The security of the physical servers and the virtualization layer is maintained by the provider.
- **Foundational Services:** Core services like computing, storage, and database management systems are managed and secured by the CSP.

Consumer

Data Security: Users are responsible for securing their own data, including encryption, access controls, and data classification.

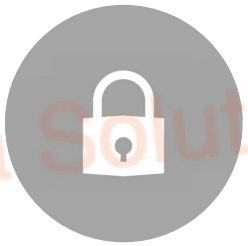
Application Security: Security measures for applications, including vulnerability management and secure coding practices, are the user's responsibility.

Identity and Access Management (IAM): Users must manage user access, permissions, and authentication to their applications and services.

Configuration Management: Users are responsible for configuring their applications and services securely to prevent misconfigurations.

Importance of the Model:

Clarity: It eliminates confusion by clearly defining the security responsibilities of both the CSP and the user.



Security: It ensures a holistic security approach, with both parties contributing to overall security.

Collaboration: Collaboration between the CSP and users is essential to create a secure environment.

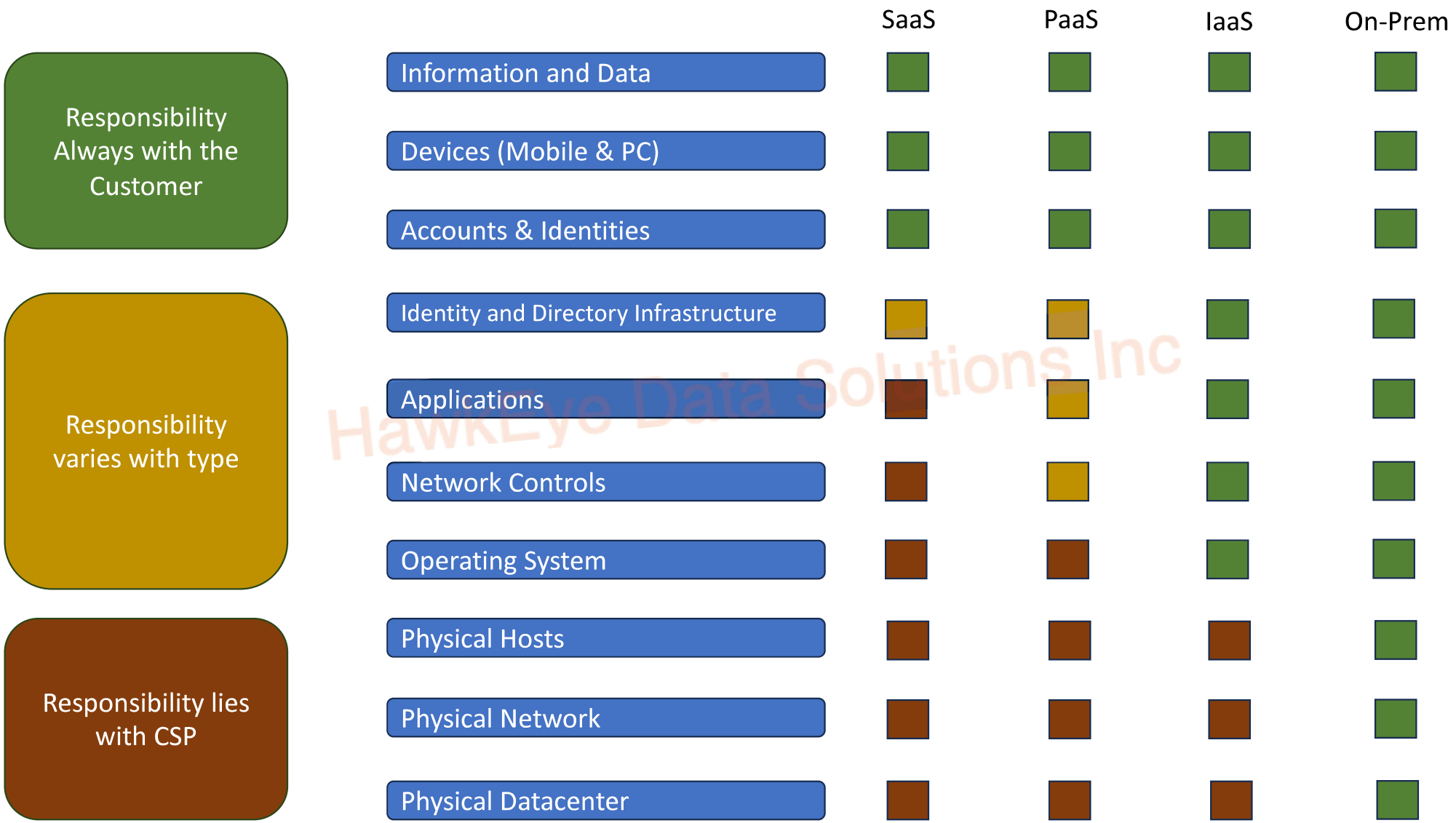
Customization: Users can implement security measures tailored to their specific needs and applications.

Cloud Service Types

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service(SaaS)



Infrastructure as a Service (IaaS)

The most flexible category that gives you maximum control over your cloud resources.

The CSP is responsible for physical security, connectivity to internet, and the hardware only – you control everything else.

Use Cases: Development and Testing Environments. Hosting Web Applications, Lift & Shift migrations

Platform as a Service (PaaS)

A middle ground between IaaS and SaaS.

The responsibility is split between you and the cloud provider.

Allows you to focus more on development & go-live than patching & maintaining infrastructure.

Think of it like a company PC – Hardware, OS, patches, databases maintained by IT support.

Excellent for development frameworks and analytics!

Software as a Service (SaaS)

The most complete cloud service model, but least flexibility.

However, it's the easiest to deploy, use, and go-live : almost like a ready-made app.

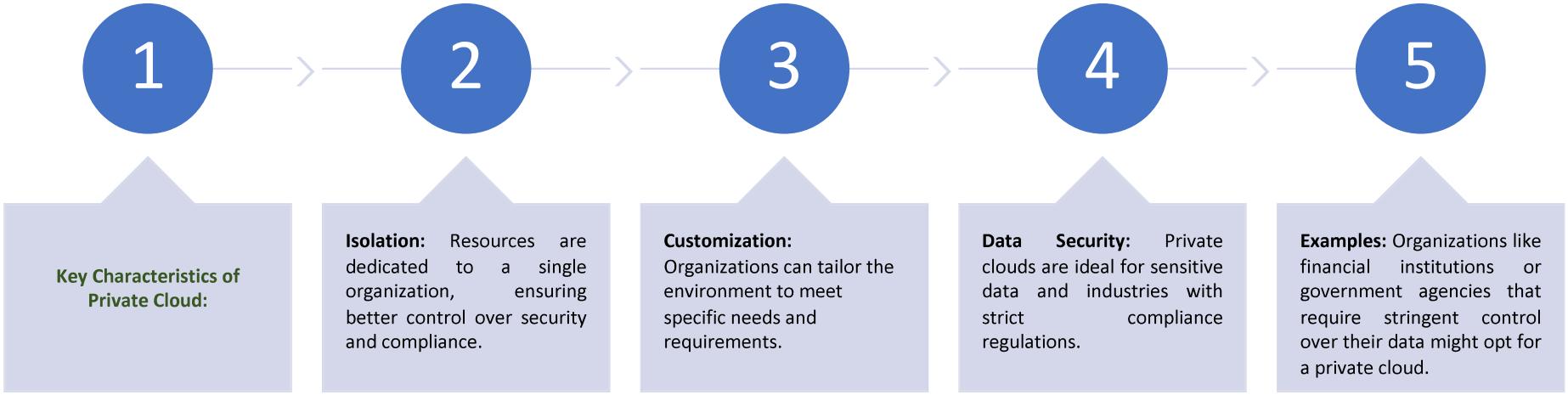
Most of the responsibility is placed on the CSP, you are responsible for the data, applications & who has access.

Examples - Email, Microsoft 365, iCloud.

Define Cloud Models

Private Cloud

- A **private cloud** is a cloud infrastructure operated solely for a single organization. It can be hosted internally or by a third-party provider. This model provides enhanced control and security for organizations that require a dedicated environment.
- However, it has fewer of the benefits of a public cloud deployment and higher costs associated to it as well.



Define Cloud Models

Public Cloud

- The **public cloud** is a cloud computing model where cloud services are owned and provided by third-party vendors over the internet. These services are available to anyone who wants to use them, making it a versatile and cost-effective option for various purposes. With a public cloud, all hardware, software, and other supporting infrastructure are owned and managed by the cloud provider.
- In a public cloud, you share the same hardware, storage, and network devices with other organizations or cloud "tenants," and you access services and manage your account using a web browser.
- General public availability is a key difference between public and private clouds.

1

Key Characteristics of Public Cloud:

2

Shared Infrastructure: Resources are shared among multiple users and organizations, optimizing utilization and cost.

3

Cost Efficiency: Users only pay for the resources they consume, eliminating the need for upfront investments.

4

Scalability: Public cloud services can easily scale up or down to accommodate changing demands.

5

Examples: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) etc.

Define Cloud Models

Hybrid Cloud

- A **hybrid cloud** is a combination of public and private clouds, designed to allow data and applications to be shared between them. This model offers flexibility and allows organizations to balance the benefits of both public and private environments.
- For many organizations, a hybrid cloud approach is a MUST due to regulatory and data sovereignty requirements, tackling low latency issues etc.
- Simply put – A private deployment can be used for the extra layer of security, and it can be coupled with a public deployment to handle surge in traffic / computing needs!

1

Key Characteristics of Hybrid Cloud:

2

Flexibility: Organizations can choose where to host different workloads based on factors like security, performance, and cost.

3

Scalability: Hybrid clouds can handle spikes in demand by utilizing resources from both environments.

4

Data Mobility: Data can be moved seamlessly between private and public clouds as needed.

5

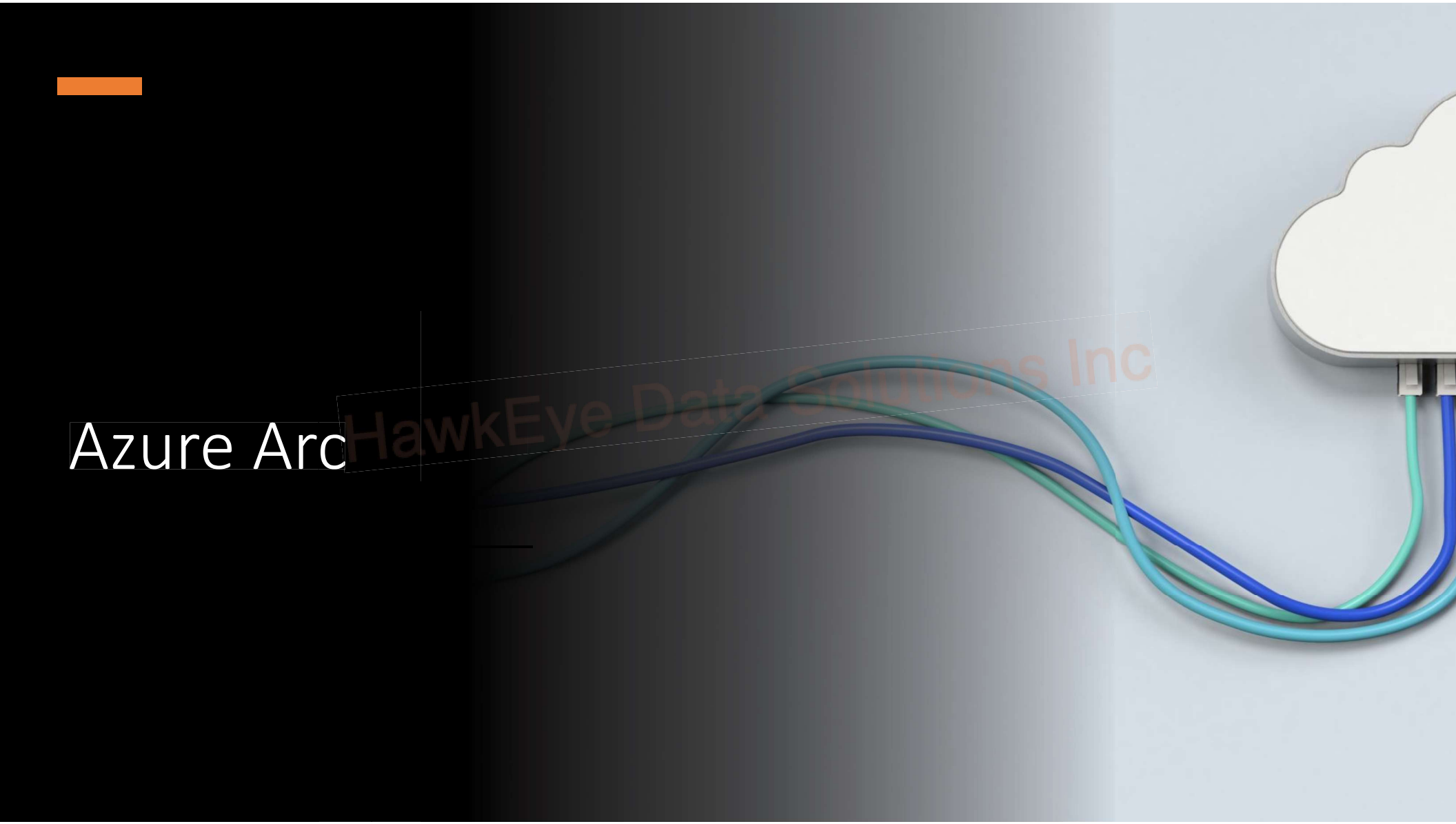
Examples: Healthcare organizations might use a private cloud for patient data storage while using a public cloud for non-sensitive applications.

Define Cloud Models

Multi Cloud

- Slowly becoming more and more popular!
- In this kind of a deployment, you utilize multiple Public Cloud Providers.
- Possible reasons are that your organization doesn't solely want to reply on one CSP only.
- Your organization started with one CSP but now wants to fully migrate to another CSP.
- Your organization wants to utilize services / tools from different CSP's.

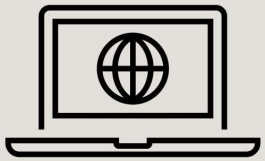
Azure Arc



Azure Arc

- Organizations are expanding their digital footprint across on-premises, multi-cloud, and edge environments - managing and securing resources can become complex.
- Azure Arc is a powerful solution, empowering organizations to streamline operations and governance across a variety of environments.
- Azure Arc allows us to extend Azure's management and governance features to resources beyond Azure's boundaries.
- It enables organizations to manage, secure, and monitor resources spread across on-premises, multi-cloud, and edge environments, all through the familiar Azure interface.

Azure Arc: Benefits



1. **Resource Management:** Azure Arc allows you to connect and manage resources, including virtual machines, Kubernetes clusters, and databases, as if they were native Azure resources.

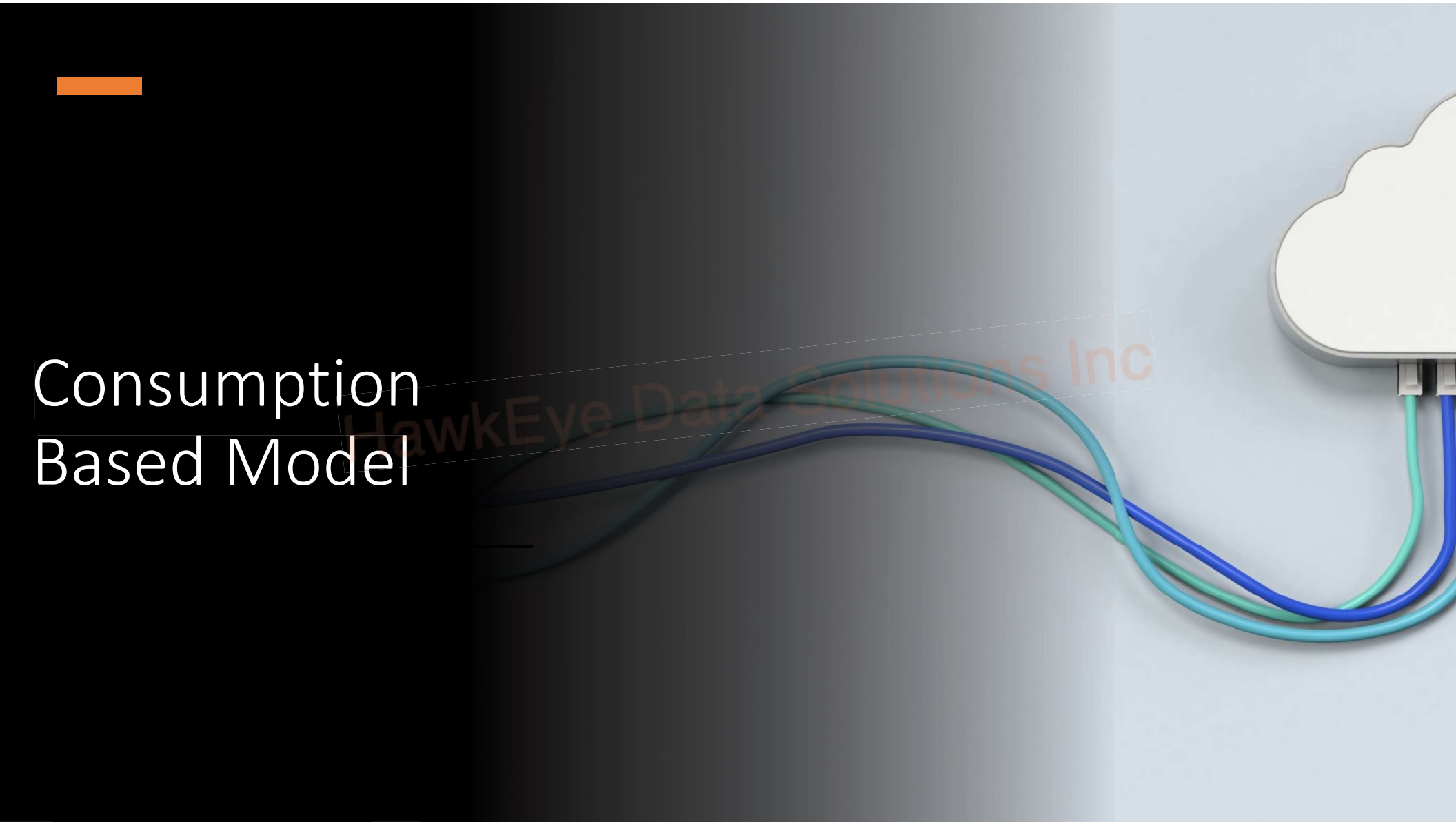
2. **Unified Management:** With a consistent Azure interface, you can apply policies, configure settings, and monitor the health of resources across various environments.

3. **Governance and Compliance:** Azure Policy and Azure Security Center can be used to enforce consistent governance and compliance policies across hybrid environments.

4. **Automation and DevOps:** Azure Arc integrates with Azure Resource Manager templates, enabling consistent resource provisioning and management using infrastructure as code.

5. **Data Services:** You can deploy Azure data services like Azure SQL Database and Azure Database for PostgreSQL Hyperscale to your preferred environment.

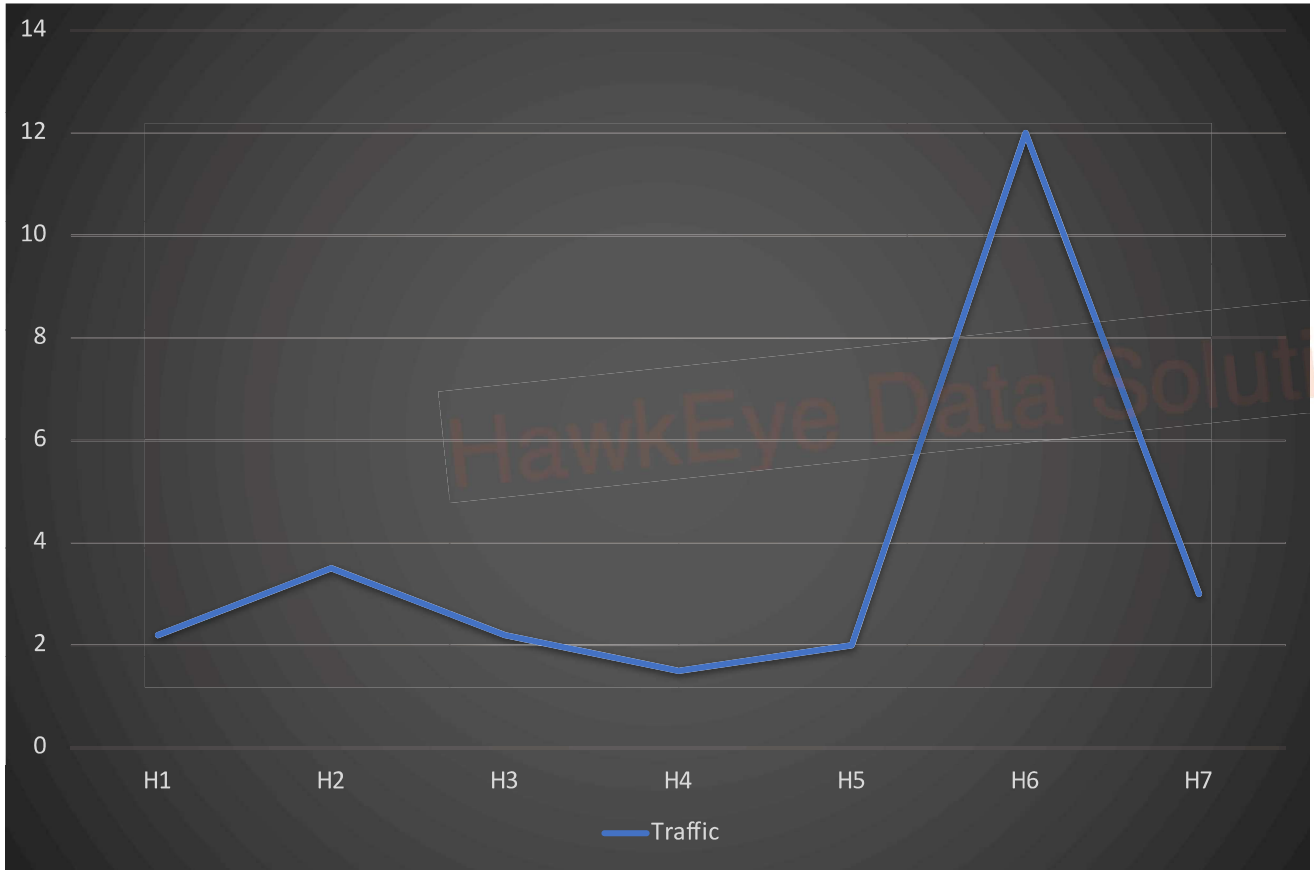
Consumption Based Model



CapEx (Capital Expenditure)

- Usually, a one-time up-front expense to purchase assets. Eg - Physical hardware, software licenses, and infrastructure to establish an on-premises data center.

- These expenditures are characterized by their long-term nature and are considered traditional IT investments.



CapEx (Capital Expenditure) : Problem

- How much hardware should we buy? (We cannot predict the future).

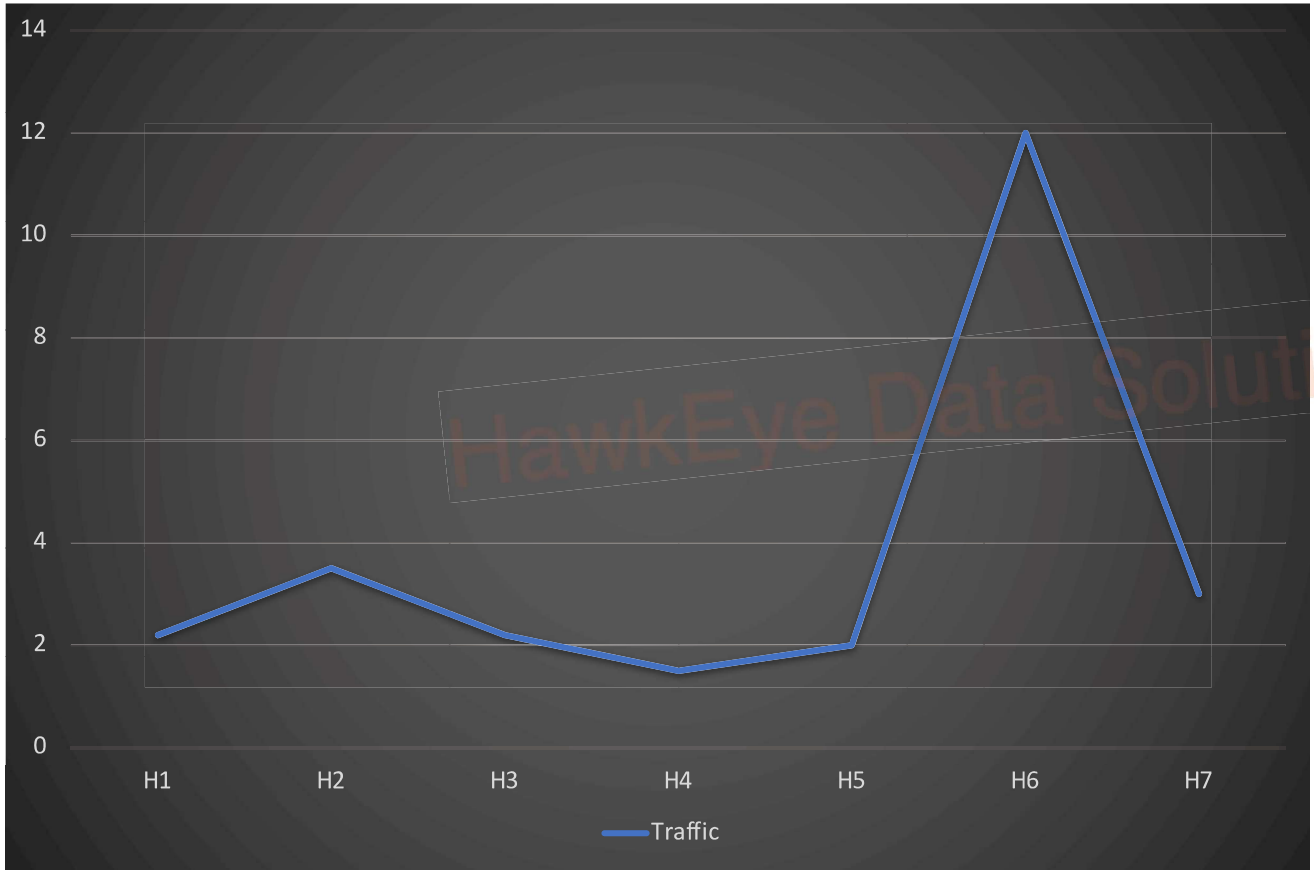
- If less hardware -> the application fails.
- If more hardware -> Unnecessary spending.
- You may not have enough capital available upfront!

OpEx (Operational Expenditure)

- Operating Expenditures (OpEx) in cloud computing refer to ongoing operational expenses incurred while using cloud services.
- Expenses are more flexible and aligned with the pay-as-you-go model of the cloud.
- Cloud Computing falls under OpEx – you don’t pay for any physical hardware, rent - only consumption!

OpEx (Operational Expenditure) Benefits

- ✓ 0 upfront costs!
- ✓ No need to manage costly and complex hardware.
- ✓ Pay more when you need more resources.
- ✓ Pay less when you need less resources.
- ✓ No need to estimate your future needs – scale as per demand and pay accordingly.

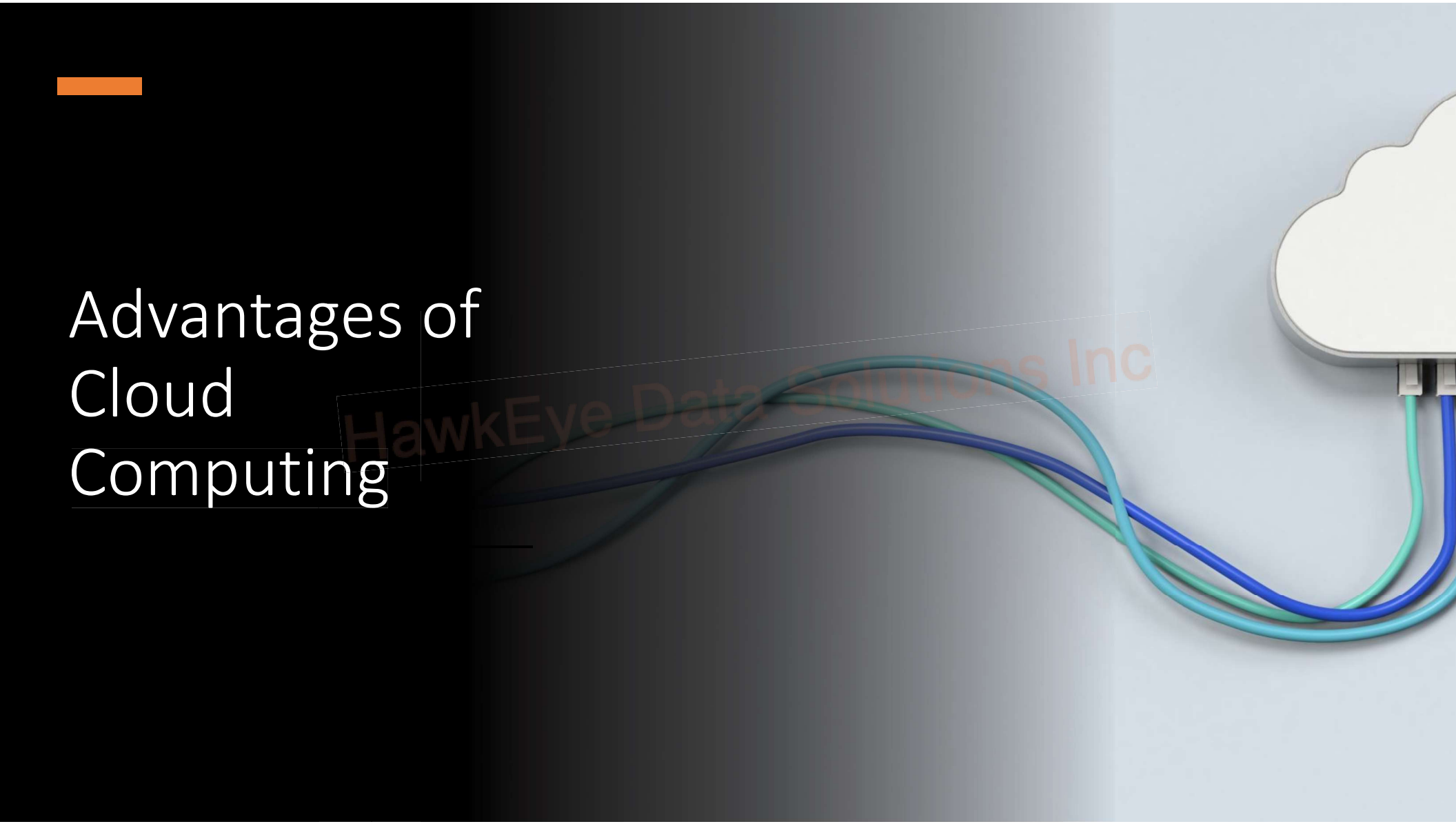


OpEx

- How much hardware should we buy? (We cannot predict the future). Now we don't need to worry.

- If less hardware -> we use less resources & pay less.
- If more hardware -> we use more resources & pay more.
- Evens out / averages over the long term & way more cost effective!

Advantages of Cloud Computing



Scalability

The ability to adjust resources to meet demand.

Peak traffic? Add more resources.

Less traffic? Shut down resources.

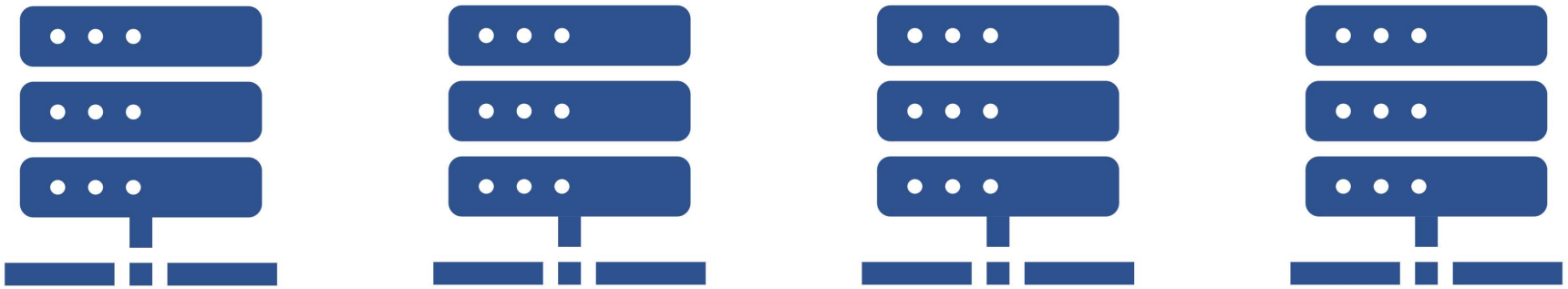
You ONLY pay for what you use.

Vertical Scaling / Scaling Up

- Vertical scaling involves increasing the capacity of existing nodes/machines.
- For example, if a server requires more processing power, vertical scaling involves upgrading the CPUs. Similarly, storage space can also be dynamically upgraded or degraded!

Horizontal Scaling / Scaling Out

- When you need to handle new demands, horizontal scaling (also known as scaling out) involves adding more nodes or machines to your infrastructure.
- For instance, if an application hosted on a server is struggling to manage traffic due to a lack of capacity or capability, the solution may be to add another server.



Reliability

The ability of a system/service to recover from failure & continue its operation.

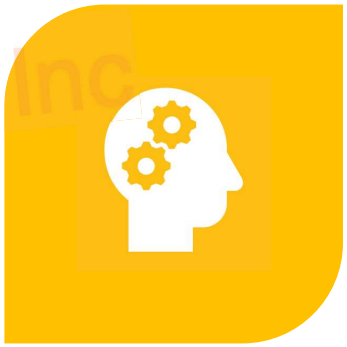
Azure has a decentralized design – no single point of failure + data centers worldwide!

Ability to quickly switch to a different data center or region.

Predictability

Focused on performance or cost.

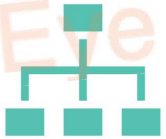
A well architected solution helps us move forward with confidence and avoid surprises.



SLA’s and cost management play a big role.

Predictability: Performance

Focuses on the resources needed to deliver a seamless experience.



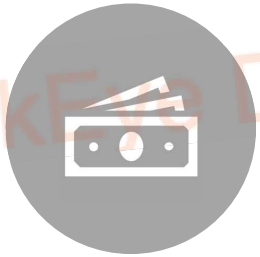
Imp. concepts – Auto-Scaling, Load Balancing, High Availability.

Auto scaling helps add / remove resources based on demand.

Load Balancing allows to distribute load evenly on not on just a few resources.

Predictability: Cost

We want visibility on our spends & not a huge bill out of the blue.



Track and control spends, apply tight budgets.

Analyze the data to optimize spending.

Tools like pricing calculator to estimate cloud spends.

Security in the Cloud

Data Protection

Encryption and access controls safeguard sensitive data.

Prevent unauthorized access and data breaches.

Threat Detection

Advanced security tools monitor for unusual activities.

Prompt detection and mitigation of potential threats.

Regulatory Compliance

Meeting industry regulations and compliance standards.

Auditable security practices ensure adherence.

Enhanced Data Privacy

Builds customer trust through responsible data handling.

Adheres to legal and regulatory data protection requirements.

Security in the Cloud

Cost Control

Optimizes resource utilization to prevent overprovisioning.

Reduces unnecessary expenses through efficient management.

Resource Management

Allocates resources based on business priorities.

Ensures efficient resource utilization across the cloud environment.

Risk Mitigation

Consistent policies reduce operational risks and vulnerabilities.

Establishes controls to prevent potential security breaches.

Agility and Innovation

Streamlines deployment processes through governance frameworks.

Encourages innovation with the confidence of established security and governance.

Manageability

Manageability of the cloud

Manageability in the cloud