Navigating Shared Responsibilities in the Cloud

An overview of cloud security responsibilities and best practices for businesses to enhance governance, reduce risks, and ensure compliance.

Foundations of Managed Services

Automated Security

Managed services provide proactive security measures, such as vulnerability scanning, threat detection, and automated remediation, to protect cloud environments.

Continuous Monitoring

Managed services offer real-time monitoring of cloud resources, providing alerts and insights to help organizations maintain the health and performance of their cloud infrastructure.

Compliance Assurance

Managed services help organizations meet regulatory and industry-specific compliance requirements by automating processes, generating audit reports, and ensuring adherence to policies.

By leveraging managed services, organizations can enhance their cloud security, streamline monitoring, and ensure compliance, allowing them to focus on their core business objectives.

Foundations of Managed Services

- **Outsourced IT Management**

  Cloud providers handle infrastructure, security, and operations, reducing operational overhead for the customer.

- **Automation & Monitoring**

  Continuous monitoring of cloud resources using AI/ML, ensuring optimal performance and security.

- **Scalability & Availability**

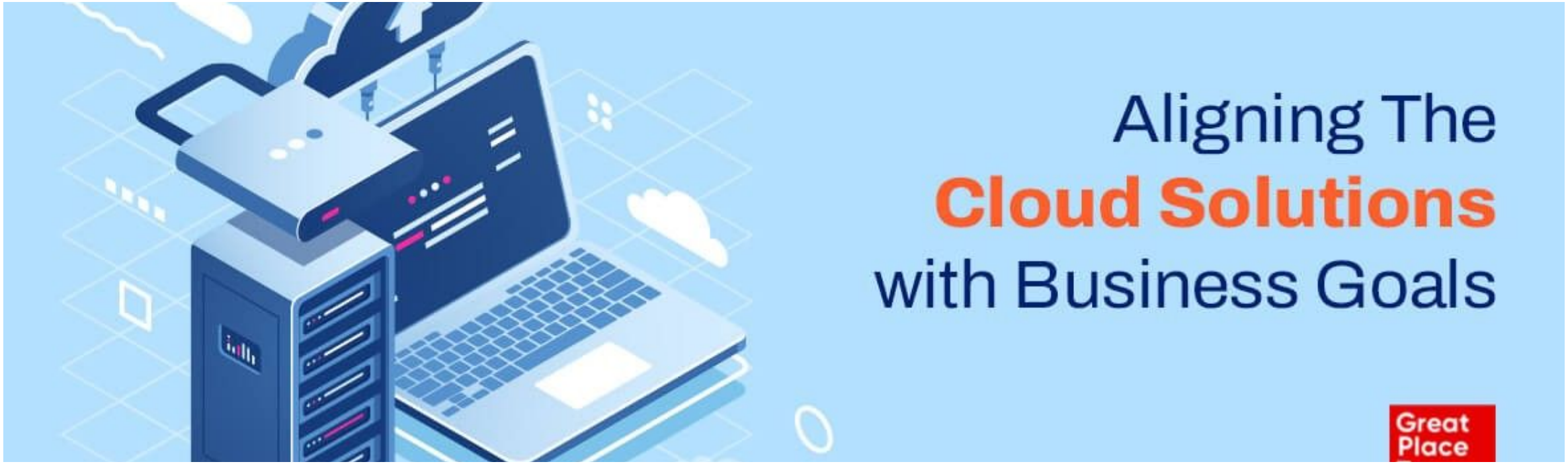
  Ensures high availability, backup, and disaster recovery, allowing businesses to scale up or down as needed.

- **Cost Efficiency**

  Pay-as-you-go pricing models minimize upfront investments, allowing businesses to scale cost-effectively.

- **Common Cloud Managed Services**

  Includes compute management, database services, security & compliance, networking & load balancing, and backup & disaster recovery.



Aligning Business Requirements

To ensure the success of managed cloud services, it is crucial to align business requirements with key SLA guarantees, compliance mandates, and scalability needs. This comprehensive approach enables organizations to maintain consistent service levels, adhere to regulatory standards, and scale their operations seamlessly.

Business Requirements

Security & Compliance

Ensure alignment with industry standards such as ISO 27001, GDPR, HIPAA, and SOC 2 to meet regulatory requirements.

Service Uptime & Availability

Meet or exceed Service Level Agreement (SLA) guarantees, such as 99.99% uptime, to ensure reliable and uninterrupted service.

Scalability & Performance

Provide dynamic resource allocation capabilities to support the growing and changing needs of the business.

Data Residency & Sovereignty

Offer options for regional data storage to comply with data privacy and sovereignty requirements.

Integration & Interoperability

Ensure seamless integration and interoperability with existing business applications and third-party systems.

Business Requirements: The Cloud Provider Perspective.

1- Cloud Provider Responsibilities: The Physical Plant.
a- Secure Hardware Components.
b- Manage Hardware Configurations
c- Set Hardware to Log Events & Incidents.
2- Cloud Provider Responsibilities: Secure Logical Framework.
a- Installation of Virtual OSs.
b- Secure Configuration of Various Virtualized Elements.
3- Cloud Provider Responsibilities: Secure Networking.
a- Firewalls.
b- IDS/IPS.
c- Honeypots.
d- Vulnerability Assessment.
e- Communication Protection.

Shared Responsibilities by Service Type

IaaS Responsibilities

In the IaaS model, the cloud provider is responsible for managing the physical data centers, networking, and hypervisors, while the customer is responsible for configuring firewalls, storage, and identity and access management (IAM). Best practice: Implement network segmentation, encryption, and secure access policies.

PaaS Responsibilities

In the PaaS model, the cloud provider manages the operating system, runtime, and middleware, while the customer is responsible for securing the applications and APIs. Best practice: Use secure coding practices and API security controls.

SaaS Responsibilities

In the SaaS model, the cloud provider manages the entire application stack, including the infrastructure and application security. The customer is responsible for configuring user access and authentication (such as MFA and SSO) and defining data retention policies and encryption. Best practice: Implement Zero Trust security, MFA, and data loss prevention (DLP).

Shared OS & Middleware Administration

Establish Baseline Configurations

Implement strong, secure baseline configurations for operating systems and middleware to establish a consistent security posture across the environment.

Patching & Updates

Develop and maintain comprehensive patching policies to ensure timely application of security updates and bug fixes for all OS and middleware components.

Configuration Management

Leverage configuration management tools and processes to automate the deployment and enforcement of approved configurations, reducing the risk of drift and vulnerabilities.

Continuous Monitoring

Implement continuous monitoring capabilities to detect and respond to any deviations from the established baseline configurations or unauthorized changes.

Shared Responsibilities

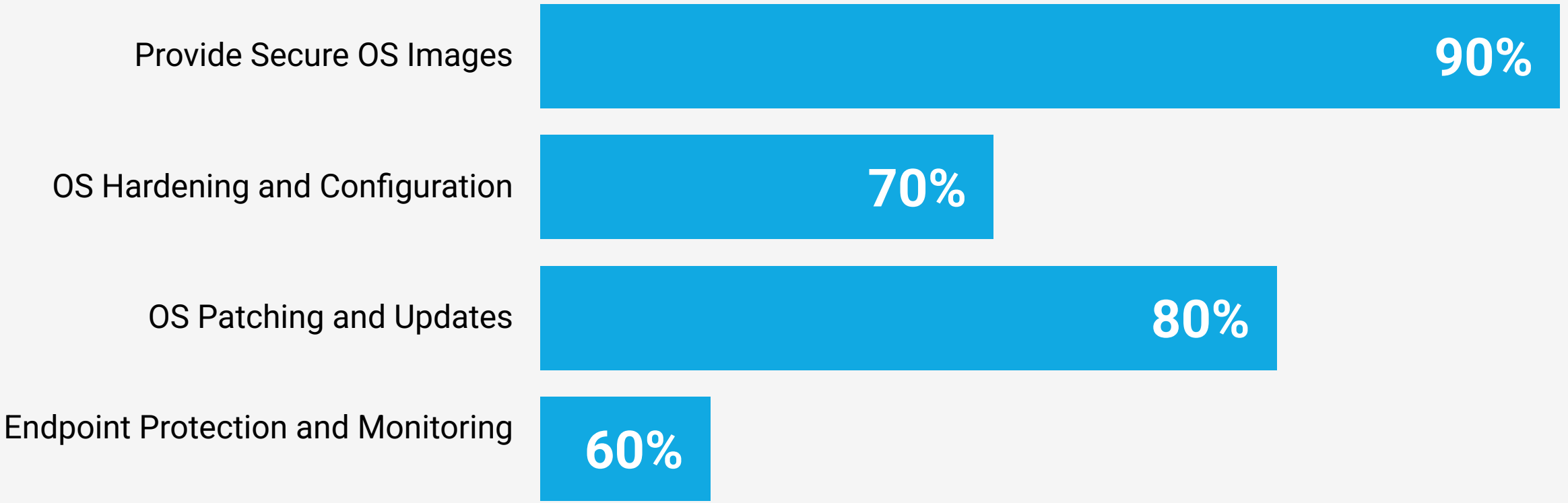
Clearly define the shared responsibilities between the cloud provider and the customer for OS and middleware administration to ensure comprehensive coverage and accountability.

Validation & Auditing

Regularly validate the security posture and conduct audits to ensure compliance with the established policies and security best practices.

Shared Administration of OS, Middleware, or Applications

Comparison of responsibilities between Cloud Providers and Customers (100% = Full Responsibility)

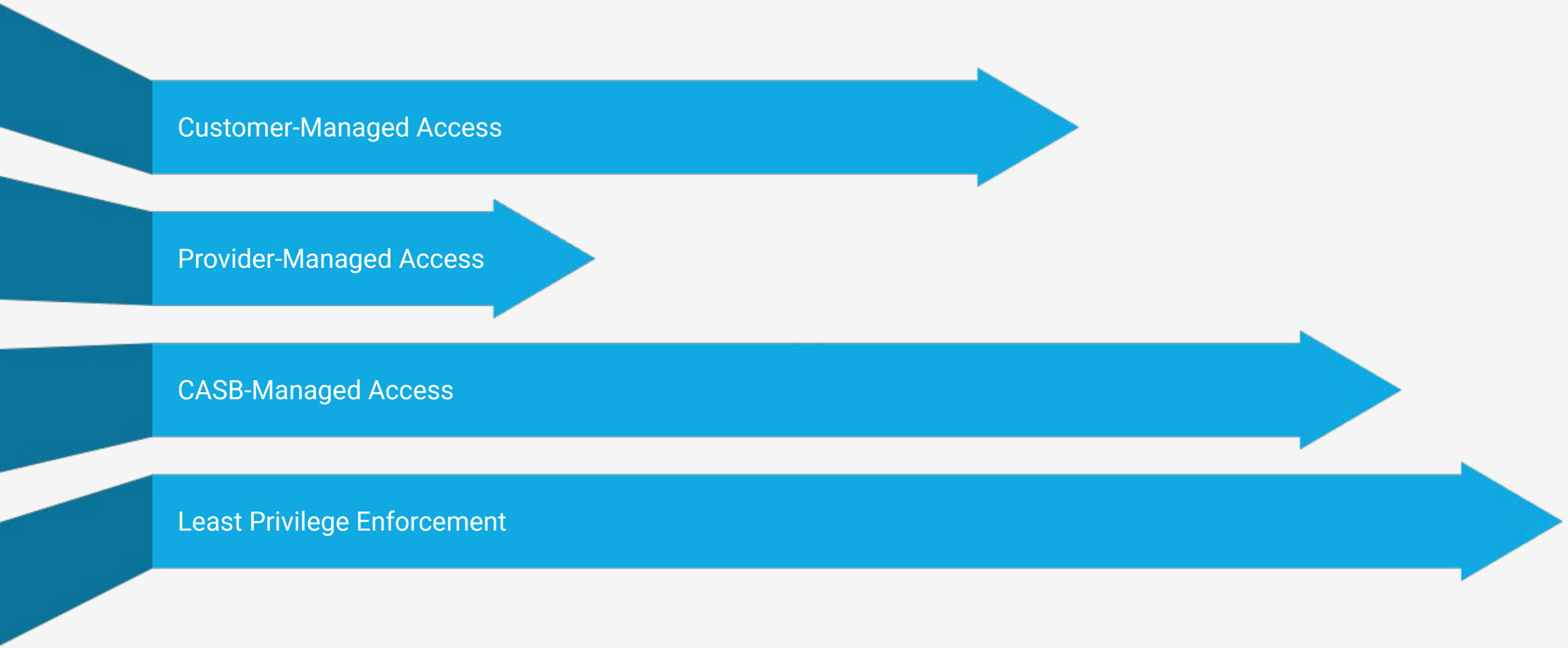


Data Access Responsibilities

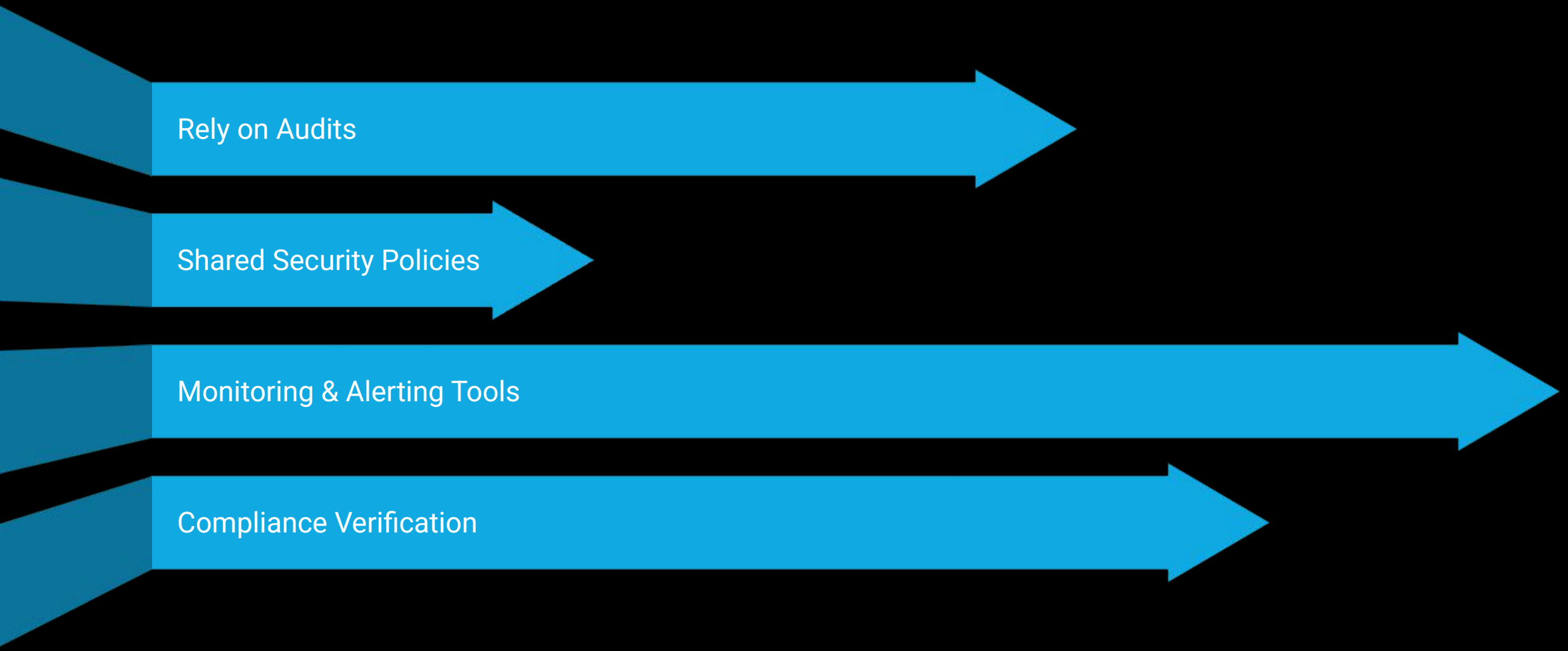
Responsibility	Customer	Provider	Third-Party
Data Encryption	Encrypt data at rest and in transit	Secure data storage and transmission infrastructure	Implement additional data encryption layers
Identity and Access Management	Manage user accounts and access privileges	Provision and manage cloud platform identities	Manage third-party user access and permissions

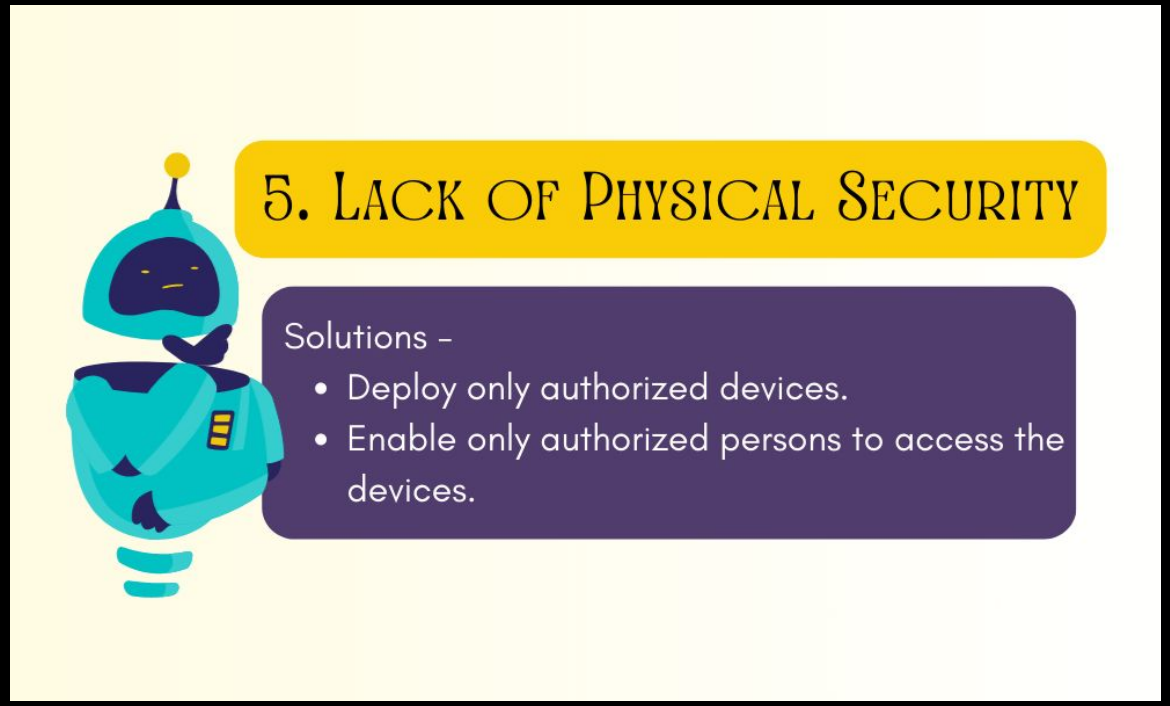
*Adapted from AWS Shared Responsibility Model (https://aws.amazon.com/compliance/shared-responsibility-model/)

Shared Responsibilities: Data Access



Lack of Physical Access





Lack of Physical Access

In cloud environments, customers lack physical access to the underlying infrastructure, as it is managed remotely by the Cloud Service Provider (CSP). This presents a unique challenge, requiring organizations to rely on audits, shared security policies, and monitoring tools to ensure the integrity and security of their cloud resources.