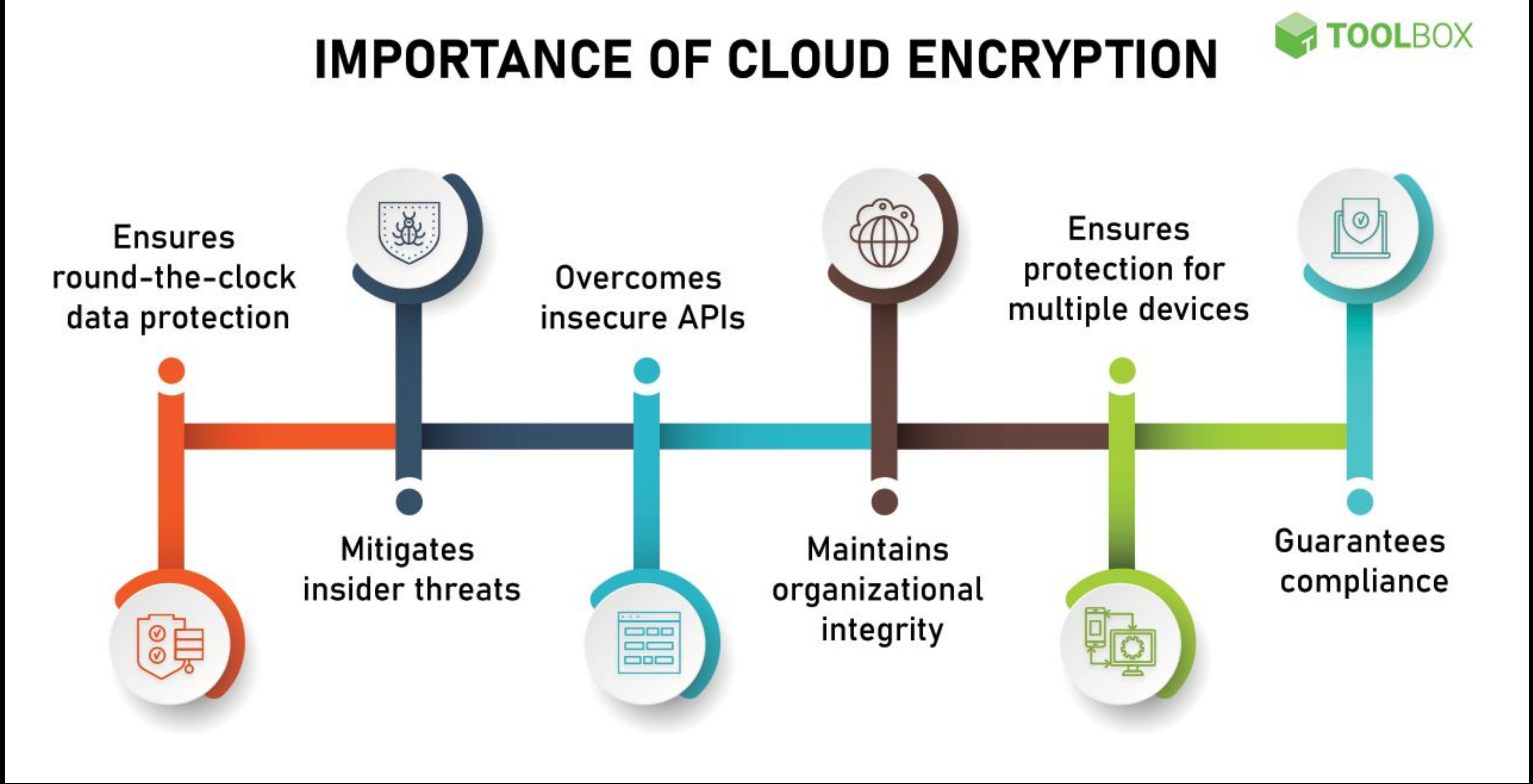

IMPORTANCE OF CLOUD ENCRYPTION
TOOLBOX
Ensures round-the-clock data protection
Mitigates insider threats
Overcomes insecure APIs
Maintains organizational integrity
Ensures protection for multiple devices
Guarantees compliance

# Securing Cloud Data: Encryption Strategies for the Modern Enterprise

# Introduction to Cloud Data Encryption at Rest

- **Application Level Encryption**

  Encrypting data within the application or at the data source level before storing in the cloud

- **File/API Encryption**

  Encrypting discrete files and data transfers via application programming interfaces (APIs)

- **Database Encryption**

  Encrypting data within relational or NoSQL databases at different layers

- **Object Storage Encryption**

  Encrypting data stored as objects in cloud storage services like S3, Blob Storage, or Google Cloud Storage

- **Volume Encryption in the Cloud**

  Encrypting entire virtual disk volumes at the application or operating system level

# Application-Level Encryption

### File/API Encryption

Encrypting files and API data transfers before storing in the cloud

### Database Encryption

Protecting sensitive data in relational and NoSQL databases

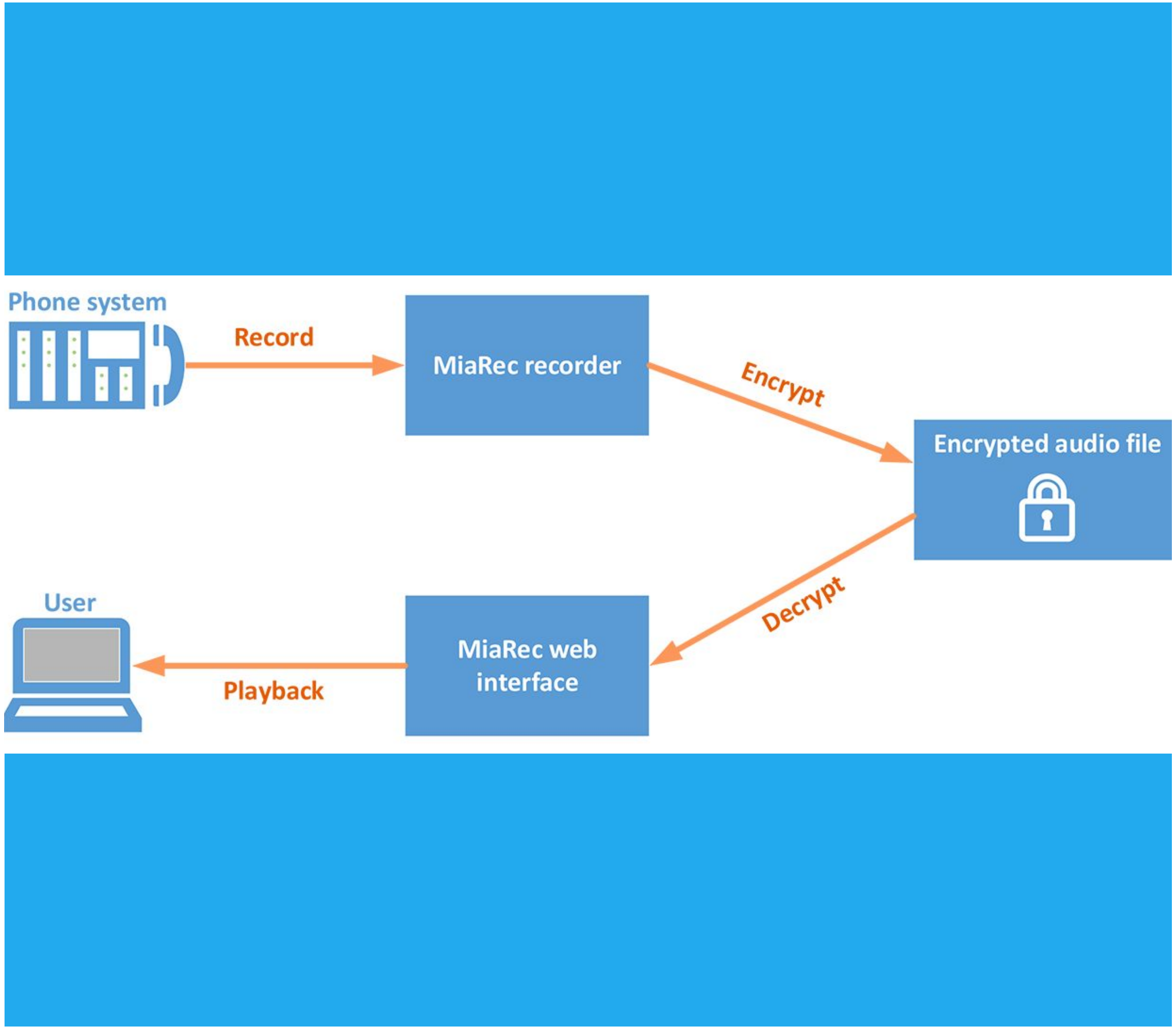
### Object Storage Encryption

Encrypting data store red as objects in cloud object storage services

### Volume Encryption in the Cloud

Encrypting entire virtual disk volumes at the application or OS level

**Application-level encryption ensures data is protected throughout its lifecycle, not just in storage.**



# File/API Encryption

File/API Encryption addresses the encryption of discrete files and data transfers via application programming interfaces (APIs). When data is generated or processed by an application, it can be encrypted at the file level before it is transmitted to cloud storage. This method is especially relevant for organizations that handle sensitive documents, reports, or files that must be transferred securely.

# Cloud Data Encryption at Rest

## Application Level Encryption

Encrypting data within the application or at the data source level before it is stored in any medium.

## File/API Encryption

Encrypting discrete files and data transfers via application programming interfaces (APIs) before storing in cloud.

## Database Encryption

Encrypting data within relational or NoSQL databases at multiple layers to protect stored records and meet compliance.

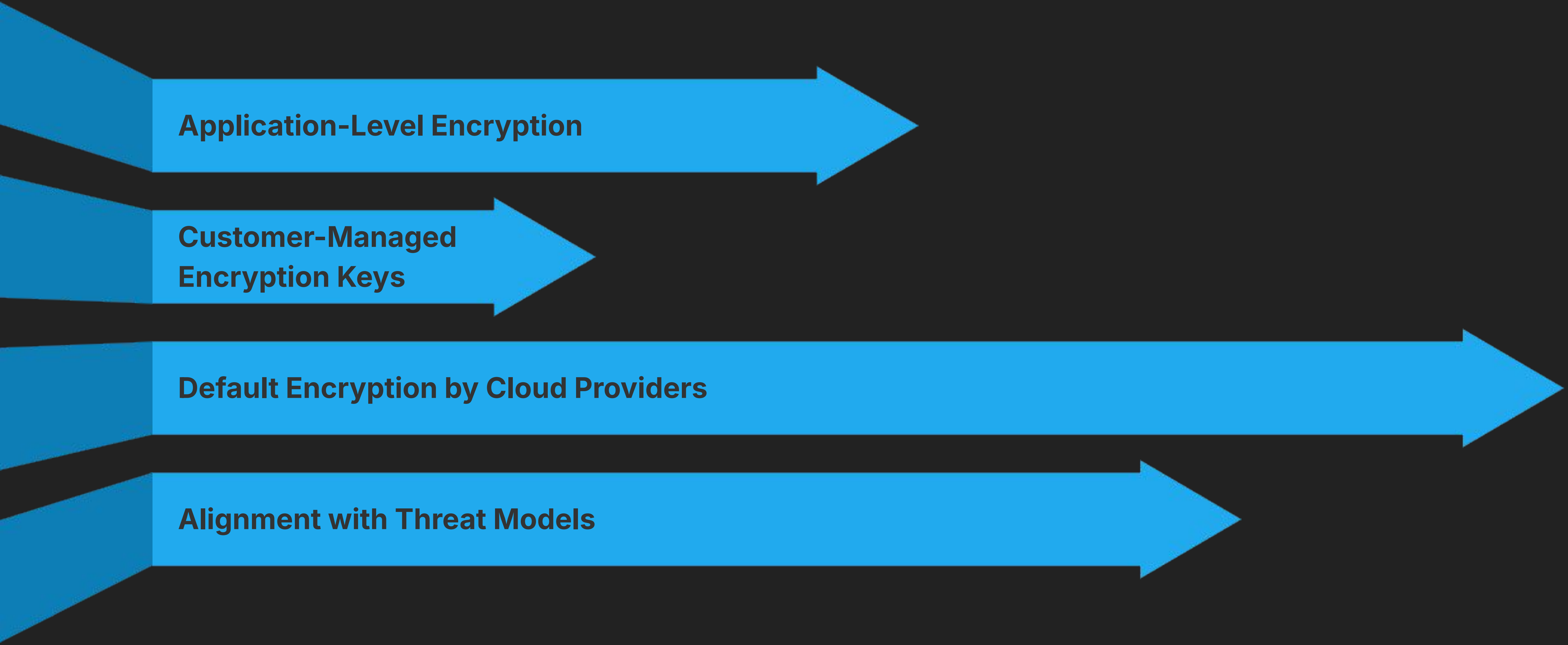
## Object Storage Encryption

Encrypting data stored as objects in cloud object storage services with customizable key management.

## Volume Encryption in the Cloud

Encrypting entire virtual disk volumes at the application or OS level to protect sensitive workloads.

# Cloud Data Encryption at Rest



Application-Level Encryption

Customer-Managed Encryption Keys

Default Encryption by Cloud Providers

Alignment with Threat Models

# Cloud Data Encryption at Rest

### Application Level Encryption

Encrypting data within the application or at the data source level before it is stored in any medium. Ensures data is protected throughout its lifecycle within the application environment.

### File/API Encryption

Encrypting discrete files and data transfers via application programming interfaces (APIs) before transmitting to cloud storage. Especially relevant for sensitive documents, reports, or files that must be transferred securely.

### Database Encryption

Encrypting data within relational or NoSQL databases, implemented at multiple layers (application-layer, transparent data, or column-level). Protects stored records, meets compliance requirements, and reduces the risk of data exposure.

### Object Storage Encryption

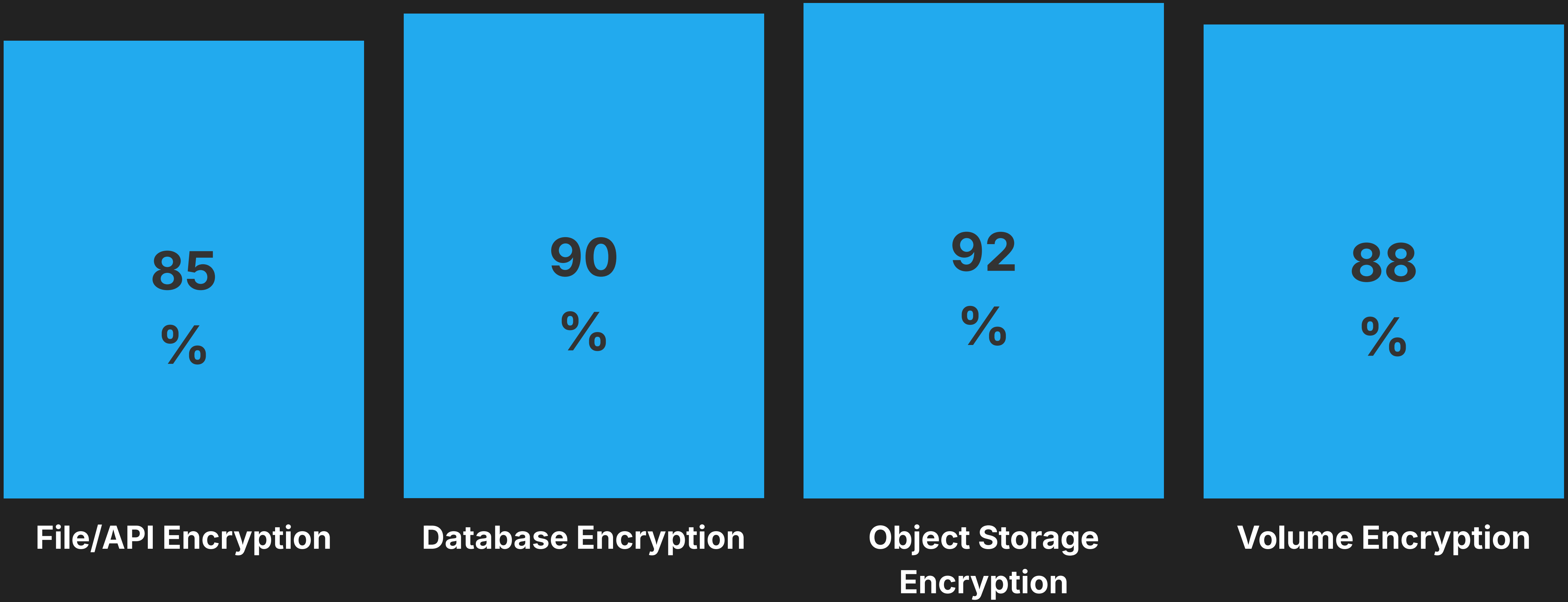
Encrypting data stored as objects in cloud object storage services. Allows customization of key management, strong auditability, and support for cross-region replication while maintaining encryption integrity.

### Volume Encryption in the Cloud

Encrypting entire virtual disk volumes at the application or operating system level, ensuring all data in a virtual machine's storage is protected. Particularly important for sensitive workloads and guarding against unauthorized access to underlying hardware.

# Cloud Data Encryption at Rest

Comparison of different application-level encryption techniques in terms of security, control, and complexity



# Cloud Data Encryption at Rest

### Application Level Encryption

Encrypt data within the application or at the data source level before storage. Ensures protection throughout the data lifecycle.

### File/API Encryption

Encrypt discrete files and data transfers via APIs before uploading to cloud storage. Relevant for sensitive documents, reports, and media files.

### Database Encryption

Encrypt data within relational or NoSQL databases. Protect stored records, meet compliance, and reduce risk of unauthorized access.

### Object Storage Encryption

Encrypt data stored as objects in cloud storage services. Provides customization of key management and strong auditability.

### Volume Encryption in the Cloud

Encrypt entire virtual disk volumes at the application or OS level. Protects sensitive workloads against unauthorized access.

### Cloud Data Key Management Strategies

Ensure encryption effectiveness through secure generation, storage, rotation, and revocation of encryption keys.

# Server-Side Encryption

### Encryption by Cloud Provider

Data is encrypted by the cloud provider before being written to disk, transparent to the end user.

### Simplified Integration

Cloud providers handle key management and encryption/decryption processes, reducing overhead for the customer.

### Compliance Certifications

Major cloud providers offer compliance certifications for their managed server-side encryption services.

### Potential Limitations

rganizations rely on the provider's encryption mechanisms, with less customization options.

**Server-side encryption provides a balance of security and simplicity, but organizations should evaluate provider capabilities and compliance requirements to ensure alignment with their needs.**

# Cloud Data Encryption at Rest

### Application Level Encryption

Encrypt data within the application or at the data source level before storing in the cloud. Ensures data is protected throughout its lifecycle.

### File/API Encryption

Encrypt discrete files and data transfers via application programming interfaces (APIs) before uploading to cloud storage.

### Database Encryption

Encrypt data within relational or NoSQL databases, protecting stored records and meeting compliance regulations.

### Cloud Data Key Management Strategies

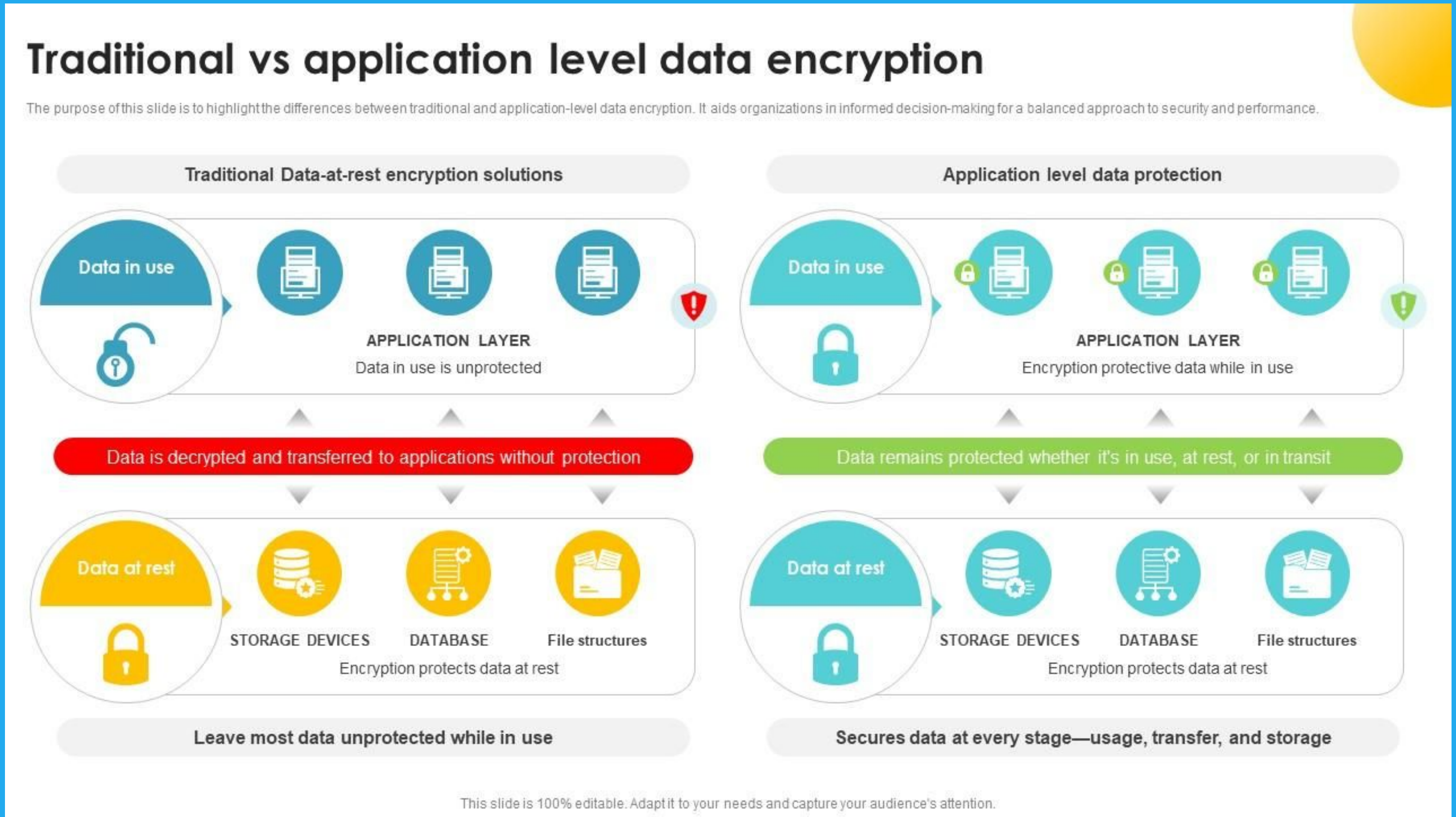
Ensure encryption effectiveness through secure generation, storage, rotation, and revocation of encryption keys.

### Customer-Managed Encryption Keys (CMEK)

Allow organizations to supply and manage their own encryption keys, integrated with a cloud provider's Key Management Service (KMS).

### Encryption Recommendations

Align encryption at rest with organizational, regulatory, and operational requirements through robust key management, SaaS considerations, and threat modeling.



## Traditional vs application level data encryption

The purpose of this slide is to highlight the differences between traditional and application-level data encryption. It aids organizations in informed decision-making for a balanced approach to security and performance.

**Traditional Data-at-rest encryption solutions**

Data in use

APPLICATION LAYER
Data in use is unprotected

Data is decrypted and transferred to applications without protection

Data at rest

STORAGE DEVICES
DATABASE
File structures
Encryption protects data at rest

Leave most data unprotected while in use

**Application level data protection**

Data in use

APPLICATION LAYER
Encryption protective data while in use

Data remains protected whether it's in use, at rest, or in transit

Data at rest

STORAGE DEVICES
DATABASE
File structures
Encryption protects data at rest

Secures data at every stage—usage, transfer, and storage

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

# Custom Application-Level Encryption

Custom Application-Level Encryption refers to using proprietary or specialized encryption libraries within the application stack. This approach can include customized algorithms or encryption libraries beyond standard provider offerings, as well as additional security layers that integrate with specific business logic.

# Encryption Recommendations

- **Application-Level Encryption**

  Encrypt data within the application before storing in the cloud

- **Client-Side Encryption**

  Encryption keys remain on the client side, limiting cloud provider's visibility

- **Server-Side Encryption**

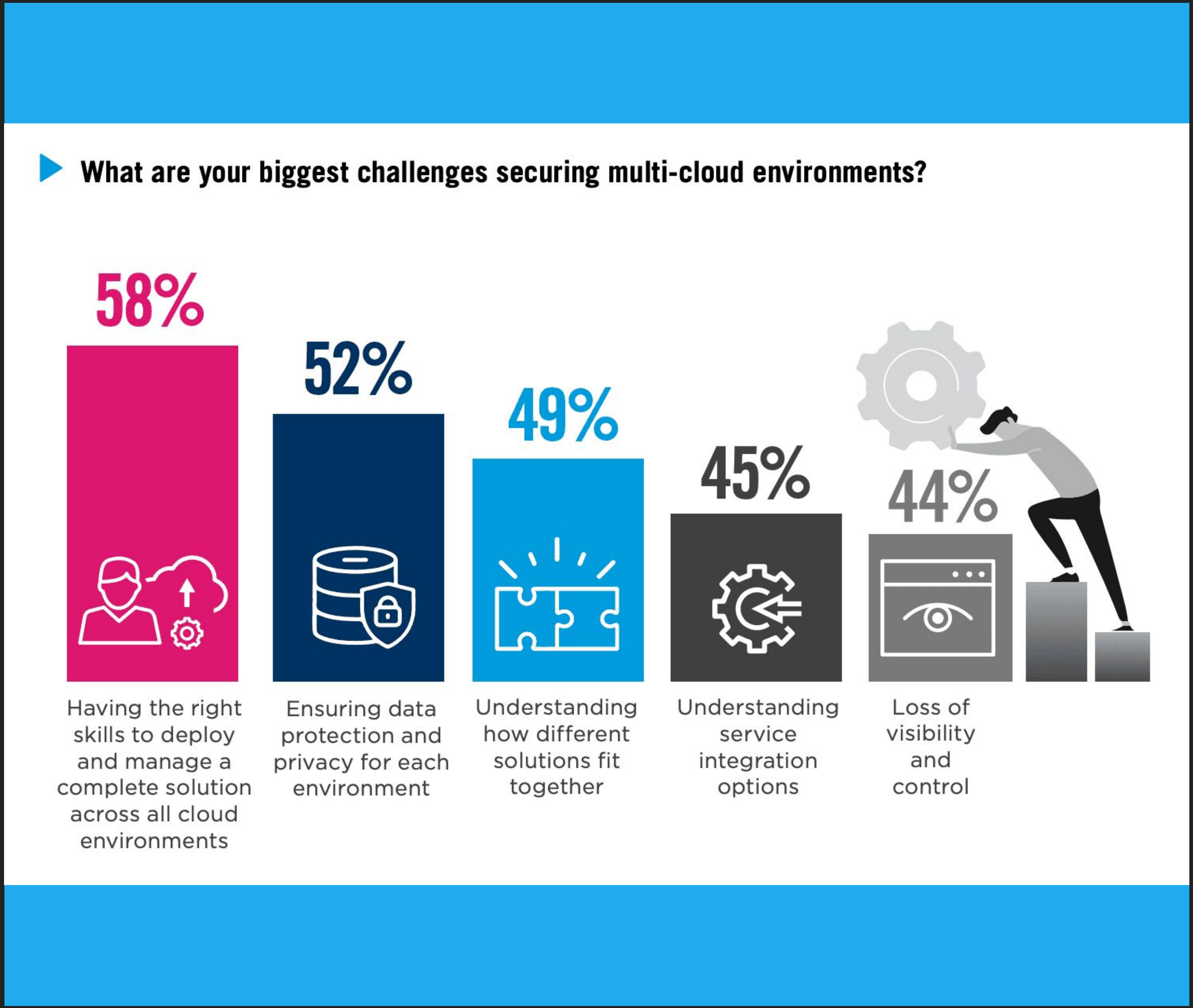
  Cloud provider automatically handles encryption/decryption, often transparent to end user

- **Customer-Managed Encryption Keys (CMEK)**

  Organizations manage their own keys, enabling greater control and audit trails

- **Key Management Services (KMS)**

  Use robust KMS solutions for automated key rotation, access control, and auditing



# Case Study: Protecting Sensitive Healthcare Records

A healthcare provider handles patient records subject to HIPAA compliance, utilizing a combination of AWS and Azure for storing patient information, with an on-premises data center for legacy systems.

# Cloud Data Encryption

- **SaaS Considerations**

  Understanding what encryption your SaaS provider offers by default

- **Default Encryption**

  Default Encryption without requiring customer intervention

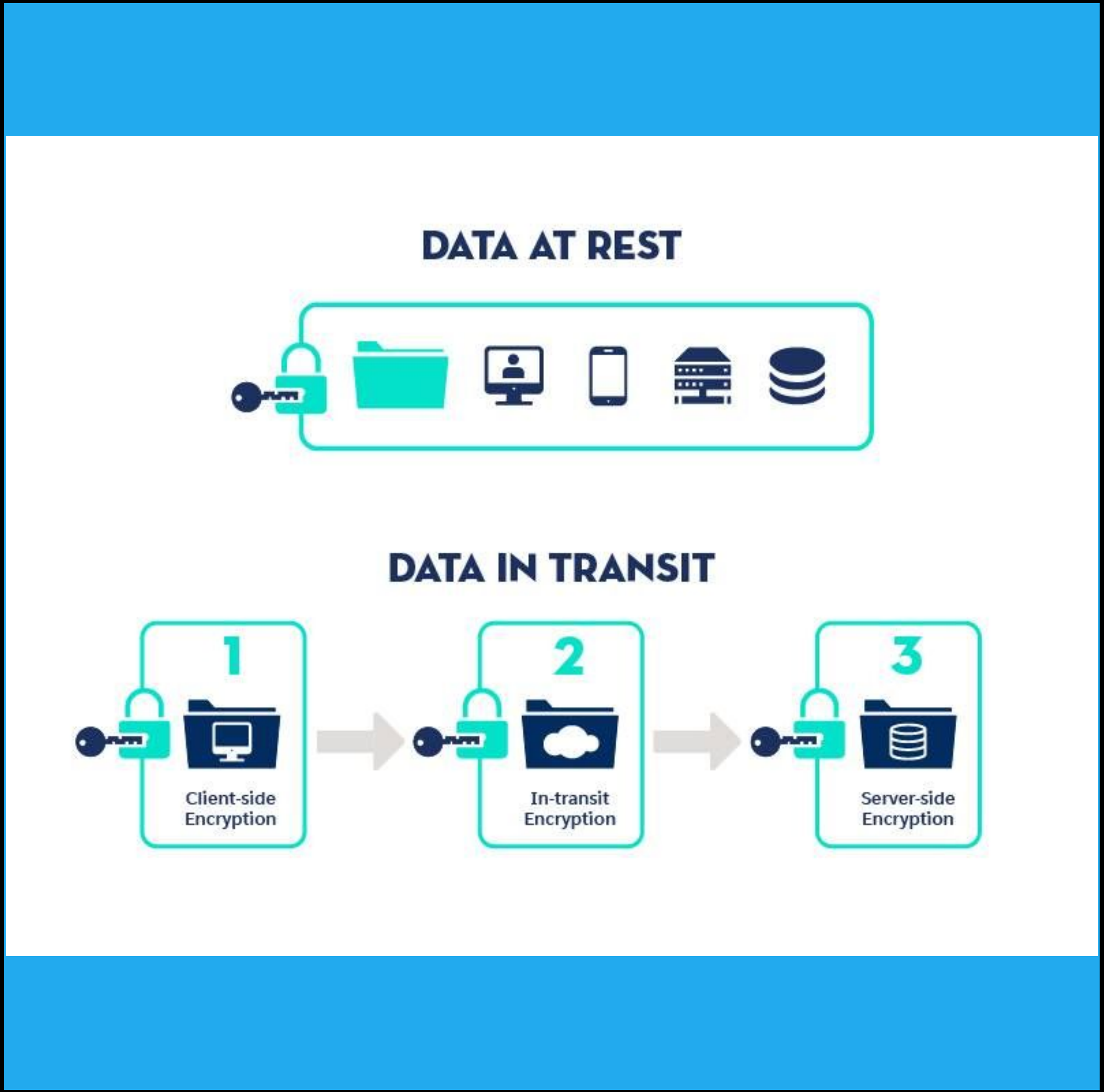
- **Different Keys for Services**

  Use different encryption keys for different cloud services

- **IAM Policies on Keys**

  Principle of least privilege

- Alignment with Threat Models



# Securing Cloud Data: Encryption Strategies for the Modern Enterprise

This slide discusses the key strategies an d best practices for securing cloud data at rest through encryption. It covers the fundamental concepts of application-level encryption, cloud data key management, and recommendations to ensure the effective implementation of encryption in cloud environments.