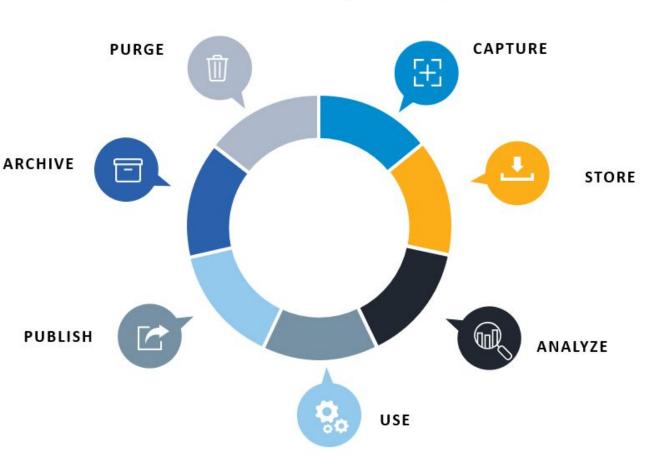
Data Security Lifecycle



SECURING THE CLOUD DATA

LIFECYCLE

An overview of the stages that data undergoes from creation to destruction in cloud environments, and the security measures required to protect sensitive data throughout its lifecycle.

THE CLOUD DATA LIFECYCLE



Defines the stages of the data lifecycle

The Cloud Data Lifecycle outlines the phases data goes
through from creation to destruction, enabling
organizations to apply appropriate security controls at each
stage.



Covers creation, storage, use, sharing, archiving, and destruction
The lifecycle encompasses all stages of data management,

The litecycle encompasses all stages of data management, from initial generation to final destruction, allowing for a comprehensive approach to cloud data security.



Ensures continuous data protection

By understanding the data lifecycle, businesses can align security measures such as encryption, access control, and retention policies to maintain data security and compliance.



Aligns with data classification and jurisdictional requirements

The data lifecycle integrates with data classification and regulatory compliance, ensuring that security controls are applied based on data sensitivity and geographic restrictions.

The Cloud Data Lifecycle provides a structured framework for maintaining data security and compliance throughout the entire data management process, enabling organizations to protect sensitive information and optimize their cloud data strategies.

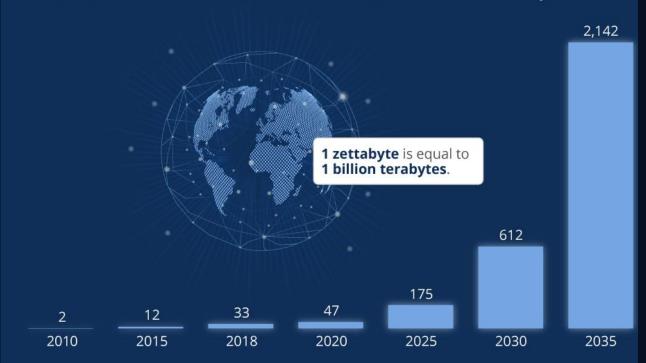
DATA CREATION

The creation stage marks the beginning of the data lifecycle, where data is generated in various forms, including user-generated content, system logs, structured database records, or machine-generated telemetry.

Ensuring that data is classified at the point of creation is critical, as this classification determines how the data should be protected and what security measures, such as encryption, access control policies, or retention rules, must be applied.

Global Data Creation is About to Explode

Actual and forecast amount of data created worldwide 2010-2035 (in zettabytes)





@StatistaCharts Source: Statista Digital Economy Compass 2019

statista 2

SECURE DATA STORAGE

Data Storage Options

Cloud storage options include object storage (e.g., AWS S3, Google Cloud Storage, Azure Blob Storage) for unstructured data, database storage (e.g., relational or NoSQL databases) for structured datasets, and file storage (e.g., NFS, SMB, or cloud file systems) for applications requiring hierarchical storage structures.

Data Integrity and Confidentiality
Implement encryption at rest to protect
data from unauthorized access. Use
redundancy and backup strategies to
safeguard against data loss due to
hardware failure or cyberattacks.

Compliance and Data Sovereignty

Consider data sovereignty and jurisdictional requirements when storing data. Comply with regulations such as GDPR, HIPAA, and PCI-DSS by selecting cloud storage regions that meet the applicable data localization and residency requirements.

Storage Security Measures

Implement automated security posture management tools, data loss prevention (DLP) solutions, and SIEM integration to address risks such as misconfigured storage permissions, lack of encryption, and inadequate backup policies.

Data Availability

Ensure high availability and reliability of cloud storage services to maintain data accessibility for authorized users and applications.

PROTECTING DATA IN USE

Access Control

Encryption in Use

Monitoring and Auditing

Implement role-based access control (RBAC) and attribute-based access control (ABAC) to ensure only authorized users and applications can interact with sensitive data. Apply the principle of least privilege to minimize permissions.

Use techniques like homomorphic encryption and confidential computing (e.g., Intel SGX, AMD SEV) to protect data while it is being actively processed, allowing authorized computations without exposing the underlying sensitive information.

Monitor user activity, API calls, and system logs using security information and event management (SIEM) solutions and cloud-native security tools. Detect and respond to abnormal behavior and unauthorized access attempts in real-time.

SECURE DATA SHARING

Encrypt Data in Transit

Implement Information Rights Management (IRM)

Comply with Jurisdictional Regulations

Secure API Gateways

ARCHIVING SENSITIVE DATA

1. Encryption
 Encrypt archived data
 using strong algorithms
 (e.g., AES-256) to protect
 confidentiality

3. Integrity Checks
Implement periodic
integrity checks and
verification processes to
detect data tampering

5. Audit Logging Maintain detailed audit logs to track data access, modifications, and destruction activities 7. Storage
Optimization
Optimize storage costs by
tiering archived data
across different cloud
storage tiers (e.g., hot,
cold, archive)

2. Access Control

Restrict access to archived data based on user roles and least privilege principles

Define and enforce automated retention policies based on compliance regulations (e.g., HIPAA, SOX)

4. Retention Policies

6. Immutable

Storage

Use immutable storage options to prevent accidental or malicious

deletion of archived data

Securely destroy data at the end of its retention period using cryptographic erasure or other approved methods

8. Secure Destruction

SECURE DATA DESTRUCTION

· Cryptographic Erasure

Permanently destroys encryption keys, rendering data unrecoverable in cloud storage systems.

· Data Overwriting

Overwrites data with predefined patterns to ensure no remnants of sensitive information remain.

· Hardware Degaussing

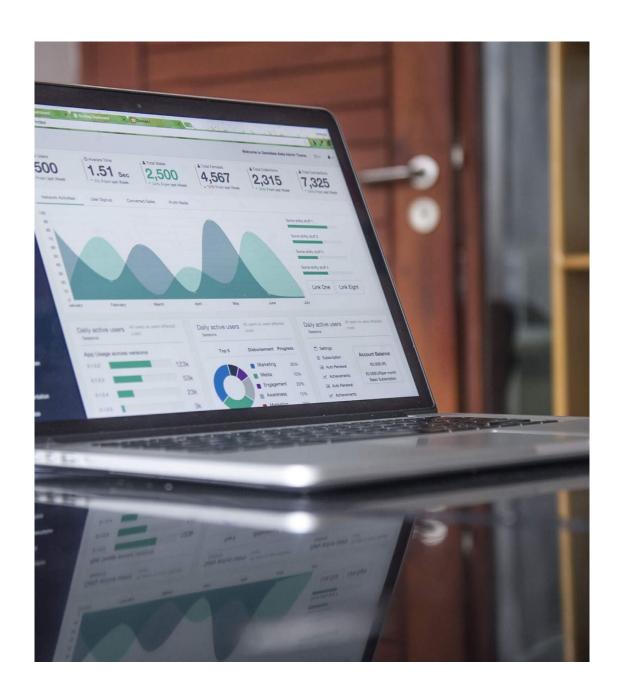
Demagnetizes storage media, such as hard drives, to erase data at the physical level.

· Secure Disposal Audit Logs

Maintains detailed records of the data destruction process to demonstrate compliance with regulations.

· Automated Destruction Policies

Enforces secure data destruction based on predefined retention periods and compliance requirements.



CASE STUDY: HEALTHCARE DATA LIFECYCLE

A large healthcare provider successfully implemented Cloud Data Lifecycle Management, improving security, compliance, and operational efficiency while minimizing data retention costs and breach risks.