

ENCRYPTION & KEY MANAGEMENT.



The algorithm is the easy part — **the real risk lives in how keys are generated, stored, rotated, and destroyed** across their entire working lifecycle.

- DATA-AT-REST ENCRYPTION
- DATA-IN-TRANSIT ENCRYPTION
- KEY LIFECYCLE MANAGEMENT
- HARDWARE SECURITY MODULES (HSM)

01 THE MECHANISM



Data-at-Rest Protection

Encrypting stored data so it stays unreadable without **the correct key, even if storage media is stolen.**



Data-in-Transit Protection

Securing data **as it moves across networks** using TLS, VPN tunnels, and encrypted channels.



Key Lifecycle Management

Controlling how keys are **generated, stored, rotated, and retired** throughout their life.

02 THE FLOW

The Encryption Lifecycle CONTINUOUS

1

A key is generated and stored in **a hardware security module or managed key vault.**

2

The key encrypts and decrypts data **whenever an authorized system requests access.**

3

The key is rotated on schedule, with **old versions retired but retained for decryption history.**

The Key Compromise Cycle LIVE EVENT

1

A key is exposed through **a misconfigured vault, leaked credential, or insider access.**

2

An attacker uses the key to **decrypt data or impersonate a trusted system.**

3

The key is revoked and rotated, and **every system using it must re-encrypt affected data.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Data-at-Rest Encryption	Protects stored data on disks, databases, and backups from unauthorized reads.
Data-in-Transit Encryption	Protects data moving across networks from interception or tampering.
Key Lifecycle Management	Governs generation, rotation, escrow, and destruction of every key.
Hardware Security Modules (HSM)	Provides tamper-resistant hardware for generating and storing keys.

04 ENCRYPTION APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Disk Encryption Alone	No	Doesn't protect data once it's decrypted for use in memory.
Application-Level Encryption Alone	No	Leaves infrastructure and backup layers unprotected.
Manual Key Storage (Files or Scripts)	No	Keys become as exposed as the data they're meant to protect.
Encryption Without Rotation Policy	No	A compromised key stays valid indefinitely once stolen.
Full-Stack Encryption + Centralized KMS	Yes	Protects data everywhere and manages keys through one lifecycle.

ENCRYPTION & KEY MANAGEMENT

PROTECT · MANAGE · ROTATE

05 PROGRAM OPERATIONS

Keys outlive the data they protect. Retired data can resurface in backups long after a key should have rotated.

Rotation policy means nothing without enforcement. A documented schedule doesn't rotate a key by itself.

An HSM protects the key, not its usage. Authorized access can still be misused to expose data legitimately.

Encryption without access control isn't confidentiality. Anyone holding a valid key can read everything it decrypts.

06 CONTROL MAPPING

NIST SP 800-57

Key management lifecycle defining generation, distribution, and retirement of keys.

FIPS 140-3

Cryptographic module security certifying hardware and software that handle keys.

PCI DSS

Payment data encryption requiring strong cryptography for cardholder data.

ISO 27001 ANNEX A

Cryptographic controls policy governing encryption use across the organization.

07 WHAT THIS DOES NOT SOLVE

Insider access to plaintext

Encryption protects data at rest; an authorized user with decryption rights can still misuse it.

Compromised endpoints

The moment data is decrypted for use, a compromised endpoint sees it in plaintext.

Weak identity controls

Encryption doesn't fix weak authentication guarding who can request the key.

Physical key material theft

Software controls don't stop a person with physical access to key material.

08 MYTHS VS. REALITY

MYTH	REALITY
"Encrypted data is safe from everyone."	Authorized users can still read, copy, or misuse the plaintext.
MYTH	REALITY
"One encryption method covers every case."	At-rest, in-transit, and in-use protection need different mechanisms.
MYTH	REALITY
"Losing a key is a minor incident."	A lost key can mean permanent, unrecoverable data loss.
MYTH	REALITY
"Keys can be managed like passwords."	Keys need lifecycle controls that passwords never require.
MYTH	REALITY
"Once deployed, encryption needs no review."	Algorithms age out; rotation and re-encryption are mandatory.

09 SPEAK THE PROGRAM — KEY TERMS

ENCRYPTION

The process of converting data into unreadable ciphertext without the correct key.

KMS

Key Management System: a service that generates, stores, and controls access to keys.

HSM

Hardware Security Module: tamper-resistant hardware that protects keys, even under attack.

DATA-AT-REST

Data stored on disk, in a database, or in backup media.

DATA-IN-TRANSIT

Data actively moving across a network connection.

KEY ROTATION

The scheduled replacement of an encryption key to limit exposure from compromise.