



Recording Files Encryption

Overview

Ensuring Confidentiality and Integrity for Surveillance Data



Definition

Cryptographically scrambles video data before saving to storage.



Purpose

Guarantees data confidentiality and prevents illegal viewing if physical drives are stolen or the network is breached.



Mechanism

Converts playable video into unreadable chaotic ciphertext securely stored at rest.

Features

Core Cybersecurity Mechanisms



Data Confidentiality and Integrity

Footage remains inaccessible for illegal viewing.



Tamper-Evident Seal

Unauthorized modifications corrupt the data, making it unplayable and triggering security alerts.



AES-256 Cryptographic Standard

Orderly video frames are transformed into indecipherable ciphertext using a securely managed encryption key.

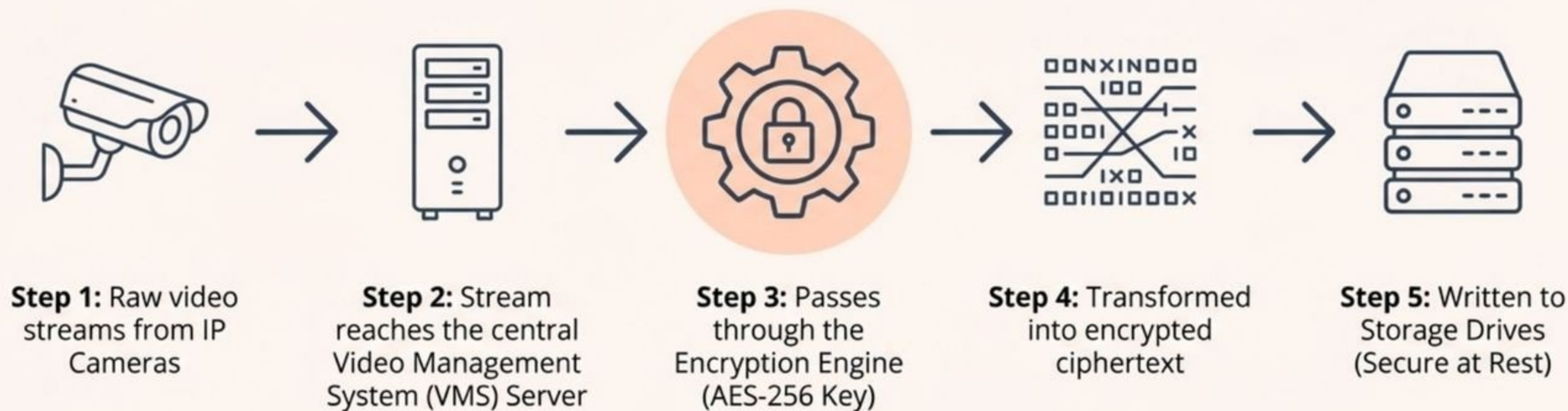


On-the-fly Decryption

Secure authentication grants temporary VMS key access to unlock scrambled data seamlessly for authorized users.

Architectures

The Encryption Workflow



Applications

Ideal Vertical Markets for Encrypted Surveillance



Government & Defense

Protecting classified facility monitoring from espionage or drive theft.



Banking & Finance

Securing vault and teller footage to maintain financial compliance.



Healthcare

Ensuring patient privacy and strictly adhering to medical data protection regulations.



Enterprise Data Centers

Safeguarding internal server room monitoring against network breaches.

Solutions

End-to-End Secure Ecosystems



Primary VMS Engine

Fully integrated and works with NVR 3 Corporate and NVR 3 Business.



Key Management System

VMS acts as the central hub for securely managing decryption keys and granting temporary access based on strict user credentials.



Capacity & Redundancy

Deployable on high-capacity standalone enterprise NVR servers designed to handle the compute overhead of continuous AES-256 encryption across multiple video streams.

Product Introduction

High-Security Recording Hardware & Software



Business NVRs (BNR Series)

Cost-effective standalone servers with embedded encryption engines.



Enterprise NVRs (GNR / INR Series)

High-capacity standalone servers designed for massive, redundant, secure deployments.



Software VMS (NVR 3 Series)

Pure software deployment for highly customized, server-agnostic secure environments.

Key Differentiator Across All Types: AES-256 Encryption Capability.

Product Matrix

Supported NVR and VMS Models

Product Type	Supported Models 
Business NVR	BNR-300
Enterprise NVR	GNR-350
High-Capacity NVR	INR-401, INR-406, INR-407, INR-413, INR-415, INR-416, INR-417-418, INR-490, INR-930, INR-960
Software VMS	NVR 3 Business, NVR 3 Corporate

Comparison

Software VMS vs. Standalone Server Deployment



Standalone Servers (BNR, GNR, INR)

- ✓ Plug-and-play appliance
- ✓ Optimized hardware-to-software integration
- ✓ Dedicated processing for real-time AES-256 encryption



Software VMS (NVR 3)

- ✓ Maximum flexibility
- ✓ Scalable to existing enterprise IT infrastructure
- ✓ Customizable redundancy

Summary

Securing the Future of Video Data



Total Privacy Protection

Videos are completely unreadable without proper VMS credentials.



Absolute Data Integrity

Tamper-evident seals immediately expose unauthorized modifications.



Risk Mitigation

Secures data at rest, neutralizing the threat of physical drive theft and network breaches.

Contact Us

Partner with ACTi Today



Website: www.acti.com



Email: sales@acti.com



Phone: +886-2-2656-2588 /
+1-866-410-ACTi (2284)



Support: Customer Helpdesk &
Project Registration available online.

Member Benefits:

Register today for
Member-Exclusive Pricing
and Project Protection.

(No MOQ or Quota Limits
guaranteed when buying
directly).