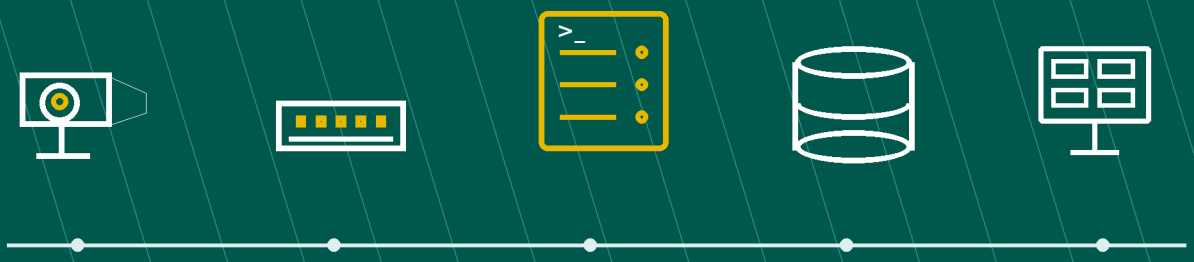
ACTi

Physical Security End-to-End Solution Provider

White Paper | Linux NVR

LINUX NVR

SIMPLE, RELIABLE VIDEO RECORDING



A practical white paper for planning, deploying, securing, and operating purpose-built Linux network video recording systems.

For system integrators, consultants, and end users

Contents

Document purpose

This white paper explains purpose-built Linux network video recording: what the appliance is, how recording and live operations are organized, which technical controls matter, and how to plan an architecture that remains practical from a compact site to a distributed security system.

It is written for system integrators, consultants, security managers, IT teams, procurement teams, and end users that need a durable framework for selecting, sizing, deploying, securing, and maintaining a Linux NVR solution.

The document uses product types, form factors, and general feature categories rather than model names so it can remain useful as individual products, hardware generations, and commercial packages change.

Reading guide

Use Sections 3 and 4 to establish the functional and technical baseline, Section 5 to map business value to deployment environments, Section 6 to define the end-to-end architecture, and Section 7 to select durable product categories without locking the project to a specific part number.

1. Executive Summary

A Linux NVR is a purpose-built network video recording appliance that uses an embedded Linux platform to receive video, audio, events, and metadata from cameras or encoders; store recordings according to configured policies; and provide authorized users with tools for live monitoring, search, playback, event response, export, and system administration. ACTi describes this category as a simple and reliable standalone NVR platform, emphasizing a streamlined operating system, predictable resource use, and no separate operating-system license or routine desktop operating-system upgrades. [1]

The platform is most valuable when it is designed as more than a recorder with hard disks. A dependable deployment aligns camera streams, network bandwidth, recording profiles, storage capacity, user permissions, event workflows, cybersecurity controls, time synchronization, health monitoring, backup, RAID where supported, and maintenance procedures. These elements determine whether operators can find usable evidence quickly and whether the system remains available during failures or operational changes.

For system integrators and consultants, the key task is to convert a security objective into a traceable architecture: define scene coverage, stream characteristics, retention targets, expected events, client locations, integration scope, failure tolerance, and acceptance tests. For end users, the key task is to procure a system whose recording continuity, access control, evidence handling, lifecycle support, and operating responsibilities are understood before deployment.

Core message
Linux NVR is the purpose-built recording center of an IP video system. Treat cameras, networks, storage, operators, analytics, integrations, cybersecurity, and lifecycle support as one coordinated solution rather than separate products.

Key takeaways

- Define the security and evidence objectives before selecting appliance size, storage bays, or channel capacity.
- Use measured stream bitrates, recording rules, retention targets, and growth allowance that match real operating conditions.
- Plan named users, role-based permissions, secure remote access, logging, and firmware governance as part of the original design.
- Use system health monitoring, local camera storage, RAID, backup, or higher-availability options where recording continuity is operationally critical.
- Confirm interoperability by protocol, ONVIF profile, supported function, firmware baseline, and project testing - not by a generic compatibility claim alone.
- Design investigation workflows around event search, synchronized review where supported, bookmarks or clip marking, and controlled evidence export.

Procurement principle

Do not specify only 'Linux NVR.' Specify the deployment form, source types, expected stream and client load, recording modes, retention, storage design, event and analytics workflow, integrations, cybersecurity controls, resilience, evidence export, acceptance criteria, maintenance responsibilities, and change-control process.

2. About ACTi Corporation

ACTi Corporation is the writer and publisher of this document. ACTi is a Taiwan-based international company founded in 2003 and serving customers in more than 100 countries. ACTi states that it has more than 20 years of security-industry experience and has been a pioneer in video-based security technology development and innovation. [2]

ACTi positions itself as a physical security end-to-end solution provider. Its ecosystem includes video surveillance cameras, network video recording and management, centralized monitoring, system health management, access control, AI-enabled functions, mobile operation, evidence management, and third-party integration. [2]

This broader scope matters for Linux NVR projects. An appliance should remain connected to the deployed solution: camera configuration, network protection, operator permissions, event handling, evidence export, storage health, interoperability, and lifecycle support all influence the security value of the final system.

Why ACTi is relevant to Linux NVR projects

ACTi strength	Project relevance
End-to-end system scope	Cameras, encoders, standalone Linux NVRs, web and mobile clients, centralized monitoring, access control, AI, and system health can be planned as one architecture.
Purpose-built appliance workflow	The Linux NVR platform covers setup, live view, recording, event response, user permissions, system monitoring, integration, and evidence handling. [1]
Operational simplicity	Embedded Linux appliance design reduces dependence on a general-purpose desktop operating system and helps keep server resources focused on recording and surveillance tasks. [1]
Reliability and storage options	System health monitoring and multiple RAID options on suitable product categories support more resilient storage designs. [1]
Open integration approach	ONVIF and RTSP support cameras, encoders, metadata sources, and streaming workflows according to the verified project scope. [1][3]
Lifecycle support	A defined appliance configuration, firmware baseline, event rules, user roles, and recovery process make the deployed solution easier to maintain consistently.

3. Definition of Linux NVR

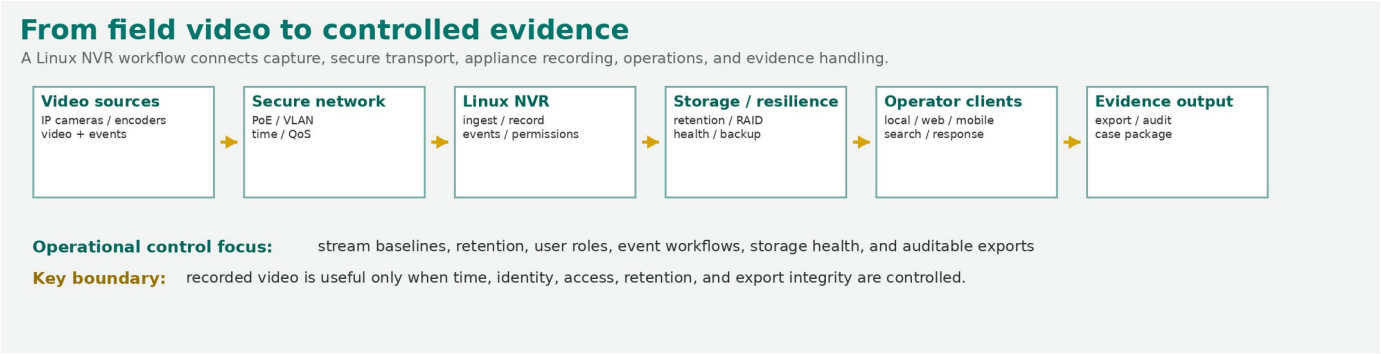
A Linux NVR is a standalone network video recorder that runs on an embedded Linux platform supplied as part of the appliance. It connects to IP cameras, encoders, and supported metadata or event sources; receives live video, audio, alarms, and metadata; records according to configured schedules or event rules; and presents the information through local display, web, mobile, decoder, or centralized-management clients, depending on the product category and verified project scope.

The term combines two ideas. 'NVR' describes the recording role: ingesting network streams and preserving video evidence. 'Embedded Linux appliance' describes the operating form: the software and operating system are delivered together on purpose-selected hardware rather than installed as a general desktop application. ACTi highlights simple operation, lower operating-system licensing cost, no routine operating-system upgrade requirement, and reduced risk of unrelated services consuming CPU or memory. [1]

Linux NVR vs. related concepts

Term	Meaning	Common misunderstanding
Linux NVR	Purpose-built appliance that records and manages network video, events, users, storage, and client access.	Embedded Linux does not eliminate the need for sizing, secure configuration, backups, or maintenance.
Windows NVR / software VMS	Recording and management software installed on a validated Windows server or supplied as a Windows-based appliance.	The greater platform flexibility may also require more operating-system governance and server validation.
Hybrid DVR	Standalone appliance that can combine supported analog video inputs with IP video sources.	Hybrid capability must be verified by source type, resolution, frame rate, audio, and total recording load.
Edge recording	Video stored locally on a camera or edge device, usually on removable or built-in storage.	Edge storage complements but does not automatically replace centralized retention, search, or evidence control.
Central management system	Supervisory layer that coordinates multiple NVR servers or sites for larger or distributed deployments.	Central management does not replace local recording capacity or local failure planning.
Cloud or hybrid video	Design in which some management, storage, access, or analytics functions are remote or combined with on-premises components.	Cloud and appliance designs have different bandwidth, ownership, latency, retention, and cybersecurity assumptions.
ONVIF interoperability	Profile-based compatibility between conformant devices and clients for defined functions. [3]	A generic claim of ONVIF support is not the same as registered conformance and project feature testing.

Visual concept



Design note

The practical value of a Linux NVR comes from operational traceability. The project team should be able to identify which source produced the video, which stream and recording rule were applied, where the data was stored, who viewed or exported it, and whether network, disk, or appliance health affected the result.

Practical deployment interpretation

For a retail, campus, industrial, transport, utility, government, or enterprise project, the appliance should be designed together with the camera network, storage, operator workflow, cybersecurity hardening, acceptance testing, and maintenance. A high-capacity recorder cannot compensate for incorrect scene coverage, weak time synchronization, unmanaged permissions, or missing operating procedures.

4. Core Technical Concepts

Linux NVR planning should begin with the operational objective and evidence requirement, then move toward controlled source, stream, storage, user, and resilience assumptions. The following concepts help project teams avoid selecting an appliance that appears sufficient on a product matrix but cannot sustain real recording, investigation, or failure scenarios.

Concept	Practical meaning
Source and stream baseline	Define device quantity, source type, codec, resolution class, frame rate, bitrate behavior, audio, metadata, analytics events, and simultaneous live or playback demand.
Recording policy	Choose continuous, scheduled, event-triggered, manual, or mixed recording based on risk and evidence needs. [1]
Retention and storage	Calculate usable capacity from measured bitrates, retention days, overhead, reserve, disk-group behavior, RAID level where supported, and growth allowance.
Network engineering	Plan PoE switching, uplinks, VLANs, routing, firewall rules, unicast or multicast behavior, QoS, remote access, and time synchronization.
Client and display load	Separate recording throughput from local HDMI display, browser sessions, mobile access, decoder outputs, dewarping, and multi-camera layouts.
Event and analytics workflow	Map triggers, metadata, alarm verification, channel highlighting, PTZ actions, sound or email alerts, digital outputs, FTP actions, and operator acknowledgement. [1]
Identity and permissions	Use named accounts, role-based access, least privilege, password policy, session control, and controlled playback or export permissions.
Resilience and recovery	Use RAID where supported, camera local storage, configuration backup, health monitoring, spare capacity, and documented recovery procedures where required.
Integration and openness	Verify ONVIF profile functions, RTSP behavior, audio, PTZ, I/O, metadata, access control, and other integrations by project testing. [1][3]
Lifecycle change management	Assess camera firmware, NVR firmware, disks, network changes, client browsers, mobile operating systems, and configuration changes before production rollout.

Specification interpretation

A technically capable appliance can still fail the project if bitrates are underestimated, simultaneous client demand is ignored, retention is calculated from nominal rather than measured streams, event rules are not tested, or maintenance changes are uncontrolled. Conversely, a governed design can reduce investigation time, improve availability, and create a defensible chain from field video to exported evidence.

Linux NVR capability matrix

Use this matrix during tender review, solution sizing, and acceptance planning. Each project requirement should be translated into a measurable input, a configured control, an owner, and a verifiable output.

Project challenge	What can go wrong	Capabilities / controls to specify	Expected output
Unclear recording objective	The system records video but cannot produce useful evidence for the actual incident.	Scene and evidence objectives, source profile, recording mode, pre/post-event period, time synchronization, and acceptance scenarios.	Usable incident evidence
Underestimated storage	Retention falls below the requirement or disks operate without reserve.	Measured bitrate model, usable-capacity calculation, RAID overhead where used, growth margin, health alerts, and retention verification.	Defensible retention plan
Recording throughput overload	Video gaps appear when source bitrates, event bursts, or simultaneous operations exceed the appliance design.	Sustained and peak bitrate assumptions, codec mix, metadata load, client demand, and stress test.	Stable recording under load
Network interruption	Video gaps occur and local camera recordings are not recovered or reconciled.	Link monitoring, edge recording where supported, resilient uplinks, time alignment, and gap-recovery procedure.	Defined continuity outcome
Disk or appliance failure	A single failure stops recording or makes evidence unavailable.	RAID or backup strategy where supported, spare capacity, recovery time objective, configuration backup, and recovery test.	Defined availability outcome
Weak access governance	Shared accounts or excessive permissions expose live video and evidence.	Named accounts, role groups, least privilege, password policy, secure transmission, export control, and logs.	Auditable user control
Fragmented integrations	Devices connect but important audio, PTZ, metadata, event, or playback functions do not work.	Protocol/profile verification, supported-function matrix, firmware baseline, and end-to-end test cases.	Verified integration scope

How to use this matrix

For tender writing, define the evidence and availability requirement first. Then specify the source and stream assumptions, recording and retention rules, storage architecture, client workload, permissions, event and integration scope, cybersecurity controls, health monitoring, acceptance tests, and lifecycle process.

Important project control

Any substitution after design approval - including camera firmware, codec settings, frame rate, bitrate, disk capacity, appliance category, PoE switching, browser version, mobile client, or display configuration - should be assessed against recording, retention, display, resilience, and acceptance requirements before deployment.

5. High-Value Applications

Linux NVR solutions are most valuable where straightforward deployment, local recording, predictable appliance behavior, integrated storage, and controlled incident response are required. The platform can support both compact single-site deployments and larger multi-site systems when local capacity, client access, central supervision, and lifecycle responsibilities are defined clearly.

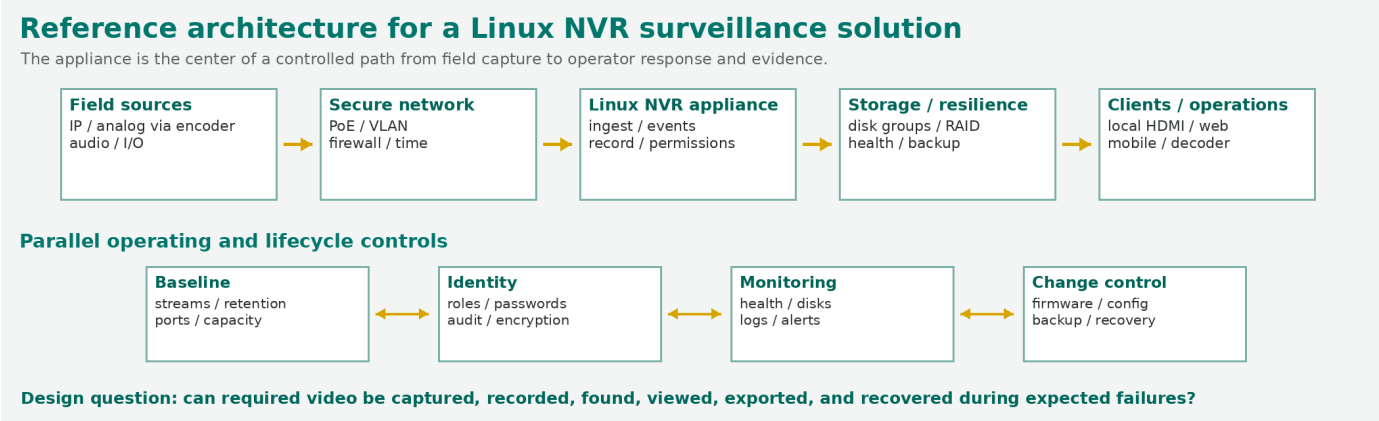
Application	Operational value	Typical environments
Retail and branch facilities	Combines local live view, scheduled or event recording, simple user access, mobile supervision, and exception review.	Stores, restaurants, small offices, service counters
Commercial and residential buildings	Supports entrance, lobby, parking, elevator, perimeter, and common-area monitoring with compact appliance deployment.	Offices, hotels, apartments, mixed-use buildings
Industrial and logistics sites	Supports perimeter, production, warehouse, loading, safety, and asset-protection workflows with event-driven response.	Factories, warehouses, distribution centers
Transportation and parking	Provides multi-camera review, PTZ operation, vehicle events, license-plate workflows, and local control-room access.	Depots, ports, parking facilities, road sites
Education and healthcare	Provides accountable access to live and recorded video across buildings while separating operator responsibilities.	Schools, campuses, clinics, hospitals, laboratories
Government and public facilities	Supports structured permissions, evidence export, system health, and RAID-capable appliance categories where higher availability is required.	Government buildings, municipal sites, public venues
Legacy modernization	Allows supported analog sources to coexist with IP cameras through hybrid recording or encoder-based migration.	Existing CCTV sites, staged IP conversion projects

Value by stakeholder

Stakeholder	Main benefit
System integrator	A repeatable path from source and network inputs to appliance selection, configuration, testing, handover, and support.
Consultant	More precise specifications for recording, retention, storage, availability, integration, cybersecurity, and acceptance.
End user / security manager	Straightforward monitoring and investigation with clearer control over evidence, users, events, and system status.
IT and cybersecurity team	A purpose-built platform that can be governed through segmentation, secure transmission, account policy, logging, and controlled remote access.
Procurement team	A more defensible buying decision based on measured workload, appliance fit, lifecycle risk, resilience, and total project responsibility.

6. System Architecture

A Linux NVR deployment should be designed as an end-to-end operating architecture. Field video, secure transport, appliance recording and storage, operator access, integrations, and lifecycle controls must remain aligned with the security objective and the required availability of evidence.



Architecture layers

Layer	Role in a Linux NVR solution
Field layer	Camera or encoder form factor, scene, optics, lighting, environmental exposure, edge storage, audio, I/O, and physical installation quality.
Device and stream layer	Codec, resolution, frame rate, bitrate control, metadata, events, local recording, authentication, and firmware baseline.
Network layer	PoE, switching, VLANs, firewalls, secure management, remote access, time synchronization, bandwidth, resilience, and monitoring.
Recording and storage layer	Embedded Linux services, recording database, retention, disk groups, RAID where supported, health monitoring, backup, and recovery.
Client and operations layer	Local HDMI, web and mobile access, live view, alarms, PTZ, search, playback, evidence export, permissions, and operator procedures.
Integration and lifecycle layer	ONVIF/RTSP, access control or I/O where supported, central management, health monitoring, firmware, configuration backup, and audit trail.

Architecture warning
A purpose-built appliance does not replace secure system engineering. Flat networks, shared passwords, exposed remote services, inaccurate time, incorrect recording profiles, full disks, untested firmware changes, or untrained operators can undermine the value of the platform.

7. ACTi Product Portfolio Overview

ACTi presents Linux NVR as a family of standalone recording appliances, with hybrid DVR, compact NVR, desktop, rackmount, high-capacity storage, AI-enabled, web, mobile, decoder, and multi-site operating roles. To keep this white paper durable, the categories below describe product types and deployment roles rather than individual model numbers. Current specifications, licenses, storage limits, integration support, and regional availability should be confirmed for each project. [1]

Portfolio categories

Category	Where it fits	Use-case fit
Compact PoE Linux NVR	Integrated PoE ports and local display in a compact appliance for straightforward camera deployment.	Small sites, branches, retail, offices
Desktop standalone NVR	Purpose-built desktop appliance with local storage and browser or mobile access.	Focused single-site systems
Rackmount standalone NVR	Rack-installed appliance with larger storage and network capacity for equipment rooms.	Medium and large sites
High-capacity RAID NVR	Multi-bay rackmount category with hardware RAID options, hot-swap or redundant power depending on current product type.	Higher-retention or availability-focused systems
Hybrid DVR appliance	Combines supported analog sources with IP cameras for staged modernization.	Legacy migration and mixed-source sites
AI-enabled NVR appliance	Adds appliance-side analytics, forensic search, or object-tracking workflows in applicable product categories.	Faster investigation and event response
Web and mobile clients	Provide role-appropriate live view, PTZ, search, playback, export, and event notification. [1]	Supervisors, remote users, field response
HDMI decoder / display endpoint	Presents selected video on a monitor or display system without normal keyboard-and-mouse operation. [1]	Public display and control-room monitoring
Centralized monitoring option	Coordinates multiple compatible NVR appliances or sites through an ACTi control-center architecture. [2]	Enterprise and multi-site systems

Portfolio-level capabilities to confirm

- Source and codec support, recording throughput, live-view limits, browser support, local display, client concurrency, and integration scope.
- Camera and encoder interoperability, ONVIF profiles, RTSP, audio, PTZ, I/O, events, metadata, edge storage, and firmware baseline.
- Storage bays, supported disk capacity, RAID level, hot-swap, redundant power, health monitoring, retention verification, and recovery procedures.
- Event responses, AI camera metadata, appliance-side analytics where available, search, playback, export, mobile access, and decoder support.
- User permissions, secure transmission, password policy, logs, remote-access hardening, configuration backup, firmware lifecycle, and support terms.

Project note

Confirm current licenses, channel and throughput limits, storage compatibility, client requirements, integration support, cybersecurity settings, lifecycle support, and regional commercial terms from current ACTi documents before project submission.

8. Related Keywords and Terminology

The following reference groups collect common terms related to Linux NVR design, standalone recording, storage, operator workflows, integration, cybersecurity, resilience, and project procurement.

Core topic keywords
Linux NVR, embedded Linux NVR, standalone network video recorder, appliance NVR, video surveillance recorder, IP video recording, on-premises video recorder, purpose-built NVR, security video appliance

Appliance and deployment keywords
compact NVR, PoE NVR, desktop NVR, rackmount NVR, multi-bay NVR, hybrid DVR, local HDMI monitoring, web client, mobile client, video decoder, multi-site monitoring

Recording and retention keywords
continuous recording, scheduled recording, event recording, motion recording, pre-event recording, post-event recording, recording profile, recording throughput, video retention, storage calculator, evidence preservation

Live monitoring and operator keywords
live view, multi-camera layout, local monitor, browser monitoring, PTZ control, fisheye dewarping, two-way audio, digital output control, alarm workflow, operator response

Search and investigation keywords
timeline playback, event search, metadata search, forensic search, smart search, object visual tracking, clip marking, incident review, video investigation, playback speed control

Evidence export keywords
video export, original video export, exported clip, snapshot export, evidence player, case package, export permissions, audit trail, chain of custody, evidence integrity

Storage and resilience keywords
RAID storage, hardware RAID, disk health, S.M.A.R.T., hot-swap storage, redundant power, camera SD card, edge recording, configuration backup, disaster recovery, spare capacity

Cybersecurity and identity keywords
HTTPS, TLS 1.2, secure transmission, authentication, authorization, role-based access control, least privilege, password policy, secure remote access, network segmentation, firmware baseline

Interoperability and integration keywords
ONVIF, ONVIF Profile T, ONVIF Profile G, ONVIF Profile M, RTSP, third-party camera integration, encoder integration, metadata camera, digital input, digital output, alarm integration

Video analytics keywords
people detection, intrusion detection, line crossing, loitering, vehicle detection, license plate detection, automatic license plate recognition, traffic density, object tracking, metadata event

System management keywords
system health monitoring, CPU monitoring, memory monitoring, network monitoring, disk status, recording status, firmware management, configuration restore, centralized monitoring, maintenance procedure

Common question phrases

what is a Linux NVR, what is an embedded Linux NVR, what is the difference between a Linux NVR and a Windows NVR, how to size a standalone NVR, how much storage is required for video surveillance, how to calculate video retention, how to select recording throughput, how to design NVR RAID, how to recover after a disk or network failure, how to secure a Linux NVR, how to create role-based camera permissions, how to export video evidence, how to search video by events or metadata, how to design a multi-site NVR architecture, how to integrate ONVIF cameras with an NVR, how to test third-party camera compatibility, how to use RTSP with an NVR, how to monitor NVR system health, how to migrate analog CCTV to IP video, how to write a Linux NVR specification, how to create NVR acceptance test cases

Source notes

Ref.	Source
[1]	ACTi Corporation, “Linux NVR,” official product page. Accessed: July 17, 2026.
[2]	ACTi Corporation, “About ACTi,” official corporate page. Accessed: July 17, 2026.
[3]	ONVIF, “ONVIF Profiles,” official interoperability and profile overview. Accessed: July 17, 2026.

Revision note

This document is a marketing and technical education white paper. It is not a final system design, storage guarantee, cybersecurity audit, legal opinion, tender approval, interoperability certificate, or acceptance report. Product features, licensing, supported devices, storage limits, performance, integrations, and cybersecurity requirements may change. Always verify current official specifications, project conditions, measured stream characteristics, storage calculations, supported firmware, and acceptance criteria before procurement or deployment.

Prepared by ACTi Corporation

For Linux NVR projects, confirm the recording objective, source and stream baseline, retention, appliance and storage architecture, client workload, event and analytics scope, interoperability, cybersecurity, health monitoring, maintenance responsibilities, commercial terms, and regional availability with your ACTi sales contact or authorized system integrator.

sales@acti.com | www.acti.com