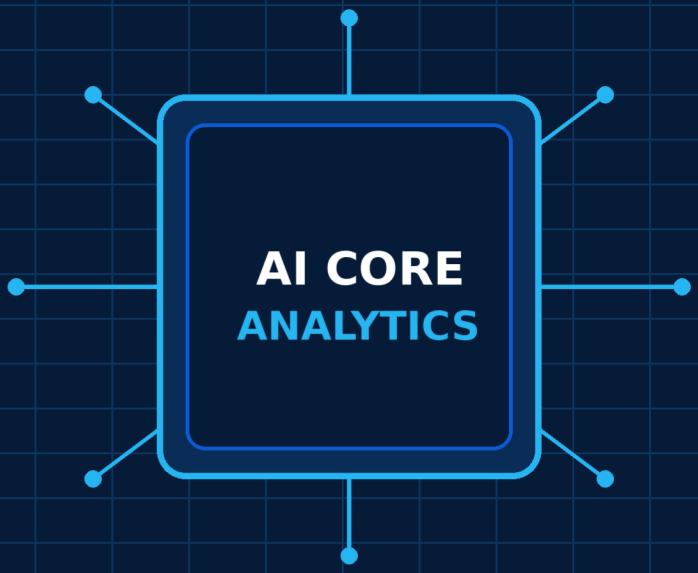
VIDEO GUARD

WHITE PAPER

AI ANALYTICS EDGE VS. CLOUD FOR MUNICIPAL SECURITY

A practical framework for deciding where video intelligence should run - at the edge, in the cloud, or across a hybrid architecture.



EXECUTIVE SUMMARY

Municipal video systems increasingly depend on AI to detect events, classify activity and surface useful information. The architecture behind that intelligence matters. Edge processing can reduce latency, bandwidth dependency and exposure of raw video. Cloud analysis can centralize compute, simplify model management and support cross-site correlation. For most public-safety deployments, the strongest design is not an either/or choice - it is a deliberate hybrid.

THE CORE FINDING

PROCESS LOCALLY. COORDINATE CENTRALLY.

Use edge intelligence for time-sensitive detection and resilient operation. Use the cloud for secure management, investigation workflows, fleet-wide visibility and analytics that benefit from centralized context.

ARCHITECTURE

EDGE PROCESSING VS. CLOUD ANALYSIS

The question is not which architecture is universally better. The question is which workload belongs where.

EDGE PROCESSING

Latency
Local inference can classify events without a round trip to a remote data center.

Bandwidth
Only selected events, metadata or clips need to traverse constrained links.

Resilience
Analytics can continue during intermittent WAN connectivity.

Privacy
Raw video can remain local unless policy or workflow requires transmission.

Scale
Compute capacity must be provisioned and maintained at each deployment.

Model Operations
Updates and model governance must be coordinated across the edge fleet.

CLOUD ANALYSIS

Elastic Compute
Central resources can scale for heavier workloads and aggregate analysis.

Central Management
Models, policies and software can be managed from a common control plane.

Cross-Site Context
Cloud services can correlate information across multiple locations.

Remote Access
Authorized users can review events and video from distributed operations.

Connectivity Dependency
Continuous cloud inference can be affected by WAN loss or congestion.

Data Movement
Sending raw video upstream can increase bandwidth, storage and governance demands.

MUNICIPAL DESIGN PRINCIPLE

Put the first decision as close to the camera as practical. Send the cloud the information that benefits from centralization - not necessarily every frame.

VIDEO GUARD

OPERATIONS

WHY ARCHITECTURE MATTERS TO A CITY

Architecture becomes an operational issue when networks fail, budgets tighten, investigations expand, or an incident requires immediate action.

PUBLIC-SAFETY PRIORITIES

FAST DETECTION

Time-sensitive events should not wait on avoidable network round trips.

NETWORK TOLERANCE

Parks, dumping sites and temporary deployments may depend on cellular, wireless or satellite links.

PREDICTABLE BANDWIDTH

Event-driven transmission can help avoid treating every camera as a constant high-bitrate stream.

INVESTIGATIVE ACCESS

Centralized event and clip access can simplify review across locations.

CYBERSECURITY

Identity, authorization, encryption and device management matter regardless of where compute runs.

LIFECYCLE MANAGEMENT

A distributed edge fleet needs disciplined monitoring, updates and health management.

SECURITY CONTEXT

NIST zero-trust guidance emphasizes protecting resources rather than trusting network location. FBI CJIS guidance also makes cloud use a governance decision involving access, encryption, personnel and data handling - not simply a hosting choice.

DECISION MODEL

MATCH THE WORKLOAD TO THE ARCHITECTURE

A useful design separates real-time event inference from centralized management and investigative workflows.

WORKLOAD	EDGE	CLOUD	HYBRID
Loitering / intrusion detection	STRONG	POSSIBLE	BEST
License plate event processing	STRONG	STRONG	BEST
Real-time safety alerts	BEST	DEPENDENT	BEST
Cross-site trend analysis	LIMITED	BEST	BEST
Central user / policy management	LIMITED	BEST	BEST
Intermittent-connectivity sites	BEST	WEAK	BEST
Large-scale model retraining	WEAK	BEST	BEST
Remote investigation workflows	POSSIBLE	BEST	BEST
Raw video archival	LOCAL	CENTRAL	POLICY-BASED

RECOMMENDED MUNICIPAL PATTERN

EDGE-FIRST. CLOUD-COORDINATED.

Use the VPU™ or MVR™ edge layer to classify events near the source. Transmit selected metadata, alerts and relevant clips through available connectivity. Use the VideoGuard platform as the centralized operational layer for authorized access, review, investigation, policy and system management.

VIDEOGUARD APPROACH

INTELLIGENCE AT THE EDGE. CONTROL IN THE PLATFORM.

VideoGuard is designed around a practical hybrid model: local intelligence where latency and resilience matter, centralized access where coordination and investigation matter.

DESIGN PRINCIPLES

01 EDGE-FIRST DETECTION

Run time-sensitive analytics near the video source.

02 EVENT-DRIVEN TRANSMISSION

Prioritize alerts, metadata and useful clips over unnecessary upstream video.

03 CONNECTIVITY FLEXIBILITY

Support 4G/5G/LTE, municipal networks, Wi-Fi, point-to-point links and satellite where appropriate.

04 CENTRALIZED OPERATIONS

Give authorized users a common platform for event review, investigation and system oversight.

05 SECURITY BY DESIGN

Apply strong identity, access control, encryption and lifecycle management across edge and cloud.

06 PHASED SCALABILITY

Start with the operational problem, measure results, then expand.

REFERENCE FRAMEWORK

- NIST SP 800-145 - The NIST Definition of Cloud Computing.
- NIST SP 800-207 - Zero Trust Architecture.
- FBI CJIS Security Policy v6.0 (Dec. 27, 2024) - cloud, access, encryption and CJI handling considerations.

This paper provides architectural guidance, not a representation that every deployment processes or stores CJI.