

SOLUTION BRIEF

VIDIZMO × JCI / Exacq

AI redaction, evidence intelligence, live detection and tamper-evident export on the VMS already in place.

VIDIZMO connects to exacqVision through Exacq's documented Web Service / REST API and client SDK. Video does not have to move. The connector reaches it, applies redaction or analysis, and returns a governed, defensible output. VIDIZMO builds and maintains the connector, so adopting it is not an integration project the organization has to run.

One Platform, Four Products

This is not three separate purchases. Nexus is the platform product. The other three are licensed separately and each is enabled on that same portal. One deployment, one permission model, one audit trail.

	PRODUCT	WHAT IT DOES
PLATFORM	Nexus	Ingest, storage, index and search, identity, permissions and retention. Watermarked, tamper-evident export with chain of custody, and the audit trail every other product inherits.
RELEASE	Redactor	Automatic detection across 36 classes covering faces, people, vehicles, licence plates, weapons and screens, plus spoken and written PII such as names, contact details, and government, financial and medical identifiers. Blur, pixelate or solid fill on video and images; silence or a beep on audio; solid fill on documents. Works on body-worn footage recorded through exacqVision, including Axis.
UNDERSTAND	AI Intelligence Hub	Natural-language search across days of recorded video. Ask where an event happened and get the timestamp, with the source cited.
WATCH	AI Live Insight	Real-time detection and correlation rules on the RTSP/ONVIF cameras already installed. Classes covering people, vehicles, weapons, PPE and hazards, with confidence and severity set per camera. Alerts carry the event, the severity and the detection snapshot.

Detection is a first pass, not the decision

Redactor's output is operator-gated. A reviewer sees every detection as a track across the timeline, merges duplicates, adjusts bounding boxes, deletes false positives, and draws what the detector missed. Tracking carries a hand-drawn region across frames the same way. The detector proposes; the operator decides what leaves the building. That review step is what makes automated redaction defensible in a records request or a disclosure.

A portal-wide redaction dashboard records what was redacted, by whom and when, with per-asset detail and export. A release is defensible in proportion to the record of how it was produced, and when a withholding is challenged that dashboard is the record.

How It Connects

ITEM	DETAIL
Integration path	exacqVision Web Service / REST API, with the C++ and C# client SDK available where deeper access is needed. Built and maintained by VIDIZMO under the Johnson Controls Connected Partner Program.
Effort required	Deployment is a matter of pointing the connector at the exacqVision server, authenticating, and selecting the cameras or archives in scope. No re-architecture of the recording estate, no change to how footage is recorded, and no development work required. VIDIZMO owns the build, maintenance and support.
Where video lives	Stays in exacqVision and is reached live over the connector, or is ingested into VIDIZMO under its own retention and permissions. Both are supported, and the choice is made per workflow.
Where review happens	Detections are reviewed and output released in the VIDIZMO studio, reached through the organization's existing single sign-on rather than a separate credential. Surfacing results and alerts inside the exacqVision client is in development.
Automation	REST API with a synchronous answer, and webhooks outbound on media actions, metadata changes and workflow completion. Single sign-on against the organization's directory; ingest from and archive to its own storage tier.
Infrastructure	AI Live Insight and the AI detection services require GPU inference; there is no CPU execution path. Throughput follows the hardware provisioned and sizing is scoped per deployment. Redaction, search and export against stored content do not change the recording estate.
Deployment	Cloud, on-premises, government cloud, air-gapped and sovereign. Not cloud-locked and not vendor-locked.

Proving the File Was Not Altered

A watermark traces a copy. It does not prove the bytes are unchanged. Two mechanisms do, and both travel with the evidence.

- **A SHA-384 hash**, recorded when content enters the platform and re-verified on demand, detecting any modification to the bytes regardless of how it was made.
- **A digitally signed integrity certificate**, downloadable, carrying that hash. A court or an opposing party needs something portable they can verify independently. A hash held inside a system the other side cannot see is weaker than a signed certificate they can check themselves.

The platform also applies visible watermarking at upload, encoding or download, so a leaked copy traces to the account that took it, and carries chain of custody, retention rules, permissions and a full audit trail.

Hashes cover content ingested while tamper detection is enabled on the portal. Verification establishes that a file has not changed since its hash was recorded; it speaks to the file, not to the truthfulness of what the file depicts.

Compliance Posture

Certification held	VIDIZMO LLC is ISO/IEC 27001:2022 certified . All VIDIZMO products are ISO 27001-aligned.
CJIS	CJIS Security Policy-aligned, with CJIS-aligned hosting available on Microsoft Azure Government. Encryption at rest and in transit, role-based access control, MFA and SSO, and audit logging support the agency's compliance obligation.
FedRAMP	Deployable on FedRAMP High-authorized infrastructure through Project Hosts or Knox Systems, or on Microsoft Azure Government with agency sponsorship.
Other	Supports HIPAA and GDPR obligations through the platform's data-protection capabilities.

Who It Is For

An exacqVision site that has to hand video to a court, a parent, a journalist or a regulator currently does it by hand. This makes that automatic, auditable and fast, on the recordings already held. These are the exacqVision verticals where recorded video carries a privacy or disclosure obligation.

SECTOR	WHAT THE FOOTAGE HAS TO SURVIVE
Corrections	Federal, state and county facilities reviewing long-form recordings, releasing investigation footage, and monitoring for weapons, fights and falls on the housing units.
K-12 and higher education	Districts and campuses fulfilling records requests and disclosing incident footage without exposing uninvolved students, and watching entrances and perimeters during the school day.
Law enforcement and public safety	Agencies releasing footage under public-records law, preparing disclosure for prosecutors, and searching long recordings for a specific event.
Healthcare	Hospitals and behavioural-health facilities releasing incident footage while protecting patients, visitors and clinical detail.
Casinos and gaming	Floors under regulatory surveillance mandates, handing footage to gaming boards and investigators.
Transportation	Transit systems, airports and ports releasing footage to investigators and insurers, across estates too large to review by hand.
Energy, utilities and manufacturing	Critical infrastructure and plant sites releasing incident footage to regulators and watching for PPE and safety breaches on live cameras.
Retail and commercial property	Loss-prevention and incident footage released to police, insurers and claimants without exposing uninvolved shoppers or staff.

[Book a meeting](#)sales@vidizmo.ai · [+1 \(571\) 969-2180](tel:+15719692180) · vidizmo.ai