Vega Systems, Inc.

Product Catalog

The Immune System for Video Infrastructure

Resilience, Migration, and Edge Transport for Mission-Critical Video Infrastructure.

INSIDE THIS CATALOG

RMF • Tandem • Surestream • XPort • Atlas • Nidhi

vega25.com | info@vega25.com | +1-669-256-2357

THE PORTFOLIO AT A GLANCE

Which product, and when

Each Product is built for a specific point of failure, or a specific project. Here's which one fits and when.

Always-on Resilience

SITE & DATACENTER

RMF

Cybersecure Redundancy across active-active sites. Object-level synchronization isolates data centers so malware cannot spread.

Milestone XProtect • **Perpetual, per device**

RECORDING SERVER

Tandem

Recorder-only HA, where failover stays invisible to PSIM, access control, and analytics. Two recorders, one identity.

Milestone XProtect • **Perpetual, per recorder pair**

OPERATOR & CLIENT

Surestream

Keep the video live on the operators' screen during a catastrophic VMS infrastructure failure. Stream directly from cameras to clients.

Milestone XProtect • **Perpetual, per device**

RETENTION & BACKUP

Nidhi

Automated media backup and restoration to the cloud or SMB for disaster recovery.

Milestone XProtect • **Annual, per Recorder**

Project & Lifecycle

MIGRATION & CONSOLIDATION

XPort

Move, Merge, or Split XProtect Deployments. Simplify upgrades. Automate life-cycle infrastructure processes and save time and money.

Milestone XProtect • **Annual, per Recorder**

Edge Transport

EDGE & TRANSPORT

Atlas

Make cameras on vehicles and remote sites appear to the SOC like local LAN cameras. Save connetvitiy costs through Edge AI. Automatically adapt streams to bandwidth.

VMS Agnostic • **Per Device Subscription**

Redundancy Management Framework

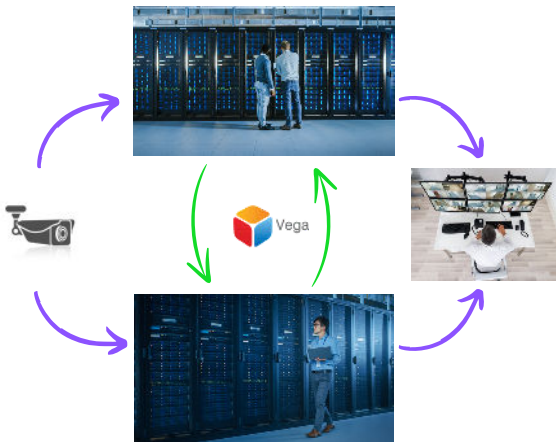
Cybersecure Redundancy for Milestone XProtect

Introduction

Almost every two–data center deployment relies on SQL or service clustering for high availability. The assumption: if one site is hit, the other survives to save you.

It doesn't. Clustering ties the sites together so ransomware or a corrupted database is carried straight into your backup site. The redundancy becomes the attack's fastest path, not a barrier.

RMF is built the opposite way. It delivers full redundancy through object-level synchronization over a narrow, limited-privilege channel — keeping your data centers genuinely separate and isolated, yet redundant.



RMF Overview

Pricing Model

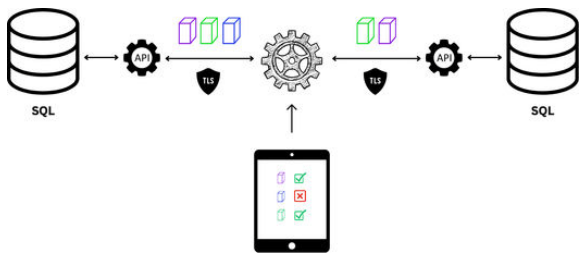
- Single perpetual license per device.
- One device is one MAC Address.
- An encoder consumes a single license, as does a multi-lens camera.

Key Features

A Cybersecurity-first Approach

Unlike traditional high-availability architectures that replicate everything—including mistakes and malware—RMF provides cybersecurity by design, in specific redundancy architectures.

It combines **selective object-level synchronization**, which prevents malicious or unintended changes from spreading, with fully isolated data centers that eliminate shared attack surfaces and block lateral threats. Together, these two layers provide a resilient and secure foundation for mission-critical video infrastructure.



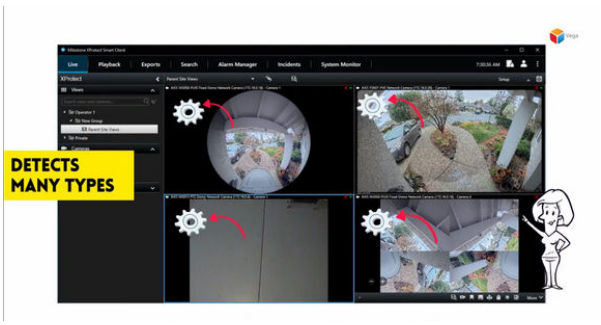
Selective Object Synchronization

Active-Active Redundancy

We exclusively support redundant active-active architectures, ensuring that both data centers are fully operational and accessible to deliver services around the clock. All video resides in each data center.

Client Side Intelligence

Detect failure events in each client window. Independently. Democratically. Align with the end-user's perception of failure. Catch a broad spectrum of failure events that impact end users, big and small.

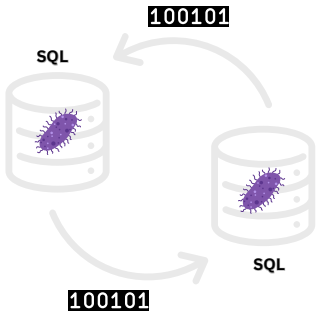


Key Cybersecurity Features

SQL Redundancy

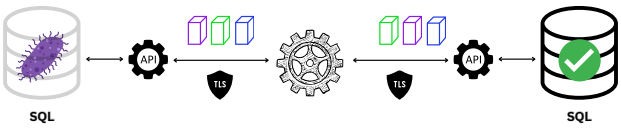
The cyber-risk in 'copy-everything' replication

Traditional replication engines, such as SQL Failover, stream every byte, healthy or hostile, from a primary database to its standby in near real-time. This blind fidelity guarantees that a single corrupt row, ransomware-encrypted page, or rogue admin account is instantly mirrored across your entire estate. In today's threat environment, that "always identical" philosophy is less a safeguard than a high-speed propagation channel for attacks.



RMF: Cybersecure Object Synchronization

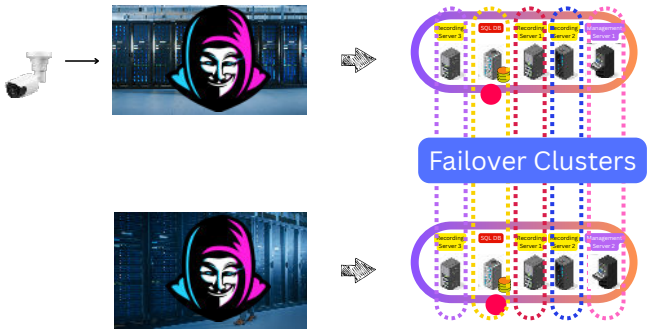
RMF's object-level synchronization inverts that risk profile by making every change pass through Milestone's API, one self-contained object at a time. Because each user, policy, or device is treated as a discrete payload, the RMF sync engine can validate, log, transform, or outright block it before it ever crosses air-gapped boundaries.



Datacenter Isolation

The traditional approach

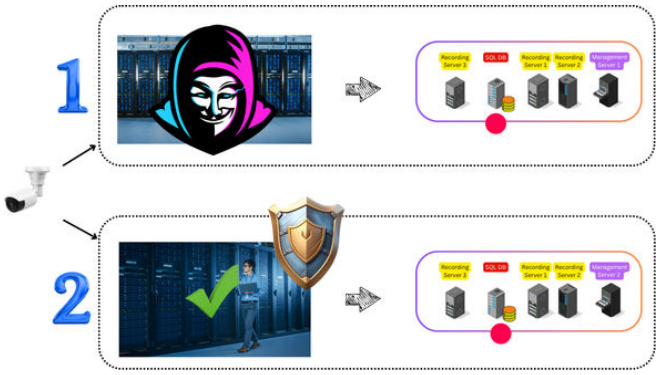
A large percentage of deployed high-availability architectures rely on cross-site service clustering, which increases cyber risk by creating shared attack surfaces.



Traditional Service Clustering: Uncontrolled Blast Radius

RMF: Enforces Narrow, Explicit Trust

RMF (when deployed in Federated or Independent architectures) replaces clustering with a service-based model that treats each data center as an independent entity. There is no requirement for shared authentication, storage, or real-time database replication. Instead, RMF operates through a lightweight service that connects the two sites over a narrow, explicitly defined communication channel with limited privileges and no direct system-level access. This design dramatically reduces the trust surface and prevents lateral movement between sites.



RMF Limits Blast Radius

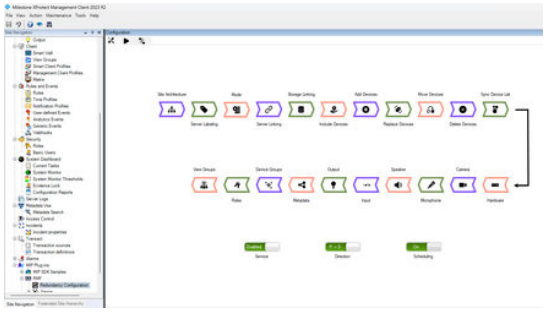
Cybersecurity Whitepaper

Explore our white paper on this topic. Discover various attack vectors that can compromise traditional redundant deployments and learn how RMF helps protect against them.

Key Mirroring Features

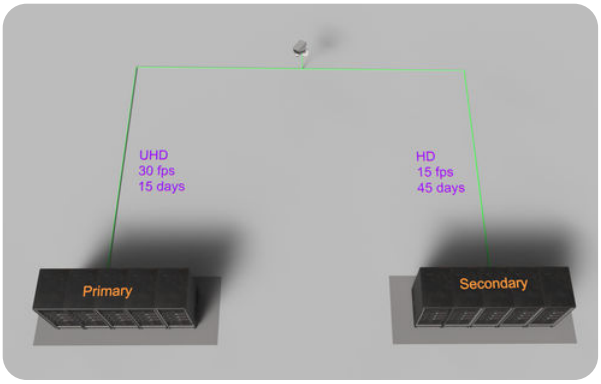
Site Mirroring

A CPU-efficient Smart Synchronization Service enables site mirroring across Federated or Independent XProtect Architectures. Enables use of the secondary site if the primary fails.



Asymmetric Redundancy

Liberate your redundant infrastructure design from the limitations of one-to-one recording server mapping. Choose different stream definitions for primary and redundant streams. Unlock a range of cost-performance architectures. You have options.



Bi-Directional Synchonization

Synchronize Devices, Streams, Roles, Views, and more from the Primary Site to the Secondary Site or from the Secondary to the Primary Site. Restore accidentally modified configurations with ease.

Scheduling

Run Synchronization on a schedule, or run at will. You choose.

Device Add, Delete, Replace, Move

Add devices on the primary data center and see them appear on the secondary. Or, Delete, Replace or even move devices and see them mirrored.

Device Groups

Add, Delete, and Rename groups. Or move cameras between groups in the primary site. RMF mirrors these changes on licensed devices.

Roles

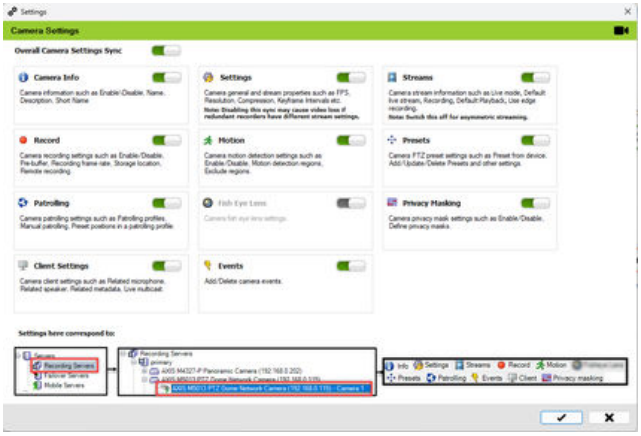
Add, Delete, or modify roles. Add, remove, or modify user permissions. We mirror these changes to the extent of MIP support.

Views

We replicate all smart client view groups to ensure a consistent user experience when logging in to secondary sites.

Precision Synchronization

Synchronize, just a chosen set of devices, Roles, Streams, or synchronize everything in either direction.



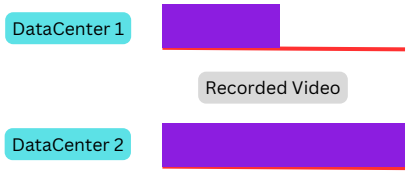
Redundancy Management Framework

Cybersecure Redundancy for Milestone XProtect

Key Client Side Features

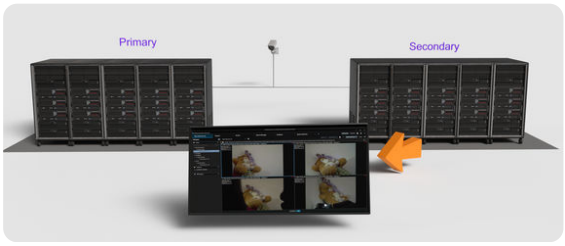
Dual Recording Reduces Missing Footage

With RMF, every camera streams independently to each data center. There is ZERO wait time to start servers or streams when one data center fails. So, there is no lost footage during failure episodes.



Rapid Live Video Recovery

Client-side intelligence enables near-instantaneous live video recovery in the client from alternate data centers. Operators hardly notice live video loss, allowing them to provide higher levels of security. It is the ***fastest in the industry***.

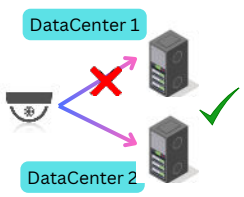


Cause Agnostic Mitigation

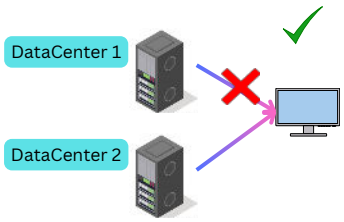
Client-side intelligence mitigates video losses due to many types of failure.

Full Rec. Server Failure

Partial Rec. Server Failure



Network Failure between Cam and Datacenter



Network Failure between Datacenter and Client

REST API

Empower other authenticated components in the deployment ecosystem, such as PSIM and Analytics, to leverage video redundancy.

Simplify Password Updates in Redundant Systems

Effortlessly update passwords across multiple cameras and data centers in a redundant architecture. Update passwords frequently and uphold high-security standards while experiencing minimal disruption.

Load Balance Recorders

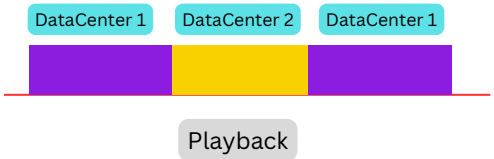
Serve some cameras from Primary Data Centers and others from Secondary Data Centers while operating in Clustered or Federated Architectures.

Flex Licenses

Assign licenses to a set of devices. Later, move those licenses to other devices. Buy and use what you need.

Automatic Playback Switching

When users play back archived footage within the RMF Smart Client plugin, the content will automatically be played back from the redundant site if the primary site is missing content.



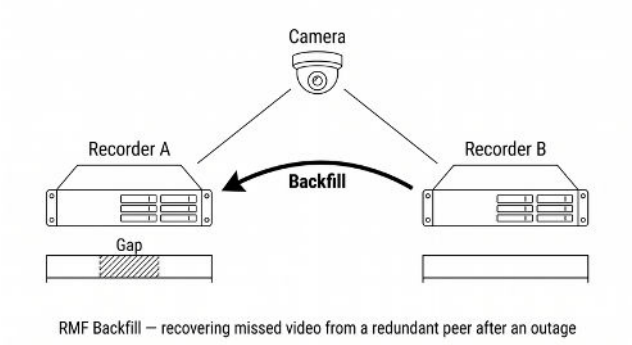
Bookmarks: Redundant Save/Retrieval

Saving bookmarks from within the RMF Smart Client plugin saves it on both the primary and secondary recorders.

Redundancy Management Framework

Cybersecure Redundancy for Milestone XProtect

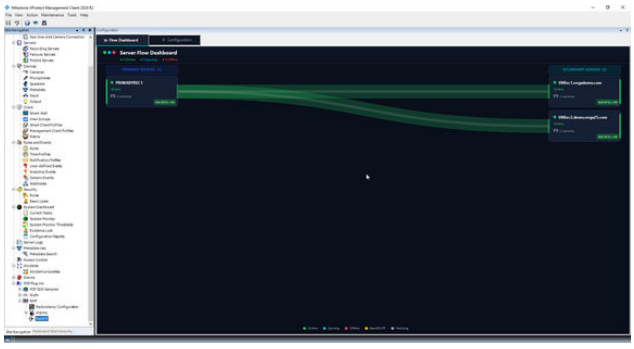
Backfill



RMF Backfill — recovering missed video from a redundant peer after an outage

RMF Backfill restores video continuity across active-active redundant Milestone XProtect recorders after an outage. When a Primary or Secondary recorder goes offline: for maintenance, a network drop, a hardware failure, or any other reason, its peer keeps recording. Once the offline recorder returns, Backfill copies the missed footage from the peer that stayed online, so both sides of the redundant pair end up with the same continuous timeline.

The Flow Dashboard



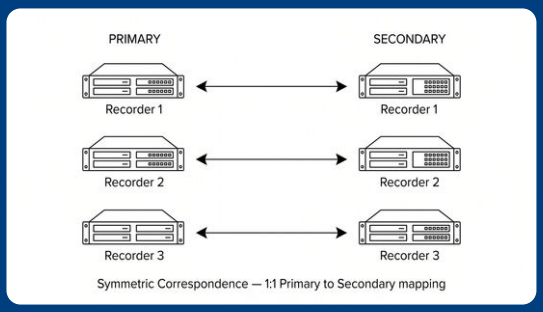
The Flow Dashboard gives a live, at-a-glance view of every recorder participating in Backfill. Primary servers appear on the left, Secondary servers on the right, with animated flow lines connecting redundant peers. Each server card shows its online state, camera count, and whether Backfill is currently enabled

Bandwidth Throttling

A throttling scheduler accepts multiple time windows, each with its own MB/s ceiling. A typical pattern is generous overnight, restrictive during business hours, and moderate in the evening — letting Backfill catch up quickly when the network is quiet without disrupting daytime operations.

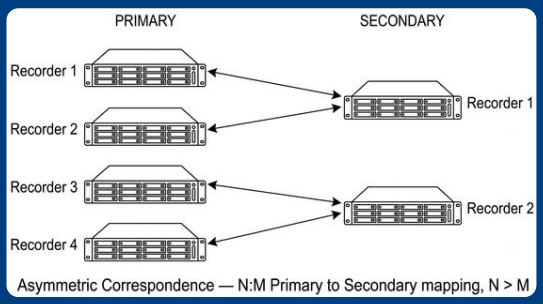
Redundancy Correspondences

Symmetric



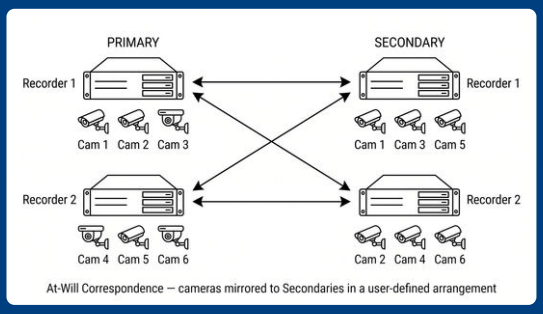
Symmetric Correspondence — 1:1 Primary to Secondary mapping

Asymmetric



Asymmetric Correspondence — N:M Primary to Secondary mapping, N > M

At-will



At-Will Correspondence — cameras mirrored to Secondaries in a user-defined arrangement

Other Features

High Availability Alarms

Leverage Redundant Events in an active-active architecture to generate High Availability Alarms. Alarms are generated even if one data center misses firing an event.

Application Verticals

Airports

Any loss of situational awareness at an airport poses a risk to public safety and is not acceptable. Our solutions provide cause-agnostic failure detection and rapid mitigation for various failures, making us a compelling choice.

Seaports

Essential, revenue-generating port operations heavily depend on live video feeds. A disruption in real-time video can directly result in significant revenue losses. Read more to learn how we help.

Data Centers

Data Centers require compliance with strict physical security standards. Our solutions help data centers in exceeding these standards.

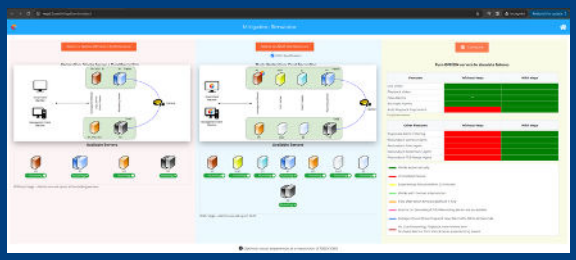
Campus

As university campuses continue to shift towards using multiple data centers for video security, choosing suitable video architectures and software is paramount for maintaining uninterrupted service delivery.

Design

Mitigation Simulator

Visualize the impact of failures of key XProtect components in a myriad of redundant deployment architectures. See how our solutions help mitigate them.



Design Assistance

The path to High Availability can be confusing, with many redundancy options available at different failure tolerances and cost points. We've navigated them all, and we're here to guide you. Share your objectives with us, and we'll help you design a redundancy architecture that meets your needs and budget.

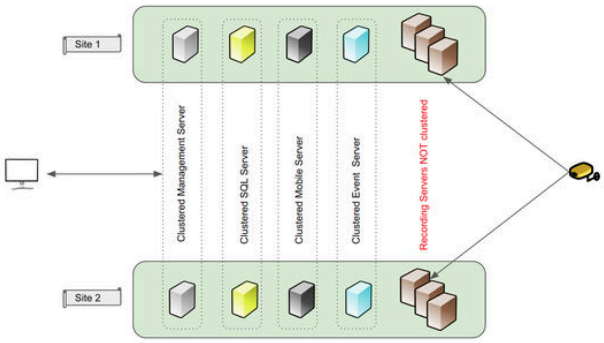
Transportation

Transportation networks, like railways, cover large areas but must be managed as a unified video security system. Our solutions are well-suited for distributed deployment and consumption needs, serving video consumers near the cameras and at remote central facilities.

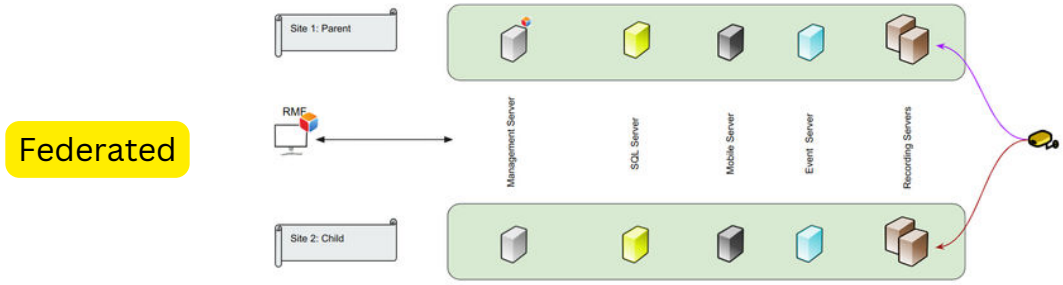
Utilities

Nuclear power utilities necessitate rapid live video recovery, low-latency event alarms, and compatibility with third-party software. We proudly provide these essential features, and are adopted in this industry.

Multi-Architecture Support



Clustered



Federated

Independent

Vega Systems Inc.

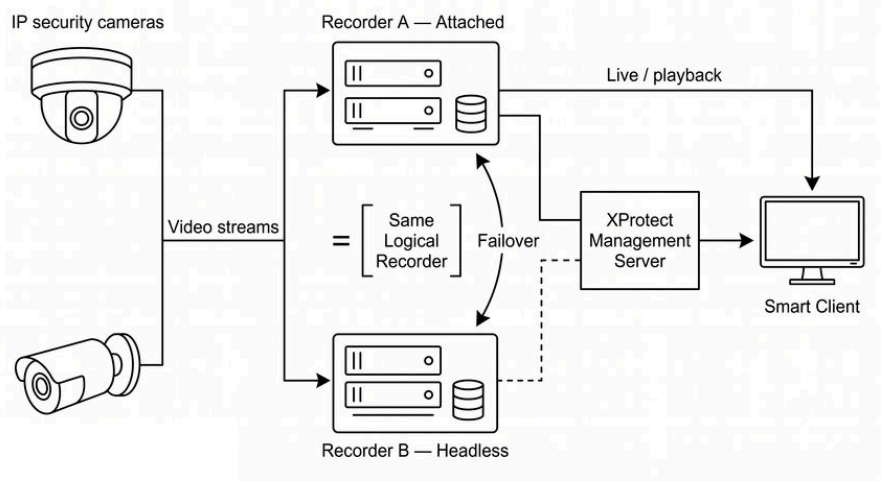
FOLLOW US

https://vega25.com
+1-669-256-2357
info@vega25.com

v 060926

Tandem

Active-Active. Two Recorders. One Identity.



Tandem provides active-active recording-server redundancy for Milestone XProtect environments. A Tandem recorder pair (physical machines or VMs) works as a single logical recorder. Both machines run simultaneously and record directly from the same cameras, so a server failure never creates a gap in recorded video. When one recorder fails, the other steps in to serve live and playback requests automatically, transparently, and seamlessly to the end users, who experience no interruption and need to do nothing. Tandem is especially well-suited for deployments in which multiple third-party systems, such as PSIM, access control, and analytics, are integrated into XProtect.

Functional Description

Beyond Standard Failover

Standard XProtect offers failover recording, but it comes with two gaps. First, the transition isn't instantaneous: when the primary recorder fails, and a failover server takes over, the video recorded during that switchover window is lost. Second, during failover, only the content recorded on the failover server is available; the primary recorder's archived footage is unavailable until the primary is restored. The result is both a gap in the recording and a hole in playback access for the duration of the outage.

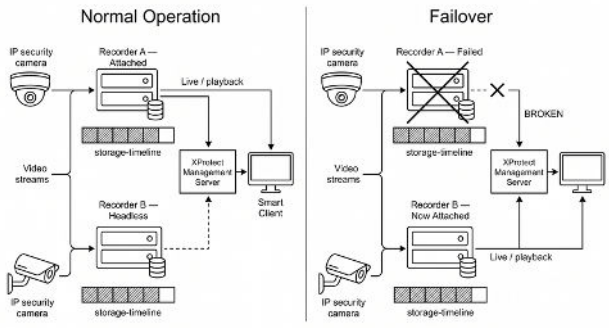
Tandem eliminates both. Because the headless recorder has been recording continuously alongside the attached recorder the whole time, and hasn't started fresh at the moment of failure, there is no switchover gap, and the footage is already available to serve.

Pricing Model

Licensed per recorder pair. Perpetual.

How Tandem Works

A Tandem pair runs in an attached / headless arrangement. Both recorders continuously capture and record from the same cameras. Only the attached recorder connects to the Management Server and serves live and playback to clients; the headless recorder records in parallel but serves no clients. If the attached recorder fails, the headless recorder connects to the XProtect services and begins serving requests; since it already holds the same footage, there is nothing to rebuild and no catch-up window.



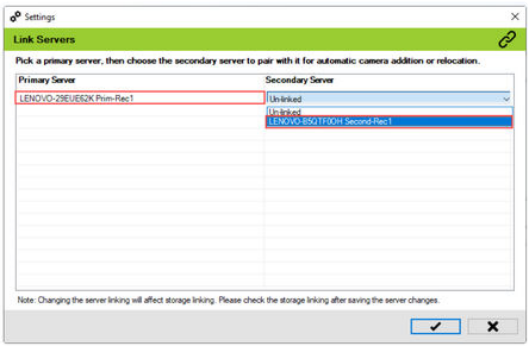
Tandem

Active-Active. Two Recorders. One Identity.

What Tandem Does

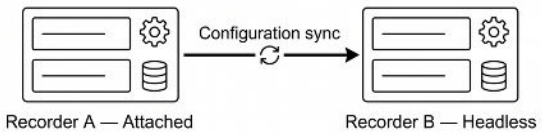
Pairing

Establishes the recorder pair and presents the two machines to XProtect as one logical recorder.



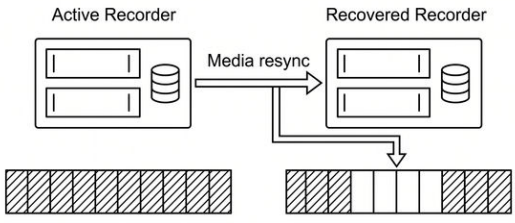
Continuous Configuration Sync

Copies configuration from the attached recorder to the headless recorder on an ongoing basis, so the pair stays identical and the headless recorder is always ready to take over with the current settings.



Media Resync on Recovery

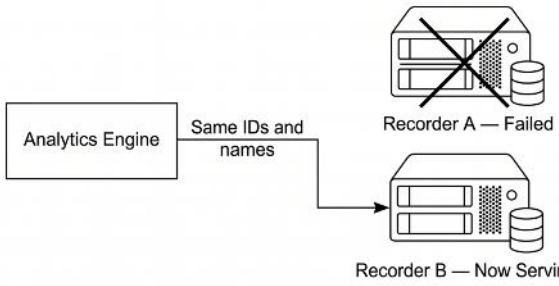
When a recorder that was offline comes back up, Tandem copies the media it missed from the active recorder back to the recovered recorder, restoring its media database to a complete state. After resync, both recorders again hold the full record.



Transparent to Third-Party Integrations

Tandem's failover is invisible not just to operators but to the third-party software layered onto XProtect. Because the recorder pair presents itself as a single logical recorder, every identifier, name, and reference that integrated systems depend on stays constant across a failover; nothing is renamed, renumbered, or re-registered.

The result is redundancy that extends through the entire stack. Failover protects not only recording and viewing, but every system built on top of XProtect.

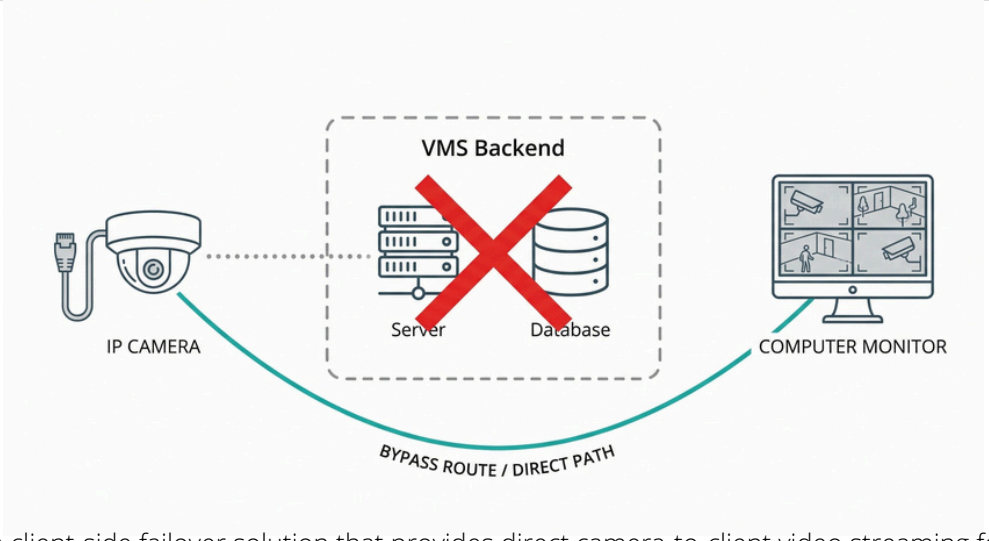


Availability

Oct. 2026

SureStream

Client-Side Video Failover for Milestone XProtect



SureStream is a client-side failover solution that provides direct camera-to-client video streaming for Milestone XProtect environments. It embeds an ONVIF video client inside the XProtect Smart Client, enabling operators to stream live video directly from cameras when VMS backend services are unavailable.

Functional Description

The Hairpin Problem

In standard Milestone XProtect architecture, all video must travel through the Recording Server before reaching the operator's Smart Client. This "hairpin" path creates a critical single point of failure. If the VMS backend crashes, the screen goes black.

The SureStream Solution

SureStream creates a direct, resilient path from camera to client. When backend services are unavailable, operators switch to preconfigured SureStream views and immediately resume live streaming via ONVIF—completely bypassing the VMS backend.

Scope

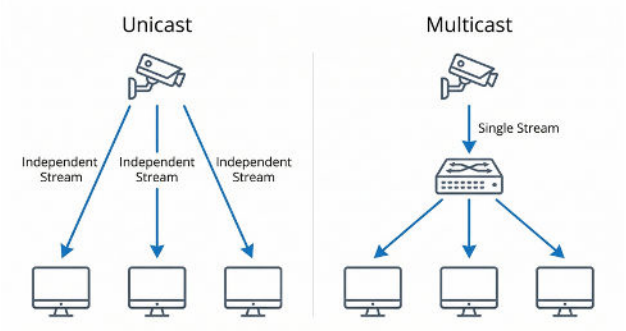
SureStream provides live video only. Playback, recording, and analytics require operational VMS servers.

Cost Model

Licensed per camera device. Perpetual.

Transport Modes

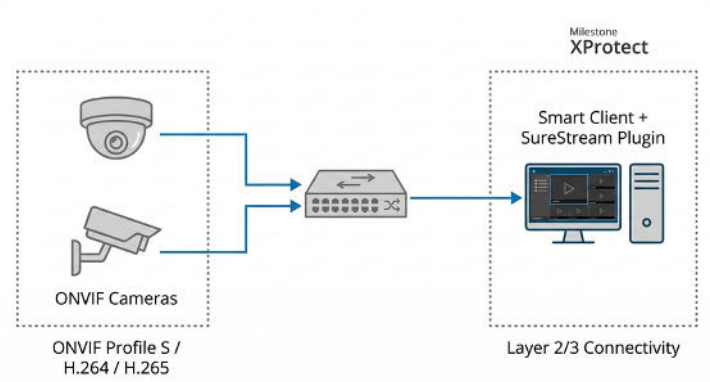
Unicast: One-to-one streaming. Each client establishes an independent connection to the camera.
Multicast: One-to-many streaming. The camera sends a single stream that multiple clients can receive simultaneously. Requires IGMP snooping on network switches for bandwidth efficiency.



PTZ Support

Full pan-tilt-zoom support via direct ONVIF commands. Operators retain camera control even when the VMS backend is offline.

System Requirements



VMS Compatibility

- **Platform**: Milestone XProtect
- **Supported Editions**: Corporate, Expert, Professional+, Express
- **Validated Versions**: XProtect 2019 R3 and later

Installation Components

- **Management Server:**
  - SureStream Management Plugin
  - Handles configuration & licensing
- **Smart Client Workstation:**:
  - SureStream MIP SDK Plugin
  - Install on each failover workstation
  - Handles Streaming

Camera Requirements

- **Protocol**: ONVIF Profile S compliant Video Codecs: H.264, H.265 (HEVC), MJPEG
- **Authentication**: ONVIF credentials required
- **Network Access**: Direct IP reachability from Smart Client and Management Client

Licensing

- **Model**: Per MAC address (workstation)
- **Activation**: Online or Offline supported

Network

Ports

For detailed port requirements by streaming mode, see: docs.vega25.com/surestream/ports

Configuration

Cameras

1. Open Management Client
2. Navigate to MIP Plugins → SureStream
3. Start From A Clean Slate
4. Import Cameras (+)
5. Review Camera Status
6. Select Streaming Mode
7. Configure Rotation (optional)
8. Set Token Timeout
9. Save Configuration

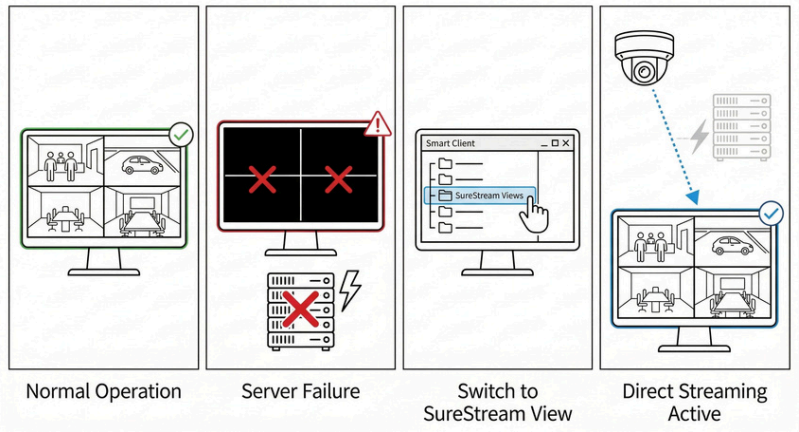
Views

1. Open Smart Client → Setup
2. Views → New Group
3. Create New View
4. Find SureStream in System Overview
5. Drag Plugin into View Windows
6. Click Camera Icon → Select Camera
7. Exit Setup → Live View

⚠ Token Timeout

Smart Clients automatically log out when the Management Server is offline. Extend the token timeout based on the expected repair time to avoid automatic logouts during outages.

Operation



Client Performance

Test Platform

Smart Client Machine

- OS: Windows 11 Pro
- CPU: Intel Core i7-13700T (16 cores, 24 logical)
- RAM: 16 GB
- GPU: Hardware acceleration enabled

Configuration

- VMS: XProtect 2023 R2
- Camera: Pelco D6230L
- Codec: H.264 High Profile
- View Layout: 3x3 (9 cameras)
- GOP: 30
- Max Bitrate: 5000 kbps

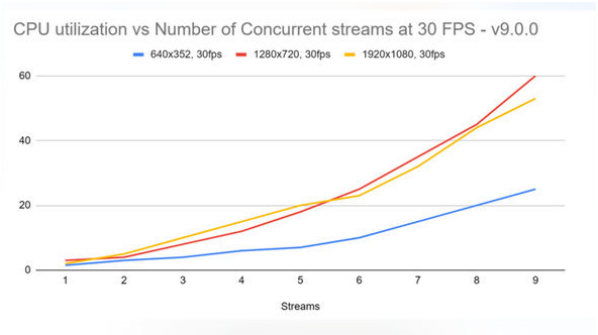
Performance Results

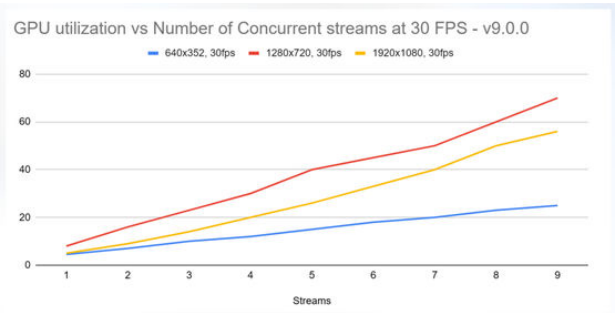
Maximum

3x3 grid (9 cameras) per SureStream view on the test platform at1080p. Native XProtect views with more cameras must be split into multiple SureStream views.

Example

4x4 native view (16 cameras) → Two 3x3 SureStream views



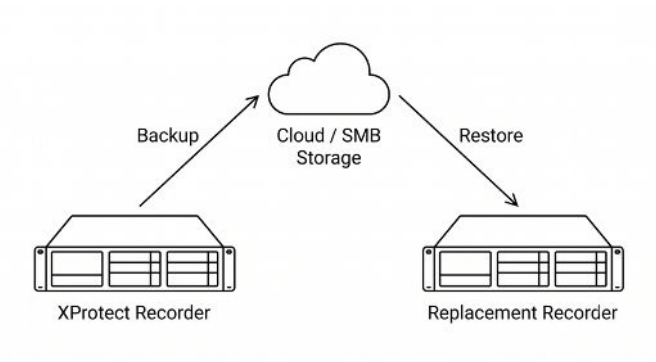


Nidhi

Backup. Restore. Move On.

Introduction

Nidhi provides automated, bandwidth-adjustable, mirrored backup of recorded video from selected Milestone XProtect storage profiles to AWS S3, S3-compatible storage, or SMB shares.
When storage fails, Nidhi provides an easy way to restore media: by individual storage profile for volume-restore workflows, or across every profile on a recorder to bring a failed recorder fully back online on replacement hardware.
Built as a decentralized, highly scalable solution, Nidhi runs an autonomous agent on each recorder and integrates with the Milestone Management Client for centralized control. An at-a-glance dashboard with proactive alerts keeps backup and restore status visible across the entire deployment.



Overview

Pricing Model

- **Annual fixed license cost per recorder**, independent of the amount of data managed or the number of cameras.

Key Features

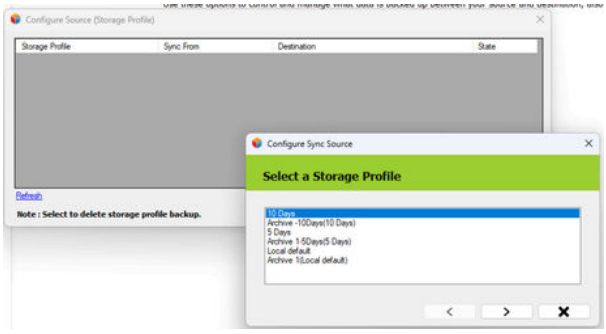
Centralized Management & Dashboard

Nidhi integrates directly with the Milestone XProtect Management Client, giving you a single place to manage backups and restores across all recorders in the deployment. An at-a-glance dashboard shows site-wide backup status: which recorders are protected, which are pending, and how much footage is backed up versus still at risk, while proactive alerts flag failed backups as soon as they occur. For sites running large numbers of recorders, this birds-eye view turns backup from something you hope is working into something you can see is working.

Dashboard in the XProtect Management Client

Selective Storage Profile Backup

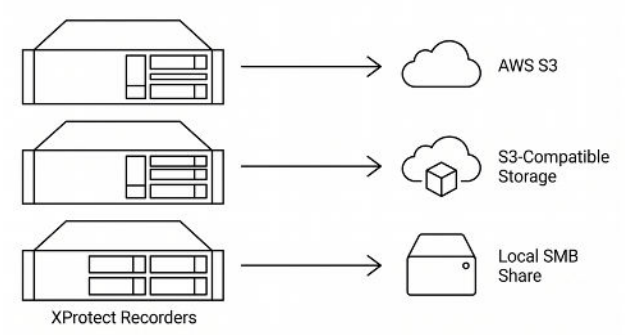
You don't have to back up everything. Most deployments have cameras that matter more than others: entrances, points of sale, critical infrastructure. Nidhi lets you protect exactly those. Group the important cameras into their own Milestone XProtect storage profile, then back up just that profile instead of every camera on the recorder. You decide what's worth protecting, keeping backup footprint and cost aligned with the value of the footage rather than paying to store everything indiscriminately.



Backup by Storage Profile

Flexible Backup Destinations

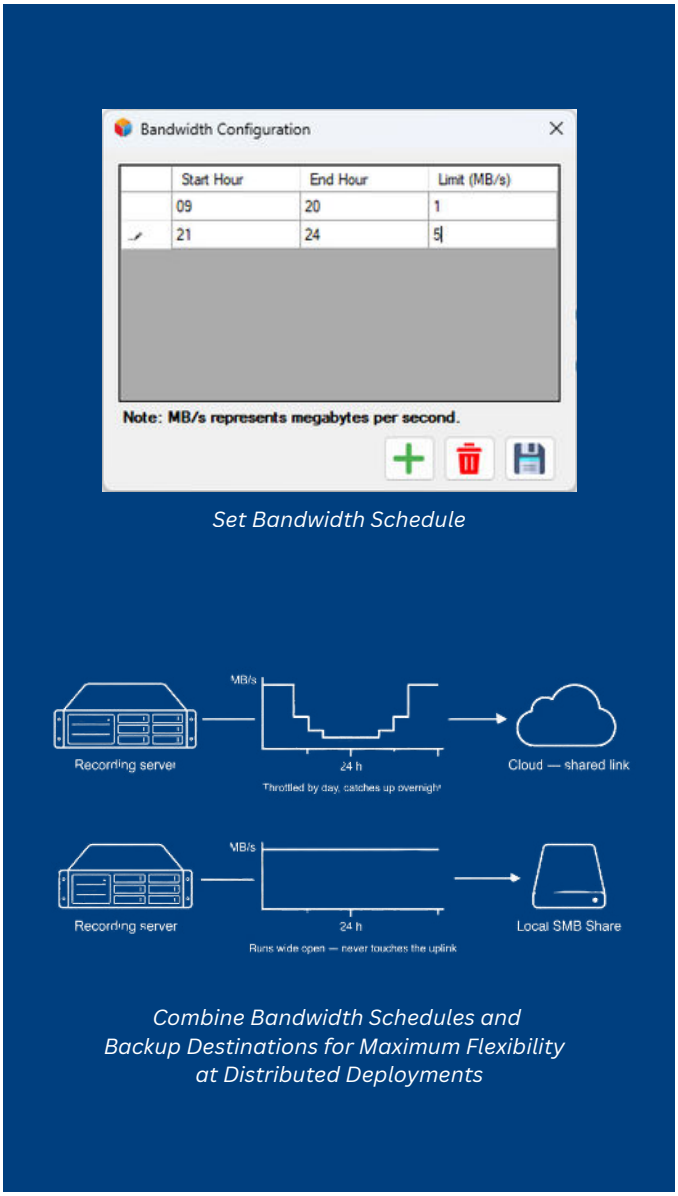
Back up each recorder to the storage that fits its needs. Nidhi supports AWS S3, any S3-compatible object storage, and SMB network shares. Because the destination is set per recorder, different recorders can target different storage. Send high-value footage to durable cloud storage, keep regulated sites on a local SMB share to meet data-sovereignty requirements, and let remote recorders over thin network links back up locally rather than straining the connection. You match each recorder to the destination that best fits its cost, compliance, and bandwidth realities.



Per-recorder Backup Options

Bandwidth-Aware Scheduling

Backup shouldn't compete with the rest of your network. Nidhi's bandwidth scheduler accepts multiple time windows, each with its own MB/s ceiling, so you decide how much capacity backup may use and when. A typical pattern throttles tightly during business hours, opens up overnight when the network is quiet, and stays moderate in the evening, thus letting backups catch up fast off-peak without disrupting daytime operations. And because the schedule is set per recorder, every site in a distributed deployment can follow its own schedule, tuned to its destination. A recorder pushing to the cloud over a shared link can stay conservative by day and catch up overnight, while one backing up to a local SMB share never touches the uplink and can run wide open around the clock.



Set Bandwidth Schedule

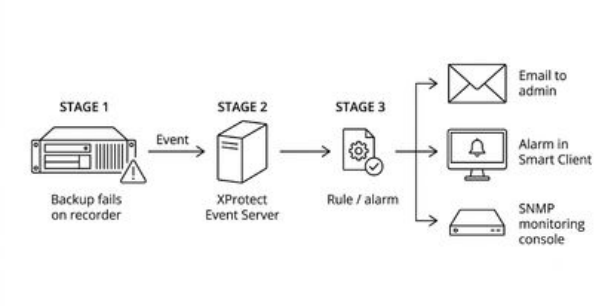
Combine Bandwidth Schedules and Backup Destinations for Maximum Flexibility at Distributed Deployments

Nidhi

Backup. Restore. Move On.

Native XProtect Alerting

Nidhi reports backup failures as native XProtect events, so alerts reach administrators through the system they already monitor. When a backup job fails, the Nidhi agent sends a generic event to the XProtect Event Server. XProtect is set up so that this event triggers a standard rule or alarm that can email the administrator, raise an SNMP trap to a monitoring console, or both. Because the alert flows through XProtect's own event and rule engine, backup failures surface alongside every other system alarm and are delivered the same way as the rest of your deployment's alerts.



XProtect Integrated Notifications

You Own Your Storage

Footage is sent to your AWS S3, S3-compatible, or SMB storage. Vega never holds, manages, or accesses your data.

Scales without Limit

Each recorder runs its own agent, so adding recorders adds no central bottleneck.

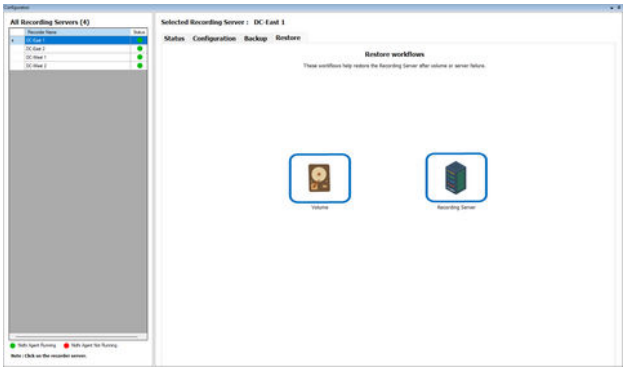
Decentralized by Design

Every recorder backs up and restores on its own; no single point of failure in the backup system itself.

XProtect Variant Agnostic

Nidhi works on all XProtect Variants.

Restore Workflows

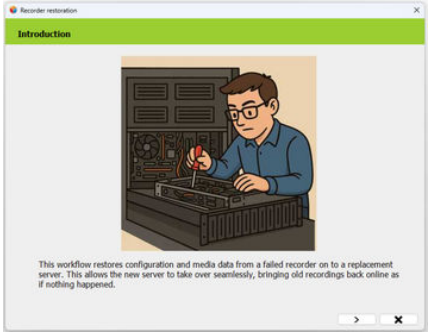


Volume Restore

When a disk fails, you don't lose its footage. Nidhi restores a backed-up storage profile to a replacement volume, bringing the recordings on that disk back online without touching the rest of the recorder.

Recorder Restore

When an entire recorder fails, Nidhi rebuilds it. It restores every storage profile for the failed recorder onto replacement hardware, bringing its configuration and recordings back so the new server takes over seamlessly; old recordings are online again as if nothing happened.



XPort

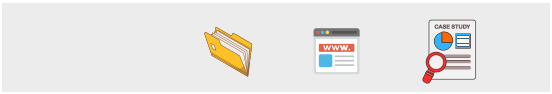
Content Portability Made Easy

Introduction

At XProtect deployments, there often arises a need to migrate content from SQL and Media databases between different hardware/software platforms. This can include scenarios such as migrating a deployment from outdated hardware to new infrastructure, consolidating multiple XProtect implementations into a single site, or implementing a more complex workflow that retains particular hardware while replacing others.

These migrations require significant expertise, often resulting in costly and time-consuming manual efforts for system integrators.

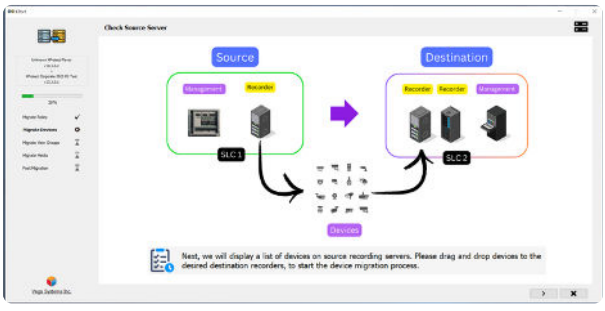
We introduce **XPort**—a solution designed to streamline this process. XPort automates the migration, **cutting costs by up to 60%**, saving time and resources while ensuring a smooth transition.



Key Features

Seamless XProtect Integration

Seamless integration with Milestone XProtect, simplifies use by offering a single pane of glass experience.



Pricing Model

- One-year migration license.
- One base license per destination SLC.
- One site license per source recorder.

Migration Made Simple

Video security administration and IT infrastructure management often require different skill sets. Currently, migration processes demand expertise in both areas. XPort simplifies this by making migration workflows accessible to video security administrators. There's no need to restore databases or edit XML or configuration files—XPort does all the heavy lifting.

Customizable, Precision Migration

XPort's API-based approach offers precise control over migration content. The user can choose to migrate just a few devices, specific roles, or every role. The user can also decide whether to include views, privacy masking, PTZ presets, or other specific content in the migration. Technicians have the flexibility to perform migrations exactly as needed.

Centralize Siloed Deployments

Customers that manage multiple siloed XProtect deployments, each tied to its own Software License Code (SLC) eventually, may seek to consolidate these into a single deployment. XPort simplifies this previously manual and challenging process, enabling seamless content merging from multiple databases—a task impossible with traditional brute-force database backup and restore methods.

Universal XProtect Compatibility

XPort is designed to work seamlessly with every flavor of XProtect, ensuring that no matter which version or edition is used, XPort can handle migration needs.

XPort

Content Portability Made Easy

One to One Migrations

From one source database to one destination database.

Same Product+ Same Version

For instance, XPort allows migration from Prof+ 2023 R2 on an old server to Prof+ 2023 R2 on a new server.

Same Product + Diff. Version

E.g., Prof+ 2023 R2 → Prof+ 2024 R1. Please get in touch with us to confirm specific compatibility.

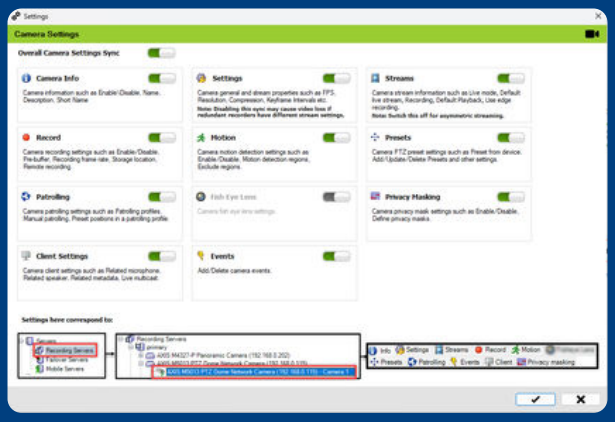
Diff. Product+ Same Version

E.g., Expert 2023 R2 → Corp 2023 R2. Check with us for specific compatibility.

Cloud Migration

Fine Grained Control

Migrate just a chosen set of devices, roles, features, or migrate everything.

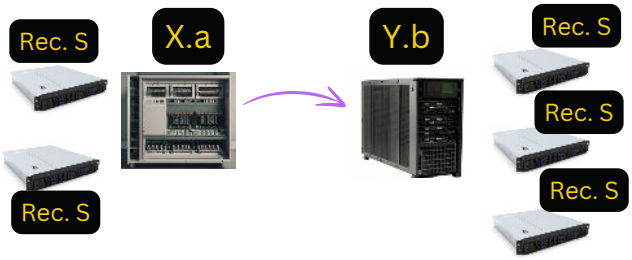


On-Prem to cloud migrations are supported.

Diff. Product + Diff. Version

E.g.: Prof+ 2023 R2 → Corp 2024 R1. Check with us for specific compatibility.

Distribute Devices



As part of the migration workflow, users can redistribute devices from fewer recorders to more or consolidate more recorders into fewer.

XPort

Content Portability Made Easy

Many to One Migration

From many source databases to one destination database.

Site Amalgamation

XPort simplifies the consolidation of siloed XProtect deployments by helping merge information from multiple databases into a unified system. It also supports complex workflows in which recording servers from the original siloed sites are retained within the consolidated site, with all recordings kept intact.

One to Many Migration

From one source database to many destination databases.

Site Splitting

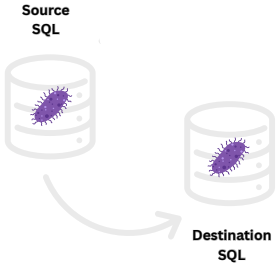
Distribute devices under a single SLC across multiple deployments. Migrate specific roles to one site and allocate others to different sites as needed. Note: Multiple XPort licenses are required for this workflow.

Cybersecure Migrations

XPort moves only the objects you select—cameras, roles, views—via XProtect's APIs. By transferring clean metadata instead of cloning the entire database, it leaves behind dormant malware, stealth accounts, and rogue SQL code that a traditional backup-and-restore would copy wholesale.

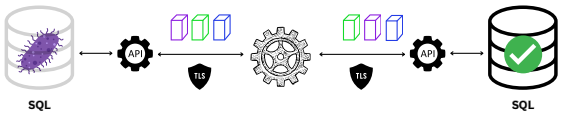
The Security Problems with SQL Restore

SQL backup/restore rapidly propagates any malware, corruption, or malicious users already present in the source site.



The XPort Method

XPort extracts meaningful objects (such as cameras, roles, and views) from the source SQL using the XProtect API. These objects are then deposited into the destination SQL via the destination's API. The method filters out latent malware from the source and prevents it from propagating to the destination.



XPort

Content Portability Made Easy

Media Migration

Starting with 5.0, XPort fully supports media database migration as part of the automated migration process.

Universal payload support

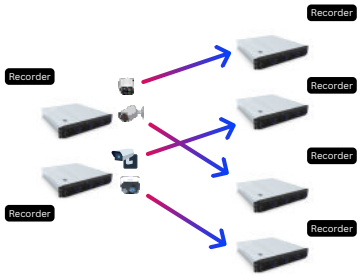
Migrate video, audio, metadata, and I/O together in one operation.

Bandwidth throttling

Limit transfer rates to protect production traffic during migration.

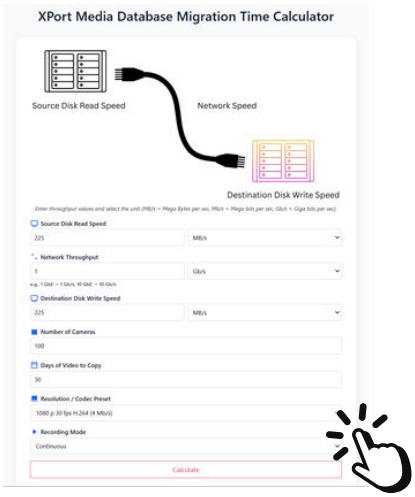
Flexible fan-in / fan-out

Map any combination of source recordings to destinations for versatile transfers.



Migration-time estimator

Receive a realistic timeline based on footage volume, disk speeds, and network speed.



Case Studies

School Districts

A Midwestern U.S. school district used XPort to consolidate multiple XProtect systems into a unified deployment with site-based recorders, resolving access and monitoring confusion. The migration, which would have taken over a month and cost tens of thousands, was completed quickly and cost-effectively

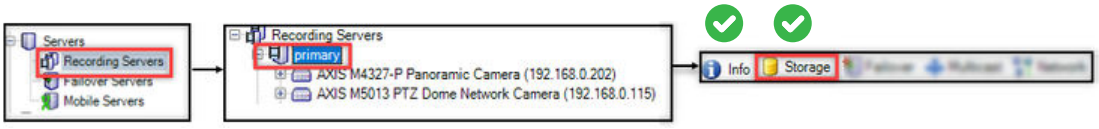
Smart Cities

A major U.S. city used XPort to consolidate fragmented Milestone XProtect sites, automating roles, devices, views, and media migration. The process, which previously took over three weeks, was completed in under two days with over 60% cost savings.

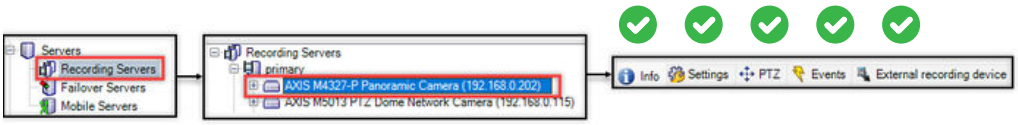
Feature Wise Migration Support Matrix

The list below details all the features that XPort can currently migrate. If a feature is not listed, it is not yet supported. For instance, Rules, Alarms, Smart Client profiles, Evidence Lock, Matrix, and Smart Wall are not currently supported, but support for these features will be added in future releases. The blurred categories below indicate features not currently supportable due to a lack of XProtect API support, though they may become supportable in the future.

Recording Server



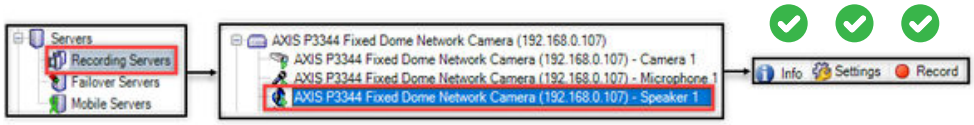
Hardware



Camera

Microphone

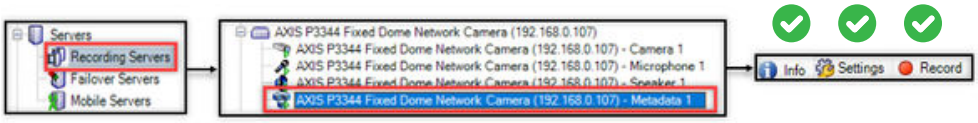
Speaker



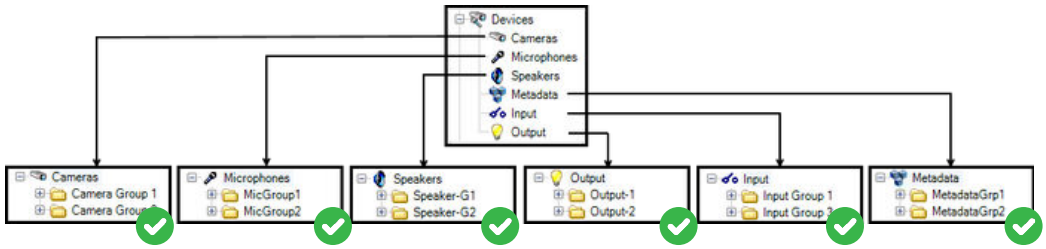
Input

Output

Metadata



Groups



Roles

Views

Vega Systems Inc.

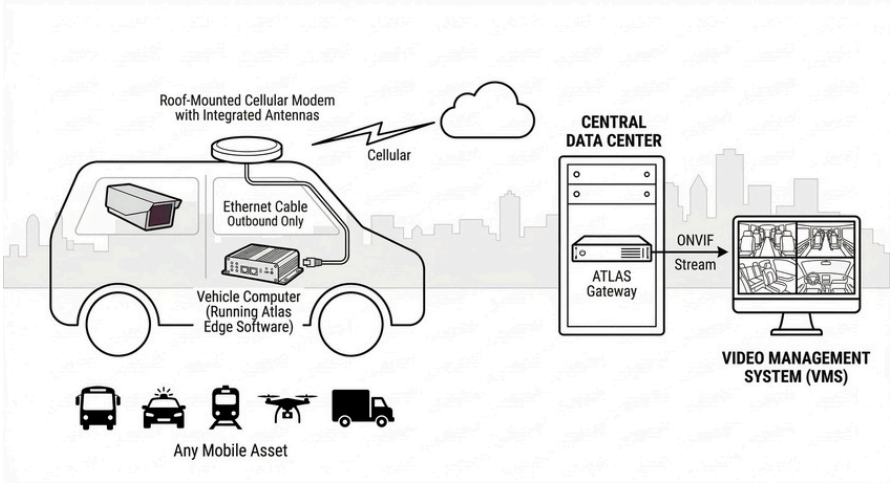
FOLLOW US

https://vega25.com
+1-669-256-2357
info@vega25.com

v 072625

Atlas

Make every camera local



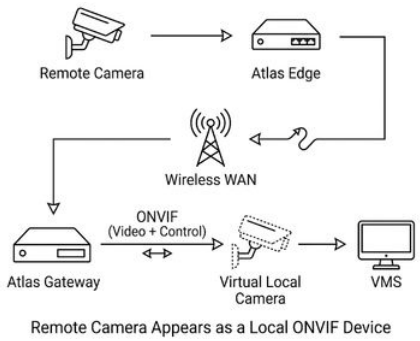
A SOC has two kinds of cameras. Local ones just work. The VMS finds them, shows them, controls them; nothing special required. Remote cameras over cellular or satellite are the opposite: custom setup, constant bandwidth and cost worries, and video that freezes when the link dips.

Atlas erases the divide. Every remote camera appears to the VMS as if it were on the local network, and each stream adapts to available bandwidth in real time; degrading gracefully instead of freezing, within the limits you set. One class of camera. Wherever it lives, it behaves like it's local to your SOC.

Key Features

ONVIF Virtualization

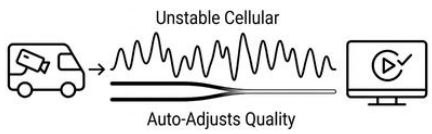
Atlas virtualizes remote cameras as local ONVIF devices. The VMS connects to them exactly as it would a local camera, while Atlas transparently delivers video streams and camera controls from the edge.



Remote Camera Appears as a Local ONVIF Device

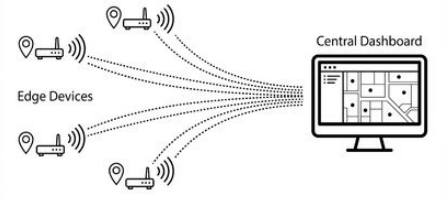
Adaptive Stream

Cellular networks are chaotic. Atlas detects jitter and packet loss in real time, dynamically adjusting streams to maintain smooth video even in low-bandwidth zones.



Centralized Management

Manage, monitor, and track every Atlas edge device from a single dashboard — whether deployed across a city or around the world. View device locations, check health status, and push configuration updates remotely.



One Dashboard — Every Device

Pricing Model

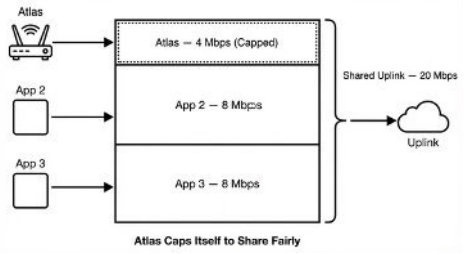
Monthly subscription per edge camera

Atlas

Make every camera local

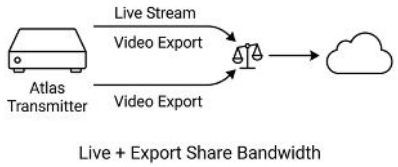
Bandwidth Capping

Each Atlas transmitter lets users set a bandwidth cap — essential when multiple applications share the same uplink. Atlas respects the limit and shares fairly.



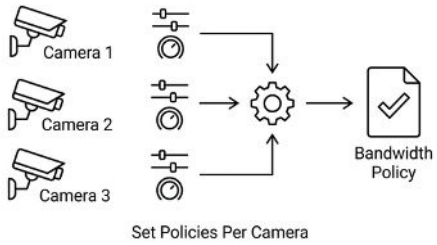
Co-operative Export

Co-operative edge video export shares bandwidth with real-time streams in a user-specified manner — live video and exports work together, not against each other.



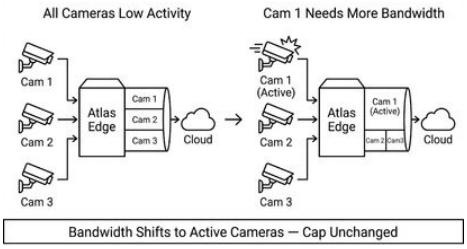
Per-Camera Policies

Users can specify bandwidth caps and sharing policies for each camera on each edge device, providing full control over resource allocation.



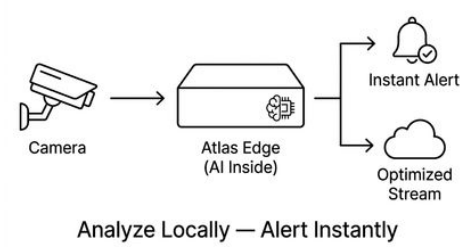
Dynamic Bandwidth Allocation

When cameras have more activity, they need more bandwidth. Atlas dynamically reallocates video bandwidth to cameras that require it, while still respecting the overall cap.



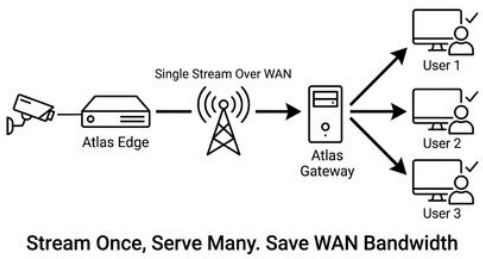
Edge AI

Run video analytics inside the Atlas Edge device — analyzing full-resolution video before transmission. Detect events locally and send alerts instantly, without relying on cloud processing or bandwidth-constrained streams.



Multi-User Streaming

Multiple users view real-time video from a single Atlas Gateway, without pulling duplicate streams across the WAN. One stream from the edge serves many viewers, saving bandwidth and reducing load on remote devices.

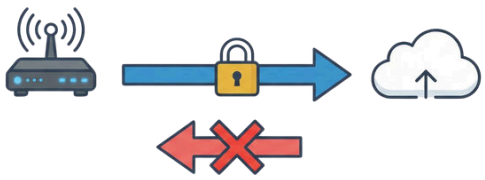


Atlas

Make every camera local

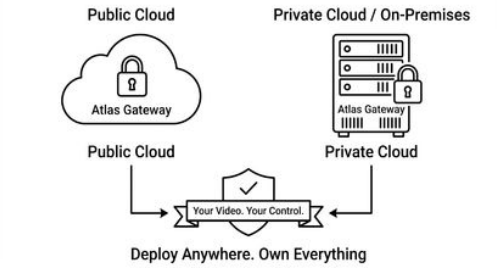
Outbound-Only Cloak

Stop exposing your fleet to network scanners. Atlas creates a secure tunnel from the inside out: zero inbound ports, zero public IP addresses, and no reverse proxy.



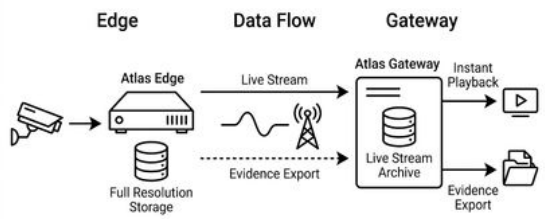
Flexible Cloud Deployment

Deploy the Atlas Gateway in the public cloud or your private data center, your choice. Either way, only you have access to your video. Full data ownership, zero compromise.



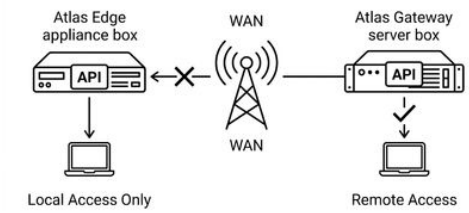
Dual Storage Architecture

Atlas stores full-resolution video at the edge for evidence-grade retrieval, exportable anytime for playback. Lower-bandwidth live streams are also stored at the Gateway for instant playback. Two locations, complete coverage.



REST API

Programmatic access at both ends. The Gateway API is available for remote setup, configuration, and monitoring. The Edge API is restricted to the local camera network.



Availability

Jan 2027

Contact Us

Resources & Support

Contact

vega25.com

docs.vega25.com

info@vega25.com

+1-669-256-2357

6455 Almaden Expressway, Ste 205

San Jose, CA 95120

Connect with us

linkedin.com/company/vega-systems-inc.

youtube.com/@vegasystemsinc

Vega Systems Inc.

FOLLOW US

https://vega25.com

+1-669-256-2357

info@vega25.com

v 062926