Vega Systems Inc.

Cyber-Secure Redundancy

Date Created:
June 11, 2025

Prepared by:
Vega Systems Inc

sales@vega25.com

669-256-2357

6203 San Ignacio Avenue Suite 110, PMB # 1319 San Jose, CA 95119

Table of Contents

Executive Summary 3
Selective Object Synchronization 4
The Cyber Risk in “Copy-Everything” Replication 4
Selective Object Synchronization 5
Eight Common Attack Vectors 6
RMF’s Object-level Control 14
Datacenter Isolation 16
Clustering Requires Broad and Persistent Trust 16
RMF Service Architecture → Narrow, Explicit Trust 17
Conclusion 18
About Vega Systems 19

Executive Summary

Unlike traditional high-availability architectures that replicate everything—including mistakes and malware—Vega Systems' **Redundancy Management Framework for XProtect** (RMF) provides cybersecurity by design. 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.

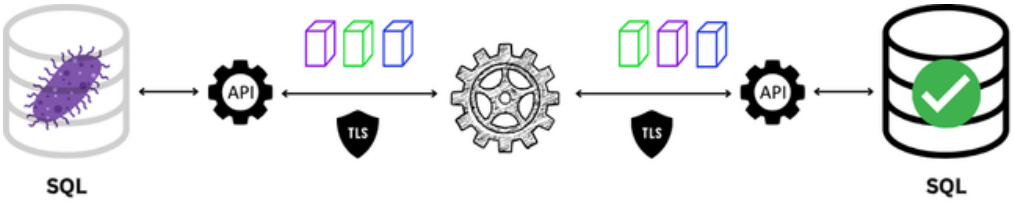

Figure 1: Selective Object Synchronization

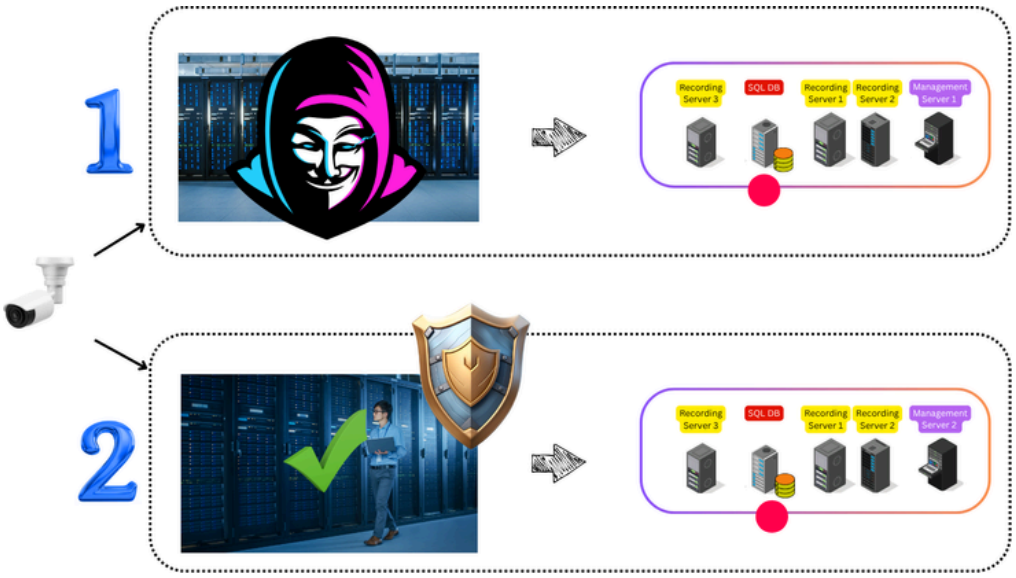

Figure 2: Data Center Isolation

Selective Object Synchronization

RMF offers an alternative to traditional byte-for-byte SQL replication, featuring object synchronization for Milestone XProtect deployments. By pushing each object (e.g., camera, view, role) through Milestone's native APIs, RMF enables selective, API-validated replication with built-in safeguards that minimize the spread of cyber threats.

The Cyber Risk in "Copy-Everything" Replication

Traditional SQL replication engines, such as SQL Server Always On Availability Groups, Microsoft Failover Cluster with shared SAN storage, VMware vSphere HA/vMotion on shared datastores, and SQL Server Log Shipping, were designed for continuity at any cost: they stream every byte, healthy or hostile, from a primary database to its standby in near real-time. This blind fidelity works wonders for availability, but it also 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.

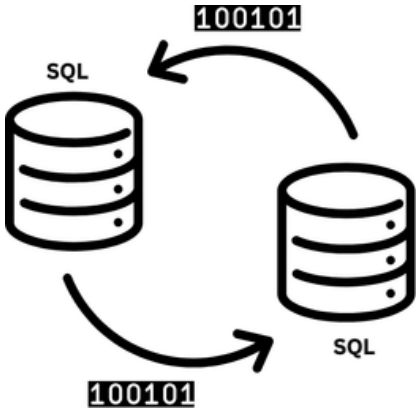

Figure 3: 'Copy-Everything' Replication

Selective Object Synchronization

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

This fine-grained pipeline operates over a single HTTPS port with narrowly scoped tokens —no open database endpoints, no sysadmin logins—eliminating the lateral-movement footholds that classic replication leaves exposed. In practice, you keep the business intent ("copy the new camera," "add this schedule") while stripping away the accidental or malicious noise that turns replicas into unwitting accomplices.

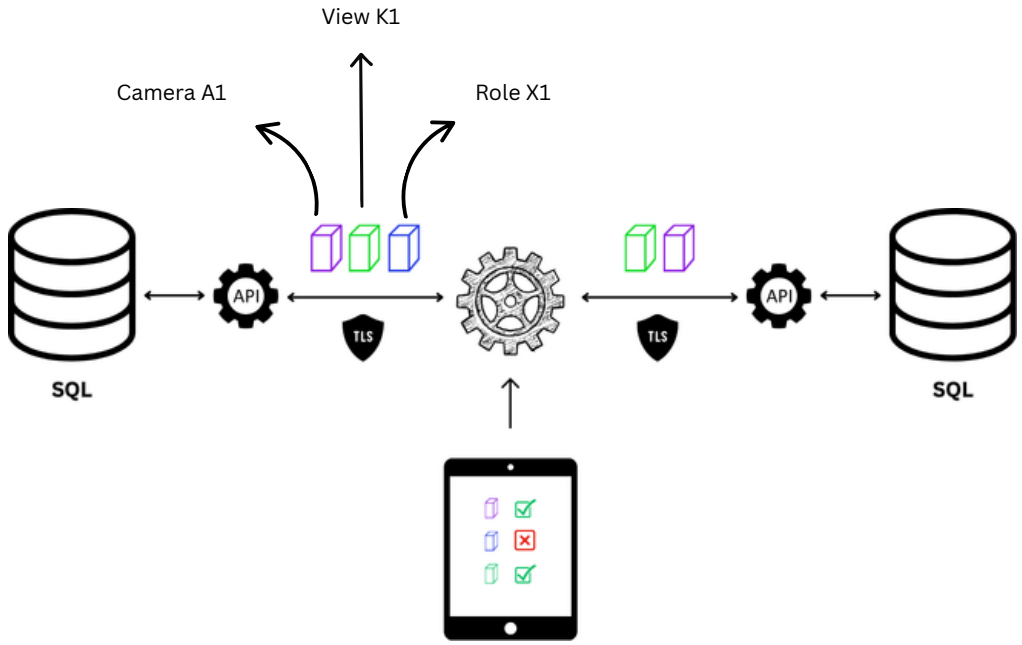

Figure 4: Object Synchronization

Eight Common Attack Vectors

The sections below walk through eight high-impact attack scenarios to illustrate exactly how RMF's object-first model contains damage to the source node instead of broadcasting it to an entire fleet.

A. Ransomware-Locked Data Pages

In this attack mode, ransomware encrypts the raw data pages of the database.

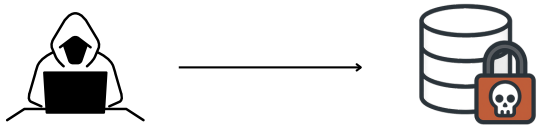

Figure 5: Locked DB

With full-image replication

Encrypted pages stream to every replica; all copies are locked.

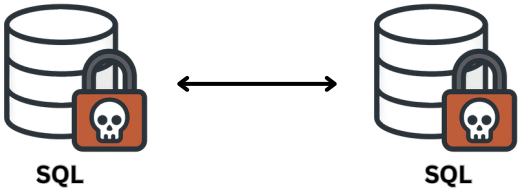

Figure 6: All Copies Locked

With RMF's Object-level synchronization

Raw pages never move. API calls to the primary database fail. Standby stays clean and can be promoted.

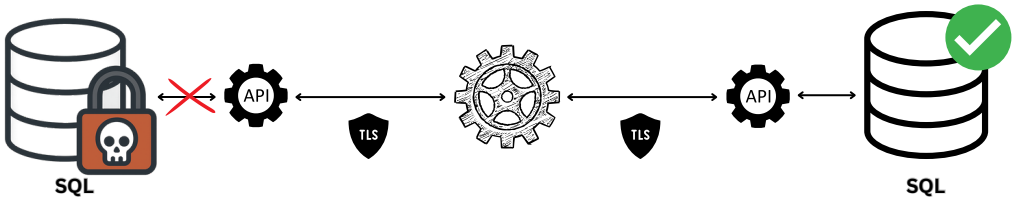

Figure 7: Backup Unaffected through object fetch

B. Rogue Admin Account Creation

In this attack mode, malware adds a rogue admin to the database.

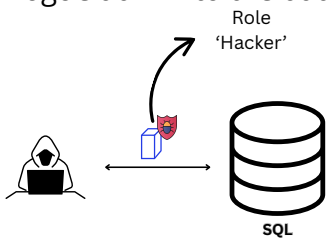

Figure 8: Rogue Admin Added

With full-image replication

All copies end up with the rogue admin. Every failover site is compromised.

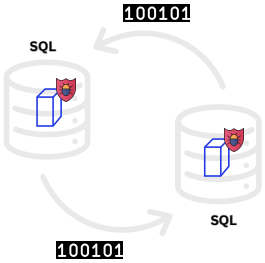

Figure 9: Rogue Admin Replicated

With RMF's Object-level Synchronization

Per-object replication control allows administrators to establish a policy that mandates manual confirmation for replicating the Users/Roles category—rogue accounts are quarantined.

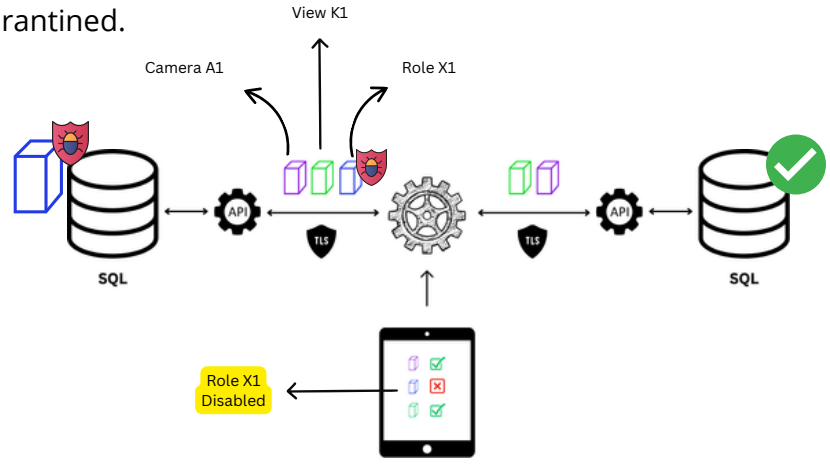

Figure 10: Rogue admin blocked from backup

C. Stealth Procedure Injection

In this attack mode, a booby-trapped procedure slips into the primary database.

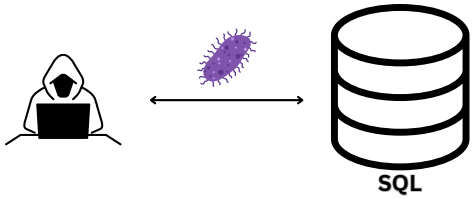

Figure 11: Stealth Procedure Added

With full-image replication

The hidden backdoor spreads every where.

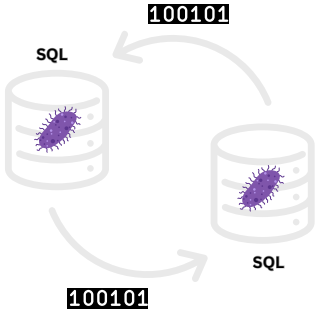

Figure 12: Stealth Procedure Spreads

With RMF's Object-level synchronization

Application APIs expose no DDL, so the procedure can't propagate.

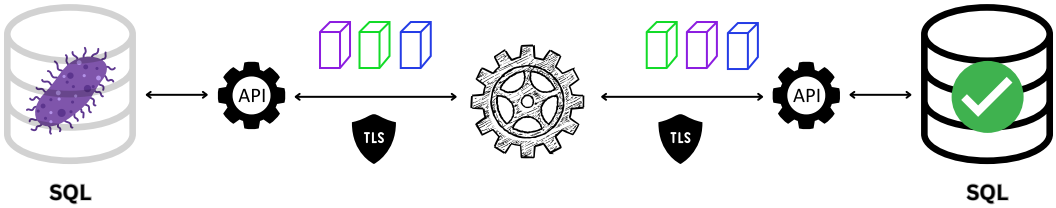

Figure 13: Stealth procedure does not propagate

D. Privilege Escalation via DB Ports

Replication needs a super-admin password and an open DB port.

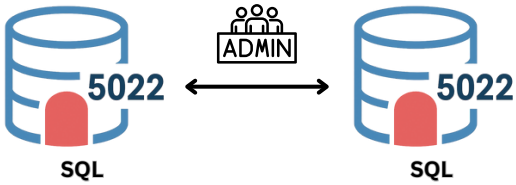

Figure 14: Exposed DB Port

With full-image replication

The attacker steals the sysadmin-level replication account via an open port 5022 and pivots into other databases.

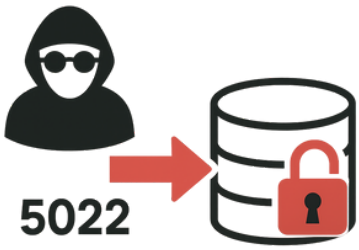

Figure 15: Hacker Exploits Open Port

With RMF's Object-level synchronization

The sync connector only makes an outbound HTTPS call with a short-lived, narrow-scope token. Even if stolen, the damage is limited, and no DB port is open.

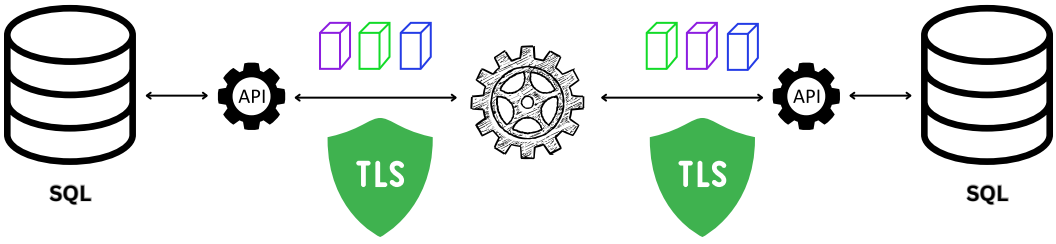

Figure 16: Scoped TLS port on the API, not DB

E. Bulk Configuration Wipeout

Malicious user wipes content from primary database.

Figure 17: Hacker Erases DB

With full-image replication

DELETE is instantly replicated everywhere.

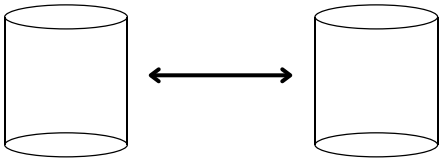

Figure 18: Sync erases back up

With RMF's Object-level synchronization

Per-object replication control allows administrators to control the replication of objects and limit blast radius.

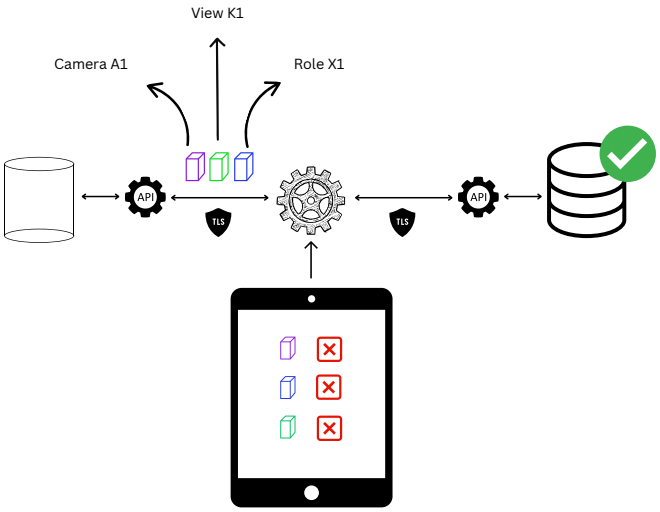

Figure 19: Backup stays clean

F. Schema Tampering and Table Corruption

Malicious user corrupts SQL tables.

Figure 20: Hacker Corrupts DB

With full-image replication

Bad datatype/column change replicates immediately, breaking queries cluster-wide.

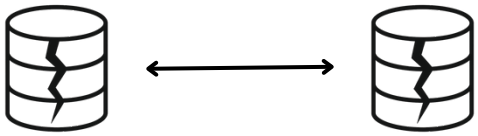

Figure 21: Corruption Spreads

With RMF's Object-level synchronization

Vendor API calls fail while trying to retrieve the object, and corruption is not replicated even if object-level controls are disabled.

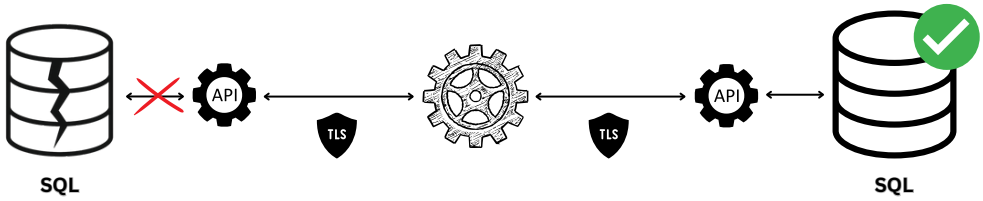

Figure 22: Backup Tables Uncorrupted

G. Sensitive Data Oversharing

With full-image replication

A system that does full-image replication sends every row and column in the database to the secondary site, whether or not that site is cleared to hold the information. If the primary contains PII, payroll data, export-controlled CAD files, or patient records, the replica now does too—even if it sits in a lower-trust network, another country, or a public cloud.

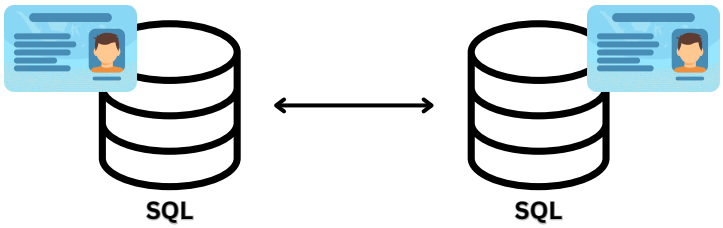

Figure 23: PII Everywhere

With RMF's Object-level synchronization

Per-object selectors – You define which object categories (e.g., Cameras, Policies) can replicate.

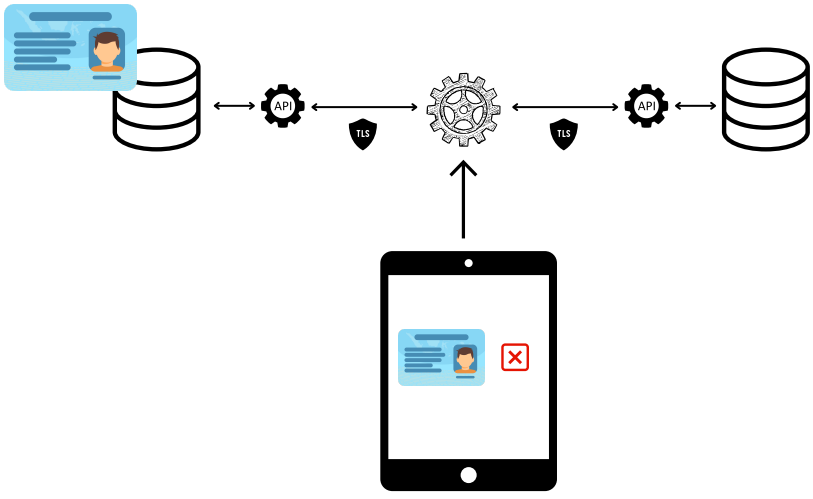

Figure 24: Admin Controls PII location

H. Standby Disk Overfill Attack

The standby server's drive fills up (maybe logs weren't cleaned, maybe an attacker dumped junk files), and it stops accepting the change data streamed from the primary.

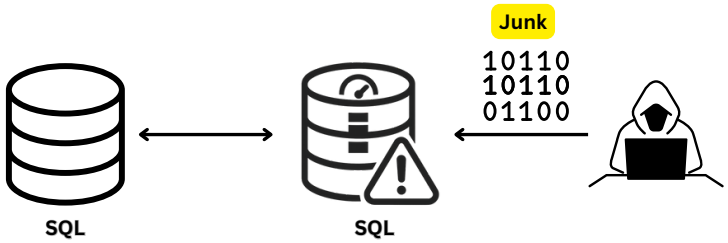

Figure 25: Hacker fills Standby DB Disk

With full-image replication

The primary continues to log new transactions, but because the standby never acknowledges them, its own transaction log can't be cleared. That log swells until the primary's disk space is exhausted as well, turning a single "full disk" on the backup into a complete outage for the entire system.

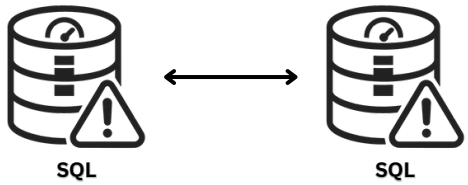

Figure 26: Primary fills and stops working

With RMF's Object-level synchronization

Because the primary and standby are no longer joined at the hip by an ever-growing transaction log, a full disk on the backup becomes a localized maintenance issue instead of a cascading system failure.

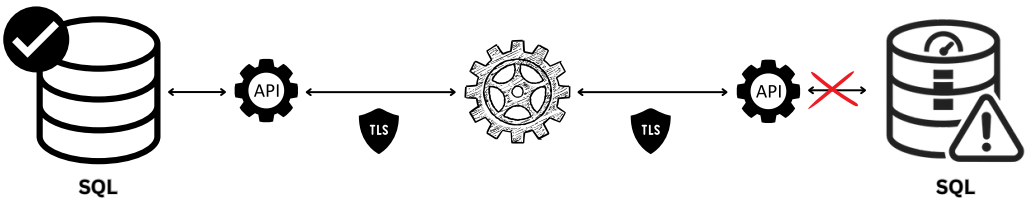

Figure 27: Primary Stays Functional

RMF's Object Level Control

RMF provides object-level control over individual devices, device groups, views, and roles, allowing users to filter replication of these objects.

Devices

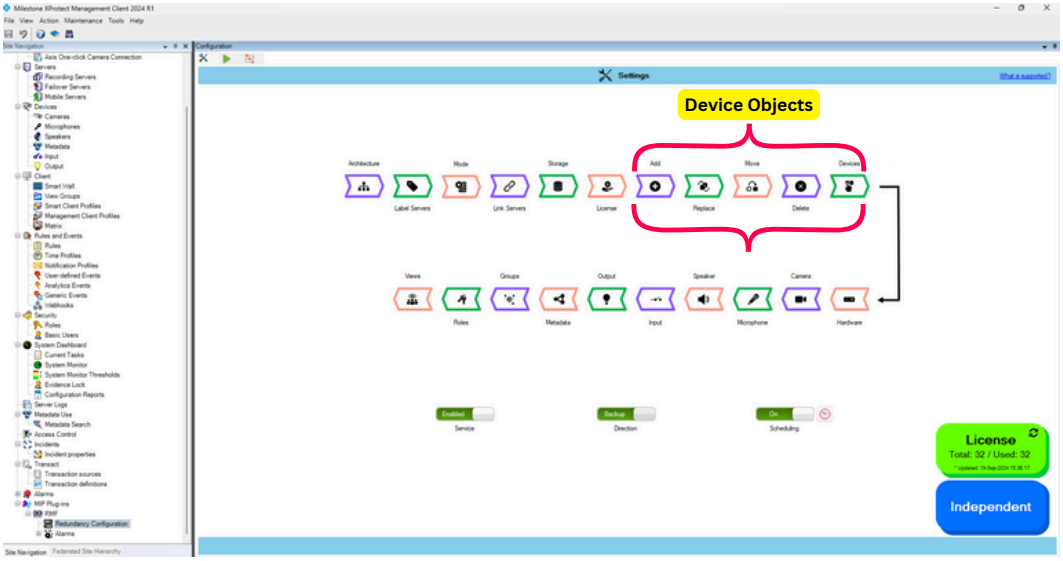

Figure 28: Device Object Support

Groups

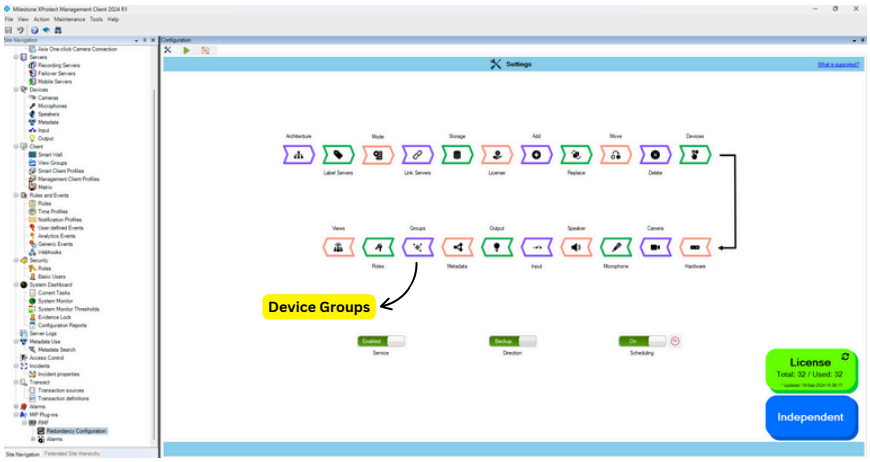

Figure 29: Device Groups Object Support

Roles

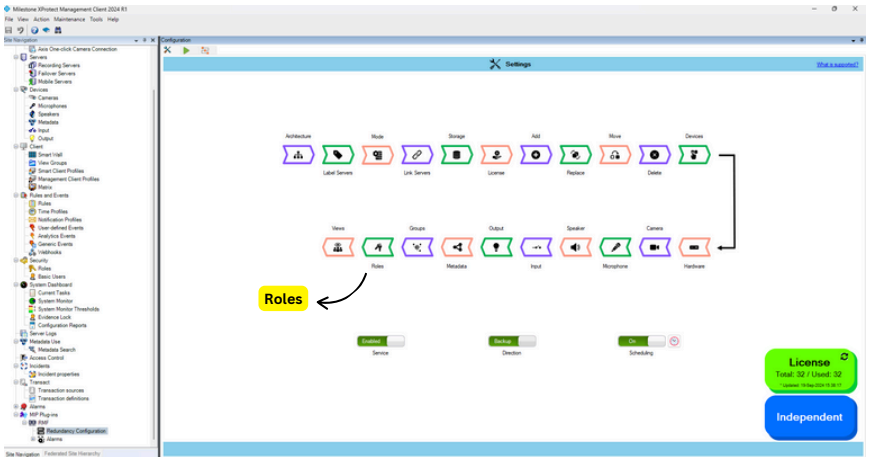

Figure 30: Roles Object Support

Views

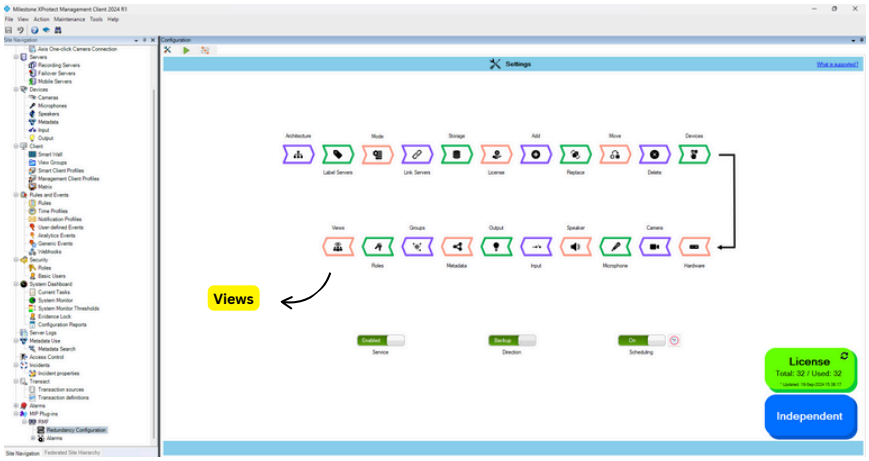

Figure 31: Views Objects Support

Datacenter Isolation

A large percentage of deployed high-availability architectures rely on cross-site service clustering, which increases cyber risk by creating shared attack surfaces. RMF, when deployed in Federated or Independent architectures, takes a different approach: each data center operates independently, with no shared clustering or storage. This isolation blocks lateral movement during an attack and ensures a clean, uncompromised environment is always available for recovery.

Clustering Requires Broad and Persistent Trust

Traditional cross-site clustering relies on deep system-level integration between data centers, typically involving shared authentication domains, real-time database replication, and mutual access to control services and storage. For the cluster to function seamlessly, each site must **implicitly trust the other across all layers** of the stack. This broad trust model means that any compromise—whether through malware, misconfiguration, or insider threat—can rapidly propagate across the entire cluster. The exact mechanisms that deliver high availability also erase meaningful security boundaries between sites, violating zero-trust principles and increasing the blast radius of a breach.

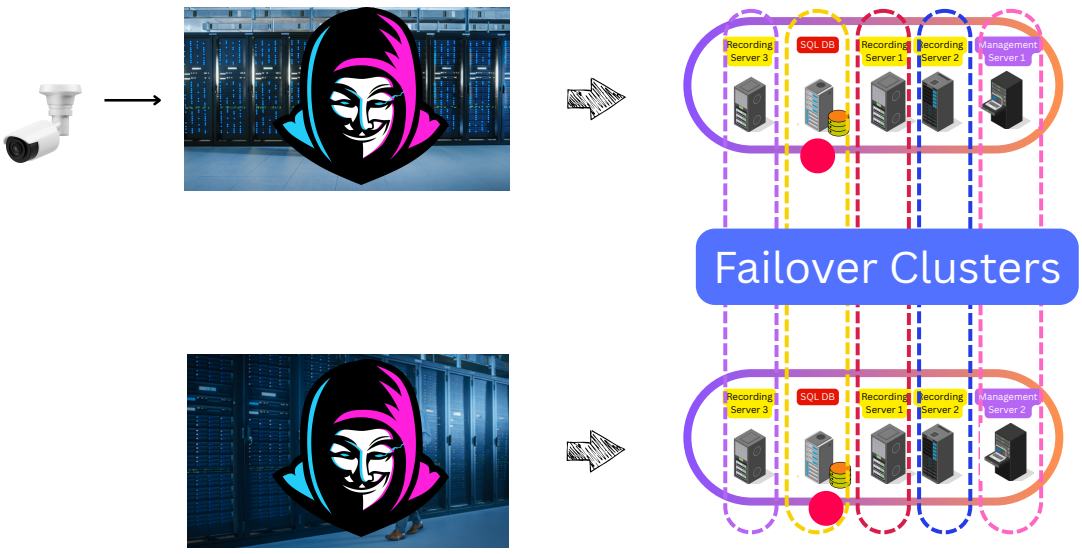

Figure 32: Clustering - Uncontrolled Blast Radius

RMF Service Architecture Enforces Narrow, Explicit Trust

The RMF solution (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. Even if one site is compromised, the other remains fully insulated. By eliminating the need for persistent cross-site trust, RMF aligns with zero-trust architecture and provides a far stronger foundation for cybersecurity and resilience.

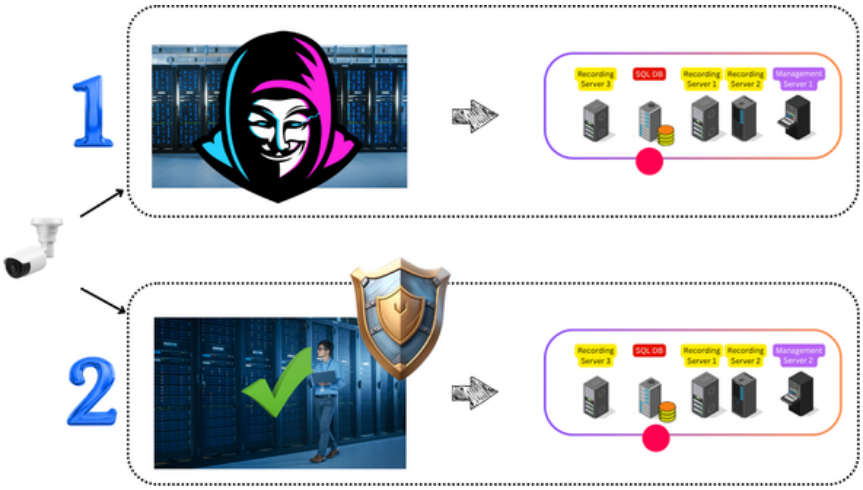

Figure 33: RMF Limits Blast Radius

Conclusion

Classic replication and clustering ensure availability but not security.
Byte-for-byte failover copies everything, including malware, rogue accounts, and corrupted data. Clustered architectures increase cyber risk by creating shared attack surfaces.

Vega Systems' RMF stops threats at the source. Instead of cloning entire databases, RMF syncs only what's safe—one validated object at a time.

- *Granular control* – Filter, block, or quarantine specific roles, devices, or views.
- *Secure architecture* – No open SQL ports or admin-level replication accounts.
- *Failover-ready* – Keeps your redundant site clean and ready for promotion.
- *Reduce the trust surface* – Reduce the trust surface and prevent lateral movement between sites.

Don't just replicate. Fortify.
With RMF, system integrators and resellers can deliver high-availability deployments that are cyber-secure by design without adding complexity.

Ready to see it in action?
Contact Vega Systems at sales@vega25.com or +1 669-256-2357 to schedule a live demo, run a proof-of-concept in your environment, or receive a detailed risk-reduction assessment tailored to your deployment.

About Vega Systems

Vega Systems Inc. develops specialized software solutions that improve the security, resilience, and manageability of video surveillance systems. Located in San Jose, California, Vega concentrates on mission-critical deployments where uptime and cyber protection are essential. Its main products—including the Redundancy Management Framework (RMF), XPort, and SureStream—are trusted by clients across various sectors, including enterprise, transportation, education, and government worldwide.

To learn more, visit www.vega25.com or contact us at sales@vega25.com.