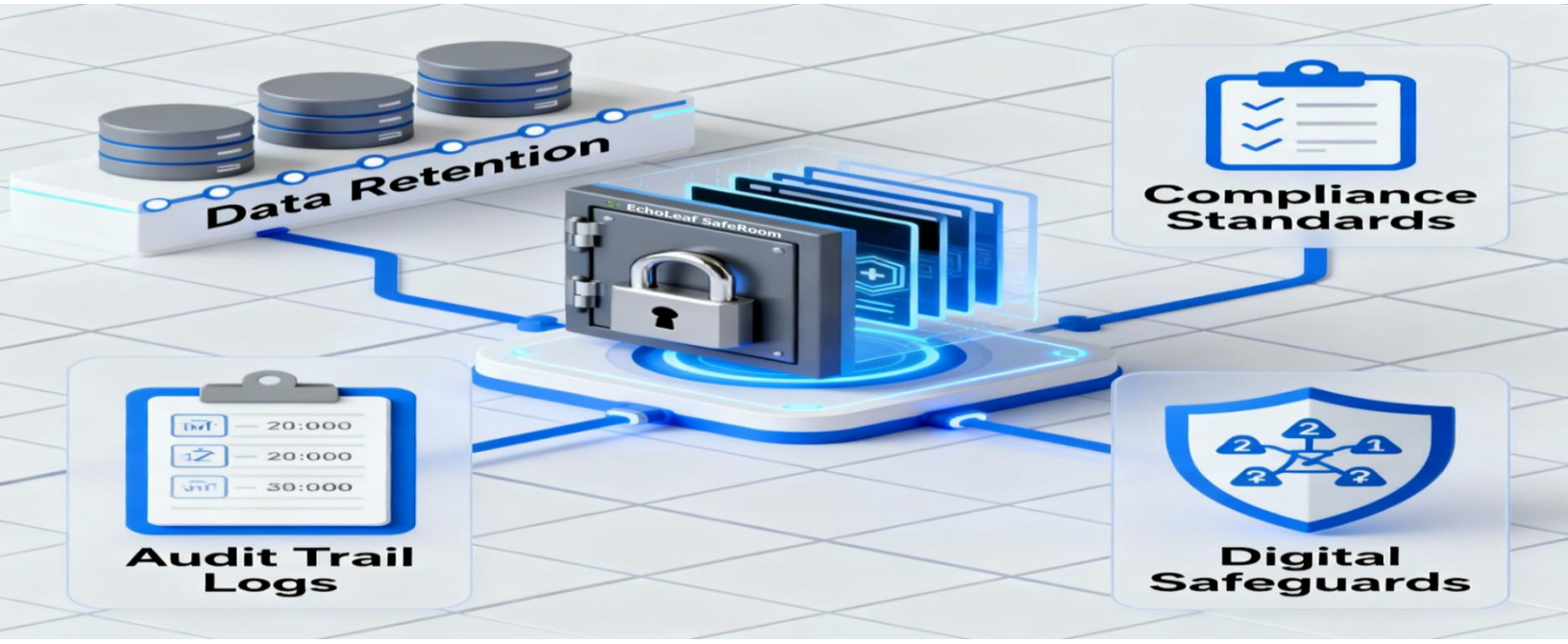
Safeguarding the Truth:

Solving the Data Retention and Compliance Challenges of Modern Video Surveillance



By Douglas Korte, CSO

Executive Summary

The video surveillance industry faces an unprecedented data storage crisis. With the global video surveillance market projected to reach $88.71 billion by 2030, growing at a CAGR of 8.5%, organizations are overwhelmed with data while simultaneously facing increasingly stringent compliance requirements and escalating cyber threats.

High-resolution 4K and 8K cameras, extended retention mandates, and the proliferation of surveillance systems across every industry have created a perfect storm: **exponential storage growth, skyrocketing costs, regulatory compliance challenges, and the need for assured integrity and greater accessibility**. Traditional disk and cloud-based storage solutions cannot keep pace economically or securely and are becoming economically and operationally unsustainable. Long-term video archives are now measured in petabytes, not terabytes. With ransomware and insider threats targeting online data stores, simply keeping everything on spinning disks or the cloud is no longer viable.

EchoLeaf Systems offers a revolutionary solution that addresses all these challenges simultaneously through our SafeRoom™ LTO-based physical air-gap storage technology. By combining EchoLeaf's patented virtualization and workflow orchestration, the immutability and cost efficiency of modern LTO tape with true physical isolation, and easy scaling for operations of all sizes, EchoLeaf provides ultimate protection and resiliency, while dramatically reducing long-term storage costs and ensuring compliance with the most stringent data retention requirements.

This white paper examines the evolving challenges of video surveillance data management and demonstrates how EchoLeaf Systems uniquely solves each of these critical problems.

The Key Data Challenges in Video Surveillance

Challenge 1: Growth Outpacing Infrastructure

The video surveillance industry is experiencing unprecedented data growth driven by three primary factors:

1. **Higher Resolution Cameras**: The shift from standard definition to HD, 4K, and now 8K cameras has dramatically increased storage requirements. A single 4K camera recording at 30fps generates up to **1 TB of data per day**.
2. **Increased Camera Counts**: Organizations are deploying more cameras than ever before. Large campuses, municipalities, and industrial operators now deploy **hundreds or thousands** of cameras. In the United States alone, there are more than 30 million surveillance cameras capturing 4 billion-plus hours of footage each week.
3. **Longer Retention Requirements**: Regulatory mandates and operational needs are extending retention periods across all industries. Retention periods that were once 7–30 days now commonly extend to **6–24 months (or longer)** for compliance, investigations, or analytics.

Industry reports estimate global video surveillance data will exceed 10 zettabytes by 2030, maintain a CAGR of 12.2-17.3% from 2025 to 2033, dwarfing every other form of enterprise content. A key driver for this growth is the increasing adoption of edge AI, including advanced behavior recognition, anomaly detection, AI-driven crime prediction, and others aimed at enhancing data security and privacy. The integration of AI and machine learning into video surveillance systems is driving robust growth with advanced video analytics and real-time monitoring capabilities.

The result: unsustainable costs, operational complexity, and increased cybersecurity exposure for organizations that continue to rely on online storage architectures.

Challenge 2: Unsustainable Storage Costs

Keeping surveillance videos on high-performance disk arrays or in cloud tiers designed for hot data is cost prohibitive. Even with compression and tiering, the economic model quickly breaks down beyond a few hundred terabytes, and accessibility suffers with delays, complexities, and added costs.

The Disk Storage Cost Problem

Storing high-resolution video on spinning disk arrays for extended periods creates multiple cost pressures:

- **Hardware costs:** Enterprise-grade disk systems are required for continuous video recording.
- **Power consumption:** Disk arrays require constant power to maintain spinning platters.
- **Cooling costs:** Heat generation from disk arrays demands extensive cooling infrastructure.
- **Replacement cycles:** Hard drives have limited lifespans (3-5 years), requiring regular replacement.
- **Management overhead:** Complex RAID configurations and storage management systems

As video quality and proliferation start to surpass disk capacity growth and the economics of disk storage become stretched, difficult choices emerge. Should you begin deleting data to free up space or sacrifice quality (and usefulness) because of escalating cost?

Cloud Storage Limitations

While cloud storage offers scalability, it introduces its own cost and accessibility challenges. Organizations can spend a small fortune storing video data in the cloud. A longer retention period translates into a higher volume of data stored, and thus, higher storage costs.

Cloud also introduces significant and highly unpredictable annual retrieval (egress) costs.

If data is kept readily accessible on the cloud, it is online and vulnerable to ransomware and other compromises by both internal and external bad actors. If surveillance data is moved to a deeper cloud archive, higher costs persist, while accessibility is sacrificed.

Cloud storage also raises concerns about data sovereignty, retrieval latency, and bandwidth costs for uploading or downloading data.

Challenge 3: Compliance and Regulatory Requirements

Retention isn't only about storage; it's about demonstrating **governance and compliance**.

Along with a shift towards stricter global regulations enforcing AI ethics and data protection, organizations must demonstrate adherence to retention schedules under legal or regulatory review, ensure data is immutable and tamper-evident, and maintain an auditable chain of custody from capture to disposal.

Privacy laws (ex., GDPR, CPRA), public-sector archives statutes, and evidence-handling standards all require **secure, defensible, and documented** storage practices.

Regulators, auditors, and even insurers expect CISOs, IT managers, and compliance leaders to define, document, and enforce data retention policies for video footage. Without a quality retention policy and the tools to execute it, organizations risk compliance violations, regulatory fines, and gaps in evidence.

Challenge 4: Cybersecurity Threats and Ransomware

Video surveillance systems have become prime targets for cyberattacks, with ransomware representing the most significant threat to video archives.

The Growing Threat Landscape

Cybersecurity risks, such as local data breaches and unauthorized access to cloud storage, continue to be a growing concern, and no one is immune.

For example, in November 2025, Check Point Research reported that in the previous October, the global volume of cyber-attacks continued its upward trajectory and that organizations worldwide experienced an average of 1,938 cyber-attacks per week, marking a 2% increase from September and a global average 5% rise compared to October 2024 (+18% in North America and +16% in Latin America) while noting rising intensity of GenAI threats.

As cyber threats escalate, the security of IP surveillance systems has become a top priority. Organizations must adhere to numerous compliance frameworks and guidelines.

The consequences of a breach are severe. When ransomware encrypts video archives, organizations lose access to critical evidence and face difficult decisions about paying ransoms.

Connected Storage Vulnerability

When surveillance archives reside entirely online—on NAS, SAN, or active cloud tiers—they are vulnerable to encryption, deletion, or corruption. IBM identified phishing, compromised credentials, and cloud misconfiguration as top attack vectors for cyber criminals, meaning any 'connected' data is vulnerable, including 'virtual' air-gapped storage.

Traditional disk arrays, NAS systems, and even cloud storage can be compromised by determined attackers who gain network access. Hackers intending to cause harm are creative and persistent. Anything connected to a network is at risk of being breached.

The Need for Immutable Storage

Data immutability is essential to ensure the sanctity of video copies or archives. Organizations need storage solutions that cannot be encrypted, deleted, or tampered with—even if attackers gain network access.

Challenge 5: Data Integrity, Accessibility, and Retrieval

While long-term archival is essential, video data must also remain increasingly accessible for investigations, compliance audits, legal proceedings, and operational review.

Chain of Custody Requirements

Chain of custody (CoC) requirements are essential across industries handling sensitive, regulated, or potentially evidentiary data—such as surveillance video, audio, health records, financial documents,

and legal evidence. An unbroken and well-documented chain of custody is critical for ensuring the integrity, authenticity, and admissibility of evidence or records in both regulatory and legal contexts.

The Accessibility Dilemma

Organizations struggle to balance two competing needs:

Security Requirements:	Operational Requirements:
Data must be immutable and isolated from networks to prevent cyberattacks and compromise.	Authorized users must be able to retrieve specific video clips rapidly without hidden costs or other performance compromises.

Traditional tape archival solutions have always struggled with this balance and the need for usability—**until EchoLeaf changed the model**!

The EchoLeaf SafeRoom™ Solution: Video Surveillance Data Archive

The EchoLeaf Systems SafeRoom™ platform addresses this need for lower complexity and provides a low entry cost & secure '**active archive'** with policy-driven lifecycle management, physical air-gapped data immutability, simple non-destructive deployment and management, and easy scalability, without sacrificing accessibility or chain-of-custody control.

EchoLeaf Systems has engineered a comprehensive solution that addresses every challenge facing video surveillance users. Our innovative and patented virtualization and orchestration technology combines the proven benefits of modern LTO tape storage and physical air-gap protection with seamless integration capabilities.

Rethinking Video Archive Architecture

From Keeping Everything Online to Tiering Intelligently While Maintaining Long-Term Interoperability

A modern surveillance data architecture requires multiple storage tiers where data may be staged on local disk for hours or days before being migrated to far more cost-effective, yet readily available, immutable, and secure active archive storage, where it is stored for months, or even decades, for long-term compliance or evidentiary needs. These requirements make surveillance video data an ideal candidate for EchoLeaf-managed LTO/LTFS (Linear Tape File System) based offline storage.

Interoperability Protection

LTFS provides a file system interface that enables users to access tape data as if on a hard drive. This includes drag-and-drop functionality for easy file management. LTFS enables LTO to act like a disk, which allows LTO to act not only as an archive medium to protect assets long-term, but also as a readily accessible nearline medium for storing raw and post assets.

Open Standard

There is no vendor lock-in, as LTO (Linear Tape-Open) and LTFS (Linear Tape File System) provide interoperability by allowing tapes formatted with LTFS to be read by any compatible LTO tape drive, regardless of the manufacturer, and EchoLeaf writes data in a non-proprietary method, simplifying data management and enhancing compatibility.

Solution Component 1: Dramatic Cost Reduction for Long-Term Storage

EchoLeaf leverages the latest LTO-9 technology, which offers unparalleled cost efficiency for long-term video retention. LTO-9 offers a native capacity of 18TB per cartridge (up to 45TB compressed), with the LTO roadmap extending to future generations, promising even higher capacities.

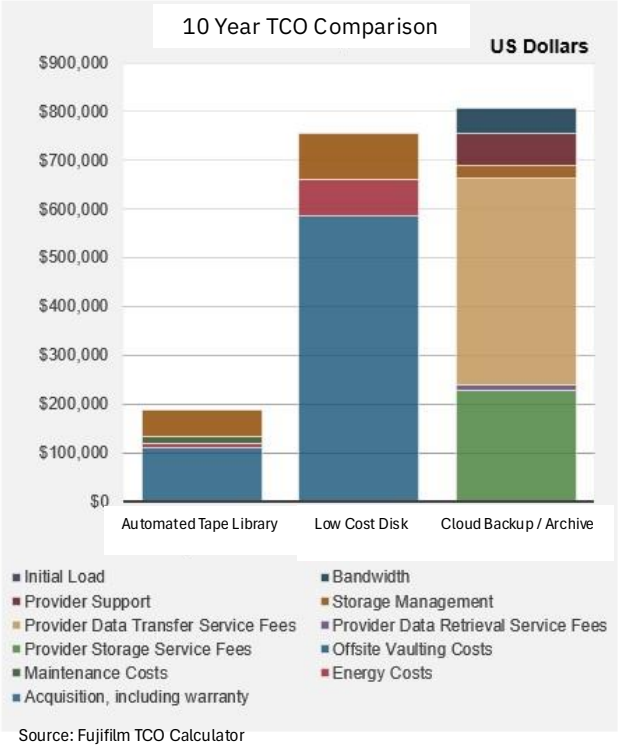
When effectively managed and virtualized, LTO is the most **secure, energy-efficient, cost-effective, and**

easily scalable medium for archives and continues to expand across markets:

- **LTO Growth: 15.4% year-over-year deployment growth** reported for last year, and the fourth consecutive annual increase in LTO deployment.
- **Lower TCO: 70–80 % lower** cost per terabyte than disk or cloud cold storage.
- **Longevity: 30+ years** of longevity with proper handling.
- **True Isolation: 'Physical' air-gap** isolation from ransomware, deletion, or other manipulation.
- **Immutability:** Available **WORM (Write Once, Read Many)** and **Hardware Encryption** support for tamper-proof storage.
- **Accessibility:** Rapid access with **no additional and costly cloud egress, storage, transport, or API charges**, or retrieval delays from deep cloud storage.

Total Cost of Ownership Benefits

LTO tape is incredibly affordable when compared to high-speed disk storage and can reduce overall video surveillance storage costs by over 75% compared to disk or cloud.



Source: Fujifilm TCO Calculator

Multi-Dimensional Cost Advantages:

1. **Lower media costs:** LTO tape is far less costly to own and operate (it has a lower long-term TCO) than either disk or cloud.
2. **Minimal power consumption:** Unlike disk arrays that require constant power for spinning platters, or SSDs that fail if not powered regularly, LTO cartridges consume zero power when stored.
3. **No cooling costs:** Offline tape cartridges generate no heat, eliminating high cooling infrastructure expenses.
4. **Extended longevity:** LTO has a 30-year shelf life, so you can depend on being able to recover data for decades to come.
5. **Reduced replacement cycles:** LTO media outlasts disk drives by a factor of 6-10x, minimizing replacement costs.
6. **Environmentally** friendly with an 86% reduction in CO2.

Scalability Without Cost Explosion

The EchoLeaf SafeRoom™ can easily and cost-effectively scale from terabytes to petabytes. As surveillance systems grow, organizations can simply add more tape cartridge capacity without the exponential cost increases associated with expanding disk arrays. EchoLeaf patented virtualization and orchestration tracks the contents of all tapes, both in and outside of the archive, so all assets appear as if they were local.

Solution Component 2: Meeting Compliance and Retention Requirements

Comprehensive Compliance Support

The EchoLeaf SafeRoom enables organizations to meet the most stringent retention requirements across all industries:

- **Multi-year retention**: LTO's 30-year shelf life supports even the longest mandated retention periods.

- **Encrypted storage**: Hardware-based encryption meets HIPAA, GDPR, and other privacy requirements.
- **Audit trails**: Complete documentation of all data writes and accesses.
- **Geographic Resiliency with EchoLeaf Gemini™**: Physical cartridges can be stored in specific jurisdictions to meet data sovereignty requirements. The EchoLeaf Gemini™ option provides support for automated data replication to systems in multiple geographic locations, adding another layer of resilience and protection.

Industry-Specific Compliance

The EchoLeaf solution addresses unique compliance needs across industries:

- **Law Enforcement/Government**: Maintains chain of custody with tamper-evident storage.
- **Education**: Family Educational Rights and Privacy Act (FERPA) compliance, record access control, secure storage, and student privacy.
- **Healthcare**: HIPAA-compliant, encrypted storage with controlled access.
- **Financial Services**: Meets SEC 17a-4 and SOX requirements for non-rewritable, non-erasable storage.
- **Commercial/Retail**: Satisfies PCI DSS requirements for payment card area surveillance and security of cardholder data and reduces the risk of fraud and data breaches.
- **Critical Infrastructure** (Energy, Utilities, Transportation): Incident accountability, security governance.

Simplified Compliance Management

Enterprises must weigh regulatory mandates against operational realities while ensuring policies remain defensible. EchoLeaf simplifies compliance by providing a single, unified archival platform that addresses multiple regulatory frameworks simultaneously.

Solution Component 3: Ultimate Protection Against Cyberattacks

True Physical Air Gap

EchoLeaf provides what no disk-based or cloud storage solution can offer: true physical air-gap protection. Our patented technology, combined with LTO/LTFS, ensures that archived video data is completely isolated from network threats.

The EchoLeaf SafeRoom™ solution provides a "True Physical Air Gap Storage that delivers the highest level of security and resiliency with the strongest defense against cyberattacks, including ransomware, as it completely isolates systems from potential cyber threats."

Immutable Storage

Once data is written on an EchoLeaf-managed LTO WORM tape, it becomes immutable, meaning it cannot be modified or deleted. This immutability protects against data tampering as the data on the tape remains in a read-only state.

Even if attackers gain complete control of an organization's network, they **cannot**:

- **Encrypt** data stored on offline LTO cartridges.
- **Delete** archived video footage.
- **Modify** existing recordings.
- **Prevent** data recovery.

Add to this the availability of hardware-based encryption, and even if tapes are physically stolen, information cannot be accessed without the access key.

Protection Against Ransomware Economics

According to the Sophos State of Ransomware 2025 report, the average ransom payment (just part of recovery costs) ranges from over $638K in small businesses to over $1.8M for larger enterprises, depending on company size, which is many times more than the initial investment in an EchoLeaf system. The investment in EchoLeaf's SafeRoom™ is minimal compared to the potential cost of a single ransomware incident.

EchoLeaf's Layered Security Architecture

EchoLeaf provides multiple layers of security:

- **Data Virtualization:** Allows assets to appear online while being physically isolated from the network.
- **Physical Isolation:** Cartridges stored in secure, offline locations.
- **Hardware Encryption:** AES 256-bit encryption with post-quantum encryption planned.
- **WORM Capable:** Hardware-enforced write-once protection; data is immutable for the lifetime of the cartridge.
- **Access Controls:** Granular permissions for cartridge handling.
- **Chain of Custody Tracking:** Audit trail of cartridge movements.

Solution Component 4: Effortless Scalability

Linear Scalability Model

Unlike disk arrays that require careful capacity planning, RAID configuration, and controller management, EchoLeaf offers simple linear scalability. Expanding storage capacity with the EchoLeaf SafeRoom involves simply adding support for more tapes. Even tapes removed from the archive continue to be tracked by EchoLeaf.

The SafeRoom™ starts at 360TB (native) and scales to 11.5PB with the current LTO-9 drive configuration, offering a more straightforward approach compared to the complexities of expanding disk-based systems.

No Forklift Upgrades

When organizations outgrow their current storage infrastructure, disk-based solutions often require expensive "forklift upgrades"—replacing entire arrays with higher-capacity systems. With EchoLeaf, scaling is as simple as adding support for more LTO drives and cartridges to the existing infrastructure.

- Built-in data virtualization lets administrators scale from hundreds of terabytes to multi-petabyte environments without re-architecture.
- Supports multi-site replication for resilience and disaster recovery.
- Easily integrates with VMS and evidence-management systems via standard NFS/CIFS interfaces.
- Tapes removed from the library remain in the EchoLeaf database, appear local, and will be requested by their unique number on file request.

Future-Proof Technology

The LTO Consortium maintains a clear technology roadmap, with LTO-9 current, LTO-10 recently introduced, and development through LTO-14 already planned. Future LTO generations are expected to reach 576TB native capacity per cartridge. The EchoLeaf SafeRoom includes a background utility that transparently migrates archived data from older LTO/LTFS generations (e.g., LTO-8) to newer ones (e.g., LTO-9), while maintaining tape-level metadata and internal references.

Solution Component 5: Simple Deployment and Maintenance

Streamlined Implementation

As noted in recent IBM and IDC reports, all industries today suffer from a shortage of experienced IT skills and personnel. According to a 2025 report by Sophos, the top operational root causes for incidents list Lack of Expertise (i.e., not having the skills or knowledge to detect and stop the attack in time) as the most common operational reason.

This is followed in very close succession by unseen Security Gaps that the organization was not aware of, and thirdly, there was the Lack of People/Capacity (i.e., having an insufficient number of cybersecurity experts monitoring their systems at the time of the attack)

In addition, cloud misconfiguration was cited by IBM as one of the top attack vectors for ransomware alongside compromised credentials and phishing.

Unlike complex disk array or cloud deployments requiring extensive configuration, RAID setup, and network integration, EchoLeaf systems can be

deployed rapidly with minimal disruption to existing operations.

Each EchoLeaf SafeRoom™ arrives pre-configured and fully integrated, ready for rack-and-stack.

Integration w/ Existing VMS & Backup Software

EchoLeaf integrates seamlessly with leading Video Management Systems (VMS) and backup software, appearing as a simple NAS, and enabling organizations to implement a two-tier storage strategy:

- **Tier 1:** High-speed disk for capturing new & actively reviewed files (days).
- **Tier 2:** EchoLeaf LTO with rapid access for medium-term retention (months), and long-term compliance for evidentiary needs (months to decades).

This tiered approach provides the best of both worlds: immediate access to recent footage and cost-effective, evidence-ready, compliant long-term archival, with rapid access for analysis / review as needed.

Low Maintenance Overhead

LTO tape systems require significantly less maintenance than disk arrays:

- No spinning disk components to fail or replace.
- No complex cloud configurations and external network connections to maintain.
- Longer replacement cycles.
- Reduced power management needs.
- Simplified hardware lifecycle management.
- 24x7 EchoLeaf SafeRoom™ system monitoring.

Solution Component 6: Data Immutability and Tamper-Proof Storage

Evidential Integrity

Thanks to a combination of WORM technology, encryption, and **verify-after-write**, EchoLeaf SafeRoom™ stored data aligns with the requirements of financial, healthcare, law enforcement, government, or any data-retention regimes that mandate integrity, confidentiality, and non-erasable preservation for specific classes of data.

Compliance with Legal Standards

The immutability of EchoLeaf SafeRoom storage satisfies the most stringent regulatory requirements:

- SEC 17a-4(f): Non-rewritable, non-erasable format for financial records.
- HIPAA: Protection against unauthorized alteration of protected health information.
- FRCP (Federal Rules of Civil Procedure): Authentic, unaltered evidence preservation.
- State retention laws: Meets requirements for tamper-evident storage.

Hardware-Enforced Write Protection

The EchoLeaf SafeRoom™ LTO/LTFS tapes are append-only, and with optional WORM (Write-Once-Read-Many) technology, provide hardware-enforced immutability. Once data is written to a WORM cartridge, it cannot be altered or deleted—even by system administrators with full access privileges.

This level of protection is impossible with disk-based or cloud storage solutions, where software-based "immutability" can potentially be circumvented by attackers with sufficient access.

Hardware-Based Encryption

The EchoLeaf SafeRoom™, utilizing LTO-9 or later drives, allows for hardware-based encryption to protect data at rest on the cartridge. Encryption helps preserve evidence confidentiality during transport and storage and supports regulatory requirements for protecting sensitive video and related metadata. If properly managed with key custody controls, it strengthens the chain of custody by ensuring only authorized parties can access the content. Evidence handling implications support data protection laws and access-control mandates for sensitive surveillance footage.

Write Verification Technology

To ensure that data written to the SafeRoom™ archive is protected, LTO drives employ verify-after-write technology, where a read head follows the

write head and verifies the data just written. This provides an automated check summing operation for all written data.

Unlike a hard drive, where all data must be read back to verify that data has been correctly written, LTO provides this capability during the archive write process, saving an entire read and restore operation.

On average, an archive and checksum operation with LTO will be four times faster than performing an archive and checksum to a hard drive.

Error Correction and Resiliency

LTO-9 employs robust Reed-Solomon error correction and advanced media protection; if a bit or sector becomes unreadable, recovery mechanisms help maintain data integrity and maximize archival longevity. This supports evidence preservation by minimizing data loss due to media degradation or minor defects, a key element for long-term surveillance archives. This reduces the chance of incomplete evidentiary sets due to media failure.

Solution Component 7: Unbreakable Chain of Custody

Legal Admissibility

The combination of immutable WORM storage, LTO CRC Verify-After-Write verification, and audit trails ensures that video evidence archived on EchoLeaf Systems supports regulatory expectations around retention periods, tamper resistance, and chain-of-custody proof. This helps satisfy compliance frameworks that emphasize long-term immutability and controlled access to evidence material.

SUMMARY

EchoLeaf delivers a purpose-built & patented cybersecurity and archive solution that not only provides a secure data SafeRoom™ to reliably shield essential data from ransomware attacks, but also addresses the critical storage, data protection, scalability, cost-effective long-term preservation, and evidence-ready compliance requirements needed for the growing video surveillance industry.

Immutability	Sequential Write & Un-alterability	Physical Isolation & Hdwr Encryption	Low Entry Cost & Easy Scalability	Accessibility	Most Cost Effective
Assures that video evidence cannot be deleted or altered, meeting legal/compliance needs and protecting against threats or ransomware. Hard drives and SSD's suffer from data corruption and loss when not powered for longer periods of time.	Provides forensic-grade audit trails and ensures the authenticity of stored footage, which is crucial for legal and regulatory defense. Multi-site replication protects against destruction of the primary location.	Limits exposure to cyber threats and eliminates shared attack surfaces, further securing sensitive surveillance content.	Enables organizations to store petabytes of video data without major capital expense, and to expand storage as the number of cameras and data collection needs grow.	Ensures that authorized users have reliable, timely access to footage in seconds with no added costs, external delays, or network constraints meeting evidentiary and privacy demands.	Demonstrably the most cost effective, secure and proven long-term storage. TCO: EchoLeaf Savings vs Cloud - 77% EchoLeaf Savings vs Disk - 75% EchoLeaf CO2 reduction - 86%

The EchoLeaf SafeRoom™ provides a software-defined, scalable, and intelligent data virtualization and orchestration management layer that unifies LTO/LTFS storage into your existing surveillance environment—appearing as a simple NFS or CIFS target, yet delivering the economics, security, and immutability of offline tape.

Key EchoLeaf SafeRoom™ Advantages

Video surveillance is the digital witness of our age. Without a sustainable and compliant way to preserve that evidence, organizations face escalating risk—financial, legal, and reputational. As camera resolutions climb and AI analytics drive even longer retention for model training, archives will grow exponentially. The winning strategy is to design for scale, compliance, and security from day one.

EchoLeaf enables this by:

- Abstracting hardware complexity through software-defined orchestration.
- Seamlessly, non-disruptive integration with existing ecosystems.
- Supporting hybrid models with local physical air-gap tiers for ultimate resilience.
- Providing verifiable data integrity for regulatory or evidentiary defense.
- Cutting long-term TCO vs disk & cloud by 75-80%.
- Physical Isolation makes the SafeRoom™ immune to ransomware.
- Low entry cost and easily scalable.

EchoLeaf Systems delivers a new standard for secure, compliant, and economical long-term video data retention:

Protect Video Data Offline Against Cyberattacks	EchoLeaf's architecture maintains true physical air-gaps between operational networks and offline tapes. Even if primary systems are compromised, archived data remains unreachable by ransomware or malicious insiders. Supports secure encryption (AES-256) and key management.
Scale Effortlessly as Data Grows	Built-in data virtualization lets administrators scale from hundreds of terabytes to multi-petabyte environments without re-architecture. Supports multi-site replication for resilience and disaster recovery. Integrates with VMS and evidence-management systems via standard NFS/CIFS interfaces.
Data Accessibility & Rapid Retrieval	EchoLeaf indexes every stored object with metadata for fast search and retrieval. Evidence is always available with rapid restoration and no added access costs or external delays. Operators can access an archive as if it were a local volume—select only the files required for retrieval.
Cut Long-Term Storage Costs with infinite, scalable storage	Offload cold video data from expensive disks or cloud to EchoLeaf's LTO-based archive and achieve up to 80% cost reduction in total cost of ownership for multi-petabyte environments along with energy savings from near-zero power draw when offline.

Meet Compliance and Retention Requirements	Immutable storage with WORM availability and hardware encryption ensures video cannot be altered or deleted before expiration. Audit logs and reports demonstrate compliance with evidence-handling and retention policies.
Chain of Custody & Tamper-Proof Storage	Write-Once, Read Many (WORM) media, which makes subsequent rewrites impossible, hardware-based encryption mode, and verify-after-write, combine to meet DOJ, CJIS, and evidence preservation standards. This immutability is essential for chain-of-custody because it prevents post-ingestion modifications without leaving a detectable audit trail.
Ease of Deployment and Maintenance	Deployed as an on-premises system appliance. Non-disruptive to your current environment and easy to maintain. No proprietary hardware lock-in—works with standard LTO libraries and LTFS. Intuitive management dashboard for policy, monitoring, and retrieval. Designed for non-storage specialists in physical security or IT operations

In an era where truth increasingly lives in pixels, EchoLeaf ensures those pixels—and the integrity they represent—are preserved, protected, and ready when the world needs them most.

Echo Your Data Today™!

To learn more, please visit www.echoleafsystems.com.

Contact:
Douglas Korte | CSO
EchoLeaf Systems, Inc.
+1 661-250-0649 (o)
Dkorte-ic@echoleafsystems.com
www.echoleafsystems.com

EchoLeaf Systems, Inc.