Securing the Future of Media Production, Post and Creative Technologies with Superna

About the Author

Overview

About this paper

MovieLabs Core Principles

- MovieLabs Principles

Security Principle 1: Security Is Intrinsic To Every Component Of Every Workflow And Does Not Inhibit Creative Processes

- How does this approach integrate security without inhibiting the content creator?
- What happens if the content creator forgets to tag the security of the asset?

- Problems addressed by a Data First Security Strategy
- How does Superna help?

Security Principle 2: The Security Architecture Addresses Challenges Specific To Cloud-Based Workflows

- Diagram 1 Golden Copy Metadata Data Movement Policy Enforcement

Security Principle 3: Production Workflows, Processes, And Assets Are Secure, Even On Untrusted Infrastructure

Security Principle 4: The Content Owner Controls Security And Workflow Integrity

- Content Owner Use Cases
- Summary

Security Principle 5: The Security Can Be Scaled To Appropriate Levels And Can Integrate With Existing Security Policy And Management Systems

- Superna's Data First Security Strategy

Security Principle 6: The Security Architecture Limits The Spread Of Any Breach And Is Adaptable To The Evolving Threat And Response Landscape

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

[Superna's Role in the Journey to the MovieLab 2030 Evolution Of Media Creation](#)

- [What problems exist today with file and object storage?](#)
- [What does this all mean?](#)
- [MovieLabs 2030 Vision Scorecard](#)
- [Conclusion](#)

About the Author

Andrew MacKay - President & CTO of Superna

Overview

This paper will discuss how Superna can help modernize Content creation in the migration to the Movielabs Whitepaper 'The Evolution of Media Creation: A 10-year vision for the future of media production, post and creative technologies" and how best to secure workflows based on the "The Evolution of Production Security", from MovieLabs.

Any business process or workflow that moves documents or transforms data can benefit from a Secure hybrid cloud architecture. Media

creation involves many steps to produce a final product. This paper will focus on the media industry but the principles apply to any business process/workflow that benefits from a hybrid cloud architecture.

Superna's core tenant of product development centers around a long history of innovation and data centric product solutions that offer a data first approach to security, orchestration, management, and analysis. A "data first security strategy" places data (files or objects) at the center of any feature or function that is designed to secure a workflow. We will explore how Superna solutions address the key design principles outlined in the MovieLabs "The Evolution of Production Security".

About this paper

This paper will highlight the benefits of a data first security strategy, how this aligns with MovieLabs 2030 vision and how Superna is delivering solutions today that move customers to this vision.

MovieLabs Core Principles

Below are the core principles to secure hybrid cloud workflows.

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

MovieLabs Principles

1. Security Principle 1: Security Is Intrinsic To Every Component Of Every Workflow And Does Not Inhibit Creative Processes
2. Security Principle 2: The Security Architecture Addresses Challenges Specific To Cloud-Based Workflows
    a. Security principle 2 has three parts to it:
    b. a) Security is centered on workflows, rather than the infrastructure they run on.
    c. b) Security is centered on assets, rather than their storage and transport.
    d. c) The integrity of assets, processes, and workflows is protected.
3. Security Principle 3: Production Workflows, Processes, And Assets Are Secure, Even On Untrusted Infrastructure
    a. For our purposes, Zero Trust security is an ideal approach. It places the control of security in the hands of the content owner, it is part of the security architecture, and it can be implemented through specification of the security of the applications and other components that are used in the workflow. Granularity is controlled by policy, not technical constraints

4. Security Principle 4: The Content Owner Controls Security And Workflow Integrity
5. Security Principle 5: The Security Can Be Scaled To Appropriate Levels And Can Integrate With Existing Security Policy And Management Systems
6. Security Principle 6: The Security Architecture Limits The Spread Of Any Breach And Is Adaptable To The Evolving Threat And Response Landscape

Security Principle 1: Security Is Intrinsic To Every Component Of Every Workflow And Does Not Inhibit Creative Processes

Security by design is the key to this principle which means the data used within a workflow determines how security should apply to each file within the workflow. As files are created, metadata is created by all applications, additional custom metadata can be applied to files or objects that signals to the infrastructure how this file should be treated.

Let's use the example of a video application creating a new video clip and saving the video file. The application typically adds metadata about

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

the clip such as project name , scene, resolution or bitrate etc… Many applications allow adding custom metadata to the file. This allows content creators to specify the security of the asset. If this asset was a new ending to a movie the file could be marked as “confidential” and this metadata attribute could be read by the infrastructure to apply security policies automatically based on this metadata.

How does this approach integrate security without inhibiting the content creator?

Content creators would be adding metadata to assets as a normal part of the workflow, integrating security at the source of asset creation simplifies the integration.

What happens if the content creator forgets to tag the security of the asset?

Security falls down when manually processes are required. This is not acceptable when security of data is at stake. The data first security strategy handles this scenario easily, because the infrastructure will see that no security handling metadata exists and can quarantine the file and lock it down (apply ACL’s to mark as read-only) and notify administrators in real-time that an asset has been quarantined. The

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

infrastructure could even send an email to the content creator to apply the security tag to the asset so that it can be used in the workflow.

Problems addressed by a Data First Security Strategy

This approach avoids securing the infrastructure and allows the data to signal to the hardware and software that processes or touches the data in the workflow to react to the data inside the workflow. It allows metadata applied at source (application or content creator) to:

1. Determine how the file/object is handled inside the workflow.
2. Data carries its metadata with it, allowing the security tag signal to be honored at each step of the workflow process
3. Data without a tag can also be rejected inside the workflow
4. Metadata within files can be extracted and moved between files and object storage systems allowing full transparency between file systems and object based systems
5. Hybrid cloud architectures can natively handle file and object and metadata transparency
6. Workflows that use the same infrastructure can change the security model without changing the infrastructure
7. Metadata allows full customization and extensions to any solution by defining customer metadata
8. Security is only one possible use case for custom metadata

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

a. number of copies of the data required for data protection
b. Encryption status for at rest protection
c. life cycle status (active, archival, short term archive, scratch data)
d. DR requirements for the data
e. Data type (pre-production, RAW, final cut, etc..)

How does Superna help?

Superna Golden Copy is a metadata aware data orchestration platform for hybrid cloud media use cases.

1. Transparent metadata extraction from file to object feature allows rich metadata on files to be exposed when data is synced, moved to object. This functionality is enabled with support for over 1500 different file types.
2. Open data format allows all data copied to object to be read, written and updated with an native tools
3. Secure data once. This means leveraging SMB share permissions to limit users access to object data synced to object stores in the cloud.

a. Who wants to manage two different security frameworks SMB, S3? **No one!**

4. Self service is always the answer

a. Storage administrators have no time to manage each and every users data access request or data movement from production file system to completed storage in S3. Self service is mandatory to enable the future hybrid cloud software defined workflow model.

b. Workflows require data to move between file and object and object back to file, content creators, editors or other production user roles need tools that allow simple secure access to data regardless of where it's stored. Golden Copy enables Cloud browser which integrates file system and object store browsing into a single user experience.

c. This enabled self-serve data movement orchestrated by Golden Copy but secured once with SMB permissions overlaid onto the object store preserving the security integrity of the data stored in the object store.

d. Active Directory login allows seamless presentation of data to end users to view versions, metadata, backup status

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

Security Principle 2: The Security Architecture Addresses Challenges Specific To Cloud-Based Workflows

Let's review the key principles of for workflow based security architecture:

This Security principle has three parts to it:

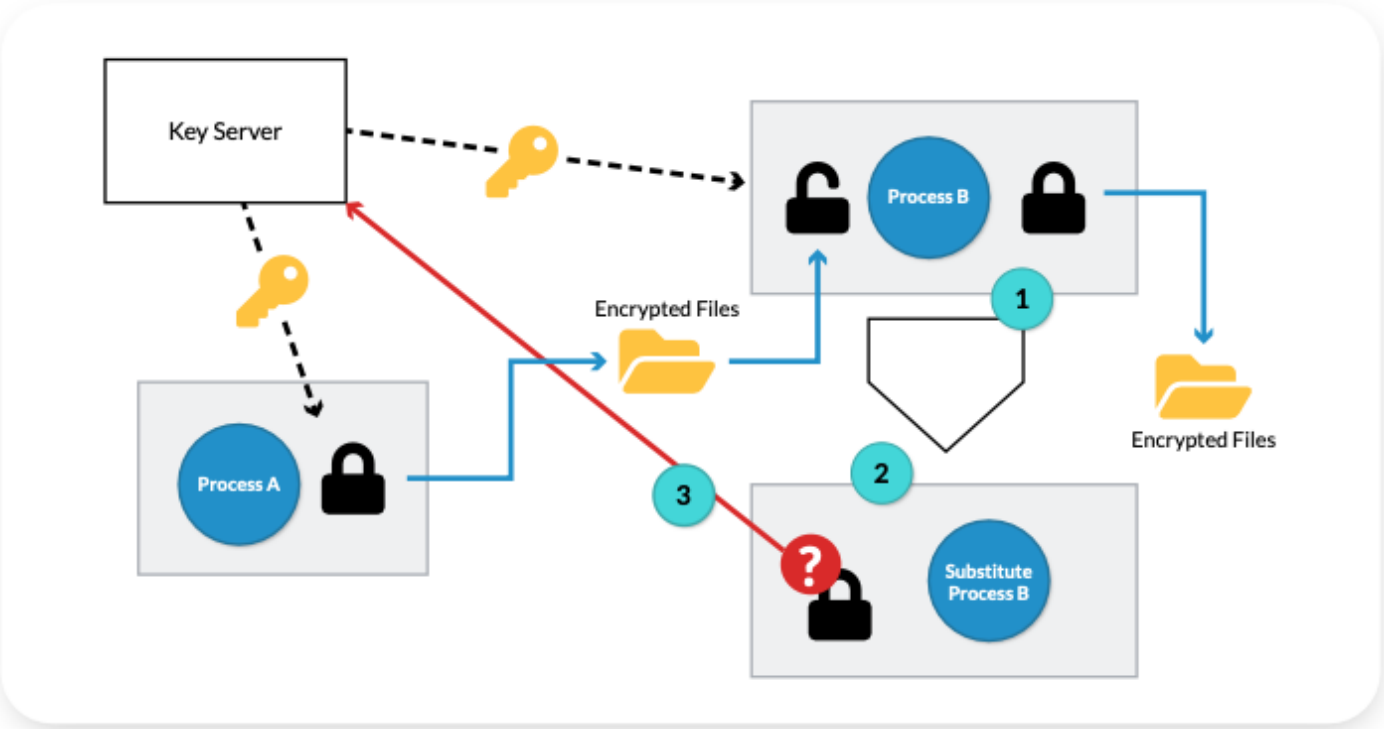
a. Security is centered on workflows, rather than the infrastructure they run on.
b. Security is centered on assets, rather than their storage and transport.
c. The integrity of assets, processes, and workflows is protected.

These principles all place data at the center of the security but only suggest moving encryption to the application layer with a Key management system to control the DRM (Digital Rights Management) of the assets. Encryption in the transport and at rest within the infrastructure can still be used but becomes redundant if the application layer owns the encryption/decryption of the assets.

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

The second aspect of securing the workflow is the hand off from one process to another. Let's reference this diagram from the MovieLabs [Evolution Of Production Security] paper.



Superna USA Inc.
3630 Peachtree Road, Suite 920, Atlanta, GA 30326

This diagram shows an application and user initiated workflow that requires the user and the application to use the same key server when data moves between processes. Remember in a hybrid cloud application architecture process A and process B could be located anywhere; on premise, in the Cloud or across 2 different Cloud providers.

The movement of data between Process A and B is not addressed in this example. Let's explore how the infrastructure can improve the security of the workflow.

Process A produces an application encrypted file, the file has custom metadata added in this example <workflow>workflow-1</workflow>. The metadata can be applied by the application or in a hybrid cloud use case the metadata can be applied by the data orchestration layer (Superna Golden Copy). As the data is placed on a NAS SMB share that is configured to sync data to a Cloud S3 bucket where it is processed by Process B.

Reviewing the diagram below, we can see that Golden Copy reads metadata and only allows copying data to Process B S3 bucket if it matches the data movement policies configured within Golden Copy.

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

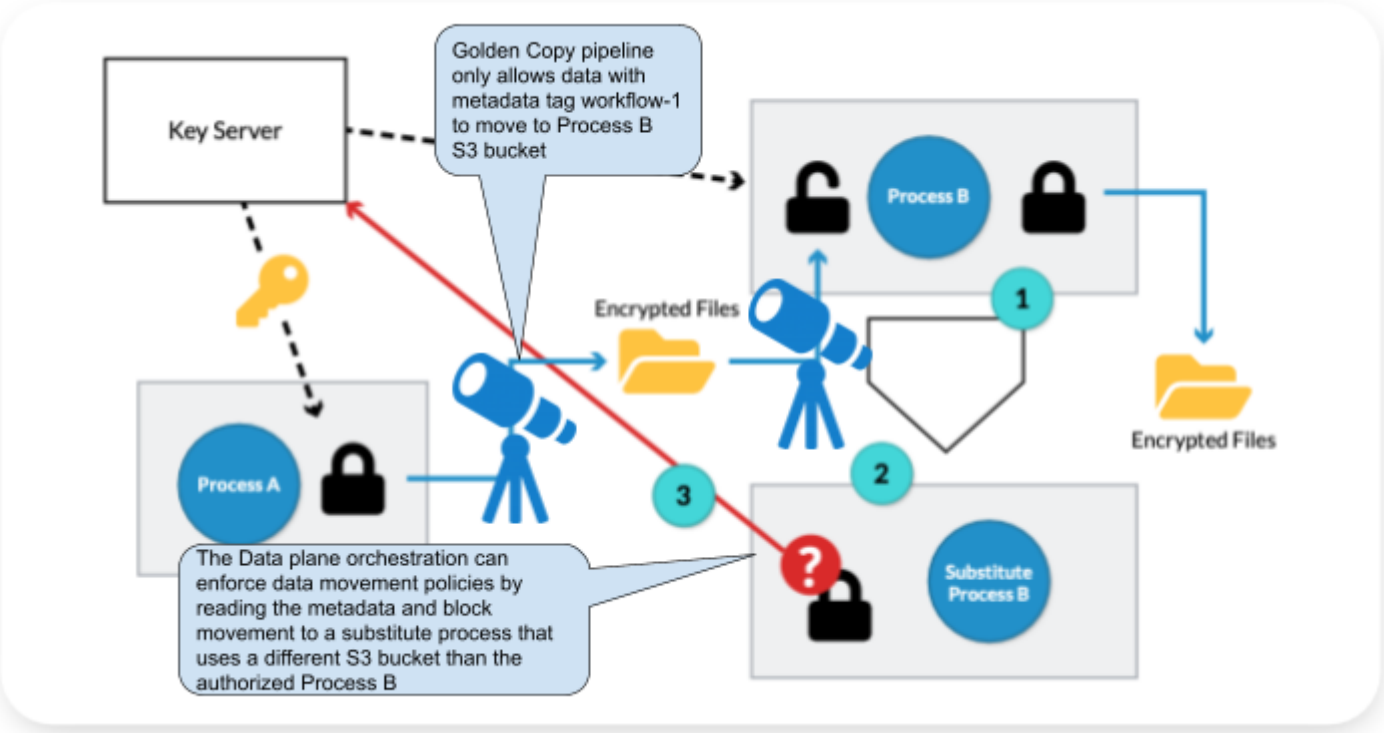


Diagram 1 Golden Copy Metadata Data Movement Policy Enforcement

How can we increase the security of this workflow even further?

The garbage in garbage out principle applies to security, if unauthorized data enters the workflow, this can lead to a potential data breach or denial of service attack on the workflow.

Superna USA Inc.

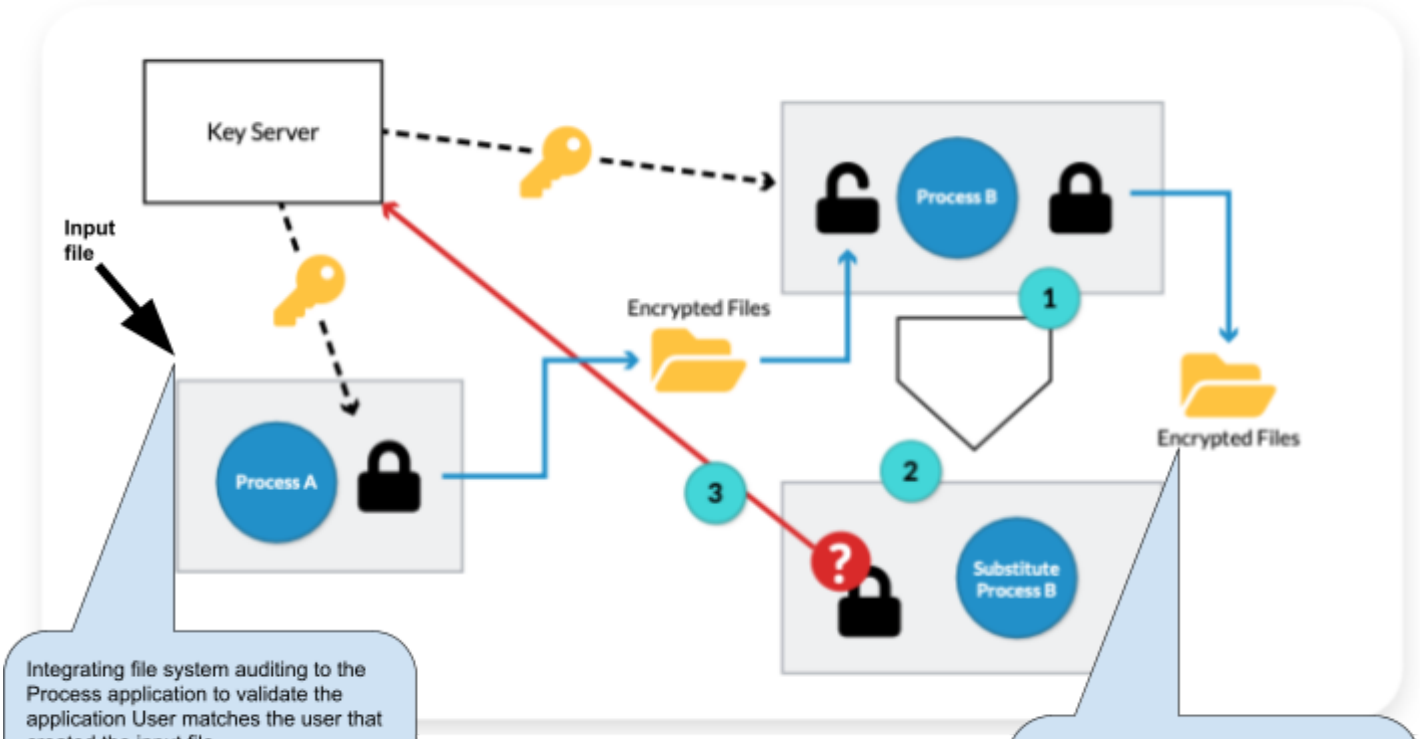
3630 Peachtree Road, Suite 920, Atlanta, GA 30326

The workflow needs to trust the data it receives, this means the application needs to trust the file that is being opened was created by an authorized user in the system. Application security and file system security are separate systems. Superna offers Easy Auditor that enables file system auditing and can identify who,what and when data is created, deleted, or modified.

What would this extra layer of security look like?

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326



Integrating file system auditing to the Process application to validate the application User matches the user that created the input file.

This would be done using a simple API to compare the file system creation of the file to the logged in user. This can be done on file open.

Let's assume Process B is an application that created an output file. Applications use service accounts to create files. The same automated method to compare the output file creation in the file system was completed by the service account (application server) using the file system auditing API

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

Security Principle 3: Production Workflows, Processes, And Assets Are Secure, Even On Untrusted Infrastructure

This principle is under the umbrella of Zero Trust architecture. The core premise is each component of the workflow: users, applications, data has Zero Trust applied at each step. What this means is that data flowing through this Zero Trust workflow design allows checking and validating that the data passing through was:

1. Created within the file system by an authorized user in the workflow (Enforced by Superna Easy Auditor validation)
2. Created by an application service account (Enforced by Superna Easy Auditor validation)
3. Has valid metadata encoded into the file before it is allowed to move between processes (Enforced by Superna Golden Copy Data Orchestration policies)
4. Has data integrity checked when moving between processes (Enforced by Superna Golden Copy MD5 checksum validations)
5. Has valid encryption by using centralized Key Management server to decrypt the data at each step in the process

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

Security Principle 4: The Content Owner Controls Security And Workflow Integrity

The Security paper focuses on the content owner controlling how their content is secured at the application level but this can easily be extended to how the data moves through workflows and other downstream applications. Here are some examples of additional use cases that a content owner can control.

Content Owner Use Cases

1. Key management with Studio, Production or delegation of keys to a VFX facility to complete a process
2. Superna Extended Data Orchestration Use cases
    a. The content owner could apply metadata to a file that signals the infrastructure to apply data centric policies to the content. Refer to examples below.

i. If the content is allowed to be moved, synced to the cloud
ii. How many copies of the asset should exist example 3-2-1 3 copies, 2 different storage technologies and 1 off site copy
iii. Versioning requirements would allow the content owner to specify how many versions of the asset should be maintained and if old versions of the asset should be archived for long term storage.
iv. Disaster Recovery requirements would mean the asset needs to be replicated to a secondary location that can present the data to applications if a site or equipment failure is detected.
v. Data lifecycle management would allow the content owner to apply metadata that signals the infrastructure to move the data to long term storage
vi. Immutability requirements for finished assets that need to be protected from modification

3. Superna Extended Asset Security Use Cases (Enforced by Easy Auditor)
    a. **DLP (Data Loss Prevention)** of sensitive data assets that need to be monitored for data copy and read requests from users or applications. This can be auto applied based on metadata

that signals the infrastructure this data should be real-time monitored for data exfiltration attempts by authorized users or unauthorized users and applications. This requires file system auditing to be integrated with the workflows.

b. **Failed data operations on sensitive data assets**. This is another file system monitoring requirement that alerts administrators or Content owners that a file operation (open for read, write, delete or other data operations) failed due to insufficient permissions to the data.

c. **Network aware data operations** - This concept places workflows inside a trusted network (Zero Trust principle) and treats all networks outside the trust zone as untrustworthy.

   i. A network is a group of IP subnets and can be used to provide real-time notification of access to workflow data from untrusted IP subnets. If application servers or users operate within a trusted network (i..e a VPN IP address space), then all data requests outside of this can be flagged as a potential breach

d. Trusted Users - The list of authorized users would be known in advance for all workflows, so applying a real-time trigger of any file system data operations attempted by a user or application service account that is outside the trusted user list can be flagged to administrators or content owners.

Summary

By extending the use cases to include a Data first security strategy controlled by content owners, the security of the workflow can be integrated with the security while still maintaining the core principles of who should control how assets are secured, accessed, protected or moved within the workflow components. The solution based on Superna's Easy Auditor and Golden Copy hides the complexity of securing , protecting data from the Content Owner. This is a core objective when Designing for Security. Your data is unmodified using metadata features of OneFS and S3 to store critical information about how your data should be treated in a hybrid cloud environment.

Security Principle 5: The Security Can Be Scaled To Appropriate Levels And Can Integrate With Existing Security Policy And Management Systems

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

In short, this security principle stipulates that security and risk management should be scalable to meet basic requirements all the way to the highest level of data/asset security. Studio's have different departments that have different security requirements and all of these different requirements need to be met with a single solution. It is also important to allow studio's to use different tools, applications, IAM systems and that SCIM (System for Cross-domain Identity Management) can help address centralized security.

Superna's Data First Security Strategy

The key to Superna's strategy of Data first security is based on metadata that is carried through a workflow to signal which policies should be applied at each point in the workflow. File system to object and object back to file system needs to preserve metadata so that it can be inspected anywhere within the workflow. The other key benefit of using metadata is that different vendor solutions can read the metadata and apply policies or extend value by simplifying defining their own metadata to differentiate or extend the workflow without concern for managing a centralized SCIM schema.

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

The likelihood of getting agreement on a multi Studio schema or standard is low but a strategy that allows vendors to innovate and allows a multi-vendor ecosystem for Studio's to integrate products into their operations is far more likely.

Security Principle 6: The Security Architecture Limits The Spread Of Any Breach And Is Adaptable To The Evolving Threat And Response Landscape

In summary, this principle discusses the architecture, not the specific technologies used within a Zero Trust architecture which determines the longevity and ability to adapt to new threats. In order to build a system that can evolve and meet this goal some building block technologies need to be selected.

The overarching goal of the MovieLabs 2030 vision is based on this diagram.

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

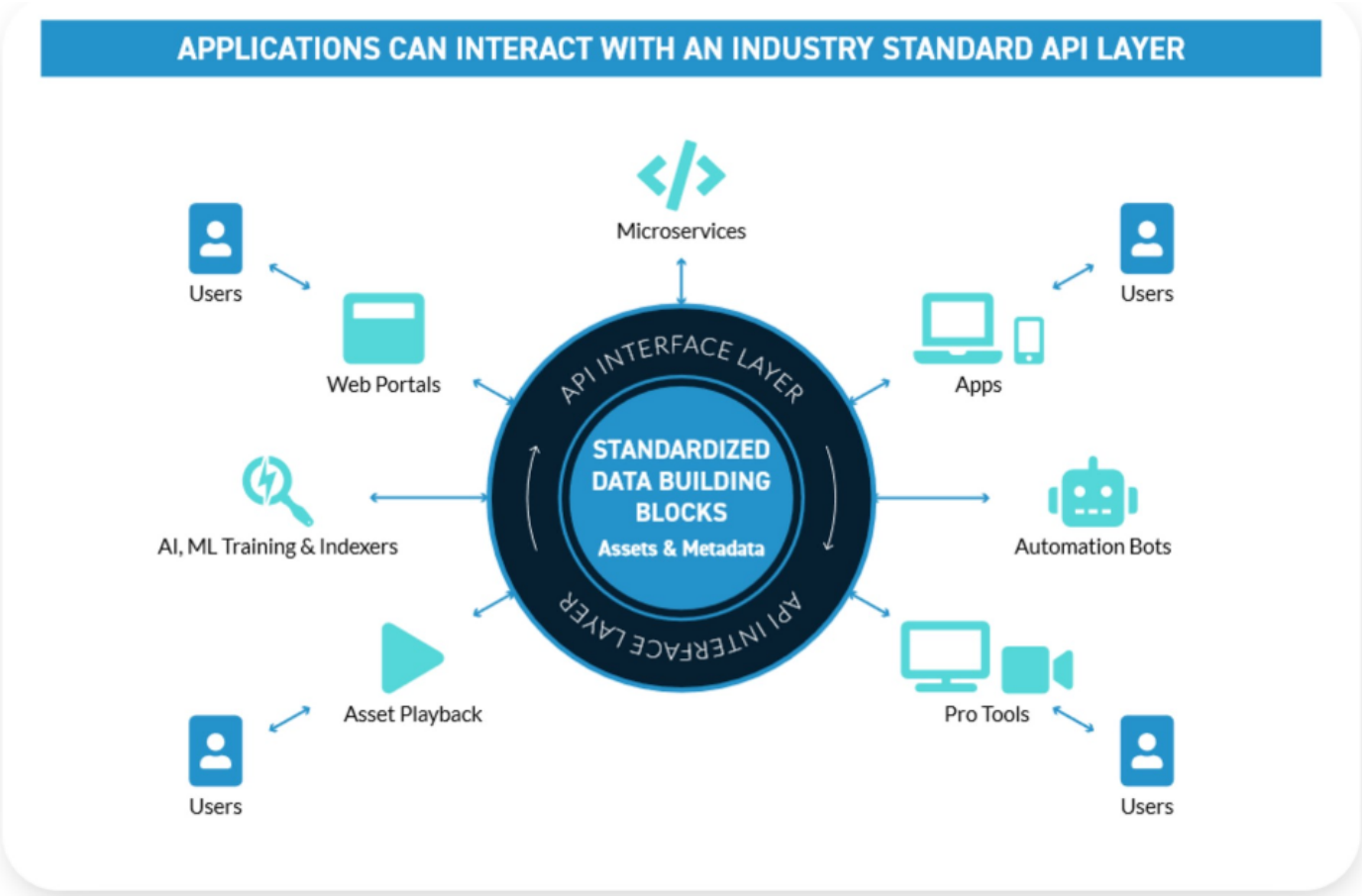


Figure 2: *Standardized building blocks contain agreed common data and metadata for key processes in production. The API interface layer abstracts that information such that any application, tools, portals or service can interface through the API layer with any other tool without needing to know about it in advance.*

Placing content owners at the center of the process allows data to carry policies with it that dictate how an asset should be secured, accessed,

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

protected, played back or processed. The above diagram shows API's that need to exist with data assets and metadata.

These API's need to execute within software that interacts with the data assets. The API's need to exist across multiple vendors to allow seamless implementations that offer consistent behavior and more importantly, consistent security across all of the use cases shown in the diagram above.

Therefore, the strategy needs to allow multi-vendor API's to be built on top of metadata that all vendors can extract to enable the use cases, workflows and security requirements of a modern media creation ecosystem.

Superna's Role in the Journey to the MovieLab 2030 Evolution Of Media Creation

The shift to a hybrid cloud or fully cloud enabled architecture needs to address the storage technology choices that limit realization of vision. Specifically the file vs object choice and the selection of the best storage for the use case. This paper is not going to answer which storage technology should be used for each workflow or use case but more

importantly highlight that either file or object or both need to co-exist to enable the vision.

What problems exist today with file and object storage?

Some background on the issues that exist when mixing and patching file and object storage within your workflows.

Function	File	Object	Issue
Byte range read and write	Yes	No	Applications need to be written differently for object, many use cases require byte range IO and eliminates object storage
Random IO	Yes	No	Same as above
Partial updates to data	Yes	No	Same as above
Symbolic links and hard links	Yes	No	1. File systems leverage symlinks and hard links for

			rapid cloning file system paths and reducing duplicate file issues for media workflows 2. S3 object storage has no functional equivalent
High performance streaming	No	Yes	Object supports parallel reading and writing with multi threads and can outperform file systems for some use cases
Embedded metadata	No	Yes	1. SMB and NFS don't allow creation of custom metadata on files, this is built into the S3 object protocol 2. Dell PowerScale supports an API to attach metadata to files, Superna Golden Copy uses this API to track data movement history as a property of the file or

			folders.
Storage tier metadata	No	Yes	S3 has the concept of storing data based on lifecycle stage at the object level, this does not exist natively within file systems
Data versioning	No	Yes	S3 has ability to store versions of data and provide read and write access to each version. File systems have no versioning capabilities
Data integrity	No	Yes	When data is moved , copied in S3 MD5 can be used by the sender and receiver to ensure data arrives error free. File systems don't have this type of built-in data integrity checking
Authentication and metadata checking and validating	No	Yes	S3 allows the metadata of an object to be included in the authentication process between and sender and a receiver. This

			means custom properties are part of the validation process. File systems have no equivalent capability.
Access Control Lists	Yes	Yes	Used frequently in file systems, rarely used in S3 but also incompatible with no simple mapping for ACL's on files and folders to S3 prefix and buckets
Inflight encryption	Yes	Yes	1. SMB uses SMB3 and is not supported on all devices and is disabled by default. 2. NFSv4 yes but very complicated to configure, rarely used. 3. S3 https works over any network, enabled by default. 4. S3 allows control over certificates for sender and receiver authentication and

			TLS level selection is easily managed

What does this all mean?

It means hybrid cloud architectures need a solution to file and object transparency or the vision will not be realized. Storage is a key building block to support modern workflows. Security should start at the data layer and move out to compute, network and end points. This is Superna's core tenant to all product innovation aimed at achieving full transparency for hybrid cloud architectures.

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

MovieLabs 2030 Vision Scorecard

The table below summarizes key functions that will be necessary to achieve MovieLabs 2030 architectures. How does the Superna solution score?

Criteria	Superna Product	Compliance with a Secure Hybrid Cloud
File to object and object to file data orchestration	Golden Copy	✓
Automation API	Golden Copy	✓
Carrier Grade upgrade (no down time upgrade containerized built for Cloud Scaling)	Golden Copy	✓
Broadcast publish (single source to multiple Clouds)	Golden Copy	✓
Contribution mode (many S3 buckets to single file system)	Golden Copy	✓

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

File auditing for integration to advanced workflows (files moved, synced, File-To-Object or Object-To-File available in JSON files for developers)	Golden Copy	✓
Transparent Security (POSIX permission transparency to object and back again)	Golden Copy	✓
4K long path names (File system to S3 URL transparency)	Golden Copy	✓
Integrated Security to data movement orchestration	Ransomware Defender	✓
Symlink and hardlink transparency for Media	Golden Copy	✓
High performance File to Object copy,sync or move	Golden Copy	✓
Single Security model (Transparent File System to Object data browsing)	Golden Copy	✓
Data Lifecycle support (S3 tiering)	Golden Copy	✓
Open object format with cross Cloud	Golden Copy	✓

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

support		
Cloud Ingest with move, sync to File Systems	Golden Copy	✓
Full file system auditing to comply with MPA Content Security Compliance	Easy Auditor provides MPA Content Security Compliance with DLP Detection, User Access Reporting, User Data access auditing, Honeypots	✓
Full Object Data Access Auditing for compliance with MPA Content Security Compliance	Easy Auditor (AWS S3, Dell ECS)	Planned
Hybrid Cloud security	Defender for AWS, Defender for PowerScale, ECS	✓
Metadata aware to expose asset	Golden Copy	✓

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326

metadata in the Cloud for advanced workflows	(Data Life Cycle Traceability with Embedded Metadata to Enable Software Defined Workflows)	

Conclusion

This paper reviewed key requirements for full alignment with MovieLabs 2030 vision and introduced challenges that need to be addressed in this journey. Superna's current shipping products are MovieLabs Ready with all the key requirements already available to customers.

Superna USA Inc.

3630 Peachtree Road, Suite 920, Atlanta, GA 30326