Get it to the Cloud

Evolving Your Edit Pipeline

Joel Sloss
Security Lead, Azure Engineering for M&E
Why Edit in the Cloud?

TPN is coming for you
- Security criteria based on use-cases (workloads + applications), not on cloud infrastructure
- Compliance depends on user configuration and admin policies/practices
- Editorial workflows can’t really be air-gapped anymore

Scale is getting away from you
- More channels, more clients, more shows
- Volume of content is eclipsing teams’ abilities to manage and understand
- Archives reaching into the tens-of-petabytes (or more)

Artists are nowhere near you
- Dealing with dailies and fast edit turnaround
- VFX workflows
- Production reviews
Before = On-premises

Not terrifically cloud-friendly workflows ...

Processes
- Hasn’t changed much in 20+ years
- Last major innovation was film->tape->DLE

Location
- Physical edit bays, locked rooms
- On PC / local server + NAS: Media Composer, ProTools, MediaCentral, Nexus

Workstations
- PC: Adobe Premiere Pro, Audition, ...
- Mac: Final Cut, ...
- Local storage / LTO
- Secure? Not really ...
Today’s Challenges: Internet-Connected

In order to move to the cloud you need ...

- Content protection / integrity along the workflow
- Anti-piracy during production – e.g., (forensic) watermarking
- Secure remote access and control for creators and IT
- Scalability of resources and talent
- File sizes / data volume – need fast-access to current work files
- Periodic access to archives
- High throughput, low latency, frame accuracy, audio sync, ...
- Workstation-level performance
**Tomorrow (is today): in the Cloud**

Increase access and scale now, securely

<table>
<thead>
<tr>
<th>New Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• AI processing -&gt; high-performance, intelligent storage with metadata and analytics</td>
</tr>
<tr>
<td>• Virtual browser-based workstations w/HDR, 4K, HFR</td>
</tr>
<tr>
<td>• Tiered-storage with addressable archive, accessible anywhere</td>
</tr>
<tr>
<td>• High-throughput networking for data ingest / (virtual and physical) appliances</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distributed Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>• New locations and (remote) reporting, securely and seamlessly (e.g., field editing)</td>
</tr>
<tr>
<td>• Features / episodic / unscripted – understand what you have and where, create content faster, leverage (older) assets</td>
</tr>
<tr>
<td>• Collaborate from anywhere, with anyone</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Robust Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Authenticated, encrypted storage and isolated networks over private links</td>
</tr>
<tr>
<td>• Role-based authorization, multi-factor auth, defense-in-depth</td>
</tr>
<tr>
<td>• Watermarks across all assets in the pipeline</td>
</tr>
<tr>
<td>• MAM/DAM, secure distribution/access of sensitive pre-release content</td>
</tr>
</tbody>
</table>
Components and Architecture – 1/2

What’s built and validated today for content creation

Workflow and Data
- Isolation
- Control
- Scalability
- Intelligence

1. Raw asset files
2. Files cataloged from Nearline
3. Files are synced to LTO
4. LTO files linked directly to MAM
5. LTO files linked directly to MAM
6. Media
Components and Architecture – 2/2

What studios and production companies are using right now

Services
Firewall, gateways, ER, VPN, threat management, monitoring, security management

Deployment
• Cloud-native
• Hybrid
• SaaS and IaaS
Controls for Secure Workflows
Meet the Trusted Partner Network

Best Practices in TPN – What you’ll be audited against

Editing in Azure (cloud and application security)

Storage
- AES-256, MFA, AD policy controls

Networking
- TLS 1.3, IPsec for VPNs, isolated / dedicated connections (ExpressRoute)
- Separate subscriptions

Virtual Machines
- Secure boot, standardized hardened configuration
- Host firewall + AV enabled, network routing rules

Asset Management

Information security policies / processes
- Use alias temporary titles (security titles)
- Restrict open internet access to editorial networks handling pre-release content
- Segregate between production networks

Standard operating procedures and incident responses
- Capture and report info regarding anomaly and incident reporting
- Create incident scoring and prioritization schema
- Test incident response plan yearly

Containers / libraries, secure access, auto-storage tiering
- Confidential information must be encrypted at rest
- Credentials must be authenticated at the same time during the logon process

Hybrid and Cloud-Native

Objectives and settings
- Encrypt confidential data before transferring between or within datacenters
- Content transfer system must use encryption that meets or exceeds FIPS 140-2 standards

IAM / permissions
- Account ID must identify an individual, group, role, or device
- Authentication must be done using an approved centralized authentication method
- Grant permissions based solely upon intended function for the role

Use-cases / deployments
- Content transfer system should be integrated into centralized identity provider
- Restrict transfer system access on a project basis, to individual users with business needs

Azure Meeting Control Objectives – Editorial Configuration

Portal
- Prohibit use of personal Microsoft accounts for administration
- Use separate Azure subscriptions to segregate work
- Logically relate and manage deployments with resource groups
- Avoid concurrent access from multiple locations
- Enforce custom session inactivity termination
- Enforce two-factor authentication for portal access

Network
- Use network security groups
- Isolate virtual appliances in their own subnet
- Apply a multi-tiered architecture using VNets
- Create separate VNets for production
- Limit default Network Security Group VNet communications
- Tightly configure endpoints
- Do not use deprecated cryptography when configuring IPSec VPN

RBAC
- Employ custom Role-Based Access roles to manage user access
- Extend on-premises identity management for access control
- Do not use the deprecated Azure Access Control service (ACS)

Key Vault
- Use a separate Azure Key Vault for each production
- Use Key Vault permissions to manage access
- Segregate data and key/secret owners
- Manage access to keys and secrets on a per key/secret case
- Audit all key management activity
- Periodically rotate keys

CLI
- Avoid caching session information

Batch
- Periodically update access keys
- Sanitize and destroy Batch accounts when no longer needed
- Create storage exclusively for specific Batch workflows
- Use security-validated application packages for Batch workflow
- Use integrity checks on application packages for Batch workflow
- Hold workflow if Batch applications fail
- Log Batch events for monitoring and diagnostics

Compute
- Use public key authentication for virtual machines
- Use only hardened OS images for VM instantiation

Storage
- Use Shared Access Signatures to access storage account resources
- Periodically update access keys

Cache
- Disable non-SSL connections
- Monitor cache performance

SQL
- Use separate Azure database instances for production and clients

Media
- Use separate Azure storage accounts for media service accounts
- Encrypt assets
- Configure Live Media archiving policy
Summary: Security-in-Practice

Understanding data flow and requirements – not simple, but absolutely necessary

Keep data safe wherever it is and wherever it goes
- Encryption-at-rest, IAM / RBAC-based access, TLS on connections, keys in an HSM
- Not on externally-facing server without a secured topology, even in a virtual network
- Rights management, forensic watermarking along the workflow
- Don’t put it on portable media if at all possible (or double-encrypt it)

Connecting to the internet is new for editorial / asset management
- Remote editors need to use secure workstations (a.k.a. “SAW”s) + VPN for creative work, or ...
- Browser-based virtual workstations (e.g., GPU virtual machine w/PCoIP client), thin-clients
- Restrict network ports, use IP filtering, anti-virus, client firewalls, security groups
- DDoS protection, WAF, etc. ... good to add in the virtual-appliance plane of the environment

Implement appropriate defense-in-depth strategies
- Security monitoring / logging, regular reporting, review access and usage – threat analytics
- Security automation and response (e.g., Azure Security Center), VM hardening
- Penetration-testing and Red Teaming for sensitive studio content
- Use M&E ISAC, FBI threat feeds, assign a security champion

New security configuration guidance is now available!
Azure: Industry-Leading Security and Governance for Media

Audit

Media

Industry

Security / Privacy

Architecture

Trust

Services

Platform

Tools & Guidance

Audit

Security / Privacy

Services

Tools & Guidance
Fix it in Post ...

Cloud will be the only way to get secure:

- Ubiquitous collaboration on high-density content
- Scale and performance across regions
- Comprehensive content protection
- Support for artists everywhere
- “Enrichment” from metadata
Thank You!