# Get it to the Cloud

## *Evolving Your Edit Pipeline*

Joel Sloss
Security Lead, Azure Engineering for M&E

Microsoft

# 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

### New Capabilities

- AI processing -> high-performance, intelligent storage with metadata and analytics
- Virtual browser-based workstations w/HDR, 4K, HFR
- Tiered-storage with addressable archive, accessible anywhere
- High-throughput networking for data ingest / (virtual and physical) appliances

### Distributed Production

- New locations and (remote) reporting, securely and seamlessly (e.g., field editing)
- Features / episodic / unscripted – understand what you have and where, create content faster, leverage (older) assets
- Collaborate from anywhere, with anyone

### Robust Security

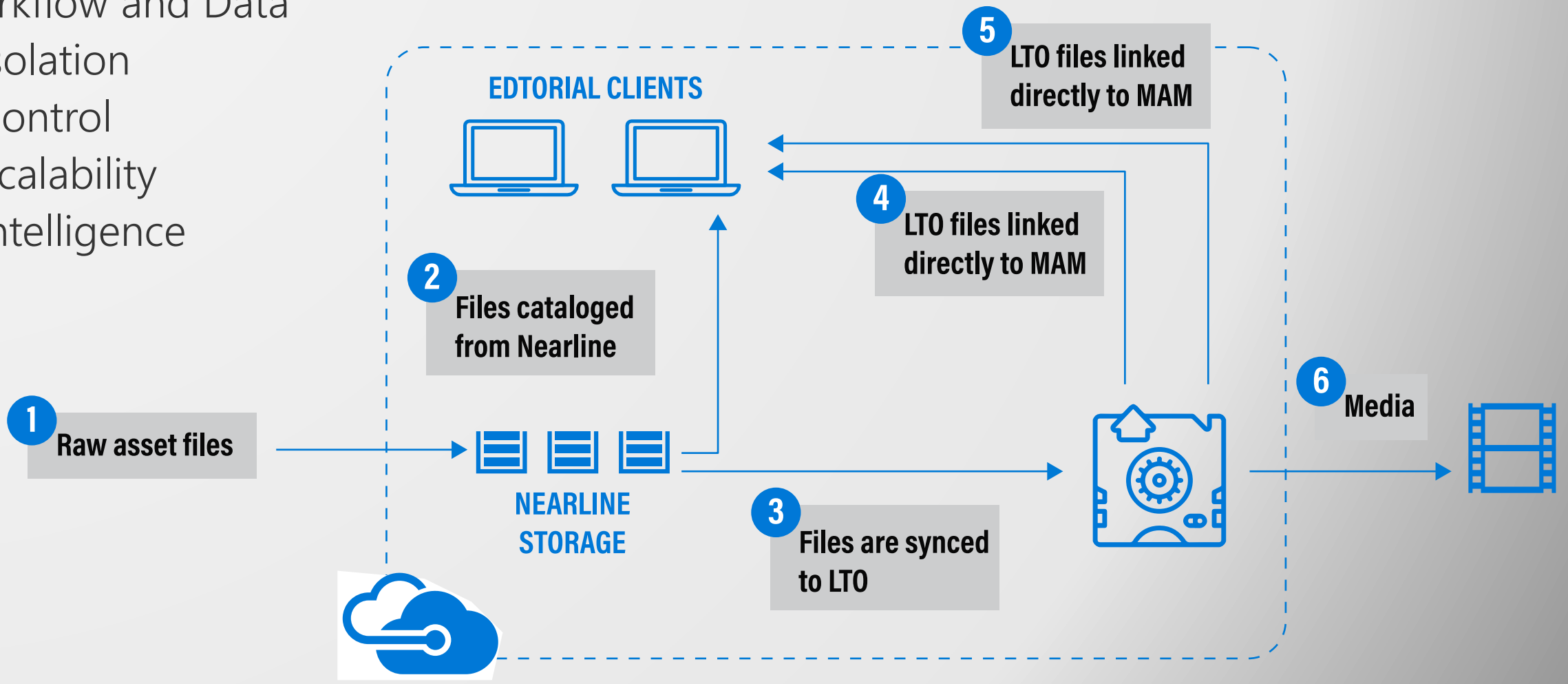
- Authenticated, encrypted storage and isolated networks over private links
- Role-based authorization, multi-factor auth, defense-in-depth
- Watermarks across all assets in the pipeline
- MAM/DAM, secure distribution/access of sensitive pre-release content

# Components and Architecture – 1/2

## What's built and validated today for content creation

Workflow and Data

- Isolation
- Control
- Scalability
- Intelligence



# Components and Architecture – 2/2

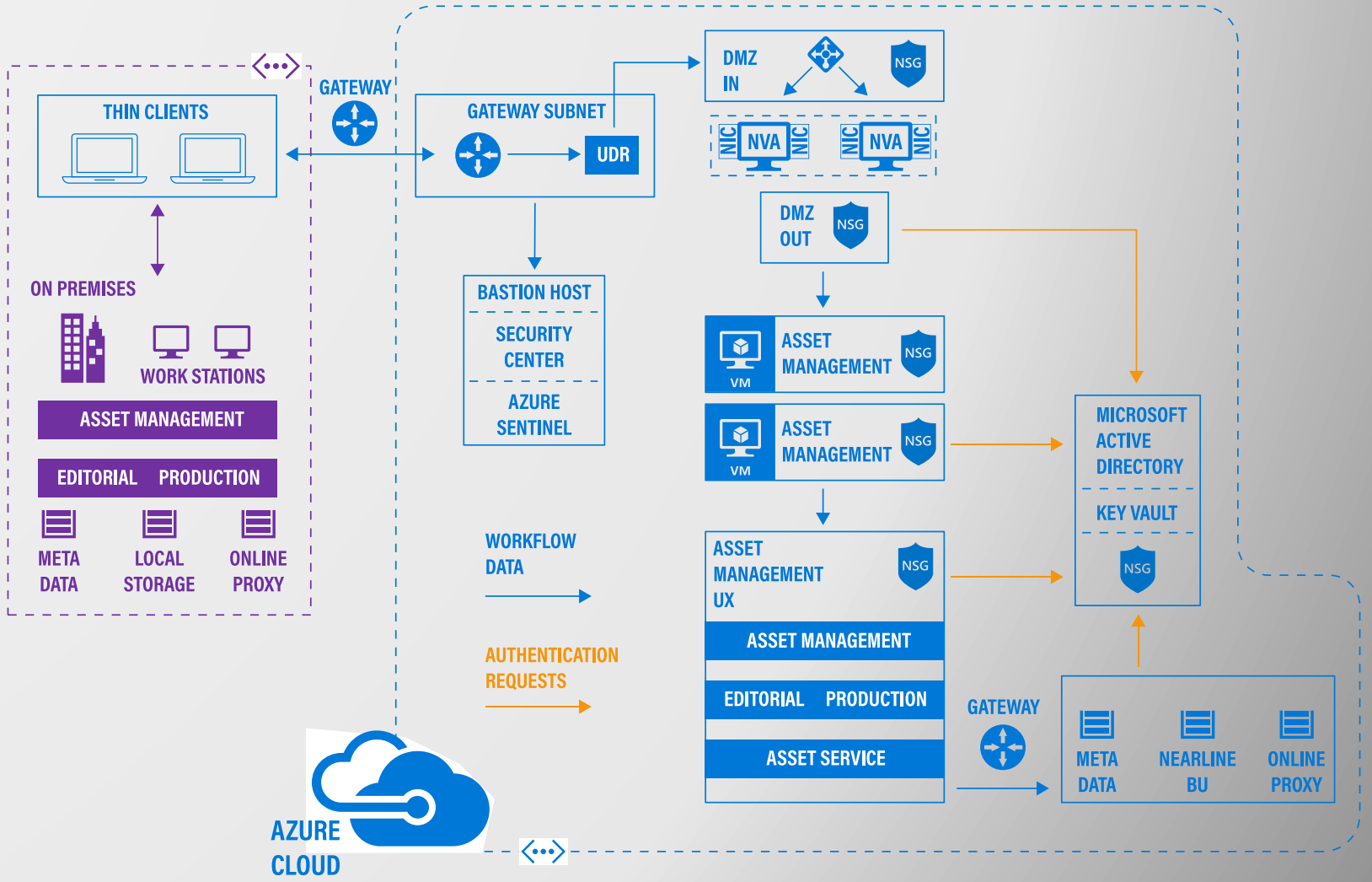
## What studios and production companies are using right now

### 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)<br>• Separate subscriptions |
| *Virtual Machines* | • Secure boot, standardized hardened configuration<br>• Host firewall + AV enabled, network routing rules |
| **Asset Management** | |
| *Information security policies / processes* | • Use alias temporary titles (security titles)<br>• Restrict open internet access to editorial networks handling pre-release content<br>• Segregate between production networks |
| *Standard operating procedures and incident responses* | • Capture and report info regarding anomaly and incident reporting<br>• Create incident scoring and prioritization schema<br>• Test incident response plan yearly |
| *Containers / libraries, secure access, auto-storage tiering* | • Confidential information must be encrypted at rest<br>• 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<br>• 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<br>• Authentication must be done using an approved centralized authentication method<br>• Grant permissions based solely upon intended function for the role |
| *Use-cases / deployments* | • Content transfer system should be integrated into centralized identity provider<br>• 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<br>• Use separate Azure subscriptions to segregate work<br>• Logically relate and manage deployments with resource groups<br>• Avoid concurrent access from multiple locations<br>• Enforce custom session inactivity termination<br>• Enforce two-factor authentication for portal access |
| Network | • Use network security groups<br>• Isolate virtual appliances in their own subnet<br>• Apply a multi-tiered architecture using VNets<br>• Create separate VNets for production<br>• Limit default Network Security Group VNet communications<br>• Tightly configure endpoints<br>• Do not use deprecated cryptography when configuring IPSec VPN |
| RBAC | • Employ custom Role-Based Access roles to manage user access<br>• Extend on-premises identity management for access control<br>• Do not use the deprecated Azure Access Control service (ACS) |
| Key Vault | • Use a separate Azure Key Vault for each production<br>• Use Key Vault permissions to manage access<br>• Segregate data and key/secret owners<br>• Manage access to keys and secrets on a per key/secret case<br>• Audit all key management activity<br>• Periodically rotate keys |
| CLI | • Avoid caching session information |
| Batch | • Periodically update access keys<br>• Sanitize and destroy Batch accounts when no longer needed<br>• Create storage exclusively for specific Batch workflows<br>• Use security-validated application packages for Batch workflow<br>• Use integrity checks on application packages for Batch workflow<br>• Hold workflow if Batch applications fail<br>• Log Batch events for monitoring and diagnostics |
| Compute | • Use public key authentication for virtual machines<br>• Use only hardened OS images for VM instantiation |
| Storage | • Use Shared Access Signatures to access storage account resources<br>• Periodically update access keys |
| Cache | • Disable non-SSL connections<br>• Monitor cache performance |
| SQL | • Use separate Azure database instances for production and clients |
| Media | • Use separate Azure storage accounts for media service accounts<br>• Encrypt assets<br>• Configure Live Media archiving policy |

# Summary: Security-in-Practice

New security configuration guidance is now available!

## 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

# Azure: Industry-Leading Security and Governance for Media

**Audit**

Media

- CDSA Content Protection & Security Program
- MOTION PICTURE ASSOCIATION OF AMERICA
- TPN TRUSTED PARTNER NETWORK
- FACT
- CSA cloud security alliance
- COMMITTED TO SECURITY dpp

Industry

- ISO 27001 Certified
- AICPA SOC SERVICE ORGANIZATIONS aicpa.org/soc Formerly SAS 70 Reports
- PCI
- +70 others

**Security / Privacy**

Architecture

- Encryption-at-Rest
- Tenant Isolation
- Global Resiliency
- Threat Protection

Trust

- Monitoring & Analytics
- Control
- Transparency
- Strong legal protections
- GDPR
- Privacy

**Services**

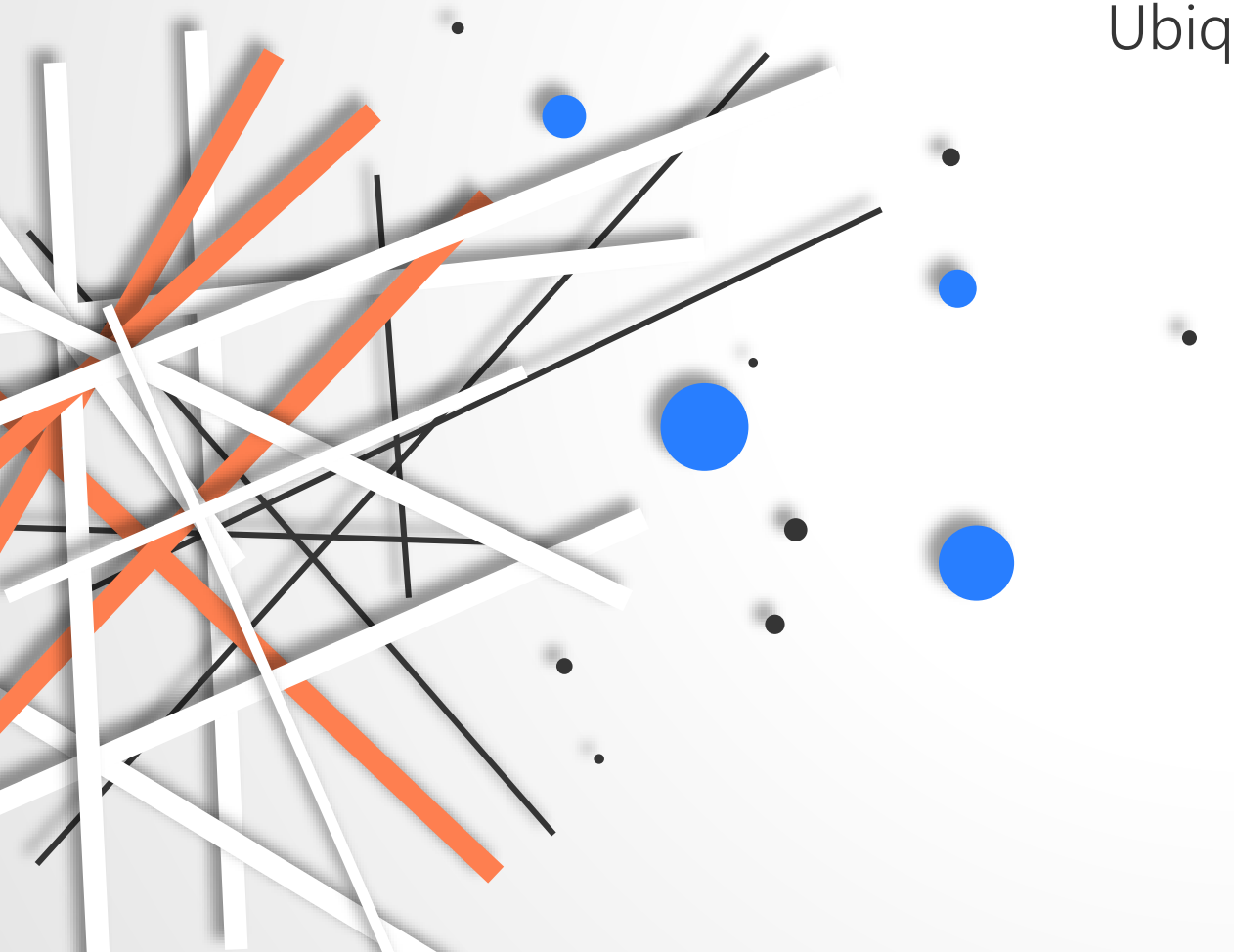
Platform

- Security Center
- Application Gateway
- Azure Active Directory
- Azure DDoS Protection
- Key Vault
- Azure Information Protection

Tools & Guidance

- Intelligent Security Graph
- HSE Independent security evaluators
- Media-specific security qualifications & best practices
- Azure Compliance Manager
- Azure Blueprints

# 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!*