Security in the Media Business

Actionable insights for modern media platforms.

KEY TAKEAWAYS

- Identity is the new security perimeter
- Zero Trust is essential for modern media workflows
- Layered defenses prevent catastrophic breaches
- Least privilege reduces insider and accidental risk
- Security is shared – and must be actively managed

1 BUILD ON PROVEN SECURITY FOUNDATIONS

INSIGHT: SECURITY MUST BE SYSTEMATIC, NOT IMPROVISED.

- [ ] Apply CIA triad (Confidentiality, Integrity, Availability) across all workflows
- [ ] Enforce authentication, authorization, and accountability everywhere
- [ ] Use established standards (not custom security models)
- [ ] Ensure controls are consistent across every system layer

2 ADOPT A ZERO TRUST MODEL

INSIGHT: EVERY ACCESS MUST BE EXPLICITLY VERIFIED.

- [ ] Verify every user, system, and request
- [ ] Remove implicit trust between cloud, on-prem, and partners
- [ ] Assume breach is already possible
- [ ] Validate access continuously, not just at login

3 IMPLEMENT DEFENSE-IN-DEPTH

INSIGHT: ONE LAYER OF SECURITY IS NEVER ENOUGH.

- [ ] Enforce protection at API, service, and data layers independently
- [ ] Prevent direct access to sensitive content storage
- [ ] Ensure failure in one layer does not expose assets

4 MAKE IDENTITY YOUR PRIMARY CONTROL PLANE

INSIGHT: THINK IDENTITY; NOT PERIMETER.

- [ ] Use federated identity (OpenID Connect - OIDC)– don't store passwords locally
- [ ] Enforce Multi-Factor Authentication (MFA) and conditional access policies
- [ ] Centralize identity across all tools and workflows

More ›

5 ENFORCE LEAST PRIVILEGE WITH ROLE-BASED ACCESS

INSIGHT: PERMISSIONS BEYOND MINIMAL NEED UNDERMINE ALL OTHER CONTROLS.

- [ ] Map roles to real production personas (editor, journalist, admin)
- [ ] Apply least privilege by default
- [ ] Prevent privilege escalation beyond defined roles
- [ ] Enforce separation of duties

6 ISOLATE CONTENT, TENANTS, AND PRODUCTIONS

INSIGHT: UNINTENTIONAL CROSS-TENANT ACCESS CONSTITUTES A BREACH.

- [ ] Enforce strict tenant isolation across all layers
- [ ] Default to fail-closed behavior
- [ ] Continuously validate isolation with testing

7 SECURE AUTOMATED & MACHINE WORKFLOWS

INSIGHT: UNVERIFIED MACHINES – SAME RISK AS UNVERIFIED USERS.

- [ ] Authenticate all systems and integrations explicitly
- [ ] Use scoped, rotating credentials
- [ ] Restrict credentials by function and environment
- [ ] Prevent compromised services from expanding access

8 ENCRYPT EVERYTHING BY DEFAULT

INSIGHT: PROTECTION MUST FOLLOW CONTENT EVERYWHERE.

- [ ] Encrypt all data in transit and at rest
- [ ] Separate key management from storage
- [ ] Make encryption automatic – not configurable

9 MAKE AUDIT LOGGING IMMUTABLE AND COMPLETE

INSIGHT: NON-REPUDIATION – A MUST FOR TRUST AND INCIDENT RESPONSE.

- [ ] Log all authentication, access, and authorization events
- [ ] Ensure logs are tamper-proof and cannot be deleted
- [ ] Control and monitor who can view logs
- [ ] Use logs for compliance and incident response

10 ACTIVELY MANAGE YOUR SHARE OF SECURITY RESPONSIBILITY

INSIGHT: SECURITY CONTROLS ONLY PROTECT WHAT IS CORRECTLY CONFIGURED.

- [ ] Enforce MFA and identity policies at your identity provider
- [ ] Maintain accurate roles and rapid user deprovisioning
- [ ] Rotate and manage credentials securely
- [ ] Classify sensitive content correctly
- [ ] Actively monitor access patterns, not just alerts

Avid Content Core is founded on these security principles.

Discover how it can help teams modernize their infrastructure securely and without disruption.

avid.com/content-core