Innovate Fast without Sacrificing Security

APIs in Media & Entertainment... why it matters.
October 20, 2020

Media and Entertainment Day
Data, Cloud, AI, Security
Disney Elevates Streaming Business in Major Reorganization

Company forms new content and distribution arms as pandemic hammers entertainment industry
What are we trying to achieve in M&E?

Digital Transformation is losing strong meaning; however, the identified market changes have not. Today’s enterprise needs to be focused on becoming dynamic. The **Dynamic Enterprise** will pivot and introduce new capabilities daily as the new norm.

- **Become Agile**
  Create an organization, processes and practices that embrace quick turns and changes in direction

- **Accelerate**
  Accelerate the delivery of new channels of engagement, accelerate creation of new capabilities, and accelerate integrations into core business platforms

- **Reduce Risk**
  Reducing risk is a balance of JIT systems, services and oversight that enable safety @ speed

- **Transform**
  Be intentional about enabling the success of these new digital practices by implementing the right organization, funding, incentives, and delivery paradigms
Considering the M&E Consumer

The rise of consumer rights.

Studios, networks and streamers are proactively focusing on the collection, storage and use of consumer data to increase trust and gain loyalty.

- GDPR
- CCPA
- Consumer Transparency
- Ethical AI
- Ethical Data Usage
- Hyper-Personalization
More Digital ➔ More Data ➔ More Risk
A recent ScreenMedia report found that **28%** of media organizations admit to having experienced a cyber attack of some type or another.
“API traffic surprised us by revealing that 83% of the hits we see are API driven.”

This is an astounding lift from just 47% in 2014.
“This shift in traffic patterns has significant ramifications in the security industry. Many, if not most, controls that have been historically used to protect the servers and systems that are the origin of traffic are focused on monitoring browser traffic.

The mechanisms necessary to apply the same controls to API traffic may be less robust, harder to configure, or nonexistent in certain environments.”
Top 10 Causes for API Breaches

1. Broken Object Level Authorization
2. Broken Authentication
3. Excessive Data Exposure
4. Lack of Resources & Rate Limiting
5. Broken Function Level Authorization
6. Mass Assignment
7. Security Misconfiguration
8. Injection
9. Improper Assets Management
10. Insufficient Logging & Monitoring

Why is this happening?

Common API breaches are due to:

• The shift from a tightly-coupled integration world to APIs which are loosely coupled
• Failing to modify architecture and security practices to match this new paradigm.
How API Security is Typically Handled

Development Process

1. Standards
2. Development Practices
3. Development
4. PMO Gates
   - Team review before moving to production
5. Monitoring & Detection
   - Utilization of Security monitoring and detection practices

Detect and Treat
Shift left in the development process and move faster

Development Process

1. Standards
   - Data Storage Practices
   - Data Risk Management
   - Identity & Access Controls

2. Development Practices
   - App Design Standards
   - Approved Design Patterns
   - Ready Reference Architectures

3. Development
   - Pre-built
   - Pre-approved
   - Continuous Testing

4. SecDevOps
   - Risk-based Automation
   - Risk-based Certification Process

5. Monitoring & Detection
   - Utilization of Security monitoring and detection practices
   - Manual Audit

Prevent