Securing Creativity in the Cloud: How a Digital Media Leader Protected Content Rights, Streaming Platforms, and Compliance with Invinsense

About the Customer

This legacy-rich media and entertainment house has evolved into a digital powerhouse, with an expansive content library distributed across OTT platforms, mobile apps, connected TVs, and global streaming partners. From original productions and Bollywood classics to devotional content and animation, the company serves diverse audiences in over 30 countries. With growing investments in digital distribution, monetization platforms, and regional language IPs, protecting content integrity, audience trust, and digital infrastructure has become a strategic priority.

Industry	Digital Media & Entertainment
Challenge	Content security, platform abuse prevention, and rights compliance across digital channels
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

As the business scaled its digital reach, it faced complex and rising cybersecurity threats:

High-value digital content vulnerable to piracy, leaks, and unauthorized redistribution

OTT platforms and streaming APIs increasingly targeted by credential sharing, session hijacking, and scraping bots

Partner portals and monetization dashboards exposed sensitive licensing, analytics, and revenue data

Regulatory obligations across IP rights management, data retention (IT Act), and platform compliance standards

Fragmented visibility across mobile apps, cloud infrastructure, and third-party syndication feeds

- Need for proactive detection of insider threats and fraud actors within distribution pipelines

The Invinsense Solution

To safeguard content, user trust, and platform compliance, the company deployed the complete Invinsense suite to bring together detection, validation, deception, and governance under one strategic program.

Invinsense XDR: Securing Content, Streams, and Sessions

Invinsense XDR integrated with the firm's OTT APIs, CDN logs, subscriber platforms, and monetization dashboards to deliver unified detection and response.

Key Results:

- 59% reduction in stream abuse (unauthorized sessions, link sharing
- Improved alert accuracy across cloud-native content delivery systems by 61%
- 74% drop in false positives via behavior-based stream monitoring
- Mean time to detect credential theft incidents dropped to 3.8 minutes

Invinsense OXDR + CTEM: Exposure Management Across Content Ecosystem

The firm operationalized CTEM using Invinsense OXDR to validate and close real-world risks in content systems and partner integrations.

Scoping	• Identified 3,200+ digital assets, including OTT APIs, content scheduling tools, mobile apps, and analytics platforms • Shadow APIs (legacy feeds, test CDNs) accounted for 17% of the exposed surface
Discovery	• Detected 138 critical exposures including insecure API tokens, excessive CDN permissions, and outdated DRM libraries • Noticed partner-facing admin panels with weak authentication
Prioritization	• Focused on risks affecting subscriber data, licensing workflows, and unreleased content • Ranked top 20 vulnerabilities by monetization impact and legal risk
Validation	• Simulated piracy tools to emulate content scraping via leaked session tokens • Simulated escalations from user support platforms into backend media storage
Mobilization	• Closed 81% of validated issues in the first 45 days • Automated remediation and testing through CI/CD pipelines tied to DRM and stream APIs

Key Result

- 59% reduction in streaming abuse incidents
- 3.9x faster validation of API exposures in OTT platforms
- 88% compliance alignment with digital IP and broadcasting norms
- 6.2x increase in threat detection precision using deception

Executive Insight

"As a content-driven company, protecting our digital assets is core to our brand. Invinsense allowed us to go beyond prevention — we now detect, deceive, and defend in real-time, across every channel."

CTEM Outcomes

- 3.9x faster validation of content-serving exposures
- 67% reduction in mean patch-to-deploy time
- 4x improvement in test coverage across OTT release branches

Invinsense XDR+: Deception to Trap Piracy Bots and Fraud Access

Deception layers were deployed to mimic unreleased content libraries, dev portals, and revenue analytics to trap insider misuse and bot automation.

Results:

6.2x increase in attacker detection through fake OTT endpoints	Detected 4 unique credential stuffing scripts within 10 days of deployment	Decoy dashboards helped flag unusual access behavior from syndication partners	Raised early alerts on anomalous access to devotional content catalog from restricted regions

Invinsense GSOS: Simplifying Compliance with IP Rights and Platform Mandates

GSOS mapped security and operational controls to frameworks governing digital content distribution and broadcasting compliance, including:

IT Act Section 72A (data protection for digital platforms)	Content rights management standards (digital watermarking & access control)	Internal legal policies for release embargo enforcement	SaaS partner audit guidelines for analytics and licensing platforms

Compliance Results:

88% alignment with IP protection and digital content compliance standards	Internal audit cycles reduced from 14 to 4 days	All legal and tech stakeholders onboarded to a unified control dashboard	Real-time visibility into rights access logs across business functions

Quantifiable Impact

Category	Improvement
Streaming Abuse Incident Rate	↓ 59%
Mean Time to Detect (Credential Theft)	↓ to 3.8 mins
Exposure Validation Cycle	↑ 3.9x faster
Deception Detection Accuracy	↑ 6.2x
Compliance Control Coverage	↑ 88%
Internal Audit Preparation	↓ from 14 to 4 days

Conclusion

For digital media platforms navigating the threats of piracy, platform abuse, and compliance scrutiny, proactive cybersecurity is a strategic necessity. This customer used Invinsense to build a multi-layered defense that protects content, supports legal obligations, and ensures trust — from creation to consumer.

Infopercept | INVINSENSE

Imprint

Contact
sos@infopercept.com
www.infopercept.com/knowledge/casestudy