AUTODESK

Safeguarding creative IP in the era of AI and the cloud

How Autodesk Flow Capture helps media & entertainment studios protect what matters most.

Contents

SECTION 1

Introduction

The media and entertainment (M&E) industry has always thrived on transformation. From celluloid to videotape to digital media, from early 8- and 16-bit games to the teraflops of today's leading consoles, innovation is a constant.

With every new wave of technology, creative teams have expanded what's possible, telling stories and building worlds that surprise, move, and inspire global audiences in new ways.

But every leap forward comes with new risks. Today, as production workflows shift to the cloud, teams collaborate from anywhere, and as AI becomes not just a fad but a proven tool, protecting intellectual property (IP) has become one of the most urgent challenges facing film, television, and video game studios.

This white paper explores those challenges in depth and shows how Autodesk Flow Capture provides a secure foundation for this new era of creativity. Built with industry-leading safeguards and aligned with initiatives like the MovieLabs 2030 Vision, Flow Capture enables studios to create with confidence: secure, connected, and future-ready.

Context

Creativity, collaboration, and control

For decades, studios relied on centralized facilities and linear processes: film labs, post houses, and VFX vendors, each operating on tightly controlled networks.

Content was moved on encrypted drives or private fiber lines, with dedicated IT teams maintaining perimeters.

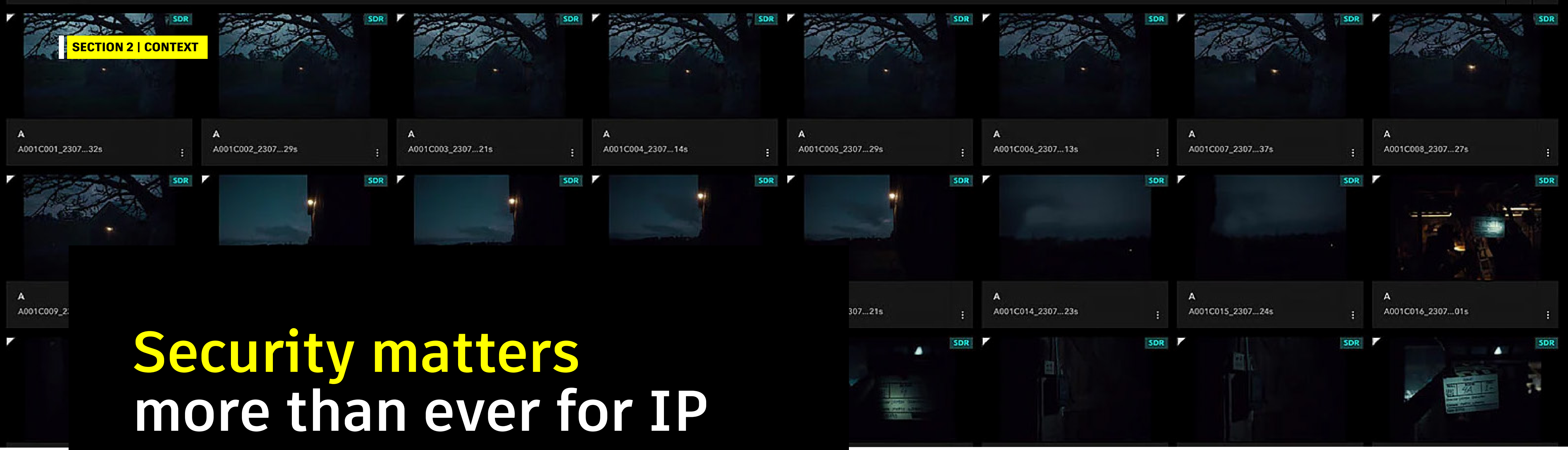
Game studios operated in a similar way.

Those days are gone. Today:

- Productions are increasingly cloud-based.
- Teams are dispersed across continents.
- Collaboration happens in real time, across dozens of vendors and hundreds of contributors.

Cloud production unlocks powerful new workflows—parallel editing, camera-to-cloud review, single sources of truth—but also demands a security architecture designed for a borderless world.

The stakes couldn't be higher: the integrity of the creative process itself—and, in turn, the creative output.



Security matters more than ever for IP

In media and entertainment, intellectual property *is* the product. Scripts, storyboards, characters, code, shots, sequences, and final edits—every asset requires investment and carries significant commercial value. And unlike many industries, entertainment projects pass through countless hands before release: artists, production teams, contractors, financiers, agencies, distributors. Each adds risk.

What makes M&E IP especially vulnerable:

Multi-party collaboration: Dozens of vendors with different IT systems and practices.

High-value targets: The more popular and recognized the IP, the more it attracts cybercriminals.

Time sensitivity: Leaks before release can devastate revenue and marketing strategies.

Evolving threats, existential dangers

Yesterday's threats came from rogue hackers seeking notoriety or a chance to share anticipated media on peer-to-peer networks. Today's attackers are organized criminal enterprises, motivated by profit.

They:

- Steal pre-release content for illegal distribution.
- Sell IP or credentials to competitors.
- Target consumer-facing platforms to hijack accounts.
- Release confidential communications to damage corporate reputations

Physical protection is no longer enough. Security must travel with the asset, no matter where it goes. Studios need systems built for a world of distributed, digital-first collaboration, systems that support creatives and connect workflows, while protecting production processes—and the media you create.

Key challenges facing IP security

Remote work: New flexibility, new security frontiers

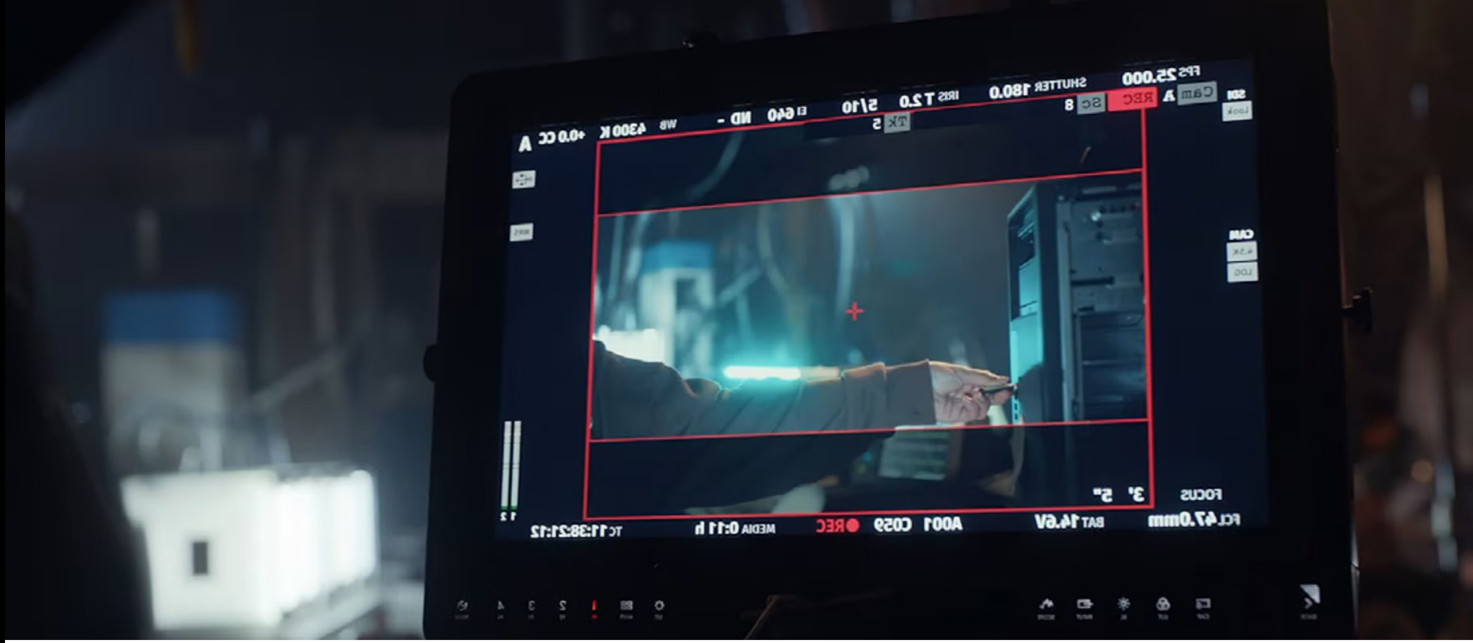
The shift to remote and hybrid work has been one of the most profound changes in media and entertainment over the past decade. The global lockdown sped up this transition in a significant way.

What began as an emergency adaptation has now become an enduring reality. Studios, production houses, and game developers are building teams across continents, relying on cloud workflows, and connecting talent who may never share the same physical space.

That evolution has unlocked enormous creative potential. Distributed workflows enable parallel workstreams, real-time collaboration, and camera-to-cloud pipelines that accelerate production from capture to post. But they also carry a hidden cost: a vastly expanded security perimeter and a more complex challenge in safeguarding intellectual property.

The new security landscape of distributed production

When creative work can happen anywhere, risks multiply. Instead of protecting a single facility's network, companies now need to secure hundreds—sometimes thousands—of endpoints across home offices, personal devices, and third-party networks. Each represents a potential entry point for a breach.



Some of the most common vulnerabilities include:

- **Expanded attack surface:** Every home router and remote device is now part of your network. Most don't match enterprise-grade security.
- **Insecure Wi-Fi:** Many home networks use default passwords or outdated encryption, leaving sensitive transfers exposed.
- **Unsecured personal devices:** Bring-your-own-device policies, while convenient, can introduce malware or outdated software into the production ecosystem.
- **Shadow IT:** Unauthorized apps and cloud services create blind spots for IT teams and risk data leakage.
- **Weak encryption practices:** Files shared or stored without robust encryption are easy targets for interception or theft.[1]

[1] Cybersecurity in a Remote Work Era: Strategies for Securing Distributed Workforces, Nikhil Bhagat, pp. 2-3

Complexity grows as teams expand

Productions today can involve hundreds of collaborators—from directors and VFX artists to marketing teams and freelance editors. Many juggle multiple projects simultaneously, often across different studios. Managing identities and access under these conditions is no small task. One studio estimated that a single user might need to log into 50 different platforms, each with its own authentication requirements.[2] The result? Password reuse, sticky notes, and other workarounds that undermine even the most stringent security policies.

Remote work is here to stay. The challenge for M&E companies isn't whether they can embrace distributed collaboration; it's how they can do so securely, without slowing down creativity or putting valuable IP at risk.

Insight

Every time a file is shared, transferred, or downloaded, it introduces a potential point of failure—from data corruption and metadata loss to accidental leaks. As file sizes and complexity grow, so too does the risk.

[2] 2030 Vision Series: The Evolution of Media Creation, MovieLabs, p. 14

Security breaches and data leaks: The growing threat to creative IP

If remote work has expanded the battleground for IP security, then the rising wave of cyberattacks has raised the stakes. The media and entertainment industry has become a lucrative target for cybercriminals. Data breaches and leaks are more frequent, more sophisticated, and more damaging than ever before. And for studios, production companies, and game developers, the stakes couldn't be higher: unreleased content, proprietary technology, and sensitive business data represent not just creative assets, but the lifeblood of the business.

An uneven playing field

The reality of cybersecurity is brutally simple: defenders need to be right every single time, while attackers only need to find one weakness. No system used by humans can ever be perfectly secure, and the tools available to threat actors are only getting stronger.

Cloud-based exploits, ransomware-as-a-service platforms, and phishing kits are readily available on the dark web. Even more sophisticated threats—like those leveraging AI for social engineering or, eventually, quantum computing—are already shaping the future threat landscape.[3] Meanwhile, the value of stolen content is growing. Global audiences are looking for it and even coming to expect it. This makes media and entertainment IP a prime target for well-funded, organized groups motivated by profit rather than notoriety or popularity.

[3] 2030 Vision Series: The Evolution of Media Creation, MovieLabs, p. 14

Real world, real consequences

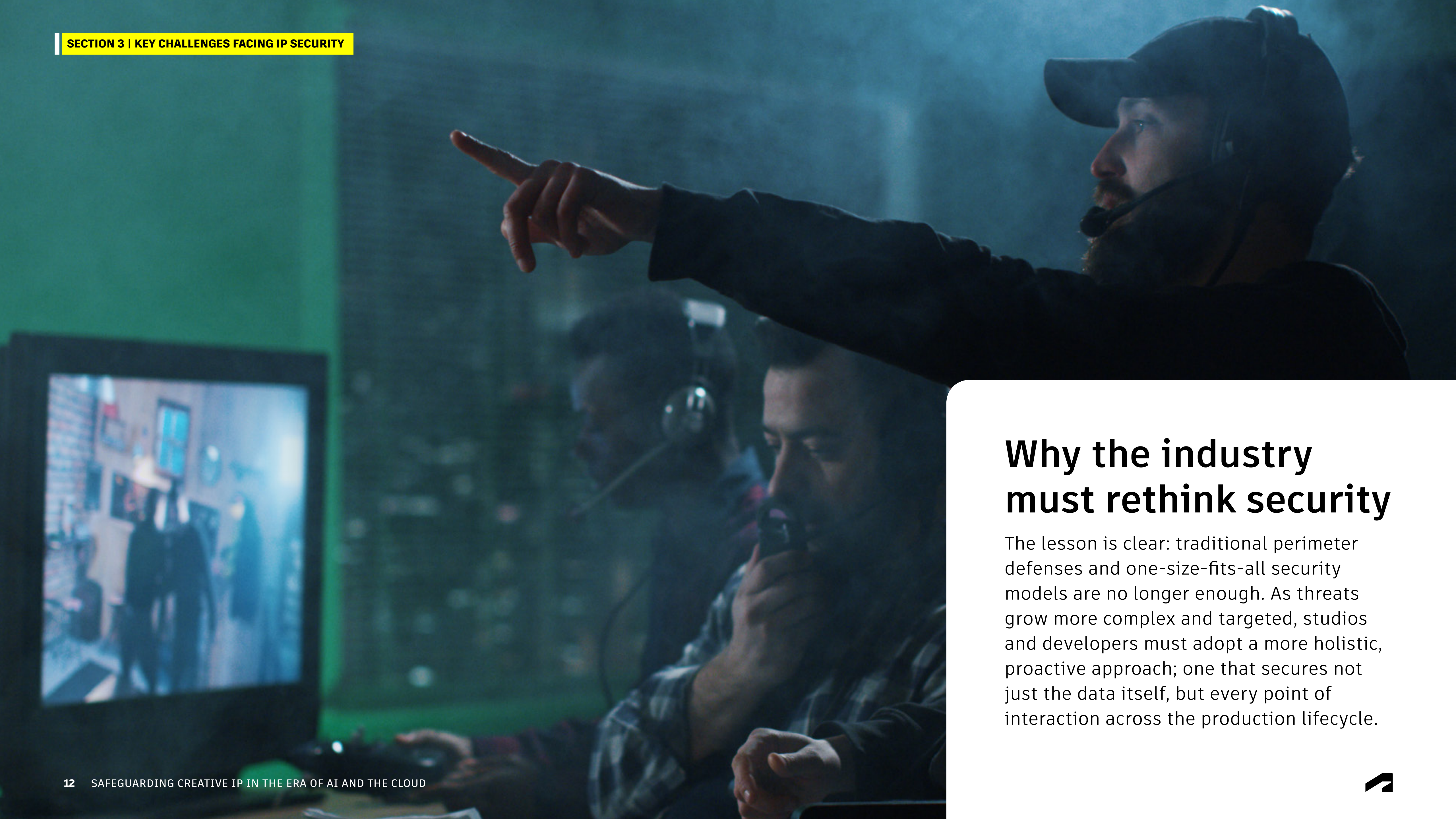
When a breach occurs, the fallout is swift and far-reaching. Unauthorized access can expose unreleased footage, confidential scripts, internal communications, and consumer data, all before a single frame or pixel hits the screen. The consequences ripple across every facet of a company's operations:

- **Financial loss:** Stolen content can undermine box office or launch-day revenue.
- **Operational disruption:** Development schedules can be delayed, halted, or completely derailed.
- **Legal exposure:** Breaches can lead to costly lawsuits, fines, and compliance penalties.
- **Reputational damage:** Once trust is broken, rebuilding relationships with partners, talent, and audiences can take years.

From leaked game builds and hijacked streaming accounts to stolen scripts and internal data dumps, recent high-profile incidents have shown how vulnerable even the largest organizations can be. And these are no longer isolated acts by lone hackers; they're coordinated campaigns by cybercrime syndicates treating IP theft as a scalable business.

Insight

Protecting creative IP isn't just about keeping attackers out; it's about minimizing the damage when they get in. Resilience, rapid detection, and smart access control are as critical as prevention.



Why the industry must rethink security

The lesson is clear: traditional perimeter defenses and one-size-fits-all security models are no longer enough. As threats grow more complex and targeted, studios and developers must adopt a more holistic, proactive approach; one that secures not just the data itself, but every point of interaction across the production lifecycle.

The AI factor: Innovation meets new IP risks

Few technologies are reshaping media and entertainment as rapidly as artificial intelligence.

From accelerating post-production workflows to generating visual effects, localizing content, and even drafting dialogue, AI is unlocking new levels of speed, creativity, and efficiency. It's transforming how studios, production companies, and game developers bring ideas to life—and how audiences experience them.

But while the creative upside is enormous, the adoption of AI also introduces a new class of risks that most organizations were barely thinking about just a few years ago.

The question is no longer just "Can someone steal our IP?" It's also "Can we accidentally compromise it ourselves?"

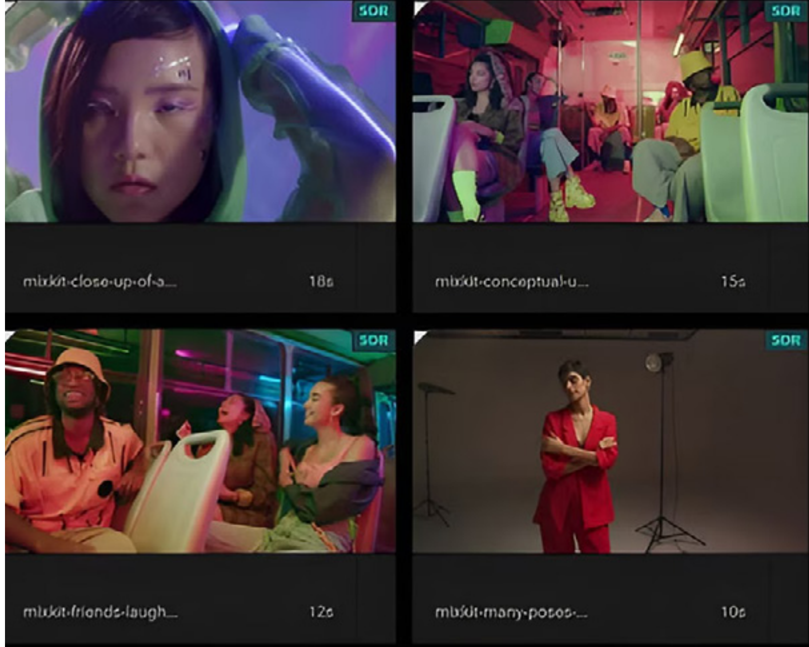
Workflow integrity in the age of AI

Traditionally, “workflow integrity” meant ensuring that what emerges from a creative process is exactly what was intended. But AI is changing that definition. When models generate assets, make editorial decisions, or fill in creative gaps, the output can diverge from the original vision—sometimes subtly, sometimes dramatically. And the risks don’t just affect the content itself. They extend to legal exposure, brand reputation, and the fundamental questions of creative authorship and ownership.

Emerging threats to IP security and integrity

As AI becomes woven into more stages of production and distribution, it brings with it a range of new security challenges that demand careful attention:

- **Unintentional IP infringement:** Generative models trained on copyrighted material can replicate protected content in new outputs, raising legal and ethical questions about ownership and liability.
- **Loss of attribution:** AI-generated work can obscure authorship, complicating royalty tracking, licensing, and compliance.
- **Deepfakes and synthetic media:** Hyper-realistic media can be misused to manipulate, mislead, or damage reputations, sometimes without the creator’s knowledge.[4]
- **Data leakage in model training:** Using sensitive or unreleased material to train internal models can result in that content reappearing in future outputs.
- **Pipeline vulnerabilities:** Each API, plugin, or cloud integration in an AI workflow introduces a potential breach point if not properly secured.
- **Bias and ethical risk:** Outputs that reflect bias in training data can harm a brand’s credibility and audience trust.[5]



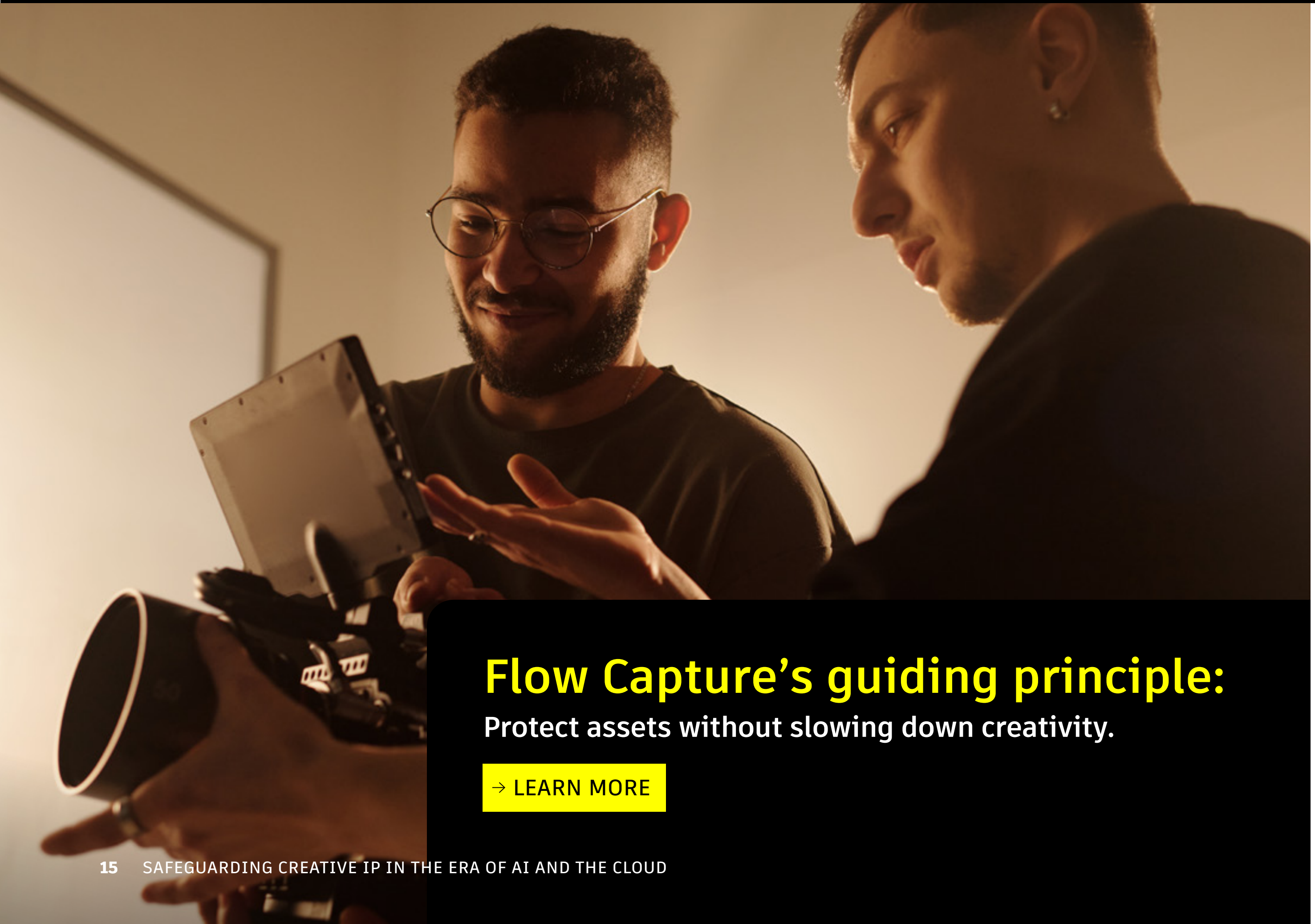
Insight

The threat landscape for IP is no longer just external; it’s also emerging from inside the creative process. Managing AI responsibly means not only protecting against theft but also ensuring your own tools don’t inadvertently put your IP, reputation, or business at risk.

[4] AI In Entertainment: 19 Practical And Ethical Challenges, Forbes
[5] The Uncanny Threat: Unraveling the Dangers of AI in the Entertainment Industry, Boesch Law Group

SECTION 5

Autodesk Flow Capture: Purpose-built for security



Flow Capture’s guiding principle:

Protect assets without slowing down creativity.

→ LEARN MORE

Autodesk Flow Capture (formerly Moxion and PIX) is designed for this moment. More than a digital dailies and review platform, it’s a secure, unified environment for production and post-production teams.

Flow Capture brings together the best of Moxion and PIX into one powerful toolset. By combining the strengths of both platforms, production teams gain access to best-in-class dailies workflows, real-time review, and world-class support - all in a single, unified product.

It offers:

- **Studio-grade security** embedded by design.
- **Seamless collaboration** across distributed teams.
- **Compliance with industry standards**, including the MovieLabs 2030 Vision, TPN, and ISO/IEC 27001.

Best-in-class security features

Flow Capture offers a layered approach to IP protection:

Encryption and access controls

- End-to-end encryption for files in transit and at rest.
- Multi-factor authentication (MFA) and single sign-on (SSO) access.
- Granular, role-based permissions down to individual assets.

Collaboration without compromise

- Secure Flow Capture Rooms for synced, live reviews.
- Dynamic watermarking to deter leaks.
- Frame-level annotations and live chat for precise feedback.
- Integrations with tools like Flame, AVID Media Composer, and Flow Production Tracking to reduce the need for file transfers between platforms.

Enterprise-grade safeguards

- Digital rights management (DRM) to prevent unauthorized use.
- Forensic watermarking for traceability.
- Continuous audit logs and real-time monitoring of all activity.
- Regular penetration tests and compliance audits.

A unified platform reduces risk

By consolidating review and collaboration in Flow Capture, studios eliminate the need to shuttle files across multiple tools and platforms, reducing both risk and complexity.

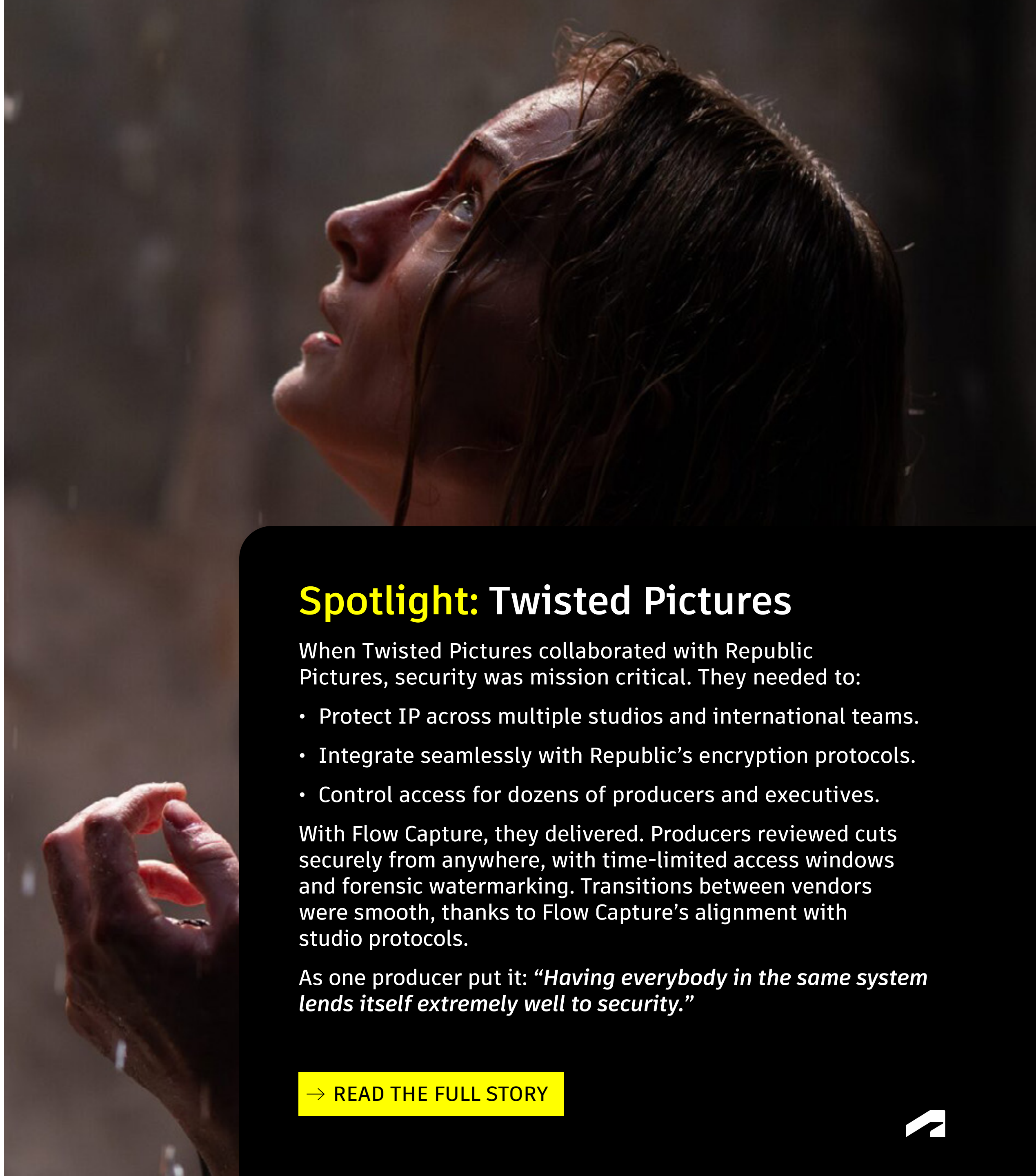
Built for compliance

Studios live and die by trust. Flow Capture supports compliance with the most demanding industry standards:

- **MovieLabs 2030 Vision:** Cloud-native, secure-by-design workflows.
- **TPN (Trusted Partner Network):** Industry-wide vendor security evaluation.
- **ISO/IEC 27001:** International standards for information security.
- **SOC2:** Security framework for service organizations to protect customer data.
- **MPAA Guidelines:** Major studio security mandates.

Compliance isn't just about checking boxes. It's about being eligible for the most prestigious projects—the ones where security is non-negotiable.

→ LEARN MORE ABOUT FLOW CAPTURE



Spotlight: Twisted Pictures

When Twisted Pictures collaborated with Republic Pictures, security was mission critical. They needed to:

- Protect IP across multiple studios and international teams.
- Integrate seamlessly with Republic's encryption protocols.
- Control access for dozens of producers and executives.

With Flow Capture, they delivered. Producers reviewed cuts securely from anywhere, with time-limited access windows and forensic watermarking. Transitions between vendors were smooth, thanks to Flow Capture's alignment with studio protocols.

As one producer put it: ***"Having everybody in the same system lends itself extremely well to security."***

→ READ THE FULL STORY

Best practices for secure workflows

Protecting intellectual property in today's media and entertainment landscape isn't about locking down a single server or setting a complex password. It's about building a holistic, proactive security posture that spans every stage of the production lifecycle—from concept and capture to post-production, marketing, and distribution. And as workflows become more distributed, cloud-based, and AI-driven, those best practices are evolving too.

Whether you're a small production house or a global game studio, embedding security into the very fabric of your creative operations is now a strategic necessity.

01 Build a security-first culture

Security can no longer be treated as a final step in the pipeline; it must be woven into every stage of production. That means shifting the focus from infrastructure alone to the workflows themselves, and from where assets are stored to how they're handled. Protecting the integrity of creative content requires that every file, every process, and every decision is secured from the outset.

A security-first mindset also means constant vigilance: staying ahead of evolving threats, updating policies as new technologies emerge, and treating IP protection as a shared responsibility across the entire team.

02

Centralize and simplify workflows

Complex workflows increase the number of potential vulnerabilities. By consolidating production processes into a secure, centralized environment, studios can reduce attack surfaces, streamline access management, and minimize opportunities for accidental leaks or unauthorized sharing. Centralization also supports consistent policy enforcement—a crucial factor for compliance with industry standards and client requirements.

03

Control access with precision

Not everyone needs access to everything. Implementing role-based access controls and granular permissions ensures that individuals can only view, edit, or distribute the content relevant to their role. The industry is moving toward a universal identity system—a single “Production User ID”—that would allow studios to validate every collaborator’s identity and manage permissions with far greater precision.[6]

04

Strengthen authentication and oversight

Multi-factor authentication (MFA) should be standard practice for anyone accessing production assets. Beyond access control, watermarking and detailed audit trails add powerful layers of security, deterring unauthorized distribution and providing valuable visibility into who accessed what, when, and from where.

05

Secure collaboration and keep policies current

Remote collaboration is here to stay, but it must be done securely. Encrypted connections, browser-based review tools, and regular security audits all help safeguard distributed teams. Just as important is the human factor: ongoing security training empowers team members to recognize phishing attempts, avoid risky behaviors, and follow secure practices by default.

Insight

The strongest security strategies don’t rely on a single tool or tactic. They combine culture, technology, policy, and people, creating a layered defense that evolves as quickly as the threats themselves.

[6] 2030 Vision Series: The Evolution of Media Creation, MovieLabs, p. 30

Future security trends in M&E: Preparing for what's next

The future of media and entertainment is bright, but it's also more complex, more connected, and more exposed than ever before. As content creation becomes increasingly global, distributed, and technology-driven, the security landscape will evolve right alongside it. For studios, production companies, and game developers, staying ahead means anticipating not just today's threats, but tomorrow's as well.

Here's a look at the key trends that will shape the next decade of IP protection.

"Zero Trust" becomes the default

The days of relying on firewalls and perimeter defenses are numbered. In a world of hybrid teams, cloud-based workflows, and constantly shifting partnerships, the old assumption that everything inside a network can be trusted no longer holds.

Zero Trust architectures are poised to become the industry standard. In this model, every user, device, and connection must continuously prove its legitimacy, regardless of where it originates. Access is granted based on identity, context, and behavior, and it's monitored and verified at every step. This shift will significantly reduce the risk of insider threats and lateral attacks, even as workflows become more decentralized.[7]

AI becomes a key line of defense

The same technology fueling new creative possibilities will also strengthen security. AI-driven detection tools can spot suspicious behavior patterns, detect anomalies, and even automate responses to potential breaches, often in real time. As attackers grow more sophisticated, the ability to respond at machine speed will become essential to minimizing damage and maintaining continuity.[8]

[7] 2030 Vision Series: The Evolution of Production Security, MovieLabs, p. 31

[8] AI Threat Detection: AI's Role in Identifying Risks, Legit Security

"Security by Design" from script to screen

Security will no longer be a bolt-on feature added late in the process. Instead, secure-by-design principles will shape workflows from the ground up, embedding protections directly into production pipelines. Systems will assume malicious intent by default, limit opportunities for exploitation, and safeguard IP across every phase—from pre-visualization to post-production.[9]

Compliance as a competitive advantage

With evolving standards like TPN, ISO/IEC 27001, and new regional data laws, demonstrating compliance won't just be a requirement; it will be a differentiator. Clients, partners, and distributors will increasingly expect verifiable proof that their content is handled according to the highest security standards.

Decentralized collaboration, centralized control

Workflows will continue to sprawl across continents, vendors, and creative teams. The challenge—and opportunity—will be enabling seamless collaboration without sacrificing control. Centralized governance, unified identity management, and consistent policy enforcement will allow studios to embrace distributed creativity while maintaining a strong security posture.

[9] 2030 Vision Series: The Evolution of Production Security, MovieLabs, p. 19

Insight

The future of IP security isn't about reacting to threats; it's about architecting systems and strategies that evolve with them. The studios and developers that invest now in secure-by-design thinking[10], intelligent automation, and rigorous compliance will be the ones best positioned to thrive in the decades ahead.

[10] 2030 Vision Series: The Evolution of Production Security, MovieLabs, p. 21

Why partner with Autodesk: Innovation, trust, and a future-ready vision

Securing intellectual property in media and entertainment is not a one-time effort; it's an ongoing pursuit. Threats evolve, workflows change, and new technologies emerge almost daily. Success in this landscape requires more than a point solution—or many of them. It demands a strategic partner with the expertise, vision, and resilience to navigate what's next. That's where Autodesk stands apart.

A proven leader in M&E innovation
For decades, Autodesk has helped shape the future of film, television, and interactive entertainment. That experience extends beyond tools and technologies; it's rooted in deep industry understanding and a commitment to helping studios and game developers thrive amid rapid change. As creative workflows evolve, Autodesk continues to anticipate what's coming next, not just react to what's already here.

Security designed for a changing world
True security isn't static; it's adaptable. The most effective systems assume that, eventually, some component will be compromised. That's why Autodesk's approach is designed to anticipate the "unknown unknowns." Our security philosophy is based on modular architectures that can be refactored and updated quickly to counter new threats as they emerge.

We design with the assumption that malicious activity will occur, that users and services cannot always be trusted, and that attackers will exploit any available opportunity. By embedding security into the core of our technology—protecting workflows and assets themselves, not just the infrastructure that supports them—Autodesk enables studios to remain resilient even under constant pressure.

Confidence to create without compromise

Partnering with Autodesk means more than adopting cutting-edge tools. It means aligning with a company committed to continuous innovation, proactive defense, and industry leadership. Our comprehensive approach builds trust at every level, enabling studios, production companies, and game developers to focus on what matters most: creating extraordinary content, confident that their most valuable assets are protected.

Insight

In a world where the threat landscape never stops changing, security isn't a feature; it's a partnership. And Autodesk is committed to being that trusted partner for the future of media and entertainment.

SECTION 9

Conclusion: Building a future-ready strategy

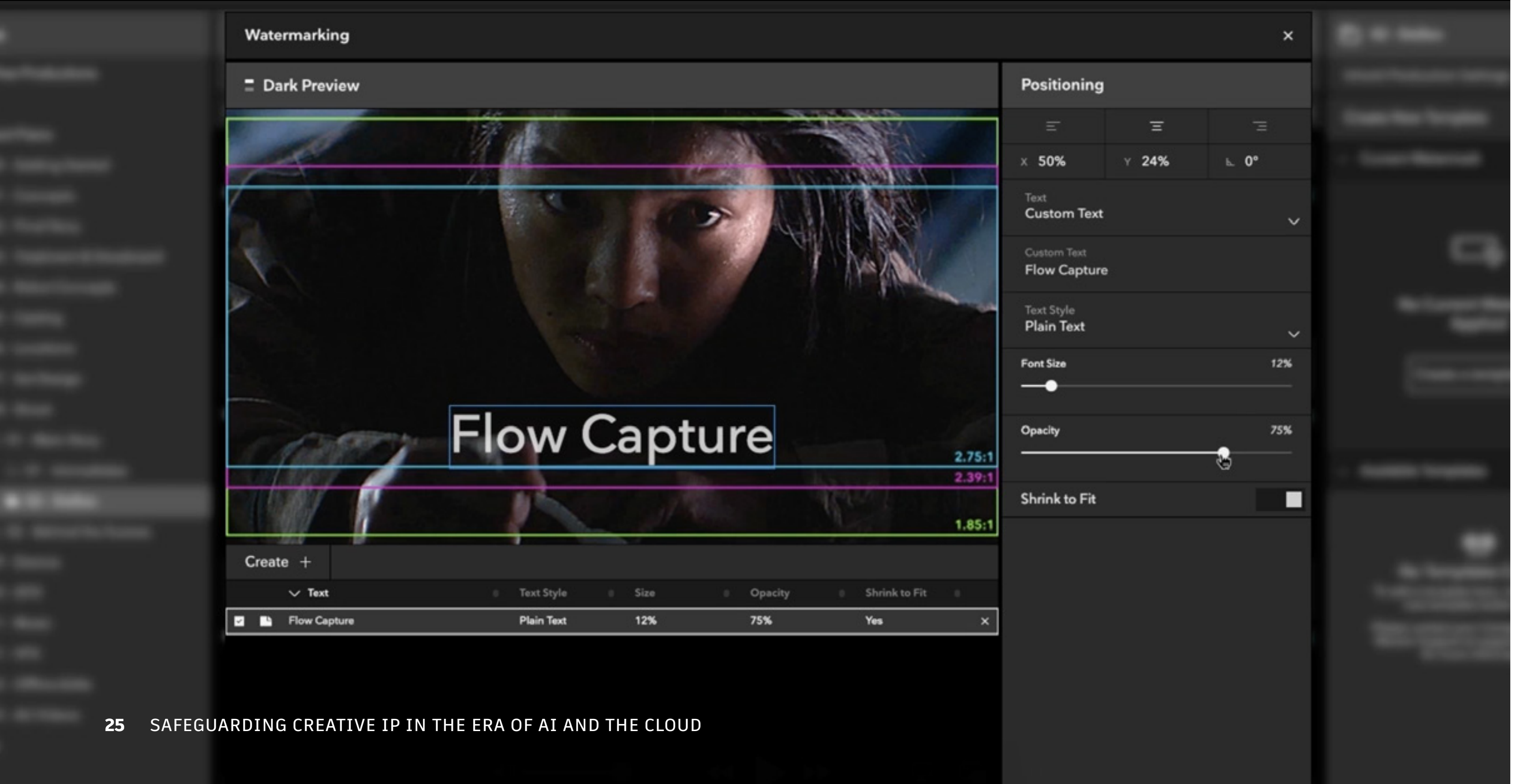
The media and entertainment industry stands at a pivotal moment. The way content is created, shared, and consumed has changed fundamentally—and there's no going back.

The shift to remote work and globally distributed teams has rewritten the rules for collaboration. The rapid rise of AI is transforming workflows at a pace few could have predicted, with new capabilities emerging every few months and more profound changes on the horizon. And the surge in high-profile breaches has made one thing clear: traditional approaches to protecting creative IP are no longer enough.

The stakes have never been higher. Studios, production companies, and game developers must now secure not just their data, but the entire ecosystem of tools, people, and processes that power their creative output. Success in this environment requires more than strong passwords and locked-down networks; it demands a holistic, adaptive, and forward-looking approach to security.

Future-proof your pipeline

The question is not whether these changes will continue; it's how you will prepare for them. And preparation isn't about predicting the future. It's about building resilience so that, whatever direction the industry takes, your workflows, assets, and reputation remain secure.



X 50%
Y 24%
0°

Text: Custom Text

Custom Text: Flow Capture

Text Style: Plain Text

Font Size: 12%

Opacity: 75%

Shrink to Fit

Text	Text Style	Size	Opacity	Shrink to Fit
Flow Capture	Plain Text	12%	75%	Yes

Autodesk Flow Capture is designed to meet the challenges of this era.

With a cloud-native architecture, security built into every layer, and alignment with the principles of the MovieLabs 2030 Vision, it offers a future-ready foundation for content creation. As threats evolve, so will Flow Capture, adapting to new risks, integrating emerging technologies, and continuously strengthening defenses.

Now is the time to get ahead of the curve, protect what matters most, and lead with confidence. With Autodesk as your partner, you can focus on creating extraordinary stories, knowing your IP is secure, no matter what the future holds.

→ LEARN MORE

AUTODESK

www.autodesk.com