Safeguarding Your Content & Platform:

MAGINE PRO'S APPROACH TO OTT SECURITY

MaginePro

Introduction

At Magine Pro, we understand that security is about more than just protecting content—it's about safeguarding your revenue, maintaining user trust, and ensuring the integrity of your platform. Our solutions are designed to tackle the evolving challenges of piracy, fraud, and unauthorised access, giving you the peace of mind that comes from knowing your platform is secure.

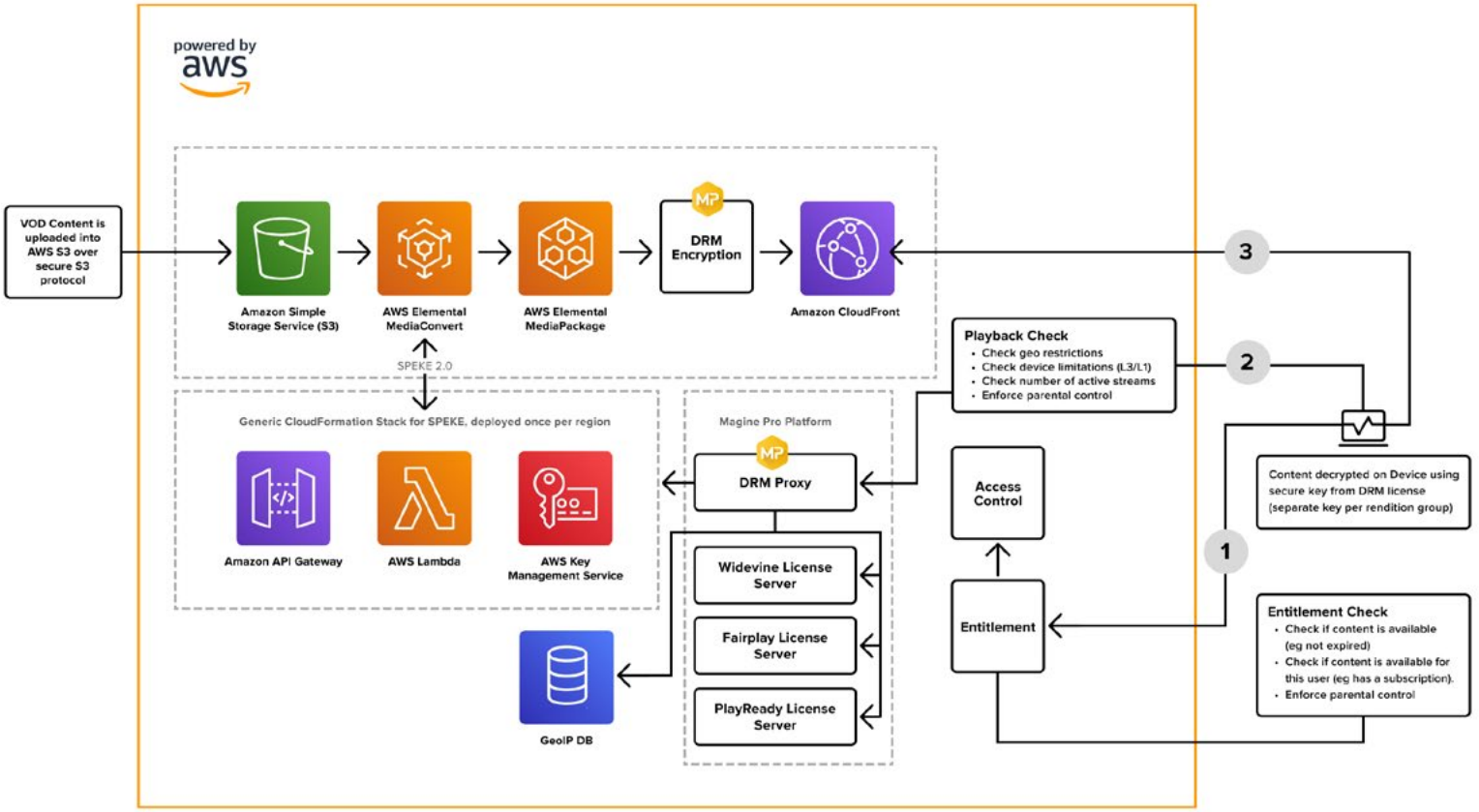
We help you stay compliant with licensing agreements, protect customer data, and prevent revenue loss, all while maintaining a trusted environment for your users. In the following chapters, we'll show you how our comprehensive security approach helps you to secure your content, strengthen your platform, and build lasting relationships with both content providers and your audience.

Content

Secure Content Upload and Delivery

Magine Pro's scalable architecture makes uploading, processing, and distributing content remarkably straightforward. We support formats ranging from live events to VOD and linear channels, allowing you to reach audiences across platforms and regions.

Throughout the entire ingestion and delivery process, our proactive security measures keep your content as safe as possible, ensuring reliability and peace of mind every step of the way.



When migrating new customers to the Magine Pro platform, we prioritise both security and data accuracy. We deliver a smooth integration process that protects sensitive user information by employing encrypted data transfers, comprehensive validation processes, and strict compliance with regulations like GDPR.

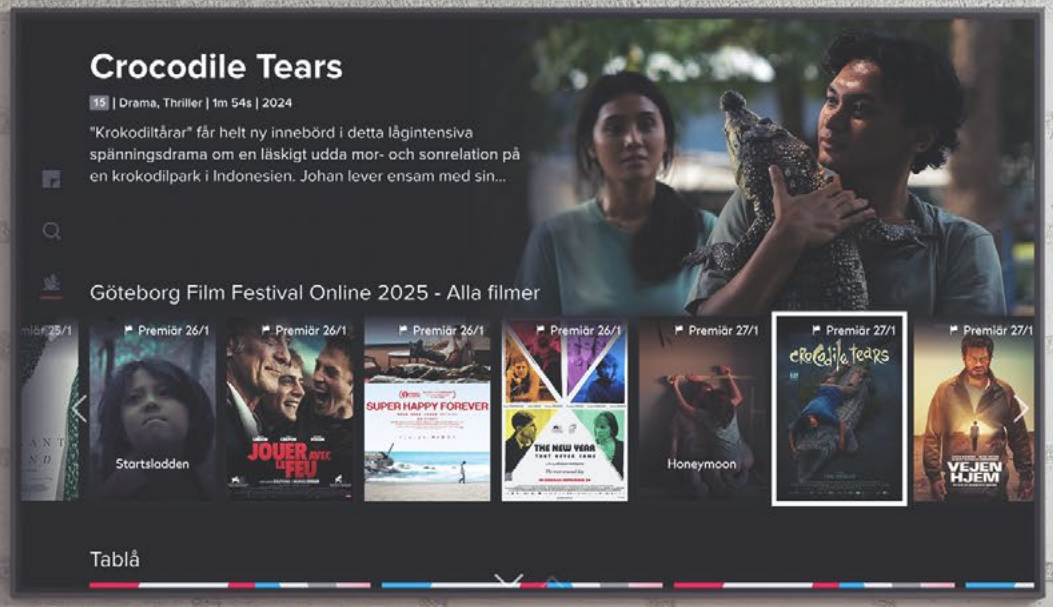
Advanced DRM for Anti-Piracy

At the forefront of content protection, Digital Rights Management (DRM) is your ultimate anti-piracy tool. It not only safeguards your assets from piracy, theft, and unauthorised access but also ensures compliance with content rights and distribution agreements as your content travels across devices and regions.

At Magine Pro, we integrate with industry-leading DRM technologies like ***Google Widevine***, ***Apple FairPlay***, and ***Microsoft PlayReady*** to protect your content and offer additional features including:

- **Key Rotation for Live Linear Content**
  We implement key rotation to ensure your content remains airtight, especially for live linear broadcasts. With keys rotating every 2 minutes, we protect content in real-time and effectively reduce the risk of unauthorised access.
- **Enhanced Security for HD and 4K Content**
  We implement advanced DRM measures, including multiple decryption keys, to ensure that only authorised devices with the latest decryption protocols can access your HD and 4K streams. Devices that fail to meet these standards are automatically blocked, safeguarding high-value content and protecting your revenue streams.
- **Offline DRM for VOD**
  Allow your users to enjoy the convenience of offline viewing without compromising security. Our DRM-secured downloads encrypt content and issue temporary licenses, ensuring downloaded files remain protected and accessible only to authorised users within predefined rights.

WIDEVINE FairPlay Microsoft PlayReady®



CASE STUDY:

Advanced DRM for HD & 4K Content

Meeting studio requirements while safeguarding premium content

The Challenge

As security demands for licensing and distributing HD and 4K content have increased, our customers and other OTT services have faced stricter requirements from studios. To meet these evolving expectations, a more sophisticated DRM solution was needed—one capable of handling multiple encryption levels while ensuring secure playback across various devices.

The Solution

In response, we upgraded our DRM system by implementing a multi-key encryption/decryption schema. This ensures that each video rendition (e.g., HD, 4K) is protected with distinct encryption keys. Additionally, hardware-based decryption was enforced for HD and 4K playback, restricting devices without this capability to SD quality. This feature is implemented via Widevine DRM, while Apple devices leverage FairPlay, which inherently supports hardware decryption.

The Result

With this enhanced DRM solution, our customers can now meet studio security requirements, enabling them to confidently license and distribute HD and 4K content.

This upgrade not only safeguards premium content but also expands opportunities to access and monetize higher-value content libraries.

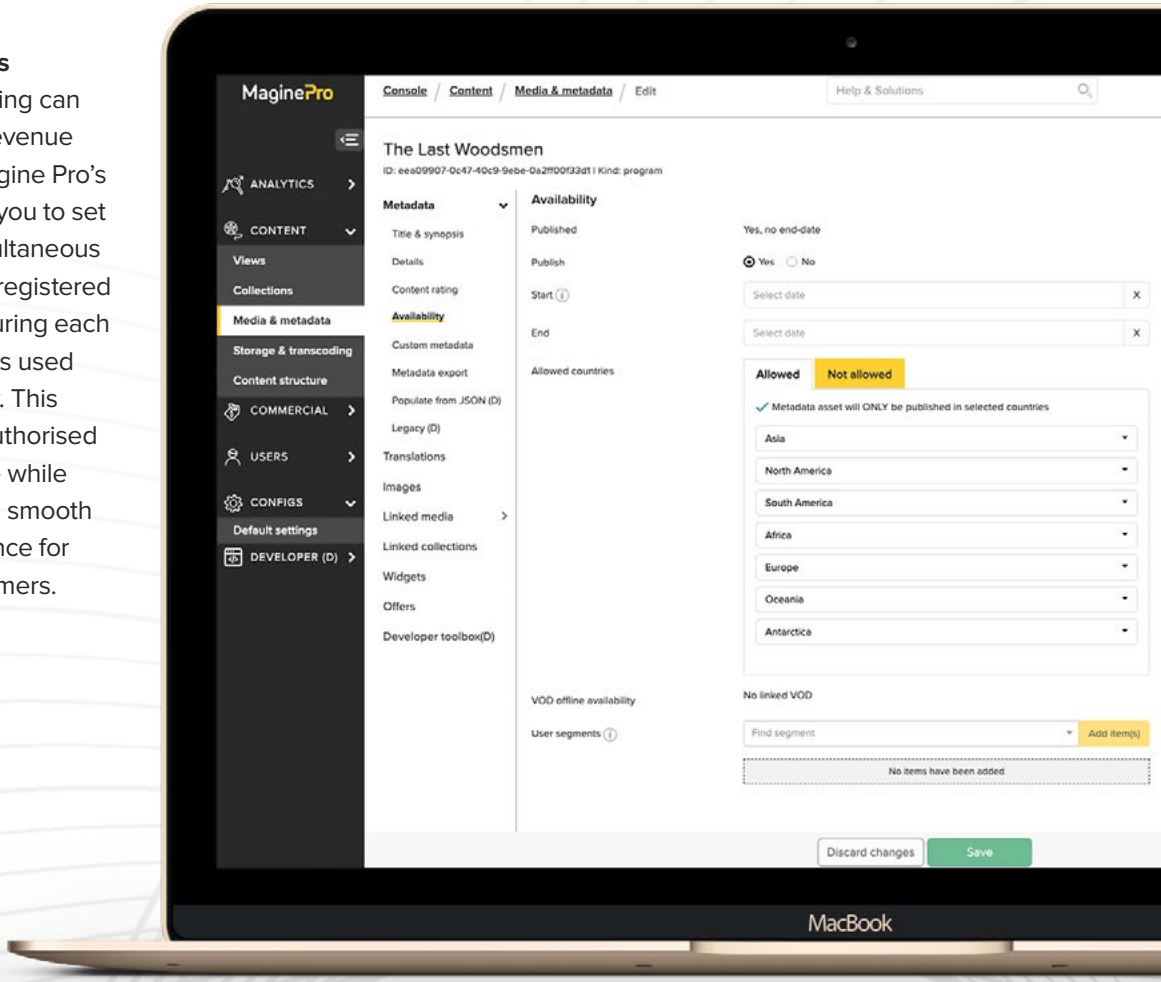
Unauthorised Usage Prevention

Unauthorised usage can erode the value of your streaming service. Magine Pro provides advanced user access controls to help defend against unapproved logins and account abuse. By implementing features that validate and limit access, you can confidently deliver content to the right audience, safeguard your revenue, and stay compliant with distribution agreements.

- **Geo-Blocking and IP Restrictions**
  With Magine Pro's CMS Console, you can restrict content by geographic location to align with regional licensing agreements. Our ***per-asset rights management*** adds precision, allowing you to set geo-blocking rules for individual titles or live events. IP-based restrictions further enhance security, protecting high-demand content like live sports or premium VOD from unauthorised access.

- **VPN and Proxy Detection**
  Unauthorised viewers often use VPNs or proxy servers to bypass geo-restrictions. Magine Pro works with trusted partner ***Digital Element*** to detect and block location-masking techniques, ensuring only legitimate viewers can access your content. This protects your content's value and ensures fair access based on licensing terms.

- **Concurrent Stream Limits**
  Account sharing can erode your revenue potential. Magine Pro's tools enable you to set limits on simultaneous streams and registered devices, ensuring each subscription is used appropriately. This reduces unauthorised device usage while maintaining a smooth user experience for paying customers.



CASE STUDY:

Concurrent Stream Limits for Linear Content

Preventing account misuse while ensuring a seamless viewing experience

The Challenge

Linear content often experiences high demand, making it particularly vulnerable to account sharing and excessive device usage. To maintain fair access for paying users while preventing unauthorized viewing, a system was needed to limit concurrent streams per account—ensuring compliance with licensing agreements without disrupting the legitimate viewing experience.

The Solution

To address this, a robust concurrent stream limit feature was implemented, enforcing restrictions through a quick, multi-step verification process before streaming begins. The system checks asset-level rules, global streams per asset, total concurrent streams, and device limits. This layered approach ensures only authorised viewers can access content, helping operators comply with licensing agreements and prevent account-sharing abuse.

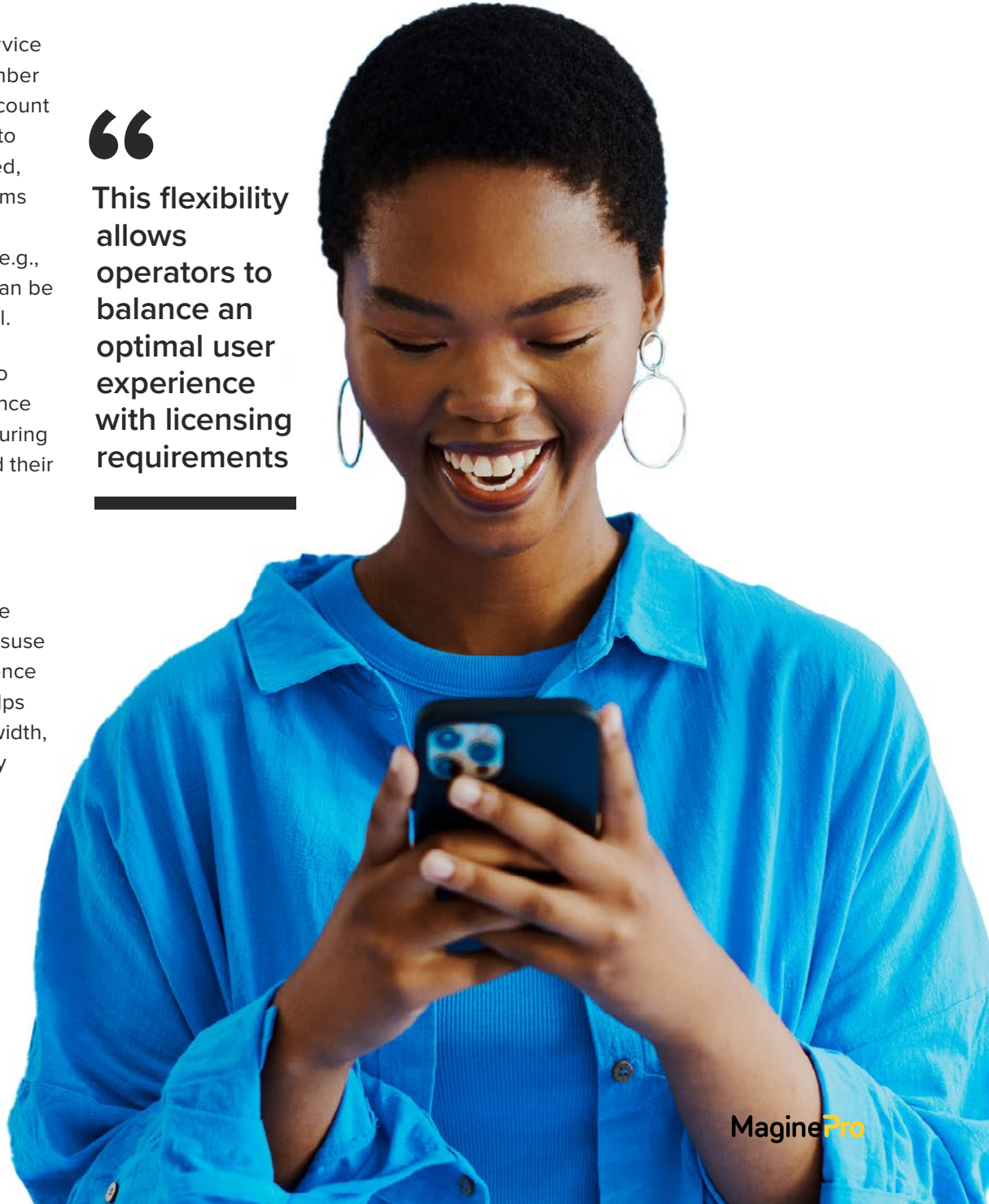
Operators can configure the service globally to define maximum number of simultaneous streams per account and per asset. For example, up to five total streams may be allowed, while limiting users to two streams for the same asset. For stricter content provider requirements (e.g., one stream per user), settings can be adjusted at the video asset level.

This flexibility allows operators to balance an optimal user experience with licensing requirements, ensuring their content remains secure and their service compliant.

The Result

With the ability to set concurrent stream limits, our customers have successfully reduced account misuse while ensuring a smooth experience for paying users. This feature helps protect revenue, optimise bandwidth, and maintain service integrity. By implementing these controls, streaming providers can strike the right balance between user satisfaction and operational efficiency, ensuring their service remains both fair and profitable.

> “This flexibility allows operators to balance an optimal user experience with licensing requirements

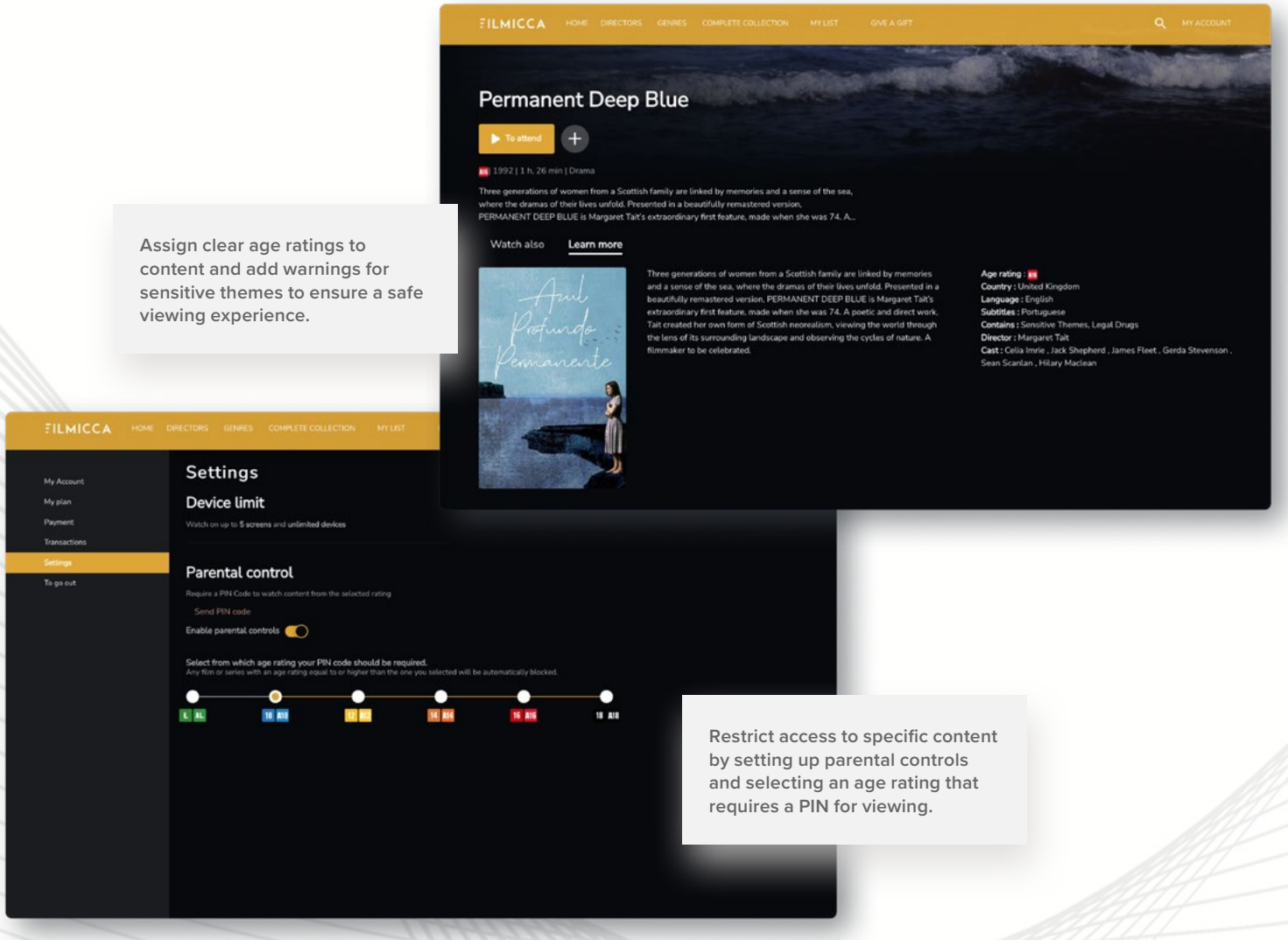


Parental Controls for Youth Protection

We provide robust parental controls to support family-friendly streaming experiences and ensure complance with strict youth protection regulations in various markets. Our platform enables you to:

- **Assign clear age ratings to content.**
- **Add content warnings for sensitive themes.**
- **Restrict access to content requiring a PIN.**

End users can also customise their parental settings, tailoring viewing preferences to their household needs. This advanced level of control safeguards content while meeting the expectations of both parents and regulatory authorities.



Assign clear age ratings to content and add warnings for sensitive themes to ensure a safe viewing experience.

Restrict access to specific content by setting up parental controls and selecting an age rating that requires a PIN for viewing.

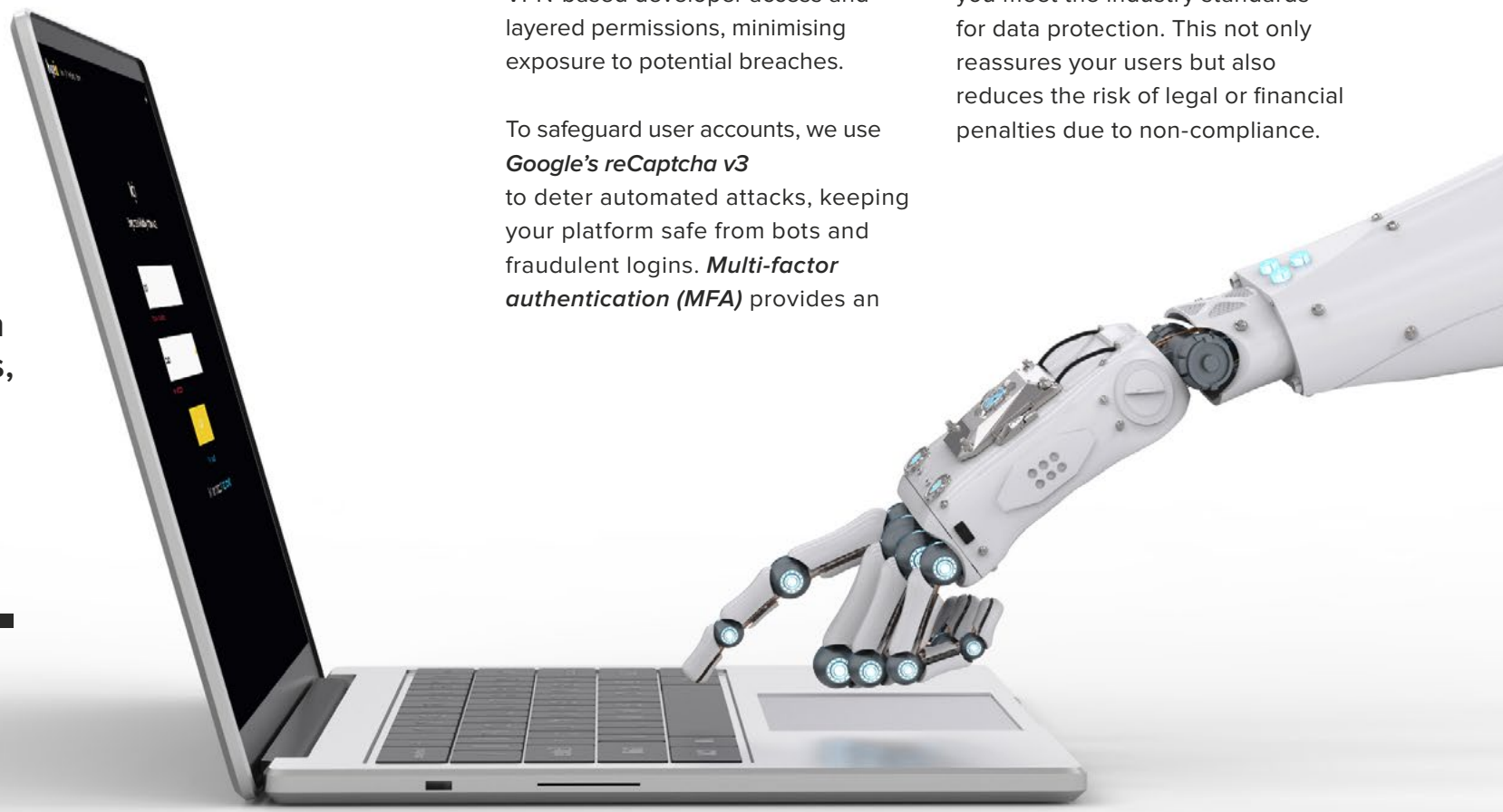
Safeguarding Subscriber Data

Protecting subscriber data isn't just about security—it's about trust and maintaining your brand's reputation. We help minimise the risk of data breaches by encrypting subscriber data using advanced protocols, ensuring that sensitive information remains secure from unauthorised access. Our architecture, built on AWS Blueprint standards, incorporates VPN-based developer access and layered permissions, minimising exposure to potential breaches.

To safeguard user accounts, we use ***Google's reCaptcha v3*** to deter automated attacks, keeping your platform safe from bots and fraudulent logins. ***Multi-factor authentication (MFA)*** provides an additional layer of security to ensure that only authorised individuals can access your user data. It requires users to verify their identity through multiple steps, such as entering a password and providing a secondary code.

By adhering to GDPR and other regional privacy regulations, we help you meet the industry standards for data protection. This not only reassures your users but also reduces the risk of legal or financial penalties due to non-compliance.

> **Our architecture, built on AWS Blueprint standards, incorporates VPN-based developer access and layered permissions, minimising exposure to potential breaches.**



Proactive Platform Safeguards

The streaming threat landscape is constantly evolving, and while no solution can guarantee perfect security, Magine Pro employs a proactive, multi-layered approach, including routine audits, updates, and robust testing, to help keep your service safe. By identifying vulnerabilities early, we give you greater peace of mind, allowing you to focus on delivering great content.

Before launching a new customer app, or device integration, we conduct thorough security testing to form a solid foundation. This includes leveraging ***Static Application Security Testing (SAST)*** with tools like Snyk to identify vulnerabilities in the code. We also employ ***Infrastructure as Code (Iac)*** security to ensure configuration files (e.g., Terraform, AWS CloudFormation) adhere to best practices, reducing risks during deployment. ***Zero Trust Principles*** are enforced at every stage of this process, granting minimal access rights to prevent privilege abuse. Additionally, ***Automated Secret Management*** via Amazon Secret Manager prevents hard-coded credentials in source code, bolstering protection against unauthorised access.

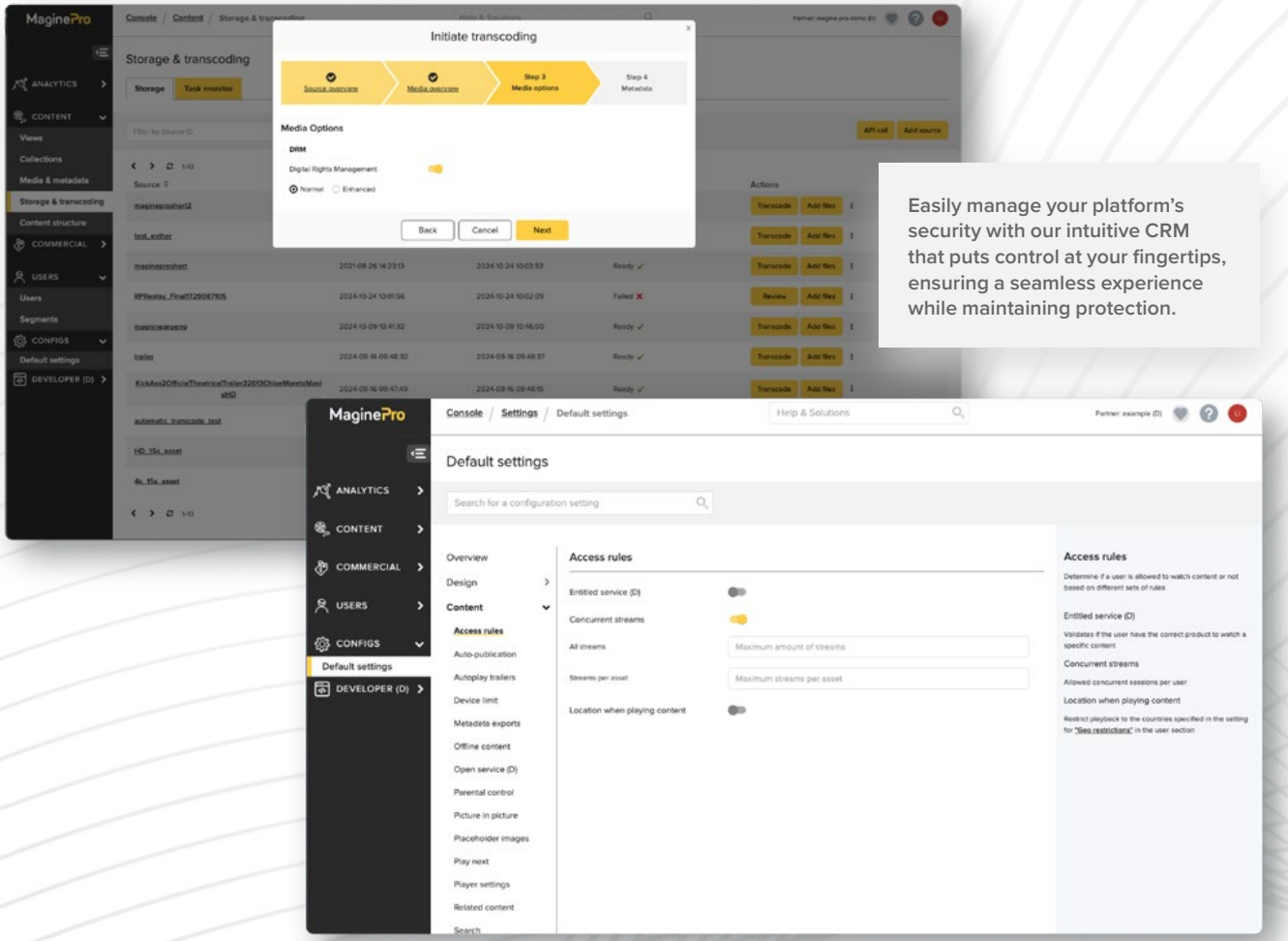
After deployment, we conduct regular internal audits and real-time monitoring to stay ahead of potential threats. While external audits and penetration tests are planned with security advisors, timely updates ensure the latest security enhancements are integrated to address emerging risks.

If issues arise—whether through audits or real-time monitoring—our 24/7 on-call team responds swiftly to resolve them. Additionally, we deploy firewalls to block malicious IPs and reduce bot traffic, adding another layer of defence to keep unauthorised users at bay.

Customisable Security Features

With Magine Pro, you can shape your security measures according to your unique requirements. Our intuitive CMS console lets you fine-tune DRM settings, set stream limits, and manage user access controls, all while preserving a smooth user experience and the ability to scale.

We also offer role-based access controls that assign each team member the right level of authority. This structured approach minimises internal threats, streamlines workflows, and secures sensitive operations.



Easily manage your platform's security with our intuitive CRM that puts control at your fingertips, ensuring a seamless experience while maintaining protection.

EXPERT INSIGHTS

Q&A with Our Head of Operations

Explore the practical aspects of OTT security in this conversation with our Head of Operations, Marcus Linden, who addresses the key questions operators frequently ask.

How quickly can Magine Pro respond to a security incident, and what kind of support will I receive?
We act fast—typically within minutes—thanks to automated alerts and our 24/7 on-call team. You can reach us directly through Slack, email, or WhatsApp, and we'll keep you updated in real-time. Our goal is to resolve issues quickly and keep you in the loop the entire time.

What is Magine Pro's approach to scaling security as my subscriber base grows?
Our platform scales dynamically, ensuring DRM, stream limits, and access controls remain strong as your subscriber base grows—whether you're launching a new popular series or streaming live events. Security grows with your audience, not against it.

> "Our platform scales dynamically, ensuring DRM, stream limits, and access controls remain strong as your subscriber base grows...

How does Magine Pro handle concurrency limits in high-demand scenarios, and can those limits be scaled up or down dynamically?
We've built the platform so you can set concurrency rules globally but also fine-tune them for specific assets, like a big live sports event. It adapts to spikes in traffic without compromising control. For example, if you're expecting a surge, you can prepare ahead of time by manually scaling up and warming up the system so everything runs smoothly when viewers log in.

What's the typical downtime or maintenance window for applying essential security patches or upgrades?
We try to avoid downtime altogether. Most critical patches are applied with rolling updates, so there's no interruption for viewers. In rare cases requiring maintenance, we schedule it during off-peak hours and keep it as short as possible. It's all about minimising disruption for your users.

What's one mistake you see most often in OTT security, and how can operators avoid it?
A classic oversight is using easy-to-guess passwords or leaving test accounts active in production environments. To avoid these pitfalls, enforce strong password policies, routinely audit accounts, and ensure test accounts are disabled or removed before launch.

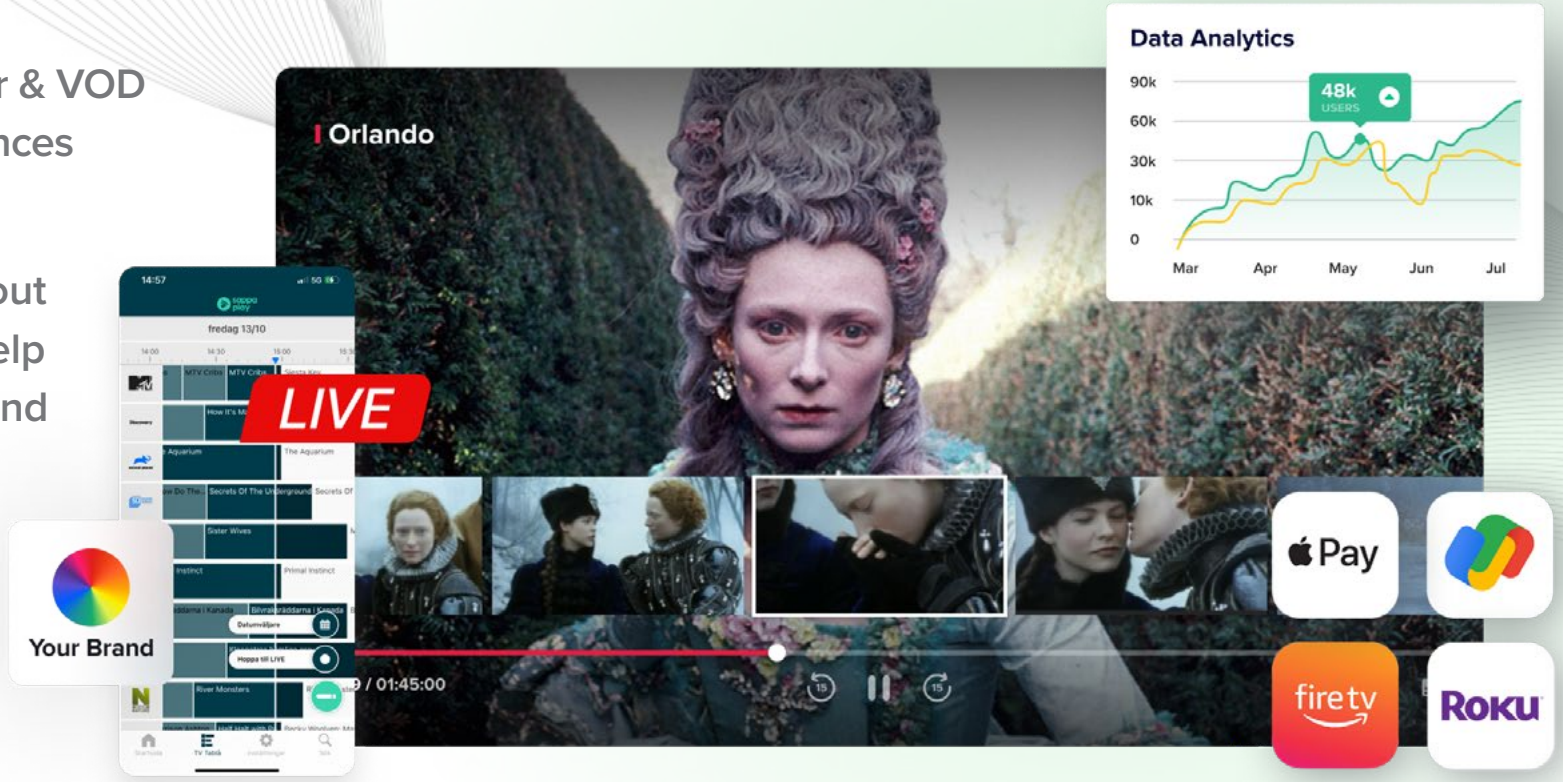
We recommend combining account monitoring with proactive tools like concurrent stream limits and multi-factor authentication to add extra layers of protection—it's better to be a bit too cautious than to risk a breach.

MaginePro

Flexible video streaming services & apps

Deliver your Live, Linear & VOD entertainment to audiences worldwide.

Want to learn more about how Magine Pro can help protect your platform and content? Contact us today to discuss your security needs.



iPhone android LG SAMSUNG chromecast AirPlay ROKU firetv tv androidtv VIZIO

maginepro.com