ES

Seguridad e Integraciones en Plataformas OTT

Un enfoque multicapa para la protección de contenidos audiovisuales, la infraestructura de alta disponibilidad y la integración segura con sistemas de terceros

La distribución de contenidos audiovisuales a través de plataformas OTT exige un modelo de seguridad riguroso que proteja los activos digitales en todas las fases de su ciclo de vida: ingestión, almacenamiento, distribución y consumo. Plenitas implementa una arquitectura de seguridad multicapa, respaldada por certificaciones internacionales (ISO 27001, ISO 14001, ISO 9001) y nacionales (ENS nivel medio), que garantiza la confidencialidad, integridad y disponibilidad de la información.

Arquitectura de infraestructura

La plataforma opera sobre una infraestructura en la nube diseñada para la alta disponibilidad y el rendimiento a escala global. La lógica de negocio se despliega en clústeres de contenedores orquestados, distribuidos en múltiples zonas de disponibilidad dentro de una misma región, lo que garantiza la continuidad del servicio ante fallos parciales de infraestructura.

Componentes principales

- **Servicios de aplicación:** el núcleo de la lógica de negocio se ejecuta en contenedores aislados, procesando solicitudes de usuarios y gestores editoriales a través de interfaces API diferenciadas, lo que garantiza la segregación funcional y la resiliencia del sistema.
- **Procesamiento asíncrono:** un sistema de colas de tareas gestiona las operaciones en segundo plano (transcodificación, generación de informes, sincronizaciones), evitando bloqueos en los servicios principales y permitiendo escalar la capacidad de procesamiento de forma independiente.
- **Clúster de bases de datos:** la capa de persistencia utiliza una configuración multi-AZ con réplicas de escritura-lectura sincronizadas con el nodo primario, optimizando el rendimiento mediante la distribución de cargas y permitiendo la escalabilidad horizontal. El redireccionamiento automático de tráfico ante fallos asegura la continuidad del servicio.
- **Caché en memoria:** una capa de almacenamiento en memoria reduce la latencia de acceso a datos frecuentes y actúa como gestor de mensajes para la coordinación de tareas asíncronas entre los diferentes módulos del sistema.
- **Almacenamiento de activos digitales:** los recursos multimedia se alojan en almacenamiento de objetos con cifrado en reposo, control de accesos granular y políticas de seguridad que restringen el acceso exclusivamente a los servicios autorizados.

Red de distribución de contenidos (CDN)

La entrega de contenidos se apoya en una CDN de nivel empresarial con presencia global, que cachea los contenidos en nodos de última milla repartidos por más de 50 territorios. Este diseño reduce la latencia, absorbe picos masivos de tráfico y descarga los servidores de origen. La CDN implementa cifrado HTTPS extremo a extremo, conmutación automática a orígenes de reserva y políticas de caché configurables por tipo de activo. Los grupos de auto-escalado y el balanceo de carga distribuyen las peticiones de forma equitativa, garantizando la estabilidad incluso durante eventos en directo con alta concurrencia.

Elección de región y residencia de datos

Es fundamental distinguir entre la distribución global de contenidos —que busca acercar los flujos de vídeo al usuario final para minimizar la latencia— y la residencia de los datos, es decir, la ubicación física donde se alojan los datos maestros, las bases de datos, los activos originales y la lógica de negocio de cada cliente.

Plenitas ofrece a cada cliente la posibilidad de elegir la región donde se despliega su solución, garantizando que los datos permanezcan alojados en la jurisdicción que el cliente necesite para el cumplimiento de su marco legal y regulatorio:

- **Unión Europea:** despliegue en regiones europeas para cumplimiento del RGPD y normativas nacionales de protección de datos, asegurando que los datos personales y los activos audiovisuales no abandonan el territorio de la UE.
- **Estados Unidos:** despliegue en regiones norteamericanas para clientes sujetos a regulaciones federales o estatales, incluyendo requisitos de proximidad y soberanía de datos.
- **Oriente Medio, Asia-Pacífico y otras regiones:** despliegue en regiones como Emiratos Árabes, Singapur, Japón u otras, según las exigencias regulatorias locales de cada cliente.

De este modo, la CDN distribuye globalmente las copias cacheadas del contenido para ofrecer la mejor experiencia al usuario final en cualquier parte del mundo, mientras que los datos de origen, la información de usuarios, las bases de datos y los servicios de backend permanecen alojados exclusivamente en la región elegida por el cliente, bajo su marco legal aplicable.

Seguridad perimetral y defensa en profundidad

La arquitectura de seguridad sigue un modelo de defensa en profundidad con múltiples capas de protección, desde el borde de la red hasta el núcleo de los servidores:

- **Protección contra DDoS:** escudos especializados en el borde de la red detectan automáticamente patrones de tráfico anómalo y aplican medidas de mitigación en tiempo real, protegiendo tanto la capa de red como la capa de aplicación sin intervención humana.
- **Cortafuegos de aplicaciones web (WAF):** filtra, monitoriza y bloquea tráfico HTTP/HTTPS malicioso mediante reglas personalizadas contra inyección SQL, cross-site scripting (XSS), inundación de peticiones y scraping. Las reglas basadas en tasa limitan automáticamente las solicitudes desde IPs sospechosas.
- **Análisis continuo de vulnerabilidades:** escaneos automatizados sobre instancias y contenedores detectan vulnerabilidades de software y configuraciones inseguras antes de que puedan ser explotadas.
- **Detección inteligente de amenazas:** monitorización ininterrumpida de la actividad de la cuenta y los flujos de red, utilizando aprendizaje automático para identificar comportamientos anómalos, minería no autorizada o intentos de escalada de privilegios.

Protección de contenidos (DRM)

La plataforma incorpora un sistema de Gestión de Derechos Digitales (DRM) multiestándar que cubre la totalidad de dispositivos y entornos de consumo: navegadores web, aplicaciones móviles, Smart TV y dispositivos de televisión conectada. El reproductor detecta automáticamente el entorno de ejecución y selecciona el sistema DRM apropiado de forma transparente para el usuario.

- **Cifrado en origen:** los contenidos se cifran mediante algoritmos estándar de la industria (AES-128) antes de su distribución, asegurando un equilibrio óptimo entre seguridad y rendimiento.
- **Arquitectura multi-key:** se utilizan claves específicas para cada ecosistema de dispositivos. Sin la clave que entrega el servidor de licencias, el contenido es ilegible.
- **Políticas de licencias dinámicas:** ventanas temporales de disponibilidad, límites de dispositivos por usuario, revocación remota de licencias en tiempo real y control de acceso por tipo de contenido, canal o perfil de usuario.
- **Protección extendida:** la arquitectura DRM se extiende a los elementos publicitarios insertados en los contenidos, garantizando la seguridad de los ingresos derivados en cumplimiento de la normativa audiovisual.
- **Prevención de capturas:** se aprovechan los mecanismos nativos de protección de los sistemas DRM para impedir la grabación de pantalla, la captura no autorizada y la extracción ilícita de flujos protegidos, especialmente en contenidos premium y emisiones en directo.

Control territorial y de acceso

El control territorial constituye un pilar fundamental para el cumplimiento de las obligaciones contractuales de distribución y para garantizar que únicamente los usuarios autorizados consuman los contenidos en las condiciones establecidas.

- **Geo-blocking en el borde:** las restricciones geográficas se evalúan directamente en la CDN, antes de que la solicitud alcance los servidores de origen. La granularidad es configurable desde el CMS para cada activo individual: sin restricción, restringido a país, región o unión económica.
- **Tokenización avanzada:** tokens firmados criptográficamente y con validez temporal limitada vinculan cada solicitud a un usuario autenticado, un dispositivo específico y un contexto de reproducción determinado. La tokenización actúa como primera línea de defensa antes del DRM.
- **Control de sesiones:** el sistema valida en tiempo real cada petición contra la base de datos de sesiones autorizadas, denegando el acceso de forma inmediata ante tokens expirados, revocados o inexistentes, e impidiendo la reutilización de enlaces y la compartición ilícita.
- **Antipiratería de publicación:** controles gestionados desde la plataforma de vídeo aseguran que únicamente los dominios y aplicaciones expresamente autorizados puedan reproducir los flujos de contenido, bloqueando cualquier intento de incrustación desde orígenes no validados.

Integraciones seguras y ecosistema API

La arquitectura de Plenitas está diseñada para integrarse de forma segura y completa con los sistemas de sus clientes. La plataforma expone una API integral con endpoints para todas las funcionalidades del sistema, permitiendo la automatización, la interoperabilidad y la extensión de la solución sin comprometer la seguridad.

Capas de securización de la API

- **Autenticación y autorización:** todas las llamadas a la API requieren autenticación mediante tokens firmados con alcance limitado y caducidad temporal. El sistema de autorización implementa control de acceso basado en roles (RBAC), asegurando que cada integración accede exclusivamente a los recursos y operaciones que le han sido asignados.
- **Seguridad en tránsito:** todas las comunicaciones se realizan sobre canales cifrados (TLS 1.2+), impidiendo la interceptación o manipulación de datos en tránsito. Se aplican políticas de certificate pinning y validación estricta de certificados en las integraciones críticas.
- **Rate limiting y throttling:** se aplican límites de tasa por cliente y por endpoint para prevenir abusos, proteger la estabilidad de la plataforma y garantizar la calidad del servicio a todos los consumidores de la API.
- **Versionado y validación:** la API implementa versionado semántico que permite la evolución de las interfaces sin interrumpir las integraciones existentes. Todas las solicitudes se validan contra esquemas estrictos para prevenir inyecciones y datos malformados.

Integraciones con sistemas de terceros

La API de Plenitas ofrece endpoints específicos para todas las funcionalidades de la plataforma, facilitando la integración con los ecosistemas tecnológicos de cada cliente en múltiples capas:

- **CRM y gestión de usuarios:** integración con sistemas de gestión de relaciones con clientes para la sincronización de perfiles de usuario, segmentación de audiencias, gestión del ciclo de vida del suscriptor y personalización de la experiencia.
- **ERP y facturación:** conectividad con sistemas de planificación de recursos empresariales para la gestión automatizada de suscripciones, facturación, conciliación de pagos y reporting financiero.
- **Comercio electrónico:** endpoints dedicados para la integración con plataformas de ecommerce, incluyendo gestión de catálogos de productos, pasarelas de pago, cupones promocionales y flujos de compra de contenidos o suscripciones.
- **Métricas y analítica:** exportación de datos de consumo, audiencia, rendimiento y comportamiento de usuario hacia sistemas de business intelligence y plataformas analíticas de terceros, permitiendo la creación de cuadros de mando personalizados y la toma de decisiones basada en datos.
- **Formación y LMS:** integración con plataformas de formación y sistemas de gestión de aprendizaje (LMS), permitiendo la distribución de contenidos formativos audiovisuales con seguimiento de progreso, certificaciones y control de acceso por alumno o grupo.
- **Publicidad y monetización:** integración con ad-servers y plataformas de monetización para la inserción de publicidad dinámica (SSAI/CSAI), gestión de campañas y reporting de impresiones.
- **Sistemas de contenidos y MAM:** conectividad con sistemas de gestión de activos multimedia (MAM) y flujos de trabajo de ingestión para la automatización del ciclo de publicación de contenidos.

Cumplimiento normativo y seguridad organizativa

La plataforma cumple con el Esquema Nacional de Seguridad (ENS) en categoría media, el RGPD, la LOPDGDD y la LSSICE. Se incorpora una plataforma de gestión del consentimiento (CMP) para la recogida granular del consentimiento y su trazabilidad para auditorías. Las prácticas organizativas incluyen gestión proactiva de riesgos, auditorías internas periódicas, procedimientos normalizados de gestión de incidentes, control de acceso por privilegios mínimos y formación continua del equipo en ciberseguridad.

ISO 27001 Seguridad de la Información	ISO 14001 Gestión Medioambiental	ISO 9001 Gestión de Calidad	ENS Medio Esquema Nacional de Seguridad

EN

Security & Integrations in OTT Platforms

A multi-layered approach to audiovisual content protection, high-availability infrastructure, and secure third-party integration

Delivering audiovisual content through OTT platforms demands a rigorous security model that protects digital assets across every stage of their lifecycle: ingestion, storage, distribution, and consumption. Plenitas implements a multi-layered security architecture, backed by international certifications (ISO 27001, ISO 14001, ISO 9001) and national frameworks (ENS – Spanish National Security Framework, medium level), ensuring confidentiality, integrity, and availability of information.

Infrastructure Architecture

The platform runs on cloud infrastructure designed for high availability and global-scale performance. Business logic is deployed in orchestrated container clusters distributed across multiple availability zones within a single region, ensuring service continuity in the event of partial infrastructure failures.

Core Components

- **Application services:** the core business logic runs in isolated containers, processing requests from end users and editorial managers through differentiated API interfaces, ensuring functional segregation and system resilience.
- **Asynchronous processing:** a task queue system handles background operations (transcoding, report generation, synchronizations), preventing bottlenecks in primary services and enabling independent scaling of processing capacity.
- **Database cluster:** the persistence layer uses a multi-AZ configuration with read-write replicas synchronized to the primary node, optimizing performance through workload distribution and enabling horizontal scalability. Automatic traffic redirection on failure ensures service continuity.
- **In-memory cache:** a memory-based storage layer reduces data access latency and serves as the message broker for asynchronous task coordination across system modules.
- **Digital asset storage:** media assets are hosted in object storage with at-rest encryption, granular access controls, and security policies restricting access to authorized services only.

Content Delivery Network (CDN)

Content delivery relies on an enterprise-grade CDN with global presence, caching content at edge nodes across 50+ territories. This design reduces latency, absorbs massive traffic spikes, and offloads origin servers. The CDN enforces end-to-end HTTPS encryption, automatic failover to backup origins, and per-asset-type cache policies. Auto-scaling groups and load balancing distribute requests evenly, ensuring stability even during high-concurrency live events.

Region Selection & Data Residency

It is essential to distinguish between global content distribution —which aims to bring video streams closer to the end user to minimize latency— and data residency, meaning the physical location where each client's master data, databases, original assets, and business logic are hosted.

Plenitas offers each client the ability to choose the region where their solution is deployed, ensuring that data remains hosted within the jurisdiction required for compliance with their applicable legal and regulatory framework:

- **European Union:** deployment in European regions for GDPR compliance and national data protection regulations, ensuring that personal data and audiovisual assets do not leave EU territory.
- **United States:** deployment in North American regions for clients subject to federal or state regulations, including data proximity and sovereignty requirements.
- **Middle East, Asia-Pacific & other regions:** deployment in regions such as the UAE, Singapore, Japan, or others, according to each client's local regulatory requirements.

In this way, the CDN globally distributes cached copies of content to deliver the best user experience anywhere in the world, while origin data, user information, databases, and backend services remain hosted exclusively in the region chosen by the client, under their applicable legal framework.

Perimeter Security & Defense in Depth

The security architecture follows a defense-in-depth model with multiple protection layers, from the network edge to the server core:

- **DDoS protection:** specialized edge-level shields automatically detect anomalous traffic patterns and apply real-time mitigation measures, protecting both network and application layers without human intervention.

- **Web Application Firewall (WAF):** filters, monitors, and blocks malicious HTTP/HTTPS traffic using custom rules against SQL injection, cross-site scripting (XSS), request flooding, and scraping. Rate-based rules automatically throttle requests from suspicious IPs.
- **Continuous vulnerability scanning:** automated scans on instances and containers detect software vulnerabilities and insecure configurations before they can be exploited.
- **Intelligent threat detection:** uninterrupted monitoring of account activity and network flows, leveraging machine learning to identify anomalous behavior, unauthorized mining, or privilege escalation attempts.

Content Protection (DRM)

The platform incorporates a multi-standard Digital Rights Management (DRM) system covering all devices and consumption environments: web browsers, mobile applications, Smart TVs, and connected TV devices. The player automatically detects the runtime environment and selects the appropriate DRM system transparently for the user.

- **Origin-level encryption:** content is encrypted using industry-standard algorithms (AES-128) before distribution, ensuring an optimal balance between security and performance.
- **Multi-key architecture:** device-ecosystem-specific keys are used. Without the key issued by the license server, content is unreadable.
- **Dynamic license policies:** availability time windows, per-user device limits, real-time remote license revocation, and access control by content type, channel, or user profile.
- **Extended protection:** the DRM architecture extends to advertising elements inserted in content, securing derived revenue streams in compliance with audiovisual regulations.
- **Capture prevention:** native DRM protection mechanisms are leveraged to prevent screen recording, unauthorized capture, and illicit extraction of protected streams, particularly for premium content and live broadcasts.

Territorial Control & Access Management

Territorial control is a fundamental pillar for meeting contractual distribution obligations and ensuring that only authorized users consume content under the established conditions.

- **Edge-level geo-blocking:** geographic restrictions are evaluated directly at the CDN before requests reach origin servers. Granularity is CMS-configurable per individual asset: unrestricted, country-restricted, region-restricted, or economic-union-restricted.
- **Advanced tokenization:** cryptographically signed, time-limited tokens bind each request to an authenticated user, a specific device, and a playback context. Tokenization acts as the first line of defense before DRM.
- **Session control:** the system validates every request in real time against the authorized session database, immediately denying access for expired, revoked, or non-existent tokens, and preventing link reuse and illicit sharing.
- **Publication anti-piracy:** controls managed from the video platform ensure that only expressly authorized domains and applications can play content streams, blocking any embedding attempt from unvalidated origins.

Secure Integrations & API Ecosystem

Plenitas' architecture is designed for secure, comprehensive integration with client systems. The platform exposes a full-featured API with endpoints for every system functionality, enabling automation, interoperability, and solution extensibility without compromising security.

API Security Layers

- **Authentication & authorization:** all API calls require authentication via scoped, time-limited signed tokens. The authorization system implements role-based access control (RBAC), ensuring each integration accesses only its assigned resources and operations.
- **In-transit security:** all communications are conducted over encrypted channels (TLS 1.2+), preventing data interception or tampering. Certificate pinning and strict certificate validation policies are enforced for critical integrations.
- **Rate limiting & throttling:** per-client and per-endpoint rate limits prevent abuse, protect platform stability, and ensure quality of service for all API consumers.
- **Versioning & validation:** the API implements semantic versioning, allowing interface evolution without disrupting existing integrations. All requests are validated against strict schemas to prevent injections and malformed data.

Third-Party System Integrations

Plenitas' API provides dedicated endpoints for every platform functionality, enabling integration with each client's technology ecosystem across multiple layers:

- **CRM & user management:** integration with customer relationship management systems for user profile synchronization, audience segmentation, subscriber lifecycle management, and experience personalization.
- **ERP & billing:** connectivity with enterprise resource planning systems for automated subscription management, billing, payment reconciliation, and financial reporting.
- **E-commerce:** dedicated endpoints for integration with ecommerce platforms, including product catalog management, payment gateways, promotional coupons, and content or subscription purchase flows.
- **Metrics & analytics:** export of consumption, audience, performance, and user behavior data to business intelligence systems and third-party analytics platforms, enabling custom dashboards and data-driven decision making.
- **Training & LMS:** integration with training platforms and learning management systems (LMS), enabling distribution of audiovisual training content with progress tracking, certifications, and per-student or group access control.
- **Advertising & monetization:** integration with ad-servers and monetization platforms for dynamic ad insertion (SSAI/CSAI), campaign management, and impression reporting.
- **Content systems & MAM:** connectivity with media asset management (MAM) systems and ingestion workflows for automating the content publishing lifecycle.

Regulatory Compliance & Organizational Security

The platform complies with the Spanish National Security Framework (ENS, medium level), GDPR, LOPDGDD, and LSSICE. A Consent Management Platform (CMP) is integrated for granular consent collection and audit traceability. Organizational practices include proactive risk management, periodic internal audits, standardized incident management procedures, least-privilege access controls, and ongoing cybersecurity training for the team.

ISO 27001 Information Security	ISO 14001 Environmental Management	ISO 9001 Quality Management	ENS Medium National Security Framework