Synamedia
SENZA

Security Whitepaper

The surge of OTT technologies in recent years has undeniably presented opportunities for Operators to exploit zero-cost endpoints like web browsers, smart TVs, and mobile devices. The rapid development and release cycles offered by contemporary web and mobile development techniques have allowed them to swiftly deliver low-cost services, adjusting to evolving market needs.

Synamedia's revolutionary new product, Synamedia Senza, is an exclusive, patent-protected network, that has entirely reimagined the concept of IP streaming. It is a disruptive solution in the realm of Over-the-Top (OTT) video services, enabling ultra-low latency video distribution and facilitating graphic-accelerated user experiences at a lower total cost of ownership.

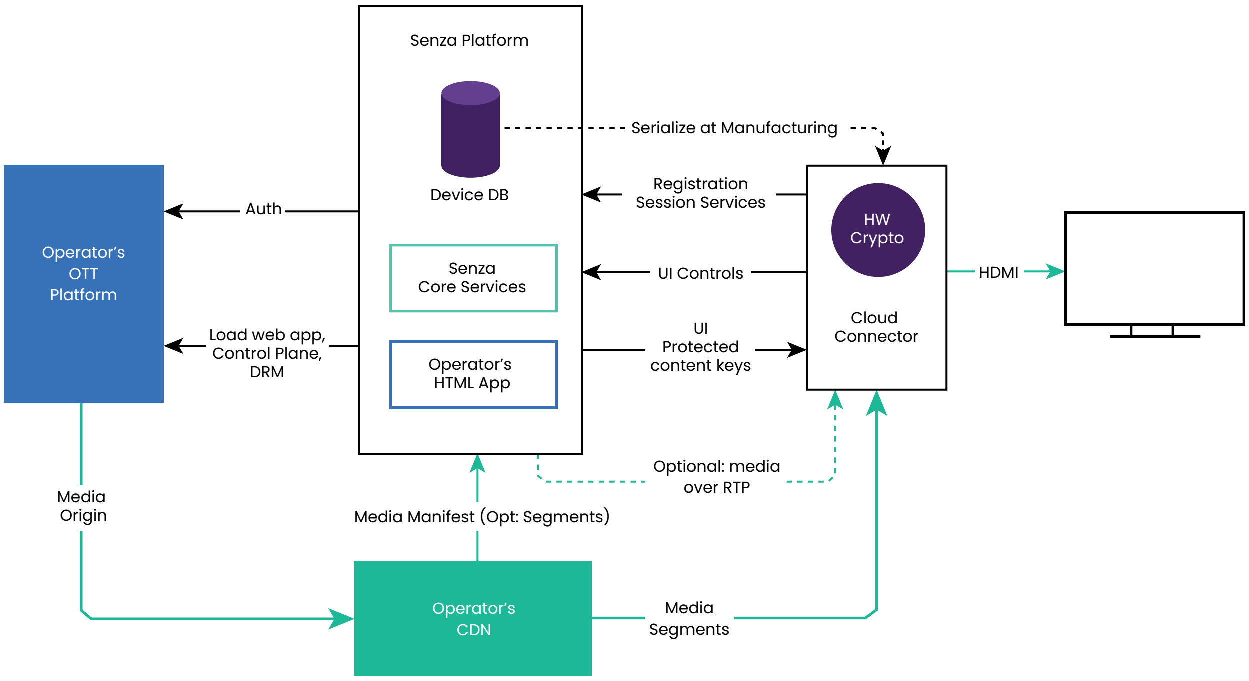
But that's not all. The distinctive architecture of Senza brings forth an exceptionally secure ecosystem for OTT content delivery, something that conventional OTT systems have struggled to match. This paper focuses on how Senza enhances the security landscape for Operators and media OTT platforms.

However, these technological advancements are a double-edged sword, giving rise to opportunities for pirates and intensifying the challenge of protecting video content from illicit acquisition. The existing security measures, largely relying on hardware-hardened endpoints, are a potential solution, but their difficult and lengthy integrations with varying devices makes them impractical, especially with standard endpoints.

Senza Architecture: Key components and their contribution to security

At the heart of the Senza network lies a sophisticated, robust architecture that fundamentally distinguishes its security capabilities from conventional OTT platforms. This section will delve into the detailed examination of the network's key components and how they each contribute significantly to reinforcing the security of the Senza network.

The analysis will underline how the architectural design and strategic elements combine to provide a formidable defense against content theft and unauthorized access, creating a secure environment for operators and content owners. The following diagram illustrates the structural layout of Senza's architecture, providing a visual representation of how its key components interact and cooperate to create a fortified, secure ecosystem for content delivery.



The **Cloud Connector** device used by Senza, receives content and the user interface over the subscriber's Wi-Fi network and displays it on a TV. It utilizes unique proprietary hardware with a secure cryptographic core, serialized with a unique ID and keys by Synamedia during production. The Cloud Connector operates hardened, encrypted, and authenticated software booted securely to ensure maximum content protection. In addition, the device's software image has limited functionality, minimizing the potential attack surface.

The **Senza platform** delivers password-less authentication and authorization of Cloud Connectors using unique secrets provisioned during manufacturing. It provides a secure cloud-based virtual browser for end-user web interface execution. Importantly, by storing key certificates in the cloud, not on the end-device, it greatly increases system resilience and reduces the risk of security breaches.

The **Operator's OTT platform** provides standard OTT video services. It handles access authorization to the OTT service, along with associating devices with their respective subscribing households. The platform provides a web-based application, executed within the secure Senza cloud's virtual browser environment. Additionally, it supports control-plane services essential for the web application and a Digital Rights Management (DRM) service for OTT content protection. Media-plane services, such as live linear and Video-on-Demand (VOD) are also facilitated over the Internet via Content Delivery Networks (CDNs).

Upon startup, the Cloud Connector utilizes a cryptographic anchor, set during manufacturing, to securely authenticate itself with the Senza Cloud and validate its identity to the customer's application. Subsequently, it establishes an encrypted communication channel with the Senza Cloud. This secure connection facilitates the streaming of the web UI to the Connector and TV.

The Cloud Connector can receive media in two formats:

1. Ultra-Low-Latency: In this method, the Senza service, which procures the content from the CDN, transmits it to the device over an ultra-low-latency protocol.
2. Adaptive Bitrate (ABR) Format: Here, the content originates from the CDN. The Senza service processes the manifest and provides the Cloud Connector with a list of segments to download.

Regardless of the format, DRM functionality is divided between the Cloud Connector and the Senza Cloud[1]. The Senza Cloud handles all cryptographic operations associated with the generation of a license request and the processing of a license response. The Cloud Connector, leveraging its hardware cryptographic capabilities, decrypts the media. This pioneering architecture, a key differentiator of our security proposition, ensures a superior level of content protection by never exposing content keys in the Cloud Connector's memory .

Given that the Senza Cloud Connectors are fully managed, it is always possible for the Senza platform to deny service access to a specific device, either temporarily or permanently.

Additional security features include watermarking for any content and the option to stream media via the Senza Cloud ultra-low-latency service, which can enhance the protection of certain assets.

- If the assets are exclusively available to end users through Senza (e.g. using a CDN access token only available to authorised users), pirates will be unable to employ CDN leeching to access the content.
- Synamedia has the capability to apply unique, per-user processing on the media as it is sent to the Cloud Connector. The media can be re-encrypted with device-specific content keys. A device-specific spatial watermark can be applied. This watermark cannot be disabled at the device level, making it more resistant to collusion-based evasion techniques.

The standout security anchors of the Senza architecture that truly set it apart from other solutions are:

1. The robust, hardware-based cryptographic identification of end-user devices. This feature acts as a solid foundation for ensuring device security.
2. The execution of sensitive cryptographic operations, such as media decryption and license processing, are either completely shielded by the devices' hardware crypto functionality or handled securely in the cloud, putting them far beyond the reach of potential hackers.

In summary, as this paper illustrates, Senza represents not just a step, but a leap forward in not only enhancing user experiences, but also in ensuring the safety and integrity of OTT services. The unique security facets of the Senza architecture make it an exceptionally secure solution, marking a significant advancement in OTT service protection.

[1] Google Widevine DRM: The Cloud Connector and Senza platform are L1 Google certified.

About the authors

Tzvi Gerstl, is the CTO of Synamedia, with over 25 years of leadership in global technology, particularly in pioneering cutting-edge technology in the video and entertainment industry. As a PhD in Scheduling Algorithms, holder of numerous patents, and author of over 25 academic papers on algorithms, Tzvi offers a unique and insightful perspective on contemporary tech challenges.

Itai Zilbershtein, a Distinguished Software Architect at Synamedia and security expert, holds an MSc in Electrical Engineering. With over 30 years of experience and 29 patents to his name, his innovative contributions have significantly shaped both software and hardware systems.