intertrust®

Case Study

Secure Systems

Major Media and Technology Firm Boosts Security Across its Apps and Devices

Industry
Media and Technology

Location
International Scope

Solution
Intertrust whiteCryption® Secure Key Box™
Intertrust whiteCryption Code Protection™
Intertrust Seacert™

Customer profile

This major Media and Technology Company (the Firm) operates multiple business divisions on a global scale. The Firm provides for the distribution of entertainment content via multiple outlets to subscribers and others. The Firm has enjoyed strong organic growth as well as expansion through key acquisitions and divestments.

The challenge

Media distribution companies around the world face similar challenges. The amount of quality content available today and in the future has and will continue to increase at an exponential rate. The methods and means that customers use to consume content continues to evolve in meaningful ways as well.

According to a study by Deloitte Consulting[1], two key trends have begun to dominate the media and entertainment sector: the skyrocketing growth of streaming and mobile video, and a shift away from traditional pay TV. Deloitte notes that 55% of U.S. households now subscribe to paid streaming video services and nearly half of all U.S. consumers stream TV content every day or weekly on all types of devices, including TVs, smartphones, and tablets.

This fundamental shift in consumer preference has been directly linked to the rise in streaming TV service such as Netflix, Hulu, Sling TV, FuboTV, and Amazon Video.

These so-called 'Over The Top' (OTT) content providers bypass traditional TV gatekeepers to deliver programming on demand via broadband connections.

The rise in OTT popularity has not escaped the attention of traditional broadcast providers. Many traditional content distribution companies have partnered with these new age TV streaming services to provide streaming options for subscribers.

With increasing subscriber fragmentation and the need to distribute content using the widest range of outlets and devices possible, the Firm was under tremendous pressure to protect its own content and that of a growing number of independent content providers such as Netflix, Amazon, Hulu, YouTube, and others.

Challenge highlights:

- Meet strict content protection and security guidelines set down by content providers or risk loss of content and revenue
- Protect vital subscriber personal information
- Deliver cryptographic protection for critical content keys
- Provide end-to-end content protection, from server to any display device, be it a smart TV, tablet, or mobile phone
- Protect legacy devices lacking any hardware security capabilities

whiteCryption Secure Key Box has been certified to the highest standards, including FIPS 140-2 Level 1… whiteCryption SKB is one of the only solutions that is resistant to side channel attacks, including cache, timing, power monitoring, electromagnetic [and] acoustic.

The solution

The Firm turned to Intertrust Technologies to help protect its end-to-end ecosystem of services and devices, including media servers, license servers, set-top boxes, DRM engines, and associated compliance and robustness rules.

The Firm chose Intertrust's whiteCryption® suite, the industry-leading application shielding solution to prevent hackers from reverse engineering and tampering with code. whiteCryption provides advanced obfuscation, runtime application self-protection (RASP), and white box cryptography for mobile apps, desktops, firmware, and embedded applications.

In order to protect millions of set top boxes (STBs) of various generations, the Firm implemented **whiteCryption Secure Key Box™** to protect the access keys to individual STBs, as well as other content distribution devices in its network. The Secure Key Box (SKB) solution works across any hardware, old or new, and can be deployed without human intervention, saving time and providing a more positive customer experience. whiteCryption SKB has been certified to the highest standards, including FIPS 140-2 Level 1 standard administered by the National Institute of Standards and Technology (NIST). FIPS 140-2 is also required by federal agencies in Canada and recognized in Europe and Australia.

whiteCryption SKB is one of the only solutions that is resistant to side channel attacks, including cache, timing, power monitoring, electromagnetic, acoustic, and other forms of side-channel attacks. The Firm also deployed **whiteCryption Code Protection™**, which protects streaming apps on handheld devices, as well as smart TVs, HDMI dongles, and other devices. Code Protection uses sophisticated hardening techniques, including advanced code obfuscation, to deliver the best protection while maintaining performance and minimizing memory impact.

Code Protection further strengthens app security with runtime application self protection (RASP) that triggers automatic defense response upon any inspection or tampering attempt. Customizable defense actions include forced program exit, data deletion, logging, and real-time notification.

This deployment of whiteCryption Secure Key Box and Code Protection is enabling the Firm to fulfill a key obligation to protect the intellectual property of its content providers[.]

The results

Through the combined impact of the two whiteCryption solutions, the Firm has fortified and is actively protecting a diverse content delivery infrastructure against hackers and other bad actors seeking to disrupt their business, steal content, and obtain private information.

This deployment of whiteCryption Secure Key Box and Code Protection is enabling the Firm to fulfill a key obligation to protect the intellectual property of its content providers and reduce the risk that it would lose important content and associated revenue as a result.

whiteCryption Secure Key Box and Code Protection provided a highly cost-effective deployment since both applications could be remotely distributed and installed via the internet wherever needed with little human intervention or set-up time required.

Both whiteCryption solutions were implemented to ensure proactive security at the core of business operations so that no stakeholder associated with the Firm would suffer damages or malpractice.

The Firm also has plans to deploy the **Intertrust Seacert™ PKI** (public key infrastructure) service to provide trusted digital certificates to authenticate the identity of devices and services. Unlike most certificate authorities (CAs), Seacert is purpose-built for consumer electronics and mobile devices, offering a highly scalable, secure infrastructure. Seacert PKI will also help support the company to grow its business in IoT markets and better control access and security for IoT devices.

1. 2019 Media & Entertainment Industry Outlook– A new world of content and advertising possibilities Deloitte Center for Technology, Media & Telecommunications