intertrust

ExpressPlay DRM

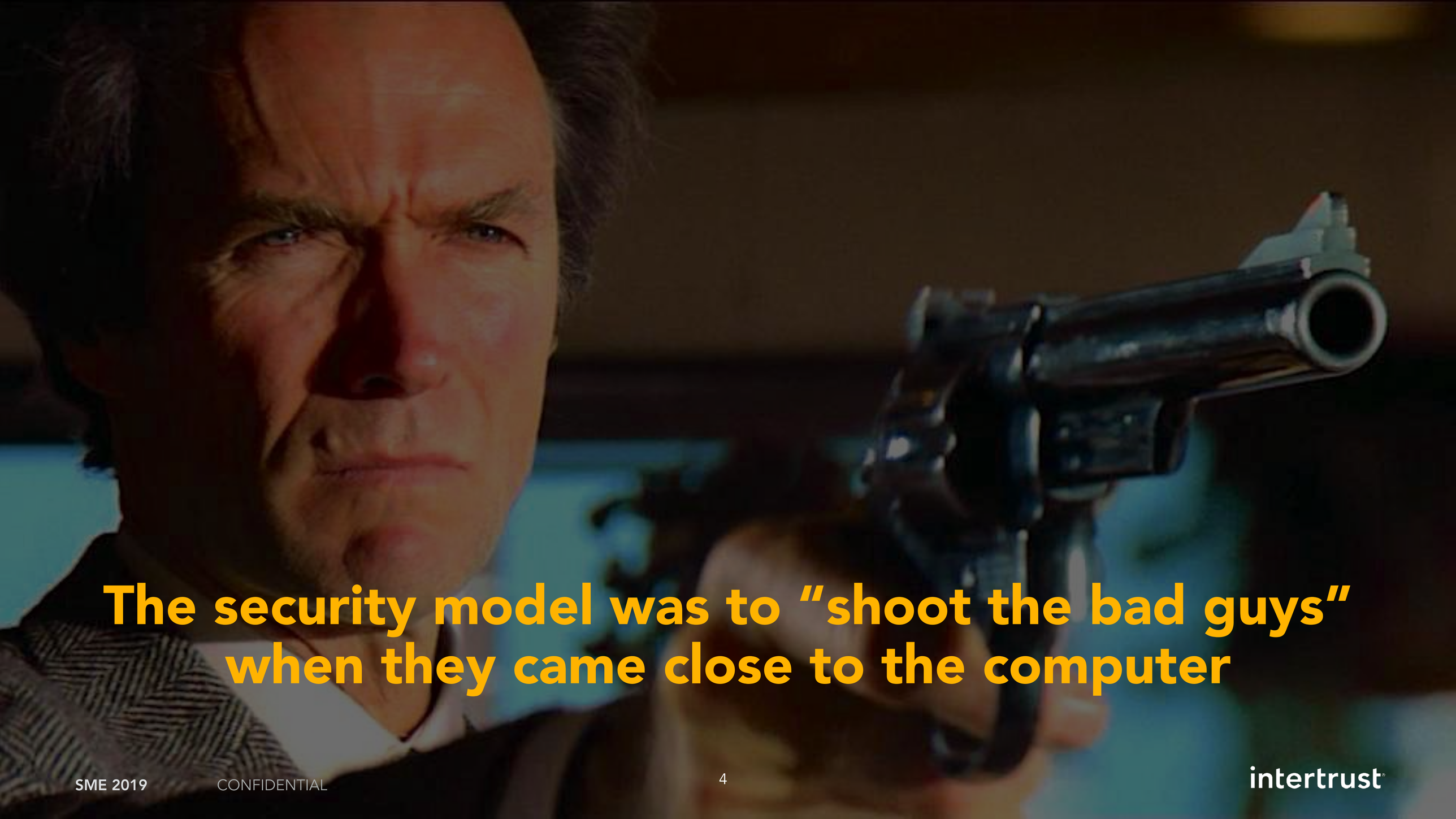
Streaming Media East 2019

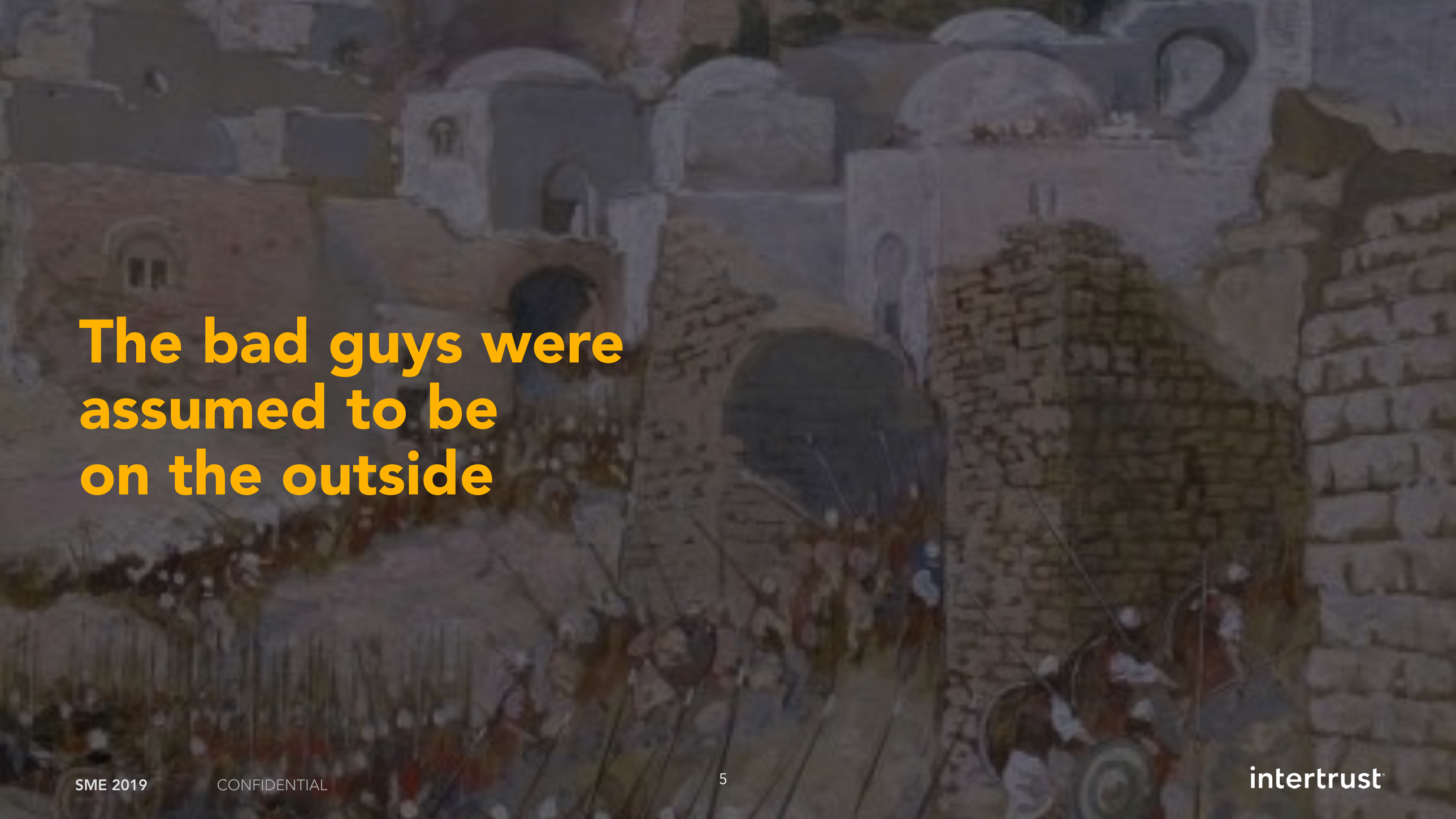
Building Trust for the Connected World

Incorporation	Founded in 1990, HQ Silicon Valley - Shareholders: WiL, Sony, innogy, Philips
Expertise	Leader in security, privacy, and trust for open networks and service-enabled devices
Inventions	Trusted Distributed Computing, Digital Rights Management, Secure Interoperability
R&D	Top research lab – top scientists including Turing Prize recipient
Markets	Media, energy, IoT, auto, data, healthcare and more
Products	Media Monetization, Internet Secure Systems, Trusted Data Platforms

The Internet was originally designed for military and government communication to be resilient, robust and distributed

not for consumer devices


The security model was to “shoot the bad guys”
when they came close to the computer



The bad guys were assumed to be on the outside


As computing became ubiquitous
and consumer devices became service-enabled
trust and security became
an inherent part of operating systems

DRM ANSWERS THE QUESTION:

“CAN I TRUST YOU WITH MY CONTENT?”

INTEROPERABILITY,
TRUST AND SECURITY
ARE CRITICAL TO SUCCESS

AND SHOULD BE INVISIBLE TO CONSUMERS

ExpressPlay DRM

ExpressPlay DRM

ExpressPlay™ DRM is trusted by some of the largest names in the industry

- Hollywood movies streamed in China by Alibaba, iQIYI, and Tencent
- iFlix with 15 million online subscribers

Why Deploy DRM at all?

AES

- All DRM use AES as the algorithm for encrypting content.
- AES is cryptographically secure, however, AES encryption is of no value if an unauthorized user has access to the key used to decrypt content.
- AES has to be supported by a secure key exchange protocol.

Secure Key Exchange

- Authentication tokens and Signed URLs are used to obfuscate the source from where the key is delivered.
- However once an authorized user has the key, there is nothing stopping them from sharing the key with non-authorized users.

Digital Rights Management

- DRM provides an extra layer of security.
- A DRM license contains rules and an encrypted content key.
- The content key is used to decrypt the content for playback.
- The DRM license and encrypted content can be freely shared without additional protection.
- Content can only be played on authorized devices according to the terms specified in the DRM license.

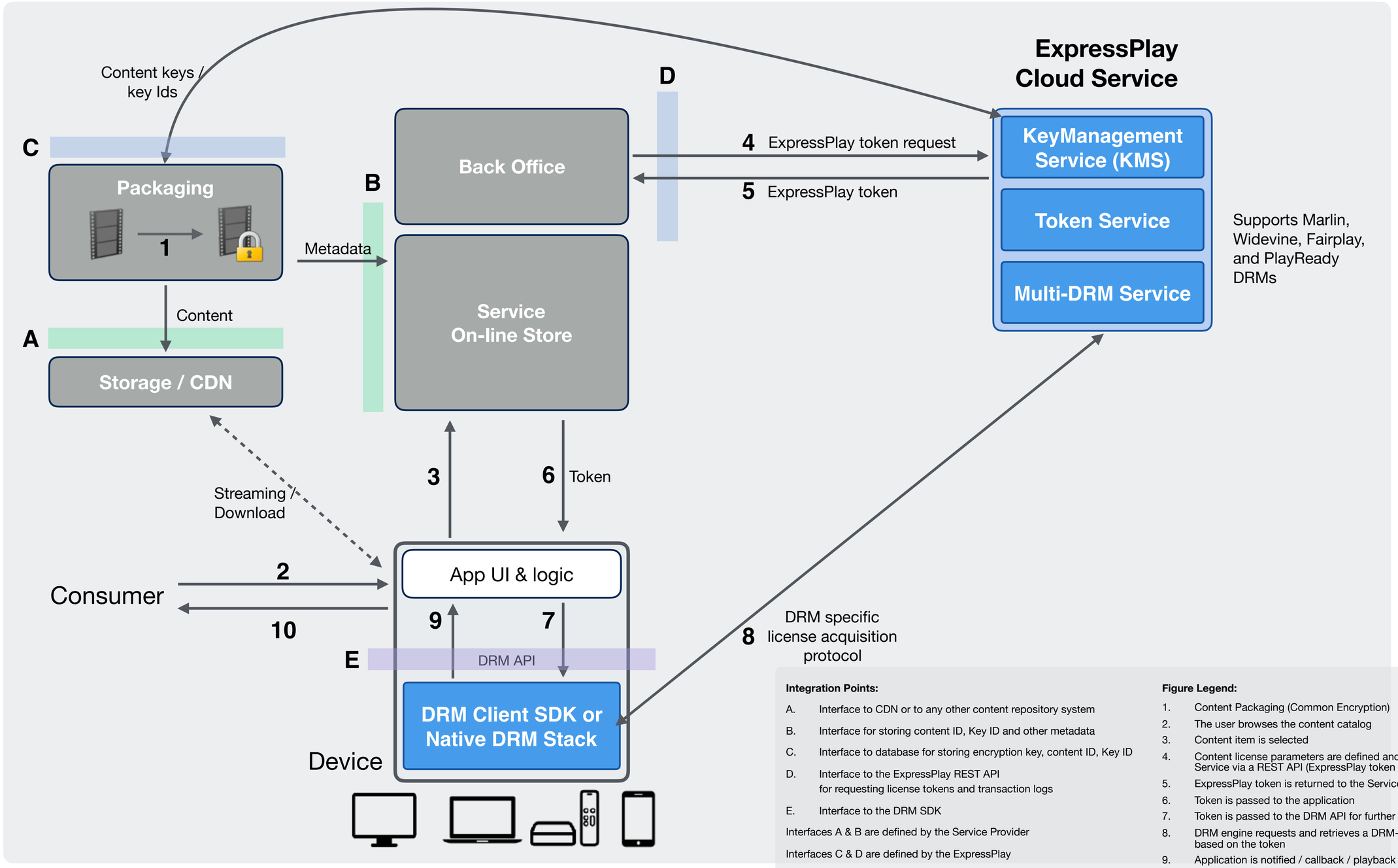
ExpressPlay DRM

- **Supports all major DRMs**
  eliminates the need to distribute multiple versions of protected assets.

- **Universal Token** enables runtime selection of DRM system, FairPlay for iOS devices and Widevine for Android devices etc. to leverage the security built into the device by a manufacturer.

- **Real time audit log** of license acquisition events
  important if you need to charge individual services for DRM usage.

- **Key Management Service** seamlessly integrated with license generation API
  for secure online storage of content keys.



Integration Points:

A. Interface to CDN or to any other content repository system

B. Interface for storing content ID, Key ID and other metadata

C. Interface to database for storing encryption key, content ID, Key ID

D. Interface to the ExpressPlay REST API
for requesting license tokens and transaction logs

E. Interface to the DRM SDK

Interfaces A & B are defined by the Service Provider

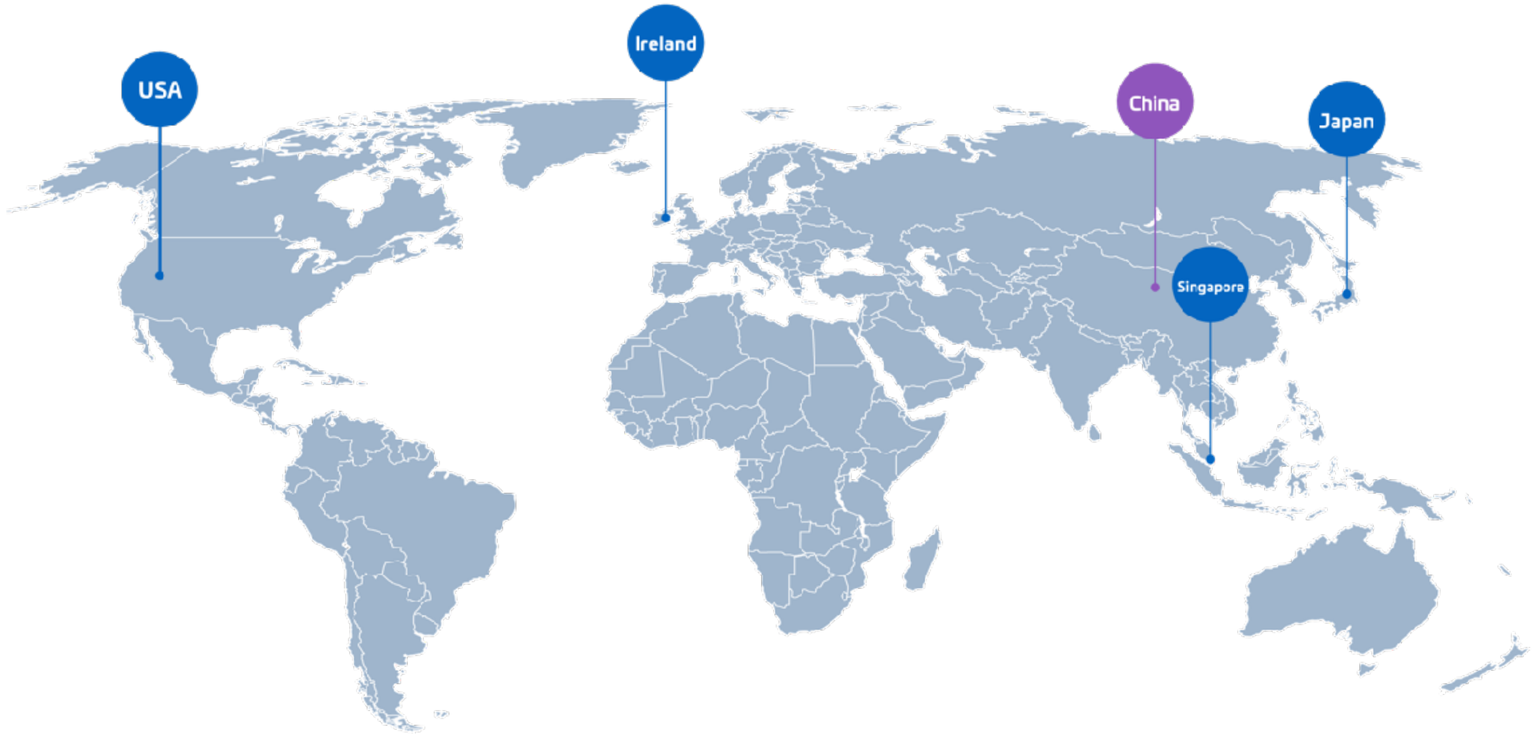
Interfaces C & D are defined by the ExpressPlay

Interface E is defined by DRM provider

Figure Legend:

1. Content Packaging (Common Encryption)
2. The user browses the content catalog
3. Content item is selected
4. Content license parameters are defined and passed to the ExpressPlay Service via a REST API (ExpressPlay token request)
5. ExpressPlay token is returned to the Service Provider
6. Token is passed to the application
7. Token is passed to the DRM API for further processing
8. DRM engine requests and retrieves a DRM-specific content license based on the token
9. Application is notified / callback / playback can start
10. The consumer can access the content

Global Deployment



- AWS with health checks and active-active failover between AWS Regions
- Requests automatically routed to fastest Region
- Deployments on multiple availability zones within each region with automatic failover
- Tens of thousands of Transactions Per Second
- Scaled for major sports events when millions of viewers tune in at the same time
- Billions of Licenses served in 2018

AWS with Amazon Route 53

ALICLOUD

The Rationale for Multiple DRMs

- Typically, each device supports one or a limited number of DRMs.
- If you want maximum device reach, you need to use multiple DRMs.

	NATIVE DRM SUPPORT / STREAMING FORMAT
HTML5 BROWSERS	
GOOGLE CHROME	Google Widevine
	DASH-CENC
FIREFOX	Google Widevine
	DASH-CENC
INTERNET EXPLORER 11 (WINDOWS 8.1+)	Microsoft PlayReady
	DASH-CENC
MICROSOFT EDGE	Microsoft PlayReady
	DASH-CENC
SAFARI (MAC OS AND IOS 11.2+)	Apple Fairplay
	HLS SAMPLE-AES

	NATIVE DRM SUPPORT / STREAMING FORMAT	MARLIN DRM / STREAMING FORMAT	
MOBILE			
IOS	Apple Fairplay	Yes, using ExpressPlay™ binary SDK for iOS	
	HLS SAMPLE-AES	DASH-CENC	HLS AES-128
ANDROID 4.4+	Google Widevine	Yes, using ExpressPlay™ binary SDK for Android	
	DASH-CENC	DASH-CENC	HLS AES-128
ANDROID 4.0-4.3	-	Yes, using ExpressPlay™ binary SDK for Android	
		DASH-CENC	HLS AES-128
EMBEDDED DEVICES			
CHROMECAST	Google Widevine, Microsoft PlayReady		
	DASH-CENC		
AMAZON FIRETV	Microsoft PlayReady		
	DASH-CENC		
SMART TVS			
SAMSUNG TIZEN	Google Widevine, Microsoft PlayReady		
	DASH-CENC		
HBBTV 1.5, 2.0	Marlin, Microsoft PlayReady	Yes, native Marlin support	
	DASH-CENC	DASH-CENC	

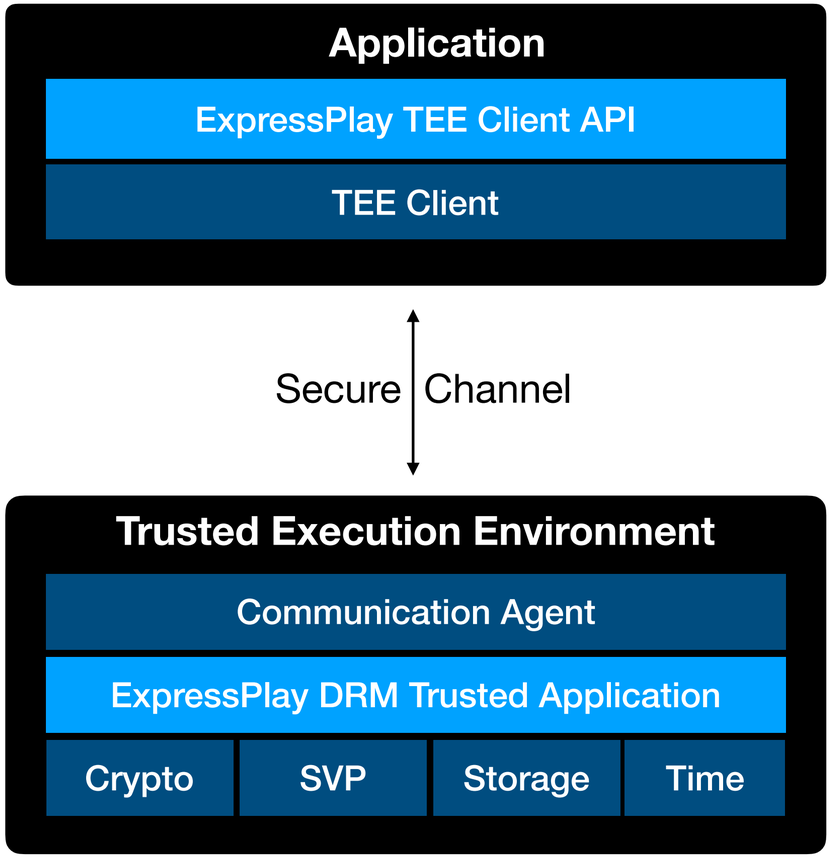
Enhanced Content Protection

ExpressPlay Porting Kit

- Enables chipset vendors to meet MovieLabs' Specification for Enhanced Content Protection (ECP) requirements using Marlin.
- A device that has undergone ECP self-certification handles content protection logic, content keys, licenses, content display and output in compliance with ECP rules.
- When a device has selected content that requires enhanced content protection from a content distribution service, a content license is created that includes an obligation that the content be handled at the ECP Security Class 4 level.
- Devices that are not ECP Licensed Products will not recognize the ECP Security Class and will therefore refuse to play the associated content.

ExpressPlay Porting Kit

- Compatible with GlobalPlatform Trusted Execution Environment (TEE)
- License Evaluation and Key Handling in TEE
- SoC key ladders can be used with decryption
- Enforcement of HDCP 2.2 output controls
- Root detection
- Secure Video Path
- Secure Storage
- Secure Clock



DRM and Watermarking

Watermarking Use Cases

Major Sports Events

Early Window Movies

The Case For DRM and Watermarking

- **Households viewing illegal content** (ABI Research)
  - 15% of households in Latin America
  - 14% in Asia Pacific
  - 9% in North America
  - 7% in EMEA

- **Source of illegal content** (MUSO Research)
  - 73% of illegal content originated from streaming sites
  - 17% originated from torrent sites

- Consumers either stream content over the internet for free, or watch content from an illegal service they pay

The Case For DRM and Watermarking

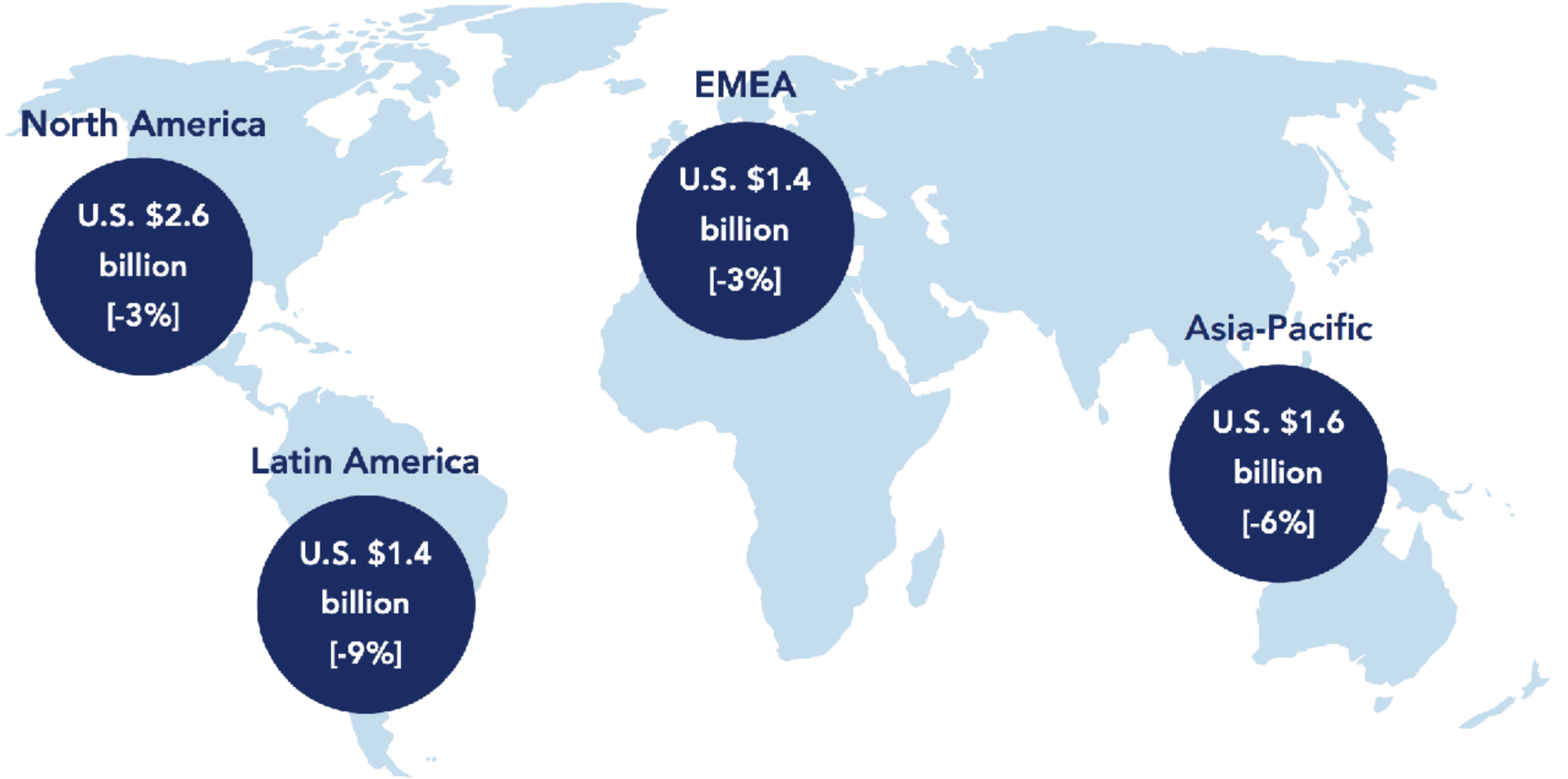
- **Game of Thrones season 8 premiere** had almost 55 million illegal views
  - 76.6% came from unofficial streams
  - 12.2% web downloads
  - 11.3% torrents
- HBO had 17.4 million paying viewers
  - 11.8 million MVPD
  - 5.6 million HBO GO and HBO Now
- Most illegal views by country
  - India about 10 million views
  - China about 5 million views
  - United States nearly 4 million illegal views

Source: MUSO

The Economics of Conversion

The pay TV industry could gain U.S. $7 billion per year by converting one in four pirates to legal users

Global = approximately U.S. $7 billion (~4% of revenue)



Source: ABI Research (pdf)

How Illegal Redistribution Is Done

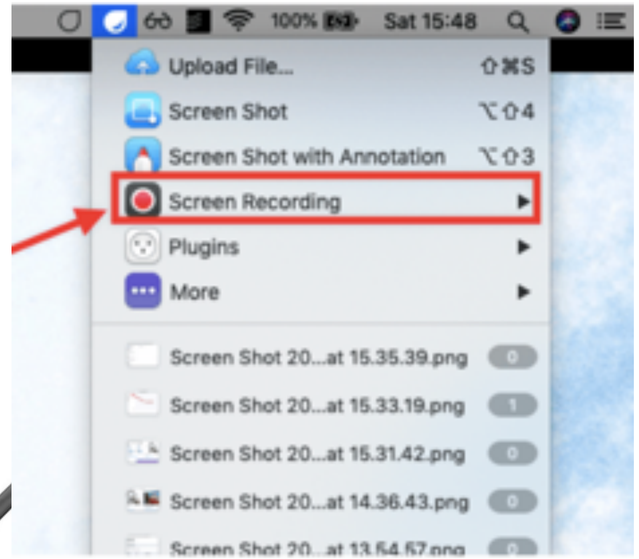
1. Subscribe to a video service
2. Decrypt the content
3. Redistribute the content without a license

   ★ What's new is that re-streaming is global

How?

- Screen scraping
- Screen casting
- HDMI splitter to remove HDCP
- Control word sharing
- Camcording

Open Broadcaster Software
Latest Release 23.1 - April 5th



Who Re-Streams Video?

- Professionals looking to profit from the theft of intellectual property
  - Looks like legal video service, reliable content delivery, quality user interface
  - Paid service is the norm, occasionally advertising
- Free-seekers looking to avoid paying

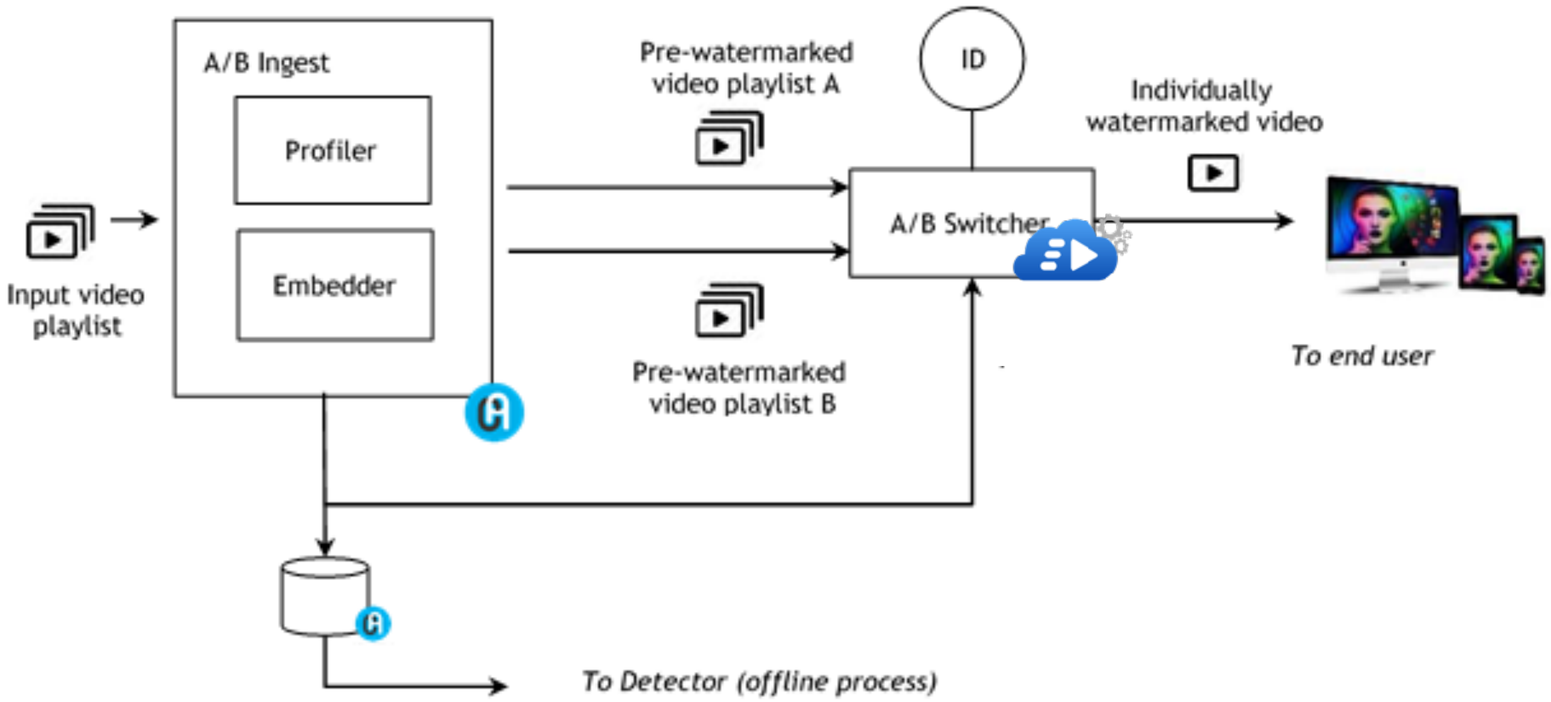
The Case For Watermarking

Watermarking can identify the source of illegally redistributed content and enable its shutdown

The Case For Watermarking

1. **Protect content**
2. **Find it when it leaks**
3. **Trace it to whoever leaked it**
4. **Shut down the source of the leak**

A/B Watermarking (1 of 2)



Content Profiling

- Content profiling done once per asset at ingestion step
- Creates two variants of same asset (‘A’ and ‘B’)

A/B switcher

- Each end user receives unique manifest based on unique session id
- Manifest of A & B variants implemented by server (or client)

Two Video Files

- Pro: server side switching in secure facility
- Con: storage/bandwidth overhead in thousands of servers

Client Watermarking (2 of 2)

- Watermarking SDK typically integrated into STB chipset driver layer or STB middleware or OTT player/app
  - Protected with tamper hardening and white box crypto
- Pros:
  1. No head-end preprocessing required, codec agnostic, transport agnostic, DRM agnostic
  2. Can be implemented with single video source (no A/B)
- Cons:
  1. Client is accessible by anyone

End-to-End Anti-Piracy Solution

1. **Fingerprinting -** reference fingerprint for each video service or content owner.

2. **Watermark** is overlaid onto video to identify a subscriber, device or player.

3. **Identification of illegally distributed content**
   - Distribution channels are continuously monitored using automated fingerprint identification algorithms to identify fingerprinted content.
   - Captured content is compared to a library of reference fingerprints.
   - When an illegal video stream is identified, the video is analyzed further and the watermark is used for subscriber level identification.

4. **Action**
   - An illegal stream can be shut down by stopping transmission of content to the endpoint who is redistributing the content illegally, or a forensic evidence package can be established for subsequent legal action.

ExpressPlay DRM - Summary

1. Global service that scales for tens of millions of simultaneous viewers.
2. ExpressPlay reduces the cost of implementing a multi DRM solution and accelerates time to market.
3. Supports all business models.
4. Protected content will play on almost all devices.
5. Robust protection with Enhanced Content Protection and watermarking.

intertrust

BUILDING TRUST FOR THE CONNECTED WORLD

Tom Carroux
tcarroux@intertrust.com