irdeto

Protect. Renew. Empower.

# TECHNICAL ISSUES AND POSSIBLE SOLUTIONS

Mark Mulready, VP Cyber Services Irdeto & Co-President AAPA
II COLÓQUIUM DIGITAL PIRACY OF AUDIOVISUAL CONTENT
Lisboa – 5 June 2024

# OTT video is exploding

## The two sides of the coin

### Direct to Consumer & Hybrid Services

*OTT subscribers' growth*

*Higher availability of services*

*Attractive offerings*

### OTT Piracy & Service Abuse

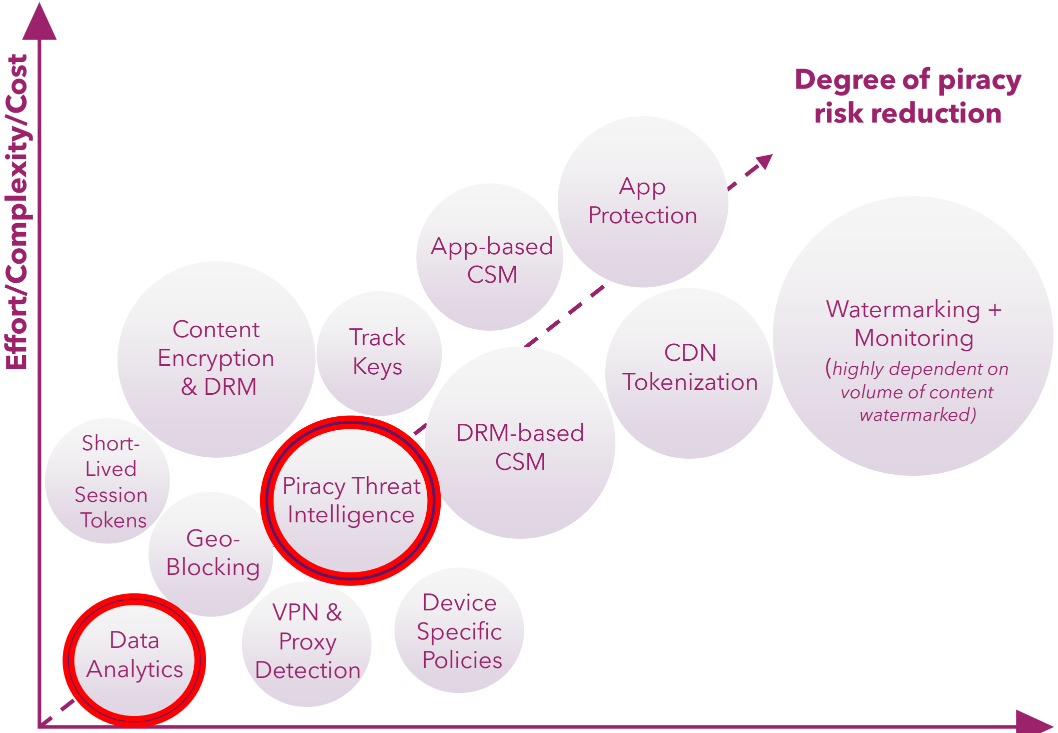
*Session sharing*

*Credentials sharing*

*Content key harvesting*

# OTT Security Strategies

## Industry best practices



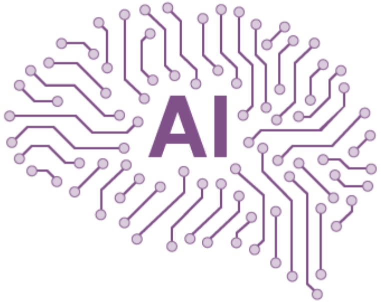
**Circle size = individual impact**

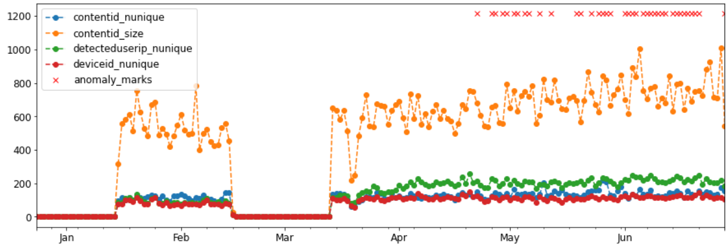
Find the **wininng balance** for your business

# Data Analytics & Fraud Management

- **AI powered anomaly detection** based on account specific data to detect suspected piracy and service abuse

- **Identify** piracy and service abuse (use cases):
  - *Subscriber accounts engaging in session sharing attacks*
  - *Subscriber accounts overriding service usage mechanisms e.g. concurrent stream limits*
  - *Subscriber accounts circumventing service geo-IP service access rules*
  - *Subscriber accounts and devices harvesting content encryption keys*
  - *Use of compromised unique devices (e.g. specific DRM device IDs)*
  - *Use of compromised device fingerprints e.g. emulators and SDKs*
  - *Identify and validate compromised DRM clients*
  - *Identify and validate new piracy attacks and tooling*





- **Investigation & validation** of vulnerabilities, tools and exploits

- **Assess impact** & implement **mitigation actions**

- **Security assessment** of OTT platform, apps and security policies

# OTT Threat Intelligence – Case Study – 7 Day Period

## 2-Step Widevine L3 Key Theft

7 Accounts
48 transactions
Android Emulators + Samsung CDMs

## Single-Step Key Theft

5 additional accounts
Systemid 4464 & 8162
Faked User Agents & Web/TV Entitlements

## Faked LG TV Widevine

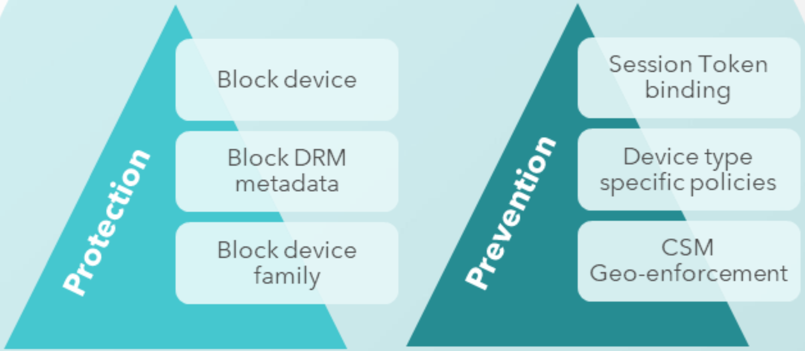
2 Additional accounts & 88 transactions
Cloudflare proxy
Faked LG User Agent

## Rebroadcast

2 Accounts
Multiple events

# Threat Mitigation

## Threat Mitigation



**DETECTION MITIGATIONS**

- Password Reset
- Warn/Suspend Accounts
- Investigations & Enforcement

irdeto

Protect. Renew. Empower.

THANK YOU!