Use Cases

verimatrix
DRIVING TRUST

How Streamkeeper with Counterspy Prevents Piracy

USE CASE:

COMMON SITUATION

Heterogeneous OTT System Operator with Many Different CA/DRM Providers & Clients Has Leaks

Operator is experiencing content leaks from their ecosystem, is getting little support to close the leaks, but needs to continue to use the leaking client or clients.

Studios and missed revenue put pressure on operator subscribers.

Often pirates abuse the Operators CDN to distribute pirated content.

Operators are also afraid to close suspected clients without independent verification of their involvement into the piracy.

HOW PROBLEM SOLVED

- Streamkeeper selected to stop piracy in its tracks.
- Verimatrix Multi-DRM closes the authentication gap and pushes pirates to use detectable hacks.
- Verimartrix' zero code technology allows the operator to inject all client applications with Counterspy functionality and client protection, hardening against piracy attacks.
- Pirates quickly identified and verified using watermarking to allow operators to confidently trace down pirate supply chains, and immediately take down offenders

RESULTS

- Unified permanent monitoring keeps the operator always informed about risks and recommends countermeasures.
- Piracy is prevented in most cases.
- If piracy happens, pirates can be removed from operator's network immediately.
- Pirates supply chains are tracked down.

verimatrix DRIVING TRUST

How Streamkeeper with Counterspy Prevents Piracy

USE CASE:

Where's My Leak?

Often the operator does not know which of his diverse clients on which platform is being abused by the pirates to steal keys and/or content.

After Verimatrix DRM Core closes the authentication gap, Counterspy detects suspicious client activity. This is helpful in case of the widespread content key distribution or URL cloning. We go beyond how distribution watermark identifies issues. The operator can decide to monitor, further verify, or take down the pirate client immediately.

HOW PROBLEM SOLVED

- Anti-piracy security agent deployed to identify the leak at its source.
- The agent utilizes app telemetry identification and shutdown capabilities found in Verimatrix Counterspy.
- Watermarking and fingerprinting technology verify the leak independently within one product.
- Together with key rotation, further abuse can be prevented

RESULTS

- Source of leak is identified and is independently verified to be the pirate source, is shut down immediately, or kept under observation to track down the supply chain of the pirates' content distribution.
- Note: Immediate shutdown does not work if the content is stolen from the CDN using a stolen key. We can shutdown rediustributed content, we cannot shutdown key distributed content if there is no key rotation, or if we do not have Edge Authenticator activated. In cases where there is slow key rotation, this is still good as it disrupts the pirates.

verimatrix DRIVING TRUST

How Streamkeeper with Counterspy Prevents Piracy

USE CASE:

I Know How My Content is Leaking, But How Can I Prevent It?

Often the operator knows how their content is being stolen but has no means to prevent it in every day situations.

Verimatrix DRM Core in combination with the protective measures of Counterspy, drive the pirates to use the few remaining attack vectors that Counterspy can prevent already in the client before it happens.

HOW PROBLEM SOLVED

- Anti-piracy security agent deployed to identify the leak at its source.
- The agent uses countermeasures against known attack vectors to prevent piracy and utilizes app telemetry to inform the operator about the attempt.

RESULTS

- Piracy is prevented.

verimatrix DRIVING TRUST

How Streamkeeper with Counterspy Prevents Piracy

USE CASE:

I Don't Know If My Network Suffers from Piracy Or Is In Danger

Often the operator does not know which of their platforms are abused by the pirates to steal keys and/or content, or if attempts are made to do so.

After Verimatrix DRM Core closes the authentication gap, Counterspy can detect suspicious client activity. The operator is presented a results page that shows threat level monitoring. Watermarking and web crawling provide independent leak tracing.

HOW PROBLEM SOLVED

- Anti-piracy security agent deployed to identify the leak at its source.
- The agent utilizes app telemetry identification found in Verimatrix Counterspy.
- Watermarking and fingerprinting technology allow independent search for the operator's content on the web.
- Both technologies combined provide a profound analytics of the operator's robustness about piracy.

RESULTS

- Operator has robust prevention in place to guard against piracy attacks.
- Piracy attacks are thoroughly and continuously monitored.
- Threat levelling is presented and continuously updated.
- Ongoing attacks that can be prevented are prevented and alerts are provided.
- Successful attacks are also monitored, and countermeasures are presented to the operator.

verimatrix DRIVING TRUST

Streamkeeper – Beta Inqueries Welcome

Artist rendering for demonstration purposes only

verimatrix DRIVING TRUST