fractal

# Advancing streaming piracy detection and prevention

## Unlock your streaming's true potential

Fractal's anti-piracy solution leverages AI, scalable data and cloud engineering, and user-centric design thinking to safeguard content, deliver real-time insights, and effectively enhance user experience in combating piracy.

# Industry landscape

In the Media & Entertainment industry, combatting content piracy, copyright infringement, and intellectual property theft has proven to be an ongoing and evolving challenge.

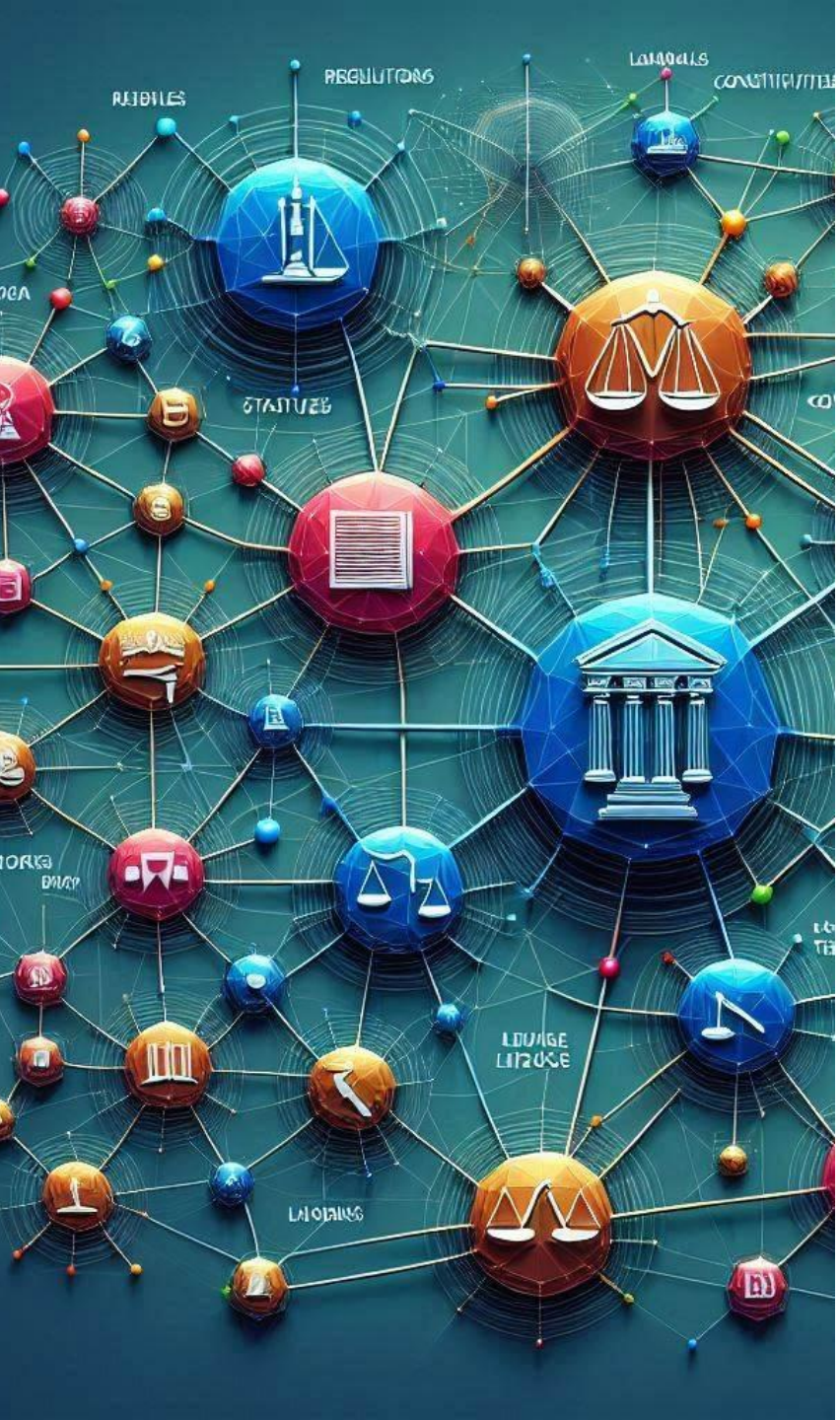
Despite substantial investments in legal and technological measures, effectively addressing these malicious practices remains daunting.

While the advent of streaming platforms initially showed promise and resulted in a temporary decline, recent years have witnessed a troubling resurgence of digital piracy.

This resurgence can be attributed to various factors:

- Insatiable consumer demand for immediate access to exclusive content,
- Economic and political instability,
- Shifts in viewing habits during the pandemic,
- Unregulated proliferation of generative AI technology.

Collectively, they contribute to piracy's prevailing and expanding presence.



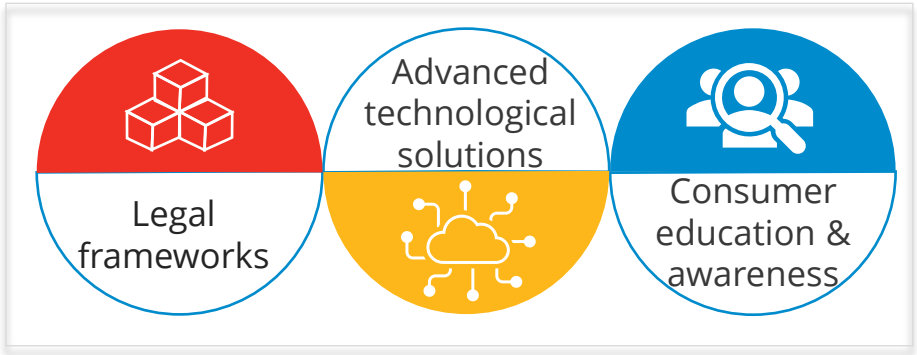
## Content piracy risks and

It is essential to recognize that piracy **undermines the revenue streams of content producers and artists and exposes consumers to significant risks**.

These risks encompass:

- Malware distribution,
- Identity theft,
- Counterfeit product dissemination,
- Potential ties to terrorism.

Addressing the content piracy issue requires a multifaceted approach leveraging...




Industry stakeholders must collaborate closely to develop and enforce robust anti-piracy measures.

Additionally, exploring **innovative business models, enhancing content accessibility, and ensuring a seamless user experience** can help mitigate the appeal of piracy.

By tackling content piracy head-on, the Media & Entertainment industry can **safeguard the interests of content creators, protect consumers from potential harm, and foster a thriving and sustainable digital ecosystem**.

The industry's current shortcomings and failure are quite evident in the alarming statistics.

Global statistics based on secondary research (FY'22-23) indicated that...

**230B views**

Pirated streaming contents represents >230B views per year

**$100B**

Media industry loses close to $100 billion annually due to digital privacy

**500K job lost**

~500k jobs are lost in the entertainment industry every year due to piracy

## Case study

In the face of mounting concerns surrounding their platform, a leading video-streaming service provider recognized the need for an intelligent solution to combat piracy proactively.

With millions of daily active users spanning multiple regions, and a vast library encompassing live sports, movies, TV series, and more, their dedicated anti-piracy team encountered numerous critical challenges.

# Framing the problem: Critical client challenges

Uncertainty regarding typical pirate behavior

Inability to pinpoint users at elevated risk of piracy

Dependence on manual and subjective decision-making procedures

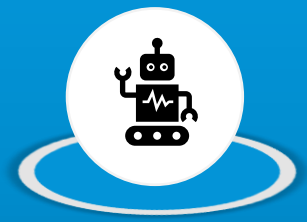
Limited visibility into piracy catalysts and indicators

Inability to adapt to evolving piracy patterns

# Client requirements

To overcome these challenges, the streaming provider joined forces with Fractal to deconstruct the overarching problem into smaller objectives.

Fractal created a robust anti-piracy framework by leveraging its AI expertise. The following requirements were identified for the framework.



### AUTOMATED RISK SCORING

Automated risk scoring of accounts, based on streaming behavior, IP address, device usage and other attributes.

### IP ADDRESS / DEVICE TRACKING

Near real-time monitoring of IP addresses and devices being used across multiple accounts and regions.

### BEHAVIOR IDENTIFICATION

Identification of other accounts with attributes and behaviors similar to identified pirates.

### SUSPICIOUS DEVICES MONITORING

Investigating suspicious devices to identify how those are used across accounts, to terminate or suspend the account.

# Fractal's anti-content piracy framework

## Key principles

Fractal has developed an approach rooted in three essential pillars of problem-solving to devise a cutting-edge anti-piracy framework that fulfills the identified requirements.

### Data and tech

Capture underlying dynamic user behavior at each point in the event journeys through real-time processing of millions of data-points.

### AI & ML

Robust and transparent algorithmic solution which can learn in real-time, identify potential pirates and drive actionable insights.

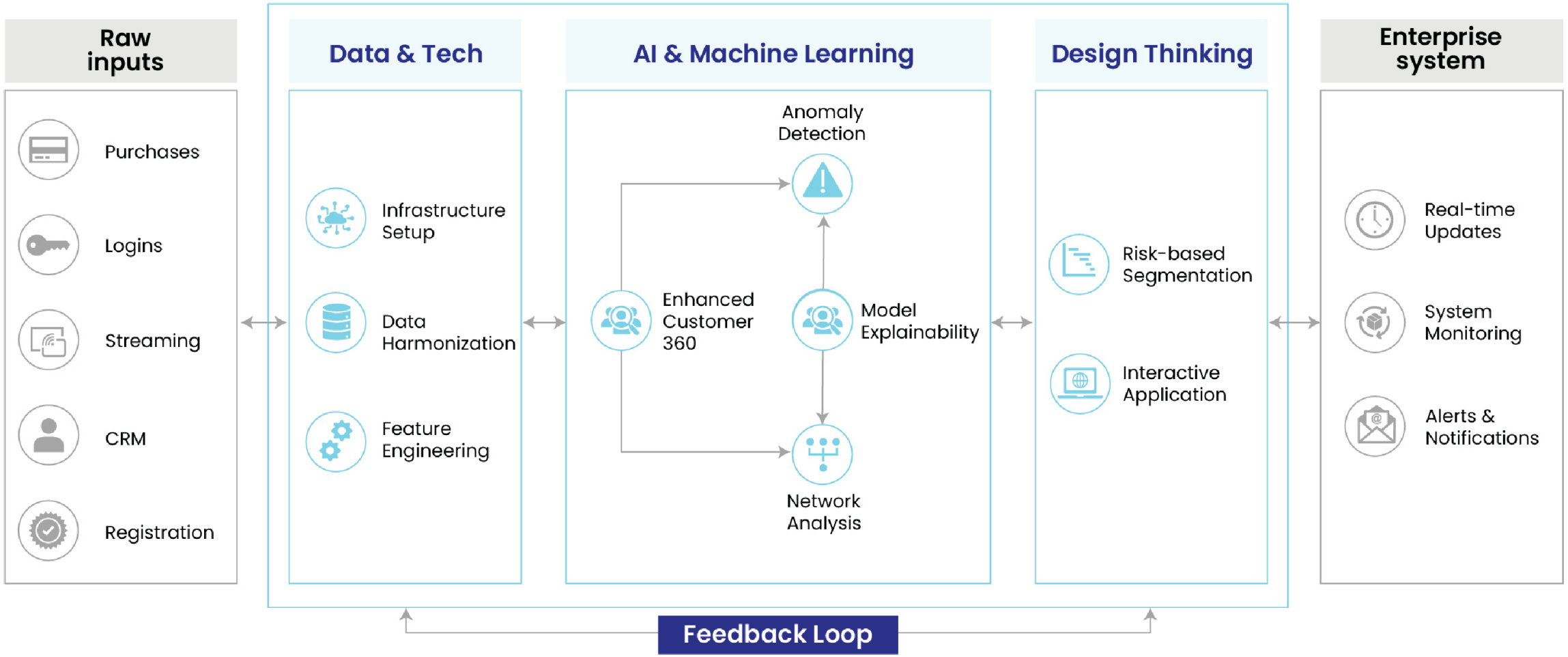
### Design Thinking

Easy-to-use interactive Web user interface to support real-time insight generation, self-service and manual over-rides, if required.

## Framework summary

The foundation of the framework is established on the robust infrastructure of Microsoft Azure. The diagram next page depicts the different components comprising this framework.

# Anti-piracy framework






fractal

# The solution’s three components


**Cloud and data engineering**


**AI**


**Design thinking**


# Cloud and data engineering

Cloud and data engineering forms the foundation of the architectural design enabling enhanced efficiency, scalability, and insights, and comprises three components: infrastructure setup, data harmonization, and feature engineering.

## INFRASTRUCTURE SETUP

To establish a scalable computational ecosystem, we leverage Azure services like **Azure Synapse Analytics, Azure Virtual Machines, Azure Blob Storage, Neo4J (**from Azure Marketplace)**, and Microsoft Power Apps**.

For data processing, the solution uses Python libraries like Pandas and NumPy, enabling both standard and customized data processing capabilities.

## DATA HARMONIZATION

The solutions **consolidates over 10 disparate data sources**, encompassing past purchases, logins, streaming sessions, demographics, and registrations. Through this process, it can establish a **single source of truth** known as Customer 360.

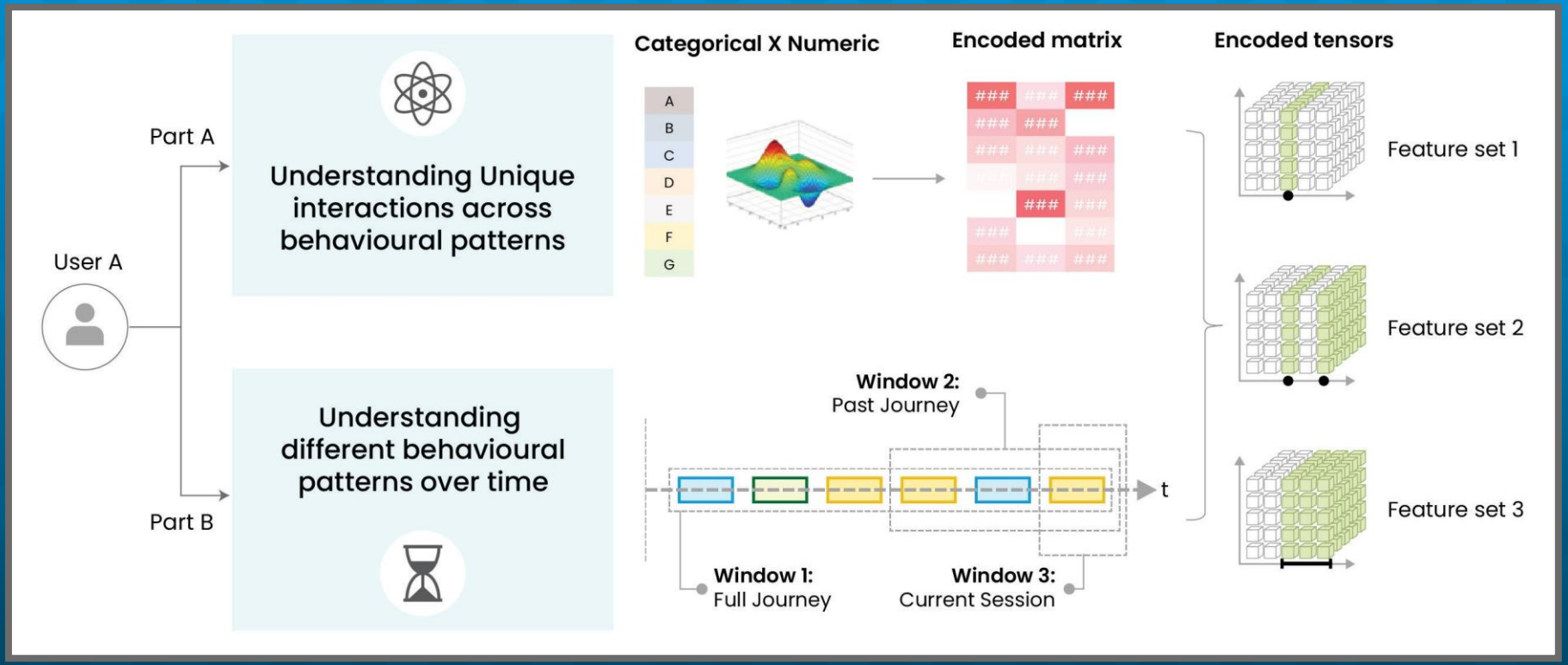
This unified data repository enables the solution to generate a comprehensive user context, empowering the customer with deep insights into user behavior, preferences, and engagement patterns.

1

# Cloud and data engineering (cont'd)

## FEATURE ENGINEERING

The solutions employs advanced data transformation and feature creation techniques to curate an enhanced **"Customer 360" profile that comprises over 500 features**. These features are the foundation for quantifying customer behavior across multiple dimensions and capturing diverse latent interactions.






fractal


# AI

The intelligent algorithm layer at the core of the anti-piracy framework is also comprised of three key components.

## ANOMALY DETECTION

Building upon the Enhanced Customer 360 data set, the solution leverages unsupervised auto-tuning anomaly detection algorithms to evaluate user behavior at the individual session/stream level. This approach enables continuous self-learning and adaptation, ensuring the solution remains vigilant against evolving piracy trends without the need for manual intervention.

Mathematically, the model can be summarized as follows:

$$r(u, s) = f(\text{Feature set 1, Feature set 2, Feature set 3}) \longrightarrow R[0,100]$$

*( r (u, s) = risk score for user "u" during session "s"; f = anomaly detection model;*
*Feature set 1–3 = features from Enhanced Customer 360 data set; R [0,100] = any real number between 0-100)*

While standalone anomaly detection plays a vital role, it is crucial to recognize that its effectiveness can be further enhanced through a holistic approach.

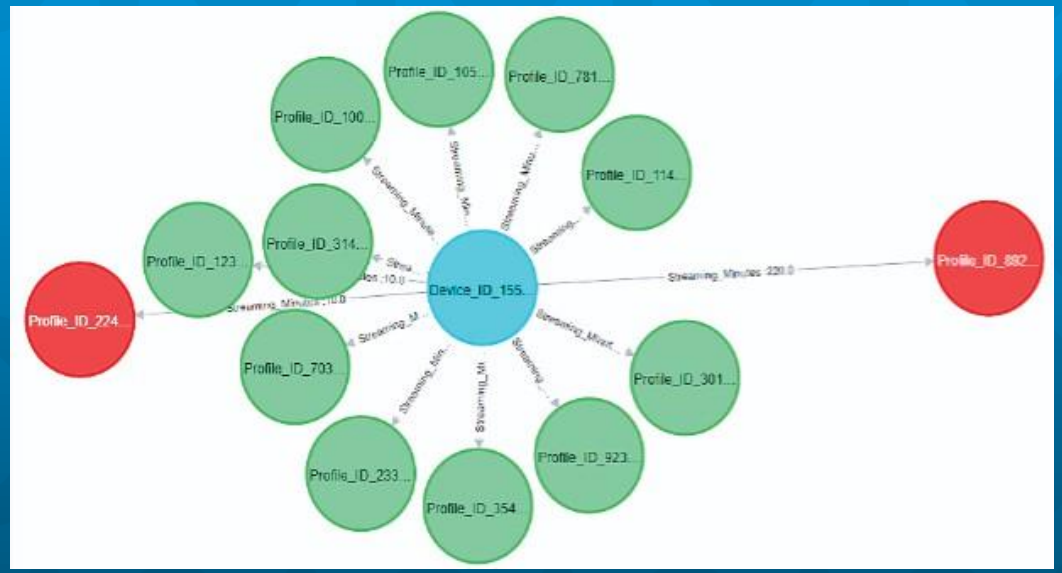
Combining network analysis techniques and model explainability methods can significantly improve piracy identification's precision while minimizing false positives.

2

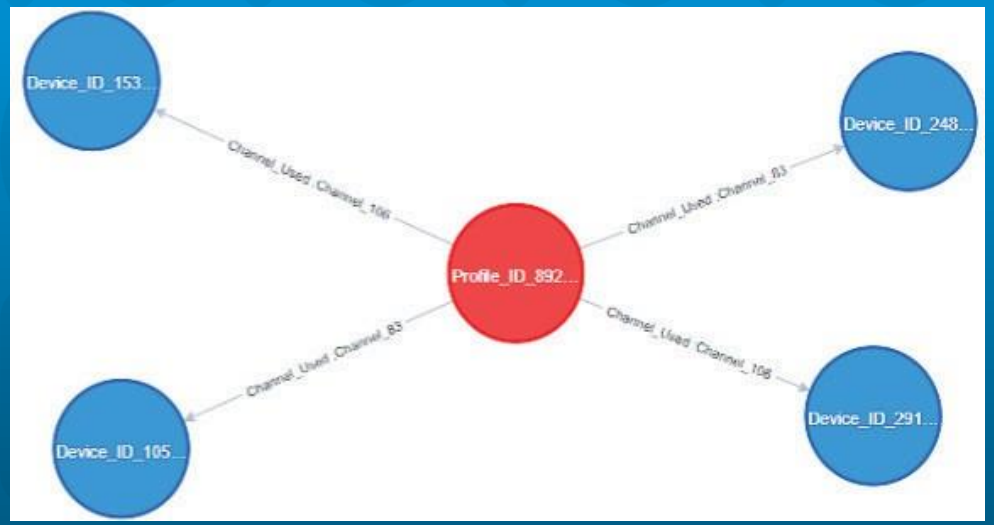
# AI (cont'd)

## NETWORK ANALYSIS

Fractal constructed dynamic graphical networks that trace extensive syndicates of users, devices, and IP addresses linked to high-risk individuals identified by the anomaly detection framework. To illustrate the impact and application of this approach, consider these examples that offer a clear perspective on its effectiveness.




Example 1: Specific device mapped to identified pirates and at-risk non-pirates.




Example 2: Particular pirate mapped to multiple devices concurrently.



fractal

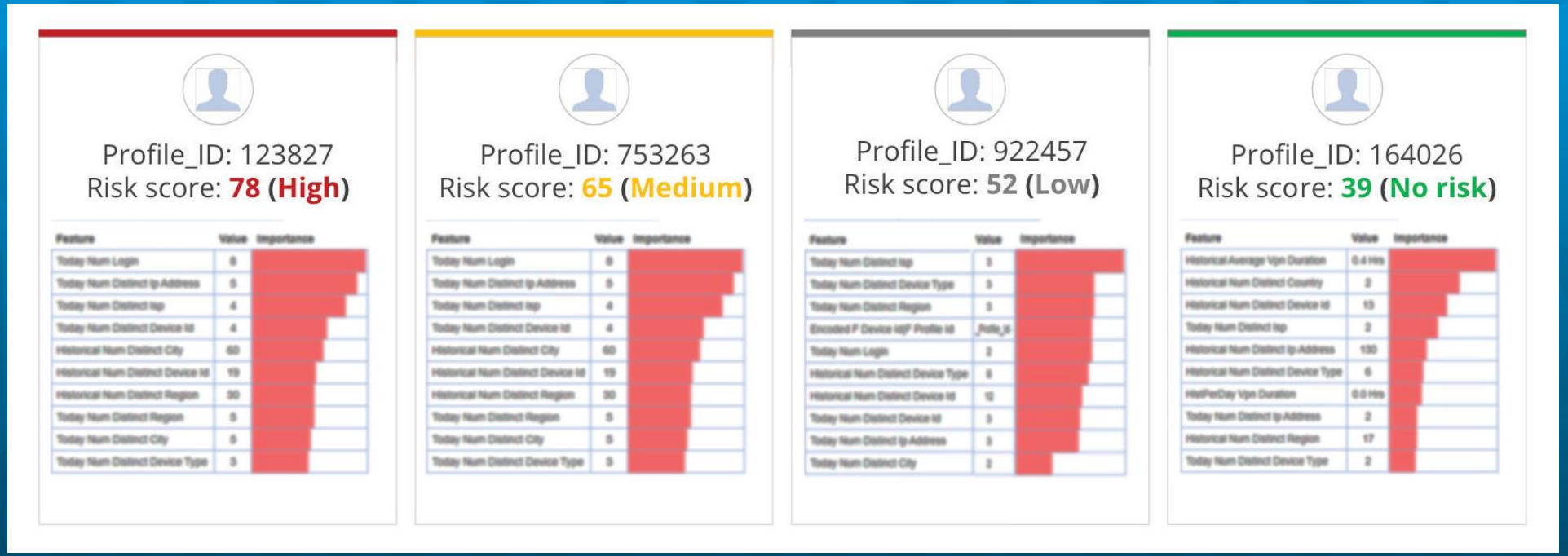
2

# AI (cont'd)

## MODEL EXPLAINABILITY

The solution prioritizes transparency by offering comprehensive visibility into the inner workings of its ML models.

By providing in-depth insights into crucial indicators and drivers, the solution allows users to validate, investigate, and take specific actions based on observed patterns. This functionality goes beyond mere risk scores, enabling users to understand the underlying factors contributing to piracy.



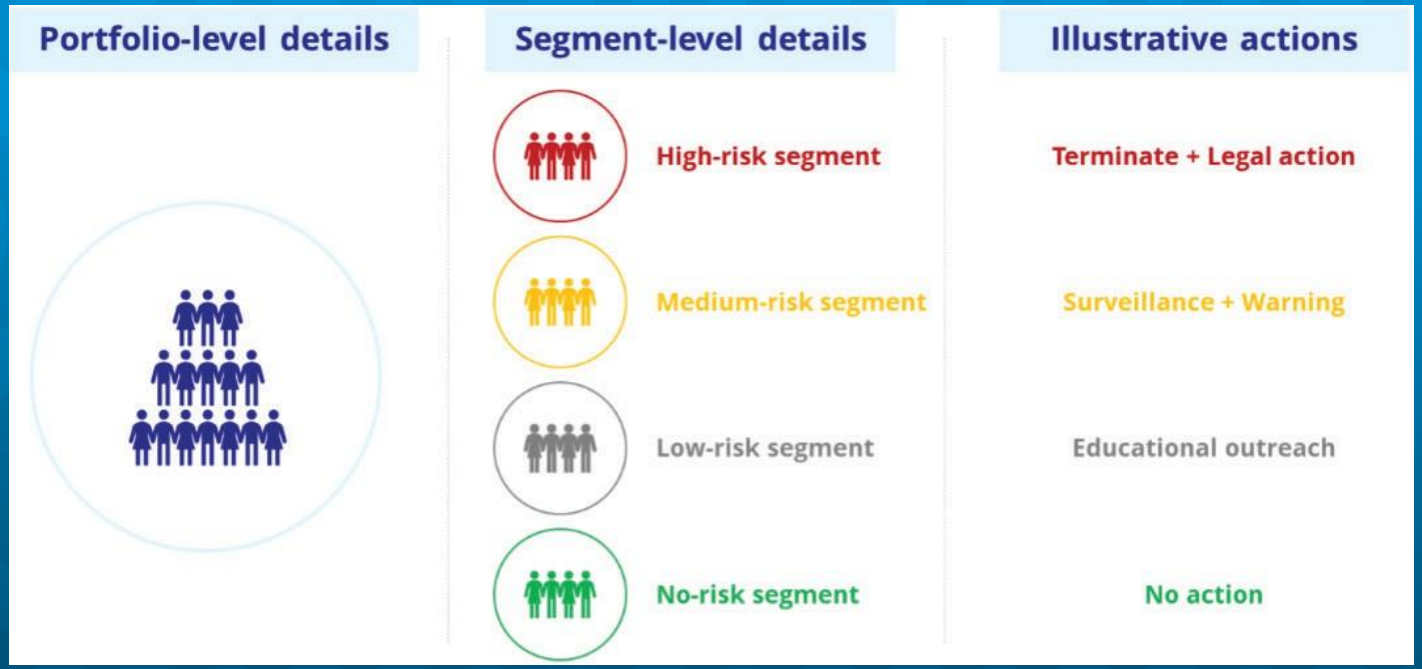



fractal

3

# Design thinking

Building upon the principles of transparency, this module places a strong emphasis on engaging human users in decision-making processes and tailoring interventions. Two critical components facilitate this approach: Risk-based segmentation and an interactive application.




## RISK-BASED SEGMENTATION

By segmenting users based on their risk levels, the solution tailors the actions and interventions for each segment.

This targeted approach addresses the challenge of personalizing interventions at the user level, while also enabling broader cohort-level interventions, which are highly effective.

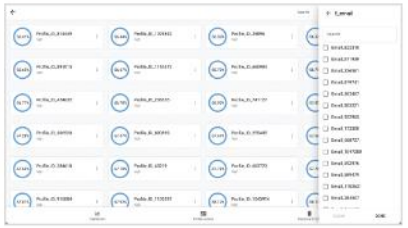
3

# Design thinking (cont'd)

## INTERACTIVE APPLICATION

To facilitate thorough investigations and incorporate human judgment in sensitive scenarios, the solution leverages Microsoft Power Apps to provide piracy analysts through a self-serve web interface.

This "human-in-the-loop" design allows analysts to delve deeper into cases and override algorithmic decisions when necessary.

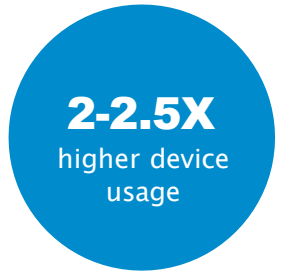
| Learn macro & micro trends | Gain real-time intelligence | Drive proactive measures | Incorporate manual overlays |
|---|---|---|---|
|  |  |  |  |
| Quick identification of key trends at, segment population, and individual customer-level. | Automatic update and re-tuning of backend algorithms as new data comes in. | Identification of geo-hotspots and network analysis of devices, IP address and users. | Manual overriding of any tags based on business knowledge and self-served investigation. |

The interface offers key functionalities essential to analysts' work, including:

- Comprehensive summary reports on piracy events
- Identification of major geographical hotspots for piracy activities
- Network analysis revealing connections between users, IP addresses, and devices involved in piracy
- In-depth driver analysis of piracy events, unraveling the underlying factors
- Trend analysis to uncover emerging piracy behaviors and patterns.


Pirates accessed VPN more often than non-pirate users


High-risk users streamed continuously for longer durations




Piracy users accessed more devices than non-pirates

## Fractal anti-content piracy solution impact

Quantifying the monetary value of piracy reduction resulting from our framework requires a comprehensive analysis involving counterfactual evaluation, quasi-experimentation, and market research. While this topic deserves a separate discussion beyond the scope of this eBook, we can still provide a high-level understanding of the business value as experienced by our client in the afore mentioned case study:

- **Reduction in revenue loss**: The framework aims to minimize revenue loss resulting from piracy by actively combating illicit activities and protecting content creators' revenue streams.
- **Safeguarding brand reputation**: By mitigating piracy, the framework helps maintain the organizations' brand reputation, fostering trust among consumers and content creators.
- **Understanding pirates**: With the capability to **process over 1 million streaming sessions daily**, our framework identified approximately 0.5–1% of sessions associated with potential pirates. Analyzing key indicators allowed us to create a data-driven profile of a typical pirate across more than 100 dimensions. To illustrate this, consider the diagram above which highlights three such dimensions: VPN usage, streaming duration, and device usage.

# Additional business impacts

## Accelerating data-to-decision time

Fractal's real-time intelligence framework significantly reduces the time required for analysts to identify, track, and investigate suspicious accounts.

With this advanced system in place, **the data-to-decision time is streamlined by an impressive 60–80%**.

Previously, these tasks would typically take weeks or even months to complete, but with our framework, they can now be accomplished in days.

## Minimizing errors

Manual tasks and laborious processes are susceptible to errors, which can lead to substantial business and legal implications.

Our framework addresses this challenge by implementing end-to-end automation, thereby significantly reducing the potential for human error.

While algorithms handle most cases, a few critical situations are escalated to anti-privacy analysts for their expertise and input.


fractal.ai

One World Trade Center Suite 76J New York, NY 10007 | +1 (646) 547 1600| info@fractal.ai

@fractalai LinkedIn.com/company/fractal-analytics