



SOLUTION BRIEF

# Outseer Risk Engine™

Powering the Decisions that Protect  
Your Business



**OUTSEER**

READ ON



## At a Glance

**Highest reported fraud detection in the Industry** Powered by Outseer Risk Engine, our solutions achieve fraud detection rates as high as 95% with intervention rates of 5%

**Genuine-to-Fraud Ratio of 1:5:1** Outseer's precision detection allows for greater protection, without sacrificing the user experience

**Continuous model enhancements** Outseer uses advanced identity science and machine-learning techniques to continuously improve its risk scoring models

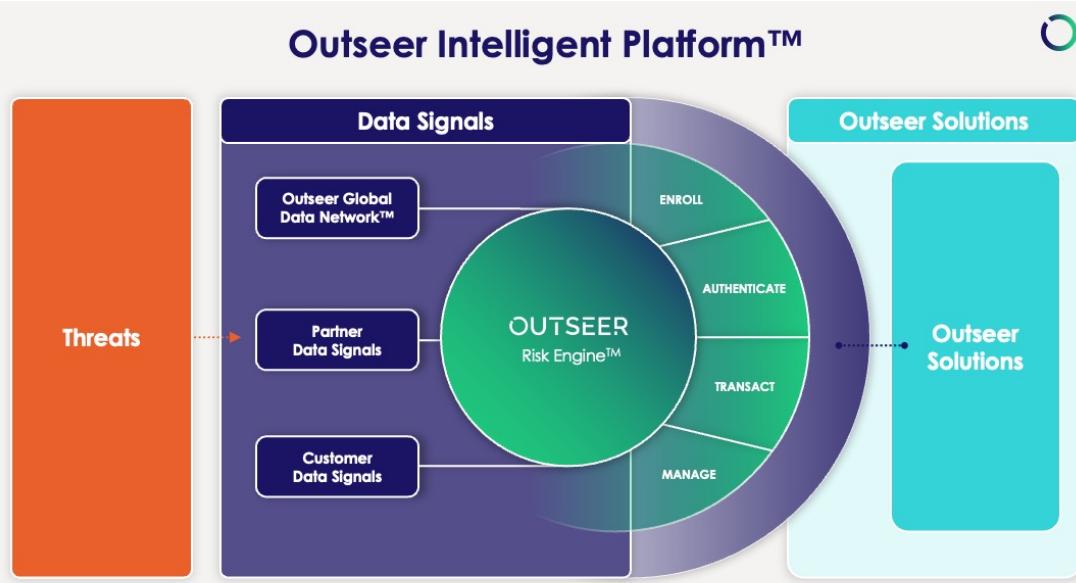
**Outseer Risk Engine predicts what others can't to deliver the best fraud detection and lowest intervention rates in the industry.**

Outseer Risk Engine assesses more than 100 different data signals to provide accurate risk evaluations to help identify and prevent fraud. By predicting what others can't, our risk engine delivers the best fraud detection and lowest intervention rates in the industry. Our data science team's fraud expertise is reflected in continuous improvements in our modeling, we deliver the right signals at the right time.

Organizations need to be prepared for these potential payment risks and challenges, and solutions need to provide security without sacrificing the user experience. By harnessing data intelligence indicators and transaction data, Outseer solutions pinpoint both authentic customers and bad actors with the highest accuracy across all digital channels. All while reducing friction for legitimate customers.

## Outseer Risk Engine: Powering Confident Decisions

The Outseer Risk Engine is the heart of our Outseer Intelligent Platform. This Platform enables our customers to provide comprehensive fraud protection across the digital journey. Point solutions are often too narrow in focus and miss the holistic view of the threats. Providing these comprehensive solutions enables our customers to have confidence they are protected and allows them to turn their focus to driving growth in their own respective businesses – higher revenues + lower fraud translates into increased profitability for our customers.



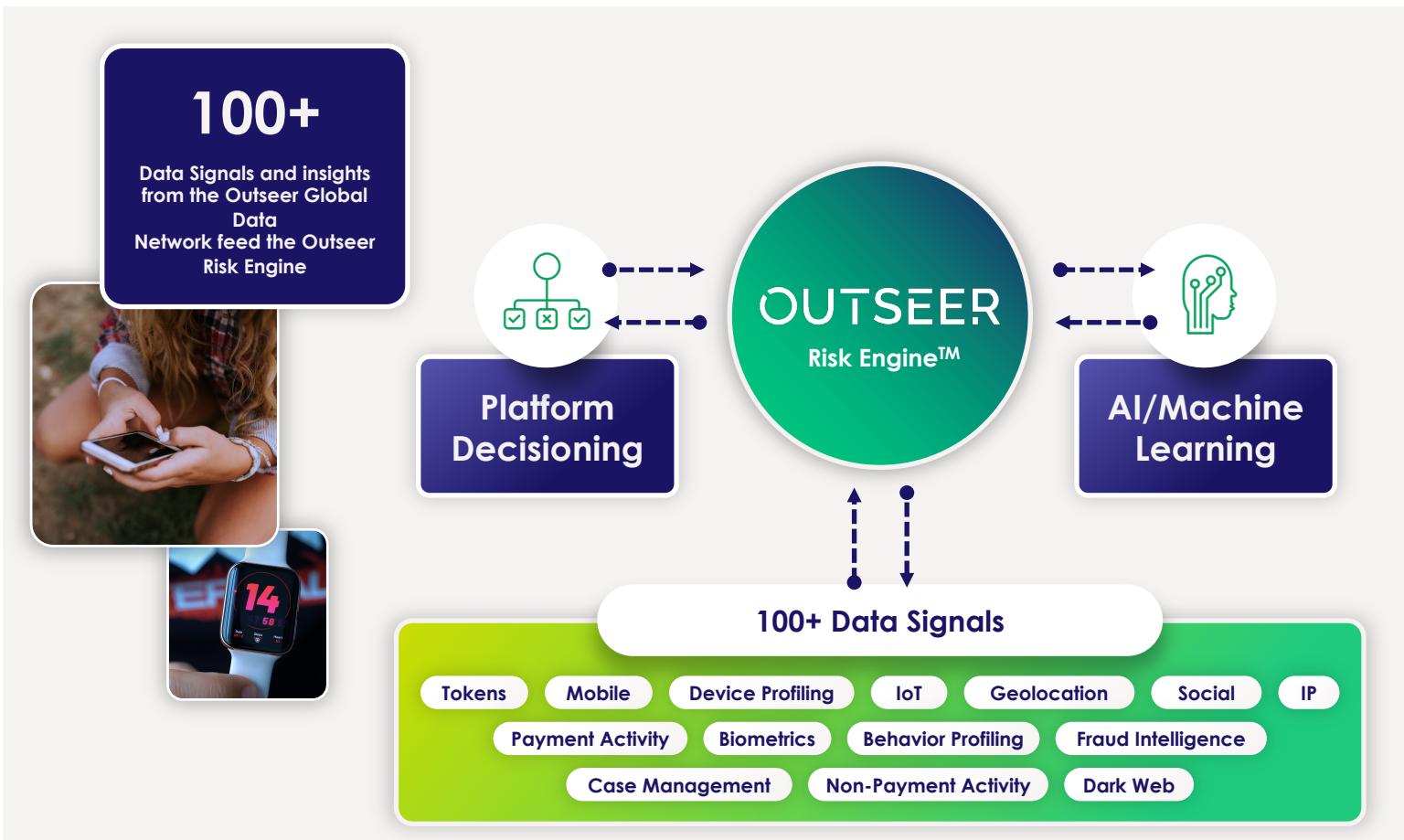
## More Detection, Less Intervention

Integrated into the Outseer solutions used by leading financial institutions, payment card issuers, and other organizations worldwide, Outseer Risk Engine reveals hidden customer truths before transactions even happen. Outseer can help you enable new business growth by providing a balance of precision detection without compromising the user experience. Better foresight will result in higher transaction approval rates, and in turn, higher revenues. Overall, the combination of lower fraud losses and more efficient operations will also result in higher growth and profitability.

Taking into consideration multiple factors including user, devices, and transactional behavior, the risk engine provides the foundation for transparent authentication—allowing the majority of transactions to pass unhindered and reserving step-up challenges for only the riskiest transactions or those identified by your policies.

## How It Works

Outseer Risk Engine analyzes a wide range of data signals associated with an activity to determine the probability of a given interaction being genuine or fraudulent. It looks at fraud and other activity patterns and uses machine learning techniques to correlate variables to score each transaction accordingly.



## **Analysis Across a Wide Array of Data Inputs**

Using a variety of sources of information, Outseer Risk Engine assigns a unique risk score to every digital transaction. The risk score and the risk policy set by an organization together determine whether a user is challenged with step-up authentication. But a risk score is only as good as the data that goes into it.

The Outseer Risk Engine further enriches the data set with a number of other important inputs received from the Outseer Global Data Network.

## **The Outseer Global Data Network**

Outseer Global Data Network is the industry's first consortium of verified fraud and transaction data. Outseer pioneered the creation of this consortium and has been leading and enhancing its value for over a decade to allow financial institutions, merchants, and other providers the ability to identify and separate legitimate transactions from fraudulent ones.

Not only does the intelligence captured within the network comes from thousands of sources, it is also composed of different types of data elements, such as: IP addresses, device fingerprints, cookies, mule account numbers, and more. For example, when a transaction or activity is attempted by a device, IP address, or payee account that appears in the Outseer Global Data network as having been associated with a fraudulent transaction, that fact will be taken into account by the risk engine.

The Outseer Global Data Network, along with the Outseer Risk Engine, underlie and power the Outseer Intelligent Platform, allowing us to deliver some of the highest fraud detection and prevention results in the industry. Outseer uses an adaptive approach. This enables you to limit interventions to only a fraction of the highest risk transactions, allowing you to maintain a seamless experience.

## **Risk Scoring: A Modern Machine Learning Approach**

After data collection, Outseer Risk Engine uses an advanced statistical approach to calculate the risk score. This method infers the conditional probability of an event being fraudulent, given the known factors or predictors. All available factors are taken into consideration, weighted according to relevance. The most predictive factors contribute more heavily to the score. The Outseer Risk Engine uses the right data, at the right time for the right use case.

This approach has significant benefits over other machine learning models used for fraud detection today. For example, artificial neural networks (ANNs) simply cannot provide information about the relative significance of various parameters. This means there's no way to understand what contributed most to the risk assessment, nor any way to visualize the contributing factors.



## **Profile Building**

In addition to its efficient score modeling, the Outseer Risk Engine takes a number of steps to meet the challenges of real-time fraud detection. This includes accumulating historical data and statistics about each user.

Through this profiling approach, the Outseer Risk Engine has the ability to instantly distinguish between established, normal user behavior and anomalous behavior that may signal fraud. The risk scores it generates enables Outseer solutions to seamlessly authenticate users in the background. As such only a fraction of users are targeted for step up authentication or other security measures. This approach leads to higher authorization rates.

## **Generating Predictors**

Profiling is used to maintain identity and behavioral facts related to end users. The Outseer Risk Engine machine learning algorithm compares a current transaction against the associated profiles to search for predictors of fraud. These predictors are data variables in the risk model assumed to correlate with fraud. They are generated when the risk engine assesses facts about the current transaction against historical data from the user's profile. The better the predictors, the more accurate the risk score will reflect the probability of fraud.

For example, the risk engine will look at variables such as the type of payment being made, if the payee account has received payment from the user in the past, the amount of the payment, etc.

## **Assigning a Preliminary Risk Score**

The Outseer Risk Engine generates a preliminary risk score for all transactions based on the probability of being genuine versus fraud, analyzing different activities and predictors that are present. If the activity falls within the established range of normal behavior for a given user, and there is no indication of malware such as a remote access Trojan, the transaction will receive a low risk score. The user is authenticated transparently. Conversely, if the behavior is atypical for the user, or there are signs indicative of malware, the risk engine will assign a higher risk score to the transaction. Depending on the score and a customers' own policies, the user may be asked to authenticate themselves to prove identity and confirm intention.

## **Risk Score Normalization**

Risk scores generated by the Outseer Risk Engine are normalized to a logarithmic scale from 0 to 1,000, using linear interpolation to convert the risk score to a common scale. This normalization provides more control over the percentage of transactions requiring intervention. In turn, it provides the ability to modulate staffing (both call center and antifraud center). It also brings predictability to the impact on score-based policies on the end user experience (intervention/challenge rates and false positives ).

## Continuous Self-Learning

Continuous Self-Learning is an important aspect of the Outseer Risk Engine.

- Case management: Outseer solutions create cases for investigation, and Outseer Risk Engine automatically modifies future risk predictions based on the investigations' results.
- Authentication results: Failed step-up authentications automatically result in higher risk scores for future transactions from the same account with similar device parameters. Likewise, successful authentications lower the risk score in future transactions.
- Chargeback data: The risk engine learns from Outseer solution data on chargebacks and automatically adapts its risk predictor weighting to identify the type of cases that it missed.

## A Core Outseer Technology

The Outseer Risk Engineer is at the core of the Outseer Intelligent Platform. Outseer Risk Engine helps provide better foresight to assess, detect and stop fraud before it occurs. This will help you achieve higher transaction approval rates, and in turn, higher revenues. And with lower fraud losses and more efficient operations, Outseer can help you drive growth and increase your profitability.

**Foundational to our offerings,  
the Outseer Risk Engine is  
unmatched in its ability to  
detect fraud.**

### Scores each transaction

Assigns an accurate risk score to each digital transaction.

### Analyzes a wide range of data inputs

Includes device profile, cross-channel activity, location, payment history, third-party risk indicators, and more.

### Supports your risk tolerance

Calibrate risk policies aligned with your business needs and broader threat environment.





# About Outseer

Outseer is on a mission to liberate the world from transactional fraud. Our market-leading payment and account monitoring solutions protect over \$200 billion in annual payments while increasing revenue and reducing customer friction for card issuing banks, payment processors, and merchants worldwide. Leveraging billions of annual transactions from more than 6,000 institutions across the globe, our identity-based science delivers the highest fraud detection rates and lowest customer intervention in the industry. See what others can't at [outseer.com](https://outseer.com).

**OUTSEER**

©2022 RSA Security LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. Published in the USA.06/21