OUTSEER
An RSA Company

Outseer Risk Engine™

Applies advanced data science to deliver fraud detection rates as high as 95% with intervention rates of 5%

Modern identity science meets predictive analytics: Outseer Risk Engine™ assesses more than 100 different data intelligence indicators 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. And because our data science team's fraud expertise is reflected in continuous improvements in our modeling, we deliver the best outcomes every time.

At a Glance

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

Genuine-to-Fraud Ratio of 2:1
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

Covid has accelerated the digital transformation of everything. Global spending on e-commerce reached $4.2T in 2020, a growth of almost 28% since the prior year[1]. Meanwhile, not a day goes by when phishing attacks, malware, and man-in-the-middle and man-in-the-Browser attacks that lead to transaction fraud don't seem to make headlines. Regardless of these threats, customers expect secure, instant, uninterrupted interactions and transactions. Financial institutions, payment card issuers, merchants, and others are challenged to meet and exceed these expectations while preventing fraud that can cost them millions.

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 identity science and global fraud and transaction data, Outseer products 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

Outseer Risk Engine is at the core of our innovative technology platform and is built for precision detection. As a foundational technology for our products, the Outseer Risk Engine assesses more than 100 different data intelligence indicators to evaluate the relative risk associated with a transaction. It then generates a risk score based on device and behavioral profiling enriched with intelligence from the Outseer Global Data Network™.

By combining rich data inputs, machine learning methods, and case management feedback, Outseer Risk Engine helps provide accurate risk evaluations to allow you to identify high risk and potentially fraudulent transactions, dramatically reducing your fraud losses.

More Detection, Less Intervention

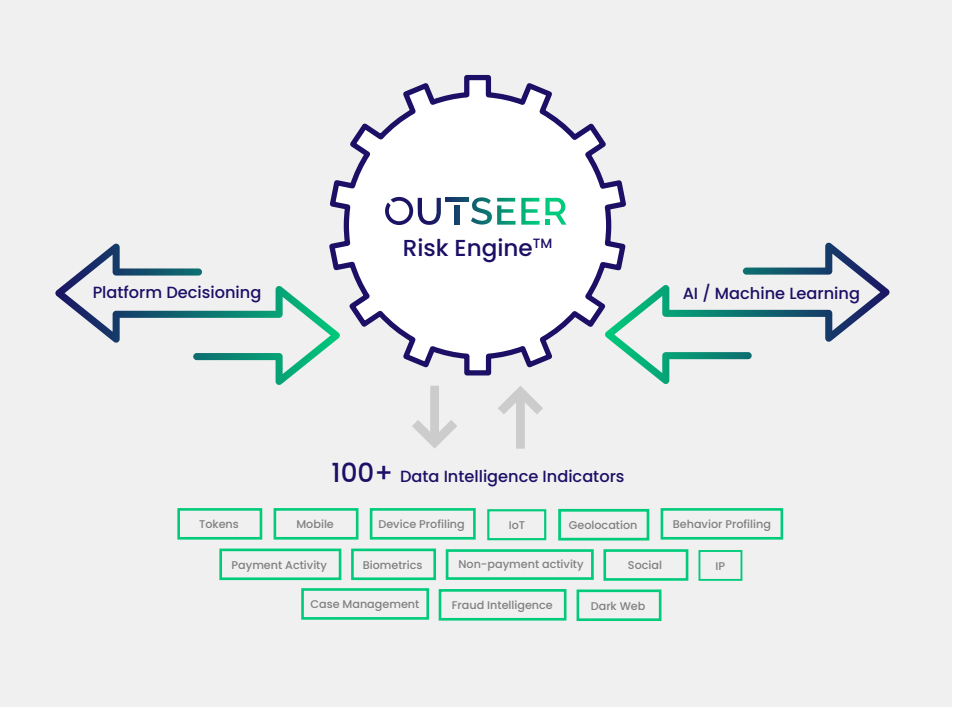
Integrated into the Outseer products used by leading financial institutions, payment card issuers, and other organizations worldwide, Outseer Risk Engine reveals hidden customer truths before transactions even happen. Outseer can help you enable new business growth by providing a balance of precision 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.

Thanks to its accurate analysis of vast amounts of login and transactional data, 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.

Taking into consideration multiple factors, including user behavior and device, the risk engine employs a self-learning statistical model alongside the Outseer policy manager that is used with Outseer 3-D Secure and Outseer Fraud Manager, to significantly reduce fraud while supporting your organization's risk tolerance and business goals.

How It Works

Outseer Risk Engine analyzes a wide range of data intelligence indicators associated with an activity to determine the probability of a given activity 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.



Rich, Diverse Data Inputs

To generate a risk score, the Outseer Risk Engine analyzes a diverse set of data points from an array of sources for every user activity, including:

- User, login and payment usage information and changes
- Device details, including IP address, browser characteristics, screen resolution, etc.
- Indicators of malware or malware-related activities
- Mobile device identifiers, geolocation, WIFI MAC address, signs of jailbreak or emulation
- Third-party risk indicators from other anti-fraud tools and customers' internal intelligence
- Case management feedback, authentication results, and chargeback data

Our risk engine also recognizes the channel (e.g., online, mobile, call center, branch) from which the activity is generated and adjusts the risk model accordingly. Risk scoring of transactions from the mobile channel, for example, will include mobile-specific device parameters and a mobile-optimized scoring algorithm will be used. Outseer Risk Engine further enriches the data set with a number of other important inputs received from the The Outseer Global Data Network.

The Outseer Global Data Network

The Outseer Global Data Network is the industry's first global consortium of reported fraud and transaction data. With thousands of contributors across 150 countries, our globally shared, cross-industry transactions and identity intelligence network informs smarter risk decisions.

100+

Data Intelligence Indicators and insights from the Outseer Global Data Network feed the Outseer Risk Engine

When a member of the network marks an activity as "Confirmed Fraud" / "Confirmed Genuine" in the case management application the associated data elements are shared across the network. When an activity is attempted and includes one of the elements from the Global Data Network the risk is automatically adjusted.

Our consortium shares data from Outseer customers spanning numerous industries across 150 countries. In service for more than a decade, our network has thousands of contributors worldwide, including financial institutions, payment card issuers, healthcare companies, internet service providers (ISPs), technology firms, as well as government and law enforcement agencies.

Not only does the intelligence captured within the network itself come from thousands of sources, it's also composed of many 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.

Risk Scoring

A Modern Machine Learning Approach

After data collection, Outseer Risk Engine uses an advanced statistical approach to calculating 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.

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.

That's a problem for ANNs as well as their more advanced counterparts, deep neural nets, or DNNs. While DNNs shine when it comes to working with huge data sets, ANNs have been shown to produce inferior results for small sample sizes. Also, the proprietary machine learning algorithm implemented in Outseer Risk Engine handles missing data well, and is computationally efficient. It also helps you understand what factors contributed most to risk scores.

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 products to authenticate users in the background while targeting only a fraction of users for step-up challenges or other security measures.

For example, the risk engine profiles each user's device, which captures different data elements. For online transactions, this might include:

- HTTP headers, operating system versions, and patch levels
- Browser type and version, software versions, display parameters (size and color depth), languages, time zone and more
- IP address, extracted IP geolocation details, and additional information on the ISP, IP owner, connection type, and so on.

For mobile-initiated transactions and interactions, the device profile contains additional identifiers. Also, the geolocation of smart mobile devices is not only based on the IP, but also on information that can be collected directly from the mobile device itself.

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 user profile to search for predictors of fraud. Generally speaking, 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 characteristic of the user's 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, given the predictors that are present. All data variables are taken into account in this preliminary score, with each one weighted based on relevance. For example, the risk engine will compare predictors against general population behavior as well as an individual user's past behavior. This action helps identify patterns of legitimate activity and ultimately help reduce false positives.

If the activity falls within the established range of normal behavior for the 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 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 kind of normalization gives you more control over the percentage of transactions requiring intervention. In turn, this gives you 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

- Case management: Outseer Fraud Manager and Outseer 3-D Secure 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 3-D Secure data on chargebacks and automatically adapts its risk predictor weighting to identify the type of cases that it missed.
- Chargeback data: The risk engine learns from Outseer 3-D Secure 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 Engine is a central component of Outseer products. Outseer Fraud Manager and Outseer 3-D Secure are significantly enhanced by the Outseer Risk Engine and its precision detection capabilities to assess and protect digital transactions. By seeing what others can't, the 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.

[1]"Global Ecommerce Update 2021." eMarketer, Jan. 2021

About Outseer

Outseer empowers the digital economy to grow by authenticating billions of transactions annually. Our payment and account monitoring solutions increase revenue and reduce customer friction for card issuing banks, payment processors, and merchants worldwide.

Leveraging 20 billion annual transactions from 6,000 global institutions contributing to the Outseer Data Network, 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