

Add a powerful layer of defense to your digital security measures

Combine LexisNexis® Behavioral Biometrics with digital identity intelligence to decrease fraud risk without disrupting user experience.



Frictionless security against fraud

Today's fraudsters are experts at avoiding detection. They deploy complex, multi-vector attacks and continually develop new strategies to bypass controls and exploit vulnerabilities.

Differentiating between legitimate citizens and high-risk users in near real time is difficult. And adding more security measures often produces unwanted friction for citizens.

The best proven approach is a layered defense to inform better risk decisions. LexisNexis® Behavioral Biometrics is an innovative fraud detection technology that adds an entirely new dimension to risk assessment without adversely affecting the user experience. When combined with digital identity intelligence, it offers unmatched protection.

Tracking how you type, swipe, scroll and click

Unlike physical biometrics, which involve innate human characteristics such as fingerprints or iris patterns, Behavioral Biometrics relates to measurable patterns in human activity. This activity can be markedly different across different groups of users and can prove an effective way of differentiating between trusted and high-risk behavior, as well as human and non-human traffic. Behavior that can be analyzed includes:



KEYBOARD BEHAVIOR

How is a keyboard used? What is the typing speed? Were any special keys pressed? Were any keyboard shortcuts taken?



MOUSE BEHAVIOR

How does the mouse move around the page? Does it ever go off page?



PHONE BEHAVIOR

Is the phone being held in landscape or portrait position? What is the rotation and angle of the phone?



TOUCHSCREEN BEHAVIOR

How is the touchscreen used? What is the swipe speed? What is the shape of the finger/ pointer? How much pressure is being exerted?

Behavioral Biometrics is able to support risk-based decisioning because it can help:

- Separate bots from human traffic
- Identify “good” user profiles
- Reliably profile fraudsters
- Detect suspicious, anomalous behaviors

Imperceptible to citizens

Traditional physical biometrics, like fingerprints or iris scanning, require special hardware for authentication. Behavioral traits can be captured in the background. The data collection is imperceptible to users, so they don't feel an increased interrogation of their transaction. Instead, you get powerful security controls to continuously assess device interactions, without imposing any of the bothersome roadblocks that typically accompany security tests.

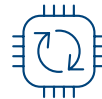
Easy deployment

LexisNexis Behavioral Biometrics can be layered with LexisNexis® ThreatMetrix® digital identity intelligence to make more reliable fraud and risk decisions.



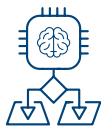
FULLY INTEGRATED

Compatible with ThreatMetrix and accessed via the existing portal



SEAMLESS PERFORMANCE

No negative impact on functionality or latency of ThreatMetrix



WHITE-BOX APPROACH

Exposes the data to rules, providing scores and associated reason codes for a variety of different risk factors



PRIVACY-BY-DESIGN

No password or PII data is captured, maintaining the privacy and security of all end-users

Powerful security controls to continuously assess device interactions, without imposing any of the bothersome roadblocks that typically accompany security tests.

A superior safeguard

The threat landscape is continually changing. Agencies must keep up with new fraud tactics. It's a constant game of cat-and-mouse against cunning adversaries. At the same time, security measures that make online interactions more challenging could lead to frustrated citizens.

When you combine Behavioral Biometrics with the digital identity intelligence from ThreatMetrix, you're adding a robust layer of defense to a market-leading fraud and identity solution. The result is transformative fraud-detection technology that protects your business and gives trusted people the positive experience they deserve.

For more information, call 866.528.0780 or visit
risk.lexisnexis.com/government/public-cio-and-it-programs



Government

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our government solutions assist law enforcement and government agencies with deriving insight from complex data sets, improving operational efficiencies, making timely and informed decisions to enhance investigations, increasing program integrity and discovering and recovering revenue.

About ThreatMetrix

ThreatMetrix®, a LexisNexis® Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion tokenized digital identities, LexID® Digital delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time.