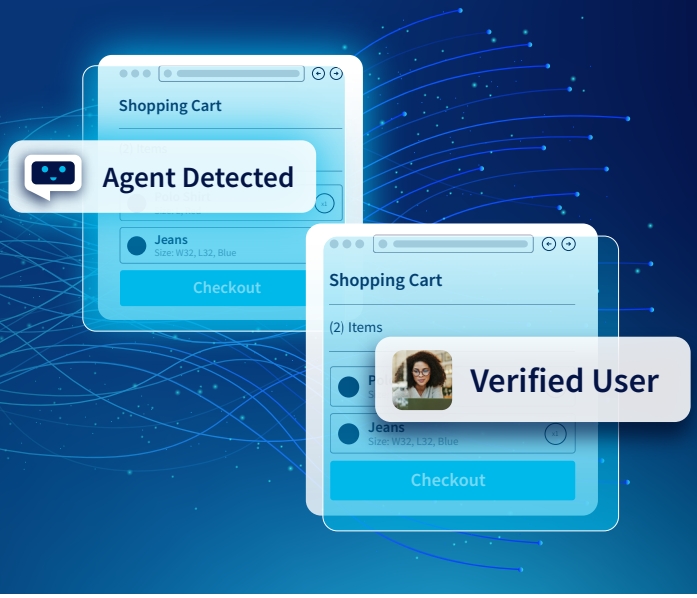
LexisNexis®
RISK SOLUTIONS



Identify each actor - human or AI

The missing trust layer for agentic commerce

As AI agents increasingly browse, research and transact on behalf of users, organizations face a new challenge: understanding not only who is behind a transaction, but whether an AI agent is involved, what authority it has and whether its actions can be trusted.

While most organizations can identify trusted customers and detect malicious bots, few can reliably identify AI agents, understand their authority or differentiate trusted agent activity from potential abuse. This creates a new trust gap where businesses lack visibility into agent involvement, behavior, intent and legitimacy.

450% increase in agentic commerce transactions[1]

900M+ weekly active ChatGPT users[2]

68% of organizations cannot clearly distinguish AI-agent actions from human activity[3]



To confidently **enable the next generation** of digital experiences, organizations need a solution that can distinguish humans, malicious bots and AI agents, while **providing the context needed** to make more **trusted risk decisions.**

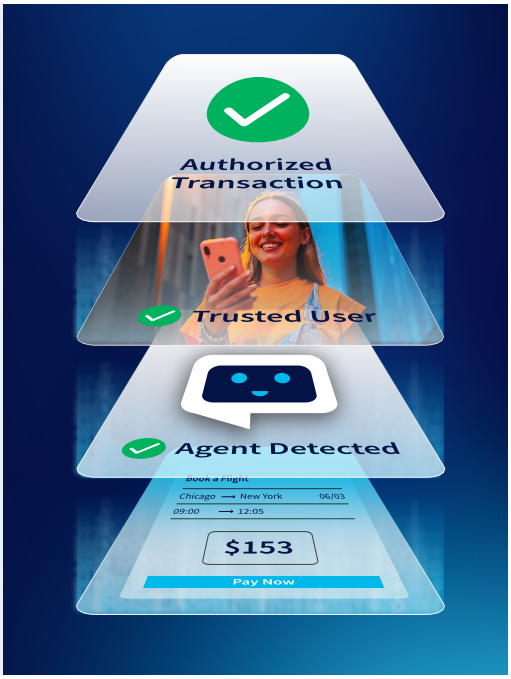
Introducing agentic intelligence from LexisNexis® Risk Solutions

A new intelligence layer that helps identify, understand and assess AI agent risk across digital interactions.

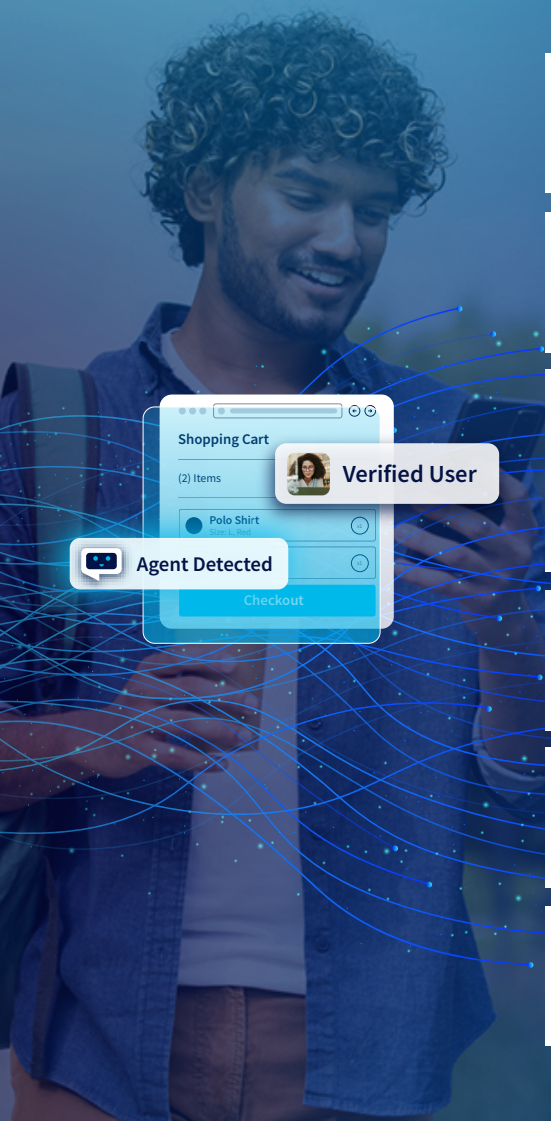
Leveraging digital risk intelligence from LexisNexis® ThreatMetrix® and LexisNexis® BehavioSec®, our solution provides visibility into AI-agent driven activity and the context needed to evaluate whether interactions are expected, trusted or require additional authentication and authorization.

Working seamlessly across evolving AI ecosystems and interaction protocols, organizations can identify when an AI agent is involved, better understand its relationship to the customer and incorporate those insights into existing risk decisions.

The result is greater trust, transparency and control in a growing agent-driven world.



Build Trust Across AI Agent Interactions



Gain Visibility into Agent Activity
Detect AI agent interactions and uncover signals associated with agent-driven behavior.

Understand Who, or What, Is Acting
Distinguish between humans, malicious bots and AI agents using robust digital risk intelligence.

Connect the Customer to the Interaction
Associate agent activity to the customer behind it with digital identity and network intelligence. Execute out of band authentication to help establish trusted relationships between customers, agents and interactions.

Strengthen Risk and Trust Decisions
Incorporate agentic intelligence into existing risk-based workflows to support more informed decision-making.

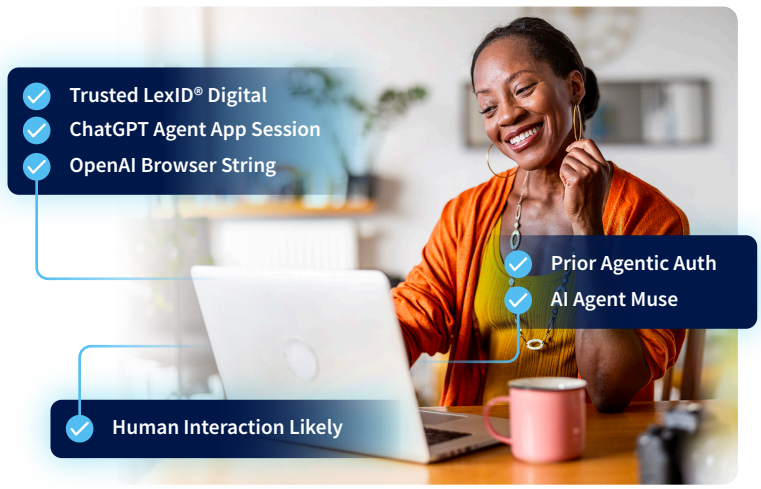
Enable Trusted AI Experiences
Balance innovation and customer convenience with the controls needed to manage risk and reduce uncertainty.

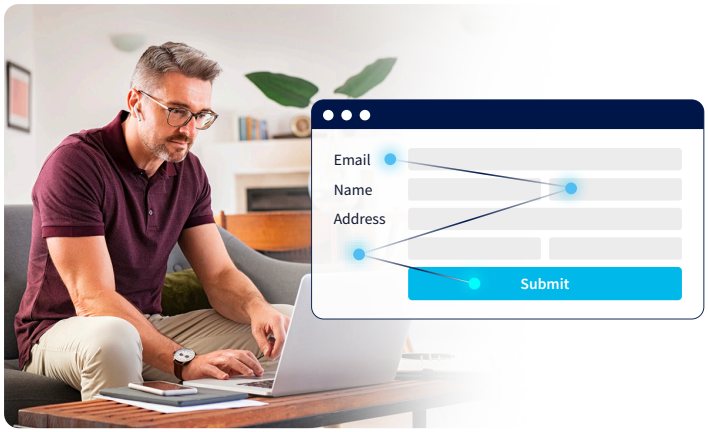
Prepare for the Future of Commerce
Build a foundation for governing trusted agent relationships and managing agent-mediated interactions as adoption grows.

How it Works:
Turning Agent Visibility into Action

Identify AI Agents

Browser, device, operating system and network intelligence can reveal recognized AI agent signatures and other indicators of agent-driven activity. Applications embedded within ChatGPT, Claude and similar AI platforms can also be profiled to establish digital identity context through browser characteristics, domains, application signals and other relevant indicators.





Establish Digital Risk Context

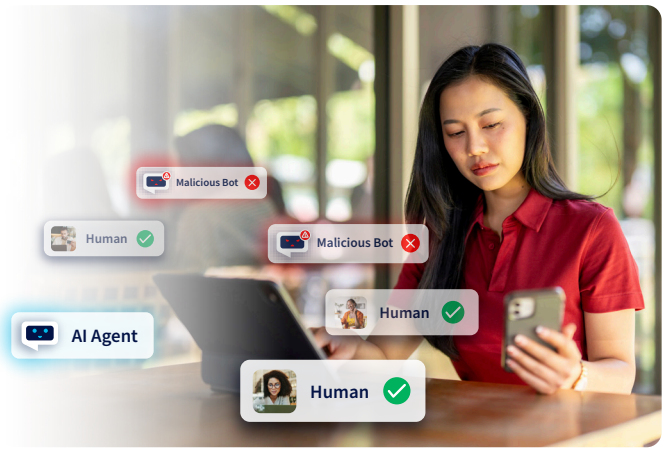
By combining device, digital identity, behavioral and network intelligence, organizations can better understand the relationship between the user, device and AI agent involved in an interaction.

Historical activity, behavioral patterns and contextual signals across LexisNexis® Digital Identity Network® help provide a more complete view of trust and risk.

Distinguish Humans, Malicious Bots and AI Agents

Technical indicators and behavioral insights help classify activity as human, malicious bot or AI agent. Rather than treating all automation the same, organizations gain the context needed to apply controls appropriate to their risk tolerance.

Trust Tags can establish persistent relationships between users, devices and agent interactions, helping organizations recognize and assess future activity with greater confidence.



Where Agentic Intelligence Adds Value

Agent-Assisted Commerce

Understand when AI agents are researching, comparing, browsing or purchasing on behalf of consumers.

Account Opening and Onboarding

Identify agent participation within application and registration journeys.

Authentication and Access Management

Determine whether an AI agent is acting with legitimate authority during account access and verification.

Banking and Payments

Incorporate agentic intelligence into login, payment, account management and digital engagement workflows.

Customer Service and Self-Service Experiences

Understand when AI agents are acting on behalf of customers to perform tasks such as scheduling returns, managing accounts or interacting with online services.

Future Agent-to-Agent Interactions

Prepare for a world where autonomous systems increasingly interact and transact with one another.

Built for the Future. Ready for Today.

LexisNexis® Risk Solutions helps organizations identify, understand and manage AI-agent activity using proven digital risk intelligence embedded within existing risk-based workflows.

This enables organizations to begin addressing the trust challenges of agentic commerce now, while building the foundation for the future of growing AI agent interactions.



Contact your account representative for additional information or questions.

To learn more about ThreatMetrix® and BehavioSec®, visit our website:

risk.lexisnexis.com

LexisNexis® RISK SOLUTIONS

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions products and services provide information, analytics, risk indicators, and decision-support tools to assist customers in evaluating digital interactions. No solution can identify, classify, authenticate, or detect all users, devices, bots, or AI agents in every circumstance, and results may vary. Customers remain solely responsible for their compliance obligations and for all business, authentication, risk, and operational decisions. References to future capabilities, industry trends, third-party products, or anticipated use cases are provided for informational purposes only and do not constitute a commitment, representation, warranty, or guarantee of future functionality or outcomes. References to third-party trademarks are for identification purposes only and do not imply endorsement or affiliation. Market and industry statistics are based on sources believed reliable but are not warranted by LexisNexis Risk Solutions.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc., registered in the U.S. or other countries. ThreatMetrix is a registered trademark of ThreatMetrix, Inc., registered in the U.S. or other countries. BehavioSec is a registered trademark of Behaviometrics AB. Other products or services may be trademarks or registered trademarks of their respective companies. Copyright © 2026 LexisNexis Risk Solutions.

[1] LexisNexis® Risk Solutions Cybercrime Report 2026
[2] OpenAI, February 2026
[3] Identity and Access Gaps in the Age of Autonomous AI, Cloud Security Alliance and Aembit, 2026