LexisNexis® RISK SOLUTIONS | Health Care

ThreatMetrix® for Healthcare

Improve Cybersecurity Defenses and Help Ensure User Identity with Shared Threat Intelligence

By the end of 2020, over 50 million patients were able to view their clinical notes through a patient portal, an increase in patient data access of more than 10 million since the prior year.* While use of devices such as laptops, tablets and mobile phones to perform tasks such as scheduling appointments, viewing lab results, filing claims and accessing telemedicine care has increased, so have concerns regarding healthcare data security and privacy.

The need to maximize security and maintain a positive user experience has driven the development of a multi-layered approach to ensure authentication of a user's digital identity. LexisNexis® ThreatMetrix® for Healthcare leverages device assessment capabilities paired with behavioral biometrics and a sophisticated contributory network to ensure that the person and the device being used to facilitate a transaction have not been compromised.

Security and User Friction are a Balancing Act

Increased access to healthcare data and the use of mobile devices have increased security risks, creating challenges:

- Users are demanding better security and privacy
- Frequent and obtrusive step-up challenges frustrate users
- Cybercriminals are sharing data with each other
- Traditional, static authentication methods are no match for sophisticated cybercriminals
- Costs of cybercrime encompass fines, reputation damage and lost profits

ThreatMetrix can transform the way your healthcare organization secures transactions and user access from cybercrime without causing unnecessary frustration.

Help prevent cybercrime while providing a seamless, personalized user experience

It's important to ensure that users are who they say they are before they are permitted to access sensitive data or perform high-risk transactions such as requesting healthcare records protected by HIPAA outside of the firewall. Data security measures, however, should verify and authenticate users without frustrating them.

ThreatMetrix helps healthcare organizations understand the digital DNA of users to spot suspicious behavior. It helps to assess the risk of the digital identity attributes of every person requesting

access to healthcare information. By combining the integral components of LexID® unique IDs and LexisNexis Digital Identity Network® insights, ThreatMetrix delivers powerful risk decisioning that combines robust digital identity intelligence with relevant transaction insights.

ThreatMetrix harnesses intelligence related to devices, locations, identities and past behaviors across one of the largest global digital networks to distinguish between trusted and fraudulent behavior. It connects online and offline identities across all touchpoints and helps protect the integrity of patient identity by proactively detecting the presence of high-risk or anomalous digital behavior that can signal a potential cybersecurity breach before a transaction can be processed.

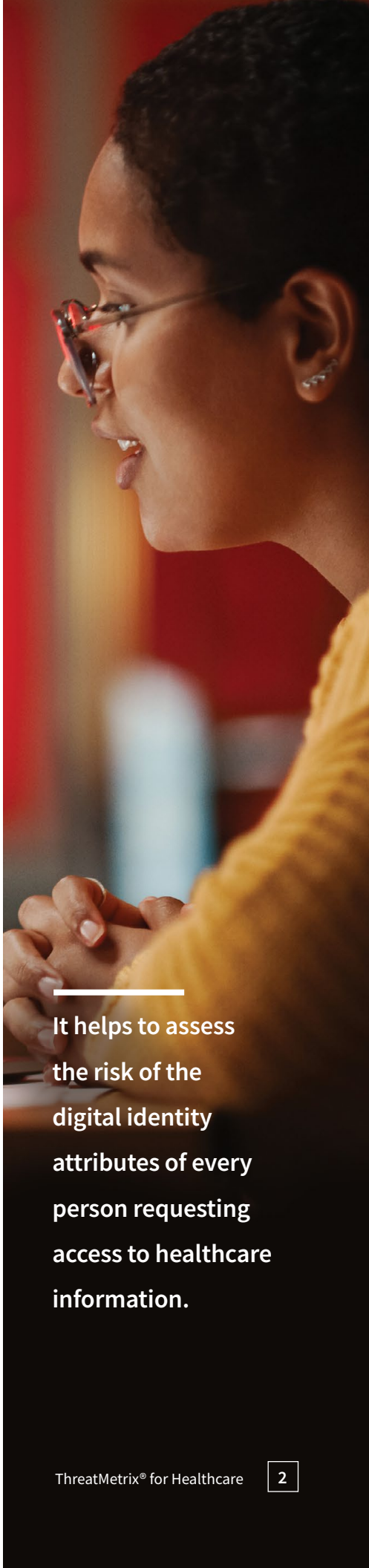
LexisNexis® Risk Solutions provides implementation and optimization of best-in-class identity and authentication solutions.

Differentiate between trusted users and cyberthreats

The best way to tackle cybercrime is to harness the power of data from a shared network. The ThreatMetrix platform collects and processes shared intelligence from millions of consumer interactions including new account applications and logins. Using this information, LexisNexis® Risk Solutions creates a unique digital identity for each user by analyzing the connections between devices, locations and anonymized personal information.

Behavior that deviates from this trusted digital identity can be accurately identified, alerting systems to a potential cybersecurity breach. Suspicious behavior can be detected and rejected before a transaction is processed.

Powered by shared intelligence from the ThreatMetrix Digital Identity Network, ThreatMetrix uses a unique, anonymous, alphanumeric identifier that transforms digital authentication and cyberattack prevention. It provides an innovative and reliable method to unite online attributes enabling organizations to help establish the true digital identity of their users. This enables organizations to recognize returning users behind multiple devices, email addresses, physical addresses and account names.



It helps to assess the risk of the digital identity attributes of every person requesting access to healthcare information.

End-to-end decisioning capabilities

Balancing the quality of a patient's online experience with effective identity verification is a complicated endeavor. The ThreatMetrix decision platform supports both objectives through four key functions:

Behavioral Analytics

Helps healthcare organizations understand user behavior, while detecting potential cyberattacks and reducing false positives.

Integration and Orchestration

Includes complementary LexisNexis Risk Solutions identity authentication solutions that allow a highly configurable, multi-layered identity assessment workflow.

Machine Learning

Integrates seamlessly with business rules and Smart Rules, which brings an element of personalization into risk decisioning. Your organization has the ability to incorporate a machine-learning model that can quickly adapt to changing behavior.

Case Management

Enables continuous optimization of authentication and trust decisions with visualization, data correlation and exception handling for complex caseloads. It integrates analyst feedback and third-party systems through an API for additional feedback, improving future trust decisions.

To optimize your user identity strategy, call 866.396.7703 or visit risk.lexisnexis.com/contact-us.

LexisNexis® RISK SOLUTIONS | Health Care

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 healthcare solutions combine proprietary analytics, data science and technology with the industry's leading sources of provider, member, claims and public records information to deliver insights that improve cost savings, health outcomes, data quality and compliance. For more information, please visit risk.lexisnexis.com/healthcare.

*ONC Final Rules Sparked 10% Patient Data Access Increase in 2020, Patient Engagement HIT, Sara Heath