LexisNexis® RISK SOLUTIONS

Government

ThreatMetrix® for Government

It takes a global digital network to fight a global cyber criminal network

Differentiate between trusted users and cyber threat users in real time

When government agencies make the shift from in-line to online or digital services, they increase ease and efficiency of access, which is a great benefit for citizens and agencies alike. The citizens being served should expect a seamless, frictionless experience across all channels in addition to secure, instant access.

At the same time however, cybercrime is increasing. Cyber criminals are becoming more sophisticated in their usage of stolen identity information to divert government payments and scripted bot attacks against online systems.

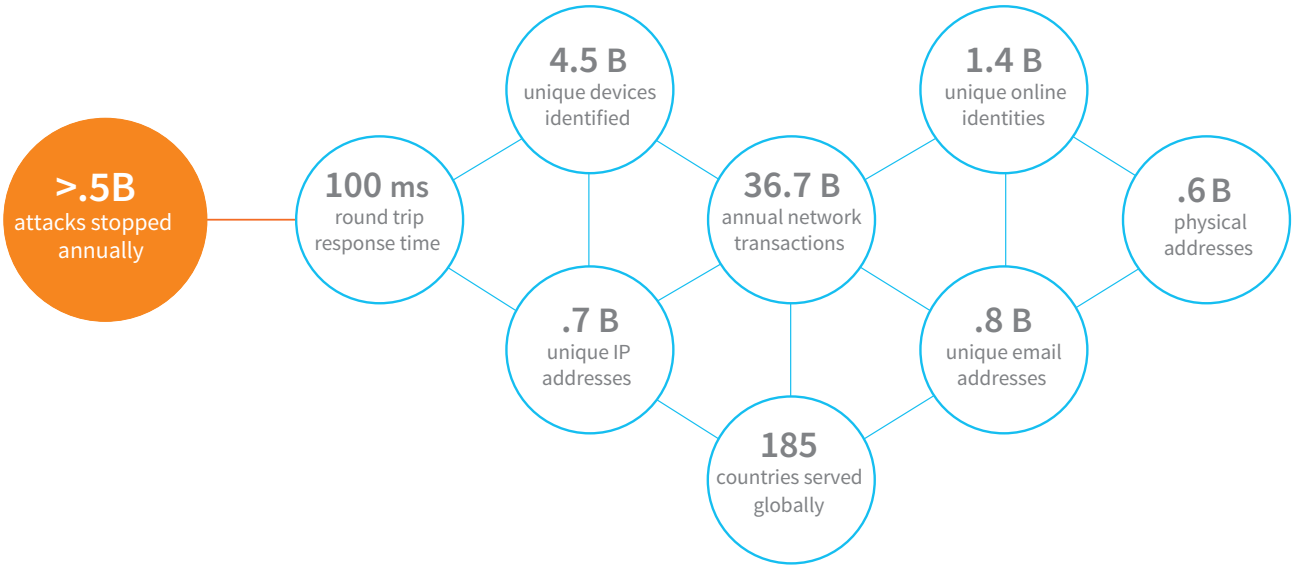
Before granting account access or facilitating any high-risk transaction, government agencies must authenticate the citizen's identity and assess the overall risk of the transaction, both from a digital and physical identity perspective. With the frequency of data breaches, stolen data is so readily available that static identity assessments that rely on identity data alone increasingly offer insufficient protection against fraud. Instead, real-time automated digital authentication must be able to differentiate a trusted citizen from a cyber criminal, beginning with account origination to every visit and transaction that follows.

ThreatMetrix® for Government is the next generation of digital identity assessment. ThreatMetrix provides government with the ability to harness intelligence related to devices, locations, identities and past behaviors across one of the largest crowdsourced global digital networks in order to distinguish between trusted and fraudulent behavior. It connects online and offline identities so you know with whom you're interacting at the time of a transaction across all touchpoints. It helps protect the integrity of government services by proactively detecting the presence of high-risk or anomalous digital behavior that signal potential fraud before access is allowed or a transaction can be processed. And it provides a holistic, singular view of your citizens, helping to prevent operational silos.

> ThreatMetrix for Government can revolutionize the way your agency recognizes online customers, accepts transactions and secures your agency from cybercrime without causing unnecessary frustration for trusted citizens.

Benefit from the strength of the Network

The best way to tackle complex, global cybercrime is using the power of a global shared network. The ThreatMetrix® for Government Digital Identity Network® collects and processes global shared intelligence from millions of daily consumer interactions including logins, payments and new account applications. Using this information, LexisNexis Risk Solutions creates a unique digital identity for each user by analyzing the myriad connections between devices, locations and anonymized personal information. Behavior that deviates from this trusted digital identity can be accurately identified in real time, alerting agencies to potential fraud. Suspicious behavior can be detected and flagged for manual review or rejection before a transaction is processed.



The contributory database in the ThreatMetrix Digital Identity Network contains 1.4 billion unique online digital identities from 4.5 billion devices in 185 countries. Contributors are typically financial institutions, e-commerce companies and media businesses. The Network analyzes over 100 million transactions a day or 36.7 billion transactions a year across 35,000 websites from over 5,000 global companies, giving agencies the exponential strength of the entire Network.

Establish the true digital identity of your citizens

Powered by global shared intelligence from the ThreatMetrix Digital Identity Network, LexID® Digital is a unique, anonymous, alphanumeric customer identifier that revolutionizes digital authentication and fraud prevention. It provides an innovative and reliable method to unite online and offline attributes in real time enabling organizations to help establish the true digital identity of their customers. The ThreatMetrix Digital Identity Network outputs the LexID Digital identifier for each citizen (currently over 1.4 billion) by analyzing the innumerable connections between devices, locations, past behaviors and anonymized personal information. This enables agencies to pro-actively recognize the same returning user behind multiple devices, email addresses, physical addresses and account names.

Every LexID Digital is comprised of three components that operationalize intelligence from the Network:

1. **Unique Digital Identifier**
   A fully anonymized and unique identifier based on anonymized global shared intelligence from the Network. This Identifier finds transactions that are related (based on associations and linkages) not just from the organization's own data but from the entire global Network.
2. **Visualization Graph**
   This interactive interface allows government to operationalize LexID Digital by showing all devices, credentials, threats and behavioral attributes related to an identity. It enables a real-time risk assessment for each persona and online transaction, and one that gets smarter with every transaction. This gives agencies a unique, global view without compromising privacy or anonymity of other organizations within the network.
3. **Confidence Score**
   This pertains to the authenticity of a user. The score gives the likelihood of a current event being associated with an identity known to the ThreatMetrix Digital Identity Network. ThreatMetrix for Government machine learning algorithm is then used to match event-specific entities with the entities linked to a digital Identifier within the Network. This then creates a confidence score for the transacting user.

With ThreatMetrix for Government, agencies can better understand the identities of their connecting citizens and determine whether they are trustworthy. Intelligence from the global Network helps accurately recognize the same returning user behind multiple devices, email addresses, physical addresses and account names. And when devices or actions differ from prior behavior by a trusted digital identity, ThreatMetrix for Government alerts you to possible fraud in real time and flags the transaction for manual review or rejection before it is processed.

End-to-end decisioning capabilities

The ThreatMetrix Dynamic Decision Platform enables organizations to leverage the best intelligence from the ThreatMetrix Digital Identity Network to make real-time digital decisions.

It optimizes the online experience by combining frictionless, market-leading risk-based authentication (RBA) with low-friction strong customer authentication (SCA) strategies. Authentication requirements are tailored to the user, based on the type of transaction they're doing, the device they're using and their associated level of risk.

Trusted citizens have a streamlined online experience with fewer step-up authentication interventions; only genuinely high-risk transactions are challenged. Transactions flagged as high-risk or requiring additional research can be routed to the appropriate authentication or identity verification service.

The ThreatMetrix Dynamic Decision Platform encompasses four key functions that provide the depth and flexibility to tailor policies to individual user behavior:

1. **Behavioral Analytics (Smart Rules)**
   Helps government agencies understand genuine user behavior, in all its rich diversity, while detecting potential fraud and reducing false positives. Smart Rules bring an element of personalization into risk decisioning.
2. **Machine Learning (Smart Learning)**
   Integrates seamlessly with business rules and Smart Rules, helping government agencies easily incorporate the machine-learning model that can quickly adapt to changing behavior.
3. **Integration and Orchestration**
   Extends the capabilities of the core ThreatMetrix platform to include a wide array of other LexisNexis Risk Solutions identity authentication offerings. This allows a highly configurable, multi-layered identity assessment workflow designed specifically to each agency's needs.
4. **Case Management**
   Enables continuous optimization of authentication and fraud decisions with visualization, data correlation and exception handling for complex caseloads. The Case Management feature can also integrate analyst feedback and third-party systems (via an application program interface (API) call) for additional feedback, improving future fraud decisions.

> Balancing the quality of a citizen's online experience with effective fraud control is a complicated endeavor for government agencies. The ThreatMetrix Dynamic Decision Platform supports both objectives by facilitating better real-time digital decisioning.

Customized to your agency's needs

ThreatMetrix® Professional Services can guide your team through the design, implementation and ongoing optimization of your ThreatMetrix deployment. As part of our on-boarding package, we'll make sure the system is configured to your agency's specific needs and workflow, taking into consideration how the different data elements interact with each other and what thresholds they need to meet.

In addition to getting you up and running, we provide professional guidance to help you make informed decisions that improve efficiency and the end-user experience. We also offer a full suite of service packages to assist you in optimizing policies and rules for navigating today's threat landscape. Our service packages can be tailored to suit your precise requirements.

ThreatMetrix For Government advantage

- **An Unparalleled Network**
  The ThreatMetrix for Government Digital Identity Network protects 1.4 billion unique online accounts using intelligence harnessed from 2 billion monthly transactions.
- **Privacy by Design**
  s for Government is unique in its ability to solve the challenge of providing dynamic risk assessment of identities while maintaining data privacy through the use of anonymization and encryption.
- **An Integrated Approach to Authentication**
  Flexibly incorporate real-time event and session data, third-party signals and global intelligence into a single Smart Authentication framework, to help deliver a consistent and low-friction experience with reduced challenge rates.
- **Advanced Behavioral Analytics and a Clear-box Approach to Machine Learning**
  ThreatMetrix for Government Smart Analytics analyzes dynamic user behavior to build more accurate, yet simpler, risk models. The result is a competitive edge in customer experience with reduced false positives, while maintaining the lowest possible fraud levels.

For more information, call 888.579.7638 or visit
risk.lexisnexis.com/government

LexisNexis® RISK SOLUTIONS | ThreatMetrix®

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.

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, ThreatMetrix ID™ delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time. ThreatMetrix is recognized as the sole Leader in the 2017 Forrester Wave™ for risk-based authentication. Learn more at threatmetrix.com