LexisNexis Risk Solutions

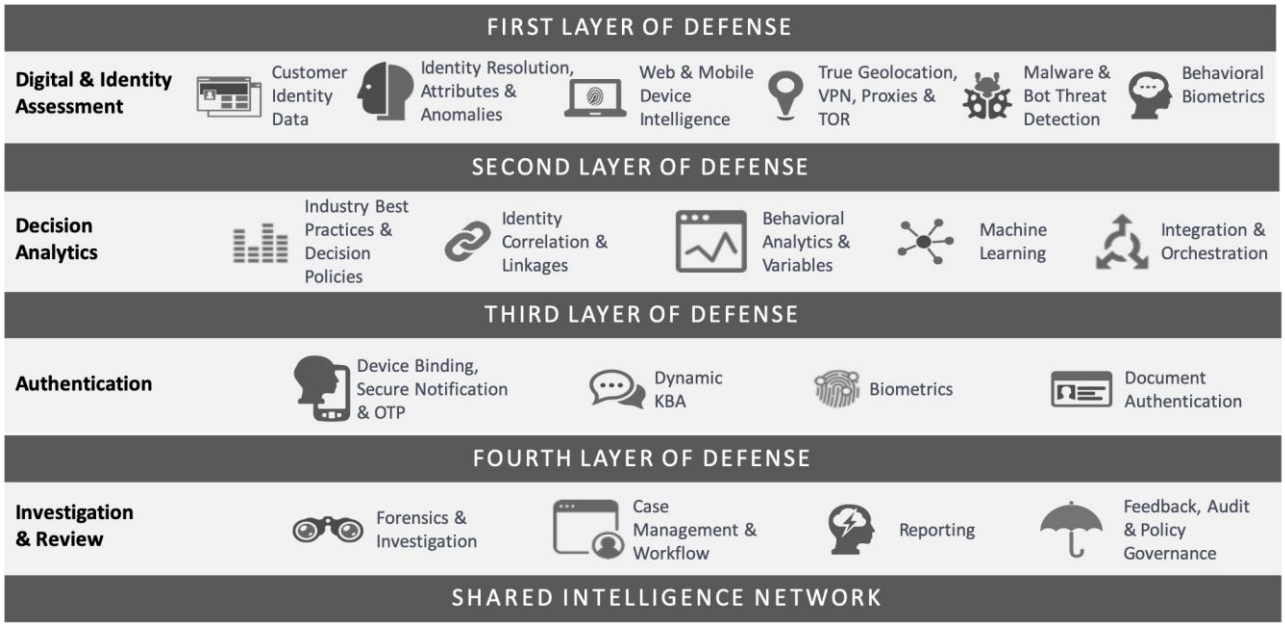
G-Cloud 15 Framework

ThreatMetrix Pricing Document

Contact:
LexisNexis Risk Solutions
Global Reach, Dunleavy Drive
Cardiff, CF11 0SN
Office: 029 2067 8555
Email: ukigcloudenquiry@lexisnexisrisk.com

Table of Contents

ThreatMetrix Overview



ThreatMetrix provides best-in-class fraud, identity and authentication services to help digital businesses and public sector organisations better distinguish trusted customers and citizens from potential fraudsters in real time, without adding unnecessary friction. Leveraging global intelligence from the Digital Identity Network, ThreatMetrix enables organisations to make more informed fraud and risk decisions.

The ThreatMetrix solution platform comprises of the following modules:

- **Digital Identity Network** – harnesses and stores real-time global data to generate a user's true digital identity by analysing the myriad of connections between devices, locations, behaviours, detected threats and critical but anonymised personal information.

- **Mobile SDK and Web Profiling** – it collects user's device (mobile application or web browser) information such as the various device identifiers, attributes, IPs, rooting and application information, and security health information in order to evaluate the security posture of the device, as well as build a unique identifier for it.

- **Profiling Server** – it collects and stores the profiling data from user's session (e.g. enrolment) and will send it to Decision Platform to perform a risk assessment.

- **Threat and Anomaly Detection** – By baselining your good customer base and combining it with ThreatMetrix session data, the product can look from discrepancies from normal. This creates a powerful ruleset around first time rules around first time location, IP (including piercing a proxy) /VPN/Tor, remote access tool.

- **Dynamic Decision Engine** – The configuration of policies (rulesets) allows ThreatMetrix to risk assess real-time incoming events (new account, login, redemption / payment) allows and understanding of

the trust and risk of the event. The policies and rules use all the data points available from both incoming and historic events. These data points include identity, device attributes, location information, network data, anomaly intelligence and also behavioural data (clicks, keyboard strokes and gestures) aggregated to a single platform.

- **Portal and Case Manager** – the toolset for analysts to complete manual reviews, investigate further linked accounts, view complete transaction histories. The Policy and rules editor also resides in the Portal and analysts and data scientists can run machine learning jobs inside the portal to optimise the rules performance. The ThreatMetrix Portal is fully audited and users have both access and configuration control over profiles and screens.

Fraud Detection

The global digital network and creation of a specific LexID digital identity persona within the ThreatMetrix Digital Identity network alongside the associations made with good and bad behaviour or risk incidents, allows any digital interactions to assessed and analysed for fraud not only in the context of local behaviour in the network, but also regionally or by industry as well globally. This creates the following benefits within fraud detection:

- Instantly recognise and prevent a range of fraud types including identity, synthetic, impersonation, account takeover, collusion and 1st party fraud
- Identify malicious identities, activity and suspicious applications in real-time as they occur and prevent loss from occurring
- Use sophisticated analytics to uncover previously unknown fraud rings, mule operations and correlated attacks
- Leverage a global repository of bad digital identities and related entities (device, email, phone, IP etc.) known to have committed fraud across the globe
- Enable cross **channel analysis**, where digital and physical transactions occur, to provide total coverage by utilising the inbuilt integration capabilities to verify and analyse physical and digital identity together

Customer Authentication

The ThreatMetrix solution LexID Digital Identity Global network allows faster authentication of legitimate users, as behaviour is analysed and considered to create a digital LexID from an entities' multiple interactions across the whole global network, not only customers' own interactions. This creates greater persona insight and confidence can be gained by understanding the digital identities interaction profile over time with other organisations within the network.

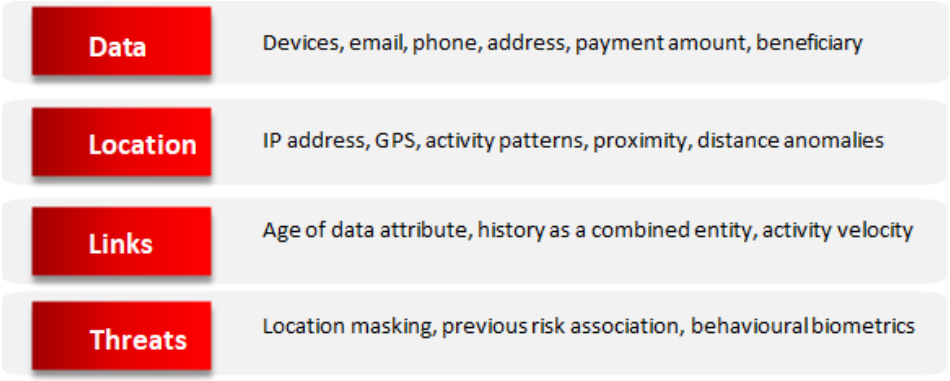
As such if a consumer only interacts with your organisation digitally sporadically, you do not draw false perception of their behaviour, as the same digital entity may be active elsewhere across the network and this information can be utilised to analyses any ongoing transactions in your environment for risk and authentication of the digital persona. This creates the following benefits:

- Leverage established online personas built from a crowd sourced identity network of over **6,000 organisations globally**
- **Recognise good returning individuals** through their online persona to ensure a smooth onboarding process
- Reduce operational false positives and **reinvest resources** into other value adding fraud investigations
- **A strong digital footprint** via existing relationships with digital players such as digital content providers and e-commerce merchants
- **Realise the benefits of trusted Authentication** (via strong ID) to allow known and classified good users to have an improved digital experience, thus growing digital engagement by improved user experience capability

Digital Identity Network

The ThreatMetrix solution is used for authenticating digital personas and transactions. LexisNexis Digital Identity Network allows organisations to profile devices and identify threats, examine users' identities and activity. The platform protects against identity fraud, account takeover, payment fraud, fraudulent account registration and allows fast real time authentication of trusted users.

The LexisNexis Digital Identity network currently consists of over 3.3 billion digital identities.



The real-time analytics on each and every transaction considers hundreds of data attributes within each transaction to build a digital persona. This allows users of the Digital Identity solution platform to implement risk and assessment policies on each and every transaction in order to either block transactions, refer for analysis, perform further validations/ step ups or to allow or fast track interactions based on the policy rules assessment scores and data.

Rules can analyse aspects such as:

- Has the device committed fraud against your website or another relevant industry before?
- Multiple applications, different users with the same device and location?
- What is the current proximity to the applicant's home address?
- Has the digital ID, device, phone and email been seen together before?

Based on the result of the digital interaction, other elements can be brought into action for the transaction to progress or the transaction be allowed to continue, such other actions could be via automated API call to do the following:

- Full document Authentication (image / scan / selfie)
- Knowledge Based Authentication – Questions based assessment
- Identity verification – Details validated against official records and databases
- 2FA validation – SMS or email or in APP push

Key Benefits for UK Public Sector Organisations

- Reduced fraud and error: Detect identity, synthetic, impersonation and account takeover fraud in real time, reducing losses across benefits, tax, grant and payment schemes.
- Improved citizen experience: Recognise trusted returning users and apply friction only where risk is elevated, supporting “digital by default” strategies without disadvantaging genuine citizens/actors.

Pricing

Transaction Services

The price is based on transactional volumes at price of £0.005 per transaction/API call subject to a minimum order value of £30,000.

Implementation Professional Services Hours

Implementation services can be purchased at an hourly rate of £250, required hours are dependent on use cases, complexity and transactional volumes.

Customer Support and Maintenance

For a required fee of 20% of the Transaction Services Subtotal (£6,000 minimum) LexisNexis Risk Solutions will provide Customer Support Services via Phone, Web, and Email on a 24x7x365 basis. Customer Support Services include one Organisation ID, and ThreatMetrix Knowledgebase access. During the term of your subscription to Transaction Services, you will qualify for support and receive periodic updates and upgrades to the software.

Customer Support and Maintenance	Description	Unit Price	Quantity	Fee
Customer Support and Maintenance	20% of Transaction Services			£6,000 min
Additional Service Activation (1 Included with purchase of Support)	• Creation of additional Organisation ID (Test or Production Environment); • Portal/Reporting configuration; and • Policy Activation (default rule activation)	£1,500		
SSL Certificate Activation (Minimum of 1 Required)	• SSL Certificates to be hosted by ThreatMetrix • Multiple-domain SSL Certificates priced at special rates.	£1,500	1	

Training

Service	Quantity	Price
Onsite Instructor Led Training		
• Fraud Analyst Class, Onsite.		£10,000
Other		
• Custom Training Class *By bid. A statement of work will be created to document the requirements, deliverables, and cost.*		

ThreatMetrix On-Demand Training (ODT) is charged as follows:

Transaction Subscription Fee		Annual Unlimited ODT Access Fee
£0	£50,000	£1,000
£50,001	£100,000	£1,500
£100,001	£250,000	£5,000
£250,001	£500,000	£15,000
£500,001+		£45,000

Additional Terms

Payment for all of the services purchased will be invoiced upon mutual execution of a purchase order. All Transactions purchased, or in a renewal order, expire upon the earlier of consumption or one (1) year from the Date of Purchase. Professional Services provided on a time and materials basis and all travel, lodging, and other expenses are not included. Unless otherwise specified, all unused services will expire one (1) year from the Date of Purchase. No credits for unused services will be issued. Professional Services in excess of the Professional Services Subtotal may be procured for £250.00 per hour.

What isn't included in the price: Any enhancements to the product during the term of the contract.