

ThreatMetrix™ Cloud-Based Fraud Prevention Platform

Our Comprehensive Fraud Platform That Helps Companies Fight Online Fraud in Real-Time During Account Creation, Login Authentication and Payment Authorization

**Incorporating:
ThreatMetrix SmartID™ Cookieless Device Identification
and Enhanced Mobile Authentication**



Introduction

Online businesses need a cost-effective way to swiftly, reliably and consistently determine whether the person at their Website is a fraudster or a customer with minimal difficulties so visitors want to stay and customers want to return. Device identification, using a visitor's computer to provide additional fraud prevention and authentication intelligence, remains the most effective first perimeter of defense to protect online transactions including payments, logins and registrations.

Benefits include:

- Zero customer imposition, providing passive two factor authentication for online transactions without requiring software or hardware tokens or challenge questions
- Not relying on the collection of personally identifiable information (PII)
- Stops first-time fraud attempts based on device anomalies and global behavior

Unfortunately, since first generation device identification technologies were introduced, the world has changed dramatically with an increase in the sophistication and globalization of cybercrime and a corresponding increase in exposure to enterprise fraud, risk and security teams. The ThreatMetrix™ Cloud-Based Fraud Prevention Platform – incorporating ThreatMetrix SmartID™ cookieless device identification – provides businesses with a crucial perimeter of defense to protect online transactions including account creation, login authentication and payment authorization. Beyond simple browser dependent solutions, ThreatMetrix also is capable of detecting the use of hidden proxies, VPN, true OS and origin detection as well as providing satellite, dial-up and mobile wireless detection.

Benefits of the ThreatMetrix Cloud-Based Fraud Prevention Platform

Sell more, grow faster, protect your brand, and provide your customers with a positive online experience.

ThreatMetrix SmartID Cookieless Device Identification

Cookies are obsolete as a reliable way to identify a device to prevent fraud. ThreatMetrix SmartID provides cookieless device identification using attribute matching and confidence scoring. ThreatMetrix ExactID™ provides parallel matching across multiple cookie equivalents. Used together, ThreatMetrix SmartID and ThreatMetrix ExactID provide cross validation to detect cookie wiping, private browsing modes, hidden proxies, botnets and cookie and device manipulation.

No Personally Identifiable Information (PII) Required

The ThreatMetrix Cloud-Based Fraud Prevention Platform, which uses anonymous data from the computer, its connection to the Internet and contextual data from the transaction, is popular among fraud analysts and IT security professionals because it does not require the use of PII to assess customer legitimacy.

One Solution for Three Web Fraud Scenarios

The ThreatMetrix Cloud-Based Fraud Prevention Platform addresses all three of the major web fraud scenarios – account creation, login authentication and payment authorization – within one integrated solution.

Stop Fraud at the First Attempt

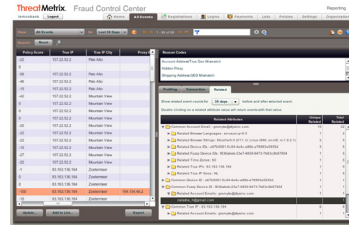
The device and its transaction data reveal risk about the person so you can decide whether to accept, challenge or reject within seconds even if you've never encountered the device before. No prior history is required.

Real-Time

The ThreatMetrix Fraud Network operates in real-time so it does not impact the experience a user has at your Website. Drawing upon hundreds of anonymous characteristics from a Web transaction and analyzing them in real-time, ThreatMetrix reveals hidden truths about the device visiting your Website to help you decide whether to trust the computer to create a new account, authenticate a login or payment.

Shared Intelligence Across a Global Network

Rather than being limited to transactions within your customer base, the ThreatMetrix Cloud-Based Fraud Prevention Platform provides you with a global perspective of risk from a worldwide network of shared intelligence across tens of millions of transactions across all ThreatMetrix customers—always up-to-date, always available.



ThreatMetrix Fraud Control Center dashboard enables customers to configure their solution and monitor recent transactions and trends.

Facilitate Positive Customer Experiences

ThreatMetrix provides passive two factor authentication for online transactions without requiring software or hardware tokens or challenge questions. Returning computers are verified instantly by the unique characteristics of their Web transaction. Instant validation that's entirely transparent to your customer enables better and smarter delivery of online services.

Device Independent

ThreatMetrix provides device identification regardless of the device – be it a smartphone, personal or tablet computer. This is critical as mobile shopping and banking are on the rise.

Cloud-Based Service

ThreatMetrix is a cloud-based service meaning that no installation is required. ThreatMetrix manages all upgrades for you, reducing your dependency on internal IT. There are also no patches or updates for you to download and install. Your fraud analysts can be up in running in a matter of hours or days, not weeks or months. Finally, since ThreatMetrix manages availability, there's no need for you to add hardware, software or IT personnel.

Customer Configurable

ThreatMetrix provides industry-specific rules-based templates that enable you to instantly review and analyze transactions based on date, score, status, or other attributes across the global ThreatMetrix network. Customize ThreatMetrix rules and transaction scoring to fit your tolerance for risk with our simple web console – or use ThreatMetrix consulting services to take advantage of expert knowledge and advice specific to your industry.

Complement Other Anti-Fraud Tools

ThreatMetrix is a powerful complement to home-grown and other anti-fraud tools, bringing critical insights and information context to Web transactions.

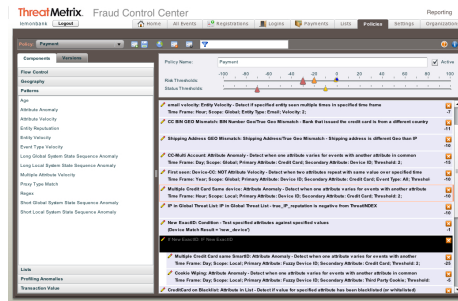
Introducing ThreatMetrix SmartID

The ThreatMetrix Cloud Based Fraud Prevention Platform represents the third-generation of device identification technology. As illustrated in the table below, ThreatMetrix device intelligence has evolved from IP address, to browser attributes, to packet fingerprinting intelligence to stay one step ahead of increasingly sophisticated fraud attacks.

ThreatMetrix goes beyond first generation device identification technologies that are limited to IP address and browser attributes with ThreatMetrix SmartID, a key component of the ThreatMetrix Cloud-Based Fraud Prevention Platform. ThreatMetrix SmartID, which incorporates unique TCP/IP packet fingerprint detection, cross correlates and scores device fingerprint attributes and behavior with session and browser cookies to more accurately establish and authenticate a device identity.

Attributes collected from the IP address and browser are easy to manipulate. For example, common browser plugins allow fraudsters to change the apparent browser and version that the Web server sees with a click of a button.

ThreatMetrix SmartID device identification overcomes these limitations by adding packet fingerprinting intelligence for greater accuracy and spoof protection. Because the information is collected as part of the standard networking and browser security model, there is no possibility of leakage of personal information, no interruption to the customer’s online experience, and no additional software or browser plugins to download or accept.



The ThreatMetrix Fraud Control Center policy editor enables customers to customize fraud screening that is specific to their business requirements.

Standard Browser Fingerprint

- Browser String
- Browser Cookies
- Browser Plugins
- Clock Time (Browser)
- IP Address and Geolocation

Easy to Subvert

Unique: ThreatMetrix IP Packet Fingerprinting

- Proxy Bypass and True IP/Geolocation
- Proxy Fingerprint and Hidden Proxy Detection
- CPU Fingerprint
- Clock Fingerprint (Packet)
- Device Uptime Detection
- True Operating System Detection
- Internet Connection Settings (e.g., Wifi or 3G)
- Botnet and Infection Detection
- Script and Non-Human Interaction Detection

Subversion Resistant

	IP Address Intelligence	Browser Attribute Intelligence	ThreatMetrix Packet Fingerprinting Intelligence
IP Geolocation	X	X	X
Known Proxy IP Detection	X	X	X
Know Botnet/Trojan IP Detection	X	X	X
Browser and Plugin Cookie Identification		X	X
Browser and Plugin Fingerprint Recognition		X	X
Time Zone and Time Difference Detection		X	X
Packet Fingerprint Recognition			X
Hidden Proxy MITM Detection			X
True Origin Detection			X
True OS and Spoofed Browser Detection			X
VPN Detection			X
Satellite, Dial Up, Mobile Wireless Detection			X

Key Components of the ThreatMetrix Cloud-Based Fraud Prevention Platform



The ThreatMetrix Fraud Control Center event viewer enables fraud analysts to review suspicious transactions and easily find others that may be related.

Component	Description
Enterprise Risk Engine	ThreatMetrix provides real-time contextual scoring based on device, customer and transaction attributes and historic analysis through a customer configurable rules engine. Default rules and algorithms will detect many anomalies such as hidden proxies, high risk geographies, anomalous language and time settings, potential cookie wiping and blacklisted attributes. More advanced rules allow for correlation of other transaction data such as detecting multiple identities, payment accounts or shipping addresses used by the same device, or an unusually high volume of transactions from a device across the ThreatMetrix network. ThreatMetrix rules can be updated by analysts and activated immediately to respond to changing threats.
Global Network Intelligence	ThreatMetrix customers benefit from anonymous and aggregated device and transaction behavior seen across the global ThreatMetrix network through both automated scoring as well as customizable fraud filters. The ThreatMetrix Cloud-Based Fraud Prevention Platform provides proactive protection that gets smarter with every customer and transaction without requiring extensive manual input.
Queue Management	Manual review of transactions is time consuming and expensive. To address this, ThreatMetrix allows for custom tuning of rules to reduce false positives, and also automated assignment of transactions to analyst queues by configurable rules. This enables analysts to focus on the highest risk transactions, for example based on score, transaction amount, or criteria such as geographical origin. When a transaction is reviewed, it can be marked as rejected/accepted to improve the ability of ThreatMetrix to score transactions through predictive scoring.
Customizable Alerting	ThreatMetrix supports automated alert rules to notify an analyst by email when a transaction meets specified criteria. These alerts can be set based on risk, transaction or device attributes or associated with specific fraud behavior. Alert content can be customized and linked directly back to the transaction for review.
Online Portal and Dashboard for Transaction Monitoring and Link Analysis	In addition to a real-time API that immediately returns device identifiers, anomaly indicators and risk scores, ThreatMetrix provides an online portal to review past transactions. It includes a dashboard that shows recent high-risk transactions and trends, as well as advanced search capabilities to assist fraud analysts to find related transactions and discover links between suspicious activities.
Bulletproof Security and Privacy Protection	ThreatMetrix provides advanced device identification technology to detect and alert based on suspicious device anomalies. For even more powerful fraud detection, transaction identifiers (such as an email address, payment account hash, phone number, etc.) can be passed to allow for more correlation. When provided, ThreatMetrix protects these identifiers with encryption and one-way hashing so that the data is never exposed or shared. In addition, power role-based permissions and full auditing meet and exceed enterprise security compliance requirements.

For more information, or to schedule a demo, call **1-650-625-1451** or email **sales@threatmetrix.com**.

© 2011 ThreatMetrix. All rights reserved. ThreatMetrix, ThreatMetrix Cloud-Based Fraud Prevention Platform, ThreatMetrix SmartID, ThreatMetrix ExactID, and the ThreatMetrix logo are trademarks or registered trademarks of ThreatMetrix in the United States and other countries. All other brand, service or product names are trademarks or registered trademarks of their respective companies or owners.

CONTACT US

ThreatMetrix Inc.
5150 El Camino Real, Suite D-30
Los Altos, CA 94022
Telephone: +1.650.625.1451
Fax: +1.888.675.3451
www.threatmetrix.com

EMEA Headquarters
ThreatMetrix B.V.
Laan van Vredenoord 33-39
2289 DA Rijswijk
The Netherlands
Telephone: +31 (0)708200508