

TrustDefender™ ID from ThreatMetrix™

Real-Time Device Identification to Stop Fraud



Introduction

Online businesses need a cost-effective way to make sure that visitors or customers are who they claim to be before they create a new account, login to an existing account, or make a transaction. But security and fraud control measures cannot interfere with the customer experience.

Traditionally, companies turn to device identification solutions for fraud prevention and authentication intelligence. However, sophisticated cybercriminals have figured out how to defeat most early device identification technologies.

TrustDefender™ ID from ThreatMetrix™ is a cloud-based, real-time device identification and identity verification solution that protects businesses against cybercriminals and helps validate returning customers and prospects.

Advanced, third-generation device identification technology uses multiple methods, including cookieless device identification, to expose an individual's intent hidden in the attributes of the user's device. TrustDefender ID looks beyond browser attributes and IP addresses to detect hidden proxies, VPNs, true OS, and origin, as well as satellite, dial-up and mobile wireless connections.

Online businesses use TrustDefender ID to protect their customers and brands from online fraud, while providing customers with a positive experience:

- Prevent individuals from creating new accounts using fraudulent identities
- Protect customer data and identities by preventing logins using stolen credentials
- Detect and deter payment and transaction fraud, including card-not-present (CNP) purchases and financial transactions, by making real-time decisions based on flexible risk scoring.

How It Works: SmartID™ and ExactID™

Early device intelligence solutions used IP addresses, browser attributes and cookies to identify devices. Criminals can easily manipulate browser attributes and IP addresses. Simple browser plug-ins can change the apparent browser and version with the click of a button. And cookies are easily manipulated or turned off.

TrustDefender ID represents the third generation of device identification technology. It incorporates unique TCP/IP packet fingerprint detection, cross-correlates and scores device fingerprint attributes and behavior with session and browser cookies. As a result, ThreatMetrix can detect fraud behind a wide range of defenses.

TrustDefender ID combines multiple technologies to deliver insight into visiting devices:

- **ThreatMetrix ExactID™** uses a variety of persistent devices, including cookies. It is useful for recognizing returning, good customers that are not attempting to cloak themselves.
- **ThreatMetrix SmartID™** is derived from the analysis of many browser, plug-in, and TCP/IP connection attributes. It works even when visitors use cookie wiping or private browsing. SmartID generates a confidence score based on a statistical model.

By combining intelligent packet and browser fingerprinting, ThreatMetrix SmartID and ThreatMetrix ExactID uncover fraud without false positives.

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

Use Third-Generation Device Identification to Stop Fraud

	IP Address Intelligence	Browser Attribute Intelligence	ThreatMetrix Packet Fingerprinting Intelligence
IP Geolocation	X	X	X
Known Proxy IP Detection	X	X	X
Known 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

Protect the Customer Experience

Traditional device identification solutions can create false positives that make life difficult for legitimate users or existing customers. TrustDefender ID device identification functions as a passive two-factor authentication that requires no software or hardware tokens or challenge questions. TrustDefender ID can instantly and transparently verify returning computers based on their device characteristics.

Unlike some fraud prevention solutions, TrustDefender ID benefits from but does not require customers to provide personally identifiable information (PII) to validate their identity.

Stop Fraud in Real-Time

TrustDefender ID operates in real-time, supporting the instant decisions important for online transactions. Real-time analysis of device characteristics reveals hidden details about devices visiting your website.

A flexible, rules-based engine supports real-time risk scoring and decisions. Industry-specific templates help you review and analyze transactions as they happen. You can customize the rules and scoring to fit your tolerance to risk, using a simple web-based console.

With real-time insight into visitors' devices and behavior, you can decide whether to accept, challenge or reject a transaction within seconds – even if you have never encountered this particular device before.

Gain a Global Perspective

You're not limited to seeing the transactions within your own customer base. Through integration with the ThreatMetrix Cybercrime Control Center, TrustDefender ID accesses a global network of shared intelligence across all ThreatMetrix customers – tens of millions of transactions daily. Your fraud intelligence is always up-to-date and available with ThreatMetrix.

Optional Personal Identity Verification

For situations that require additional layer of screening, ThreatMetrix offers an optional Identity Verification Service. This on-demand service, delivered from the cloud, integrates identity verification services from TransUnion with the ThreatMetrix Cybercrime Defender Platform for efficient, real-time fraud prevention.

All the Benefits of the Cloud

TrustDefender ID is the fastest and most cost-effective way to protect the integrity of online transactions. As a cloud-based solution, it requires no hardware or software to install or manage. ThreatMetrix manages all upgrades, reducing the ongoing cost of ownership for the solution. Fraud analysts use a web-based console and can be up and running in hours, not weeks or months.

Who Uses It?

TrustDefender ID is used with success in over 600 customers in industries including e-commerce, financial services, government agencies, healthcare, and other Fortune 1000 organizations. It helps businesses protect employee logins, online banking and financial transactions, and online transactions with customers and partners.

Part of a Unified Platform for Integrated Protection

TrustDefender ID is part of the ThreatMetrix™ Cybercrime Defender Platform, which protects the integrity of online transactions as well as employee logins. By integrating advanced device identification with sophisticated malware detection in a single platform, ThreatMetrix Cybercrime Defender Platform can protect entire online transactions – ensuring that the user is not fraudulent and that the transaction itself is free of malware.

The ThreatMetrix Cybercrime Defender Platform provides a common view of users and devices across all systems, helping identify cybercriminals across a consortium of sites sharing fraud intelligence. It is the most comprehensive fraud prevention solution available today.

As a single, integrated platform delivered from the cloud, the ThreatMetrix Cybercrime Defender Platform provides superior fraud intelligence and protection with a low total cost of ownership.

Platform and Availability

TrustDefender ID is delivered as a cloud-based service that requires no software or hardware installations.

Advanced device identification technologies are device-independent, and work with smartphones, laptops and tablet computers.

For more information, or to schedule a demo, call **+1-408-200-5755** or email **sales@threatmetrix.com**.

© 2012 ThreatMetrix. All rights reserved. ThreatMetrix, TrustDefender ID, TrustDefender Cloud, TrustDefender Client, 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

USA Corporate Headquarters
ThreatMetrix Inc.
160 West Santa Clara Street
Suite 1400
San Jose, CA, 95113
Telephone: +1.408.200.5755
Fax: +1.408.200.5799

www.threatmetrix.com

EMEA Headquarters
ThreatMetrix B.V.
Laan van Vredenoord 33-39
2289 DA Rijswijk
The Netherlands
Telephone: +31 (0)70 8200 508