Never before have so many system break-ins and data breaches occurred – and the pace is accelerating.

The vast majority of such attacks succeed because the authentication systems use outdated technologies that rely on easily compromised credentials such as user IDs and passwords. While tokens and other methods are available to strengthen security, they can be expensive and take significant resources to roll out and support. Substantial user interaction is also required, leading to user resistance.

**ThreatMetrix™ Context-Based Authentication**

Two-factor, context-based authentication (CBA) from ThreatMetrix evaluates much more than a user’s traditional login credentials, immediately recognizing legitimate users while detecting cybercriminals, even if they are using valid – but stolen – user IDs and passwords. This frictionless solution is completely transparent to users, and does not burden the IT staff with added disparate solutions or maintenance.

All users have numerous system and individual characteristics and behaviors that the ThreatMetrix Digital Identity Network can capture and analyze. This information, along with other user-related data an organization may have, can be privately stored within ThreatMetrix to form a unique and rich Persona ID for every individual – identifying their specific devices, logon habits, typical locations, user IDs, email addresses, accounts, phone numbers, shipping addresses, and other identifying information. In addition, businesses can add their own data to provide customized, targeted analysis looking for compromised IP or email addresses, banned country lists for compliance, and countless other threats.

This comprehensive data, along with advanced device identification, connection information, and data from the world’s largest shared global trust intelligence network, enables ThreatMetrix to 1) develop a comprehensive view of everything pertaining to attempted connections; 2) detect anomalies and intelligently establish levels of risk and trust; and 3) establish a comprehensive trust score based on the organization’s predefined policies to enable an informed allow - reject - review decision.

**Powerful Features Not Found in Traditional Authentication Systems**

Utilizing sophisticated analytics, along with custom policies and rules for each application, CBA provides numerous capabilities not found in other authentication systems:

• Device-Specific Identification: Each PC, laptop, tablet, phone, or other device is profiled and uniquely identified and associated with specific individuals.
• Frictionless Two-Factor Authentication: Utilizing both device ID and user login credentials, CBA provides transparent, behind-the-scenes Two-Factor Authentication.
• Malware Detection: Detects malware and other threats that can compromise security.
• Device History: Devices that have been compromised by malware or involved in fraud are disclosed. Conversely, devices with high levels of trust are also identified.
• Detection of Suspicious Connection Paths: Devices using TOR networks, VPNs, or other networks that attempt to hide or anonymize locations or identities are revealed.
• Private Data Store: With Persona DB, customers can have their own private extensible database allowing organizations to privately store a wide range of customer/employee identifying attributes, characteristics, and behaviors as well as any other information relevant to authorizing visitor access. Persona DB can contain account information, phone numbers, email and shipping addresses, typical locations, compromised accounts, compromised IP or email addresses, or banned country lists for compliance.
• Legitimate Locations and User Behavior: CBA establishes normal and legitimate user behaviors, including elements like IP addresses and geolocations, language(s), devices used and their...
configurations, login times, frequency and speed of login attempts, impossible locations based on recent transactions, and more.

- Instant Recognition of Valid Users: Trust Tags allow organizations to label users and their devices as “trusted” for future encounters. Valid users don’t experience unnecessary step-up authentication, and can be granted access with minimal input or friction.

Dynamic Decision Platform
The SaaS-based ThreatMetrix Dynamic Decision Platform evaluates the entire context surrounding each login attempt. Only ThreatMetrix includes all the intelligence and processes necessary for CBA in a single solution.

Largest Shared Global Digital Identity Network
ThreatMetrix profiles tens of millions of users and their devices daily, and regularly processes hundreds of millions of logins, payments, and other transactions. The Digital Identity Network is the repository for this wealth of data.

- Extensible Private Data Integration
ThreatMetrix provides the ability for users to add a private data store only accessible to them to expand and enrich the global data available via the Digital Identity Network.

- Profile Any Device and Identify All Threats
Profile desktops, laptops, smart phones, or tablets accessing your website, uniquely identifying each device and detecting malware and anomalies that indicate high risk.

- Examine Users’ Identity and Behavior
Comprehensive details about online user identities and behaviors, such as user name, password, email address, and more.

- Configure Business Rules
A powerful yet easily customizable Policy Engine allows you to model your business process and incorporate your own tolerance for risk.

- Validate Business Policy
Constantly evaluate risk scores and corresponding business policies.

- Enable Detailed Analysis
Visualizations and analytical reports enable your security and fraud analysts to see and understand enterprise application activity, and take the necessary steps to reduce unauthorized access.

The ThreatMetrix Advantage
ThreatMetrix offers the most advanced solution available to provide strong, context-based authentication without burdening your IT resources or your users.

- Rapid, lightweight and cost-effective deployment: The SaaS-based Dynamic Decision Platform provides context-based authentication without the need to add or deploy servers, tokens, or additional infrastructure.

- All logins protected without hindering customers or employees: Unlike strong authentication solutions that require token deployments and extra user steps to log in, the ThreatMetrix solution easily secures all logins without any added burden on customers or employees.

- Up-to-date, local and global insight: Integration with the Digital Identity Network and private data stores provides constant access to current customer/employee and device data, relevant organizationally supplied data, as well as threat intelligence derived from millions of continuing transactions.

- Real-time responsiveness: ThreatMetrix delivers real-time insight so you can detect cybercriminals before they gain access or conduct a transaction.

ThreatMetrix®, The Digital Identity Company®, operates a global shared intelligence network to differentiate trusted customers from fraudsters. The ThreatMetrix Digital Identity Network® recognizes behavior and identities across 4.5B unique devices from 1.4B anonymized users worldwide. More than 5,000 businesses rely on ThreatMetrix as their decision engine to deliver a frictionless digital customer experience across all online transactions, for increased profitability and security.

For more information, or a demonstration of how the ThreatMetrix solution can work for your business, contact us at:

T +1 408.200.5755
F +1 408.200.5799
sales@threatmetrix.com
www.threatmetrix.com
160 W Santa Clara Street
Suite 1400
San Jose, CA 95113