ThreatMetrix

WHITEPAPER

Combating Cybercrime – A Collective Global Response

ThreatMetrix Global Trust Intelligence Network

WHITEPAPER

ThreatMetrix™

Contents

ThreatMetrix™

Executive Summary

Cybercrime is costly for all online businesses and can no longer be ignored. Well-organized cybercriminals operate in powerful networks that allow them to attack thousands of online businesses using an efficient and scalable model.

A prime example of the sophistication of attacks and profit-motivated information exchange is the evil nexus between enterprise data breaches and online fraud. Specialist hackers focus on gaining access to enterprise systems and steal millions of credit cards and identity data. Using underground networks and messaging systems, hackers connect with fraud rings across the globe to sell credit card and identity data. Due to the nature of online businesses and with technologies such as proxies and VPN, fraud rings are able to launch global fraud attacks from anywhere in the world.

In contrast, online businesses operate in silos. They fight back with limited technology and resources. More importantly, online businesses have to be extremely sensitive to the overall customer experience for the genuine customers that account for 95%-98% of their transactions. Online businesses need to balance reducing friction in customer transactions with using the right technology to detect online fraud.

ThreatMetrix detects web fraud by analyzing online identities and their associations with devices using anomaly and velocity rules to make real-time decisions. ThreatMetrix builds a comprehensive Online Persona of the user performing the online transaction by combining online identities and device fingerprints while detecting any anomalies and malware-based compromises. Business policies allow configuration of user trust levels to fit each organizations business model. Shared Intelligence across millions of daily transactions as part of the Global Trust Intelligence Network provides the predictive analytics to protect online businesses and reduce customer friction.

Cybercrime Onslaught – Enemy at the Gates

The costs of cybercrime are significant. Various reports1 peg the number anywhere from $US 3.5 billion to $US 3.8 billion globally. This number represents just the loss of goods, gift cards and fraudulent money transfers. When you add the time and resources consumers, ecommerce merchants and financial institutions spend combating cybercrime, the estimated2 loss is well north of $US 274 billion.

According to Gartner, companies worldwide will spend $67.2 billion in 2013 on cybercrime. Gartner expects that to increase to $86 billion in 2016. That raises a serious conundrum – with companies spending billions in cybersecurity, the rate and cost of cybercrime should decrease, not increase.

Upon close inspection, the data is not surprising. Cybercriminals operate as a unified network, while enterprises operate in individual silos. On the surface, enterprises collaborate with industry conferences, best practices and joint committees, but lack real collaboration through sharing of data in a global network. ThreatMetrix is on a mission to break the traditional enterprise silos and provide a unified response to combat cybercrime without compromising security and privacy. To this end, it has created the Global Trust Intelligence Network.

To better understand the role of a global network of persona and device intelligence in preventing web fraud on a daily basis, we will first examine the cybercrime network and fraud ecosystem.

Evil Nexus of Data Breaches and Fraud

Data breaches and fraud are two sides of the same coin. Cybercriminals truly operate as an organized institution and a global network to perpetuate end-to-end criminal activities. At a macro level, moving from data breaches to online fraud is a four-step process based on tight collaboration, community and a network of sharing information across different groups of cybercriminals.

The first group of cybercriminals – often called harvesters and hackers – concentrate on breaching enterprises to steal credit card and consumer online identities by the millions. They use extremely sophisticated techniques including malware, Trojans, phishing and social engineering to penetrate the enterprises through their networks, endpoints and datacenters. Once inside the enterprise, they break into databases and file systems to haul millions of credit card, login/password and Personally Identifiable Information (PII) records such as SSN, phone numbers, and address etc.

The harvesters make their money by selling these credit cards and identities through underground forums to hundreds or thousands of fraud rings across the globe. This network of forums and secret handshake between the harvesters and fraud rings is a key nexus between the two worlds. The fraud rings purchase credit cards at a going rate of between $10 - $15 per card and online identities at $5 - $10 per identity. For example, harvesters from the data breach at Adobe could sell the 2.9 million credit cards and user names and addresses for a significant profit.

1 Reports include an annual Online Fraud Report by Cybersource, a unit of Visa Inc. and Nilson Report, a leading payment industry newsletter.
2 Based on Cybercrime Report by Norton, Symantec

The fraud rings called *cashers* have made significant investments in acquiring credit cards and online identities. Cashers will immediately used the stolen credit cards and online identities across thousands of ecommerce and financial institutions – the two places that you can transact online and perpetuate significant financial fraud. Online merchants and banks are open for business 24x7. The cashers use the most competitive feature of these businesses against them – online transactions can be initiated from anywhere in the world.

Gift cards, digital goods and money transfer services are most vulnerable, as it is easier to convert these goods into cash without any risk of tracing their originations. For physical goods such as phones, cameras and other consumer-friendly items, cashers employ drop zone specialists that receive shipped merchandise and convert them to cash. *Money mules* are used for concealing bank transfers and creating multiple money transfer channels, obfuscating traces to the fraud rings.

Tools and technologies such as malware, Trojans, spyware, keyloggers and bot networks are all available as a service for rent. Harvesters and fraud rings effectively have their own underground SaaS model. The key to their effectiveness in cybercrime is collaboration and operating as a global network.

ThreatMetrix provides Global Trust Intelligence for context-based authentication and web fraud prevention to accelerate revenue, reduce costs and eliminate friction. Global Trust Intelligence is based on **shared anonymized** insight into **Online Personas, Device Fingerprints** and **Cyber Threats** detected including malware-compromised devices and identities and sessions analyzed in real time with business context. ThreatMetrix currently has more than 1,900 customers and 9,000 websites in its Global Network across a variety of industries, including financial services, enterprise, ecommerce, payments, social networks, government, and insurance.

Web Fraud – Attack Channels and Vectors

Online businesses – including ecommerce, financial institutions and social media – establish an online presence through multiple

channels. End users can transact with these businesses using browsers through any endpoint device – PCs, Macs, tablets and smartphones. Today, 20%-30% of all transactions originate from mobile devices including purpose-built mobile apps. Cybercriminals indiscriminately use all of these transaction channels to perpetuate online fraud.

We have seen that based on the nexus of data breaches and fraud, cybercriminals have stolen credit cards and online identities when they access online businesses.

Pretending to be genuine customers, cybercriminals use different techniques to attack online businesses:

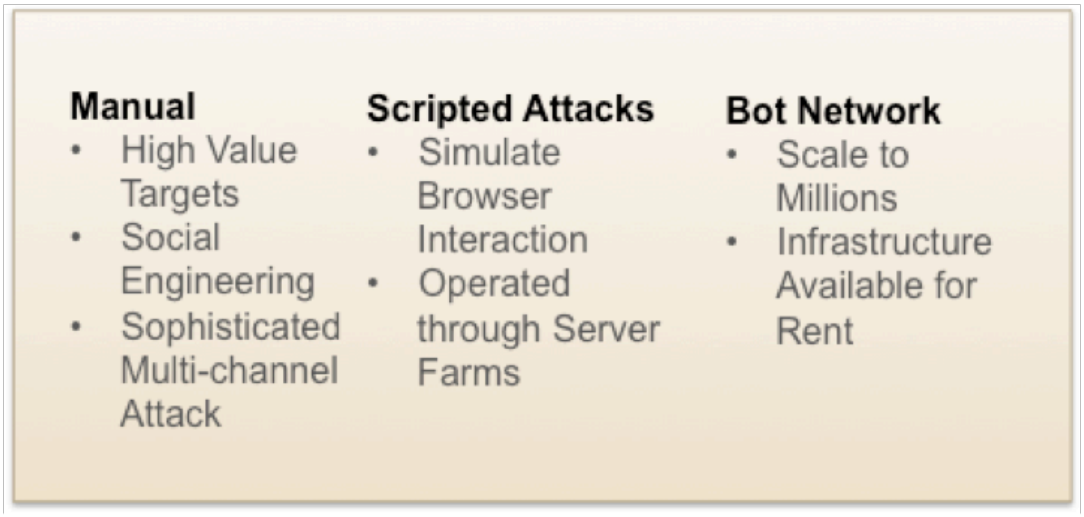
- **Card Not Present Fraud:** Cybercriminals use stolen credit cards and matching identities including name and address to purchase merchandise. In most cases, the fraud is detected months after the fact, when the cardholder issues a chargeback for the transaction. Unlike off-line transactions in which the issuing bank assumes liability, for online transactions it is the merchant who is liable for lost goods and refund of payment.
- **Account Takeover:** Having access to a consumer's account, whether ecommerce site account, social media, email or banking accounts, provides cybercriminals multiple avenues to a profit. Using malware, cybercriminals are able to intercept communication to and from the consumer's browser and the online business. Traditionally known as Man-in-the-Browser (MitB) attacks, the sophistication and

ingenuity of these attacks have made these a popular attack channel, especially in the online banking and certain high value ecommerce transactions.

- Cybercriminals can transfer money-to-money mule accounts, purchase merchandise or gift cards using credit cards linked to the account and gain detailed information on the consumer to perpetuate even more fraud under an assumed identity.
- **Fictitious Fraudulent Account Origination:** Cybercriminals use stolen identities and often synthetic/fabricated identities to create new accounts on social networks, ecommerce sites and banks. The main objective is to pretend to be a genuine customer. Once they have created a new account through the online channel, cybercriminals can use stolen credit cards and link them to these new accounts to buy gift cards and merchandise. In financial institutions that offer instant credit cards or line of credits to new accounts, cybercriminals use these accounts to finance fraudulent purchases.

Tools and Technologies used by Cybercriminals

Cybercrime is an organized business engineered at a global level. Cybercriminals no longer fit the stereotypes of a cyber geek as a lone wolf operating from a basement. To operate at scale –



cybercriminals have millions of stolen credit cards and identities – they use sophisticated technologies, including cloud based datacenters and millions of drone machines as part of botnets. Cybercriminals script site navigation by reverse engineering and site scraping techniques. They are then able to script the entire site navigation experience, from login to payment checkout in ecommerce sites or money transfer for banking sites. These scripts are orchestrated using different payloads – the millions of stolen credit cards and online identities. Scripts with dynamic payload can be executed from servers in a datacenter rented from server farms. To achieve scale and hinder any traceability, cybercriminals increasingly use bot networks – millions of end user machines – that are under central

command centers. Botnets can be used to execute any scripts with dynamic payload. Fraud rings in most cases do not even have to own these bot networks. These are available for rent, making them an effective way to launch a campaign with a fresh haul of stolen credit cards and online identities immediately and then promptly turn over the bot networks to the next fraud ring.

Business Realities – Avoiding Collateral Damage

Trusted Customer Identification

Although the focus is always on cybercriminals in fraud discussions, we cannot lose sight of the fact that trusted customers account for 95% of all business transactions. And in almost all types of businesses,

transactions from repeat customers account for the majority of the business. Identifying trusted customers should be an important capability for any fraud or access management system.

Identifying and recognizing trusted customers dramatically reduces customer friction. In most businesses, reducing customer friction significantly enhances the positive experience, leading to reduced abandonment of online transaction and ultimately increased revenues. Besides the positive impact on revenue, identifying trusted customers reduces fraud by establishing a baseline set of trusted customers and detecting anomalies from this baseline typically exhibited by cybercriminals. It can also dramatically reduce fraud review queues and case investigation workloads.

Bad Things Happen to Good People

Having their real world identity stolen can wreak havoc on any person for no fault of their own. Account takeover and a user's device being turned into a bot under the command of cybercriminals are

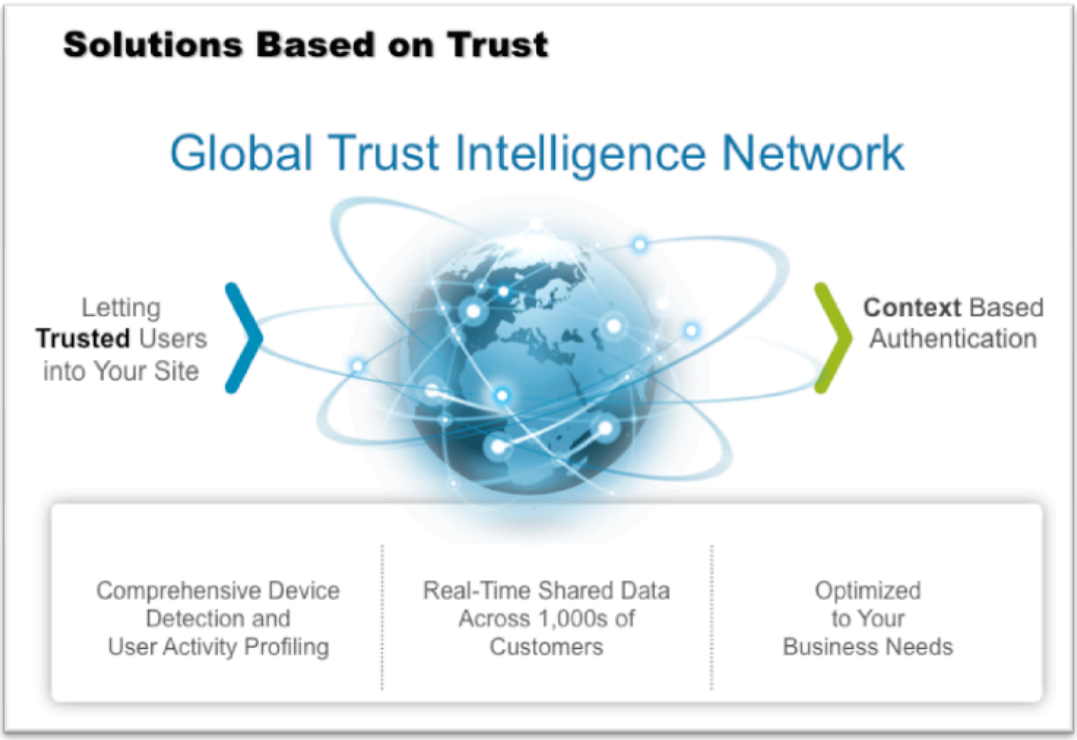
nightmare scenarios in the online world. Most consumers use the same login-password combination for a number of online accounts including banks, ecommerce sites and social media. When data breaches lead to a user's account getting compromised with one business, cybercriminals use the stolen identities on various other ecommerce and banking sites.

Similarly, a user's machine can become infected from malware, turning the machine into a bot used by cybercriminals to launch attacks against banks and ecommerce sites. Instead of using an account and device blacklist that only further victimizes a genuine trusted customer, recognizing the behavior and historical context of the persona and devices alerts the business of the nefarious situation.

Global Trust Intelligence Network – Collective Response to Cybercrime

ThreatMetrix provides a comprehensive fraud detection platform with trust as the cornerstone of the solution. Consumers conduct business online using digital identities. Businesses are engaged in transactions with digital identities and trust that these identities are genuine, safe, secure, and mean no harm to the business. Trust is a simple and fundamental concept, yet is very powerful. The ThreatMetrix mission is to deliver trust for all online transactions.

ThreatMetrix authenticates transactions based on the context of the business and the type of transaction. It compiles comprehensive data on the device and user persona and compares this data across billions of transactions gathered from 1,000s of online businesses across the globe to establish trust for each specific transaction.


Solutions Based on Trust
Global Trust Intelligence Network
Letting Trusted Users into Your Site
Context Based Authentication
Comprehensive Device Detection and User Activity Profiling
Real-Time Shared Data Across 1,000s of Customers
Optimized to Your Business Needs


Profile
Device and Threats
Examine
Identity and Activity
Configure
Business Rules
Validate
Business Policy
Enable
Detailed Analysis
Smart ID
Desktop and Mobile Threats
Malware
Hidden Proxy
MitB Attacks
VPN
Cookie Wiping
Related Events
Identity Information
Address Information
Transaction Attributes
Custom Attributes
Payment Information
Model Business Process
Identity, Behavior & Transactional Anomalies
Define Risk Tolerance
Automated Policy Score
Validate Business and Risk Policies
Authenticate
Truth Data Derived From Global Behavioral Results
Measure Trust
Ad hoc and Defined Reports
Comprehensive Business Analytics
Case Management
Cloud, Mobile App & Client
Real-time API
Persona ID
Policy Engine
Trust Tags
Reporting Portal
Real-time Global Trust Intelligence
Global Policy Engine, Machine Learning

Delivering Global Trust Intelligence

ThreatMetrix has identified a unique pattern for establishing trust across all types of online transactions to protect businesses from account takeover, card-not-present and fictitious account registration frauds.

Profile Device and Threats

In the online world, devices ranging from personal computers to mobile devices and networks are connecting consumers to businesses. ThreatMetrix device profiling is based on two technologies that help to uniquely fingerprint each device – both mobile and desktop –detecting cybercriminals and easily authenticating returning customers without false positives:

- Exact ID: Positive identification and context-based authentication based on cookies and multiple device identifiers across PCs and mobile device
- Smart ID: Cookie-less device identification using dynamic attribute matching based on network packet and browser attributes instead of static fingerprint matching
- SmartID technology uses a statistical regression analysis model that takes into account per-customer and global device profile patterns to generate reliable device identifiers with confidence scores. Unlike other fingerprint methods that are effectively static, ThreatMetrix SmartID provides adaptive, cookie-less identification that is tolerant of incremental and non-linear device changes.

Both SmartID and ExactID are globally unique and are generated in real-time based on data collected for that transaction and matched against billions of device profiles stored in the ThreatMetrix Global Trust Intelligence Network.

Mobile Device Attributes

Mobile devices are different than laptop/desktops, so the ThreatMetrix solution uses different techniques and algorithms to profile mobile-specific data. Attributes collected include:

- IMEI data
- Carrier information
- Protocol information
- SIM card-related information
- Mobile device attributes
- Mobile device configuration information
- Other supported mobile device Identifiers

Other mobile-specific data such as GPS coordinates add authentication context, assuming the user has granted appropriate location service permissions.

Network Identification Technology

ThreatMetrix leverages unique and patented network protocol identification technology to reveal the true IP address and geolocation of each device.

- Proxy-Piercing – Ability to pierce network proxies and establish the true IP address of the machine/user
- VPN Detection – Ability to distinguish the presence of VPN connections that indicates IP and Geo-location obscurity

In addition, ThreatMetrix provides detailed classification of proxies used in the transactions identifying hidden proxies, anonymous proxies and transparent proxies. Proxies and their attributes are good indicators of anomalies and suspicious activities. When combined with device and persona anomalies, these provide reliable indicators of fraudulent transactions by cybercriminals.

Malware Detection

ThreatMetrix has the most comprehensive approach to man-in-the-browser attacks by detecting zero-day attacks. It can also classify malware based on its behavior signature.

A common pattern for malware-based compromise is to alter a web page by adding extra input fields, tricking users into disclosing sensitive information such as account numbers, passwords etc. ThreatMetrix zero-day detection solution fingerprints web pages for the business and then detects any deviation of the web page when that page renders on the end user's browser. The unique characteristics of this malware detection approach include:

- Verification of webpage integrity against any Trojans and Man-in-the-Browser (MitB) attacks
- No software installation required on the end user's machine
- No reliance on known configuration files, blacklists, etc.
- Non-signature based approach does not rely on malware signatures, but instead uses a whitelisting strategy to identify anomalies from known state

To further add threat intelligence as part of the transaction evaluation, ThreatMetrix introduced an innovative approach of detecting malware targeted at *any* site, not just the business's website. This malware-fighting strategy uses honeypot detection techniques – a trap set to detect unauthorized webpage modification in the browser –to detect malware using a non-signature-based methodology. The honeypot techniques make it appear to the malware that the user is navigating to high-value websites commonly targeted by malware. As the malware attempts to attack the user by injecting new forms in the web page, ThreatMetrix detects these changes in real-time. Since this malware detection is real-time, it provides threat intelligence that is used to assess the risk associated with real time transactions.

Examine Identity and Activity

Genuine online transactions are about people at a keyboard or phone screen interacting with the business's web applications. ThreatMetrix enables the capture of comprehensive details for online identities and attempted activities, such as opening a bank account. It uses this information for real-time scoring. Looking at identities, devices and their associations and velocities over time, businesses can create their own Persona ID to model good, bad and suspicious customers based on actual behavior on site and across the global network.

Identity Attributes

ThreatMetrix offers a broad API that captures and analyzes identity information to model end consumers and identify positive behaviors.

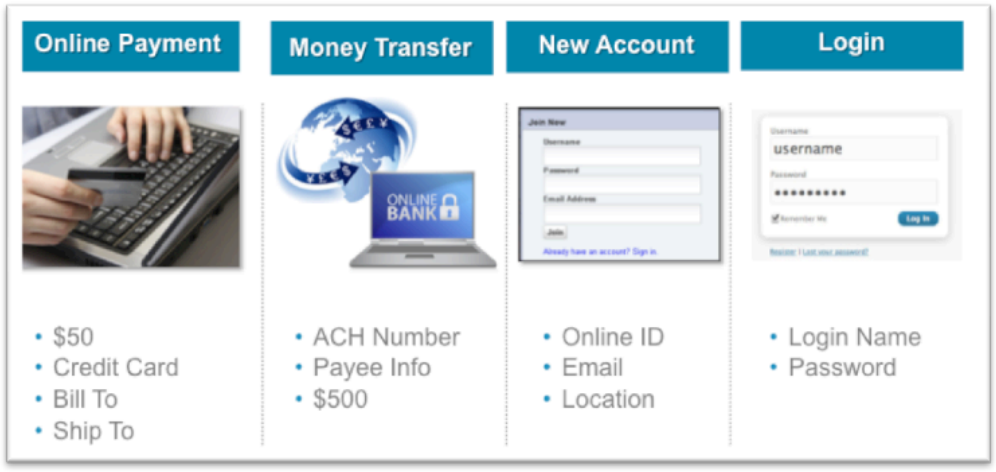
- *Online Identity* – Captures associated online handles on popular social and business networking sites
- *Account Information* – Account name and metadata such as *first seen* and *last seen* dates for the account
- *Account Login Information* – Creates a password hash with the associated account login information to track frequency of password changes
- *Account number* – Directly relevant to banks, captures account number hash to compare if the account number is associated with any other account name
- *Account Email* – Creates an email hash associated with the account to track changes of email address
- *Account address and phone* – Details containing associated address and phone numbers for the account
- *Shipping Address* – Information containing various Ship To address associated with the account

Transaction and Authentication Activity

ThreatMetrix API also captures the business and transaction context based on the type of activity being attempted. The types of actions that can be tracked range from customers accessing an online merchant's store, customers interacting with their bank accounts and social media interactions to customers purchasing physical and digital goods, making payments and money transfers through their banks, etc. Tracking these activities in real-time is reflected through a Persona Behavior Score that describes the collective acceptance, review and rejection of transactions performed by each Persona across the global set of businesses in the ThreatMetrix network.

The types of transaction and authentication activity meta data that can be tracked includes:

- Payment Amount
- Payment sums over time
- Payment Type
- Currencies
- Reward Status
- Account Type
- Account Age



Global Trust Intelligence – Network of Personas, Devices and Threat Information

Instead of analyzing each transaction in isolation, ThreatMetrix compares each transaction against baselines created by billions of previous transactions across all businesses that are part of the ThreatMetrix global customer base.

Device Identifiers such as Exact ID and Smart ID are associated with Persona ID and vice versa. Additionally, network anomalies and malware-based threat information is universally associated with device identifiers and Persona ID.

Billions of transactions containing device, persona and threat information are stored in a data warehouse that is analyzed and correlated for associations. Global Trust Intelligence Network is the amalgamation of hundreds of attributes capturing device, persona and threat information across billions of transactions.

Configure Business Rules

Businesses across industry segment, including ecommerce, banking and social media, have a common objective for real-time decisions for each transaction, deciding whether to accept, review or reject the transaction. But the each organization individually defines its own business rules to make these real-time decisions.

ThreatMetrix offers a highly configurable system for defining business rules to manage the outcome of each transaction. These rules are primarily based on Persona ID and used to model good, bad and suspicious customers. For example, a business may decide that the instance of fraud greatly increases when a consumer has more than five active email addresses; when those email addresses are less than 30 days old; when that “Persona” has more than five associated devices, (a laptop, mobile phone, office computer); or when the number of IP addresses that consumer has used in the past 30 days exceeds 10.

All of these business rules are evaluated against billions of transactions across the global trust intelligence network.

Examples of global business rules include:

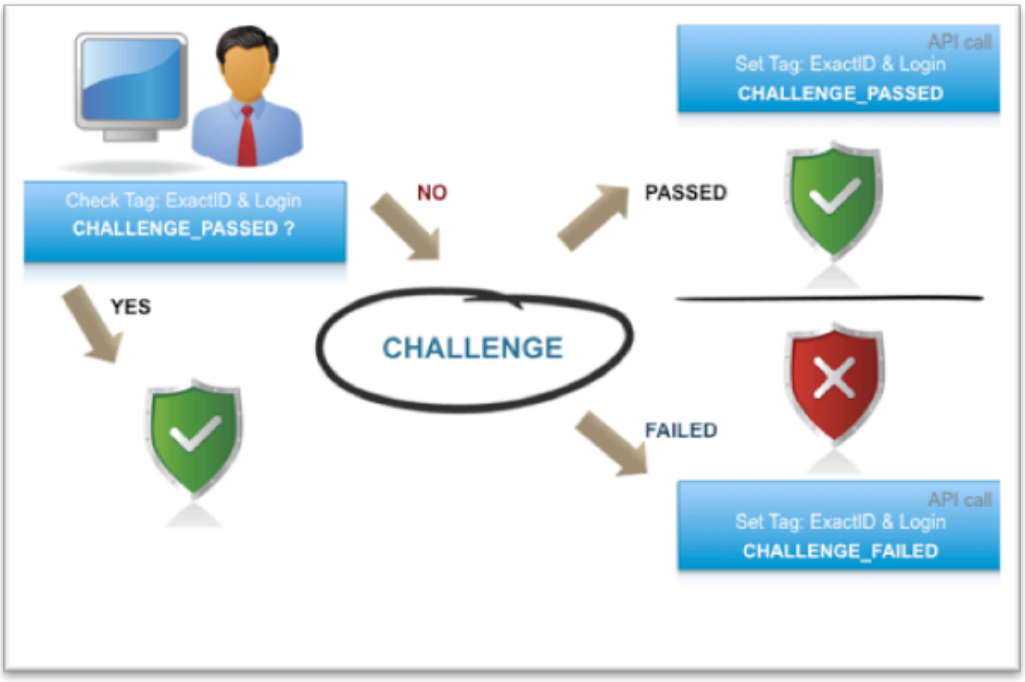
- Exact ID to Smart ID comparison: if a Smart ID is associated with two or more devices, this behavior typically indicates the act of cookie wiping and is highly indicative of fraud.
- Five or more accounts accessed on the same device in a short period of time
- Five or more accounts accessed from the same IP address in a short period of time
- Login/account associated with five or more credit cards
- Device associated with five or more email addresses
- More than three or four purchases across the ThreatMetrix network in an hour

Validate Business Rules

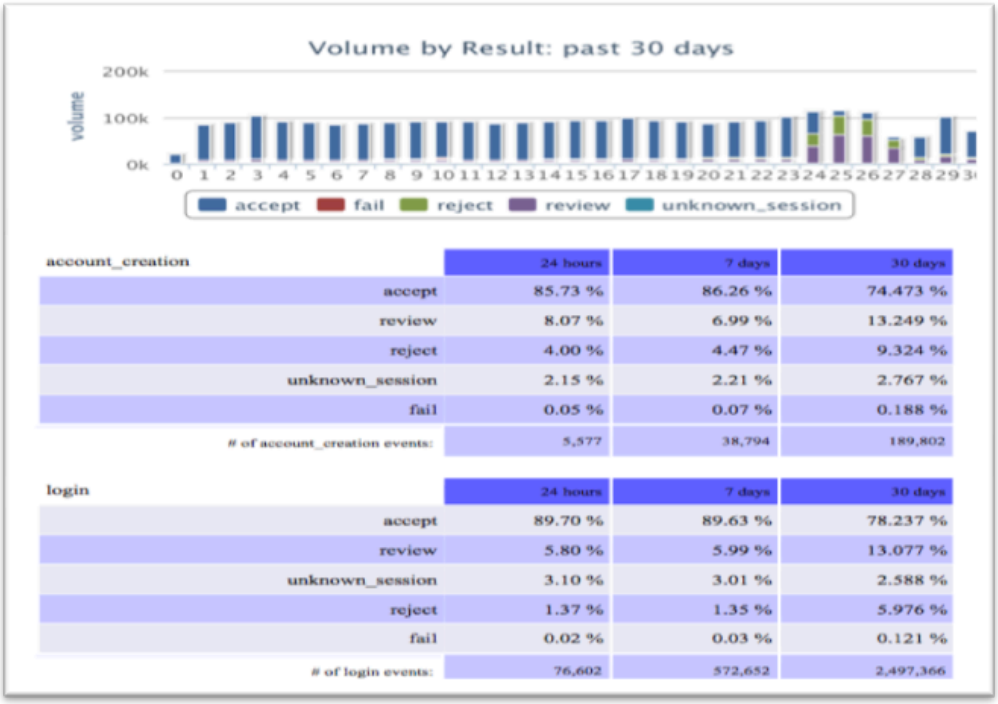
Businesses need to evaluate fraud policies on an ongoing basis. ThreatMetrix provides flexible mechanisms to capture feedback for each transaction. The key objective is to identify and validate genuine customers and reduce friction for these returning customers.

Trust Tags allow customers to validate the past behavior of a consumer in a completely anonymous and passive fashion. TrustTags have the ability to validate any information captured in Persona ID against actual transaction data across the entire ThreatMetrix customer network. Any combination of device, transactional or Persona attributes can be combined to test validity of that consumer behind a transaction.

For example, if a consumer happens to be a new customer for an online banking site, the business may not have a history of the device and persona information. Through policy rules, the online banking site can query Trust Tags on the device and persona attributes across the global network. If the combination of device and attribute has positive Trust Tags associated, the online banking site can authenticate the user with confidence. Alternatively, the online banking site can choose to perform step-up authentication using an out of band provider. Once the consumer is authenticated through this channel, the online banking site can set Trust Tags on the combination of device and persona attributes. This identifies the genuine customer and reduces the need for any step-up authentication when the consumer returns to the online banking site in the future.



Additionally ThreatMetrix automatically scores each transaction based on accept, review and reject status of the policies across global customers. These Persona Behavior Scores provide automated feedback to all businesses in the global network.



account_creation	24 hours	7 days	30 days
accept	85.73 %	86.26 %	74.473 %
review	8.07 %	6.99 %	13.249 %
reject	4.00 %	4.47 %	9.324 %
unknown_session	2.15 %	2.21 %	2.767 %
fail	0.05 %	0.07 %	0.188 %
# of account_creation events:	5,577	38,794	189,802

login	24 hours	7 days	30 days
accept	89.70 %	89.63 %	78.237 %
review	5.80 %	5.99 %	13.077 %
unknown_session	3.10 %	3.01 %	2.588 %
reject	1.37 %	1.35 %	5.976 %
fail	0.02 %	0.03 %	0.121 %
# of login events:	76,602	572,652	2,497,366

Detailed Analysis

ThreatMetrix offers analytical reports with visualizations to enable security and fraud analysts to make better-informed business and policy decisions. These reports deliver summarization and trends that help the analyst detect the different types of cybercriminal attacks and also provide insight for fine-tuning policies

Summary

Cybercrime is an organized business that operates with sophisticated technology and a powerful alliance between hackers and fraudsters. Data breaches resulting in loss of millions of credit card and identity data and fraud perpetuated through account takeovers and card not present are two sides of the same coin. ThreatMetrix protects its customers through a collective response combining the intelligence gathered from billions of transactions in the Global Trust Intelligence Network.

For more information, please visit us at:
www.threatmetrix.com