



Cybercrime Protection

Fraud Prevention

Increase Revenue and Reduce Fraud

November 2013

Trusted User or Cyber Threat?



“On the internet, nobody knows you’re a dog.”

Protecting Over 1,900 Customers

ThreatMetrix™

E-Commerce



Financial Services



Social Networking



Partners



Intelligence Network of 9,000+ Websites

Some Use Cases Online Classifieds

- Filter/Block Advert Placement
- Automated Bidding Monitoring/Prevention
- Identify Buyer/Seller Collusion
- Account Takeover
- Reduce Friction for Returning Customers
- Compliance Requirements
- Criminal Investigation

BRAND REPUTATION



How Can ThreatMetrix Help?

Visitor Intelligence Across Devices

ThreatMetrix™



TrustDefender™ Cloud

Safeguard Online Transactions
and Customer Identities
with Device Identification
and Malware Detection



TrustDefender™ Mobile

Deliver Real-Time Fraud
Screening for Mobile
Applications Using a
Comprehensive SDK



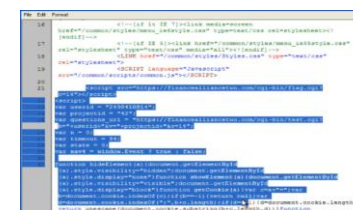
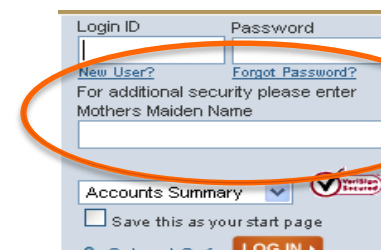
TrustDefender™ Cybercrime Protection Platform



Global Trust Intelligence Network

Endpoint Information Obtained

- Device Profile
 - 150+ Raw Attributes, e.g. platform, browser, screen resolution, timezone, language settings, plugins, etc
 - Device Identification
- TCP/IP Connection Analysis
 - IP Geolocation
 - Proxy Server - Detection and Piercing
 - VPN Signatures
 - Phishing Detection
- Page Profile
 - Verifies integrity of page against Trojans & Man-in-the-Browser (MITB) injection attacks



Global Trust Intelligence Network



Real Example from the Online Classifieds World



How does ThreatMetrix Help?

Step 1 DETECT Device Anomalies

We Start with Comprehensive Device Data Capture



TrustDefender Cloud

- Hidden Proxy
- Web
- Scripted Attacks
- MitB Attacks
- Mobile
- VPN, Proxies
- Mobile Threats
- Secure Client
- Malware

Smart ID

The Foundation...
But You Need More than Device Data for Protection

Anomalies lead to Risk



Device associated with multiple logins



Geo Location



Age of Device



Are proxies being used?



Is this a return device that has wiped cookies?



Velocity of login attempts for a given login



Is the device associated with other blacklisted attributes?



Are there unexpected browser, language or time settings?



of Proxies used by login or device



Past locations the device and login have been used



Is the IP address associated with multiple logins?



Bot or scripted attack

Step 2 EXPAND Profiling

We Add Transaction Insights to Enhance Our Profiling

100's of Attributes to
Define a User



Delivering The Complete Picture of Who Is Visiting Your Site

Trusted Customer Identification is 95% of Fraud Prevention

ThreatMetrix



Step 3 CONFIGURE Business Policies

“Compromised Device”

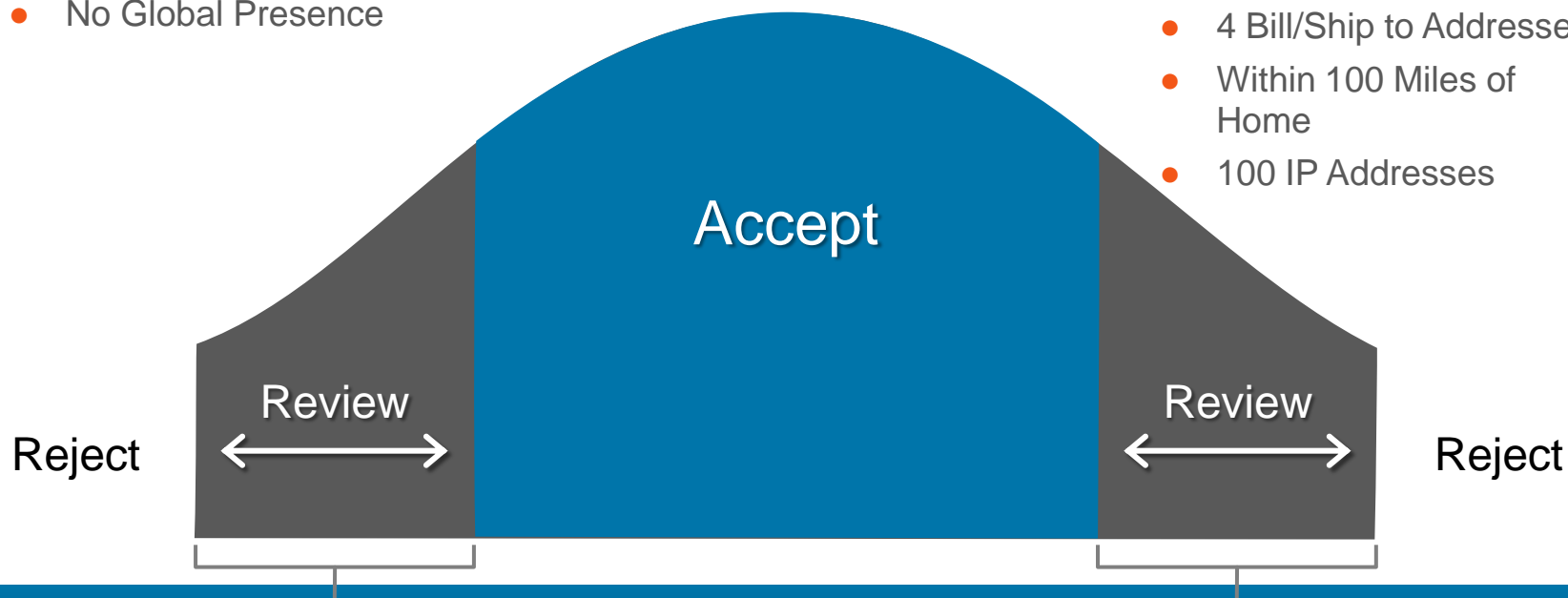
- Windows XP Device
- No Transactional Markers
- No Global Presence

“Trusted Customer”

- Validated Device and ID
- 3 Email Addresses
- 2 Ship to Addresses
- Validated Phone #

“Compromised Identity”

- Windows 7 Device
- 10 Email Addresses
- 4 Bill/Ship to Addresses
- Within 100 Miles of Home
- 100 IP Addresses



VALIDATE Business Policies

ThreatMetrix

We Track User Behavior Across Global Network to Ensure Detection



TrustTags

Anonymous Truth Data

*Does this customer
consistently score well, poorly
or inconsistently?*

Reduce Step-Up Authentication
and Out of Band Authentication

Reduce Friction to Process
Returning Customers



Thank you.

Hassan van de Riet,
Sales Director Europe, Middle East & Africa
has@threatmetrix.com
Tel: +31 70 8200 509