

# ThreatMetrix™ Cybercrime Defender Platform

A Single, Integrated Platform for Protection from Malware and Fraud



## Introduction

The Internet threat environment is changing and escalating, with increasingly sophisticated crimeware toolkits and covert attacks targeting sites and insecure endpoints for financial gain. The potential for financial loss and brand erosion is huge.

While the risk escalates, the number of devices to exploit is multiplying. Consumers and remote employees expect to do online banking with their smartphones or tablets, and login remotely to work from insecure home computers or laptops. Personal devices often lack the security of computers under enterprise control, and are particularly vulnerable to malware.

Online businesses need layered defenses to protect themselves from data breaches and fraud. Essential defenses include:

- Malware detection to identify Trojans, man-in-the-browser (MitB) and other attacks
- Malware protection on endpoint devices
- Device identification to detect and prevent fraud.

A traditional cybersecurity approach using multiple technologies from different vendors is costly, complex and inefficient, requiring integration across technologies and data silos. It is difficult to get a common view of devices and users across all systems. Cybercriminals can slip through the gaps, particularly with attacks using multiple vectors.

## A Unified Platform for Layered Defenses

The ThreatMetrix Cybercrime Defender Platform integrates malware detection and advanced device identification in a single, easy-to-use platform delivered from the cloud. Instead of piecing together multiple solutions and silos of data, the platform delivers a unified view of users and devices, backed by global intelligence. With a unified solution, businesses can protect the integrity of online transactions and identities efficiently and cost-effectively.

The ThreatMetrix Cybercrime Defender Platform gives online businesses the real-time insight and global intelligence context to:

- Protect the integrity of the entire online transaction, from the customer endpoint to the site
- Detect malware in online transactions and give customers tools to eliminate or isolate it
- Detect individuals using stolen credentials leveraging a global network of intelligence, protecting both business data and customers' identities.

## How It Works

The ThreatMetrix Cybercrime Defender Platform integrates the following ThreatMetrix solutions:



**TrustDefender™ ID** is a real-time device identification solution that protects companies against cybercriminals and helps validate returning customers. It gives businesses a crucial first perimeter of defense to protect online transactions, including account creation, login authentication and payment authorization.



**TrustDefender™ Cloud** is a cloud-based, real-time solution that helps companies defend against fraud, malware, MitB and Trojan attacks, and data breaches. It identifies hidden malware that may compromise authenticated sessions to steal data, identities or money.



**TrustDefender™ Client** is a client-based solution that mitigates the risk of hidden malware compromising authenticated sessions to steal data, identities or money. A small client component installed on end-user computers identifies and isolates malware, verifies legitimate websites, protects the online session with the business, and communicates with the business to identify potential fraud.



**TrustDefender™ Mobile** is a software development kit (SDK) that embeds risk intelligence into mobile applications. It creates cross-validating device fingerprints based on hardware, OS and application parameters. Integration with the ThreatMetrix™ Cybercrime Defender Platform offers risk-based, real-time fraud screening for transactions from mobile apps.

**Cybercrime Control Center** is the foundation of the ThreatMetrix Cybercrime Defender Platform. It controls the sharing and processing of information throughout the entire ThreatMetrix global network. In addition to providing global intelligence, it also controls critical functions including: device and risk intelligence, policy-driven defense logic, unified intelligence analytics, and queue management, review, audits and alerts.

# ThreatMetrix™ Cybercrime Defender Platform

## Cybercrime Control Center



### TrustDefender™ ID

Detect online fraud in real-time with cloud-based device identification.



### TrustDefender™ Cloud

Safeguard online transactions and customer identities with cloud-based MitB and malware detection.



### TrustDefender™ Client

Secure devices and remote access sessions against malware threats with a small downloadable client.



### TrustDefender™ Mobile

Deliver real-time fraud screening for mobile applications using a comprehensive SDK.

## Essential Features of the Platform

In addition to the core malware and device identification capabilities, the ThreatMetrix Cybercrime Defender Platform offers the following key features:

**Enterprise Risk Engine:** ThreatMetrix provides real-time contextual scoring based on device, customer and transaction attributes and historic analysis through a configurable rules engine. Default rules and algorithms detect many anomalies, such as hidden proxies, high-risk geographies, anomalous language and time settings, potential cookie wiping and blacklisted attributes. Advanced rules correlate other transaction data, such as detecting an unusually high volume of transactions from a device across the ThreatMetrix network. Analysts can update rules 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 and customizable fraud filters. The ThreatMetrix Cybercrime Defender Platform provides proactive protection that gets smarter with every customer and transaction.

**Queue Management:** Manual transaction reviews are time consuming and expensive. ThreatMetrix allows custom tuning of rules to reduce false positives, and automated assignment of transactions to analyst queues by configurable rules. Analysts can focus on the highest risk transactions, based on score, transaction amount, or criteria such as geographical origin. Analysts can mark transactions as rejected/accepted to improve predictive scoring.

**Customizable Alerting:** Automated alert rules notify an analyst when a transaction meets specified criteria. Alerts can be set based on risk, transaction or device attributes or associated with specific fraud behavior. Alert content can link directly back to the transaction for review.

**Online Portal and Dashboard for Transaction Monitoring and Link Analysis:** An online portal helps analysts review past transactions. A dashboard shows recent high-risk transactions and trends. Advanced search capabilities assist fraud analysts in finding related transactions and discovering links between suspicious activities. For programmatic integration, a real-time API returns device identities, anomaly indicators and risk scores.

**Bulletproof Security and Privacy Protection:** Advanced device identification technology detects and alerts based on suspicious device anomalies. For more powerful fraud analysis, passing transaction identifiers (such as an email address, payment account hash, phone number, etc.) supports further correlation. ThreatMetrix protects these identifiers with encryption and one-way hashing so that the data is never exposed or shared. Role-based permissions and full auditing meet enterprise security compliance requirements.

## Who Uses the ThreatMetrix Cybercrime Defender Platform?

ThreatMetrix solutions are successfully deployed in over 600 customers in industries including e-commerce, financial services, government agencies, healthcare, and other Fortune 1000 organizations. Any organization that must protect the integrity of online transactions or identities can benefit from the ThreatMetrix Cybercrime Defender Platform.

For more information, or to schedule a demo, call **+1-408-200-5755** or email **[sales@threatmetrix.com](mailto:sales@threatmetrix.com)**.

### 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](http://www.threatmetrix.com)**

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