

WHITEPAPER

TrustDefender™ Client

Integrated Endpoint Cybercrime Protection

ThreatMetrix™ Cybercrime Defender Platform



Contents

Overview	3
The Need for an Integrated Endpoint Cybercrime Solution	3
Two-way Authentication	3
Network Access Control Software	4
Endpoint Security Software	4
Secure Browsing	5
No Integration of Client Security and Backend Policies	5
Introducing TrustDefender Client	6
Mutual Authentication for True Secure Communication	6
Secure Lockdown	7
Client-side Integrity Checking and Policy-based Access Control	7
Advanced Malware Forensics and Detection	8
Safe & Secure Mode for Complete Malware and Rootkit Protection	9
Zero-impact Remote Installation	9
Silent and Self-help Modes	9
Cloud-based Policy Configuration, Risk Scoring, Alerts and Analytics	10
ThreatMetrix Cybercrime Defender Platform for Integrated, Cost-Effective Protection	11
Conclusion	11

Overview

TrustDefender™ Client is a small download that goes beyond securing the browser to provide an integrated endpoint protection solution that stops malware and man-in-the-browser (MitB) Trojans without impacting performance and productivity. As an integrated component of ThreatMetrix™ Cybercrime Defender Platform, it provides a next-generation online transaction and access security solution specifically designed to meet the needs of consumers and employees while enabling financial institutions, banks, brokers and online businesses to secure online transactions and access in real-time – using any device, anywhere in the world – to effectively lock out online criminals.

The Need for an Integrated Endpoint Cybercrime Solution

On the Internet a transaction can only be as secure as the device from which it originates. Today a number of legacy endpoint solutions exist including antivirus, access control, secure browsers and software tokens, but to date no offering provides integrated endpoint protection with cloud intelligence to provide comprehensive cybercrime protection for online transactions and access.

The following section provides an overview of existing endpoint protection technologies and their advantages and limitations.

Two-way Authentication

Phishing attacks are only possible on the public Internet today because there is yet no broadly adopted method of reliably authenticating a user to a trusted and secure web service, and the web service to a trusted and secure user. Even if a website uses SSL certificates and the customer correctly types in the correct domain name, malware can change the .hosts file on the client device to point the domain to a hacker's IP address hosting a phishing site.

Similarly, even if the online enterprise validates the user's login and password, there is no guarantee that they aren't the same credentials being replayed from the aforementioned attack. Two-way authentication solutions, when correctly implemented, ensure that the client knows that it is connecting to the correct and valid service and the online business is assured that it is communicating with a known, trusted client. Example providers of two-way authentication software include ActivIdentity and Entrust. Unfortunately, while two-way authentication does address the problem of mutual trust, it does not in itself assure that either the trusted client or online service is secure.

Network Access Control Software

Network Access Control (NAC) technologies pioneered by companies such as Cisco and Microsoft are an extension of endpoint and network perimeter protection solutions for corporate and government networks. While NAC can incorporate some form of mutual authentication, it goes a step further and recognizes that even trusted computers can turn bad. NAC technology tries to manage this risk by ensuring that the endpoint's security state, or posture, is in compliance with a defined set of policies.

For example, before a computer is granted access to servers on the network, the NAC policy verifies that a firewall is enabled, disk drive encryption is in use, the latest OS patches have been installed and antivirus systems are up to date. If the device is found to be out of compliance it can be quarantined to a guest network that does not have access to corporate servers.

While NAC provides for finer-grained access control to resources on a network, it is not a malware solution, does not protect against credentials being stolen and does nothing to secure customer transactions and access against cybercrime. The biggest contribution that NAC has advanced is the recognition by the largest operating system and router vendors that effective security must extend beyond authenticating credentials that are easily stolen to include device identification and verification of risk.

Endpoint Security Software

Companies such as Symantec and McAfee sell integrated endpoint security suites that provide spyware, antivirus and firewall functionality. Potentially providing a false sense of security, these technologies primarily rely on signatures that regularly become outdated. Crimeware is now open-sourced and polymorphic, meaning zero-day attacks are commonplace. With malware injection attacks targeting reputable websites, there is truly no safe place to surf on the web. Once a computer has been rooted by sophisticated malware, it can be very difficult if not impossible to remove, leaving dormant zombie machines that can be woken back into action at the bidding of a remote command and control computer. Sites like Virustotal.com that compare malware detection rates across antivirus vendors clearly demonstrate that while endpoint protection is necessary, no single vendor or technology is sufficient to stem the cybercrime tsunami.

Even if endpoint protection could be made 100% effective, it doesn't protect the user's identity, credit card and banking details from being phished or leaked from any number of websites on which this data may be stored. Unless websites themselves are armed with cybercrime intelligence to differentiate between a customer and a cybercriminal, or differentiate between trusted and compromised computers, the problem will continue to escalate.

Secure Browsing

Prevx and Trusteer are examples of companies that offer secure browsing technologies. Secure browsing technologies work by shielding transaction and identity details entered into a browser, typically by encrypting keystrokes, from malware installed on a computer. As part of a layered security strategy these browser-hardening technologies provide valuable protection from malware that can bypass device identification and two-factor authentication technologies by intercepting one-time passwords and changing transaction amounts and payees on the fly.

Unfortunately, the heavy resource-intensive nature of approaches that rely on encryption have seen consumers complain and opt-out due to performance issues and bugs associated with browser updates and releases. Being tied to the browser also means that maintaining compatibility with all browser and platform configurations is virtually impossible. For example, Safari on Mac OS X may be supported but not Chrome. The reason why man-in-the-browser Trojans are so effective and widespread is that they use JavaScript injection in order to be 100% cross-browser compatible.

Regardless of the technology used, another limitation of secure browsing technologies is that they require a download which some proportion of customers or employees can't or won't be able to install due to incompatibilities, lack of smartphone support, non-compliance with corporate standard operating systems, or simply lack of trust ingrained from learning never to download software from the Internet. Secure browsing is also not a solution for online payments or new account enrollments where there is not an existing trust relationship between the user and the website.

No Integration of Client Security and Backend Policies

With such a huge variety of client environments, no system is the same. However, no website provider can effectively distinguish between a "good" computer and one that is compromised. Therefore the website cannot provide adequate protection for its customers who need additional security. Current backend policies are limited by the fact that they don't include any client security parameters.

Introducing TrustDefender Client

TrustDefender Client is a Windows and OS X downloadable component of the ThreatMetrix Cybercrime Defender Platform that covers all the key requirements of an effective endpoint solution for online transaction and access security:

1. Mutual authentication for secure communication
2. Client-side integrity checking and access control
3. Advanced malware forensics and detection
4. Secure lockdown for complete malware and rootkit protection
5. Zero-impact remote installation
6. Silent and self-help modes
7. Cloud-based policy configuration, scoring, alerts and analytics
8. Integrated device identification, transaction integrity verification and anonymized shared intelligence

Mutual Authentication for True Secure Communication

Unlike SSL and HTTPS that only provide limited domain authentication, TrustDefender Client protects both the client device and the online organization to provide true secure communication. The online organization (e.g. an online bank) provides the following information that is stored in a ThreatMetrix client policy database and verified by TrustDefender Client during any attempted communication:

- One or more hostnames/URLs
- One or more SSL certificate fingerprints
- One or more IP addresses/ranges

Once installed, TrustDefender Client analyzes all outgoing connections and detects when the device is connecting to a service protected by ThreatMetrix. At the same time, and prior to completion of the outgoing TCP-handshake, TrustDefender Client will upload the anonymized TrustDefender Client user ID, encrypted hardware fingerprint, connection fingerprint details and other client security parameters to be evaluated by the enterprise policy engine.

Secure Lockdown

Through the client policies described above in mutual authentication, the TrustDefender Client can effectively distinguish between Internet requests that belong to the current web service (e.g. your online bank) and any unrelated Internet requests (e.g. stolen data sent to a Command & Control server). Secure lockdown, enabled by the enterprise policy, will block all untrusted Internet requests by default.

Imagine the case of an online bank that is using two-factor authentication. Any client side attack will need to send the one-time-password to the hacker immediately and before they are sent to the bank. The secure lockdown will provide an effective protection against any of these session-based attacks.

Client-side Integrity Checking and Policy-based Access Control

Unlike traditional Network Access Control services, TrustDefender Client gives an enterprise a single integrated view of both employee and unmanaged consumer devices.

As part of the mutual authentication handshake described above, a securely signed XML file containing information about the device's security state is uploaded using an encrypted HTTPS Post Request for evaluation by the enterprise policy engine. This XML file contains essential anonymized forensics information and gives the enterprise visibility into the following types of information:

- Is a client antivirus engine active?
- Is the client antivirus up-to-date?
- Is Windows Update turned on?
- When was the last successful Windows Update?
- Is the firewall enabled?
- Suspected malicious software detected?
- Known malicious software detected?
- Can user override security policies?
- Has user overridden security policies (e.g. proceeds with transaction)?
- Is the location of the device consistent?
- Has the device fingerprint been tampered with?
- Has the Security XML file been tampered?
- Is this a new device for the user?
- Does the device have disk drive encryption enabled to ensure compliance with federal regulations?

Advanced Malware Forensics and Detection

TrustDefender Client provides the most advanced malware and rootkit detection available on the market today. At its core, the Kernel Forensics Engine will ensure that any system anomalies and traces will be picked up, even for attacks that are unknown at the time. It succeeds in this claim because it is integrated deeper into the client operating system, is transaction aware, and uses a globally maintained whitelisting approach so it is not susceptible to zero-day attacks like traditional antivirus solutions.

Rather than taking a heuristics or blacklist approach to analyzing files and executables, TrustDefender Client – through the global ThreatMetrix Cybercrime Defender Platform – understands valid system-level state information of the operating system, applications, processes and plugins while a transaction is being conducted. Because it is not tied to the browser, TrustDefender Client provides more complete and thorough protection across all the applications that customers and employees use to interact with an enterprise. Proprietary integrity checks performed by TrustDefender Client include:

- Detection of hidden applications used to circumvent antivirus scanners using its Usermode Rootkit Scanner
- Detection and verification of active kernel drivers against a globally maintained trusted signature list
- Detection of hidden kernel drivers by independently verifying information obtained from the operating system using its Kernel Rootkit Scanner
- Detection of malicious malware injections that have hooked at either userland (e.g. malicious browser helper object) or kernel level (e.g. keylogger)
- Detection of any system anomalies through its Kernel Forensics Engine
- Detection and verification of inbound and outbound connections

Unknown signatures belonging to new malware or untrusted applications/plugins are automatically uploaded for evaluation by ThreatMetrix malware forensics experts and classified accordingly. The enterprise is also armed in real-time with the necessary information to reject, warn or challenge the user, based on the knowledge that the user's device is in an untrusted state.

Safe & Secure Mode for Complete Malware and Rootkit Protection

TrustDefender Client goes beyond malware detection to actively protect both the user and the online enterprise via its “Safe & Secure” mode that can be automated or optionally confirmed by the user during a transaction or login.

TrustDefender Client will not directly uninstall any malware, as there may not be any contractual or legal rights to do so. Instead it temporarily disables all known malware and untrusted processes, plugins and connections immediately prior to and during the transaction or login by using sophisticated memory forensics, CPU management, packet interception and other isolation techniques. All malware is effectively rendered deaf, dumb and blind and starved of resources while allowing the user to safely and conveniently proceed with the transaction. In this way, TrustDefender Client complements antivirus software that will hopefully eventually remove the Trojan once its signature has been reverse engineered.

Unlike alternatives, TrustDefender Client attacks the malware problem at its core by recognizing and disabling the malware itself instead of relying on band-aid patches to the browser, keyboard and screen as new exploits are found.

Zero-impact Remote Installation

TrustDefender Client is an executable, small enough to be downloaded over dialup and unlike alternatives, does not require the user to restart their computer or browser or abandon their attempted transaction. Furthermore, it doesn't rely on administrator privileges and can also be installed without them.

TrustDefender Client can either be installed manually (e.g. for a remote worker) or via HTML scripts placed on appropriate pages on the website. The download scripts automatically detect whether the TrustDefender Client is already installed and will prompt new users to download TrustDefender Client. Depending on the operating system and browser version detected, either an ActiveX, JAVA or Click-Once loader is used.

Silent and Self-help Modes

Based on the enterprise policy configuration, the organization has complete control of the user's experience and participation in remediation, if any. For example, the enterprise may insist that all employees remedy any found anomalies before proceeding with a login to the corporate VPN while automatically activating Safe & Secure mode for customers without any user notifications. If the user is notified, TrustDefender Client provides the option for self-help “Fix-it” advice that is

tailored to the user's device and configuration and the particular issue at hand. ThreatMetrix maintains this service and keeps helpdesk support affordable while re-enforcing the enterprise's trust relationship at the moment of truth – before the user discloses their confidential and personal information and not after. By involving users in the active resolution of their compromised devices, TrustDefender Client customers have seen the added benefit of a steady reduction in the total number of at-risk devices and transactions that need to be screened.

Cloud-based Policy Configuration, Risk Scoring, Alerts and Analytics

TrustDefender Client provides centralized intelligence and control through the cloud-based ThreatMetrix Cybercrime Control Center.

The Cybercrime Control Center allows custom configuration of both endpoint and application behavior based on the assessed risk of the device and transaction:

- Integrate real-time risk scores, reason codes and attributes into existing 3rd party authentication and authorization applications via a secure web API. More than 40 configuration security attributes from the user's device are available to combine with transaction and user screening via a configurable rules engine.
- Enforce security policies to make sure that computers have no malware detected, or that Safe & Secure Mode is active before connecting to private networks. Devices that don't comply can have access to the application blocked remotely.
- Enable Silent Mode for retail consumers wanting a transparent security experience.
- Enforce the use of a minimum level of a vendor-neutral security software, such as maintaining an up-to-date virus engine and Windows patches.
- Send notifications to individual account owners and/or administrators. These notifications can be configured for individual events or for trending analysis such as a spike in suspicious activity.
- Customize risk thresholds based on the type of transaction being performed, such as the transactions exceeding \$5,000 in a day or \$15,000 in a given month.

The ThreatMetrix Cybercrime Control Center also delivers powerful insights into the vulnerabilities and risk characteristics of connecting devices to help visualize the state of security of all end users regardless of customer or employee. For the first time, online enterprises can develop more effective cybercrime protection strategies by having a realistic understating of their true threat landscape:

- Percent and number of customers with TrustDefender Client installed
- Percent and number of malware infected machines
- Percent and number of machines with suspicious/untrusted processes
- Percent and number of protected sessions/transactions
- Percent and number of phishing attacks attempted
- Trend of infected machines over time
- Percent and number of devices with firewalls disabled
- Percent and number of devices with antivirus out of date
- Distribution and usage of antivirus and firewall products
- Distribution and usage of browsers and versions

ThreatMetrix Cybercrime Defender Platform for Integrated, Cost-Effective Protection

A key reason why criminals are always able to slip through defenses is the large number of disparate technologies and vendors that enterprises are forced to bear the cost and complexity to integrate. One system is deployed for screening devices, another for transactions, another for authenticating customers and yet another for its employees. It is difficult to get a common view of users across all systems and virtually impossible to identify returning cybercriminals across channels on one site, let alone across a consortium of sites sharing fraud intelligence.

TrustDefender Client is an integral part of the ThreatMetrix Cybercrime Defender Platform, which offers the following complementary products to protect customers and employees across payments, logins and enrolments:

- TrustDefender™ ID: TrustDefender ID is a cloud-based, real-time cookieless device identification solution that protects companies against cybercriminals and helps validate valuable returning customers. TrustDefender ID provides integrated shared reputation intelligence and identity verification to provide businesses with a crucial first perimeter of defense to protect online transactions including account creation, login authentication and payment authorization.

- **TrustDefender™ Cloud:** TrustDefender Cloud is a cloud-based, real-time solution that helps companies defend against fraud, malware, MitB and Trojan attacks, and data breaches. It mitigates the risk of hidden malware compromising authenticated sessions to steal data, identities or money the first-time, every-time.
- **TrustDefender™ Client:** TrustDefender Client provides malware protection without a performance hit. 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:** TrustDefender Mobile is an embeddable SDK for smartphone applications that creates cross-validating device fingerprints based on hardware, operating system and application parameters normally hidden from remote servers. In conjunction with TrustDefender ID's cloud-based device identification technology, TrustDefender Mobile provides bulletproof cross-platform authentication and fraud prevention without leaking personal information.

Conclusion

In this age of cybercrime, if a device is compromised, then by definition so is the transaction or login session. Online enterprises need cost effective, integrated endpoint cybercrime protection for both customers and employees. TrustDefender Client, integrated with the ThreatMetrix Cybercrime Defender Platform, provides the most complete, comprehensive and affordable solution available on the market.

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

EMEA Headquarters:

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

www.threatmetrix.com

www.threatmetrix.com/fraudsandends