Trusteer

Trusteer Rapport for Online Banking Explained

White Paper

*new threats, **new thinking***

Trusteer

Table of Contents

Trusteer

About This Document

This document is intended for Security Architects and Product Managers interested in evaluating Trusteer Rapport for Online Banking, an advanced software solution that protects endpoints against financial fraud perpetrated by malware and phishing. This document provides a solid understanding of how Trusteer Rapport actively protects endpoints and the supporting Trusteer services that make it an effective fraud prevention tool.

Trusteer Rapport for Online Banking Overview

Trusteer Rapport provides instant PC and Mac anti-fraud protection for financial institutions' clients. Trusteer Rapport protects against financial malware (e.g. Zeus, SypEye, Timba, Carperb, Shylock, and others) as well as phishing attacks.

Preventing Financial Malware Based Fraud

Multi-layer protection against known and unknown financial malware is enabled by leveraging two security mechanisms: **Application Protection** and **Algorithm Inspection**. These mechanisms complement one another to prevent fraud, **Algorithm Inspection** detects, blocks and removes known threats by identifying malicious algorithms running in memory while **Application Protection** secures the browser against any malware, identifies suspicious attempts to bypass security and sends threat information to Trusteer Intelligence for analysis – turning zero-day threats to known threats.

Preventing Phishing Based Fraud

Anti-phishing protection is an additional level of security including two main protection mechanisms to **prevent credential loss to suspected phishing sites** and **block access to known phishing sites**.

Product Components

Trusteer Rapport includes the following components:

Software Agent: The Software Agent is a small executable program which is downloaded and installed on the client's computer. The agent is the actual component that secures the computer from malware and phishing attacks.

Enforcement API and HTML Snippet: The HTML snippet is a piece of code that can be integrated into online banking applications to allow integration with the Enforcement API on the Trusteer Cloud. The API and Snippet allow the banking application to identify whether the end user has the Trusteer Rapport Software Agent installed, and if not, enforce download and installation of Trusteer Rapport on computers as optional or mandatory deployment.

Trusteer Management in the Cloud: Trusteer provides cloud-based management, analysis, alerting, and reporting service. The service includes:

- Automated software and configuration updates to all Trusteer Rapport agents.
- Actionable alerts on endpoint security health, and on malware and phishing attacks.
- Management console with customizable out-of-the-box reports, dashboards, and customer-controlled configuration settings.
- Repository of security events from Trusteer Rapport agents. Events can be analyzed to detect emerging threats.
- Secure Authentication enabled Web-based access to ensure that only authorized staff can access data and change configurations.

Application Protection (Browser Protection)

For online banking customers, Trusteer Rapport's Application Protection is applied on the web browser and is referred to as Browser Protection. The concept behind Browser Protection is simple: isolating the browser from malware that may reside on the computer. Browser Protection locks down all the interfaces that potentially allow malware to access the browser and access sensitive data. This is true zero-day protection against malware attacks. Browser Protection assumes that the malware is unknown and, instead of trying to detect it, locks down access to the browser so any malware is unable to access sensitive information.

Browser Protection locks various interfaces: the ability to log keystrokes that are sent to the application, the ability to take screenshots of the application, the ability to tamper with the application's memory, and more. Protecting the browser prevents login credential theft, information theft, and session tampering such as injecting or modifying transactions.

Trusteer's Application Protection technology is not only capable of protecting the browser but is also capable of detecting new zero-day malware attacks. Trusteer Rapport's Application Protection technology controls all access points to the browser including memory access, API access and access to the keyboard driver. While the customer is browsing to a financial institution's web application all these access points are shut down, preventing malware from accessing information or tampering with information. When a certain software component tries

to go through one of these access points during a connection with the web site, Trusteer Rapport logs the attempt and is also capable of capturing a sample of this software component based on what it actually tries to do in the browser. This information is sent to Trusteer for analysis. Automated cloud services process this information and flag suspicious software components to Trusteer's security group. These suspicious software components are then analyzed by Trusteer's malware analysts who are capable of detecting new types of malware. Using this process Trusteer was the first to detect most new financial malware attack in recent years including Oddjob, Bugat, Ramnit, Sunspot, and Shylock, all first discovered and named by Trusteer's security group.

Below is a list of the different restrictions that Browser Protection applies on client applications:

- Anti-keylogging
- Anti-screen capturing
- Man-in-the-Browser - Process Tampering Prevention
- Man-in-the-Browser - Malicious browser add-ons protection
- Man-in-the-Browser - Browser DOM access protection
- Man-in-the-Middle protection

Anti-Keylogging

A keylogger can reside either in user-space or in the operating system's kernel. User-space keyloggers are the most common type of keyloggers.

User-space keyloggers capture keystrokes by using one of the following methods:

- Subscribing to Windows events related to keyboard activity. These events occur when a key is pressed, resulting in internal Windows messages.
- Directly performing asynchronous sampling of each and every key in the computer keyboard, using a Windows keyboard interface. This method allows the keylogger to determine the state of each key, and to therefore ascertain the text typed on the keyboard.

Kernel-level keyloggers implement a keyboard filter driver to capture keystrokes between the keyboard driver and user-space.

To prevent keylogging, Trusteer Rapport encrypts keystrokes from the keyboard driver to the client application window. Keystroke encryption is effective against both user-space and kernel-level keyloggers.

The keystroke encryption layer integrates with the operating system's interrupt layer. It creates a secure and encrypted channel between the keyboard driver and the client application. Whenever the user generates keystrokes, Trusteer Rapport copies the keystrokes into the secure channel and replaces the original characters with arbitrary characters. When the arbitrary characters arrive at the client application presented on the user's screen, Trusteer Rapport replaces them again with the real characters that arrived through the secure and encrypted channel.

With keystroke encryption, active kernel-level and user-space keyloggers receive arbitrary characters, not the real characters. Keyloggers cannot access the secure and encrypted channel, and do not have access to the real characters that the user typed.

The secure and encrypted channel terminates in two different places. For most keystrokes, Trusteer Rapport terminates the channel and returns the real characters when they enter the client application. This is done to allow the client application to present the real characters to the user.

The second termination point is in the WinInet component, and is used when the user types passwords into a browser. WinInet is an operating system component that generates the SSL connection with the website. When the user types a password, Trusteer Rapport creates an encrypted channel between the keyboard driver and WinInet. This means that even while in the browser, the password is encrypted. If malware bypasses Trusteer Rapport's Man-in-the-Browser protection and accesses the password inside the browser, the password is encrypted and therefore cannot be read by the malware. As WinInet is the SSL termination point, it also means that the password is encrypted (with the SSL certificate) from the keyboard all the way to the website. Trusteer Rapport encrypts the password from the keyboard driver to WinInet and WinInet generates an encrypted SSL connection with the website, and then can transmit the password or other data to the application at the financial institution.

Application Protection also protects the running browser networking component (WinInet) itself, thus keeping the information protected from injection at any given time until it's safely submitted over SSL to the web application.

Anti-Screen Capturing

Trusteer Rapport prevents automated tools from capturing the browser screen. This is done by controlling operating system API calls which are used to capture screens. When an application tries to capture the screen, Trusteer Rapport checks whether sensitive information is presented, and if so, prevents the screen capture attempts and returns a black image instead.

Trusteer Rapport also protects against malware which tries to capture the screen by synthetically generating the Print Screen keystroke. Whenever a Print Screen keyboard event arrives and a sensitive web application is presented, Trusteer Rapport displays a message to the user asking to confirm that the user is really trying to capture the screen. The user must positively confirm for the screenshot to be taken.

Man-in-the-Browser - Process Tampering Prevention

Process Tempering is used by many notorious malware such as Zeus and SpyEye. Using this technique, the malware patches specific application functions in memory, and injects its own code into these functions. Once patched, the malware operates inside the application's process, and whenever the application calls the patched function, the malware code runs and has full access to all the information inside the application.

In-memory function patching is a well-known technique. Any application can access other applications' memory and look for functions. When the function is found, it is possible to override it with a different code. The malware can override the beginning of the function with its own code. The malware can also make sure that the code, which was overridden, runs when the malware code completes its execution. Function patching might sound complicated, but it is actually very easy to do. There are many code samples, as well as freeware and commercial tools that make it very simple to patch various functions inside the browser or one of its components (such as WinInet).

Trusteer Rapport constantly monitors browser functions. Whenever an attempt is made to override such functions, Trusteer Rapport intercepts it and analyzes it. If Trusteer Rapport is unfamiliar with the patch, it removes it and sends it to the Trusteer Intelligence Cloud for analysis. Some legitimate software use function patching to hook applications such as the browser. Known function patches are usually performed by antivirus solutions to control certain browser functions. Trusteer Rapport includes a white-list of legitimate patches (Fortunately, there aren't many of them.), and allows these patches to persist. The cloud service runs intensive tests on each patch, and can determine if a patch is legitimate. The cloud can then instruct Trusteer Rapport whether to allow this patch or remove it.

Man-in-the-Browser - Malicious Browser Add-ons Protection

Browser add-on technology allows adding of software components into the browser. These add-ons can control everything that occurs within the browser. Add-ons add features to the browser including toolbars, animated mouse pointers, stock tickers, and pop-up ad blockers. Many add-ons come from the Internet and require the user to authorize their installation. Some, however, may be installed without the user's knowledge. Although this technology was created to add useful features to the browser, it is widely used by attackers to perform malicious activity such as stealing sensitive information, injecting transactions into authenticated sessions and changing information viewed by the user.

To defeat malicious add-ons, Trusteer Rapport controls the interface between the browser and the add-ons, and acts as a filtering proxy between them. The browser and add-ons communicate through Trusteer Rapport, which "mediates" all requests and responses.

Trusteer Rapport intercepts the browser's attempt to load an add-on, and presents itself to the browser as the add-on. Consequently, the browser loads a Trusteer Rapport component instead of loading the actual add-on. Trusteer Rapport then loads the requested add-on by calling the add-on initialization function, and becomes a proxy between the two.

An add-on can subscribe to browser events. However, as it does not have direct access to the browser. The add-on actually subscribes to Trusteer Rapport, which in turn subscribes to the same events in the browser.

During the user's session, the browser initiates events (such as form submissions, URL navigations, and document load/unload). These events reach Trusteer Rapport, but do not reach the add-on. Trusteer Rapport decides in real-time whether to forward the event to the add-on. The decision is based on parameters such as

the website's domain name, the current URL, the current form, the event type, and most importantly, the add-on ID and add-on signature.

An add-on may also attempt to access the browser (for example, by reading from or writing to the DOM). However, since it does not have a direct pointer to the browser object but rather to the Trusteer Rapport object, Trusteer Rapport can decide whether to allow the add-on to perform this action. The decision is based on parameters such as the website's domain name, the current URL, the add-on ID, the add-on signature, and the requested action (read/write access, specific sub-object, location, etc.).

Trusteer Rapport also incorporates black-lists and white-lists of add-on signatures and IDs. The default policy is to allow properly signed add-ons, as well as white-listed add-ons (i.e. well-known add-ons), while blocking all others.

In summary, Trusteer Rapport enables granular access control over what add-ons can do when the user navigates to a protected website. All add-ons are allowed to load and function normally, as long as the current website is not protected. Once the user browses to a protected website, Trusteer Rapport protection initiates, and based on the selected policy denies add-on access to the browser.

Man-in-the-Browser - Browser DOM Access

Add-ons are not the only way to communicate with the browser. The same API used by add-ons to control the browser is available to any program on the user's computer. Malware can easily retrieve a reference to the browser, and use this reference to access the browser's Document Object Model (DOM) and browser APIs.

Trusteer Rapport's protection against external DOM access is very similar to its protection against malicious add-ons. Trusteer Rapport controls the API calls which are used by external applications to get a reference to the browser. When such an attempt is made, Trusteer Rapport returns its own reference to the requesting application, and then connects itself to the browser. Effectively, Trusteer Rapport acts as a filtering proxy between the requesting application and the browser. The requesting application and the browser communicate through Trusteer Rapport, which mediates all requests and responses and follows the same logic it applies for malicious add-ons.

Man-in-the-Middle Protection

In a Man-in-the-Middle (MITM) attack, the attacker redirects the communication between the client application and the target web servers. Under this attack, the client application is connected to the attacker and the attacker forwards the communication to and from the application servers. In MITM attacks, the end user is unaware that the communication passes through the attacker's systems.

MITM attacks have the following two implications:

- **Eavesdropping:** While sitting between the browser and the genuine servers, the fraudster is exposed to the communication and can read sensitive information sent by the servers to the end user, as well as sensitive information sent by the end user to the servers. This includes login information (e.g., usernames and passwords), and transaction details (account and payee).
- **Fraudster's Ability to Change Traffic in Both Directions:** The fraudster can change web pages the user is viewing. For example, the attacker can replace banners and messages that appear on the website, or even change the account balance that the end user sees in an online banking site. From the end user to the website, the attacker can change transactions and orders. For example, when the end user asks to transfer $50,000 to a certain payee, the attacker can change the transaction to transfer $100,000 to a different payee.

To execute a MITM attack, the attacker needs to force the end user's browser to redirect traffic to the attacker's site. This can be achieved using three main tactics, all of which are addressed with Trusteer Rapport protections:

- **Real-time Phishing Tactics:** The end user receives a fraudulent email with a fake link that directs to a fraudulent website. The end user clicks the link and is connected to the attacker's website. The attacker forwards the communication to the real website and acts as a relay between the end user and the website. In this scenario, the browser's address bar shows a different address than the website's real address. Assuming that the end user clicks on links in unsolicited emails, and that the end user does not notice the fake URL in the browser, this attack can succeed.

  See Phishing Protection

- **DNS Hijacking/Poisoning:** DNS hijacking, or poisoning, is a process in which DNS entries for a certain domain name are modified, thus translating the DNS address into bogus IP addresses. As a result, the attacker can receive sensitive traffic such as user, password, PIN, and transaction details. The attacker can proxy this traffic back to the financial institution while recording the data or inserting fake login screens to collect sensitive login information.

  An unauthorized change of DNS entries can be achieved in many ways. For example, the attacker can hack into a DNS server such as the one used by the user's ISP or can hack into a wireless router and change entries there. Another common method is modifying the "hosts" file on the user's PC. This file, which contains a local set of URL-to-IP address translations, can be changed by malware to direct the user to the IP address of the fake website.

  Trusteer Rapport allows financial organizations to configure the IP address ranges associated with their domain. When a user tries to access the web application, Trusteer Rapport checks the IP address to which the computer intends to connect. If the IP address is not included in the range of authorized IP addresses, Trusteer Rapport generates a new DNS query to a trusted DNS server. This trusted DNS server can be configured by the organization. Trusteer Rapport then forces the computer to send the traffic to the IP address, receiving the traffic from the trusted DNS query, instead of to the original IP address.

When the end user tries to access a protected website using HTTPS, Trusteer Rapport examines the certificate (in parallel to the Browser). If the certificate used by the Browser does not match the certificate identified by Trusteer Rapport the user is alerted.

Algorithm Inspection

Application Inspection effectively detects polymorphic malware strains such as Zeus, SpyEye, and Dark Comet. Polymorphic malware is the biggest problem anti-malware solutions face today. Cybercriminals who develop malware tools put a lot of effort into building kits that are capable of automatically generating an unlimited number of variants for the same malware. Each variant has a different file footprint and signature, which makes it extremely hard for anti-malware to detect. Malware installation and infection detection through identification of out-of-profile application behaviors have proven to be extremely inaccurate. Malware authors are very careful not to include unique behaviors that could trigger anti-malware solutions. They use programming interfaces and techniques which are common to all programs.

Trusteer Rapport's Algorithm Inspection offers a real breakthrough in malware detection and removal. Instead of looking at files and file behaviors, the Trusteer research center conducts a full reverse engineering process on each malware strain. The output of this reverse engineering is the actual algorithm used by the malware. Algorithms are unique to malicious applications, and as such the algorithms can be considered as the malware's "Programmable DNA". While cybercriminals can automate the creation of file variants, it's impossible to automate generation of different algorithms. Trusteer has developed and incorporated an Algorithm Inspection Engine (AIE), which allows inspection of file execution and identifies specific algorithms running in memory. Once Trusteer reverse engineers a malware strain and reveals its algorithm, it uses Algorithm Inspection Language to describe the algorithm to the Trusteer Rapport's Algorithm Inspection Engine. The new algorithm is then communicated from the Trusteer cloud to all Trusteer Rapport instances.

The Algorithm Inspection Engine (AIE) is the heart of Trusteer Rapport's Algorithm Inspection technology. AIE is a micro virtual machine capable of running pieces of code and sanitizing their algorithm. This technology is a result of many years of research and is radically different from any other anti-malware technology available today.

The effectiveness of Trusteer's Algorithm Inspection technology has been proven over hundreds of installations and millions of end users. The product has been consistently tested by various independent 3rd parties and was found to block 100% of financial malware, including zero-day malware created by the 3rd party. In March 2012, Mandiant (a malware research firm) independently collected financial malware samples, such as Zeus, SpyEye, Bugat, Carberp and Shylock and tested them with Trusteer Rapport. The results indicated that Trusteer Rapport neutralized all 25 banking Trojans with a 100% success rate.

In February 2012, MRG (a security research firm) conducted multiple test comparing various tools in the market, and in all cases found Trusteer stopped 100% of malware attacks while none of the other solutions were able to stop all attacks.

Tests performed by leading research firm S21sec in February 2011 concluded that Trusteer Rapport successfully identified 100% of over 300 Zeus samples tested, confirming the power of the Trusteer technology.

While other anti-malware solutions need millions of signatures and behavioral rules to fight malware, Trusteer is capable of providing 100% protection against malware and with just a single Algorithm Inspection rule for each malware family. Trusteer Rapport's Algorithm Inspection technology is capable of addressing a long list of malware strains that have already been reverse engineered by Trusteer's Intelligence Center.

Trusteer Rapport's Algorithm Inspection technology is used for three main purposes:, preventing malware installation, preventing malware download, and removing already installed malware, as discussed below.

Installer Blocking

Using its Algorithm Inspection technology, Trusteer Rapport prevents specific malware strains from installing on the computer. Similar to any other desktop application, malware comes prepackaged with an installer. The purpose of the installer it to place the malware files, and make other necessary changes (e.g. registry) on the computer so that the malware will run each time the computer starts. Each malware strain has its own proprietary installer which uses sophisticated obfuscation techniques to prevent anti-malware solutions from detecting that the malware is being installed. However, while the installer file and behaviors keep changing, the algorithm that is used by the installer remains static. As explained above, algorithm generation cannot be automated and therefore rarely changes. By reverse engineering these installers and revealing their algorithms, Algorithm Inspection Engine (AIE) can detect and remove the installer before the malware ever installs on the computer.

AIE works as follows: Trusteer Rapport looks at any new file that executes on the computer. Once the file starts executing, Trusteer Rapport monitors all calls that the file's process makes to the file system, registry, and other operating system resources. Once a call is made, Trusteer Rapport captures the executed code and runs it in the AIE. The AIE identifies the algorithm that this code executes and compares it to algorithm rules produced by Trusteer. If a match is found, Trusteer Rapport immediately terminates the process and deletes the file, preventing the installation of the malware from completing.

Algorithm Inspection works quietly in the background and has very low impact on the computer, as it doesn't involve file system or memory scanning, or heavy operations. It looks at new files only and triggers only when the file tries to run an installation process.

Removal of Installed Malware

When malware is already installed on the computer, Algorithm Inspection is capable of detecting its operation and completely removing it from the computer. This scenario is relevant when Trusteer Rapport is installed on an already infected computer or when the malware managed to install itself on the computer before Algorithm Inspection included rules to detect the installer.

Typically, the Algorithm Inspection detection and removal process doesn't involve any scanning of the computer and doesn't rely on signature or behavioral rules. When the malware is on the computer. it injects its payload into existing processes and applications. This is the inspection point where Trusteer Rapport looks at the payload, detects its algorithm and traces it back to its files and then removes it. The ability to trace the malware back to its files is based on the understanding of the malware's algorithm and the full reverse engineering of the malware which allows Trusteer Rapport to fully understand where the malware sits in the file system.

Phishing Protection

Trusteer Rapport Phishing Protection works differently than phishing filters used by browser and desktop security solutions such as antivirus. Common phishing filters (now part of Internet Explorer, Google Chrome and Firefox) consist of a black-list of known phishing websites. The filter blocks the user from reaching black-listed websites. The three main challenges with phishing website black-listing are (1) the huge number of phishing websites (2) the dynamic nature of these sites, and (3) the fact that many phishing sites are targeted and therefore visited by very few victims. This combination of challenges makes it nearly impossible to build an accurate and up-to-date black-list.

Trusteer takes a different approach to Phishing detection and protection. Using a set of heuristics Trusteer Rapport is capable of detecting zero-day phishing attacks and warns the customer before the customer enters credentials into the website. An example for such heuristic is when a password field is being submitted over an HTTP (instead of HTTPS) connection. Another example is when the website into which the customer enters information is visually similar to the financial institution's website. Trusteer Rapport alerts the user that this site is not secure by presenting an alert

There is no need for Trusteer Rapport to learn "protected" passwords or user intervention to confirm them. The entire process takes place in the background.

In addition to warning customers about zero-day phishing attacks Trusteer Rapport also reports these attacks back to the financial institution. The attack is first reported to Trusteer. Trusteer fraud analysts verify the phishing attack within minutes and an alert is sent to the financial institution with information about the new phishing website.

The financial institution is notified of users navigating to phishing sites and users submitting PII to a Phishing Site. Financial institutions can take mitigating actions such as timely initiation of phishing web sites and user re-credentialing, as well as integrating the phishing information into a risk engine to factor potential credential loss and malware infection into the risk score. Trusteer Rapport Phishing Protection mechanisms protect online banking login credentials and payment card data.

Trusteer Rapport Self Protection

To prevent malware from removing Trusteer Rapport or disabling its protection layers, Trusteer Rapport includes the following self-protection mechanisms:

- Tamper Prevention
- Tamper Detection
- Malware Uninstall Prevention

Tamper Prevention

Trusteer includes built-in protection mechanisms that guard its installation by protecting files, process, registry keys and other objects. These mechanisms are designed to evolve and respond to new threats as they arise.

Tamper Detection

Tamper detection is based on multiple mechanisms running at all times to detect the occurrence of malicious activity designed to alter Trusteer processes or aggressively disable Trusteer. This watchdog process ensures that Trusteer is always aware of any attacks. If Trusteer identifies an attack, it notifies the Trusteer Cloud about the attack and the financial institution is notified with compromised customer information.

Malware Uninstall Prevention

Legitimate program removal attempts must pass through a CAPTCHA mechanism to ensure they are initiated by a human and not by malicious code on the computer. Any attempt to bypass the CAPTCHA mechanism or aggressively remove Trusteer software agents without the legitimate process is identified as such. Multiple watchdog mechanisms in 2 separate processes monitor the Trusteer Rapport's software agent health and removal attempts. When any such attempt is identified, a report is sent to Trusteer and the Trusteer customer for further investigation and remediation action.

Trusteer Management Application (TMA)

The Trusteer Management Application (TMA) is a web-based administration console that gives the financial institution access to its reports and configuration. The TMA provides centralized management of all deployed products. Financial institutions can monitor endpoint security health, adoption and usage of Trusteer services, and respond to alerts about specific threats by suspending transactions, taking down phishing sites, re-credentialing users and removing threats on infected endpoints.

TMA allows the financial institution to control website descriptors, security policies (protection modules).

Website Descriptors

Website descriptors describe the financial institution websites. Using the descriptors, the financial institution can build groups of hosts and URLs, and form parameters that are used by its web applications.

Security Policy

The security policy controls the various protection mechanisms that Trusteer Rapport implements. The financial institution can enable or disable protection mechanisms for each of its websites or specific parts within, by associating security policies with specific website descriptors.

Once completed, the configuration (security policy and website descriptors) can be pushed to all Trusteer Rapport software agents. Once the configuration is published it is made available for download. The Trusteer Rapport software agents automatically check for new configurations every few minutes. TMA responds with "updates available" when a new configuration is published. The software agent then downloads the new configuration from the TMA and applies it immediately. The configuration file is encrypted and signed, and the software agent verifies the signature before starting to use the configuration. TMA distributes configurations over a leading Content Delivery Network (CDN), to guarantee maximum availability of information.

The financial institution can edit the configuration at any given time by logging into TMA and republishing a new configuring. The entire process of configuration updates is completely transparent to end users who run Trusteer Rapport.

TMA provides multitenant configuration management where one financial institution cannot access (e.g. read, edit, delete) the policies of another financial institution. Each financial institution can only set policies related to their set of protected sites.

TMA also provides the Trusteer Rapport software agent with software updates which are controlled by Trusteer. When such an update is available, it is placed in the TMA. When Trusteer Rapport checks for new updates, it gets a message that a new software update is available which it then downloads and applies the update. The update process itself is transparent to end users.

TMA is an infrastructure for distributing configuration and software updates to Trusteer Rapport. If TMA is not

available for any reason, Trusteer Rapport continues to operate normally but is unable to retrieve new updates. Once TMA becomes available, Trusteer Rapport downloads the latest updates.

The TMA's Assessment section offers ongoing updates on the financial institution's customer base. including on customer computer hygiene, malware distribution, infected log-in data, etc.

The status of a specific Trusteer Rapport agent can be found by accessing the Agent Status page and entering the Trusteer Rapport ID of the agent.

TMA Reports

TMA provides a set of Trusteer Rapport reports that cover all data related to deployment, agent status, malware infection and attacks, phishing attacks and compromised credentials.

Trusteer Rapport related reports in the TMA include:

Deployment Report

- Trusteer software agent downloads
- Trusteer software agent distribution

Trusteer Client Reports

- Financial institution customer's computer hygiene
- Detected malware
- Malware-infected logins
- Infected machines
- Compromised payment cards
- Trusteer agent status

Trusteer Rapport Phishing Prevention

- Detected phishing sites and servers
- Phishing trends

Actionable Feeds Reports

- Trusteer agent installed on infected machines
- End user machine became infected
- Trusteer agent uninstalled on infected machines
- Trusteer agent attacked
- New customer accounts
- User submitted PII to phishing site
- User navigated to phishing site

Actionable Intelligence Feeds

Actionable Intelligence Feeds are sent via flat files (CSV or xml), parse-able email messages or integrated to fraud prevention frameworks through a standard API. Feed emails are sent to the business to keep managers updated on immediate new threats requiring their attention. The delivery method and the recipients of the feeds are configured in the TMA.

Feeds delivered include:

- Trusteer Rapport installed on infected machine
- User machine became infected
- Trusteer Rapport uninstalled on infected machine
- Trusteer Rapport attacked
- New account indication
- User machine became infected
- Phishing site detection
- User encountered risky site requesting payment card (credit/debit) information

For information about Trusteer feeds, please refer to the document entitled "Best Practices of Using Trusteer Actionable Intelligence Feeds." For technical data on the feeds, please refer to the "Trusteer Actionable Intelligence Feeds Reference Guide."

About Trusteer

Trusteer is the leading provider of cybercrime prevention solutions that protect organizations against financial fraud and data breaches. Hundreds of organizations and millions of end users rely on Trusteer to protect their computers and mobile devices from online threats that are invisible to legacy security solutions. Trusteer's Cybercrime Prevention Architecture combines multi-layer security software and real-time threat intelligence to defeat zero-day malware and phishing attacks, and help organizations meet regulatory compliance requirements. Leading organizations such as HSBC, Santander, The Royal Bank of Scotland, SunTrust and Fifth Third are among Trusteer's clients.

For more information visit: **www.trusteer.com**.