Enterprise

Trusteer

Trusteer
for Enterprise Cybercrime Prevention

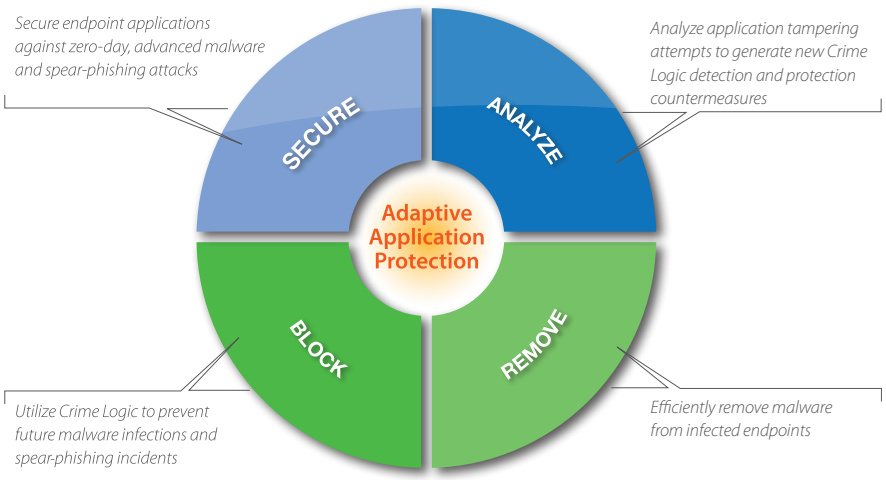
Adaptive Application Protection Against Advanced Malware, Spear-phishing and APTs

Hundreds of organizations and tens of millions of their customers rely on Trusteer's field-proven architecture to protect their computers and mobile devices from cybercrime. Trusteer's global footprint, unique people, technology and processes enable our customers to achieve sustainable cybercrime prevention and meet regulatory compliance requirements.

The Trusteer Difference

- *Crime Logic, not signatures:* Through intelligence gathered from millions of protected endpoints, Trusteer processes tens of thousands of malware attack attempts every day into Crime Logic, a unique, compact, and actionable footprint of cybercrime targets and tactics.
- *Rapid adaptation to emerging threats:* Trusteer's Adaptive Application Protection process quickly turns zero-day attacks into known Crime Logic. New Crime Logic is automatically integrated into Trusteer's products to promptly detect and block these attacks on protected endpoints.
- *Real-time application protection:* Trusteer's Application Protection technology transparently secures the browser and sensitive client applications against zero-day malware and phishing attacks. This unique technology prevents malware from tampering with these applications while immediately alerting Trusteer of any abnormal behavior that could represent a new attack.

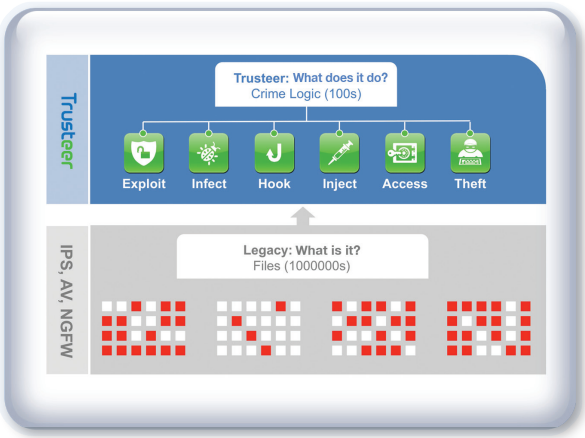
Trusteer's Adaptive Protection Process



new threats, ***new thinking***

Stopping Advanced Threats with Adaptive Application Protection

Increased workforce mobility, Bring-Your-Own-Device (BYOD), and desktop virtualization initiatives have dramatically expanded the risk of advanced threats to enterprise assets. Using a spear-phishing or drive-by-download attack, advanced malware can compromise client applications and enable cybercriminals to access sensitive business data. Operating "under the radar," advanced malware is designed to evade legacy security controls that detect malicious code signatures in files and packets. Evasion techniques vary: from limited distribution polymorphic variants to memory-resident threats that hide within applications and system processes. By the time signatures are captured and propagated, the damage is already done.



Crime Logic vs. Files and Signatures

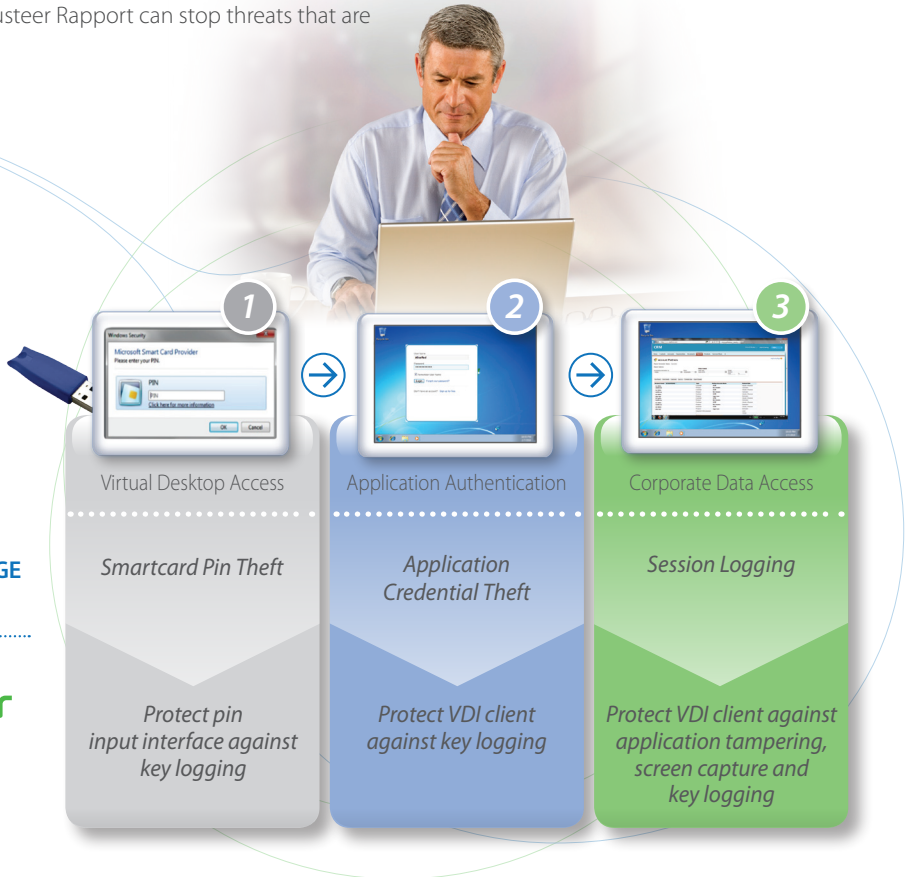
Trusteer Rapport for Enterprise

Trusteer delivers ***Adaptive Application Protection***, a new approach to protecting enterprises against advanced threats to employees' computers. Trusteer combines real-time endpoint protection with expert analysis of global real-time intelligence to quickly detect and stop emerging attack tactics ("Crime Logic"), such as web vulnerability exploits, malware infection techniques, process hooking methods and injection mechanisms. By focusing on a finite number of Crime Logic ("What the threat does"), irrespective of a specific footprint from an infinite number of files ("What the threat is"), Trusteer Rapport can stop threats that are undetectable by legacy security measures.

The customer:
Global 1000 Company

The challenge:
Securing anytime and anywhere access to Citrix Virtual Desktop

The solution:
Trusteer Rapport for Enterprise



Trusteer Rapport for Enterprise

Endpoint-centric Adaptive Application Protection

Shields Client Applications Against Exploitation and Tampering

Trusteer Rapport secures sensitive client applications such as VPN clients, Virtual Desktops (VDI), email and Office against advanced malware. It detects and stops real-time attempts to exploit application and operating system services and gain access to business data accessed by these applications. Attack events such as application tampering, key logging and screen captures of sensitive data are reported to IT security and Trusteer Intelligence Center in real-time. Trusteer experts detect changes in Crime Logic and deploy countermeasures as needed.

Prevents Attack Reconnaissance and Social Engineering

The Web browser is used extensively to access internal and cloud-based enterprise applications. Trusteer Rapport protects the browser to prevent session logging and malicious web page injection. Session logging is a key step in complex attack reconnaissance as it provides visibility to the flow and structure of enterprise applications. Web injection is used to social engineer employees into surrendering credentials and other confidential information.

Stops Credential and Personal Information Theft

Trusteer Rapport prevents login credential and personal information theft by disabling malicious key logging and screen capturing of sensitive applications. It warns the users if they choose to enter enterprise credentials into non-secure web sites or reuse them in consumer-oriented sites. Trusteer Rapport also protects users accessing Facebook and LinkedIn from data theft through social engineering. Data stolen from social networks can later be used to orchestrate spear-phishing attacks against employees.

Closes the Door on "Back Doors" and Data Leaks

Remote Access Trojans (RATs) provide cybercriminals with unlimited access to infected endpoints. Using the victim's access privileges they can access and steal sensitive business and personal data including intellectual property, personally identifiable information (PII) and patient health information (PHI). Trusteer Rapport detects RATs presence and stops the execution of remote access sessions into the endpoint.

Blocks Malware Infection, Removes Existing Malware

Upon installation, Trusteer Rapport removes existing advanced malware from end-user machines. It prevents future infections by stopping attempts to exploit system vulnerabilities and malware installation processes.

Enterprise Controlled Client Deployment and Management

Trusteer Rapport clients can be deployed on PC, Mac and Virtual Desktops (e.g. Citrix) using software delivery tools (e.g. Microsoft SMS, HP CM) and code updates can be controlled by IT security. Unmanaged devices can be instantly secured using an on-demand deployment option when enterprise resources need to be accessed from home computers or on the road. Enterprises can set policies controlling the ability to disable or uninstall Trusteer Rapport and monitor the deployment and client status through a cloud-based management application.

Protecting Against Crime Logic

- *Spear-phishing*
- *Web Injection*
- *Application Tampering*
- *Remote Access*
- *Screen Capture*
- *Key Logging*
- *Vulnerability Exploitation*
- *Malware Installation*

40%

of CIOs reported

malware related internal breaches

Source: 2010 Deloitte-NASCIO Cyber Security Study

Trusteer Intelligence, Forensics and Management

Crime Logic Analysis and Forensics, Centralized Management

Emerging Crime Logic Analysis from Tens of Millions of Endpoints

A network of tens of millions of Trusteer-protected endpoints continuously propagates Crime Logic information to the Trusteer Cybercrime Intelligence cloud. Trusteer Intelligence Center experts use advanced data mining and analysis tools to identify new Crime Logic.

Adapting Trusteer Products to Stop New Crime Logic

Trusteer Intelligence Center creates detection and protection countermeasures that are immediately integrated into Trusteer products to address new Crime Logic. The research and analysis are also published in the Trusteer Situation Room portal that allows enterprises to gain insight into global and organization-specific threats and attacks.

Cloud-based Management

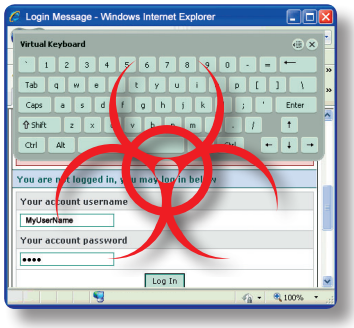
Trusteer Management Application provides centralized management of all deployed clients. Enterprises can monitor endpoint security health and usage of Trusteer services, and respond to alerts about specific threats and suspected infections.

Malware-driven Attack Investigation

Following a suspected malware-driven fraud incident, the Trusteer Flashlight endpoint analysis product enables the security teams to instantly initiate a remote malware forensic investigation. Trusteer experts provide detailed analysis of the infection to support the incident review process. Ultimately, Trusteer Rapport is deployed to remove the infection and enable safe enterprise application access.

Crime Logic: Virtual Keyboard VPN Login Attack

1. *Employees access the VPN login*
2. *User is prompted with virtual keyboard*
3. *Employee uses mouse to type login credentials*
4. *Malware captures screen on every mouse click*
5. *Malware sends screen capture sequence to drop zone*
6. *Fraudsters decipher credentials from mouse cursor position*



Zeus malware attacks a Citrix virtual keyboard

Trusteer Research, October 2010

Trusteer Situation Room

Trusteer Management Application: Policy Management

new threats, ***new thinking***

Trusteer for Enterprise Cybercrime Prevention

Trusteer Rapport

Trusteer Rapport for Enterprise

- *Detects and blocks advanced malware and spear-phishing attacks against enterprise endpoints*

Trusteer Rapport Feeds

- *Actionable feeds on device security configuration and threat activity*

Trusteer Intelligence & Management

Trusteer Management Application

- *Consolidated management and reporting system for Trusteer products*

Trusteer Situation Room

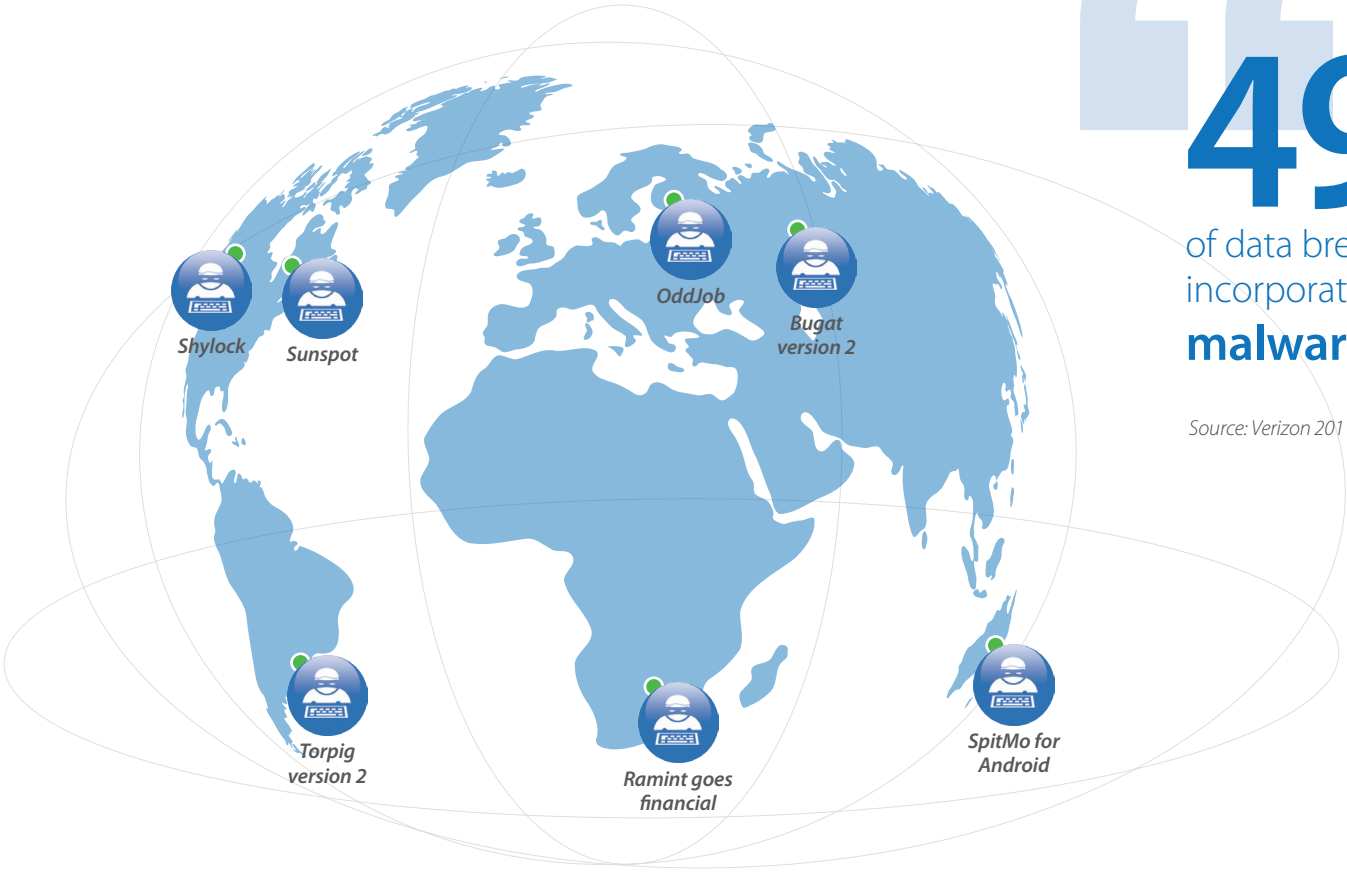
- *Intelligence portal for industry-wide and enterprise specific online threats*

Trusteer Flashlight

- *Investigates malware infection and attack incidents*

Trusteer is the Global Leader in Endpoint Cybercrime Prevention

Trusteer Cybercrime Prevention Architecture helps organizations to protect their employees and customers against malware and spear-phishing attacks. Trusteer has created a unique process that combines endpoint protection technology and expert analysis of real-time intelligence to quickly detect, analyze and adapt to new Crime Logic. With hundreds of customers and tens of millions of end users, Trusteer is proven to eliminate cybercrime from protected endpoints. To learn more about how you can protect your customers and employees, visit ***www.trusteer.com****.*



49%

of data breaches incorporated **malware**

Source: Verizon 2011 Data Breach Report

Trusteer Inc.
545 Boylston Street, 5th Floor
Boston, MA 02116
T: +1 (866) 496-6139
F: +1 (646) 304-4075
info@trusteer.com

trusteer.com

Trusteer