financial Services

Trusteer Products Overview

Trusteer
an IBM Company

Cybercriminals continuously target financial institutions, enterprises, eCommerce sites and other organizations to steal money and business information. Legacy solutions are hard pressed to prevent these attacks as they lack threat intelligence and real-time visibility to the full attack life cycle.

Trusteer has pioneered a holistic, integrated cybercrime prevention architecture that has been successfully deployed in hundreds of organizations and over a hundred million users globally. Trusteer's solutions prevent or detect the full range of attack vectors (including phishing and malware targeting end users, and account takeovers perpetrated by criminals) responsible for the majority of online, mobile and cross-channel fraud.

Trusteer's cybercrime prevention architecture is based on four key principles; that prevent fraud, sustain protection over time, streamline the customer experience and minimize the load on the organization's resources.

The Four Key Benefits of Trusteer's Cybercrime Prevention Architecture

Effective and accurate fraud prevention

- **Prevent** the root causes of most fraud attempts: malware and phishing
- **Detect** active threats in real-time
- **Analyze** risk factors related to a device, user, account, and transaction to conclusively flag account takeover attempts and high-risk transactions

Adapt to emerging threats

- Use real-time global intelligence from tens of millions of endpoints
- Dynamically adapt the various protection layers to ensure sustainable protection

Streamline end users' experience

- Deliver transparent protection
- Minimize disruption to customers performing legitimate transactions
- Increase the effectiveness of an organization's support, fraud, and risk teams

Provide fast time to value

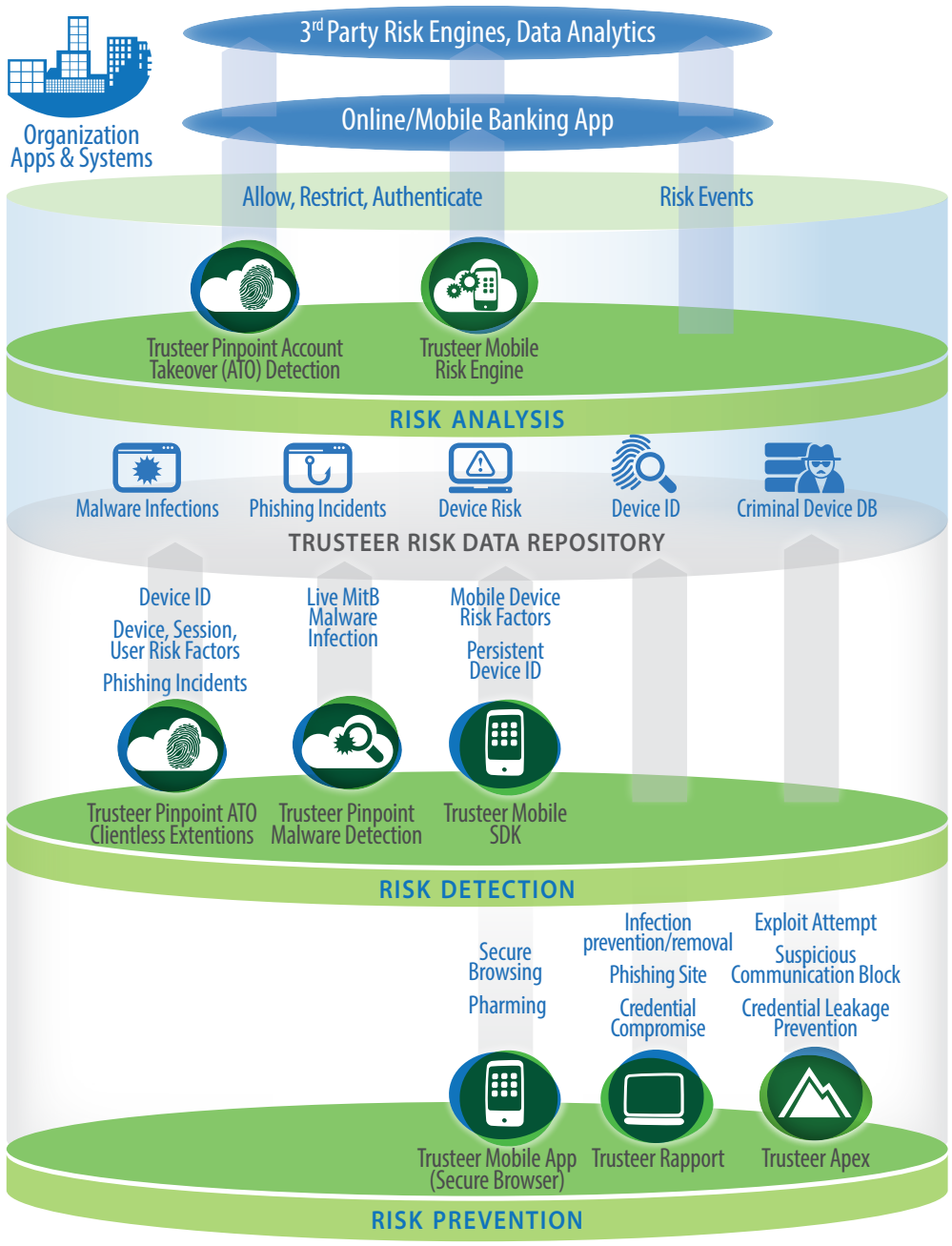
- Offer a turnkey software as a service (SaaS) solution for rapid deployment
- Provide an immediate response across all online and mobile applications

Trusteer Products Overview and Key Capabilities

	Product	Overview	Key Capabilities	
Clientless Fraud Prevention	**Trusteer Pinpoint Account Takeover Detection (PPATO)**	Conclusive detection of criminals and account takeover attempts	• Detects new, spoofed (proxy) and known criminal devices using complex device ID • Identifies real-time phishing incidents • Seamlessly integrates extended malware and phishing risk indicators from Trusteer Pinpoint Malware Detection and Trusteer Rapport (if available)	• Correlates device risk (i.e. new, spoofed, known criminal devices) and account risk (i.e phishing incidents and malware infections) for conclusive criminal and account takeover detection • Maintains a global criminal device database based on intelligence from hundreds of organizations worldwide
	Trusteer Pinpoint Malware Detection (PPMD)	Accurate, real-time detection of live Man-in-the-Browser malware infected devices	• Detects live Man-in-the-Browser (MitB) infections on PC/Mac/mobile devices	• Feeds malware detection events via email, batch files, or directly into Trusteer Pinpoint Account Takeover (ATO) Detection and 3rd party risk engines
	Trusteer Mobile Risk Engine (MRE)	Conclusive detection of mobile-specific fraud risks from compromised end user devices and criminal-owned devices	• Detects high risk mobile access from smartphones and tablets • Risk analysis is based on device, session and user risk factors captured by the Trusteer Mobile SDK, Trusteer Mobile App (Secure Browser), and 3rd party apps	• Correlates cross-channel risk factors (malware infection and phishing incidents in the online channel) to address complex online/mobile attack scenarios
Endpoint Security	**Trusteer Rapport**	Client-based endpoint protection against financial malware and phishing attacks	• Prevents infection and removes live and inactive Man-in-the-Browser malware from infected computers • Protects browsing session even if active malware is present	• Detects phishing sites and specific compromised account credentials and payment card data • Notifies fraud teams of malware infections and removals, to enable user re-credential and eliminate future threats
	Trusteer Mobile SDK	Dedicated security library for iOS and Android that can be embedded in proprietary mobile banking apps to detect compromised and vulnerable devices and generate persistent device ID	• Detects the following risk factors: - Jailbroken/rooted - Malware infection - Rogue applications installed - Unsecured Wi-Fi connection - Outdated OS - GEO location - and more	• Generates persistent device ID based on hardware and software attributes that is resilient to application reinstall
	Trusteer Mobile App (Secure Browser)	Enables risk-based analysis of web access/ transactions from mobile devices	• Incorporates Trusteer Mobile SDK in order to deliver device risk factors and persistent device ID to the web app • Prevents Man-in-the-Middle attacks (ensures users browse to the genuine site)	• Alerts the user of device risk factors and provides remediation guidance
	Trusteer Apex	Protects employees' endpoints, against advanced malware by stopping zero-day exploits and data exfiltration	• Protects Java, browsers, Adobe, MS Office, etc. against zero-day exploits • Prevents malware data exfiltration	• Prevents credentials theft via spear-phishing and re-use of enterprise credentials on consumer sites • Supports managed and unmanaged employee endpoints

Trusteer Product Overview - Data Flow

The diagram below shows Trusteer's holistic security architecture, as well as the data and intelligence flow between Trusteer products.



About Trusteer

Trusteer, an IBM Company, is the leading provider of endpoint and clientless cybercrime prevention solutions that protect organizations against account takeover, credentials theft, and fraudulent transactions. Hundreds of global organizations and millions of end users rely on Trusteer to protect their managed and unmanaged endpoints from online and mobile fraud.

Trusteer, an IBM Company
545 Boylston Street, 5th Floor Boston, MA 02116
T +1 866 496 6139 F +1 617 606 7756 trusteer.info@us.ibm.com **trusteer.com**