IBM Security
Solution Brief

Create a seamless experience for customers throughout their digital journey

Seamlessly establish digital identity trust across the omnichannel customer journey with IBM Trusteer

Introduction

In today's digital world, consumers expect a frictionless experience—whether they're making a purchase, registering for an account, conducting a transaction, signing up for a loyalty program or service, or simply updating their contact information.

Regardless of your industry, delivering on this frictionless customer experience across channels is key to digital growth, innovation and increased competitiveness. When consumers are required to perform extra authentication steps, frustration can increase and result in higher abandonment rates, lower net promoter scores (NPS) and missed sales opportunities.

How will your organization assess risk to know which users to trust?

The IBM® Trusteer® platform is designed to help companies quickly and transparently establish digital identity trust so they can seamlessly welcome in true customers, and maintain and nurture that trust throughout the digital journey, all without compromising on security.

Digital identity trust from IBM Trusteer features:

- Continuous digital identity assurance throughout the digital omnichannel lifecycle for new customers, guests and both low- and high-risk existing customers
- A scalable, agile cloud platform that simplifies deployment and enables real-time risk assessments based on the latest intelligence
- Intelligence services layered with advanced AI and machine learning

Continuous digital identity assurance

Companies often struggle to confirm user identities when they don't have prior information or customer records, when the information they rely on is publicly available, and when cybercriminals exploit new digital features, use stolen identities or employ tactics across multiple channels.

The IBM Trusteer platform offers a multilayered, holistic user view and a modular approach that is designed to transparently identify unauthorized access and activities. Low-risk users can receive a more seamless experience, while users deemed a higher risk can be subject to stronger step-up authentication.

To assess risk, the Trusteer platform draws on a wide variety of network, device, environment and behavioral intelligence:

- Behavioral analysis, including behavioral biometrics, and user journey analysis
- Device identification, association, authenticity, hygiene and spoofing evidence
- Phone number and email intelligence
- Identity linkages
- Session and network attributes

This data, combined with our analytics and intelligence services, can help organizations create a seamless experience that lets true customers in while orchestrating strong step-up authentication for users deemed high-risk.

Intelligence services layered with advanced analytics

Just as user expectations for access are evolving, so are the ways malicious actors operate. IBM Trusteer includes agile intelligence services that help identify emerging patterns and evolving threats and can rapidly adapt protections as the threat landscape changes.

Our security infrastructure is comprised of:

- Advanced AI and machine learning capabilities that analyze billions of sessions daily
- Cross-organization, global, real-time threat data delivered through the cloud
- Emerging patterns identified by IBM X-Force®, one of the world's most experienced commercial security research teams

Continuous digital identity assurance
Transparently identify unauthorized access and activities

Scalable and agile cloud platform
Establish cross-organizational, actionable insights via real-time assessments

Advanced AI and machine learning layered with intelligence services
Assess risk, operational costs, and improve efficiencies and security

By combining these intelligence capabilities with human intelligence from experienced threat researchers, we can help organizations better assess risk, improve security measures and only challenge high-risk users with the extra steps, such as two-factor authentication.

Real-time actionable assessments with a scalable, agile cloud platform

IBM Trusteer solutions are built on a scalable, agile cloud platform that simplifies deployment and enables real-time risk assessments based on the latest intelligence for increased operational efficiency and reduced costs. Trusteer cloud-based services can grow with each business, processing virtually any number of sessions in real time and flexibly integrating with third-party solutions.

Tackle a wide range of digital identity trust challenges with one platform

The IBM Trusteer multilayered and modular approach can help organizations address a wide range of digital identity trust challenges.

Establish trust: Identity proofing for new and guest users

What happens when you need to validate a new or anonymous customer? Is the user a true customer or are they intent on initiating payment fraud or abusing your loyalty program? Which guests or new customers should you let in unimpeded, and which ones should complete step-up authentication?

Using advanced intelligence and global visibility, the IBM Trusteer Pinpoint™ Assure solution is designed to help detect and predict the risk of fraudulent intent for new and guest customers. It also enables companies to conduct early account monitoring for new accounts. It’s this type of insight that’s critical to reducing abandonment caused by friction in security measures, increasing loyalty program registrations, and growing the digital channel.

Sustain trust: Continuous authentication for trusted users

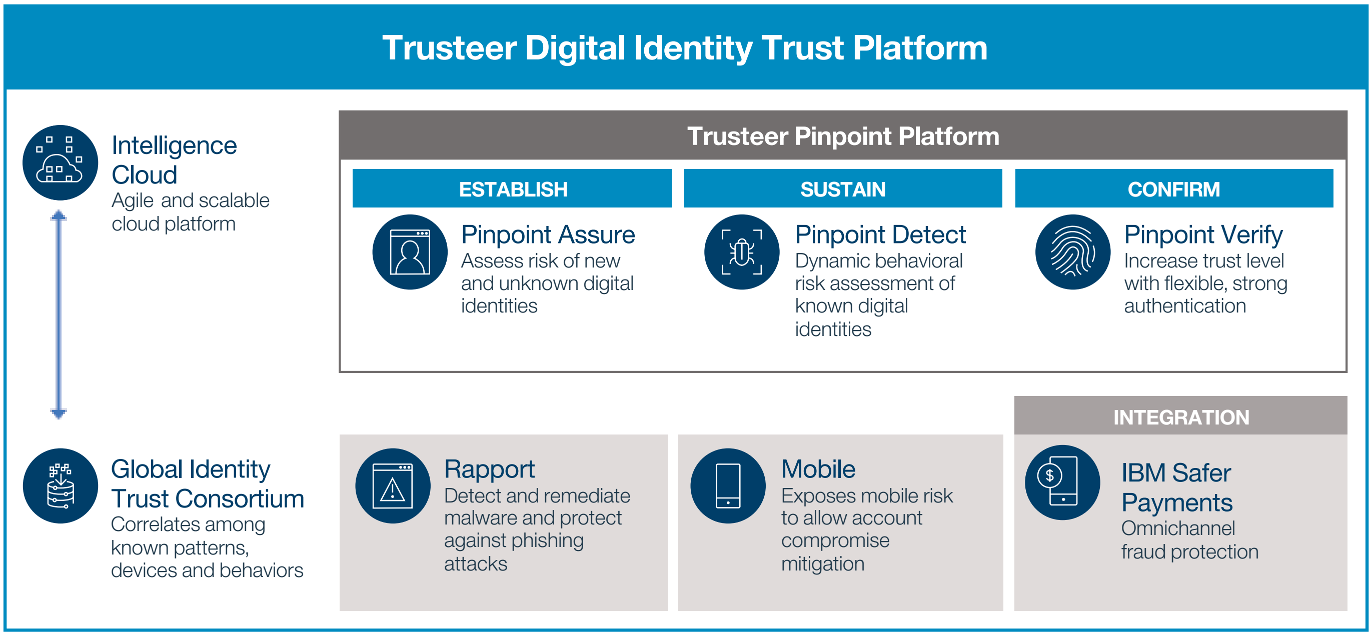
How can you better protect customer accounts and their payment journeys from being compromised? Detecting account takeovers, or unauthorized logins and activity, requires a comprehensive view of account access from the device, session and user perspective. IBM Trusteer Pinpoint Detect delivers this kind of visibility, using both behavioral biometric capabilities and behavioral analytics to transparently build user profiles and continually authenticate online identities.

Using machine learning and patented analytics, the platform analyzes patterns of mouse movements, at astonishing speeds and volumes, to differentiate an account user’s “normal” digital behavior from abnormal behavior. This insight is combined with device activity and evidence, transactional data and geolocation data. If either abnormal user behavior or known fraudster behavior is detected, Trusteer Pinpoint Detect provides a recommended action in real time along with the detailed reasoning and session details so your organization can take steps to confirm trust when necessary.

Confirm trust: Combine omnichannel risk assessment with strong adaptive authentication

How do you confirm trust when abnormal user behavior or suspicious activity is identified? The IBM Trusteer Pinpoint Verify cloud-based authentication service seamlessly integrates with Pinpoint Assure and Pinpoint Detect to help companies apply strong step-up authentication when necessary.

Application developers simply use the exposed interfaces of the service to challenge users to perform a second factor authentication via their digital application. Users can then choose to enroll in various forms of two-factor authentication, from one-time passcodes via email, SMS or mobile push notification to biometric authentication.



Trusteer Digital Identity Trust Platform
Intelligence Cloud
Agile and scalable cloud platform
Global Identity Trust Consortium
Correlates among known patterns, devices and behaviors
Trusteer Pinpoint Platform
ESTABLISH
Pinpoint Assure
Assess risk of new and unknown digital identities
SUSTAIN
Pinpoint Detect
Dynamic behavioral risk assessment of known digital identities
CONFIRM
Pinpoint Verify
Increase trust level with flexible, strong authentication
Rapport
Detect and remediate malware and protect against phishing attacks
Mobile
Exposes mobile risk to allow account compromise mitigation
INTEGRATION
IBM Safer Payments
Omnichannel fraud protection

Protect against malware and phishing

Cybercriminals often use malware and phishing as part of carefully planned and well-coordinated omnichannel attacks. As a result, organizations that fail to monitor and take into account such risks and compromises on consumer devices may be missing the bigger picture, which can lead to greater overall risk. IBM offerings are designed to help address these common tactics:

- Trusteer Pinpoint Detect offers clientless fraud detection with unified malware and criminal detection.
- IBM Trusteer Rapport® provides endpoint fraud protection to help defend against man-in-the-browser (MitB) attacks and remove malware from endpoint devices. Trusteer Rapport also uses machine learning and patented analytics to rapidly detect new phishing sites and alert customers if they're entering a phishing site.
- The IBM Trusteer Mobile solution offers visibility into a wide range of mobile risk indicators and behavioral anomalies. It also can create a persistent mobile device ID, which allows organizations to distinctly identify any mobile device (iOS or Android).

Trusteer solutions offer simple and standardized interfaces and can be easily integrated into an organization's existing infrastructure.

Offering	Key capabilities
IBM Trusteer Pinpoint Assure: Helps organizations detect and predict identity risk for guest and new users during the new digital account creation process.	• Correlates rich proprietary insights, mobile carrier intelligence and global security intelligence specific to new and anonymous users, including: – Behavioral and user journey analysis to help detect malicious BOT attacks or known malicious activity usage patterns – Device identification, association, authenticity and hygiene to identify if the device may not be trustworthy – Phone number and email intelligence – Identity linkages that show if the same identity or identity attributes are opening new accounts or conducting transactions at a velocity and rate that does not match legitimate activity at other companies using IBM Trusteer solutions – Malicious evidence consortium data from a worldwide network • Provides an ecosystem-friendly approach that exposes and enables leveraging of IBM Trusteer new account intelligence
IBM Trusteer Pinpoint Detect: Helps detect account takeover fraud across digital channels. When deployed with IBM Safer Payments, the integrated solution offers broad omnichannel visibility to place activities from digital and cashless payment channels in context.	• Enables real-time risk assessment and provides recommended actions to help detect and mitigate fraudulent activities • Enables fraud analysts to customize new policies and rapidly deploy countermeasures with visibility to IBM Trusteer crime logic • Uses behavioral biometrics capabilities to seamlessly authenticate users by building models based on patterns of mouse movements in real time and analyzing patterns against learned user behavior and known fraud patterns • Identifies access using compromised credentials • Monitors transactions
IBM Trusteer Pinpoint Verify: Offers strong authentication for high-risk users to help remediate identity risk.	• Delivers one-time passcodes via email, SMS or mobile push notification • Supports biometric authentication, including fingerprint, face and user presence
IBM Trusteer Rapport: Provides client-based endpoint protection against malware and phishing attacks.	• Helps protect against and remove malware infections from user devices • Helps protect browsing sessions, even if active malware is present • Detects phishing sites and specific compromised account credentials and payment card data, warning users and notifying fraud teams • Notifies fraud teams of malware infections and removals to enable user re-credentialing and help protect against future threats
IBM Trusteer Mobile: Helps protect native mobile applications through device risk factor analysis and the use of a persistent mobile device ID. To help further improve detection in the mobile channel, IBM Trusteer mobile solutions can be used standalone or seamlessly integrated with Trusteer Pinpoint Detect for wider digital fraud detection.	• Helps detect mobile-based risk factors, including: – Jailbroken/rooted and spoofed devices – Malware infections and SMS stealers – Active overlay malware – Installation of applications from untrustworthy sources – Unsecured sessions and connections – Outdated operating systems – SIM information for SIM swaps and porting – User behavioral data, such as location • Generates a persistent device ID based on hardware and software attributes that are resilient to application reinstallation

For more information

To learn more about seamless digital identity trust, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security/fraud-protection/trusteer

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
November 2018

This document is current as of the initial date of publication and may be changed by IBM at any time.

Not all offerings are available in every country in which IBM operates. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

♻ Please Recycle