IBM Security

IBM

Accelerating growth and digital adoption with seamless identity trust

IBM Trusteer helps organizations seamlessly establish identity trust across the omnichannel customer journey

Let’s get started

Contents

Introduction

If your company is like most, accelerating growth and increasing digital channel adoption are top priorities. Market forces have made digital transformations a necessity for companies to meet customer expectations, reach new markets and grow revenue.

But what many companies have found is that going digital is only half the battle. Consumers demand a *frictionless* experience online—whether they're making a purchase, registering for an account, signing up for a loyalty program or service, or simply updating their contact information.

When consumers are required to perform extra authentication steps to conduct a transaction, apply for services or access their accounts, the digital channel can become a source of dissatisfaction rather than delight. This can result in higher abandonment rates—with users moving either to competitor sites or higher cost channels. And higher abandonment rates can lead to lower net promoter scores (NPS) and missed sales opportunities.

Unfortunately, the anonymity of the digital channel allows individuals with the right tools to conceal their identities and abuse the digital channel.

Imagine what it would mean if companies could trust true customers: more seamless transactions, greater digital growth and innovation and increased competitiveness.

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.

How can organizations continuously and transparently establish identity trust across the digital journey so they can seamlessly welcome in new, guest and existing customers, while keeping malicious activity out?

To deliver a better, frictionless experience, organizations should consider real-time, multilayered, omnichannel identity trust assessments that analyze a wide variety of intelligence—including network, device, environment, behavioral and global intelligence.

Do you know your digital customers?

The IBM® Trusteer® platform is designed to help companies quickly and transparently create trust with anonymous users, establish trust with new customers, and sustain trust with existing customers throughout the digital omnichannel lifecycle. It features continuous digital identity assurance; a scalable, agile cloud platform for increased efficiency; and an intelligence service layered with advanced AI and machine learning capabilities.

The many facets of establishing identity trust across channels

Malicious actors can easily mask their true identities. They can use stolen identities to open new accounts or register for a service or special member's program. They can purchase products with stolen payment data. They can create fake or synthetic identities (identities which add stolen or false data to real identities) to conduct payment fraud, new account fraud and even first-party fraud. They can also impersonate existing customers, compromising accounts to buy products with stored payment information or capture personal data for future fraud.

To unmask malicious activity, companies need to assess each user's identity on two essential levels: how they connect to the digital channel and who is connecting. Even if a device or connection looks legitimate, the user may not be.

At each level there are myriad data points to consider. The more data incorporated into risk assessments, the more effective the risk assessments can be. The more transparent risk assessments are to true users, the better companies can deliver the frictionless experience and trust that consumers expect. Ultimately, in the digital era, companies need to be smart about which users they ask to complete extra security measures to confirm their identities.

Assessing risk across a wide range of scenarios

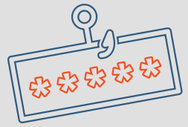
Users

- Guest customers
- New accounts
- Enrolled customers - frequent access
- Enrolled customers - rare access

Tactics

- Identity theft
- Synthetic identities
- Fake identities
- Stolen credentials

Risks



- Payment fraud
- Loyalty program abuse
- First-party fraud
- Account takeover - cashing out points - using stored payment data - changing shipping data
- New account fraud
- Data leaks

Omnichannel Interactions

- Website
- Mobile app
- Mobile phone calls to call center
- Store/branch
- Live chat/chatbot interactions

Key Clues

- Email pattern and reputation
- Mobile phone number intelligence
- Behavioral and user journey patterns
- Behavioral biometrics
- Device authenticity and hygiene
- Connection and network attributes
- Spoofing evidence
- Identity linkages
- Malicious evidence consortium data

Building trust with new, guest and registered users

The tension between security and usability is often felt most keenly when establishing trust with anonymous users and new customers. The IBM Trusteer Pinpoint™ Assure solution is designed to help companies understand, detect and predict the risk of malicious intent for guest and new customers. It also enables companies to conduct early account monitoring for new accounts. It works transparently to correlate rich proprietary insights and global intelligence specific to these segments.

- **Behavioral and user journey analysis** can detect malicious BOT attacks or known malicious activity usage patterns. These can include use of techniques and patterns to fill out digital forms, as well as mouse movements, keystroke patterns and website navigation associated with malicious activity.
- **Device identification, association, authenticity and hygiene** can identify if the device may not be trustworthy, be it spoofed or compromised by malware or used in the past by a malicious actor in another malicious attempt. It can also identify if the device can be associated with the user as a trusted device.
- **Phone number intelligence** can help flag increased risk. For example, a user with a burner phone may be considered a higher risk than a user with a three-year-old account. A phone registered with a carrier known to be used by fraudsters due to lax measures is considered a higher risk than a phone registered with an established carrier. Account owner information can be matched with identity details, registration location information, roaming indications and line status, and correlated with global intelligence and user context and activity.
- **Identity linkages** can 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 IBM Trusteer protected companies.
- **Malicious evidence consortium data** from a worldwide network can help reveal malicious activities.

The benefits of digital trust for retailers

- Increase loyalty program registrations through transparent security
- Protect your customer accounts from being compromised
- Reduce abandonment caused by friction in security measures
- Protect your end user's payment journey

Sustaining trust with existing customers

How do you sustain trust with enrolled customers so you can deliver an exceptional customer experience every time? IBM Trusteer Pinpoint Detect is designed to transparently build user and devices profiles for existing customers and continuously authenticate online identities to help detect account takeovers or unauthorized login or activity. It offers a comprehensive view of the user and account activity from multiple perspectives—device, session, user and omnichannel views.

Device identification, authenticity, hygiene and spoofing evidence. Device identification can be beneficial, but it is susceptible to spoofing and malware. A more robust strategy includes multiple layers of security that look at device authenticity, hygiene and spoofing evidence along with device identification.

Session and network attributes help identify where users connect from and when, what kinds of connections are used, and any suspicious session activity that may increase risks.

User behavioral, behavioral biometric and user journey analysis and insights establish user patterns to help identify anomalies, such as atypical mouse movements, typing patterns or user navigation patterns through the application.

Malicious pattern intelligence helps detect attempts to manipulate or circumvent authentication measures, as well as detect when known attack tools, such as Remote Access Trojans (RATs) or malware, are present. This insight can help identify social engineering attacks that may have a very slim footprint in digital interactions.

Malicious actor consortium data from a worldwide network can help detect known malicious actors attacking other organizations.

Omnichannel and cross-channel view for a view of the user's activity across the website, mobile app, mobile phone calls to call center, store/branch, and live chat or chatbot interactions.

IBM Trusteer Platform

- Continuous digital identity assurance
- Scalable, agile cloud platform
- Intelligence service layered with advanced AI and machine learning

Why IBM Trusteer?

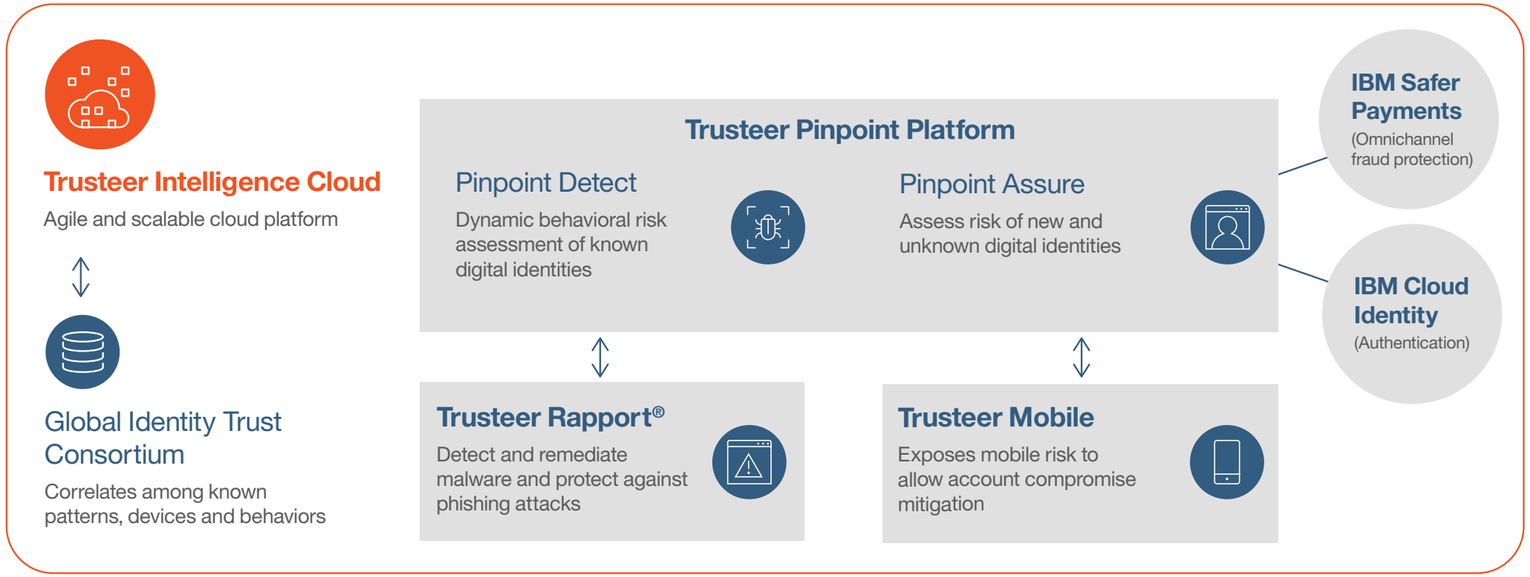
IBM Trusteer offers a multilayered and holistic user view as well as a modular approach that can help companies transparently build identity trust with a wide range of users for a seamless digital customer experience.

IBM Trusteer solutions benefit from its powerful intelligence service. This service combines AI and advanced analytics technology that analyze billions of sessions daily together with human intelligence and experienced threat researchers. Cross-organization, global consortium and new threat insights are all combined to identify emerging patterns and evolving threats, and rapidly adapt protections.

Additionally, a scalable, agile cloud platform simplifies deployment and enables real-time risk assessments based on the latest intelligence for increased operational efficiency and reduced costs.

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

IBM Trusteer: Discover identity. Build trust.



IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
June 2018

29016929-USEN-00