Security
White Paper

Insurance

Building a seamless digital experience for insurance customers

IBM Trusteer helps insurers transparently assess digital identity risk

Contents

2 Introduction

3 The value of strong risk assessments

4 Considerations when assessing digital identities

4 Establishing trust over digital channels

6 Remaining agile with adaptive intelligence

6 Building your own polices with IBM Trusteer advanced intelligence

7 Conclusion

Introduction

Once upon a time, insurers' primary channel to interact with customers was through their insurance professionals (also known as insurance agents). While insurance professionals still play an important role in the customer journey, the insurance market, like many other industries, is increasing its use of low-cost digital channels to better connect with external users and reach new markets.

In recent years, insurers have rolled out digital applications that enable consumers to check policy information, review benefits, compare costs, pay bills, initiate claims, and even apply for coverage from their mobile phones or desktops. This transformation effort reduces the cost of customer service, while generating fresh opportunities to get closer to customers and strengthen brand loyalty.

As the digital transformation continues, insurers are setting their sights to expand sales with new insurance products designed for the digital channel—either delivered directly through their sites or via partners using application programming interfaces (APIs). Insurers have also invested in streamlining processes and services with third party providers that administer claim settling services (e.g., doctors, home repair firms, automotive windshield repair companies). This work can help insurers deliver claims settling services to customers, and help attract more providers to work with the insurer.

But creating a seamless digital experience for consumers, providers, and insurance professionals can be challenging.

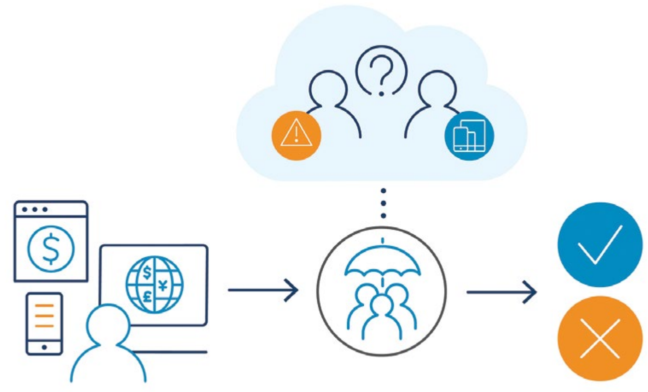
Today's consumers, providers and insurance professionals expect convenience—both in terms of ease in using digital services and in the ability to obtain service at any time and from anywhere. Multiple steps (either too many steps for authentication or too many forms to be submitted via an insurance professional or digitally) can be perceived by users as onerous. Such process complexity can affect the user's digital experience and, ultimately, result in a high abandonment rate, with consumers, providers and insurance professionals either turning to more expensive channels, such as the call center, or engaging with another insurer instead.

In this digital era, consumers have the power, at the touch of a screen, to compare prices and offerings, and even dictate how and when they want to do business with the insurer. A reputation for poor customer service or for a lapse in security can have a significant impact in this highly competitive industry. Additionally, a compromised provider or insurance professional digital account can pose a high risk to the insurer as a claims account may be used to submit hundreds of claims or generate low-cost policies.

So, the question is: How can you establish trust over digital channels so you can seamlessly welcome in both new and existing customers, as well as providers and insurance professionals, while keeping bad actors out?

The answer lies in how you assess the risk of digital identities.

To help transparently identify true users in the digital channel and help detect potential bad actors more accurately, insurers need a strong digital identity risk assessment capability to examine each user's digital footprints from various machine sensory inputs.



How do you seamlessly welcome in customers, while keeping bad actors out?

The value of strong risk assessments

Listed below are four potential benefits of conducting strong risk assessments at the outset of any digital interaction (whether it's a new customer applying for a policy, an existing client using the digital channel in lieu of a traditional channel, or a provider logging in to submit new claims).

Deliver a more seamless user experience

First, conducting strong digital identity risk assessments can help you deliver a more seamless experience to existing users every time they log into their account. With continuous, risk-based authentication, instead of burdening users with multiple authentication protocols at every log in, you have insights enabling you to only challenge those users with a high risk of malicious intent. In addition, using continuous authentication, you can evaluate users whenever they are about to perform a highly sensitive operation, thus revalidating trust and risk only when needed. Insurers that offer a poor digital experience, with additional friction for authentication, may ultimately face user abandonment of digital services to competitors or higher-cost channels.

A more seamless experience may also help insurers increase customer loyalty scores. Often, an existing customer's use of the digital channel arises due to a stressful life event—an auto accident, an illness, a loved one's death. Some of these customers may not log in to their accounts on a regular basis, and are more likely, as a result, to struggle with a complex authentication process or forgotten passwords. By making the process easier, insurers can demonstrate their commitment to help customers navigate life's challenges and use these moments as an opportunity to build greater brand loyalty. For a provider or insurance professional, every minute spent on authentication can mean lost revenue of attending to additional claims. Reducing authentication challenges without compromising on security can go a long way toward maintaining customer loyalty and preference of doing business with the insurer.

Help gain and retain customers

Second, it can help insurers gain and retain customers. Excessive authentication challenges are a significant impediment for consumers who want the freedom to buy new coverage anytime, anywhere. Give them too many hurdles to demonstrate they are who they say they are, and they may seek other insurers who can provide the frictionless experience they demand.

Help protect customer data

Third, it can support risk and policy initiatives to help protect customer data. Cybercriminals have devised many ways to circumvent authentication processes, including two-factor authentication, to impersonate users. One compromised insurance professional or provider account can expose hundreds of clients' data to a rogue actor. Strong digital identity risk assessments using passive authentication can help uncover hidden patterns indicating the user logging in isn't a legitimate customer, provider or insurance professional, but a bad actor who has obtained the user's credentials.

Help reduce operational impact

Finally, strong digital identity risk assessments can help reduce the operational impact of malicious attempts. By stopping bad actors at the outset of a digital interaction, insurers can potentially reduce the cost of manual investigations and processing as well as avoid the need to send rejection explanation letters or handle extensive data breech costs. Legacy tools with antiquated technologies often require too much ongoing human interaction. Strategies based on adaptive intelligence, leveraging more automation and decreasing dependencies on human involvement, can help increase accuracy at scale while reducing fraud risk and operating costs.

Considerations when assessing digital identities

One of the challenges in effectively assessing digital identities is that insurers face many evolving threats in the digital landscape.

Different types of crime are committed by different types of bad actors at different stages of the user interaction lifecycle—from buying insurance to submitting claims to delivering customer service. Their tactics may include:

- Creating fake or synthetic identities (identities which incorporate stolen data or add false data to real identities) for third and first-party fraud.
- Using real but stolen identities—a growing issue given the extent of user information, such as name, address, date of birth, middle name, and social security number, that's been compromised through data breaches.
- Impersonating existing customers, providers or insurance professionals to make claims, obtain payments, liquidate or take out loans against a policy, or simply steal customers' data.
- Repeatedly buying insurance from different insurers only to submit a claim and obtain a settlement.

As a result, the more data you can incorporate into your risk assessments, the greater the accuracy of your alerts. Increased accuracy can help lead to fewer false positives for your fraud team to chase and can help drive down operational costs.

Therefore, insurers should consider a wide range of data as they assess the legitimacy of each user. This includes:

- Device authenticity and spoofing evidence to help improve reliability of device fingerprinting. Device fingerprinting and associating the devices to users can support transparent authentication. However, because device fingerprinting is being spoofed by bad actors, use of it should be validated to be reliable.
- Connection and network attributes to help identify where users connect from and when, and what kinds of connections (web, mobile, VPN, etc.) and encryption they use.
- Behavioral and biometric insights to establish users' behavior patterns—including mouse movement patterns and keyboard typing cadence patterns—and to help identify anomalies.
- User journey analysis to learn how a user navigates through the application and identify anomalies to their behavior.
- Mobile carrier intelligence to gain additional insight into the potential risk of the user. For example, a user with a two-day-old burner phone is 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.
- Malicious patterns, both on an individual level and across institutions, to help detect attempts to manipulate or circumvent authentication measures, as well as identify 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 and bad actor consortium data from a worldwide network to help detect known bad actors attacking other organizations.

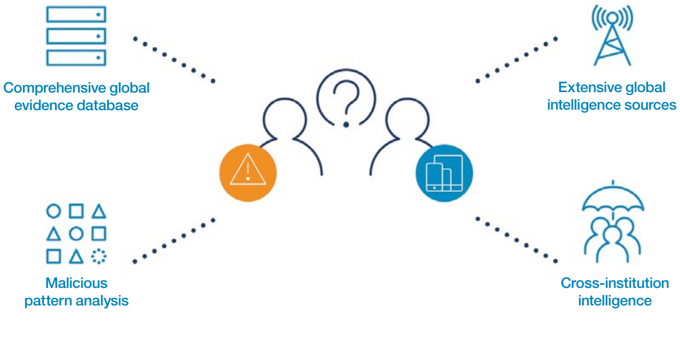
Without this wide range of data, it can be much more difficult to confirm a user is indeed trustworthy.

Establishing trust over digital channels

The opportunity is significant: When you can more accurately confirm legitimate activity, and identify potentially malicious activities, you can more easily deliver the seamless experience users demand.

IBM® Trusteer® helps insurers establish a trusted digital relationship with users right from the start of an interaction. It combines comprehensive intelligence on users' behavior, sessions and devices with real-time cognitive analytics to help transparently determine the legitimacy of every digital activity and support continuous, risk-based authentication.

To achieve this, the Trusteer solution uses a "trust but verify" approach, working behind the scenes to uncover clues in digital activity that might signal bad actors at work.


Comprehensive global evidence database
Extensive global intelligence sources
Malicious pattern analysis
Cross-institution intelligence

IBM Trusteer can help insurers establish trust over digital channels by correlating rich proprietary insights with global intelligence sources.

Validating user information behind the scenes

With a global worldwide network, IBM Trusteer incorporates a wide array of data into its risk assessment to validate user information. This data includes:

- Mobile carrier intelligence to assess if the phone number provided may indicate that the user is not trustworthy.
- Device intelligence to identify if the device being used may not be trustworthy, be it compromised by malware, spoofed by bad actors, or used in the past by a bad actor in another malicious attempt.
- Network and session intelligence to reveal a mismatch in location information or point to unique methodologies employed by cyber-gangs, such as location of their cyber sweatshops or unique tools and browsing patterns.
- Behavioral biometrics that passively identify user's behavior throughout their journey to help seamlessly separate true users from bad actors. For new customers, behavioral biometrics can detect malicious BOT attacks or known bad actor usage patterns that target identity theft compromises. For existing customers, behavioral biometrics can learn customer usage behaviors to be able to continuously and transparently validate users as they access the site to check policy information, manage claims or request account changes.
- Proprietary intelligence maintained in IBM Trusteer's global evidence database. This intelligence includes insights into previously identified evidence and known evidence on bad actors such as email addresses, phone numbers, device elements, organized crime rings and mule accounts—all gathered based on security intelligence from hundreds of organizations worldwide.

Uncovering patterns indicating malicious intent

Bad actors often demonstrate different behaviors than legitimate users. Such behaviors are often quite subtle, such as how they enter information into an application or how quickly they fill out a form. As a result, IBM Trusteer also identifies and incorporates malicious patterns into its risk assessment using machine learning to analyze a multitude of data elements of device, session and usage patterns. Some of the analyzed data elements include the following:

- Insights into the user journey, including how long users spend on a page, how the form is filled out, how fast users type, and what the journey looks like—whether it matches true user behavior or may raise a suspicion from machine sensory input that something may not be right.
- Identity linkages. Is the data being used to apply for a new policy or open a new account used in a different application or previously at another institution?
- Insights into new account activity. Is there any activity associated with malicious patterns occurring post-account creation that may signal that the account was set up by bad actors?

Leveraging cross-institution intelligence

Bad actors often use the same tactics, or the same stolen or synthetic identity elements, across different organizations. As a result, IBM Trusteer solutions also analyze malicious patterns across other providers worldwide that are protected by IBM Trusteer solutions. With this global cross-institution intelligence, IBM Trusteer can help organizations identify and detect if:

- The identity requesting to apply for coverage has already attempted to open one or more accounts at a velocity and rate similar to known malicious patterns with other providers protected by IBM Trusteer solutions.
- The device, or the same identity elements, is requesting to open multiple accounts on behalf of different users.
- The same phone number, email or address is used on multiple applications for different people.

Remaining agile with adaptive intelligence

What tactics will bad actors use in the future? To help insurers gain the greatest advantage in a landscape that's constantly changing, IBM Trusteer enlists both advanced technologies and world-class security specialists to track daily changes in the threat landscape.

The Trusteer security infrastructure continually incorporates new intelligence using the following:

- Machine learning capabilities, including layers of cognitive fraud detection and analytics, to understand, detect, and predict the risk of malicious attempts during digital activities
- Global, real-time threat intelligence and global insights delivered through the cloud
- Emerging patterns tracked by IBM X-Force®, one of the world's most experienced commercial security research teams

This continual augmentation of data provides a new dimension of insight and makes the platform truly versatile. It can help insurers to quickly understand, detect and predict the risk of malicious attempts, protect against evolving cybercrime tactics, increase the accuracy of assessments and reduce operational costs—all while enabling a seamless customer experience.

Building your own polices with IBM Trusteer advanced intelligence

Insurers often must deal with a variety of global and local business requirements, depending on the patterns of use they encounter and according to each institution's sensitivity to risk.

As a result, many organizations seek control over the models they use when evaluating potential risk. The IBM Trusteer policy manager provides organizations with visibility into models, ability to adapt models, and flexibility to rapidly validate the effectiveness of and apply new countermeasures so they can build new account policies to address internal and external requirements and regulations.

The policy manager uses machine learning to synthesize knowledge of current and emerging threats and trends that organizations face and provides the ability to customize new policies, simulate rules and adapt risk models automatically, or based on specific intelligence and insight—all without prerequisite knowledge or advanced skills.

Conclusion

The digital transformation is creating new opportunities for insurers to both strengthen their engagement with existing customers, providers and insurance professionals, as well as attract new customers and providers through innovative products and services. In the digital age, consumers, providers and insurance professionals expect the ability to obtain or change information, claims and coverage on demand.

As a result, insurers' success in the coming years may be as dependent on how easy it is for users to use their digital channels as what digital products and services they offer. More importantly, as insurance firms look to expand and diversify offerings, solutions, like the Trusteer solution, can afford dynamic abilities to crossover into that next venture.

App or process complexity, such as multiple authentication challenges, can potentially lead to user frustration, affecting satisfaction scores and possibly resulting in abandonment of the digital channel experience for a higher-cost channel or a competitor's offering. Conversely, a seamless digital experience can help insurers build, or repair, brand loyalty and reputation in the marketplace for customer service.

By establishing a trusted digital relationship with users, insurers can enable legitimate consumers to apply for new policies and legitimate providers and insurance professionals to log in to their accounts without onerous authentication requirements, while requiring users identified as high risk to fulfill additional authentication requirements.

How will you welcome true customers into your digital channel? How will you maintain that digital trust? How will you keep bad actors out?

The IBM Trusteer solution is designed to help insurers establish that trusted digital relationship quickly and transparently. It validates user information passively, uncovers patterns that can signal malicious intent, and draws on intelligence gathered from global network of financial service organizations to help your organization establish that the user is a legitimate customer and not a bad actor in disguise.

For more information

To learn more about Trusteer digital identity risk assessment solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security/trusteer

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 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 performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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