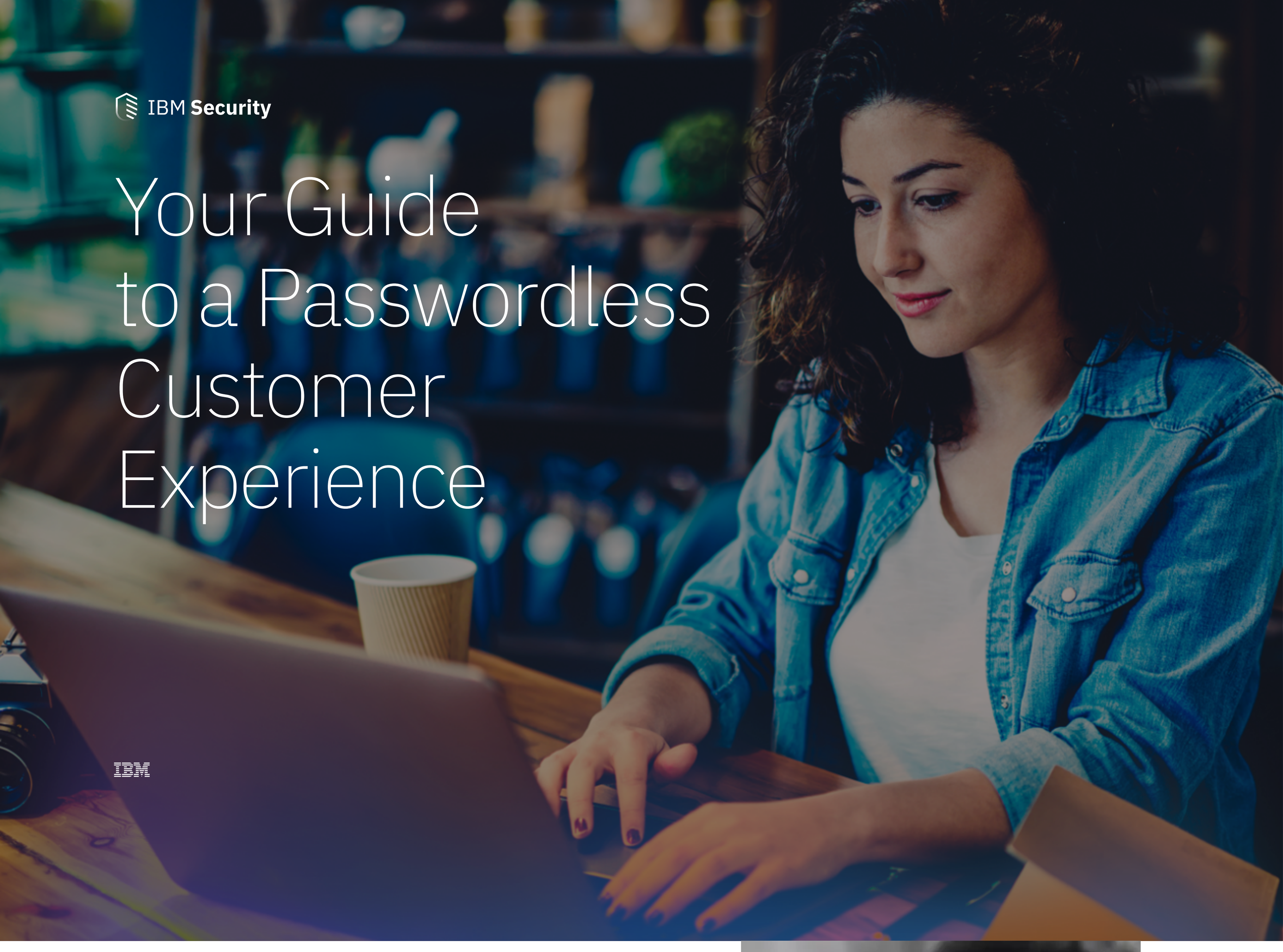
IBM Security

Your Guide to a Passwordless Customer Experience



Imagine a Secure World — Without Passwords

When users open a new online account, they are likely to reuse a password they already have. It makes sense why: At a moment's notice, any one of us might need to recall the passwords for around 90 accounts.[1] Customers have password fatigue so they may devise workarounds and ad hoc solutions to help keep things simple but this can also sacrifice security. In our attempt to find a balance between simplicity and security, many of us just end up shuttling back and forth between the two, sometimes opting for security, and at other times opting for simplicity.

In fact, 59 percent of consumers mostly or always use the same password, while 42 percent also store passwords in documents on their devices.[2] Fernando Corbato — the man who invented the technique for using computer passwords back in the early 1960s — even called the password system, "kind of a nightmare."[3]

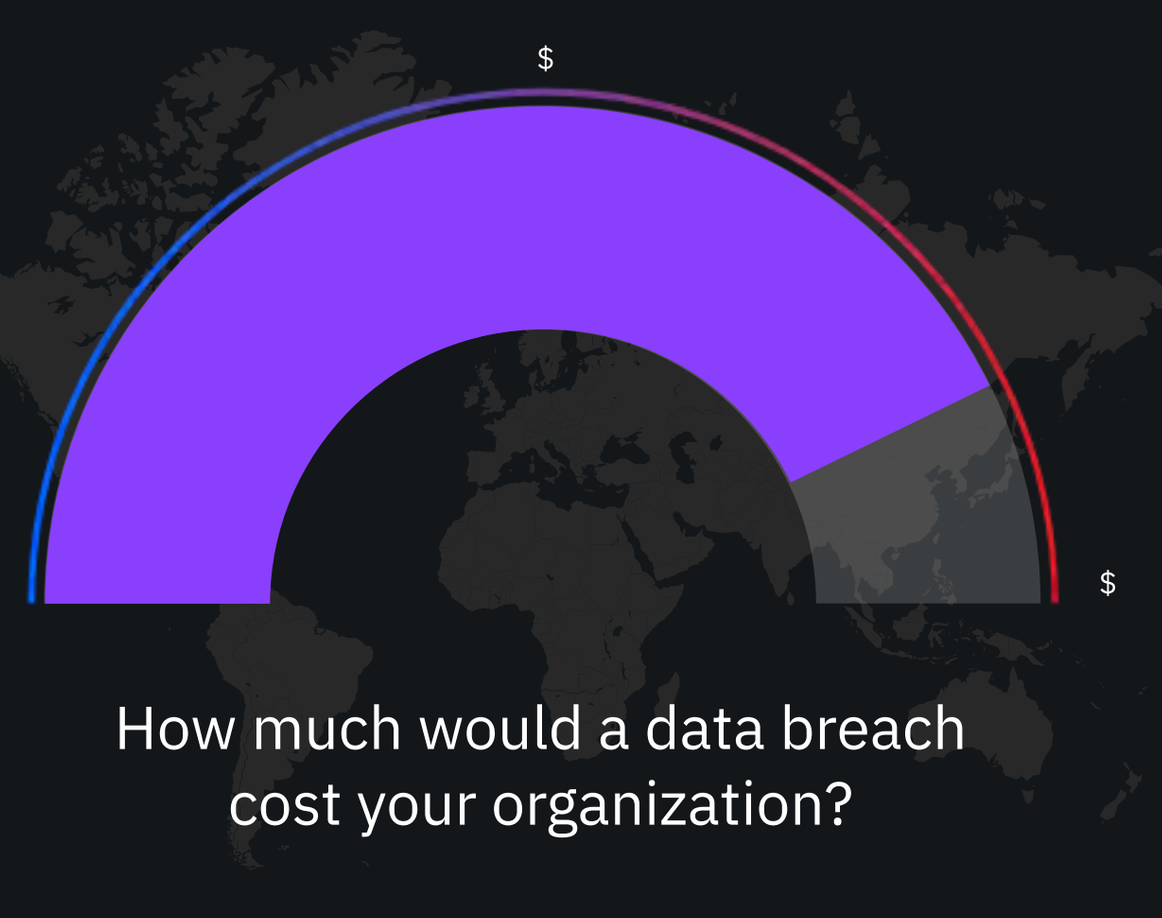
Now imagine a world where your digital identity isn't based on a random set of characters that you need to remember. Instead, you seamlessly gain access to your account at a swipe of a finger or a click of a button and go about your business with the same confidence and trust that you're securely logged into your account. It's possible and, even better, already exists. But how do you create this passwordless experience for your customers?

Photo via Computer History Museum

Step Out of Your Comfort Zone

The reality is mega breaches are a growing problem and they aren't going away or getting any cheaper. The average cost for each lost or stolen record containing sensitive and confidential information is $148, according to the 2018 Cost of a Data Breach Study by the Ponemon Institute sponsored by IBM. The global average cost for an individual organization of getting a data breach is $3.86 million (in US dollars).

View 2018 Cost of a Data Breach Report →



How much would a data breach cost your organization?

Businesses have reacted to the rise in fraud (and the resulting loss of customer trust) by requiring users to make their passwords more complex. However, to create a passwordless experience, the challenge is to not let the threat of breaches lull you into the false comfort of forcing stricter password regulations. Doing so can impact your business beyond just the cost of a data breach.

As security measures become less intuitive, they become increasingly frustrating to users. In turn, this adds to the cost of doing business. Customers might proceed to other channels, leaving your site altogether or contacting the call center to gain access to their account.

Call centers — once thought of as a cost savings — can drive up expense. For example, it's estimated that business spend $1.3 trillion to service call centers every year.[5] Aside from the added cost, call centers can also create a fractured customer experience.

As a result, a password-first comfort zone might actually create an uncomfortable customer experience that can directly impact your bottom line.

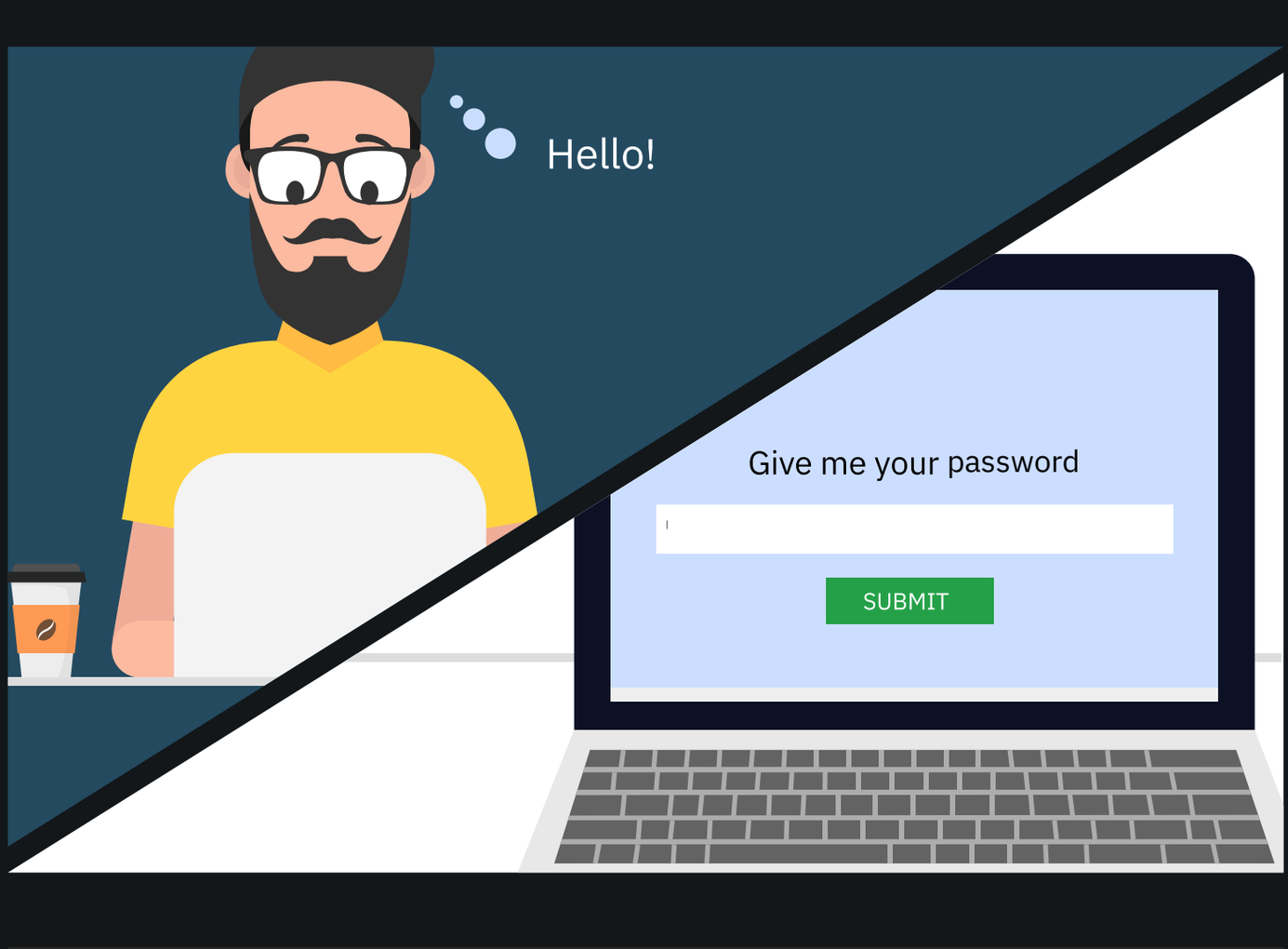
KEY POINT

It's estimated that business spend $1.3 trillion to service call centers every year.

Password Frustration vs Passwordless Bliss

Tour Trusteer →

The traditional method is based on users proving their identities.



User: Hello!
Site: Give me your password.
User: It's LongPasswordWithNumbersAndSymbols&#!
Site: Wrong.
User: Oh, that's right. You made me change it. It's now ExtraLongPasswordWithNumbersAndSymbols&#!
Site: Code sent to your phone. You have 10 minutes to enter the code.
User: It's 123456!
Site: Try again. That code expired a minute ago.
User: It's 36912!
Site: You may enter.

The passwordless experience is balanced and based on trust.

User: Hello!
Site: I see you are on your previously enrolled phone.
Site: I also see that phone isn't jailbroken or rooted.
Site: You are connecting from your usual region and there are no signs of malware on the device.
Site: Your activity is also in a low-risk area. . .
Site: Welcome, User!

Don't Play the Hoop Game

Organizations are prone to deploy initiatives that default to a process of not trusting anyone, forcing verification, and then only allowing the least possible access. This overly intrusive method puts users through the "hoop game" where they are asked to jump through hoop after hoop as they authenticate themselves to prove their own digital identities.

This means your customers might feel they are being treated like potential bad actors — when bad actors are actually comparatively rare.

< 0.1%

IBM Trusteer research shows less than 0.1 percent of users are suspect

Your goal should be to treat your customers as customers – people who want to use your products and services for their intended purpose and benefits – not bad actors.

Authentication and convenience don't need to be at odds. Stop worrying about finding balance between the two, and instead look for a solution that offers both strong security and the frictionless process your customers want.

Avoid the "hoop game" and take steps to deliver a frictionless experience that provides both authentication and convenience.

Build a Foundation for Passwordless

Passwordless authentication starts with having the proper user context. When you have contextual data set against a decision-making framework, you can deliver a seamless end-user experience for the vast majority of your legitimate users.

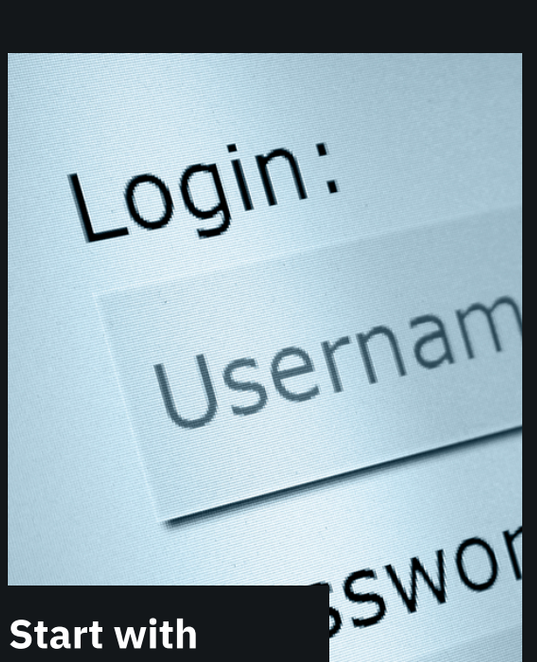
There are three core components that sit behind this goal:
- Minimize security interactions that remove focus from the service you're providing to the customer.
- Progressively learn about the user end-to-end, across their digital journey.
- Continuously develop a comprehensive view of the user through interaction — which in turn increases trust.

You must transparently analyze the authenticity of the user at every transaction to build the foundation of a passwordless experience.

KEY POINT

Your goal should be to treat your customers as customers – not bad actors.

Digital Identity Trust Begins with Context



Start with the user

- Is this a human or a bot?
- Is there any malicious evidence available?

Onboard the user's device

- Is this a pre-paid phone?
- Has it been rooted or jail-broken?
- Is this a legitimate phone number or email?

Assess the user's activity

- Are these known malicious patterns?
- Has the out-of-band authentication (OOB) been bypassed?

Identify the user's network

- Is there a logon proxy?

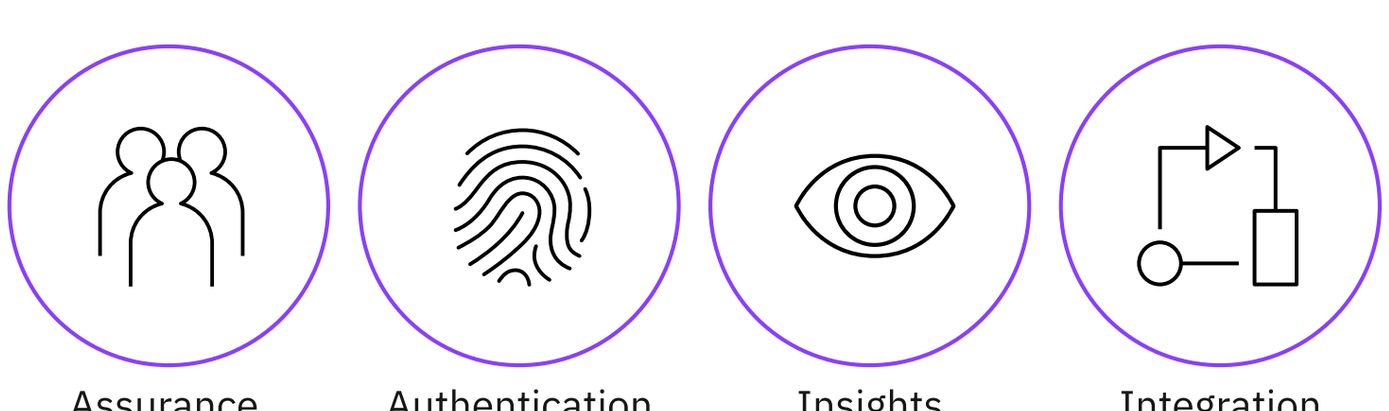
Monitor the user's behavior

- Is this a known user-behavior pattern?
- Are there unusual automated mouse movements?

Understanding Your Digital Trust Framework

Your foundation for passwordless security built with contextual data is only as good as how you apply that context against a digital trust framework. Ultimately, your framework should be dynamic and flexible. It should give users access to different layers of security depending on how much contextual information has been connected to the user.

Here are four building blocks to help you apply a digital trust framework:



These interlocking blocks allow your security to be continuous and always-on, largely working in the background. It allows you the flexibility to implement policies as the situation requires. You can then easily implement new policies based on your ever-changing, specific business needs.

Let Customers Know You Are Protecting Them

Protection can't be invisible because your customers might not believe you are protecting their personal data — and *they* may lose trust. Create trust with your users by letting them know you are protecting their digital identities in a seamless and flexible way. You accomplish this by:

- Including authentication enrollment
- Allowing your customers to choose their verification methods
- Using step-up authentication, when needed

You know that passwordless doesn't mean securityless.
Make sure your customers realize this.

KEY POINT

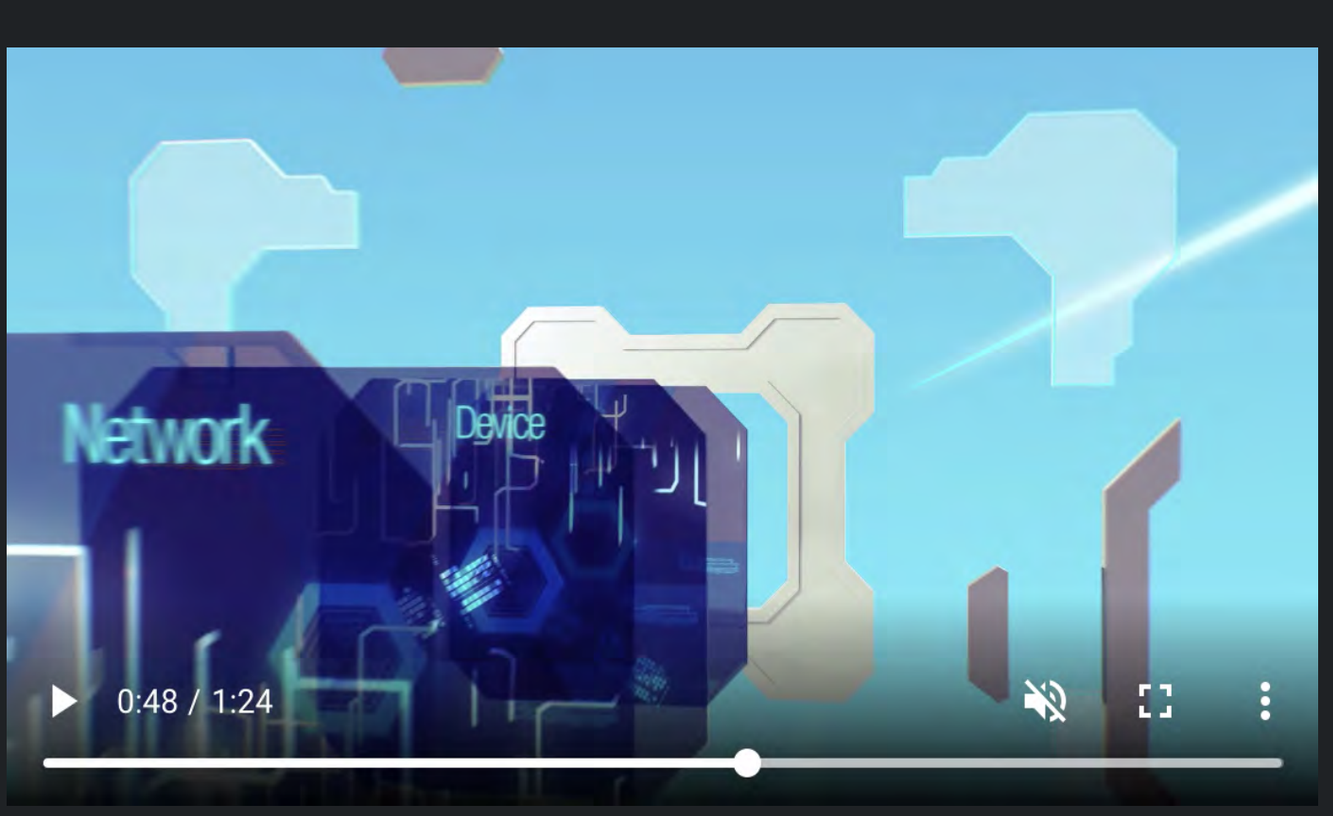
You know that passwordless doesn't mean securityless. Make sure your customers realize this.

You Can Still React to Risky Behavior

The passwordless environment does not mean reducing the level of security. When risky behavior is detected, and authentication involving interaction with the user is appropriate, you need to act.

The IBM Trusteer Pinpoint products work behind the scenes, continuously authenticating users throughout their digital journeys, from guest users to new account setups. They operate throughout customers sessions as they consume services so there is no interference with their experience and you can still protect and react to fraudulent users when necessary.

By using cloud-based intelligence, backed by artificial intelligence and machine learning, Trusteer helps you welcome both new and existing customers, while protecting against malicious users.



There is a Cost to Doing Nothing

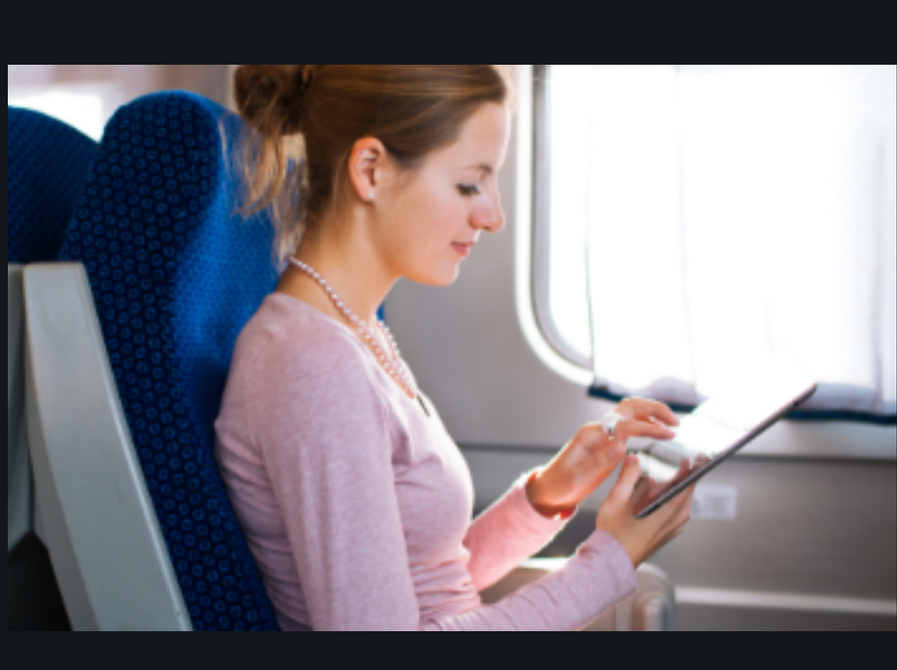
There is an inherent cost to doing nothing, in the form of declining competitive value. According to Gartner, by 2022, 60 percent of large and global enterprises, and 90 percent of midsize enterprises will implement passwordless methods in more than 50 percent of use cases — an increase from fewer than five percent today.[6] Businesses unable to use machine-learning capabilities for user authentication may lose market share as others provide customers with the assurances they require.

KEY POINT

Businesses unable to use machine-learning capabilities for user authentication may lose market share

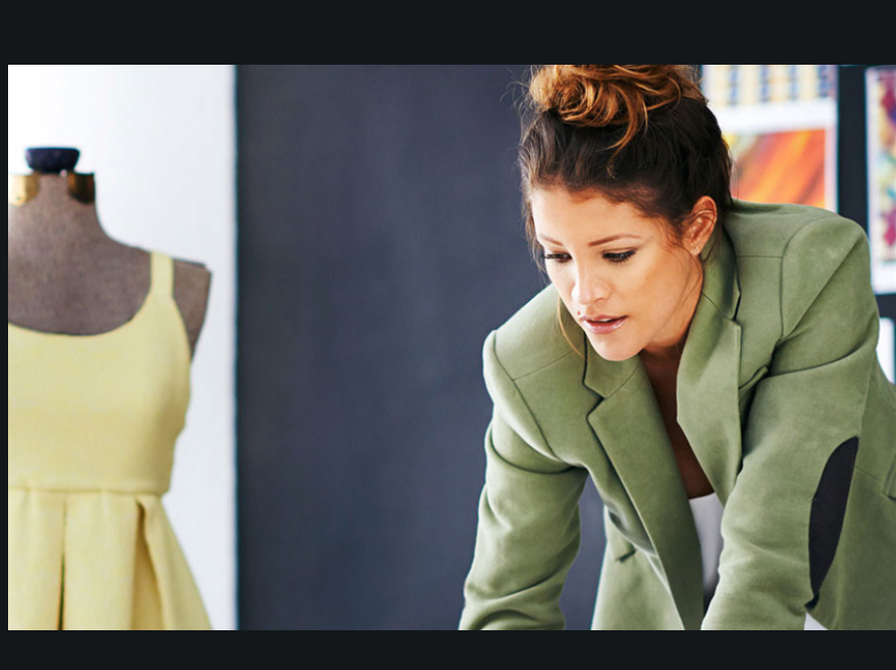
Trust is fundamental to business and security is vital to trust.

Next steps



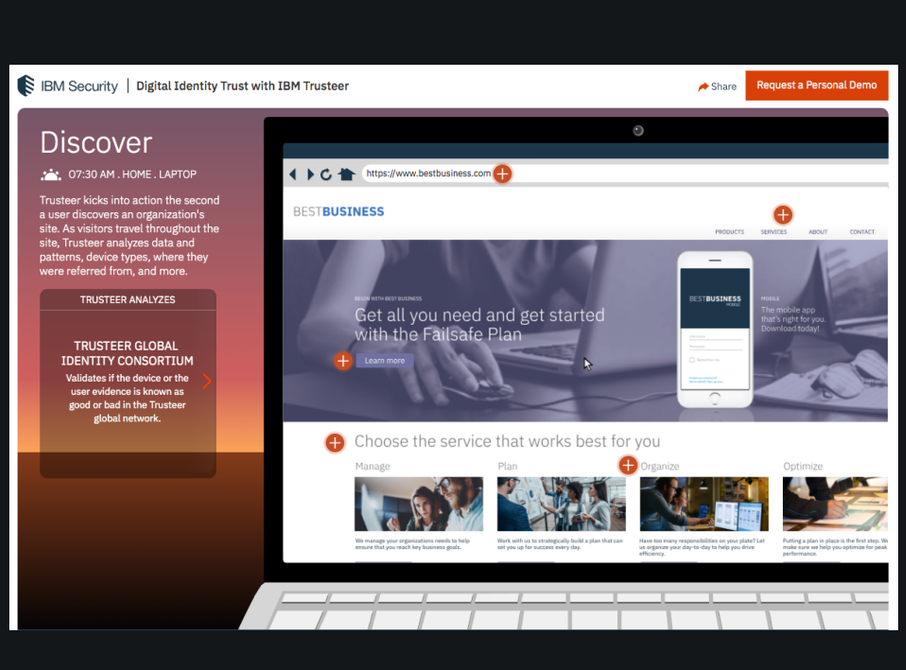
IBM Trusteer Solutions Brief
Creating a seamless digital customer journey.

Read solution brief



Digital Identity Trust eBook
Build a circle of identity trust.

Download the eBook



Tour Trusteer
Discover digital identity trust with IBM Trusteer.

Take the tour

Sources

1. Phys.org, When Customers Forget Their Passwords, Business Suffers, Tim Johnson, June 20, 2017
2. LastPass, New Research: Psychology of Passwords, Neglect is Helping Hackers Win, Katie Petrillo, May 1, 2018
3. Wall Street Journal, Man Behind the First Computer Password: It's Become a Nightmare, Danny Yadron, May 21, 2014
4. IBM and Ponemon Institute, Cost of a Data Breach Study, July 2018
5. IBM, How Chatbots Can Help Reduce Customer Service Costs by 30 Percent, Trips Reddy, October 17, 2017
6. Gartner, Market Guide for User Authentication, Ant Allan and David Mahdi, November 26, 2018