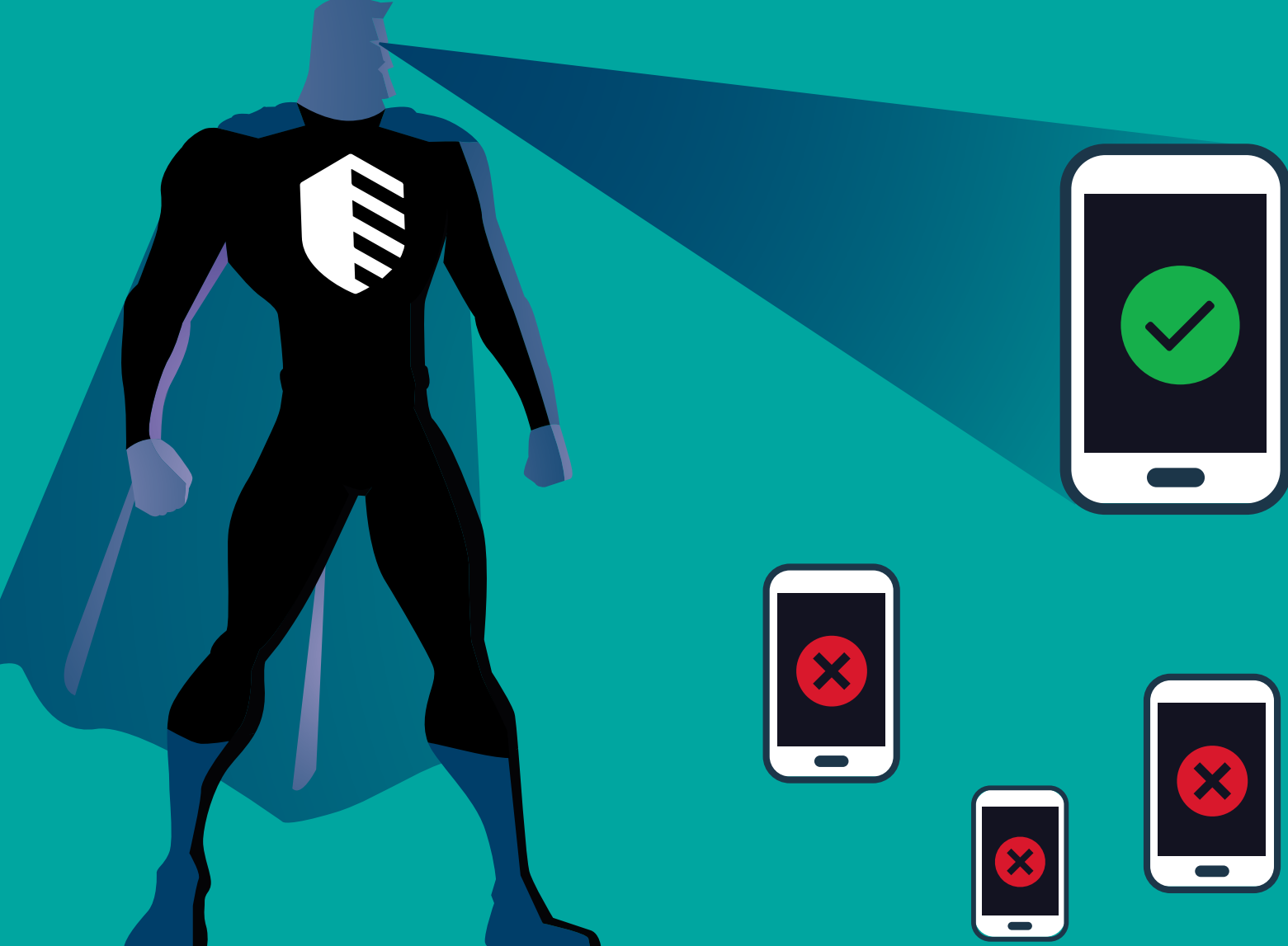


# GET X-RAY VISION FOR DIGITAL ACTIVITY

SEE THROUGH USER INTERACTIONS TO BUILD IDENTITY TRUST



## LOOK BENEATH THE SURFACE

Your customers expect a frictionless digital experience. But digital fraud is forcing organizations to create complex and frustrating authentication. This can lead to poor adoption rates and high abandonment. You need ways to know if new and existing customers are legitimate—without creating a painful user experience.

### Build digital identity trust

Multilayered *dynamic risk assessments* help provide a clear view of customer-provided data:



Unobtrusively analyzes user behavior



Compares gathered information to known users and fraud vectors



Transparently identifies fraudulent transaction attempts

All of this can help you welcome in new and existing customers, while keeping bad actors out.

# 1B+

Monthly user sessions monitored by IBM® Trusteer®<sup>1</sup>

## UNCOVER TRANSACTION ATTRIBUTES

When data looks authentic but isn't verified, it's tricky to approve online transactions. But with...

Continuous and transparent identity assurance

A scalable and agile cloud platform

Advanced artificial intelligence and machine learning

...you can shine a light on transaction attributes—from where the transaction originates to exact user interaction data.

Device intelligence: Transaction origin, malware or spoofing evidence

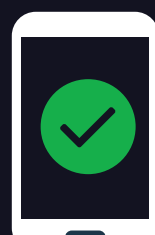
Connection analytics: Customer sign-on location, risky ISP or mobile carrier

Browser details: Vulnerable version or malicious extensions

Passive biometrics: Script-entered data, abnormal mouse movements

## SEE INSIDE USER ACTIVITY

Transaction data + IBM X-Force® threat intelligence = digital identity trust across the omnichannel customer journey.



### Application details

Name: Jonathan Smith  
Email: jasifasfdonny@gmail.com  
Address: London, England  
Mobile number: 441833650723

IP geolocation is London, England: **Match**  
Device type is: **Mobile**  
Device status: **Reachable**  
Email domain name: **Match**  
Typing pattern: **Manual entry**  
Time on page: **10 minutes**

Applications in this name in last month: **0**  
Applications from the device in last month: **0**



### Application details

Name: John Doe  
Email: johndoe@email.com  
Address: Atlanta, GA, USA  
Mobile number: 447398377960

IP geo location is Novosibirsk, Russia: **Mismatch**  
Device type is: **Prepaid**  
Device status: **Unreachable**  
Email domain name: **Risky**  
Typing pattern: **Copy and paste**  
Time on page: **30 seconds**

Applications in this name in last month: **0**  
Applications from the device in last month: **0**

# 500+

Organizations that rely on IBM Trusteer solutions

## REVEAL DIGITAL IDENTITY TRUST

With IBM Trusteer Pinpoint™ Assure, you can:



Help provide a more secure experience across the digital lifecycle



Seamlessly identify true customers and keep bad actors out



Leverage global X-Force security data to identify evolving threats



Improve customer experience while helping to reduce fraud

Read

“Accelerating growth and digital adoption with seamless identity trust” to learn more about how you can establish digital identity trust across the omnichannel customer journey.



© Copyright IBM Corporation 2018. All Rights Reserved. IBM, the IBM logo, ibm.com, Trusteer, Trusteer Pinpoint, and X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States.

1 “LexisNexis Card Issuer Fraud Study, 2016,” LexisNexis, 2016.

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.