Introducing the IBM Trusteer Digital Identity Trust Score

Webinar

Sep 18, 2019

Maxim Shifrin, Trusteer Offering Manager, IBM
Trusteer Risk Score – current situation

- Reason
  - Recommendation
    - Allow
    - Allow and Restrict
    - Block/Deny
    - Authenticate

No granularity between 0 and X

Rest of population – 99.95%

Risk population 0.01%-0.05%

For 1M sessions, generating 100-500 alerts

- Risk Score is used by customers:
  - ~90% for Fraud use case
  - ~10% for RBA use cases
- Typically passed to a centralized risk engine
- High score generates alert
- Metrics – DR (detection rates) and FP (false positives)
From Risk Score to Trust Score

Granular score

- Reason
  - Recommendation
    • Allow
    • Allow and Restrict
    • Block
    • Authenticate

Rest 99.95% of the population
Divided into different levels of Trust

- Trust Score may be used by customers in 3 main use cases:
  • (Current state) Fraud – Generating recommendation and alert upon high risk activities
  • Seamless Risk Based Authentication – get the right authentication decision based on a Trust level
  • Reduce Operational Cost - Granular trust score can reduce FP in centralized risk engine systems
  • Only High score generates alert – no change from current state

Sample numbers, split of the population
Introducing the IBM Trusteer
digital identity trust score

How you build your seamless authentication strategy?
Are you calling for step-up authentication only when needed?

<table>
<thead>
<tr>
<th>Value Propositions</th>
<th>Key Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduce friction caused by step up authentication</td>
<td>• Provide digital identity trust on every digital interaction</td>
</tr>
<tr>
<td>• Support PSD2 scenarios</td>
<td>• Customize policies based on trust score</td>
</tr>
<tr>
<td>• Reduce operational cost caused by MFA</td>
<td>• Visibility on a balance between user experience and risk</td>
</tr>
<tr>
<td>• Reduce operational cost caused by high false positive rates in integrating risk engines</td>
<td></td>
</tr>
</tbody>
</table>
## Trust Score Reason examples

<table>
<thead>
<tr>
<th>% in Population</th>
<th>Label</th>
<th>Risk reasoning examples</th>
<th>Access Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0.05%</td>
<td>High risk</td>
<td>High risk indication Known fraudster’s device/pattern.</td>
<td>Block</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allow and Restrict</td>
</tr>
<tr>
<td>&lt;10%</td>
<td>Medium risk</td>
<td>Suspicious user anomaly/Risk indicator</td>
<td>Allow and Restrict</td>
</tr>
<tr>
<td>20%</td>
<td>Low risk</td>
<td>• Unknown device, minor user anomaly, no risk indicators.</td>
<td>Authenticate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unusual geolocation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access from hosting service</td>
<td></td>
</tr>
<tr>
<td>30%</td>
<td>Trusted</td>
<td>• New device for the user, but known good in Trusteer consortium</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40%</td>
<td>Highly trusted</td>
<td>• Known device for the user’s account</td>
<td>Allow (transparent authentication)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User identification using behavioral biometrics</td>
<td></td>
</tr>
</tbody>
</table>
Trust Score Components

**Device & User Similarity Assessment**
Assessment of the current session’s device and user attributes compared to past activities in the account.

**Risk Assessment**
Assessment of the current’s session risk parameters.

**Behavioral Biometrics Assessment**
Assessment of the current’s session behavioral biometrics attributes compared to past activity in the account.

**User Routine Assessment**
Assessment of the current session timeline parameters based on the user’s activity patterns.

**Un-Authorized Access**
A mechanism to deal with unauthorized accesses to the account, prior to the fraudulent session by the fraudster.
Digital identity trust lifecycle powered by AI and machine learning

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

<table>
<thead>
<tr>
<th>ESTABLISH</th>
<th>SUSTAIN</th>
<th>CONFIRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pinpoint Assure</td>
<td>Pinpoint Detect</td>
<td>Pinpoint Verify</td>
</tr>
<tr>
<td>Assess risk of new and unknown digital identities</td>
<td>Dynamic risk assessment and authentication of known digital identities</td>
<td>Increase trust level with flexible, strong authentication</td>
</tr>
</tbody>
</table>

New Feature: Trust Score

Incorporates:

- Rapport
  Detect & remediate malware & protect against phishing attacks
- Mobile
  Exposes mobile risk to allow account compromise mitigation
- IBM Safer Payments
  Omnichannel fraud protection

INTEGRATION
Thank you

Follow us on:

ibm.com/security
securityintelligence.com
ibm.com/security/community
xforce.ibmcloud.com
@ibmsecurity
youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM’s current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.