

# Introducing the IBM Trusteer Digital Identity Trust Score

Webinar

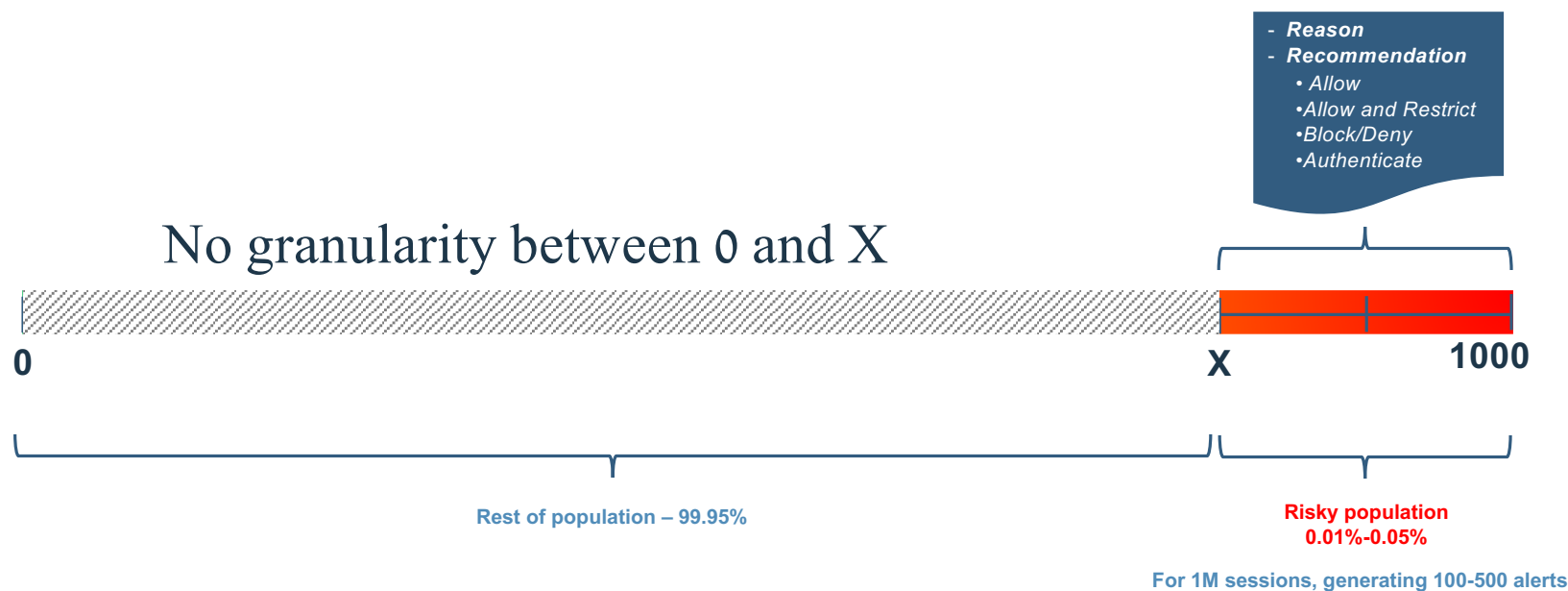
Sep 18, 2019

Maxim Shifrin, Trusteer Offering Manager, IBM

**IBM Security**

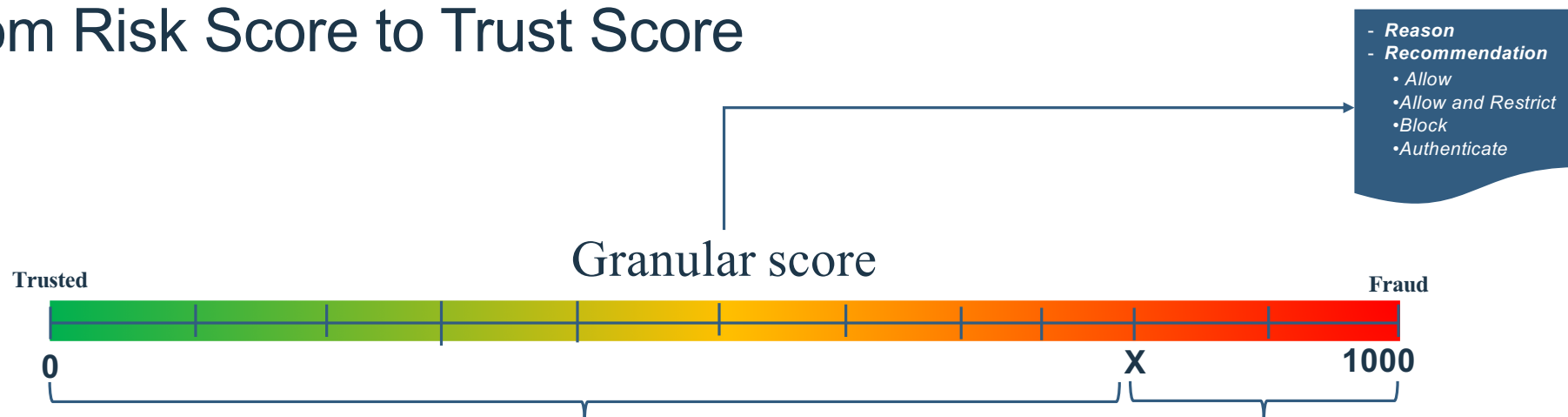


## Trusteer Risk Score – current situation

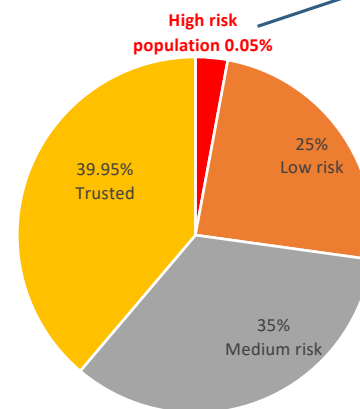


- Risk Score is used by customers:
  - ~90% for Fraud use case
  - ~10% for RBA use cases
- Typically passed to a centralized risk engine
- High score generates alert
- Metrics – DR (detection rates) and FP (false positives)

# From Risk Score to Trust Score



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



Sample numbers, split of the  
population

- 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

# 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?

## Value Propositions

- Reduce friction caused by step up authentication
- Support PSD2 scenarios
- Reduce operational cost caused by MFA
- Reduce operational cost caused by high false positive rates in integrating risk engines

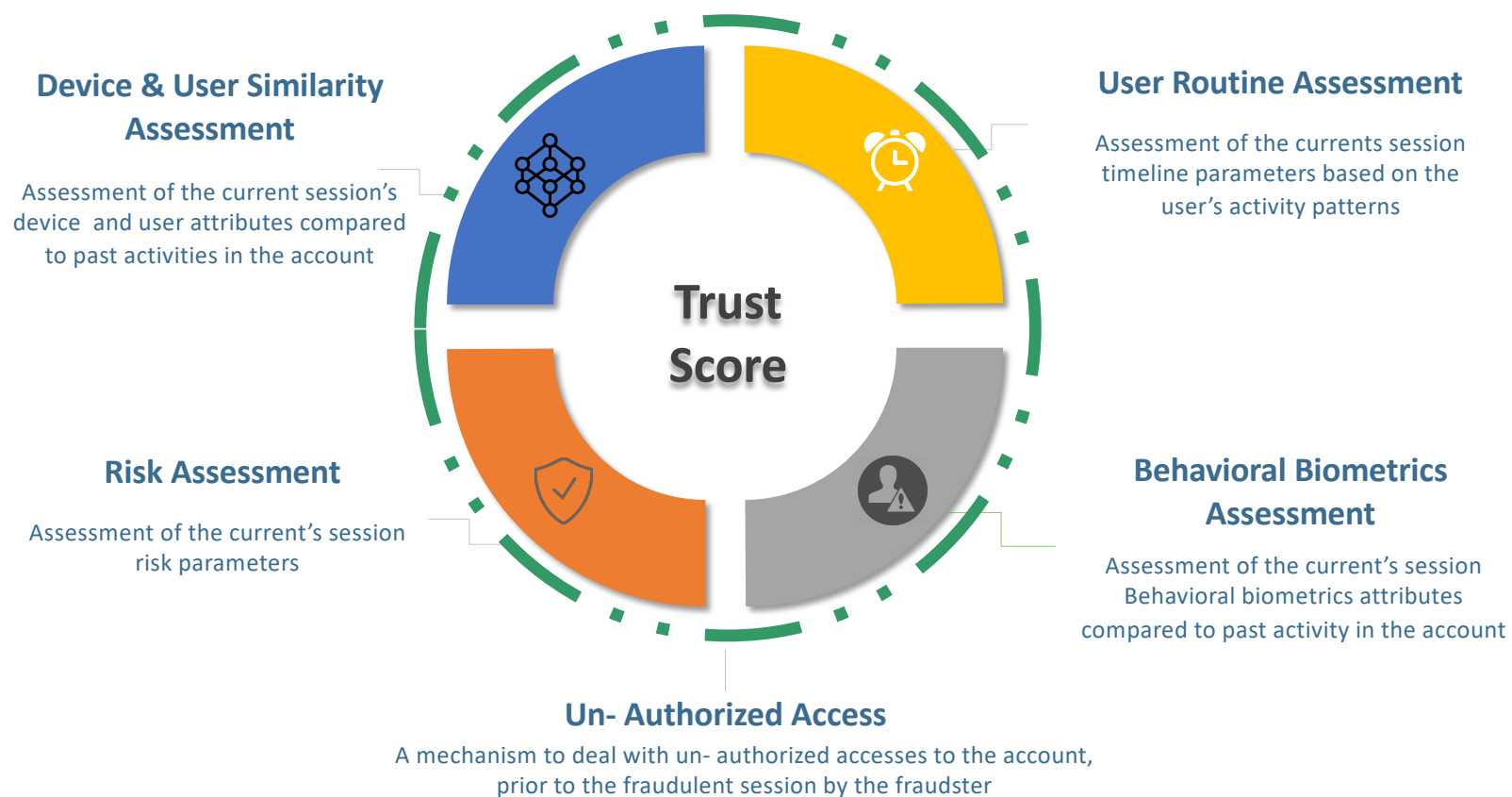
## Key Capabilities

- Provide digital identity trust on every digital interaction
- Customize policies based on trust score
- Visibility on a balance between user experience and risk

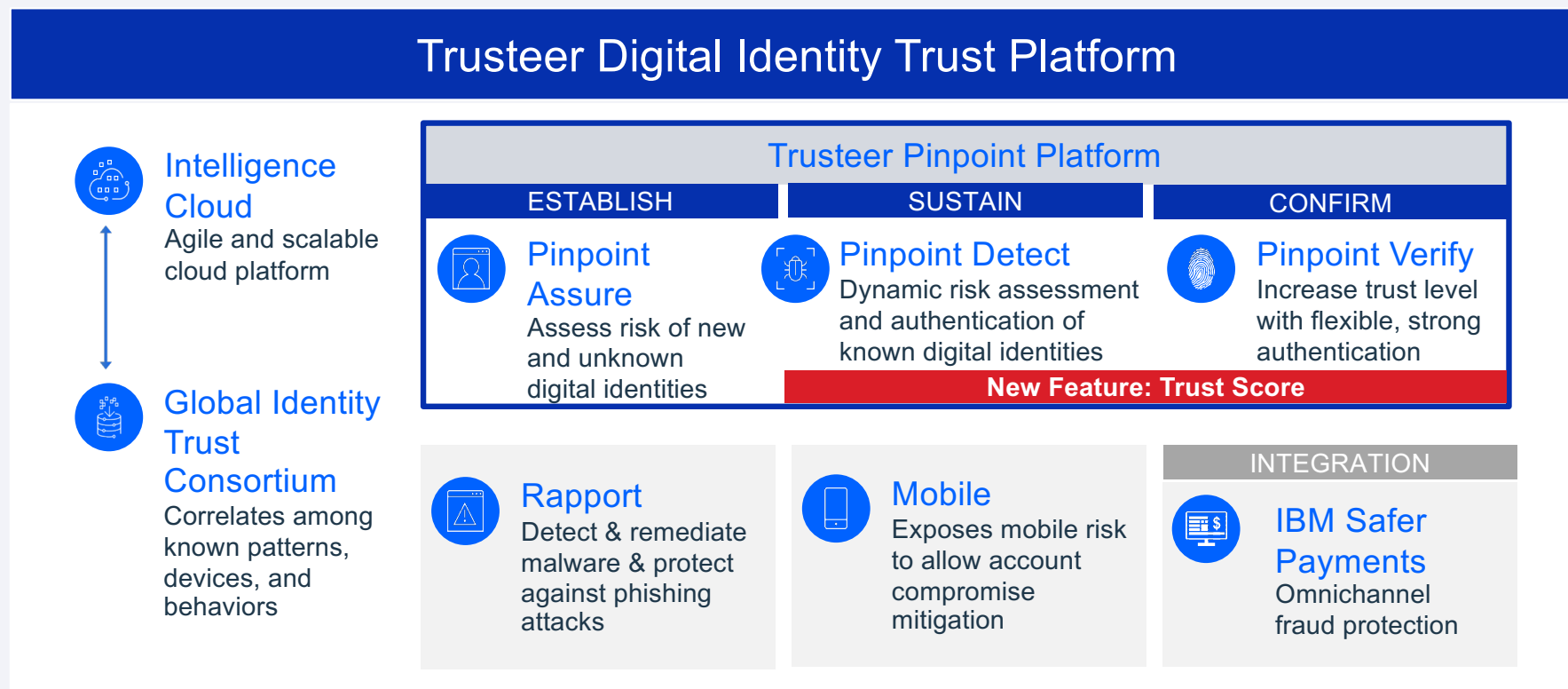
## Trust Score Reason examples

% in Population	Label	Risk reasoning examples	Access Recommendation	
<0.05%	High risk	High risk indication Known fraudster's device/pattern.	Block Allow and Restrict Authenticate	EXISTING
<10%	Medium risk	Suspicious user anomaly/Risk indicator	Allow and Restrict	
20%	Low risk	<ul style="list-style-type: none"> <li>Unknown device, minor user anomaly, no risk indicators.</li> <li>Unusual geolocation</li> <li>Access from hosting service</li> </ul>	Authenticate	NEW
30%	Trusted	<ul style="list-style-type: none"> <li>New device for the user, but known good in Trusteer <u>consortium</u></li> </ul>	Allow	
40%	Highly trusted	<ul style="list-style-type: none"> <li>Known device for <u>the user's account</u></li> <li>User identification using behavioral biometrics</li> </ul>	Allow (transparent authentication)	

# Trust Score Components



# Digital identity trust lifecycle powered by AI and machine learning



# Thank you

Follow us on:

[ibm.com/security](https://ibm.com/security)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[@ibmsecurity](https://twitter.com/ibmsecurity)

[youtube/user/ibmsecuritysolutions](https://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.

**IBM Security**





The image features the IBM logo, which consists of the letters "IBM" in a bold, sans-serif font. The letters are white and are set against a dark blue background. The background has a subtle gradient, transitioning from a lighter blue at the top to a darker blue at the bottom. The logo is centered horizontally and vertically within the frame.