Introducing the IBM Trusteer Digital Identity Trust Score

Webinar

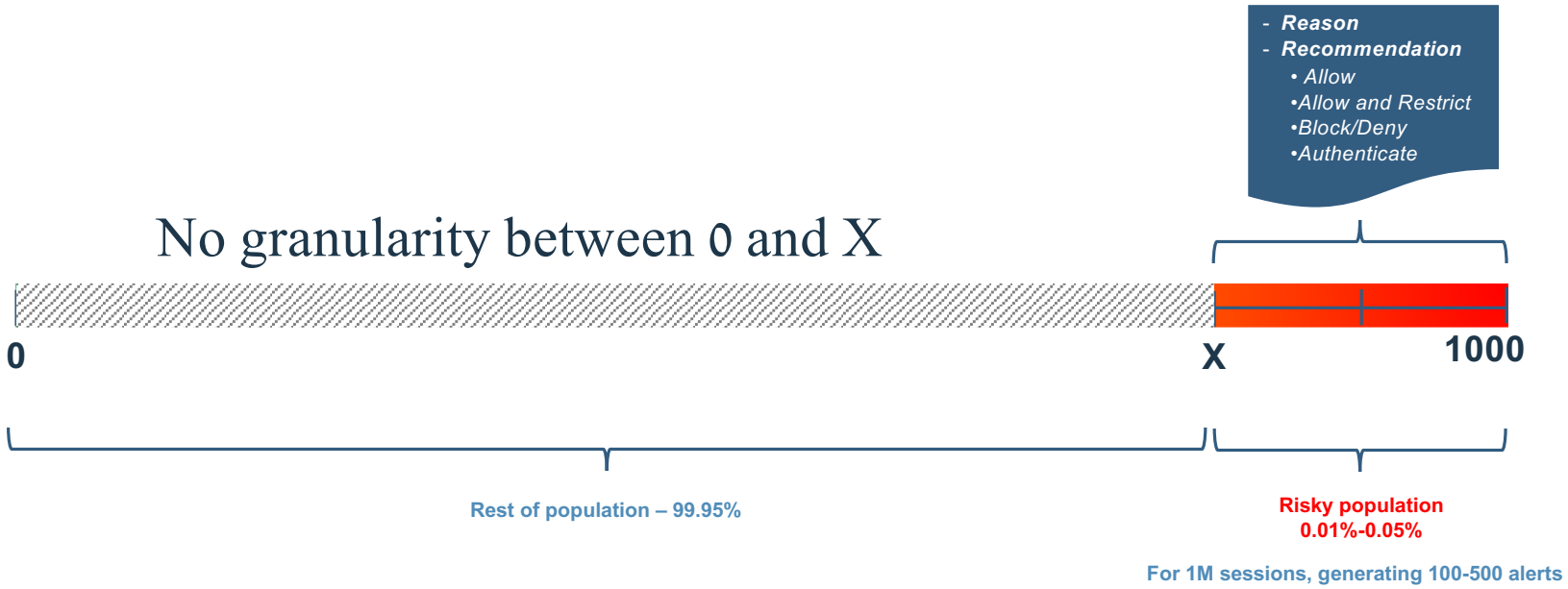
Sep 18, 2019

Maxim Shifrin, Trusteer Offering Manager, IBM

IBM **Security**

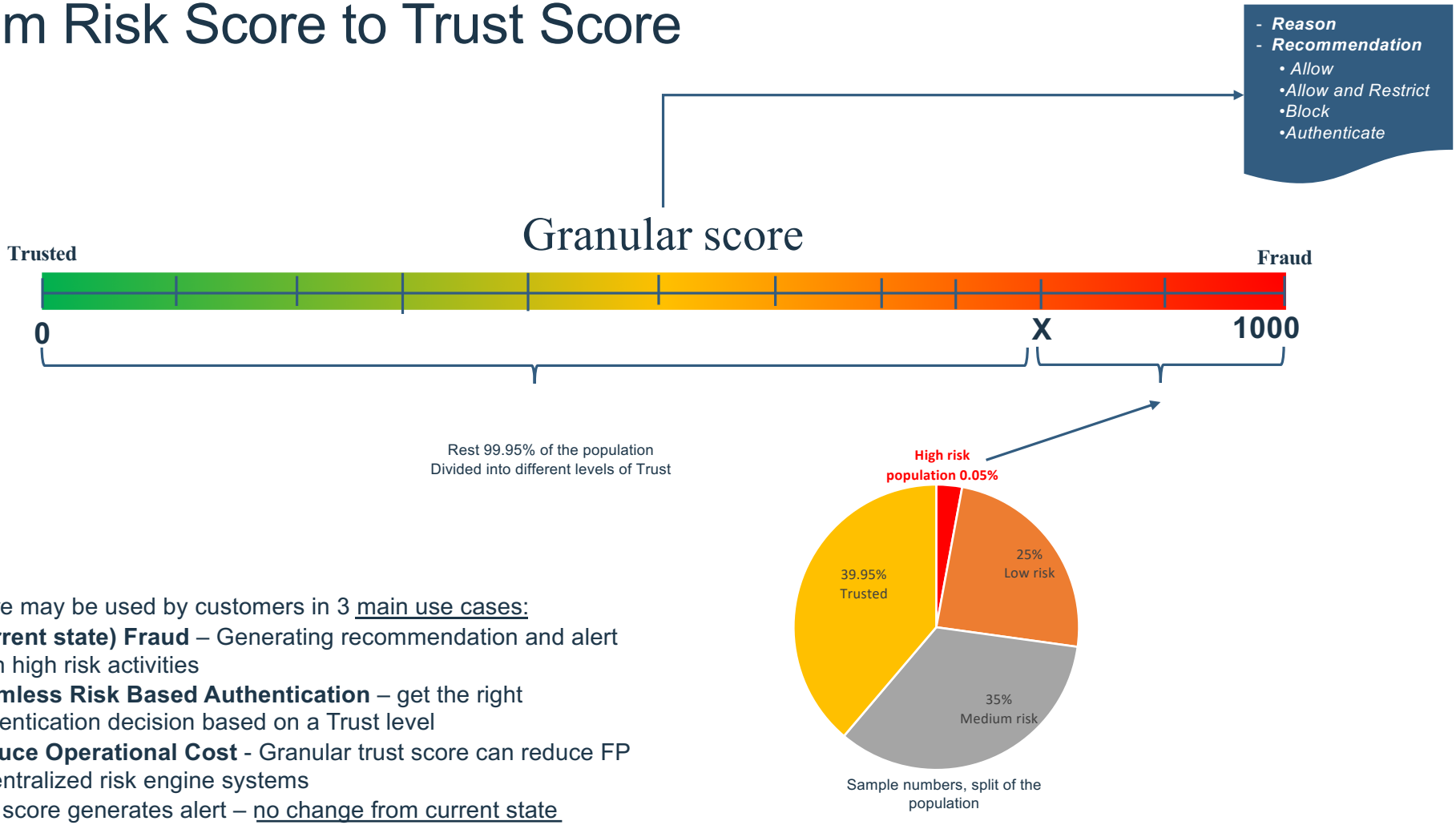
IBM

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



- 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
<10%	Medium risk	Suspicious user anomaly/Risk indicator	Allow and Restrict
20%	Low risk	• Unknown device, minor user anomaly, no risk indicators. • Unusual geolocation • Access from hosting service	Authenticate
30%	Trusted	• New device for the user, but known good in Trusteer consortium	Allow
40%	Highly trusted	• Known device for the user's account • User identification using behavioral biometrics	Allow (transparent authentication)

EXISTING

NEW

Trust Score Components

Device & User Similarity Assessment

Assessment of the current session's device and user attributes compared to past activities in the account

User Routine Assessment

Assessment of the currents session timeline parameters based on the user's activity patterns

Risk Assessment

Assessment of the current's session risk parameters

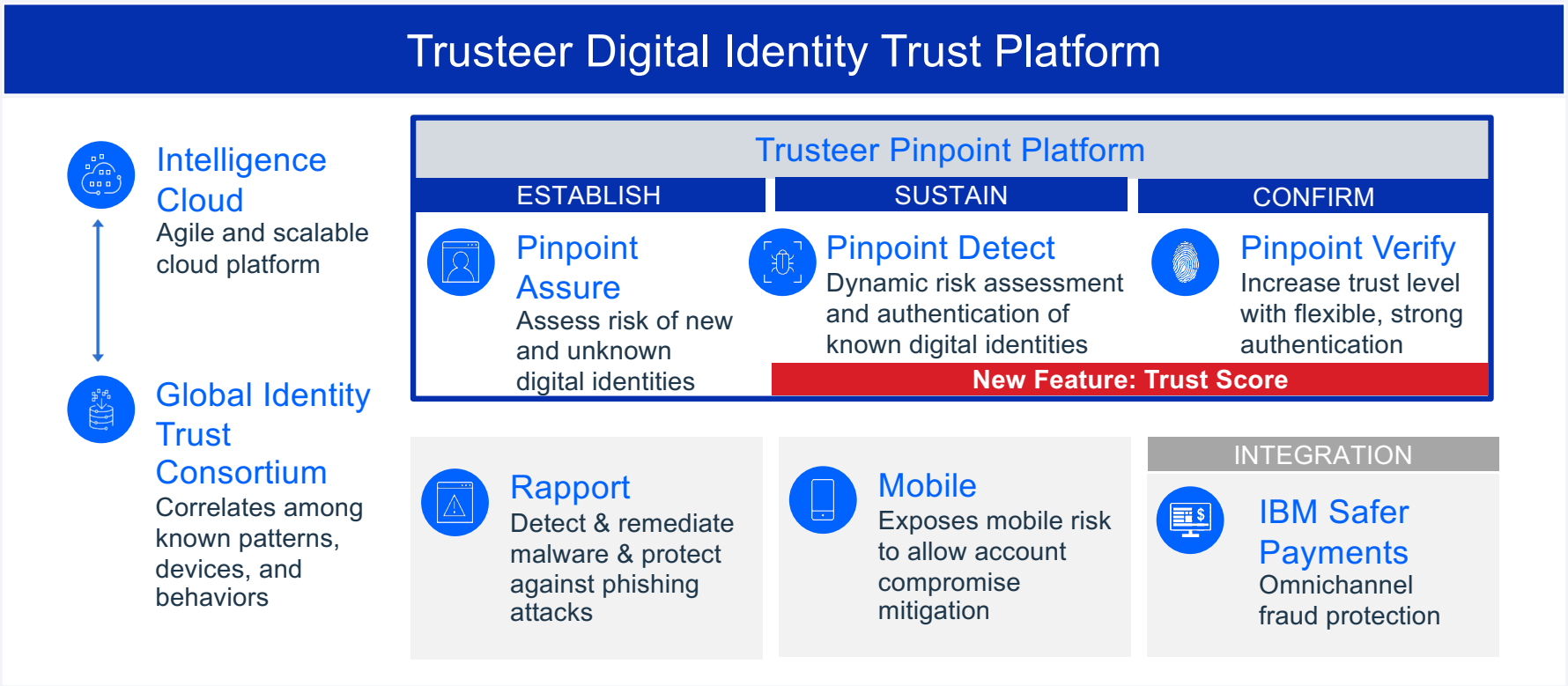
Behavioral Biometrics Assessment

Assessment of the current's session Behavioral biometrics attributes compared to past activity in the account

Un- Authorized Access

A mechanism to deal with un- authorized accesses to the account, prior to the fraudulent session by the fraudster

Digital identity trust lifecycle powered by AI and machine learning



Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

IBM **Security**

IBM


IBM