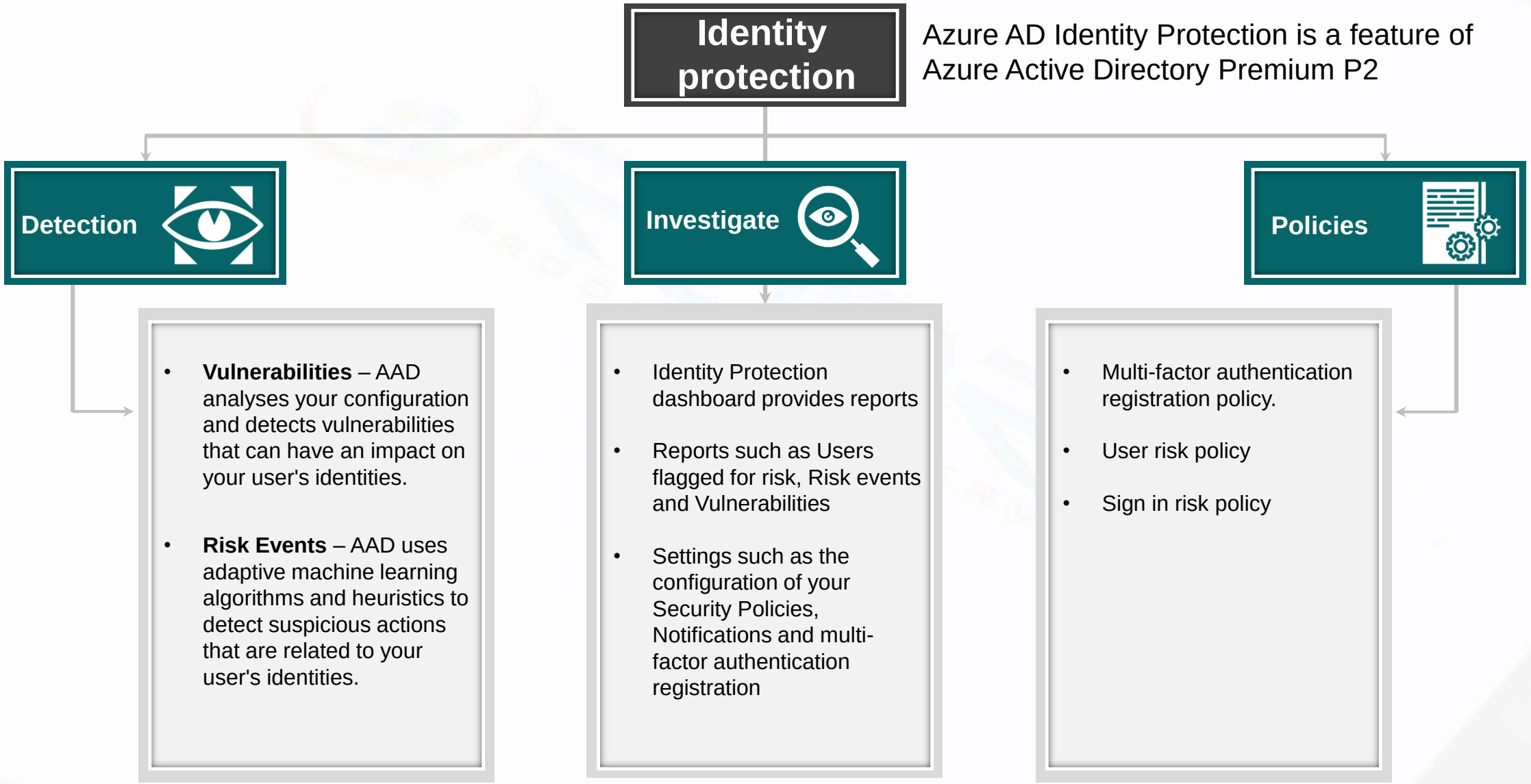
Introduction to Azure AD Identity Protection

Identity Protection capabilities



Types of risks

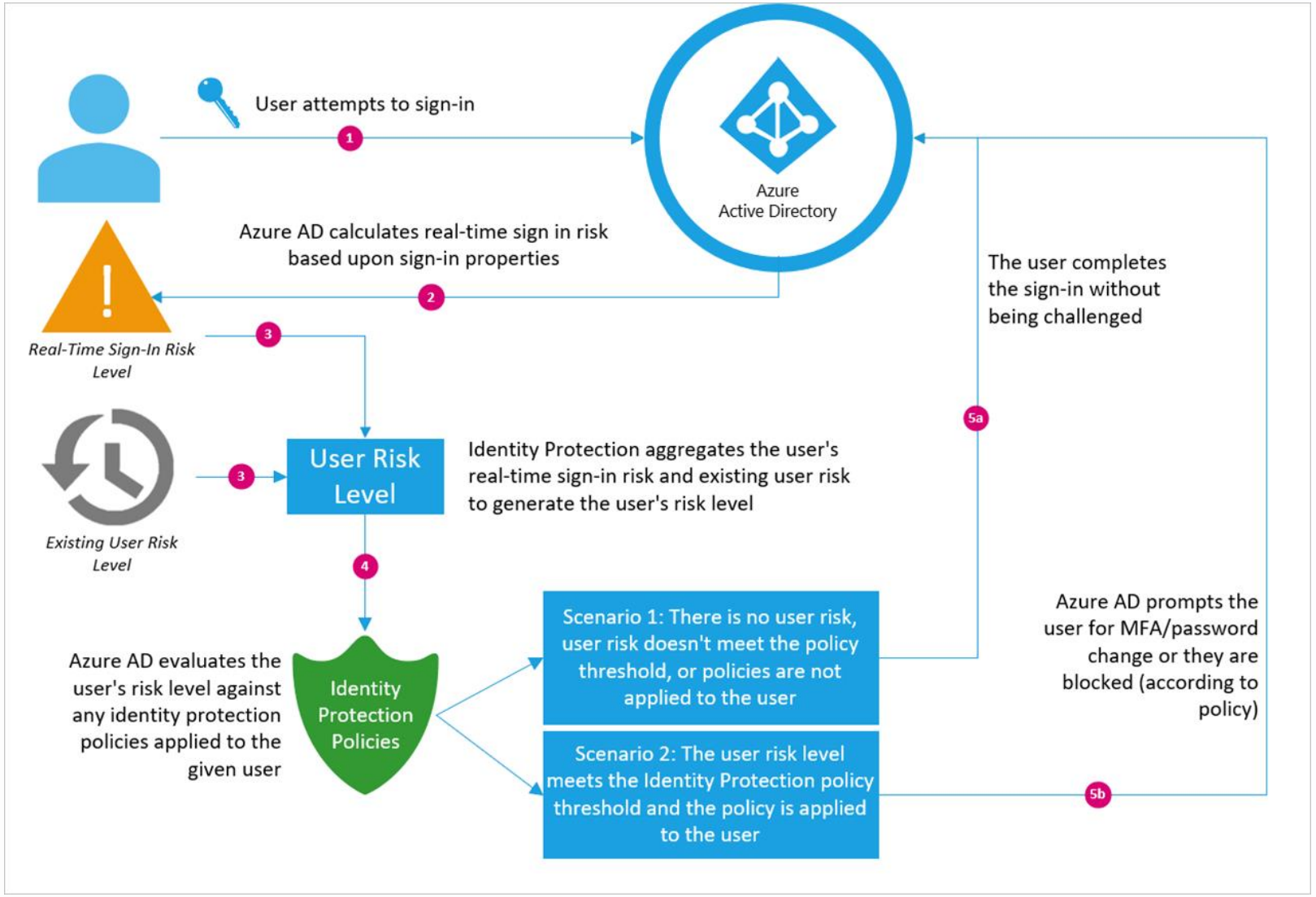
Sign in risk

- A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.
- **Sign-in risk real time** (such as sign-ins from anonymous IP addresses)
- **Sign-in risk aggregate** - Total sign-in risk is the aggregate of detected real-time sign-in risks as well as any subsequent non-real-time risk events associated with the user's sign ins

User risk

- User risk reflects the overall likelihood that a bad actor has compromised a given identity. User risk contains all the risk activities for a given user, including:
  - Real-time sign-in risk
  - Subsequent sign-in risk
  - Risky user detections.

Identity protection risk detection flow



© Microsoft