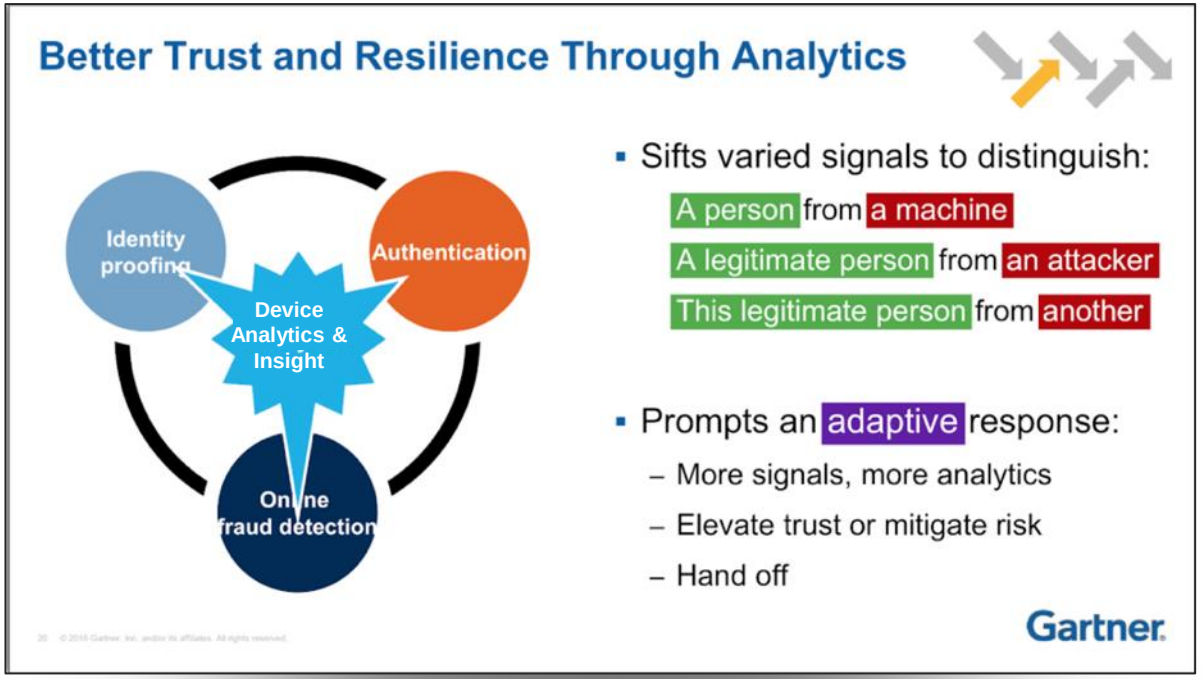
Will Your Fitbit Replace Your Password?

Dwayne Melançon, CISA - VP of Product, iovation Inc.

November 2017

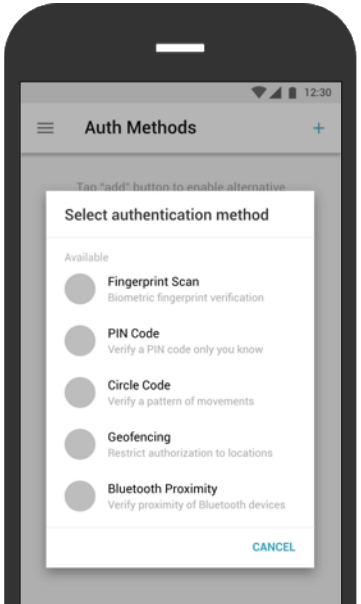
VISION:
CONVERGENCE IN AUTHENTICATION & RISK

HOW SEPARATE TECHNOLOGIES MERGE TO CREATE NEW VALUE



WHERE'S THIS GOING?

SIMPLE OMNICHANNEL ACCESS



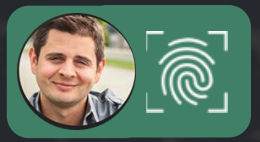
PERSONALIZATION WILL BE VITAL

UNIFIED, SIMPLIFIED AND PERSONALIZED MULTIFACTOR AUTHENTICATION

Circle / Pattern - Graphic pattern uses customer's mobile device

Proximity – Leverages nearby Bluetooth or NFC devices, and/or Wi-Fi networks

PIN Codes - Authenticate using user-defined PIN codes



Biometric - Biometric scans using customer's mobile device

Let consumers or admins choose the methods they prefer

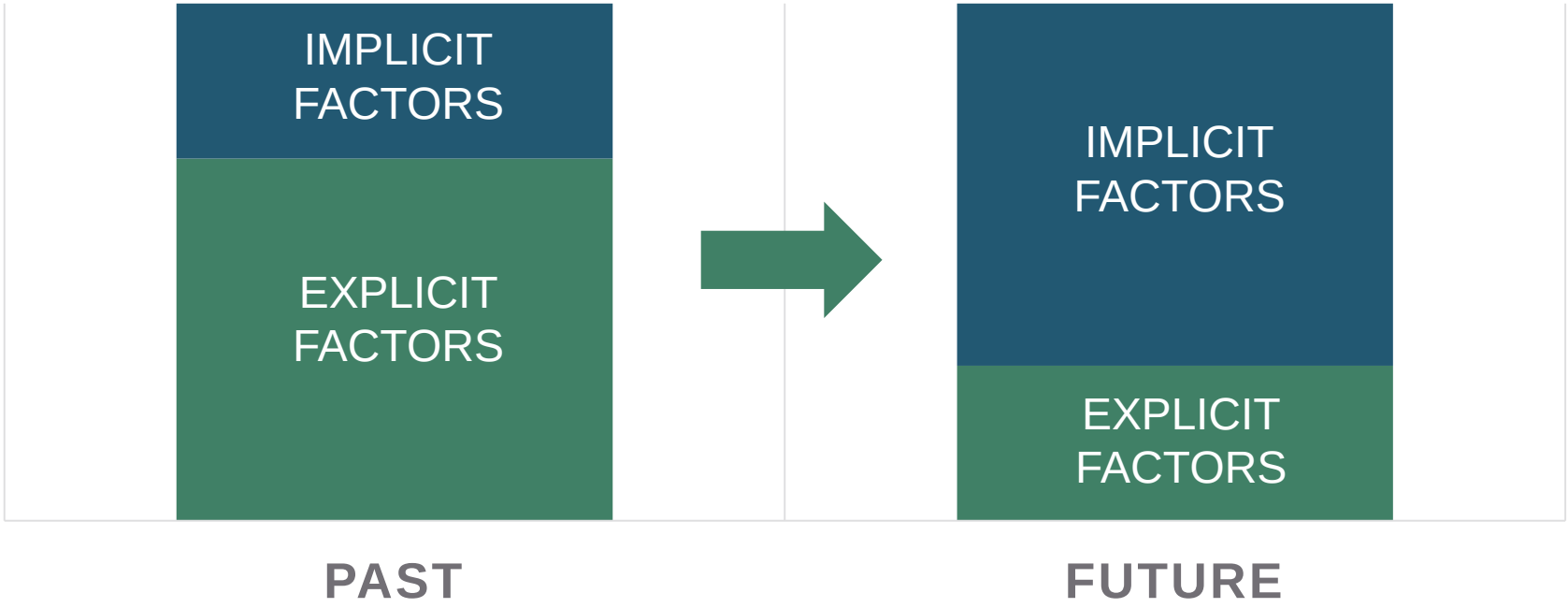
Single-party or multi-party real time swipe authorization

Geo-fencing and time-fencing constraints create secure login zones

Drive *all authentication* through one fully configurable experience

IoT and IDENTITY

TREND WILL FAVOR IMPLICIT FACTORS



CONSIDERATIONS

Use Cases and User Populations

- Factors
  - Active or passive?
  - How many factors?
  - Confidence:
    - How unique?
    - How persistent?
    - Possession as a factor
  - How easily controlled, revoked?
- Process and Workflow
  - User friction
    - How much will this introduce?
    - How much will my users tolerate?
    - How do I match the friction with the risk?
  - Authentication vs. Authorization
    - Workflow and challenges should match requirements and risk

WHAT IS THE OBJECTIVE?

Authentication – confirms who you are:

- I am an employee of the company. Here is my ID badge.

Authorization – determines what you're allowed to do:

- As an employee of the company, I am allowed entrance into the building.

Verification - used to mitigate circumvention of controls:

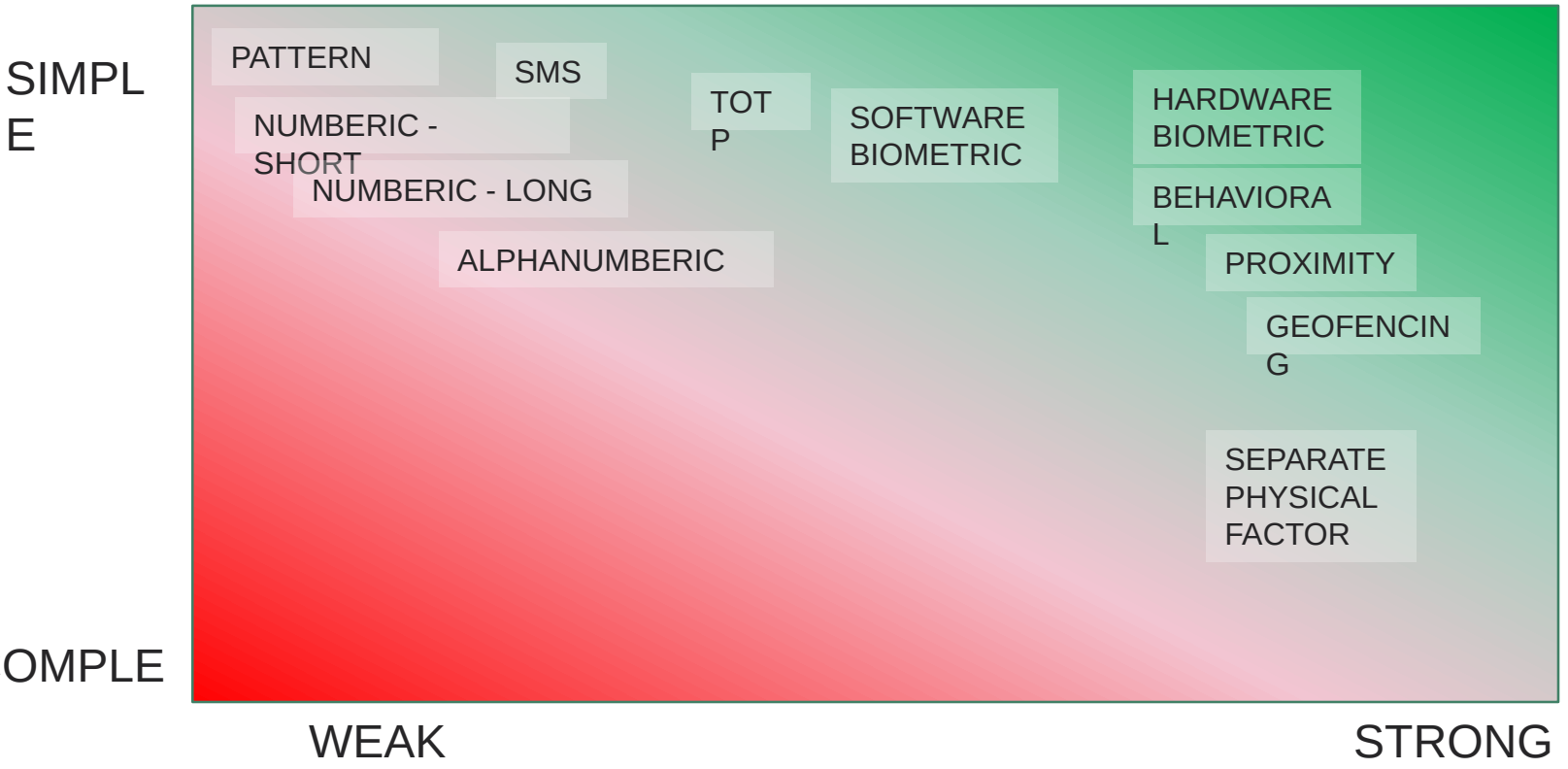
- Sending confirmation to Authorized, Authenticated person via an out-of-band challenge

CONSIDERATIONS

- Risk analysis
  - Value / impact if ineffective?
  - Frequency of use?
  - Ability to monitor / audit?
  - Ability to perform 3rd-party or out-of-band validation?
  - Control over factors and credentials?
  - Legal or Regulatory Requirements?
    - PSD2, NY State CyberSecurity Regulation, etc.
- Cost
  - Implementation, TCO, Etc.

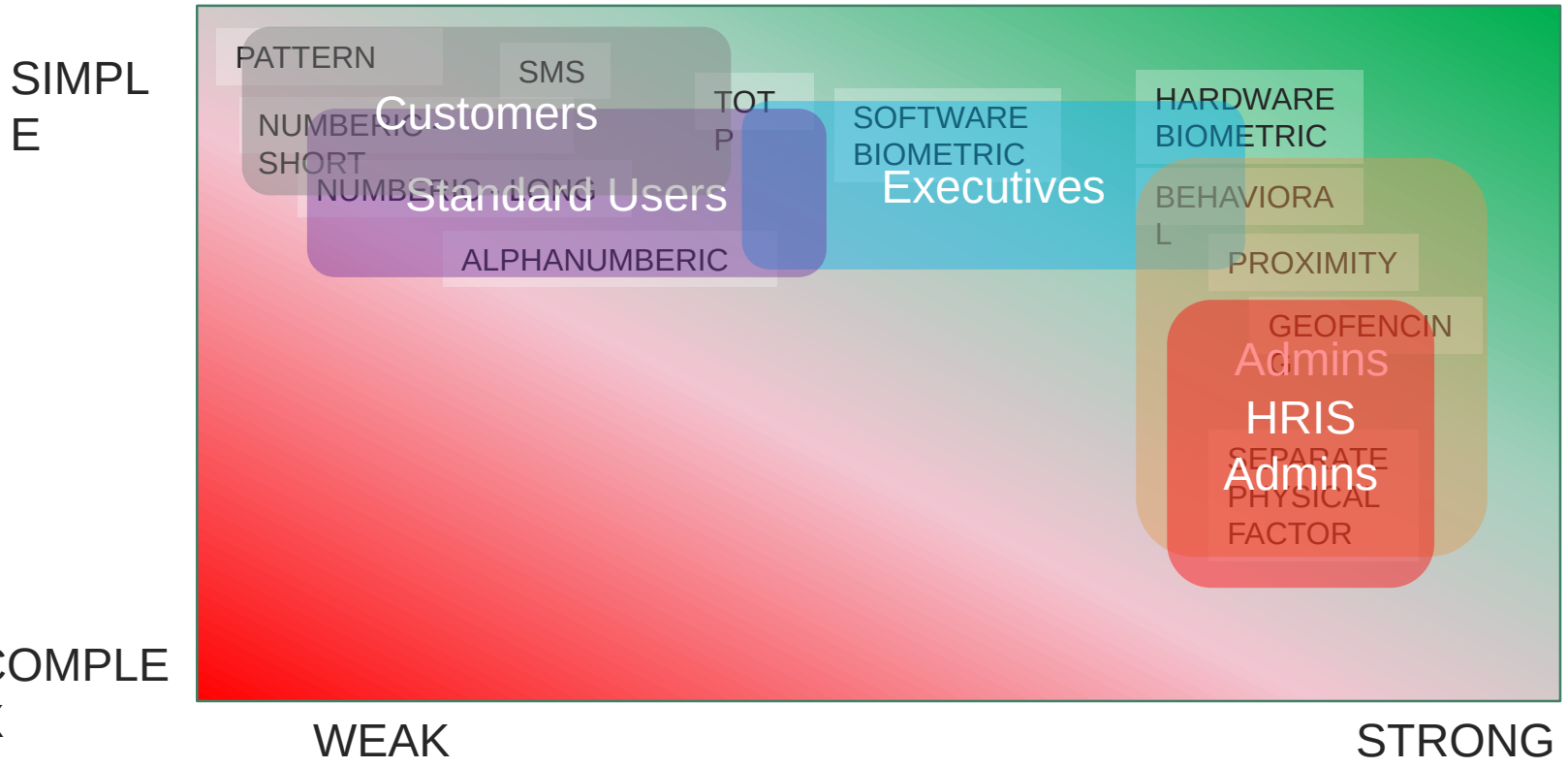
WHAT ARE THE TRADEOFFS?

SOME EXAMPLES FOR RISK DISCUSSIONS



WHAT ARE THE TRADEOFFS?

SOME EXAMPLES FOR RISK DISCUSSIONS



COMMENTARY ON METHODS

- KBA (Knowledge Based Authentication
  - Easily compromised; high friction
  - Low assurance
- “Local” KBA
  - Harder to compromise; high friction
  - Low / Medium assurance
- Centralized Password Stores
  - Easily compromised; medium friction
  - Low / Medium assurance
- Biometric / device-level auth
  - Hard to compromise; low friction
  - High confidence
- Proximity authentication
  - Medium to compromise; low friction
  - Medium to high confidence depending on number, type
- Geofencing
  - Medium to compromise; low friction
  - Medium confidence – should not be sole factor

BLUETOOTH PROXIMITY

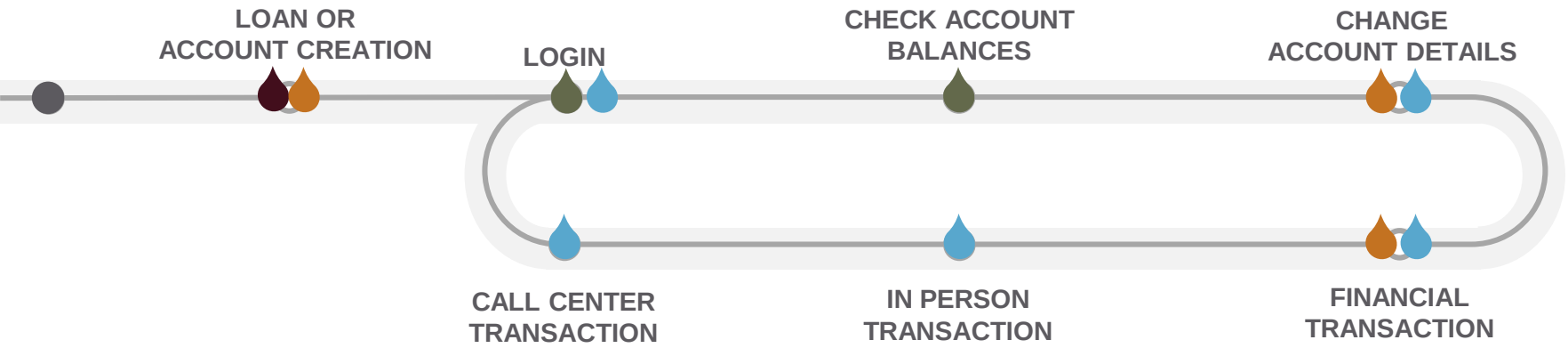
- Authenticate based on the proximity of one or more pre-paired Bluetooth-enabled devices
- Transparent, completely frictionless authentication
- Works in conjunction with all other authentication methods
- Wi-Fi networks can also be used as a lower-confidence proximity factor

STRATEGIES AND COUNTERMEASURES

- Risk-Aligned selection of factors
  - Layers and segmentation
  - Multiple vs. single factor
  - Active vs. passive
  - Strong binding vs. loose binding
  - GeoFencing
  - Device reputation analysis
- Challenges and Step-up
  - Enrollment
  - Identity proofing
  - Out of band vs. in-band challenges
  - Dynamic, Contextual Multifactor Authentiction
  - Resets and lost / stolen devices
  - Continuous vs. point-in-time

DEVICE FINGERPRINTING REDUCES RISK

Example OmniChannel Customer Journey For A Bank



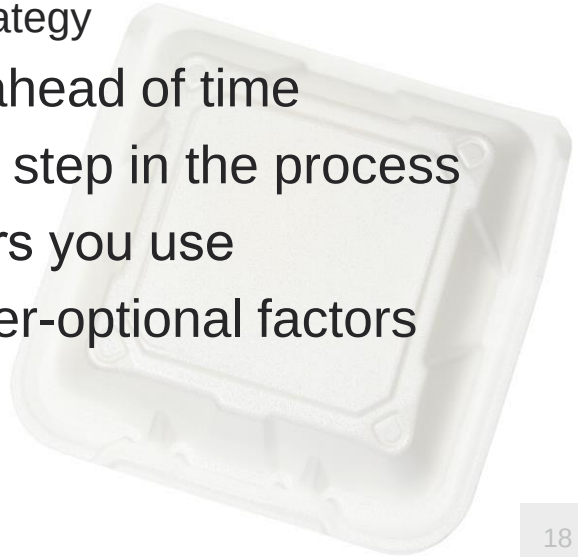
Passive Device Check	***Active Reputation / History Check***	***Device Based Authentication***	***Dynamic, Contextual MFA***
Improve customer experience & grow revenue using predictive analytics to identify the best customers	**Stop fraud in real-time** using contextual, behavioral, historical, and other risk indicators	**Improve security and customer experience** using transparent, frictionless, device-based authentication	**Improve security and customer experience** using interactive, customizable, multi-method authentication

MEASURING EFFECTIVENESS

- Measure the indicators
  - Successful vs. failed authentications
  - Password resets
  - Account lockouts
  - Support / service requests
  - Emergency access requests
- Use percentages vs. hard numbers
- Look for trends to identify issues
  - Factor issue?
  - User population issue?
  - Complexity?
  - Frequency?

TAKEAWAYS

- No one-size-fits all – focus on the user experience
  - Embraced the move to passive and implicit factors, but don't blindly trust them
- Discuss risks, objectives, and user expectations before choosing strategy
  - Align with the business strategy, not just the security strategy
- Document your workflows and document goals ahead of time
- Determine assurance control objectives for each step in the process
- Study the strength and "spoofability" of the factors you use
- Determine policy on company-mandated and user-optional factors
- Monitor for effectiveness



Dwayne Melançon, CISA
VP of Product, iovation Inc.
@thatdwayne

References

- NIST: “Proximity-based Authentication for Mobile Devices” http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=150218
- Gartner: “Take a New Approach to Establishing and Sustaining Trust in Digital Identities” Gartner Document ID: G00324312
- Gartner: “How Context and Adaptive Techniques Impact the Authentication Market” Gartner Document ID: G00269547
- “Come Closer - Proximity-based Authentication for the Internet of Things” www.vs.inf.ethz.ch/publ/papers/mshafagh_mobicomposter14.pdf
- MDPI: “One-Time URL: A Proximity Security Mechanism between Internet of Things and Mobile Devices” http://www.mdpi.com/1424-8220/16/10/1694