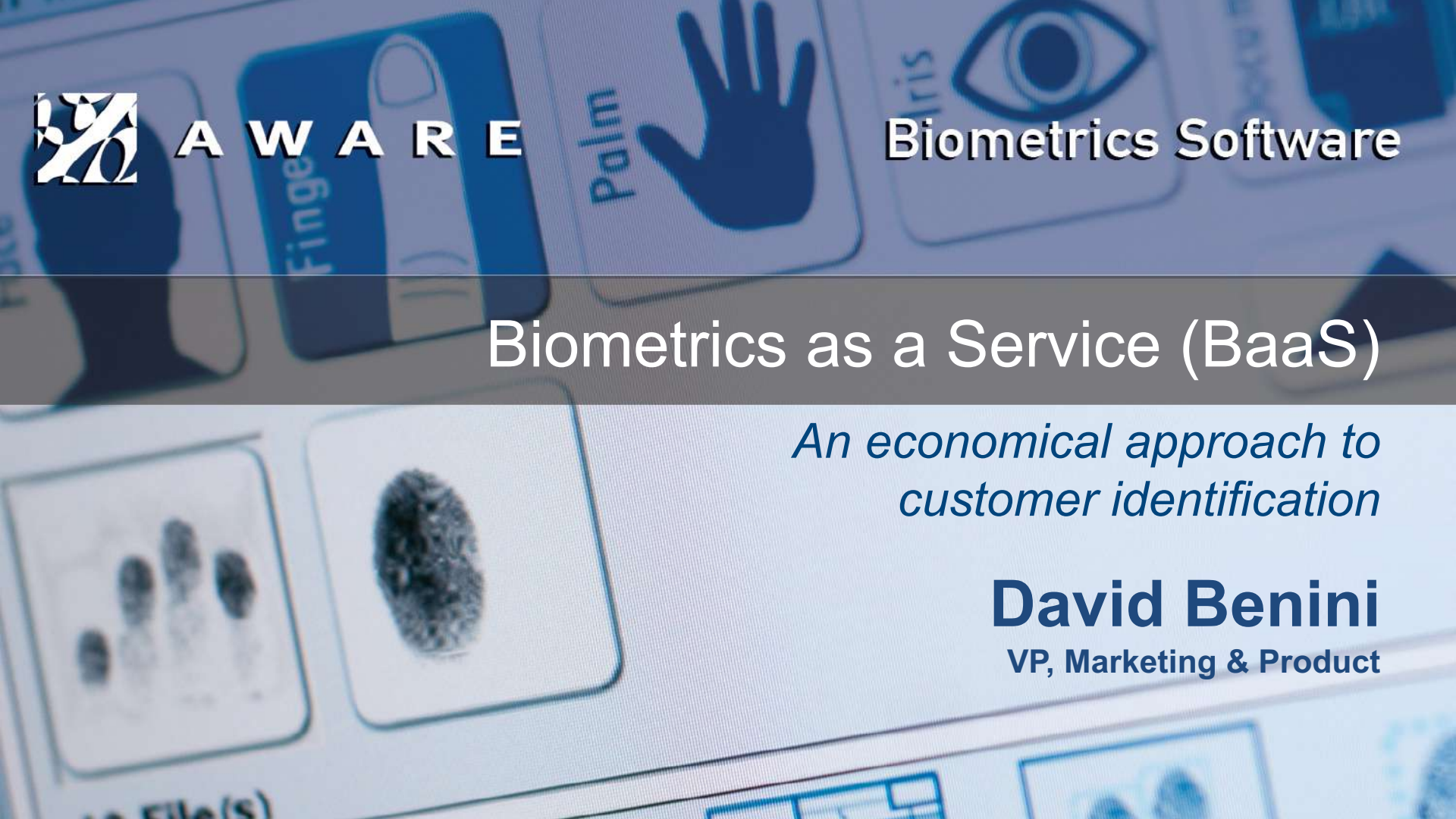


Biometrics as a Service (BaaS)

An economical approach to customer identification

David Benini
VP, Marketing & Product

Agenda

- Software as a Service
  - Biometrics as a Service
    - Use Case: Patient ID
      - Case Study: Patient ID
- Facial Recognition
  - Liveness Detection

SaaS Revolution

“The Cloud” dominates the enterprise software landscape

Operating vs Capital Expenses

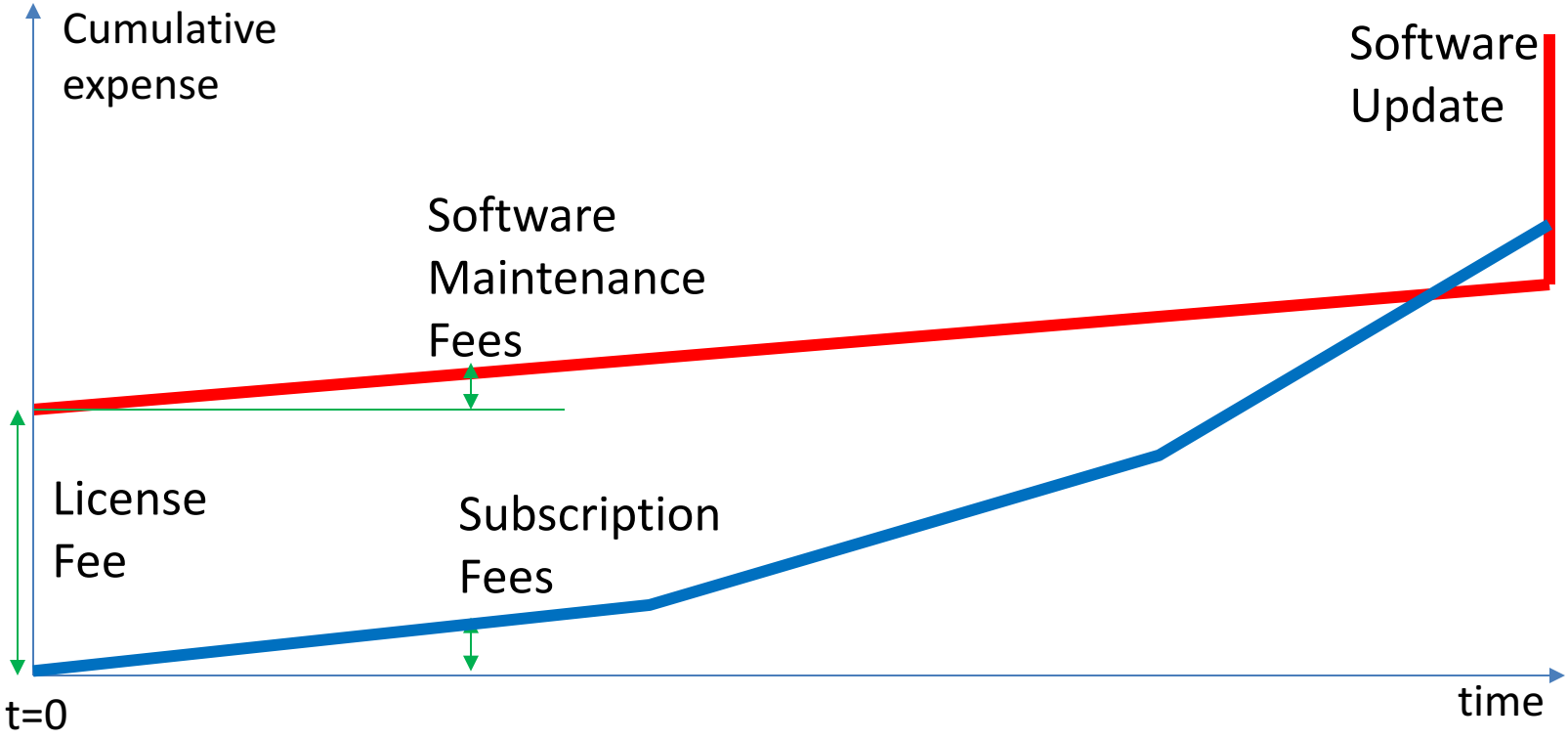
“Rent” a Depreciating Asset

“Pay As You Grow”

Lower Risk, Uncertainty, and Cost

Rapid Setup + Exit Flexibility

Capital Expense vs. Operating Expense



SaaS…A Natural Fit for Biometrics (“BaaS”)

Consider the earliest digital biometric systems (AFIS)…

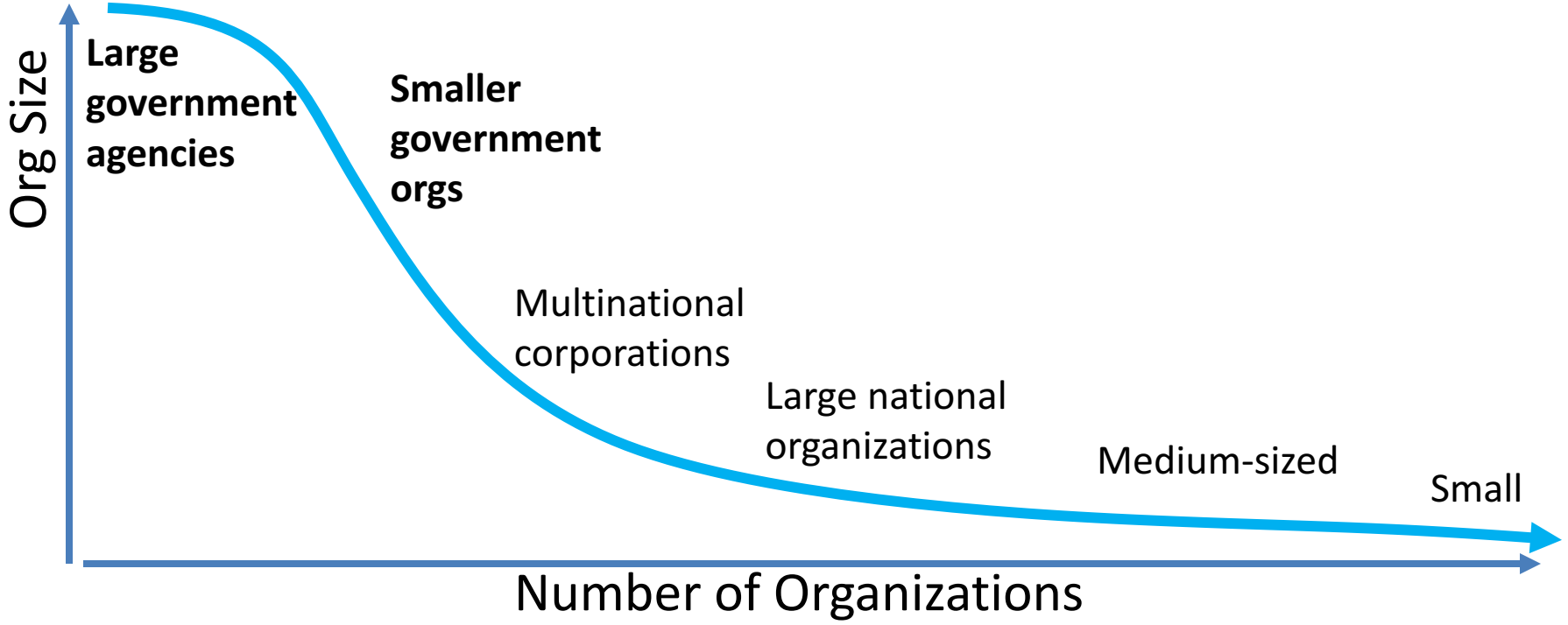
Local police

search result

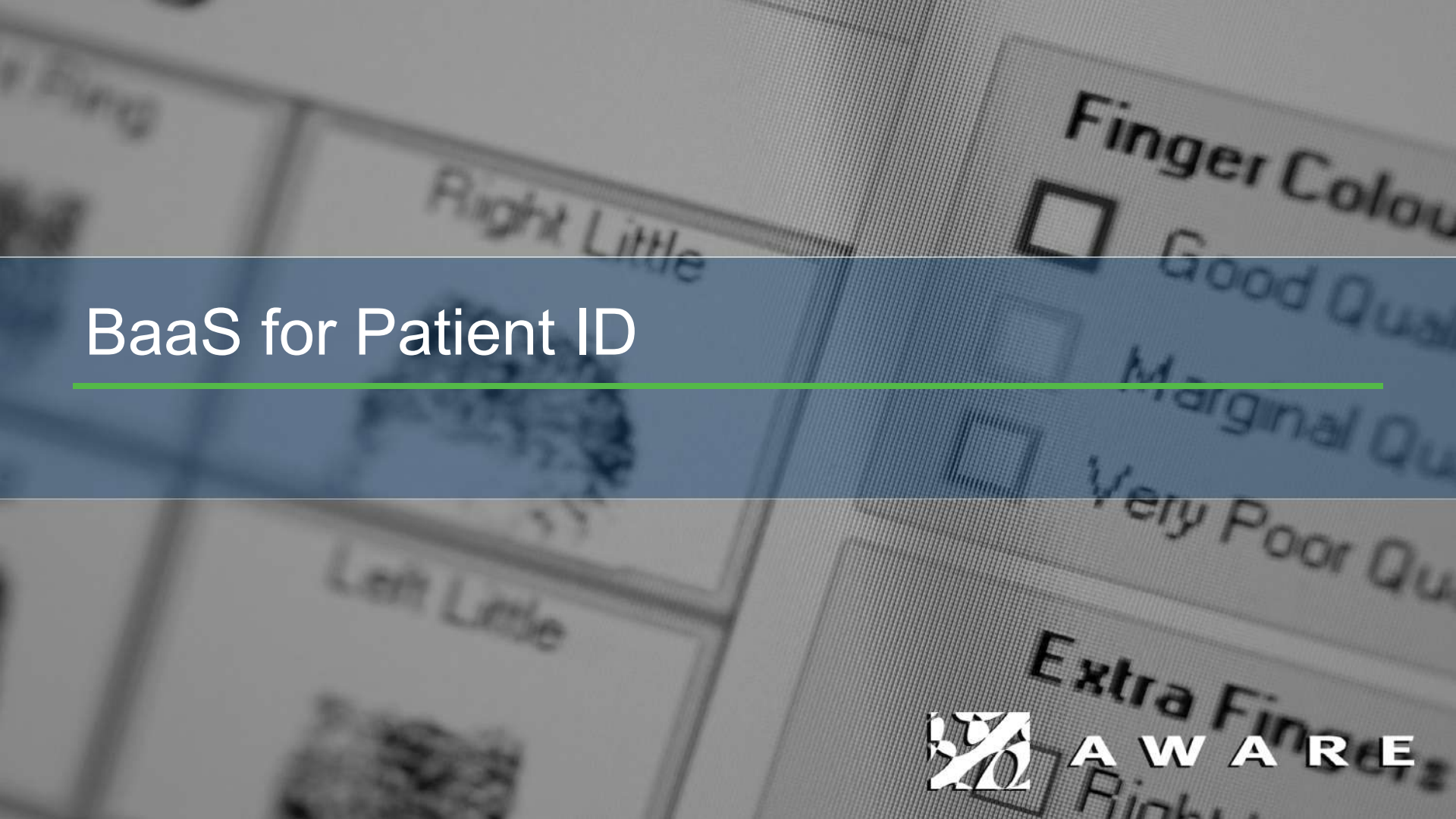
Federal police

…biometrics have always been a “SaaS”

BaaS Enables Adoption Down the Long Tail



BaaS for Patient ID



Patient Misidentification is a Serious Problem

Professionals agree…

Happens frequently

64 percent

of healthcare professionals surveyed by the Ponemon Institute said patient *misidentification happens frequently*.

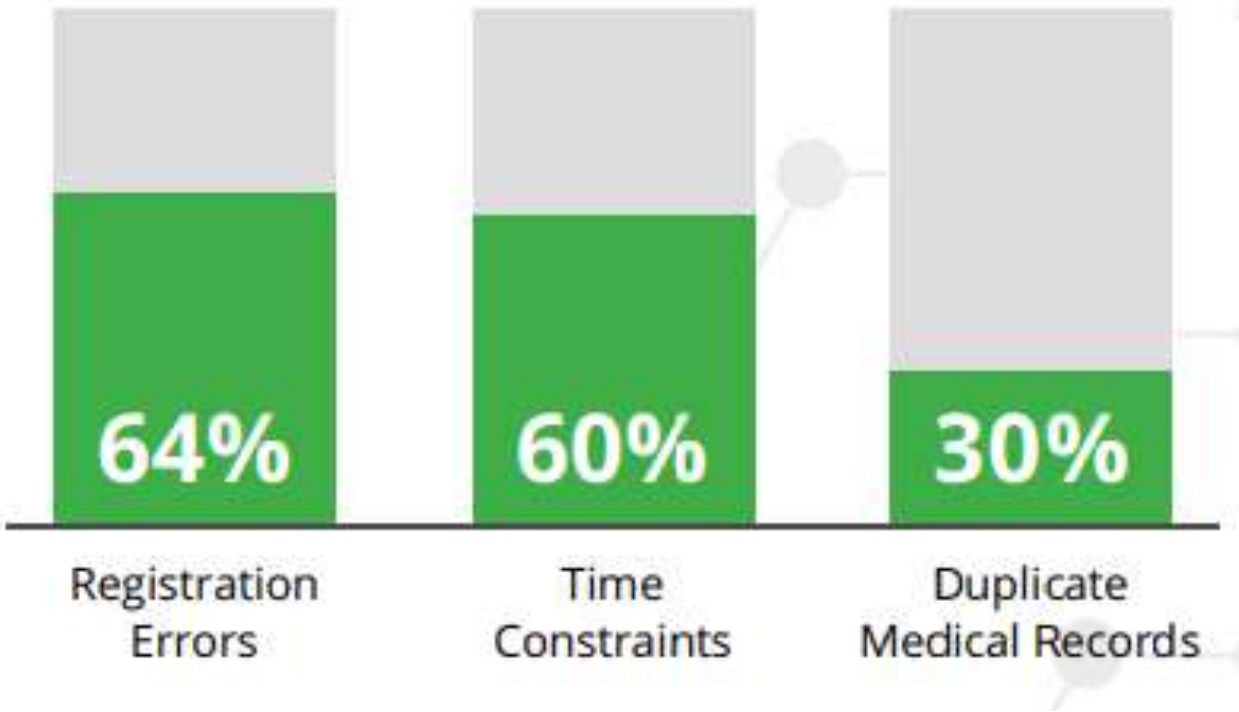
Can cause injury and illness

84 percent

said they "strongly agree" or "agree" that misidentification *can lead to medical errors* that induce injury or illness.

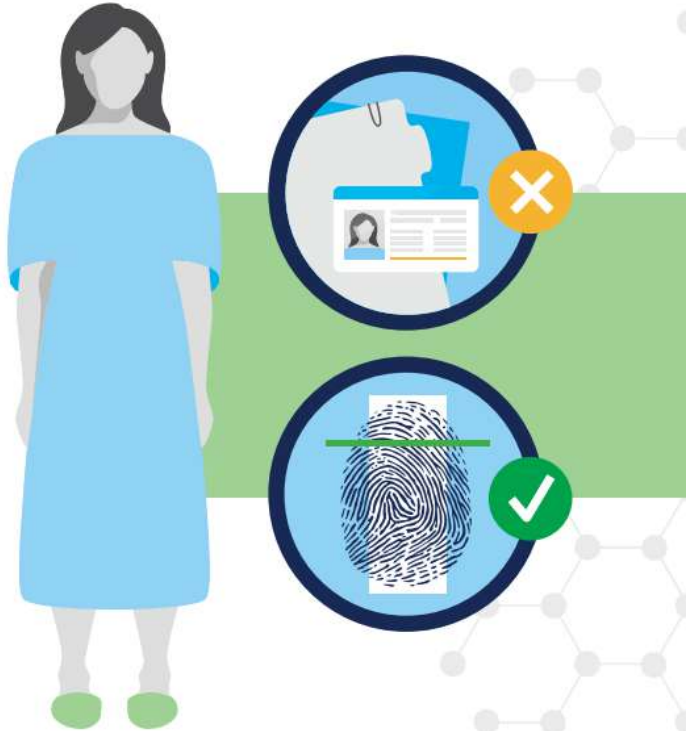
Source: Ponemon Institute

Top Reasons for Patient Misidentification



The Problem with Text-Based Biographic Identifiers

- Not unique
- Not consistent
- Not permanent
- Can be stolen
- Rely on credentials

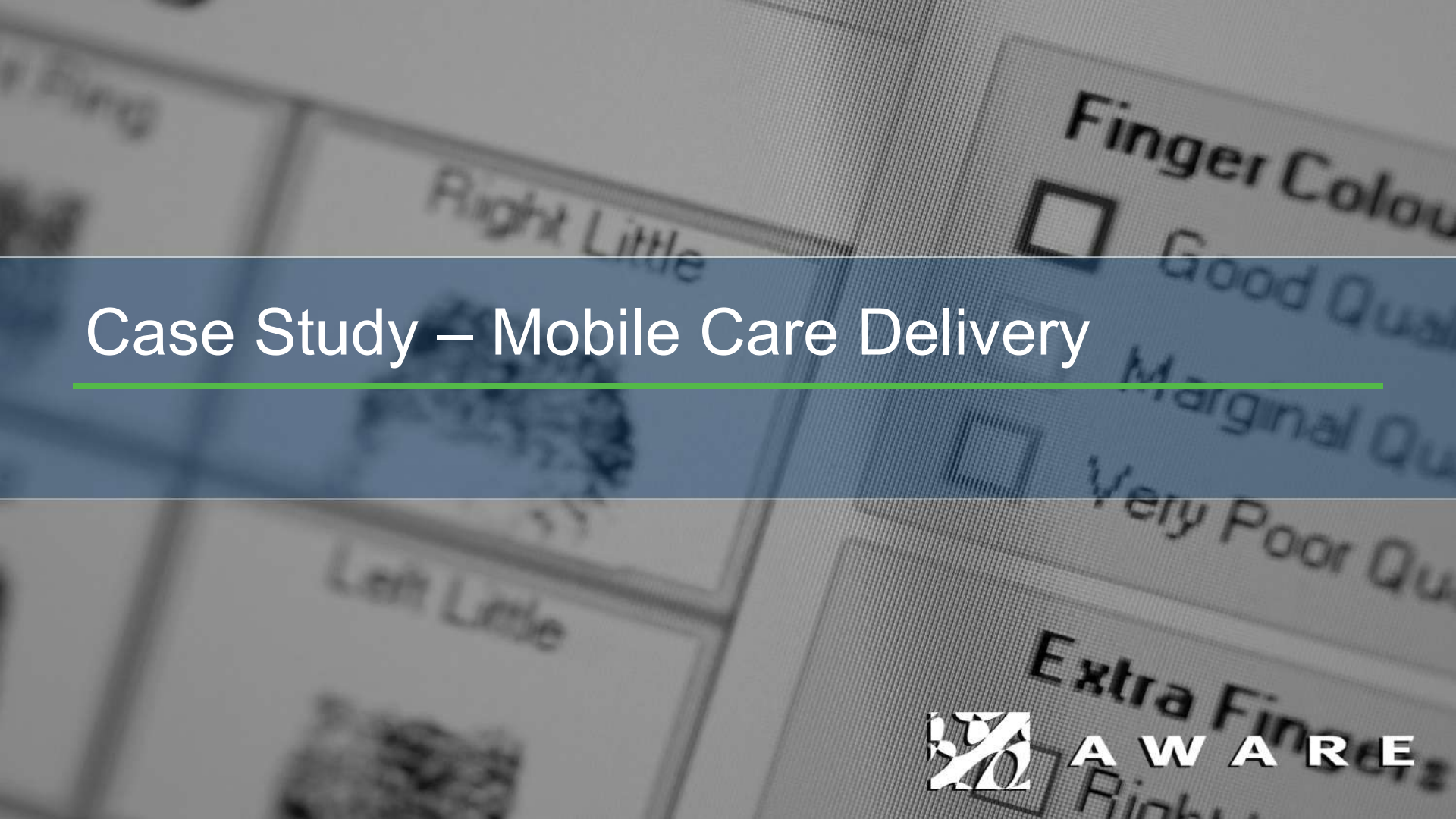


Biometrics address these shortcomings

Biometric Patient Registration Process

1. **Identity proofing: thorough identity inquiry**
   - Proof-of-identity documents
2. **Collect biometric data**
   - e.g. fingerprints, face
3. **Biometric search for duplicates, existing records**
   - Fusion of fingerprint, face results
   - If none, enroll data

Case Study – Mobile Care Delivery

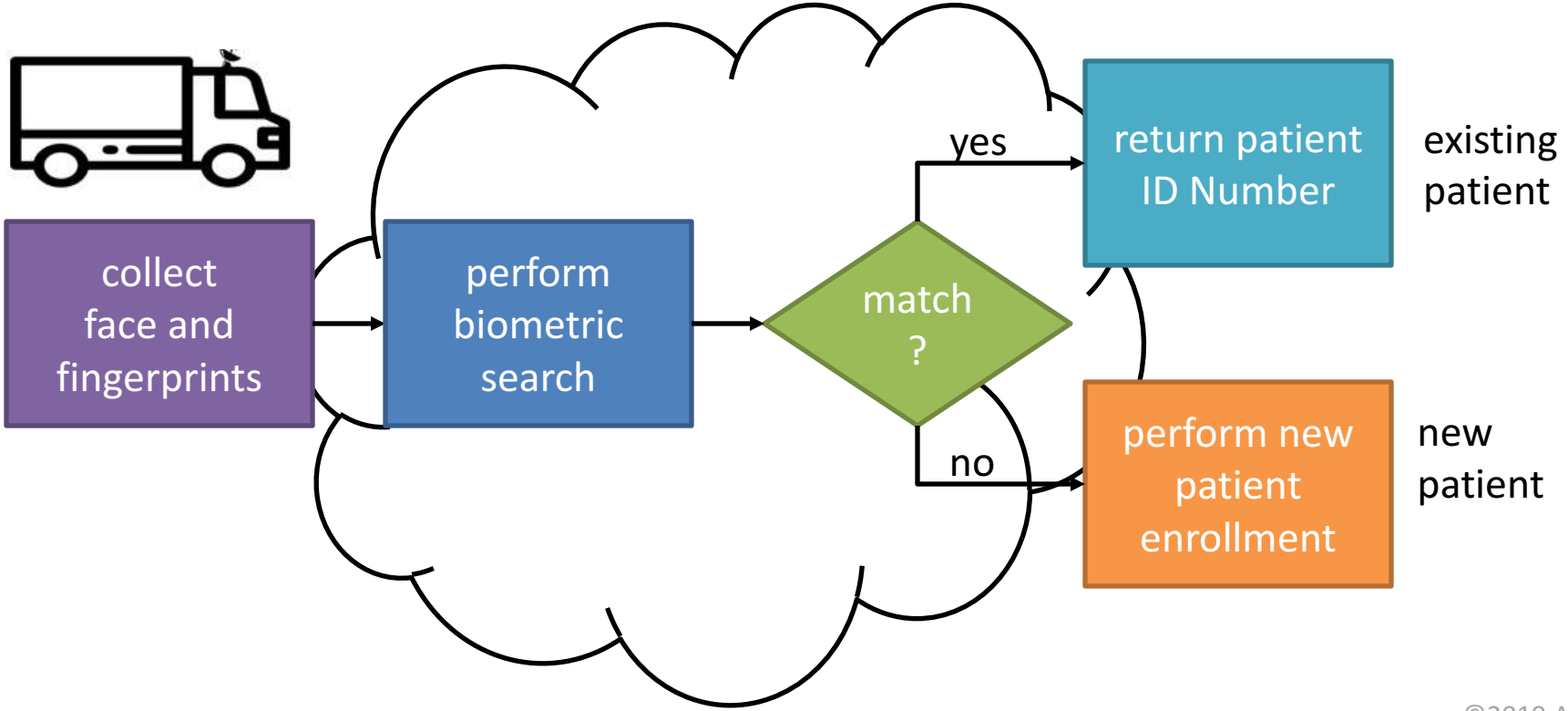


AWARE

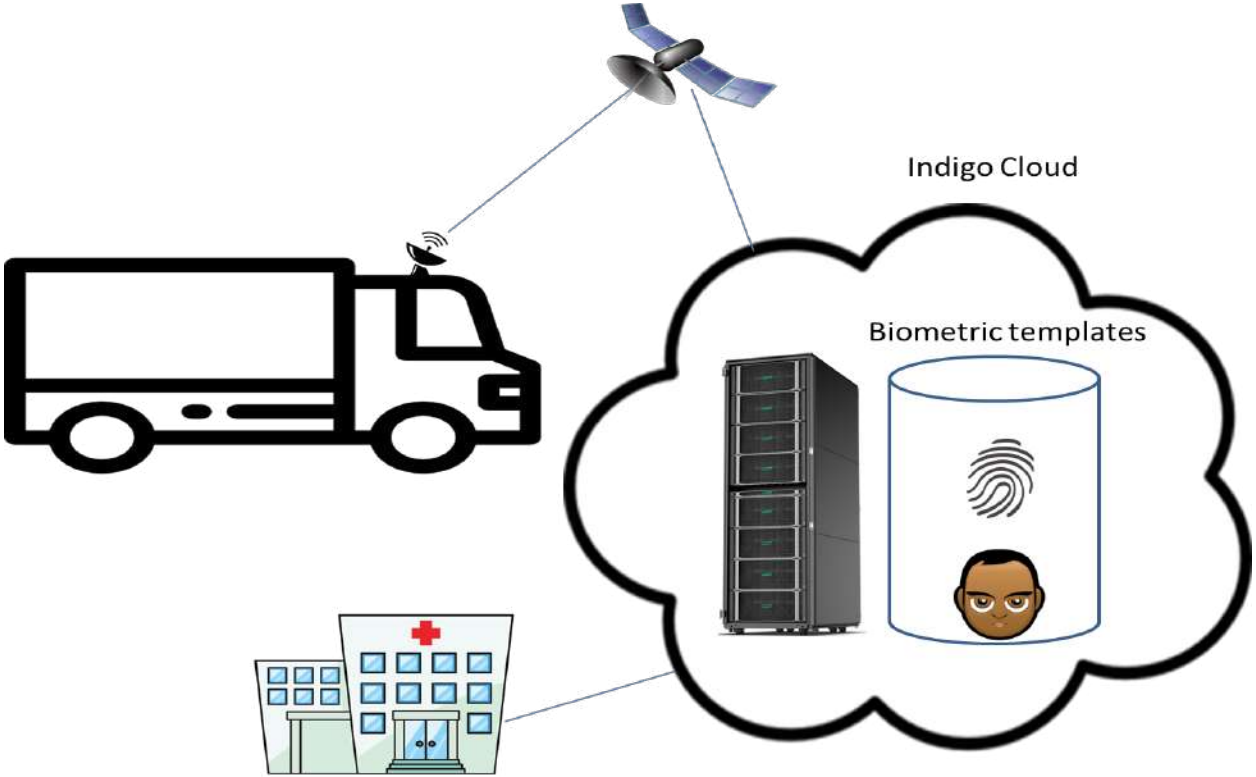
Patient ID Upon Mobile Remote Care

- Mobile diagnostic HIV testing services
- Truck visits remote locations
- Face + fingerprints collected using browser-based kiosk
- Network connectivity to cloud via satellite
- Automated enrollment workflow
  - Biometric match in database → Retrieve patient records
  - No biometric match in database → provision new patient ID

Upon Patient Visit…Automated Workflow



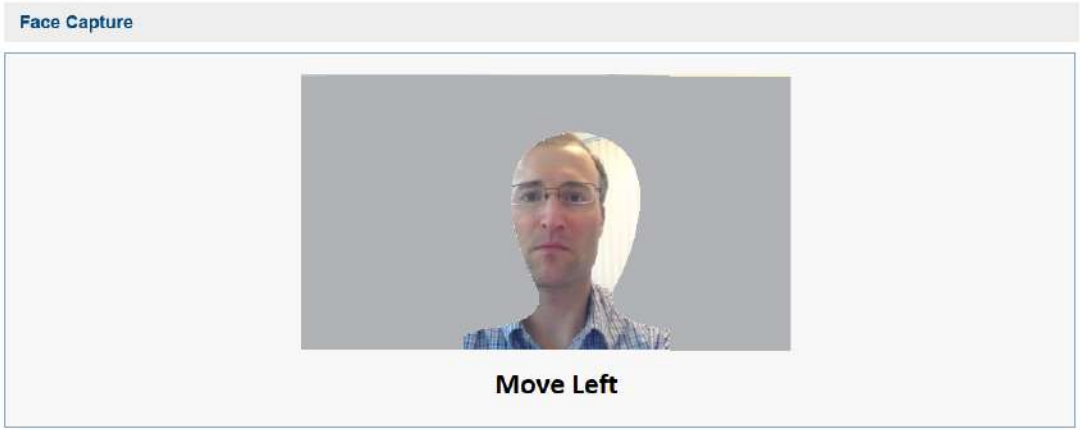
Architecture: Remote Health Delivery



Trucks Equipped with Enrollment Kiosks

BioComponents Integrated into Legacy Kiosk UI

- Biometric enrollment “iframes” incorporated into customer user interface




SHOUT-IT-NOW
HIV SERVICES. FAST. FREE. FRIENDLY.


Test & Treat Today
SHOUT-IT-NOW
HIV SERVICES. FAST. FREE. FRIENDLY.


SHOUT-IT-NOW
HIV SERVICES. FAST. FREE. FRIENDLY.


SHOUT-IT-NOW
HIV SERVICES. FAST. FREE. FRIENDLY.

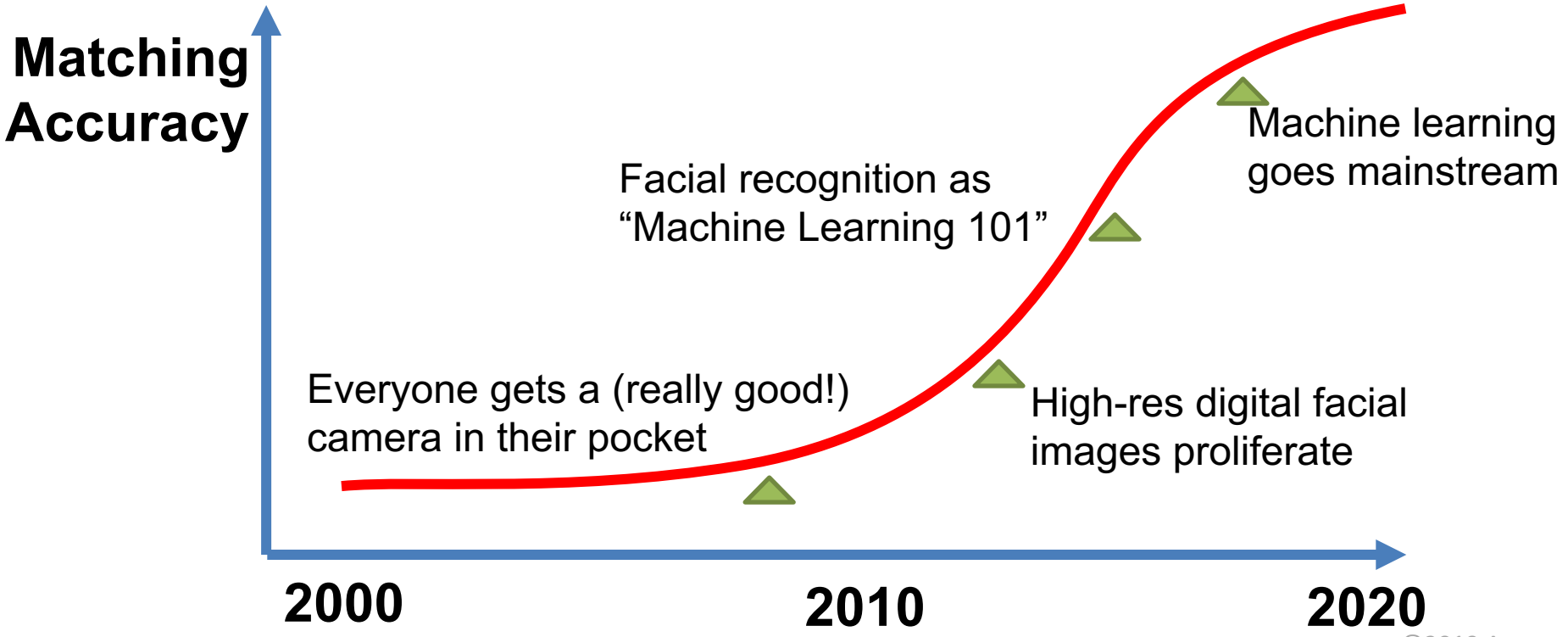

SHOUT-IT-NOW
HIV SERVICES. FAST. FREE. FRIENDLY.

Facial Recognition and Liveness Detection

Update

AWARE

Facial Matching Algorithm Performance Over Time



NEWS

NIST Evaluation Shows Advance in Face Recognition Software's Capabilities

November 30, 2018

*"Between 2014 and 2018, facial recognition software got **20 times** better at searching [1:N] a database to find a matching photograph"*

Facial Recognition Programs Are Improving.

Best performing program at identifying a person from a set of 1.6 million photos.

YEAR	PERCENTAGE ACCURATE
2010	92.3
2014	95.9
2018	99.7

Chart: WIRED • Source: NIST

Facial Recognition : The Good and the Bad

Facial biometrics are ideal for identification…

Accurate, familiar, and convenient!

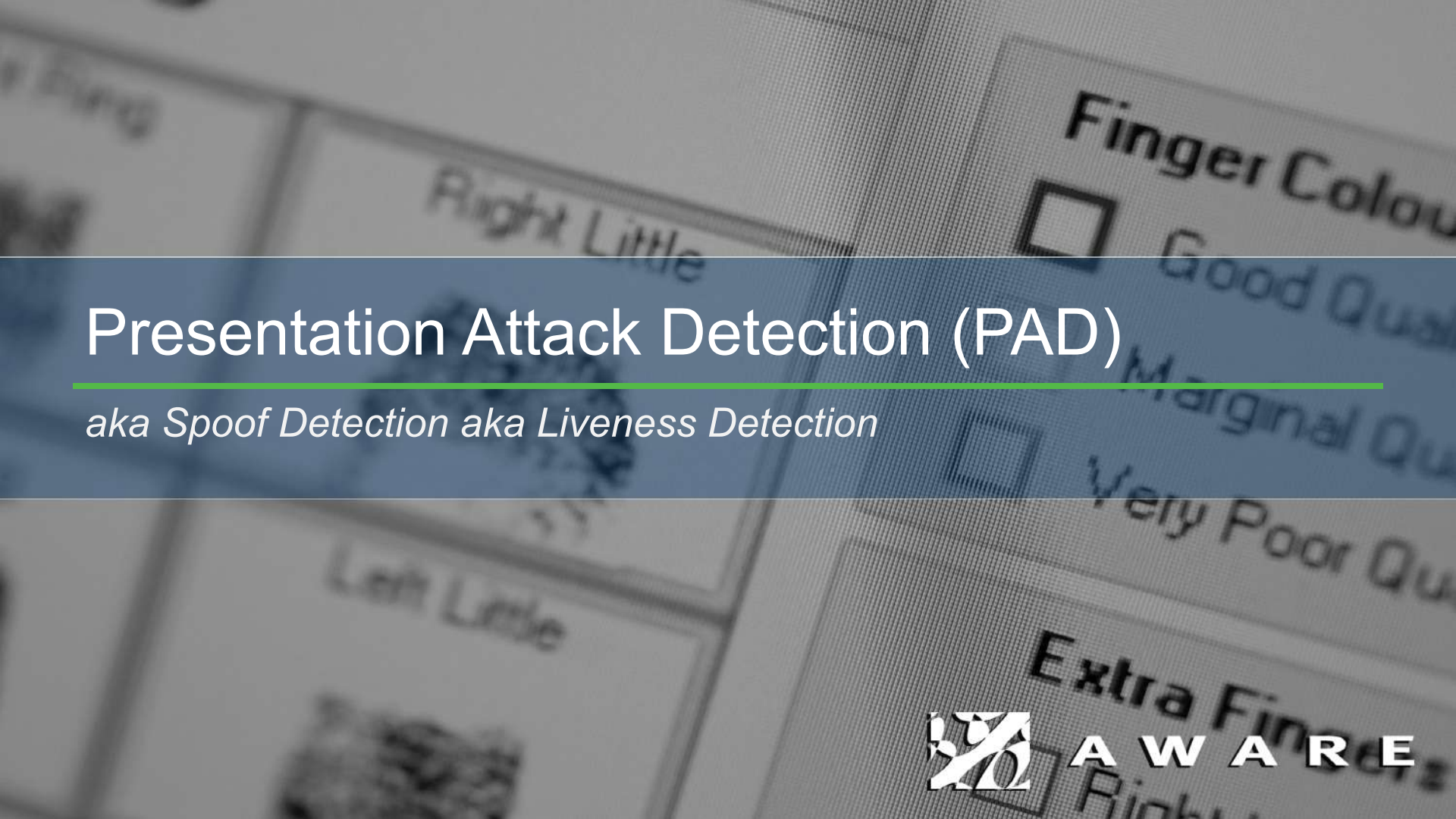
…but they are relatively easy to spoof

Trillions of HD digital images of our faces are out there


THE NEWS
READ ALL ABOUT IT!
FACIAL MATCHING ALGORITHMS ARE VERY ACCURATE
ATTENTION TURNS TO CONVENIENCE AND ATTACK DETECTION

Presentation Attack Detection (PAD)

aka Spoof Detection aka Liveness Detection



AWARE

What is ***Liveness***? Why Is It Important?

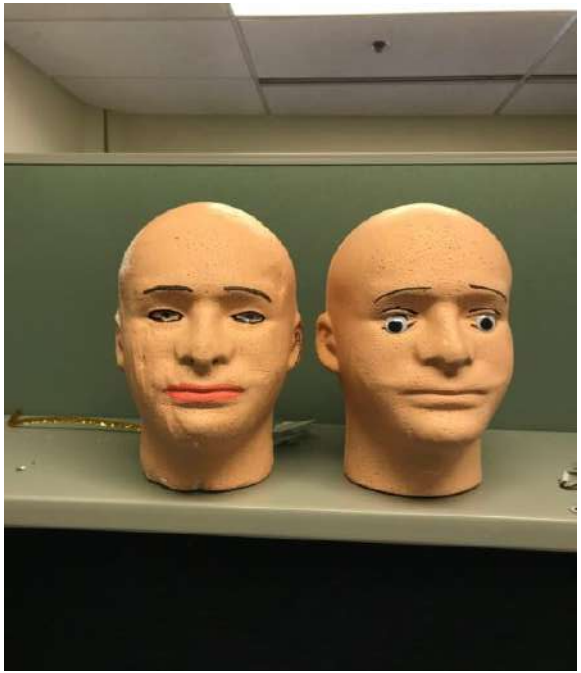
- Security of biometrics must not depend on their secrecy
- Biometrics are useful ONLY to the degree they are:
  - **INHERENT**
    - ergonomically viable for reliable presentation by the genuine owner
  - **DETECTABLE**
    - can be economically sensed/detected; reasonable signal-to-noise ratio
  - **UNIQUE**
    - not easily/accidentally produced by a fraudster/imposter
- Spoofing vulnerability degrades their UNIQUENESS

What We Want…and What We Get

Genuine

Spoof attacks

A Wide Variety of Spoofs Must Be Detected



Not Matchable to Victim…Do We Care? Yes!

Liveness for Authentication Vs. Onboarding

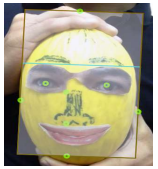
Authentication

- Trusted reference sample previously registered
- Biometric non-match prevents false-match spoofs
- No match, no spoof

Onboarding

- No reference sample
- Many orgs want to use faces for **mobile onboarding**…
- Face image should be searchable
- Image should be citable as evidence in court

Must Prevent False Non-Matches for Onboarding



Fraudster's Desired Outcome

	False Non-Match	False Match
Authentication	Low utility	Spoof attack
Onboarding	Avoid detection; Fraudulent duplicates	Identity theft

For onboarding, must detect non-matchable face images to prevent false non-match attacks

PAD Is a Hard Problem (Harder Than Matching!?)

- Technical constraints
  - Mobile CPU, sensor performance, device variety, network bandwidth, server scalability
- Unpredictable real-world environments
  - E.g. bright sun or darkness
- Noisy data

- Friction! Consumers are very sensitive to it
- Wide variety of attacks to address
- No abundance of ready-made scrapable training data

First, Let's Get Better at Measurement!

NIST SOFA-B

Strength of Function For Authenticators – Biometrics

The concept of "Effort"

BEAT-EU

Biometric Evaluation & Testing

Testing methods and metrics

ISO 19795-1/2

Biometric performance

Testing methods and metrics

ISO 30107-1/3

Presentation Attack Detection

Testing methods and metrics

FIDO Biometrics Requirements

Performance thresholds

Examples of Face Spoofs and Levels

Table of Example PAI Species for Face

Species	Level
Face image printed on inkjet or laser printer	A
Face image printed at photograph laboratory	A
Displayed photos on electronic/mobile devices	A
Displayed videos on electronic/mobile devices	B
Paper masks	B
Masks made of specialized materials (ceramic, silicone, and/or theatrical)	C
3D printed faces	C

Lots of Approaches

- **"Active" – physical user challenge/response**
  - Challenge/response (blink, smile, motion)
- **"Passive" – in the background; little/no user awareness**
  - Skin color and texture
  - Sharpness
  - Parallax
  - Artifacts (e.g. cutouts)
  - **Machine learning-based approaches are promising…**

Machine Learning for PAD

- ML is accelerating improvements to spoof detection
  - Similar trajectory as matching
  - But arguably more difficult algorithmic challenge
- Some ML approaches avoid user friction, security vulnerabilities
- Need more data! Nowhere near as much exists as for genuine faces

Thank You!

David Benini
VP, Marketing & Product
Aware, Inc.
Boston, USA
dave@aware.com

Introduction to Aware, Inc.

- Founded in 1986 by MIT mathematicians
- Biometrics software supplier since 1993
- Publicly traded since 1996 (NASDAQ:AWRE)
- Headquartered near Boston, USA
- Strong balance sheet (US$50M) and profitable
- 50+ research scientists and software engineers
- Leading provider of military-grade biometric solutions for public and private sector

Our Long History of Innovation in Biometrics

1990s

- Founding supplier to a small biometrics community
- Helped FBI design WSQ fingerprint image compression algorithm for first large-scale US Federal Government AFIS
- First successful supplier of COTS biometric SDKs

2000s

- Among first companies to enable biometric e-passports
- First to license a COTS biometric services platform (BioSP)
- First to license biometric enrollment applets and .NET controls
- Primary supplier of biometric PIV software for USG

2010s

- First to commercialize browser-based biometric enrollment
- Ground-breaking innovations in mobile authentication and liveness detection

How Aware Is Different

- One-stop shop for wide range of biometric software solutions
- Agile and innovative
- Modular products enable extremely open architecture
- Independence from hardware peripherals and algorithms
- Cooperative, collaborative customer relationships
- Transparent, accessible organization
- Highly responsive technical support