IBM Security

A Guide to Optimizing Digital Identity Risk and Experience with Adaptive Access

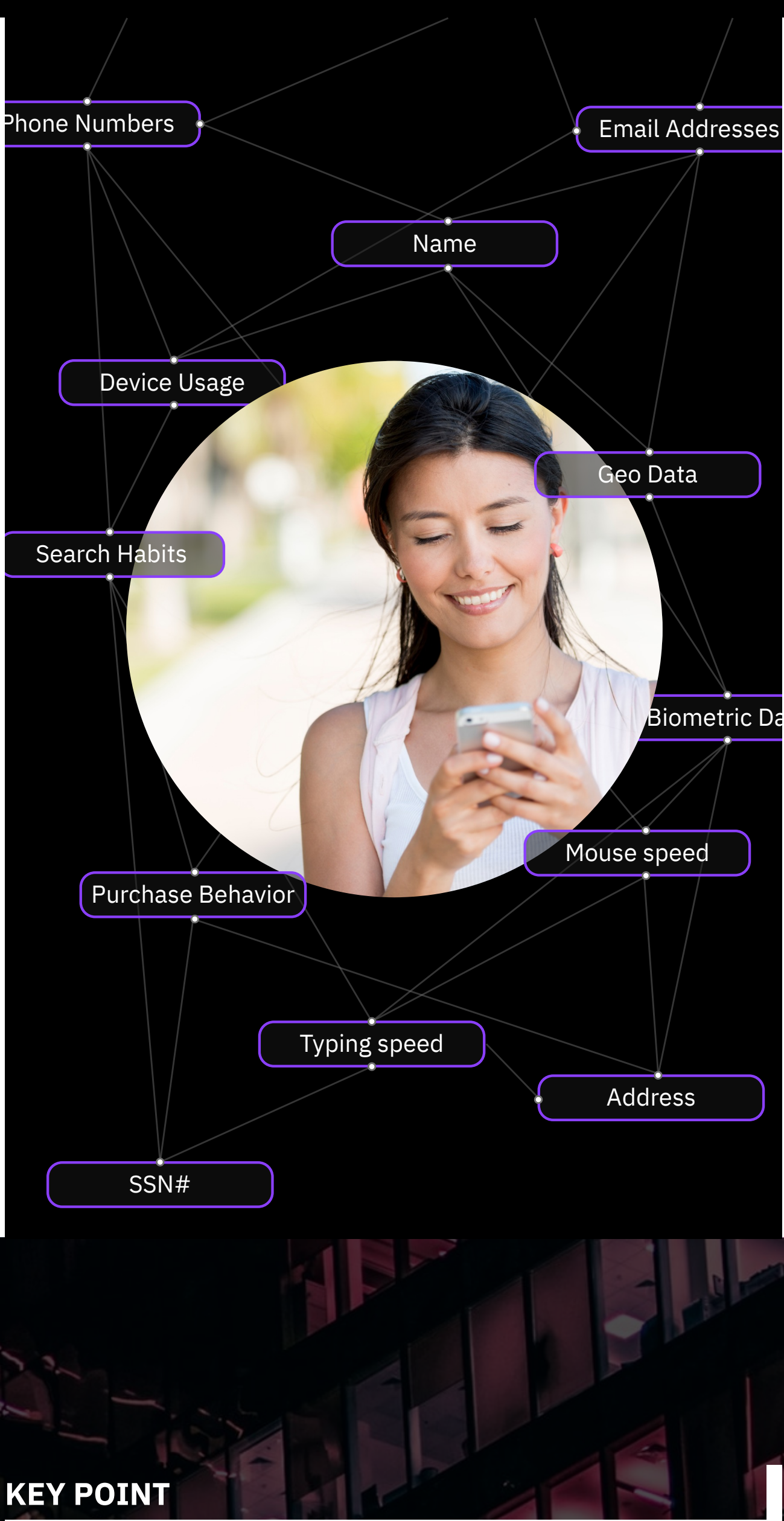
The Power of Identity

Our digital identities are fundamental to how we interact with each other and the online world.[1] The ability to prove who we are provides us with control and allows access to people, information and economies. Digital trust in those identities is power.

But creating a trusted digital identity can be difficult. It's a complex network of traditional instruments of ID such as name, address, birthday and social security number and data points like email address, username and password, search habits, purchasing behavior and so on.

This personally identifiable information (PII) is made up of the unique attributes associated with an individual and is the gateway to every online exchange. These actions rely on context to understand identity.

As the exchanges increase, however, so do vulnerabilities.[2] Bad actors are constantly finding new ways to exploit PII for identity theft or to hack businesses for valuable data. In 2018, the number of consumer records exposed containing sensitive PII shot up to 126%.[3] In 2019, the cost of a data breach increased to nearly $4 million.[4]



Kicking the Can

The problem is people don't exactly understand cybersecurity,[5] and many organizations are still protecting critical applications through username and password alone when there's a better way. Multi-factor authentication (MFA) can add another layer of security and makes it much more difficult for unauthorized persons to gain access. So why is everyone covering their eyes and kicking the can down the road?

Despite a predicted increase and being more secure, only a fraction of organizations use MFA.

They often (mistakenly) believe the risk of frustrating end users, employees and customers is greater than that of a breach. Despite a predicted increase and being more secure, only a fraction of organizations use MFA. According to Gartner, "By 2022, 60% of access management (AM) implementations will leverage user and entity behavior analytics (UEBA) capabilities and other controls to provide continuous authentication, authorization and online fraud detection, up from less than 10% today." [6]

KEY POINT

Despite a predicted increase and greater security, only a fraction of organizations use MFA.

Experience Versus Security

Consider that average business users manage 191 passwords[7] — usually badly with the same password over and over. If this quantity isn't annoying enough, try getting them to wait for a text or email with a code to login.

Or, ask them to identify pictures with cars or traffic lights when most of the pictures appear to have both. Then bombard them with another email warning them of the recent access they just went through multiple steps to gain — that's if they get that far. Only 28% of U.S. adults can even identify an example of two-factor authentication.[8]

Extend this cumbersome process to customers, and they may never return. Today, experience is a key differentiator, so treating customers like cybercriminals risks the bottom line.

Access management does not have to be an either-or choice. MFA isn't clumsy when it's smart. Usability and security can be optimized if security works silently in the background, gathering context about the user and behavior. It then utilizes that context to provide the right authentication process for the situation — creating seamless, adaptive experiences.

KEY POINT

Only 28% of U.S. adults can even identify an example of two-factor authentication.[8]

Olly Olly Oxen Free

With access management that enforces MFA only when risks are detected, you can free your users from friction. Trust is created with a through line of context that starts with the user and flows to the user's device, activity, network environment and behavior.

Device

Activity

Network

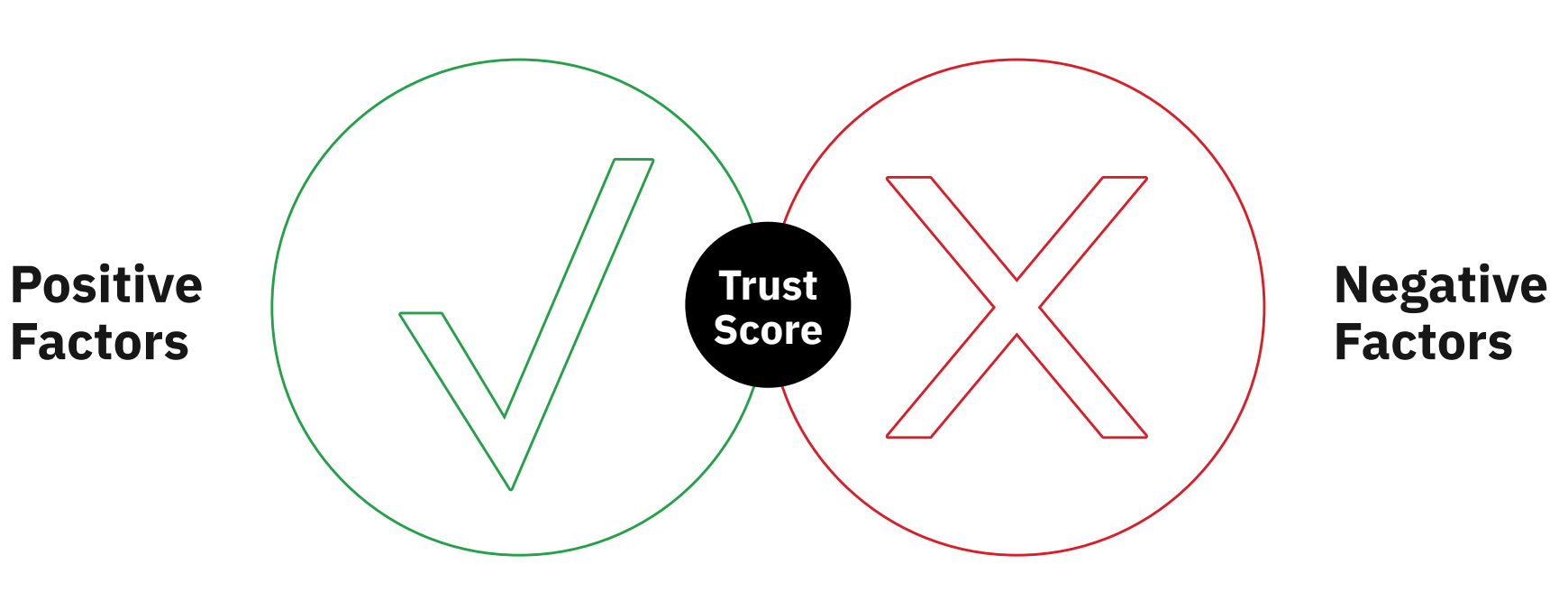
Behavior

Trust Scoring

AI powered risk detection uses machine learning models to synthesize context on mobile devices, web sessions and VPNs based on criteria like known fraudsters, malware infections and other anomalies to automatically recommend MFA in high-risk scenarios.

The context analysis combines both positive and negative factors to build a single indicator of trust. This score takes your strategy from all or nothing to a more nuanced understanding of the level of trust between you and your users. This flexibility is the foundation of an adaptive access strategy.

Once you have a trust score, you no longer need to rely on static rules for authentication. Instead, you can build a smart authentication strategy that delivers frustration free access to your trusted users and can limit access as risk increases. With this approach, low risk users can have a passwordless experience and gain access with no manual effort to assess their identities.



Smart authentication determines:

- Is this a human or bot?
- Does malicious evidence exist?
- Is the phone pre-paid, rooted or jail-broken?
- Does it have a legitimate phone number or email?
- Are patterns malicious?
- Has out-of-band authentication been bypassed?
- Does a login proxy exist?
- Is the user behavior pattern known?
- Do mouse movements seem unusual or automated?

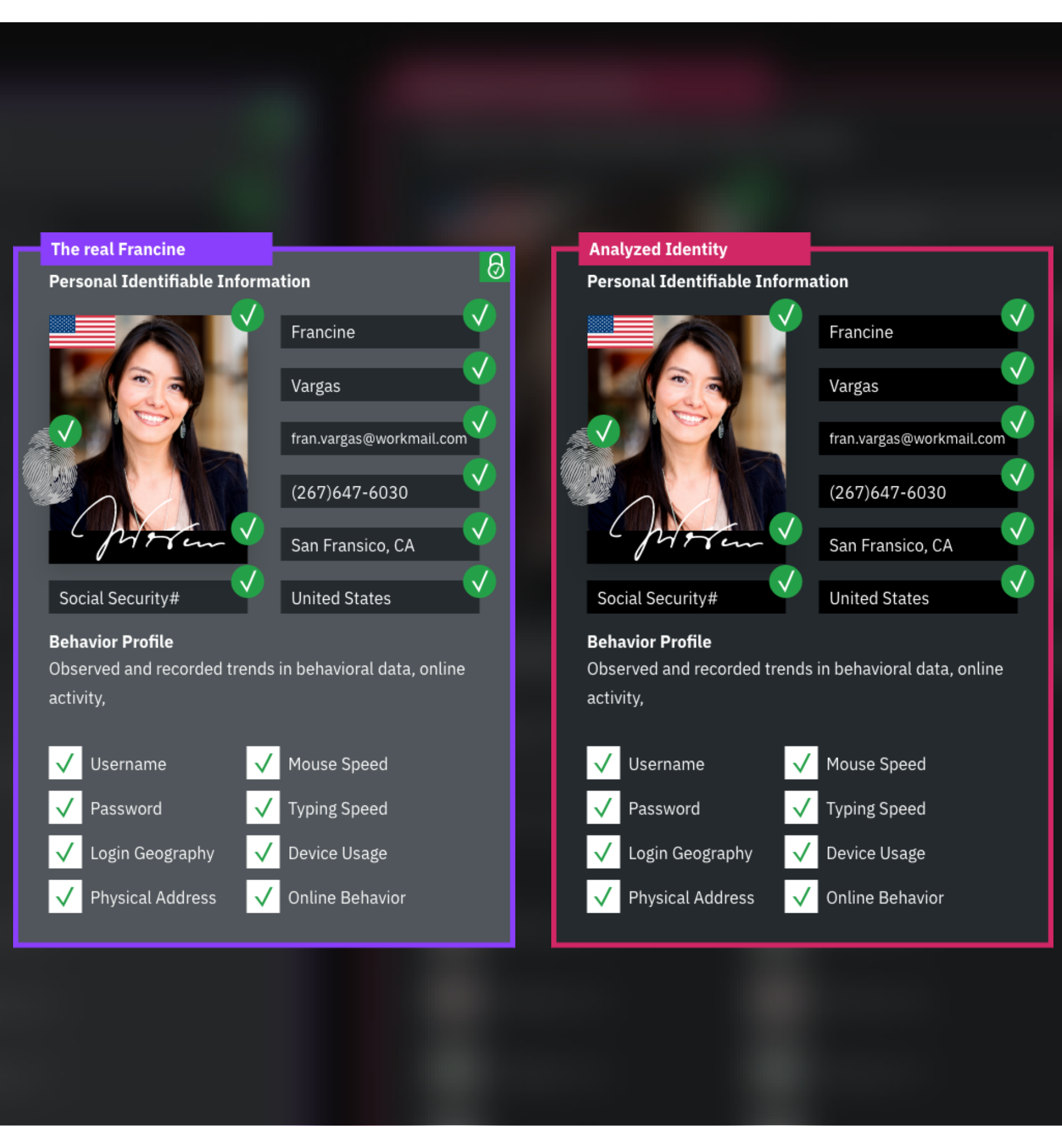
KEY POINT

The context analysis combines both positive and negative factors to build a single indicator of trust.

Trust Scoring: How it works

For example, a user with some minor anomalies may be allowed in with some restrictions on transactions or activity. Users who are highly trusted, with known devices and positive behavioral biometrics scores could be allowed in without a password.

Try the demo



The real Francine

Personal Identifiable Information

Francine ✓
Vargas ✓
fran.vargas@workmail.com ✓
(267)647-6030 ✓
San Fransico, CA ✓
Social Security# ✓
United States ✓

Behavior Profile

Observed and recorded trends in behavioral data, online activity,

☑ Username
☑ Password
☑ Login Geography
☑ Physical Address
☑ Mouse Speed
☑ Typing Speed
☑ Device Usage
☑ Online Behavior

Analyzed Identity

Personal Identifiable Information

Francine ✓
Vargas ✓
fran.vargas@workmail.com ✓
(267)647-6030 ✓
San Fransico, CA ✓
Social Security# ✓
United States ✓

Behavior Profile

Observed and recorded trends in behavioral data, online activity,

☑ Username
☑ Password
☑ Login Geography
☑ Physical Address
☑ Mouse Speed
☑ Typing Speed
☑ Device Usage
☑ Online Behavior

The Adaptive Access Promise

Static rules set the bar for verification too low or too high. IBM Security Verify with adaptive access is an intelligent access management platform that combines advanced risk detection with a robust access policy engine to assess the full context of a user's identity as they attempt to access a digital service. The promise of a frustration free digital experience can be recognized without sacrificing the necessity of security.

For organizations that struggle to optimize identity risk and ease of use, IBM Security Verify with adaptive access reduces authentication complexities by providing frustration free intelligent access to applications and data.

The solution is easily integrated into applications with low to no coding required, through an API for custom applications and pre-built templates for commonly used cloud apps.

KEY POINT

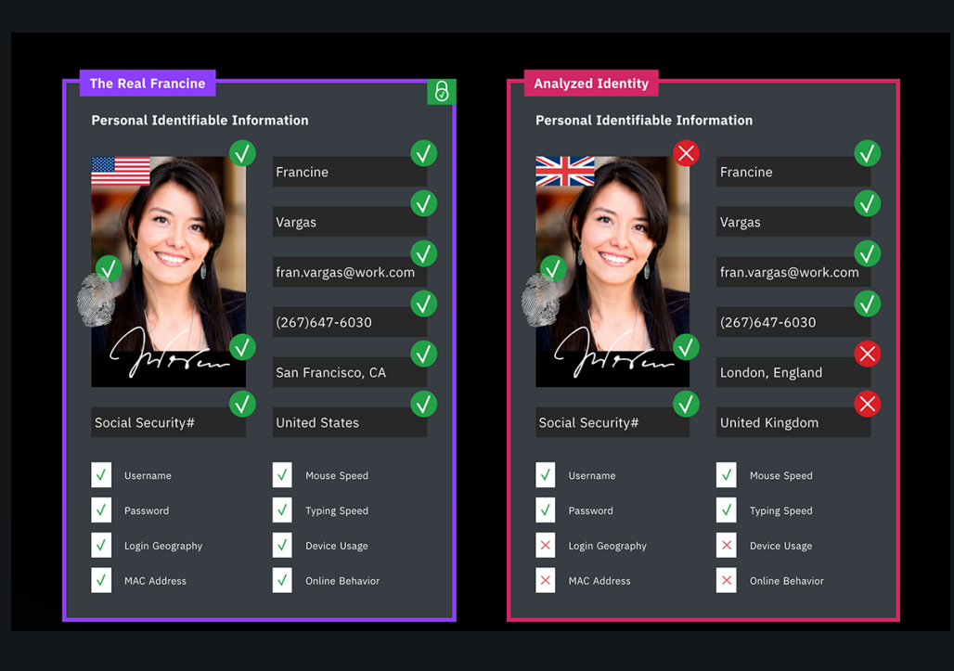
For organizations that struggle to optimize identity risk and ease of use, IBM Security Verify with adaptive access reduces authentication complexities by providing frustration free intelligent access to applications and data.

Authentication should be smarter. Smart authentication adapts.

Next steps

Learn more
Explore three different ways you an supercharge your identity and access management

Read the blog post.



Try the interactive demo
See how Verify with adaptive access works in the real world.

Try the demo.

Hear from Forrester analysts
See why IBM was named a leader in risk-based authentication.

See the report.

Sources

1. IBM, Digital identity management: How much of your personal information do you control?
2. IBM Institute for Business Value, Trust me: Digital identity on blockchain, April 2017
3. Identity Theft Resource Center, Consumers At Risk: 126% Increase In Exposed Consumer Data, 1.68 Billion Email-Related Credentials, Jan. 28, 2019
4. IBM, Cost of a Data Breach, 2019
5. Pew Research Center, What the Public Knows About Cybersecurity, Aaron Smith, March 22, 2017
6. Gartner, 2019 Magic Quadrant for Access Management. Abhyuday Data, Michael Kelley, Henrique Teixeira
7. Security Magazine, Average Business User Has 191 Passwords, November 6 , 2017
8. Pew Research Center, Americans and Digital Knowledge, Monica Anderson and Emily Vogels, October 9, 2019

IBM