RSA

SIX ROADS TO SUCCESSFUL **IDENTITY ASSURANCE**

Whether you're planning a roadtrip or simply commuting to work, your vehicle may force you to compromise on comfort, fuel efficiency, or performance. Likewise, traditional authentication solutions often required a tradeoff between security and usability. Today's enterprise, however, demands a more sophisticated approach—one that can effectively protect critical applications and deliver secure access regardless of where the road takes you.

Risk-based identity assurance uses intelligence to provide a broader context for the user and situation—optimizing both user convenience and access security.

Identity assurance helps quantify the answers to questions like these:

81%
of hacking-related breaches leveraged stolen and/or **WEAK PASSWORDS**[1]

Intelligence-driven identity assurance can result in **90%** **FEWER INTERACTIVE AUTHENTICATIONS** while maintaining MFA-level protection[2]

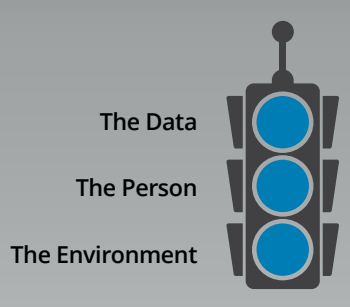
#1
STRENGTHENING IDENTITY AND ACCESS SECURITY is the #1 driver for choosing an IAM solution[3]

GET ON THE FAST TRACK TO **IDENTITY ASSURANCE**

Put your organization on the fast track to identity assurance that's both secure for the organization and convenient for the user.

#1 Business Context: What, Who And Where

Business context underlies baseline assumptions about an access request. It has three fundamental components: data, people, environment.



28%
of smartphone owners don't use a lock screen[4]

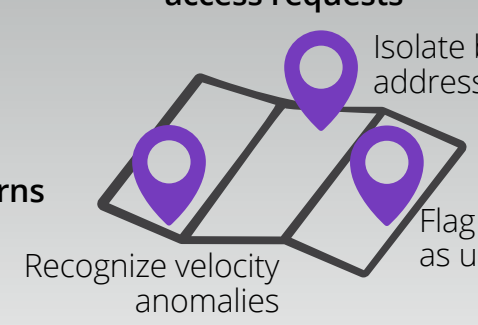
#2 Anomaly Detection: Business As Usual—or Not?

Watching behavior to determine what's normal and what's not—anomaly detection—can unleash broader capabilities, improving both the user experience and security.

Recognizing normal behavioral patterns

- User
- Device
- Location
- Network
- Time of day
- Access patterns

Identifying abnormal access requests



Hackers compromised more than **ONE BILLION** records in 2016[5]

#3 Machine Learning: Getting To Know Users

Machine learning helps track attributes and identify user patterns for even higher confidence in user identity. It can analyze access traffic patterns:

- Location/network
- Time of day
- Device fingerprint
- Pattern of access
- Keystroke dynamics

75%
of breaches are perpetrated by outsiders[1]

#4 Broader Ecosystem: Input From Everywhere

Just as smart cities can help pave the way for safer, hassle-free commutes, access systems should leverage intelligence from sources including threat detection solutions, enterprise mobility management, and physical security systems to ensure a broad view of what's happening around them.

2/3
of organizations averaged five or more breaches in the past two years[6]

#5 Consistent Experience: What's Good for the User

Users are creatures of habit. Consistent behavior should produce consistent results—generating a user experience that's intuitive, easy, and predictable.

38%
of security execs felt their IAM was mature[7]

#6 Flexible Authentication: To Each Their Own

One-size authentication does not fit all. You need flexible authentication for a diverse set of users and use cases, supporting:

- Choice
- Favorites
- Preferences
- Consistency

SIMPLIFYING USER ACCESS was cited by survey respondents as an important element in choosing an IAM solution[3]

GET IN THE **FAST LANE**

These six roads to identity assurance make access both convenient and secure—requiring as little effort as possible on the part of the user while providing the highest level of security for the organization.

RSA SecurID® Access uses risk-based analytics and context-aware user insights to provide seamless authentication, through a variety of authentication methods that don't impede work—and make your trip more enjoyable. Give your organization the confidence that people are who they say they are, while providing a consumer-simple user experience.

87%
of companies surveyed expect to maintain or increase IAM spending in the next 12 months[3]

Learn more at **RSA.com/authentication**

Sources: 1. Verizon. *2017 Data Breach Investigations Report.* 2. RSA Data Science Team 3. IDC, *Global Identity Management Assessment Survey, September 2016.* 4. Pew Research Center, *Lee Rainie and Andrew Perrin, "10 facts about smartphones as the iPhone turns 10", June 28, 2017.* 5. Forrester Research, *Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, January 2017.* 6. Forrester Consulting, *"Stop the Breach: Reduce the Likelihood of an Attack Through an IAM Maturity Model," February 2017.* 7. EY's 19th Global Information Security Survey 2016-17, *Path to Cyber Resilience: Sense, Resist, React.*