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

#2 Anomaly Detection: Business As Usual—or Not?
Detecting behavior to determine what’s normal and what’s not—anomaly detection—can unlock broader capabilities, improving both the user experience and security.

#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, pattern of access, device fingerprint, and keystroke dynamics.

#4 Broader Ecosystem: Input From Everywhere
Just as smart cities can help pave the way for safer, hassle-free commutes, access solutions can 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.

#5 Sustainable Experience: What’s Good for the User
Users are creatures of habit. Consistent behavior should produce consistent results—giving an user experience that is intuitive, easy, and predictable.

#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, preferences, and consensuality.

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.

Learn more at RSA.com/authentication

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.

Identity assurance helps quantify the answers to questions like these:

- How confident am I that users are who they claim to be?
- How sure do I need to be to access another application?
- How are breaches being prevented?
- How can I identify potential security threats?
- Is my IAM solution #1? How do I know?
- How can I ensure that my IAM solution is delivering value?

81% of hacking-related security breaches involve stolen or weak passwords.

80% of security execs feel their IAM was mature.

90% of organizations expect to maintain or increase IAM spending in the next 12 months.

28% of smartphone owners don’t use a lock screen.

75% of security execs felt their IAM was mature.

2/3 of organizations averaged five or more breaches in the past two years.

38% of security execs felt their IAM was mature.


Lessons Learned From The World’s Biggest Data Breaches And Privacy Abuses, January 2017.

2/3 of organizations averaged five or more breaches in the past two years.

The Data
The Person
The Environment

Identifying abnormal access requests
Recognizing velocity anomalies
Spot hot IP addresses
Flag locations as untrusted

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

Strengthening Identity and Access Security is an easy place to start—Choosing the right solution.

2018 Digital Identity Report. In its analysis before the information in this document is acquired or its publication date. The information is subject to change without notice.


How confident am I that users are who they claim to be? How sure do I need to be to access another application? How are breaches being prevented? How can I identify potential security threats? Is my IAM solution #1? How do I know? How can I ensure that my IAM solution is delivering value?