RSA

SOLUTION BRIEF

Risk-Based Authentication

The greater the risk, the higher the bar for access

Risk-based authentication makes it possible to base authentication requirements and access decisions on the level of risk an access attempt poses.

Today, you have more resources to protect, more users needing access from more places, and more threats of credentials-based attacks than ever. As a result, it's tough to keep those resources secure while still making them easily accessible to people who legitimately need them. To do it, you need risk-based authentication, so you can base authentication requirements and access decisions on the level of risk an access attempt poses. Simply put, the greater the risk, the higher the bar for access. Here's what that requires in practical terms:

A variety of tools for assessing risk based on context

Knowing the context for an access request—who is making it, from what device, in what location and other contextual information—is key to determining the level of risk. Behavioral analytics, anomaly detection and related technologies play important roles by uncovering relevant context for an access attempt. That context makes it possible to quickly and easily assess the risk, and determine whether to raise the bar for access.

Machine learning to enable continuous improvement

Technology that can characterize behavior and assess risk is good, but technology that can learn from those experiences and apply that learning to future assessments is even better. Machine learning capabilities mean that when an access request comes in, the technology will retain the relevant details, which can then become part of a growing base of knowledge to be used for comparison and assessment as future requests come in.

A range of choices for step-up authentication

Once it's clear that an access request poses enough risk to warrant further authentication, the next challenge is to ensure that the means of authenticating is stringent enough to repel someone or something that shouldn't have access—but without overburdening a legitimate user. Users need to be able to choose from a variety of strong methods of authentication, to make stepping up to an additional authentication factor as frictionless as possible.

OWN YOUR IDENTITY.

OWN YOUR IDENTITY.

RSA: A context-driven, technology-based approach to risk-based authentication

RSA provides the robust technology and capabilities needed for frictionless risk-based authentication, including:

- **Dynamic, real-time risk scoring**, the result of rigorous data review and interpretation involving multiple inputs and contextual factors
- **Machine learning that draws on ongoing experiences** to drive continuous improvement of risk assessment and decision-making
- **Ability to link to threat detection systems** for access to real-time threat data, which provides added intelligence to gauge access risk
- **A wide range of secure, convenient authenticator choices** that are part of the most widely deployed MFA solution in the world
- Learn more about how RSA risk-based authentication can make securing resources easier without making access harder.

About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to RSA.com.

RSA