SecurID

Risk-Based Authentication: Recognizing and Responding to Risk

Today, you have more resources to protect, more users needing access to them 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 keeping them accessible to people who legitimately need them. To achieve and maintain that balance, you need risk-based authentication, which makes it possible to assess the level of risk an access attempt poses and respond accordingly—alerting the security team to it, for example, or introducing an additional factor of authentication, depending on established policy. 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 associated with the request. Behavioral analytics, anomaly detection and related technologies play important roles in this process by uncovering relevant context for an access attempt. That context makes it possible to quickly and easily assess the associated risk, and establish a basis for further action.

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 of the request. That information 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

If the level of risk associated with an access request warrants 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 not so stringent that a legitimate user finds it difficult to authenticate. Organizations should consider methods of strong authentication that make stepping up to an additional authentication factor as frictionless as possible.

Risk-based authentication makes it possible to assess the level of risk an access attempt poses and respond accordingly.

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

SecurID 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
- When additional authentication is required, **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 SecurID risk-based authentication can make securing resources easier without making access harder.

About SecurID

SecurID, an RSA business, is the trusted identity platform for 13,000 organizations around the world, managing 50 million identities and providing secure, convenient access to 30 million users. SecurID 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, SecurID connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to **securid.com**.

SecurID
An RSA Business