SecurID

Single Sign-on: You Need It Now More Than Ever, for Convenient, Secure Access

The principle is simple: The more resources people need access to, the more they need single sign-on (SSO). And it's not just about making access convenient; it's about making it secure. By reducing the number of access points (and all the easily compromised passwords that go with them), SSO reduces an organization's points of vulnerability. At the same time, by enabling users to sign on once and have access to multiple resources—which today can number in the dozens—SSO reduces the effort required for access. Here's what to look for in SSO solutions to ensure your organization realizes the greatest benefit from SSO—in both security and convenience.

Single sign-on—but not single sign-on alone

SSO works best as part of a comprehensive, multi-faceted approach to identity and access management (IAM). For example, combining SSO with multi-factor authentication can improve security by requiring additional authentication factors beyond the user's SSO log-in.

Risk-based authentication

When multi-factor authentication includes risk-based authentication, it not only improves security but also increases convenience. A risk-based approach means the user is required to step up to an additional factor of authentication when the level of risk warrants it—and only when the level of risk warrants it. That determination is based on who is requesting access, to what, from where and other variables.

A foundation of strong identity governance

A comprehensive approach that brings together MFA, SSO and identity governance is fundamental to delivering fully on the promise of access that is secure without excessively inconveniencing the user. Identity governance enables policy-based access decisions, ensuring that SSO is governed by the organization's established access management policies.

By reducing the number of access points (and all the easily compromised passwords that go with them), SSO reduces an organization's points of vulnerability.

SecurID: The ideal combination of modern authentication and identity governance for successful SSO

SecurID includes SSO capabilities that provide users with a single web-based portal for accessing web and SaaS applications, mobile apps, VPNs and virtual workspaces. SecurID SSO:

- Enables users to **log in everywhere with a single identity,** and for administrators to manage access based on that identity
- Validates access attempts based on user's role, location, network and other factors, then makes **policy-driven, risk-based authentication decisions** in real time
- Provides **tested and certified technology integrations** for SSO access to hundreds of applications and environments, plus open standards to support thousands more integrations
- Makes it easy to populate the SSO portal with applications and other resources using **web-based and SaaS connectors**

Learn more about streamlining access for users and simplifying access management for administrators with SecurID.

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