SecurID

DATA SHEET

SecurID®

Authenticator choice

The choice is yours

For many decades, customers have trusted the one-time passcode (OTP) technology delivered by SecurID, available in a broad range of easy-to-use form factors. Now, SecurID is making the choice easier than ever by supporting new and emerging standards and offering the broadest portfolio of authentication methods for any use case, on-premises or in the cloud. To suit a wide variety of organization and application requirements, SecurID offers the following authentication methods:

Mobile app

Quickly set up advanced mobile MFA options and give users a single authenticator to access both on-premises and cloud applications on all the major mobile platforms (iOS, Android, Microsoft Windows). The SecurID mobile app provides convenient authentication methods, such as push notification, device biometrics, FIDO and OTP, to seamlessly access on-premises (e.g., virtual private network/VPN) or cloud applications (e.g., Microsoft 365).

Fast IDentity Online (FIDO) authentication

As a U2F and FIDO2 certified vendor, SecurID enables a passwordless experience with the broadest support for FIDO authentication, including hardware, software, wearable and embedded options.

Software authenticators

Deploy SecurID software tokens on mobile devices, desktops and laptops, and make strong authentication a convenient part of doing business. SecurID software tokens are available for the following platforms: SecurID Software Token for Microsoft Windows, SecurID Software Token for macOS X, SecurID Software Token for iOS, SecurID Software Token for Android, SecurID Software Token Converter and more.

Hardware authenticators

Protect sensitive data and mission-critical systems with the industry's highest-quality two-factor authentication device, the SecurID hardware token. Gain two-factor authentication, hard disk encryption, email and transaction signing capabilities with a single hardware token.

On-demand: SMS text/voice/email

The SecurID On-Demand Authenticator enables users to receive an OTP as an SMS message delivered to their cell phone or via email. Users are sent an OTP to use as a login to their SMS-enabled mobile device.

Backed by the power of risk-based authentication

SecurID's risk-based authentication automates the analysis (contextual or behavioral) of a series of risk indicators, such as device attributes, user behaviors and geolocation. The higher the risk level presented, the greater the likelihood that it is a fraudulent identity or action. If the risk engine determines the request to be above the acceptable policy, then a "step- up" action is required with another form of authentication.

Highest availability and security with hybrid approach

Organizations need an easy, secure and cost-effective way to support the continually growing collection of authentication methods—a hybrid approach to managing identity risks. SecurID instills confidence with its highly available, secure, scalable and convenient hybrid platform with on-premises, virtualized, cloud and hybrid-cloud options for the most security-sensitive organizations. The SecurID platform with Identity Assurance includes:

- An unrivaled hybrid approach that not only simplifies cloud adoption, but also ensures that modern authentication methods protect both cloud and on-premises resources.
- 24x7 authentication availability and protection, and the confidence to move to the cloud.
- True "no fail-open" offline authentication for both Microsoft Windows and macOS laptop users who are not connected to a network. While other solutions may provide limited offline access, SecurID ensures that users are fully authenticated to sign in, even offline; it provides truly secure access with a seamless experience.
- Conditional access enhances detection of abnormal user, device and network activities inside or outside of the corporate premises. With threat intelligence, organizations can mitigate the risk of insider threats and data breaches, and ensure stronger, continuous authentication.
- Continuous innovations and a Direct Upgrade feature that enable next-generation capabilities; eliminate time-consuming, step-by-step serial upgrade processes; and improve your total cost of ownership (TCO).

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