SecurID

SOLUTION BRIEF

SecurID

Modern authentication for today's identity challenges

Identity is your weakest link

As organizations turn on a growing number of on-premises, cloud and mobile applications, their attack surfaces increase, as does the probability that a single compromised identity can lead to a catastrophic data breach. With most attacks relying on compromised identities somewhere in the chain, identity has become the most consequential threat vector that organizations are facing today.

Now more than ever, organizations need a high level of assurance that users are who they say they are. But to be effective, and to ensure their businesses stay agile, they also need a secure access solution that won't slow users down, but instead provide them with a common and convenient experience to any application, from any device.

Setting the standard for modern authentication

We work hard so you don't have to

Most midsize to large organizations have hundreds of applications deployed and in use. It's not just the number that poses a challenge, but the fact that they have a mix of on-premises, cloud and mobile apps—all of which need protected access.

SecurID provides the most reliable multi-factor authentication (MFA) solution for on-premises applications like virtual private networks (VPNs) and for cloud and mobile applications, including Office 365, Salesforce and Workday.

For over twenty years, SecurID's dedicated partner engineering team has been working hand-in-hand with leading technology vendors to test, certify and support all of our application integrations, to ensure that your security works flawlessly out of the box, and keeps working smoothly even after application providers patch and update their code.

Whether you're new to MFA or have been using it for years, SecurID provides a single, strong authentication platform that covers you from ground (desktops) to the cloud.

Transforming Secure Access

SecurID, the world's most widely-deployed multi-factor authentication solution, delivers a comprehensive set of modern capabilities so you can protect what matters most. You need authentication that's:

- **Convenient** for end users and easy for IT to deploy and maintain
- **Intelligent** and uses real-time context to challenge to the level of risk
- **Pervasive** and can be deployed everywhere

That's SecurID.

Secure and convenient authentication methods

While employees will always be a main concern, organizations have a growing need to provide third parties access. Contractors, partners and customers all need access, for a variety of reasons and use scenarios—and all with different preferences and requirements.

Users need easy and convenient access, while you need the confidence of knowing they are who they say they are. With SecurID, you don't have to trade convenience for security. In addition to our award-winning tokens, we offer a broad set of authentication options that work directly on users' mobile phones—including push to approve, biometrics, SMS and more—ensuring you have the "right size" authentication for each user and every use case.

Whether you need the "air gap" security hardware tokens uniquely provide or the low touch capabilities of SMS, SecurID delivers a solution that's easy for users to use, and for you to deploy, while giving you peace of mind that your most sensitive assets are protected.

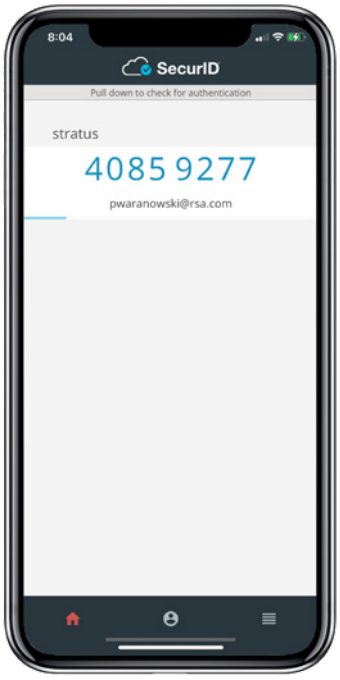
Push-to-Approve

Going beyond multi-factor

For added security and improved usability, we've taken authentication beyond simply two or three factors. SecurID uses machine learning behavioral analytics, business context and threat intelligence to draw a comprehensive picture of the user and the risks associated with their access.

Analyzing contextual attributes related to when and where an access request comes from, the security posture of a device, the user's role and sensitivity of the application, and whether they've been associated with known fraud or exposed to known threats, provides a 360-degree view of the risk associated with user access.

SecurID automatically, and without requiring any intervention, calculates an identity confidence score (Low or High) for each user, based on a variety of data points. By doing this in real time, organizations can automatically challenge users based on the level of risk—ensuring that high risk is met with high security, while low-risk cases are afforded the convenience of not being asked for any additional authentication.



Mobile OTP

Simplifying authentication requirements

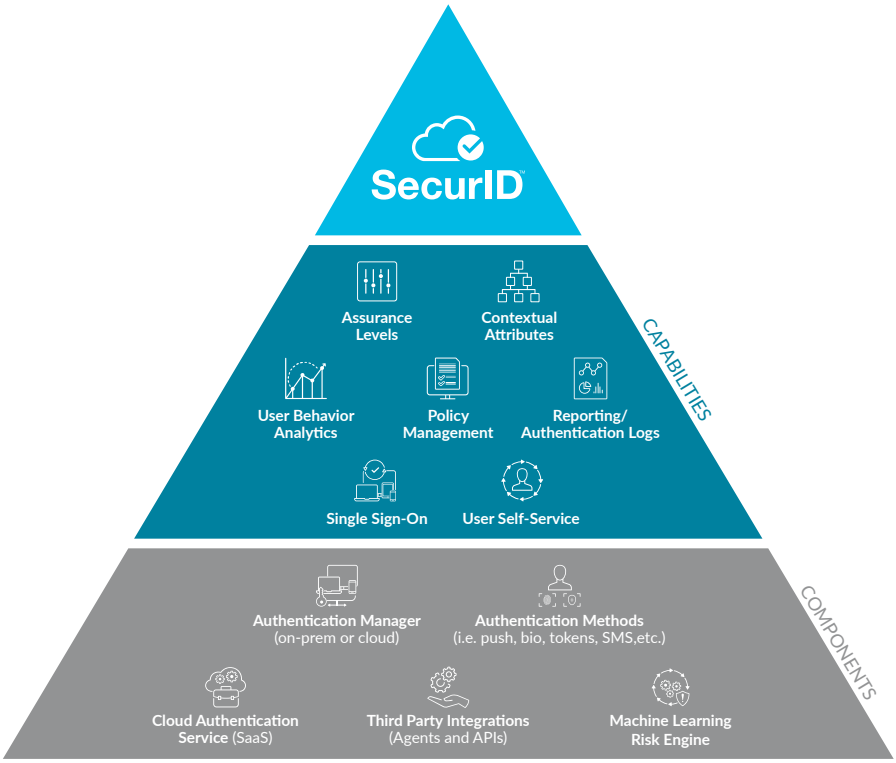
With a large number of applications to support, and an increasing variety of ways to verify users and measure access risk, organizations need an easy way to pull it all together—a simple way to define their authentication requirements.

Since different use cases require different levels of authentication, SecurID provides organizations an easy way to configure authentication options based on the user, application, context and risk information it collects.

SecurID assurance levels enable organizations to simply group their use-case requirements into three levels—Low, Medium and High assurance. Each level corresponds to the relative strength of security organizations require for a particular

application or use scenario. Low-risk scenarios need low levels of assurance (verification), while those of the higher-risk variety may require different, more secure types of access controls.

SecurID core components



Authentication methods: In addition to our award-winning tokens, SecurID offers a broad set of phone-based authentication options including push to approve, OTP, biometrics, SMS and more. Further, SecurID also offers risk-based or adaptive authentication, which uses machine learning behavioral analytics to determine a real-time confidence score for each user.

Cloud authentication service is a software-as-a-service (SaaS) access and authentication platform that provides single sign-on (SSO) and multi-factor authentication for SaaS, cloud, web and mobile applications. The Cloud Authentication Service can also accept authentication requests from third-party SSO solutions or cloud applications that have been configured to use SecurID as the identity provider (IdP) for authentication.

SecurID authentication manager verifies authentication requests, and centrally administers authentication policies, SecurID tokens, users, agents and resources across physical sites, to help secure access to on-premises, cloud and web-accessible applications such as VPNs and web portals.

SecurID agents and APIs: We provide connectors and standard agents for SAML and RADIUS-based applications, as well as for IIS/Apache, Windows, Unix/Linux and ADFS. In addition, SecurID provides a REST-based API so organizations can add multi-factor authentication to their custom applications.

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