![Symantec - A Division of Broadcom]

Product Brief

Symantec Advanced Authentication

Overview

Symantec Advanced Authentication provides a secure, user-friendly, and cost-effective way to protect mobile and web applications. The solution allows organizations to silently and transparently collect data and assess risk based on device identification, geolocation, and user behavior, among other factors. Symantec Advanced Authentication also provides a wide variety of software-based, two-factor authentication credentials to make logins more secure. Combining risk assessment and multifactor credentials enables an intelligent, layered, security approach. This approach prevents inappropriate access and online identity fraud without impacting the user experience.

Business Challenges

Your employees, partners, and customers all need easy access to your online applications; and you need to protect your sensitive data from improper access. Organizations like yours must meet the following challenges:

- **Improve security for online transactions.** Passwords can be easily compromised. Organizations need an adaptive way to identify users and protect against inappropriate access.
- **Enable mobile devices securely.** Mobile devices and apps are becoming the preferred method for users to interact with the business. Organizations need a consistent authentication strategy that accommodates all channels of access and devices.
- **Meet regulatory compliance directives.** Many regulations and industry guidelines are recommending or requiring stronger authentication mechanisms. Organizations need to address these requirements in a cost-effective manner.
- **Provide a superior user experience.** Users are fickle and impatient. Organizations need to increase security without impacting the user experience.

Solutions Overview

Symantec Advanced Authentication is a packaged solution that combines two leading authentication products:

- **Symantec Risk Authentication** performs a transparent, intelligent risk analysis to provide greater assurance that the user is who they claim to be. The software evaluates risk based on device, geolocation and user behavior for any online transaction, and can initiate step-up authentication when the risk score exceeds defined thresholds.

Key Benefits

- Provides a frictionless user experience through transparent risk analysis and software-based 2FA credential.
- Reduces exposure to data breaches, inappropriate access, and identity theft.
- Lowers cost of operations by reducing online fraud.
- Helps meet government regulations and industry guidelines for stronger authentication.

Key Features

- Performs real-time risk assessment to protect sensitive logins and transactions.
- Evaluates risks based on device identification, geolocation, user behavior and other factors.
- Supports out-of-band methods such as push notification and one-time passwords (OTP) delivered by email, text, or voice for step-up authentication.
- Provides default rule sets covering typical fraud patterns that are easy to use and customize.
- Supports a wide variety of credentials, from passwords and security questions, to 2FA software and hardware tokens.
- Protects web and mobile channels and integrates data for comprehensive fraud management
- Offers several standards-based integration options: OATH, RADIUS, REST, SAML and SOAP.
- Integrates tightly with CA Single Sign-On and other web access management systems.

- **Symantec Strong Authentication** provides multifactor authentication for web and mobile apps with a wide range of credentials and methods. The software allows you to deploy the right credential with the right level of security based on the app being accessed.
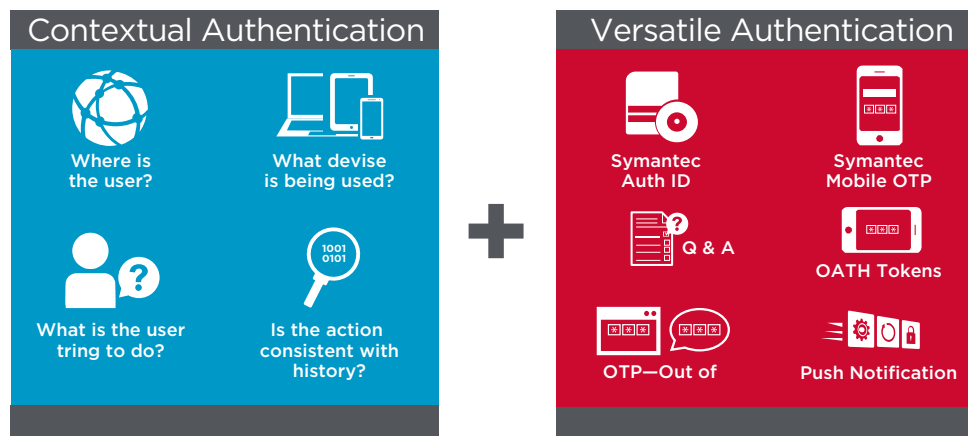
Together, these products enable a layered security approach that gives you the right balance of cost, convenience, and security to protect your applications and user identities. This results in better security, an improved compliance profile, and lower operational costs.

Two best-of-breed components that can be deployed individually or together.

Contextual Authentication — Where is the user? What devise is being used? What is the user tring to do? Is the action consistent with history?

Versatile Authentication — Symantec Auth ID, Symantec Mobile OTP, Q & A, OATH Tokens, OTP—Out of, Push Notification

Critical Differentiators

Symantec Advanced Authentication is a complete solution that offers the following critical differentiatiors:

- A white-box philosophy provides visibility into each risk rule, decision, and outcome. You also have the ability to refine the balance of risk and user convenience that is appropriate for your organization.

- User behavior profiling reduces friction by learning a user's behavior patterns and detecting when this deviates from the norm.

- A flexible rules engine gives you complete control of your environment, especifically the ability to create custom rules, policies, and actions to adapt the risk engine to specific use cases and transactions.

- Flexible authentication supports a wide variety of authentication credentials and flows, and allows you to set different step-up authentication methods based on risk level.

- Case management includes a policy-based system to review and manage cases of suspicious activity.

- Password protection eliminates the risk of stolen password files because passwords are never stored on the user's device or within any backend system; passwords are also never transmitted over the internet.

- Cryptographic camouflage is a patented key concealment technology used to protect the unique AuthID and Mobile OTP credentials from brute force and dictionary attacks.

Related Products

- **Symantec SiteMinder.** Enable Web single sign-on for on-premises, hosted, or partner-based applications for your customers and business partners.

- **Layer7 API Gateway.** Provide a trusted API security solution for integrating across apps, devices, and businesses.

Symantec™
A Division of **Broadcom**