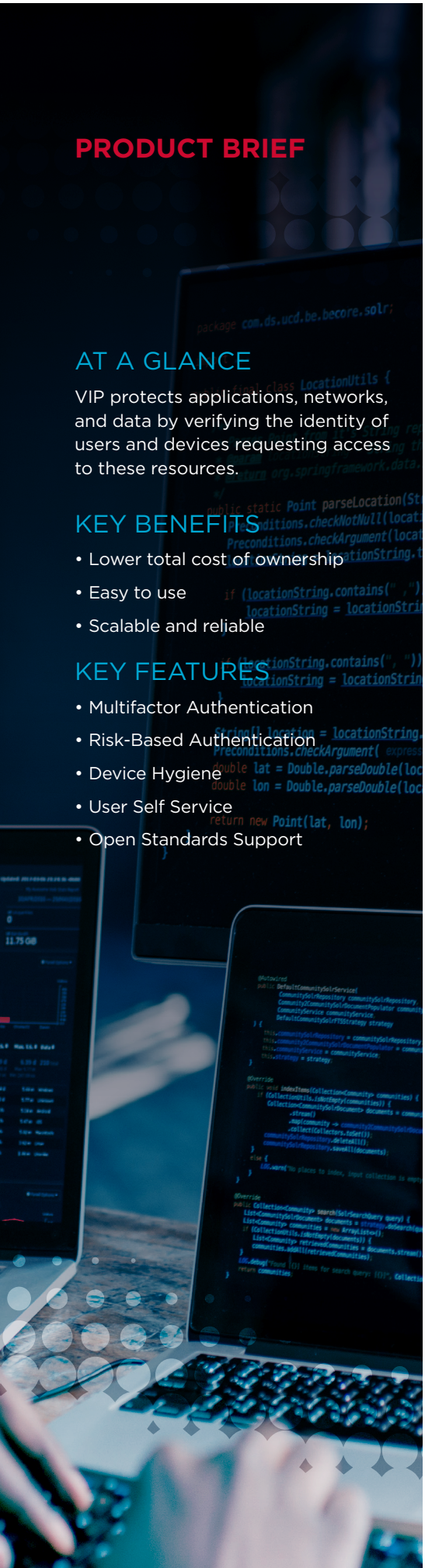
PRODUCT BRIEF



AT A GLANCE

VIP protects applications, networks, and data by verifying the identity of users and devices requesting access to these resources.

KEY BENEFITS

- Lower total cost of ownership
- Easy to use
- Scalable and reliable

KEY FEATURES

- Multifactor Authentication
- Risk-Based Authentication
- Device Hygiene
- User Self Service
- Open Standards Support

Symantec® VIP

Overview

The modern world is becoming more complex and dynamic. Every user interaction, both internal and external, is driven by a connected application, a device-based interface, a web-based portal, or in many cases, the option to use all three. The number of new online services being deployed is expanding faster and faster. To thrive in this new reality, organizations need to deliver a superior customer experience with every touch. For many, this need means providing a seamless and consistent user experience across all access channels without compromising security. The initial point of interaction is the login process, which requires something stronger than a password, but does not add undue friction.

Symantec® VIP is a leading cloud-based strong authentication service that protects networks and applications by verifying the identities of users and devices to prevent unauthorized access. VIP also enables convenient and frictionless two-factor authentication for consumer access to applications, to provide that extra layer of security against account takeover. The core capabilities of VIP strengthen security and maximize the user experience through six key features:

- **Multifactor Authentication:** VIP delivers two-factor, cloud-based strong authentication that combines something you know (such as a password) with something you have (such as a token or device).
- **Risk-Based Authentication:** VIP leverages device and user behavior profiling to challenge risky login attempts without changing the legitimate user's login experience.
- **Device Hygiene:** VIP denies access to compromised devices before they attempt to authenticate to your applications or network, and it tracks advanced and persistent threats.
- **User Self Service:** VIP improves adoption and experience through a secure and intuitive credential provisioning and user onboarding process.
- **Open Standards Support:** VIP integrates with popular VPNs, cloud and web applications, and user directories with popular standards such as SAML and RADIUS.

With these core features, VIP applies the appropriate level of security to verify users and devices to enable Zero Trust access across your hybrid environment.

Multifactor Authentication

Being able to positively identify legitimate users from fraudulent ones is an important first step to achieving Zero Trust, and a critical step in designing a modern identity fabric. VIP enables enterprises to deliver secure access to corporate networks and applications from anywhere in the world, providing improved productivity and better insight. The service offers a multitude of user-friendly authentication options to protect against unauthorized access, including a broad range of second-factor options such as push, SMS or Voice OTP, mobile authenticators, FIDO2, and biometrics. VIP also offers a series of hardware-based authenticators, including cards, keys, and tokens that can be purchased separately. These options can be used for internal employees or partners. Finally, the cloud-based service is also built to protect consumer-facing mobile and web applications, resulting in increased customer confidence and reduced fraud costs.

Risk-Based Authentication

Hackers leverage sophisticated ways to compromise user accounts to gain unauthorized access, and stronger authenticators are not always sufficient to prevent these attacks. Fortunately, user behavior analytics enables organizations to assess risk and quickly detect abnormal activity. VIP captures user and device profile data during the initial login attempt, compares that data against historical data to assess risk, and then either grants or challenges access based on the results. For example, the risk engine evaluates the user's location against their prior authentication location to determine if they have traveled an impossible distance. It reviews the historical authentication locations and increases the risk if the latest authentication is coming from somewhere new. This is just one of the behaviors evaluated, the engine can also identify risky countries or IP addresses that should challenge the user for additional authentications.

Device Hygiene

VIP includes a device hygiene SDK that can be used inside of a mobile application to evaluate the device for malware, jailbreaking, and network risk. The SDK also lets your client deny access to compromised devices before they can attempt authentication to your network, and track advanced and persistent threats.

User Self Service

One of the most critical success factors when implementing stronger authentication mechanisms is to optimize the end-user experience, to balance better security against convenience. Those that succeed will see high user adoption. The first part of this process is to select the right authentication approach to deliver protection for a variety of users and use cases; VIP meets that need by providing a broad range of authenticators. The second part is to provide a seamless process to onboard users and provision their credentials. VIP provides an intuitive credential provisioning portal for end users that reduces help desk and administrator costs. The service also requires users to authenticate their identity before they are allowed to register their device to ensure secure onboarding.

Open Standards Support

As cloud infrastructure, VIP delivers a secure, reliable, and scalable authentication service without the need to deploy on-premises hardware; however, VIP does integrate with networks, servers, and applications that might exist both on-premise and in the cloud. VIP does this integration using open standards, including SAML and RADIUS (leveraging the VIP Enterprise Gateway). Additionally, VIP provides APIs and an SDK that enables organizations to easily integrate or embed two-factor authentication mechanisms with their web and mobile applications.

Summary

The world's largest organizations rely on VIP to deliver strong authentication to protect their network and corporate applications. With a proven track record of success, VIP's cloud-based infrastructure delivers scalability and reliability to support millions of users. With a volatile authentication market, you can rely on Broadcom being there for you as a trusted security partner long after the competition is gone.

For more information, please visit: broadcom.com/symantec-vip

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SED-VIP-PB101 April 17, 2023