SOLUTION BRIEF

CHALLENGE

Effectively distinguishing legitimate users from fraudulent ones is a crucial step in enforcing Zero Trust access policy controls, but implementing strong authentication impacts user experience.

OPPORTUNITY

Building an identity fabric begins with a modern authentication service, which establishes confidence that the user is whom they claim to be without undue friction.

BENEFITS

The Symantec® VIP solution delivers a modern authentication service that accelerates business operations by providing unified, frictionless access across diverse security layers within an organization.

Multifactor Authentication Made Easy

Introduction

The digital revolution is unlike anything previously experienced in its scale, scope, and complexity. To adapt, modern enterprises are increasingly migrating their IT infrastructure to the cloud. However, these transformations are not without risks. As the physical perimeter is broken, traditional IT defenses are being strained to protect the expanded hybrid landscape. In fact, the World Economic Forum recently stated that, "traditional cybersecurity measures are increasingly being rendered obsolete by the growing sophistication of cybercriminals." Organizations rush to address policy inconsistencies and security gaps, but the strategic solution to these challenges in a modern identity fabric.

The Modern Identity Fabric

As organizations migrate to the cloud, most of their applications and data are running in someone else's infrastructure. Under this scenario, the only real assets owned by an enterprise are the user identities, the access they are given, and the information that they interact with. The universal glue that ties everything together is identity, and it must exist everywhere.

A modern identity fabric that embraces the principles of Zero Trust will securely bridge yesterday's data center with today's hybrid environment to provide strong and consistent controls over access to your network, applications, and data, no matter where they reside or how they are accessed. A modern identity fabric accomplishes this through the following functions:

- Authenticating users to positively identify who is trying to access apps and data
- Authorizing access continuously, based on risk and data sensitivity
- Allowing, adjusting, or blocking access automatically to mitigate attacks
- Monitoring access and normal behavior to recognize risky activity patterns
- Managing and governing entitlements to ensure least privileged access

Zero Trust adoption begins with authentication—positively identifying legitimate users from fraudulent ones is a foundational step as least privileged access cannot be enforced if you do not know who is requesting the access. Identity is the last, and sometimes only, defensible perimeter in the hybrid cloud world as business users need to access data from any device, any location, and at any time. This is also crucial for consumer applications, but far more difficult to achieve as the need to balance security against user convenience is precarious. Symantec® VIP provides strong authentication that verifies the identities of users and devices while delivering a superior customer experience. Furthermore, VIP now offers two deployment models that enable even greater flexibility and control to customers.

Introducing Symantec VIP

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 four key areas:

- **Multifactor Authentication:** VIP delivers two-factor, cloud-based strong authentication that combines something you know with something you have.
- **Risk-Based Authentication:** VIP leverages device and user behavior profiling to challenge risky login attempts without changing the legitimate user's login experience.
- **User Adoption:** VIP improves adoption and experience through a secure and intuitive credential provisioning and user onboarding process.
- **Interoperability:** VIP integrates with popular VPNs, cloud and web applications, and user directories with popular standards, such as OIDC and SAML.

VIP Authentication Hub is included with the VIP SaaS service and offers an alternative deployment option for organizations seeking two-factor authentication for employee and consumer application access. Leveraging a cloud-native architecture and API-first philosophy, the VIP Authentication Hub delivers modern authentication and identity services as microservices, and offers more control and flexibility over these services than is normally available from a cloud-based service.

Which VIP is Right for Me?

The two VIP deployment options offer comparable features and capabilities.

Multifactor Authentication

One of the primary differences between VIP SaaS and the VIP Authentication Hub is the ability to perform primary and secondary authentication. VIP SaaS provides secondary authentication, which means that during the authentication process, the user presents their initial login credential, most likely a password, which gets verified. This is the primary authentication. Next, the application requests a secondary or step-up authentication from the VIP SaaS, which then sends a challenge to the user. This could be a push notification or a one-time passcode sent via text or email. The user must complete this challenge before they are successfully authenticated. VIP SaaS does not store user passwords in the cloud; however, it can support integration via the VIP Enterprise Gateway for primary authentication. The VIP Authentication Hub also supports both primary and secondary authentication services:

- In terms of primary authentication mechanisms, the VIP Authentication Hub supports basic authentication.
- Both VIP SaaS and VIP Authentication Hub support step-up two-factor authentication methods, including 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 mechanisms can be triggered automatically based on policy or risk.

That being said, VIP SaaS and VIP Authentication do both support passwordless authentication, which is considered a primary authentication mechanism. In this case, both solutions support FIDO2-compliant credentials, which enables passwordless authentication and addresses recent Federal mandates for phishing-resistant credentials. This allows both solutions to support device and embedded biometric sensors, including fingerprint and facial recognition.

The final differentiation between VIP SaaS and VIP Authentication Hub, from an authentication point of view, is policy enforcement. VIP SaaS has a basic group policy that can control which credentials are available to a group of users; however, VIP Authentication Hub provides more control over the authentication journey. When implementing stronger authentication mechanisms, organizations seek to strike the right balance between security and convenience, only prompting users for additional credentials when it is absolutely required. VIP Authentication Hub enables the creation of policies that orchestrate authentication flows based on factors such as risk, group memberships, and IP location This also includes options that, for example, allow users to indicate that their device should be trusted, so they can bypass MFA requirements on subsequent logins.

Risk-Based Authentication

Contextual risk analysis helps mitigate identity fraud and augment password-based authentication while minimizing friction, requesting second-factor credentials only when the risk surpasses a specific threshold. VIP SaaS and VIP Authentication Hub both provide this capability by utilizing a risk engine to enhance password-based authentication. With each login or transaction attempt, the risk engine analyzes the user's endpoint device and normal login behavior to determine the likelihood that the attempt comes from a known and legitimate user. The VIP Authentication Hub also can be easily integrated with external risk engines and leverage their risk scores in authentication policy decisions.

Interoperability

Strong authentication protects networks and applications by verifying the identities of users and devices to prevent unauthorized access. It also enables convenient and frictionless two-factor authentication for consumer access to applications, to provide that extra layer of security against account takeover. This is only achieved if the strong authentication can be easily integrated and consumed by external applications. VIP SaaS and VIP Authentication Hub integrate with cloud and web applications, and user directories with popular standards such as OpenID Connect, OAuth, and SAML. Furthermore, both solutions support the recent Federal mandate for phishing-resistant credentials by supporting FIDO2-compliant credentials.

Comparative Analysis

The two VIP deployment options offer comparable features and capabilities. There are, however, a few notable differences which are captured in the table below:

Features and Capabilities	VIP SaaS	VIP Authentication Hub
Deployment Model	*Cloud Service (SaaS)*	*Cloud Native (Kubernetes)*
Multifactor Authentication		
Primary Authentication	*Yes, with EGW*	*Yes*
Secondary Authentication	*Yes*	*Yes*
Passwordless Authentication	*Yes*	*Yes*
Authentication Policy Enforcement	*No*	*Yes*
Credential Type		
FIDO2	*Yes*	*Yes*
Time-Based OTP (software and hardware)	*Yes*	*Yes*
Push Notification	*Yes*	*Yes*
Mobile SDK and App from Stores	*Yes*	*Yes*
OTP via SMS	*Yes*	*Yes*
OTP via Voice	*Yes*	*Yes*
OTP via Email	*No*	*Yes*
Risk-Based Authentication		
User Behavior Analytics	*Yes*	*Yes*
Device Hygiene	*Yes*	*Yes*
Third-Party Risk Engine Integration	*No*	*Yes*
Identity Services		
Identity Store	*No*	*Yes*
Full Lifecycle Management for Users and Groups	*No*	*Yes*
Self-Service Password Recovery	*No*	*Yes*
Password Management and Policy	*No*	*Yes*
Self-Service Account Unlock	*No*	*Yes*
Self-Service MFA Registration and Provisioning	*Yes*	*Yes*
Interoperability		
APIs	*SOAP and REST*	*REST*
OAuth	*Yes*	*Yes*
OpenID Connect	*Yes*	*Yes*
RADIUS	*Yes*	*No*
SAML	*Yes*	*Yes*
SCIM v2	*No*	*Yes*

Integration Made Easy

Broadcom has been delivering identity and access management solutions to the world's largest enterprises for over 50 years, starting with access management on the mainframe with ACF2™ and Top Secret™, to securing online access with SiteMinder™, securing APIs with Layer7™, managing and governing user entitlements with IGA, and protecting privileged access with PAM. One of our design philosophies is to ensure that strong authentication can be leveraged and easily integrated across all of these solutions. The following table highlights which solutions natively support VIP SaaS and VIP Authentication Hub.

Solution	VIP SaaS	VIP Authentication Hub[a]
IGA	*Yes*	*Coming Soon*
Layer7 API Gateway	*Yes*	*Yes*
Mainframe	*Yes*	*Yes*
PAM	*Yes*	*Coming Soon*
SiteMinder	*Yes*	*Yes*
VIP SaaS	—	*Yes*

[a] The VIP Authentication Hub is provided as a no-charge entitlement to customers who have licensed specific solution SKUs.

Summary

The foundation for accessing sensitive data relies on establishing sufficient trust in the identity of the requesting user. This concept is reinforced by the emergence of Zero Trust principles, which require the verification of the identity of every device and user seeking access. As a result, regulatory bodies and auditors now mandate the implementation of stronger authentication mechanisms when users access personal, financial, and health-related data. Symantec VIP SaaS and VIP Authentication Hub deliver modern authentication services that protect networks and applications by verifying user and device identities, preventing unauthorized access. They also offer convenient two-factor authentication for employee and consumer application access, adding an extra layer of security against account takeover. But which solution is right for you?

- **VIP SaaS** is the ideal solution for customers seeking multifactor authentication, but do not need complex authentication flows or integration with third-party risk engines. This is ideal for safeguarding consumer applications that may still be using passwords as the primary authentication mechanism.
- **VIP Authentication Hub** may be better for customers who do not want to use SaaS or maybe desire more control over the authentication flow, or who want to leverage existing risk or fraud engines as part of their authentication process.

The case could be made for organizations who have use cases that require both, and for that reason, the VIP Authentication Hub is provided at no additional cost as part of the VIP SaaS subscription; however, regardless of which option you select (or both), the VIP solutions enable organizations to strike the right balance between security and convenience, safeguarding resources against unauthorized access and aligning with Zero Trust initiatives access across your hybrid environment.

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

BROADCOM®
connecting everything®

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

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
SYM-MFA-SB100 January 30, 2024