Technical White Paper

Symantec™ VIP Intelligent Authentication

Who should read this paper

This white paper is intended for a technical audience interested in learning how Symantec™ VIP Intelligent Authentication's risk-based authentication approach protects enterprise and web-based applications, such as SSL VPNs, webmail, single sign-on gateways, and collaboration tools, against unauthorized access. A working knowledge of networking and information security principles is recommended.

Content

Introduction

Your organization's confidential systems require more protection against today's sophisticated attacks than a simple user name and password can provide. Keyboard logging software, malware installed in users' browsers, and good old-fashioned social engineering attacks are eroding your organization's ability to defend its sensitive information. Attackers are constantly changing tactics, and your organization needs to stay ahead of these emerging authentication threats.

Yet for many applications and users, organizations must strike a balance between the security required to protect sensitive applications and the convenience that their users demand. Organizations require the ability to restrict access to sensitive infrastructure and data, without hampering the productivity of its employees or placing an undue burden on its customers or partners. The Symantec™ VIP Intelligent Authentication feature of Symantec™ Validation and ID Protection Service (VIP) protects your organization's network and applications against unauthorized access and delivers:

- **Simple, convenient strong authentication:** VIP Intelligent Authentication delivers strong authentication without changing the logon experience for legitimate users. By examining device and behavior characteristics, VIP Intelligent Authentication transparently authenticates known users exhibiting expected logon behavior.
- **Superior protection from emerging threats:** VIP Intelligent Authentication defends your organization against high-risk logon attempts from malicious sources identified by the Symantec™ Global Intelligence Network, a global network providing comprehensive, up-to-date information on sources of malicious Internet activity. For users of Symantec™ Endpoint Protection, Norton® AntiVirus, or Intel® Identity Protection Technology (IPT)-enabled computers, VIP Intelligent Authentication can leverage hardware-based device identifiers to strengthen the authentication process.
- **Comprehensive, scalable authentication:** VIP Intelligent Authentication is part of the Symantec™ Validation and ID Protection Service, a unified enterprise authentication solution. With Symantec VIP, organizations can also deploy hardware or software one-time-password (OTP) tokens, mobile OTP tokens, and SMS or voice-enabled OTP authentication. Symantec VIP's cloud-based approach enables organizations to scale to millions of users easily and cost-effectively, without requiring in-premise authentication servers.

Who Should Read This Document

This white paper is intended for a technical audience interested in learning how VIP Intelligent Authentication's risk-based authentication approach protects enterprise and web-based applications, such as SSL VPNs, webmail, single sign-on gateways, and collaboration tools, against unauthorized access. A working knowledge of networking and information security principles is recommended.

What You Will Learn

This technical overview details how VIP Intelligent Authentication can be deployed to protect enterprise and web-based applications. By the end of this white paper, the reader will understand how VIP Intelligent Authentication assesses the riskiness of a logon, enables a transparent logon for legitimate users, responds to a high-risk logon attempt, and integrates with an organization's enterprise and web-based applications.

Solution Overview

The best practice for protecting confidential networks and applications, and the solution required by many regulatory and industry mandates, is to deploy strong authentication. Strong authentication is a way of verifying a user or device's identity using more than one authentication factor, where an authentication factor is one of:

- **"Something you know":** information such as a password or the secret answer to a question that is known only to you and the organization to which you need to authenticate.
- **"Something you have":** a hardware or software credential, such as a one-time-password token or digital certificate installed on a user's machine or on a smart card.
- **"Something you are":** a trait inextricably tied to the user, such as a fingerprint, or the behavior exhibited by the user in prior interactions with the organization.

Combining two or more of these factors dramatically increases the difficulty of impersonating an individual or device, and decreases the risk of unauthorized access to protected resources.

A Risk-Based Approach to Authentication

VIP Intelligent Authentication differs from traditional enterprise two-factor authentication approaches that rely on one-time-password tokens to augment password-based authentication. For each logon attempt, VIP Intelligent Authentication examines the user's endpoint device and the user's logon behavior to assess the likelihood that the logon originates from a known, legitimate user.

In essence, VIP Intelligent Authentication allows the user's device to act as the "something you have", and the user's behavior to provide the "something you are". This approach has the benefit that the process of authentication is invisible to a legitimate end user, creating a simple and transparent logon experience.

Transparent Authentication Process

When integrated with an enterprise or web-based application, VIP Intelligent Authentication transparently assesses the risk posed by each authentication attempt by examining the user's device, its configuration, its geographic location, and its network origin. These inputs are used to assess the risk posed by the logon attempt in the context of expected device characteristics and user behavior, as well as intelligence on sources of malicious network activity provided by the Symantec Global Intelligence Network.

For any given logon attempt, there are two paths the authentication process can follow – that of a low-risk logon attempt, and that of a high-risk logon attempt – as illustrated in Figure 1.

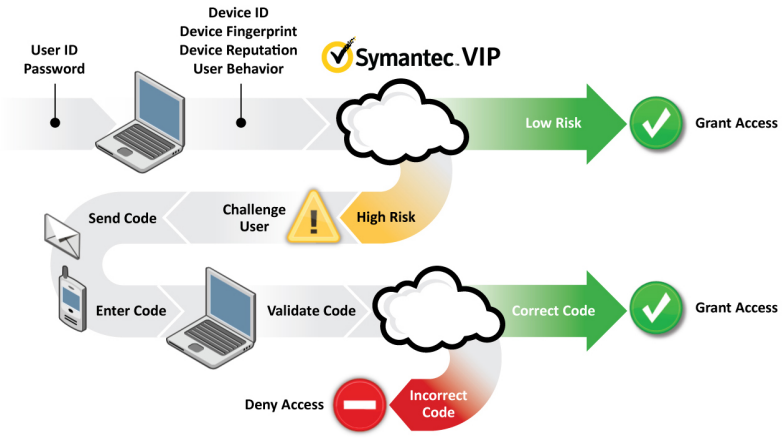

Figure 1: VIP Intelligent Authentication Process

Based on the user's device and behavior, VIP Intelligent Authentication calculates a risk score for a logon attempt and compares it against a threshold set by the administrator and either:

- **Grants access:** For a risk score below the threshold set by the administrator, VIP Intelligent Authentication immediately grants the user access to the protected application or network. Users only experience what they've always experienced: they enter their user name and password and are granted immediate access to a protected resource. This is the experience for legitimate users most of the time.
- **Challenges the user:** For a risk score above the threshold set by the administrator, VIP Intelligent Authentication prompts the user to complete an out-of-band (OOB) authentication challenge. VIP Intelligent Authentication sends a security code to the user by SMS text message, email, or a voice phone call, and the user must enter that code to complete the authentication challenge. Users that fail to complete the challenge will be denied access to the application or network.

With each successful logon, VIP Intelligent Authentication continually updates and tracks information about the user's device and behavior. This not only allows it to monitor routine and expected changes to the device (such as updates to software on the user's device), but also to account for changes in the user's behavior over time, such as logon attempts from previously unknown locations or unusual changes to the device's configuration.

System Architecture

The core of the VIP Intelligent Authentication system, shown in Figure 2, is a rules engine that computes a risk score for each logon attempt, representing the likelihood that a particular logon attempt is from a known and legitimate user.

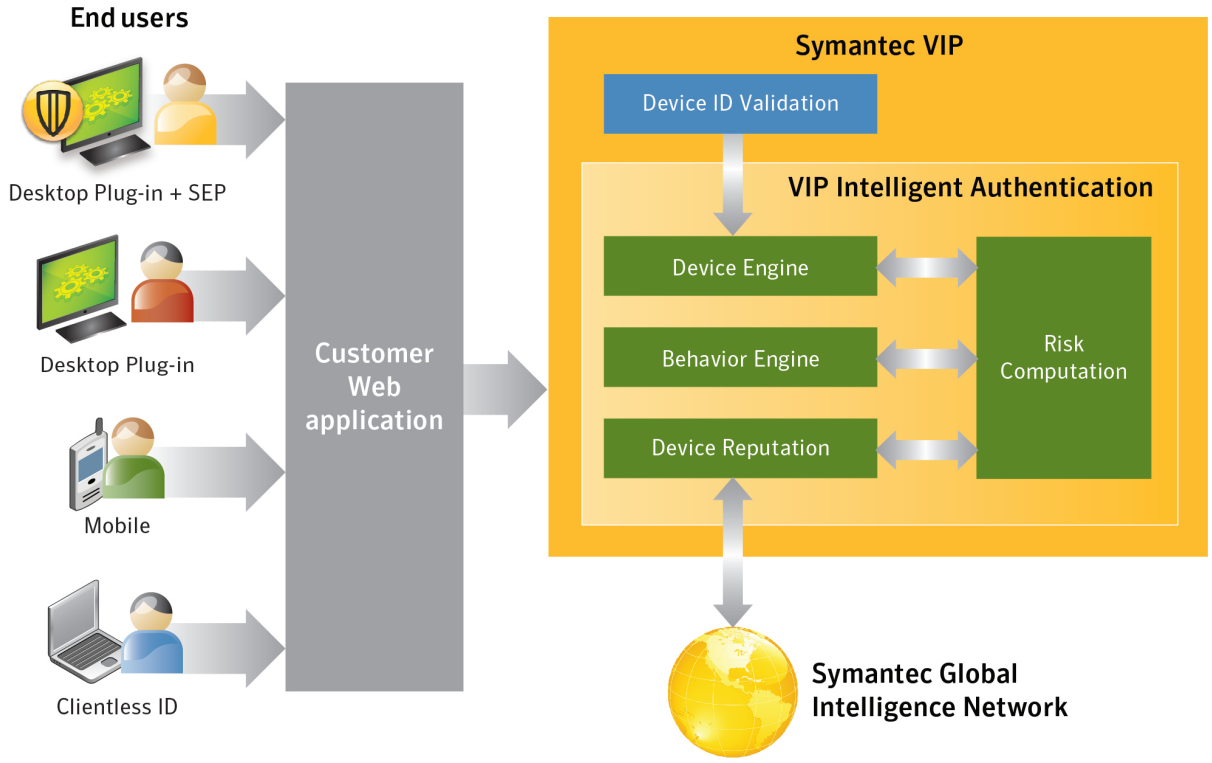

Figure 2: VIP Intelligent Authentication System Architecture

This rules engine relies on three main categories of inputs to drive the calculation of a risk score for each logon attempt:

- **The identity of the user's device:** VIP Intelligent Authentication's Device Engine uniquely identifies a device to track it over multiple logons.
- **The reputation of the device, location, and network origin:** VIP Intelligent Authentication gathers information on the device's physical and network location, as well as the presence of Norton or Symantec Endpoint Protection antivirus.
- **The behavior of the user and device:** VIP Intelligent Authentication's Behavior Engine assesses the behavior of the user and their device versus a profile gathered during prior successful logons.

Risk Assessment Process

For any logon attempt, VIP Intelligent Authentication calculates a score on the basis of these categories of inputs that represents the risk that a legitimate user is not responsible for the logon attempt. To calculate this risk score, VIP Intelligent Authentication:

1. **Gathers inputs:** Information about the user's device, geographic location, network origin, and behavior are gathered for evaluation against rules specified by VIP Intelligent Authentication.
2. **Evaluates the rules:** Each rule may combine one or more of the set of inputs to calculate a risk score for one aspect of the logon attempt.
3. **Weights each rule's output:** VIP Intelligent Authentication assigns different relative weightings to the score generated by each rule, reflecting the importance of a particular rule to the overall risk assessment. These weightings are dynamically generated, and the process of determining the weighting of a particular rule's input into the final risk score may rely on evaluating the risk scores generated by multiple rules.
4. **Computes a combined, normalized risk score:** VIP Intelligent Authentication adds together the weighted risk scores generated by each individual rule, and normalizes the result against a scale of zero to 100.

VIP Intelligent Authentication evaluates the normalized risk score generated by this process against a risk threshold specified by the administrator. Risk scores exceeding the threshold trigger an out-of-band challenge process, and require the user to enter a security code sent by VIP to the user via SMS text message, email, or phone call.

The lower the risk threshold set by the administrator, the higher the possibility of VIP Intelligent Authentication challenging a user's logon attempt; for example, setting a risk score of zero would result in the user always being challenged by VIP Intelligent Authentication. The higher the risk threshold is set, the less likely it is that the user will be challenged; for example, setting a risk threshold of 100 would result in the user almost never being challenged[1].

Rule Definitions

Known Device

The Device Engine within VIP Intelligent Authentication uniquely identifies a device, and enables the system to track a device and its user's logon behavior over multiple logons. VIP Intelligent Authentication supports both client-based and clientless mechanisms to uniquely identify and track devices, including both traditional desktop and mobile devices. Logon attempts from unknown devices will result in a higher risk score being generated by the Known Device rule.

1-The user may still be challenged if they failed to complete the authentication challenge for a prior logon, or they are using the Registered Computer functionality and failed to authenticate using the Registered Computer device certificate.

Client-based Device Identification Options

Symantec™ VIP Access Desktop

Symantec™ VIP Access Desktop is a desktop client application that provides VIP Intelligent Authentication with access to unique, hardware-based identifiers embedded in the user's device. These identifiers allow VIP Intelligent Authentication to track a user's device over multiple logons with a higher degree of confidence versus the clientless device identification option supported by VIP Intelligent Authentication.

VIP Access Desktop is not only available from Symantec as a free download, but also is pre-installed and enabled on many laptop and desktops featuring second-generation Intel® Core™ chipsets enabled with the Intel® Identity Protection Technology (IPT). Intel IPT-enabled laptops are available from a number of leading PC vendors.

Registered Computer

As an alternative to the Device Engine, VIP Intelligent Authentication can leverage the Registered Computer feature of Symantec™ VIP to identify a device using a device and user-specific digital certificate. The Registered Computer feature of Symantec VIP leverages a browser-based plugin to silently install a device certificate on the user's machine, and then use that device certificate to authenticate the device to VIP Intelligent Authentication. Unlike other solutions that leverage digital certificates, this approach is completely transparent to the user, and does not require any PKI lifecycle management.

Clientless Device Identification Options

VIP Intelligent Authentication does not require client software to reliably identify devices, and supports clientless device identification mechanisms. This not only allows VIP Intelligent Authentication to address the needs of users and organizations that wish to avoid deploying client software, but also the needs of users accessing applications through their mobile device's web browser.

To reliably identify a device without client software, VIP Intelligent Authentication leverages three key technologies:

- **Network connection analysis:** VIP Intelligent Authentication gathers information about the user's device and network connection, including details on their user agent, the content type accepted by their browser, their browser character settings, and their configured browser language.
- **JavaScript™-based device fingerprinting:** Client-side JavaScript integrated into the logon page for the organization's enterprise or web-based application gathers information about the user's device. Gathered information includes the device's browser, language, operating system, system time zone, screen resolution, and installed browser plugins. This information provides a fingerprint of the user's device that can be used to profile the device and help assess changes to the device that may indicate an elevated risk on a future logon attempt.
- **Persistent device tagging:** In addition to gathering a device fingerprint, VIP Intelligent Authentication also deposits a unique ID on the device to associate the fingerprint to a device profile stored in VIP Intelligent Authentication. This device tag consists of a server-generated unique and anonymous ID, a time stamp, and is associated with an encrypted version of the JavaScript-derived fingerprint stored in the VIP Intelligent Authentication service. Browser-based techniques are used to deposit this tamper-proof unique ID using combinations of HTML5 local storage, browser cookies, and other browser-based persistent caching techniques.

VIP Intelligent Authentication doesn't store any personal information about the end user, and instead only collects information regarding the user's operating system, IP address, browser type, network connection, geographic location (which may include city, state or country), and the presence of existing Symantec Endpoint Protection or Norton® AntiVirus software. All the information stored by VIP Intelligent Authentication is stored in an encrypted format.

Behavior Engine Check

VIP Intelligent Authentication assesses each logon attempt against a profile of the user and device behavior exhibited during prior successful logons to identify anomalous behavior. To identify anomalous behavior, VIP Intelligent Authentication:

- **Gathers information on the user and device:** VIP Intelligent Authentication examines the combination of the user's IP address, network location, geographic location, browser configuration, and operating system.
- **Evaluates the gathered information against a historical profile:** Information gathered by VIP Intelligent Authentication is analyzed versus a historical behavior map to pinpoint unexpected or behavior that doesn't conform with the profile. Unexpected behavior results in an elevated risk score.
- **Updates the behavior profile:** After a successful logon, VIP Intelligent Authentication evolves the historical behavior profile to include new observed behaviors, and to expire outdated behaviors.

Norton/Symantec Endpoint Protection Device Reputation

In cases where the Symantec VIP Access Desktop client software is installed, VIP Intelligent Authentication can also leverage an available Norton or Symantec Endpoint Protection installation to evaluate the health and trustworthiness of the device. Not only can VIP Intelligent Authentication verify that antivirus protections are in place, but also can inspect the number of infections reported by the machine, the number of known-bad files submitted by the machine, and the timestamp of last infection report submission by the machine. All of the information gathered by Norton and Symantec Endpoint Protection installations is shared with Symantec with the consent of the user.

This device reputation information provides VIP Intelligent Authentication with additional insight into the current state of the device and the likelihood that a particular device poses an increased authentication risk. Devices that are infected frequently, report numerous bad files, or have not been checked recently are an increased risk. These machines may harbor malware designed to steal authentication credentials or hijack a user's session to bypass authentication protections, and hence VIP Intelligent Authentication assigns such machines an elevated risk score as part of the risk assessment process.

Known Fraudulent IP Address

VIP Intelligent Authentication checks the IP address of the user's device against a watchlist provided by the Symantec Global Intelligence Network, a global network providing comprehensive, up-to-date information on sources of malicious Internet activity. This watchlist includes the top 100K attacking IPs, including sources associated with botnets, unallocated IPs, and known anonymous proxies. Logon attempts from known sources of malicious Internet activity will result in a higher risk score being generated by this rule.

Risky Country

VIP Intelligent Authentication performs a geolocation check on the device's IP address, and checks the device's location against a customer-specified list of restricted countries. Logon attempts from a country considered to pose additional risk will increase the risk score generated by this rule.

Difficult Travel

VIP Intelligent Authentication performs a geolocation check on the device's IP address, and compares the current location against that of the last successful logon. If the distance traveled in the time elapsed since the last successful logon is impossible or highly improbable, this rule will generate an elevated score.

Failed Previous Logon

If the user failed to complete a previous authentication challenge, this rule will generate an elevated risk score. This rule prevents an attacker from attempting to compromise an account by using several different devices, network locations, or geographic locations in the hope of finding one which matches the user's existing profile.

Risk Assessment Examples

The following scenarios are designed to illustrate how VIP Intelligent Authentication assesses risk to both enable transparent access for a legitimate user, and invoke an authentication challenge for a risky logon attempt from a potential attacker.

For these scenarios, we follow John Smith, a hypothetical enterprise user. John's organization has deployed VIP Intelligent Authentication to protect the corporate network from unauthorized access. After the initial deployment, John logs on regularly from work using his employer-provided laptop, and VIP Intelligent Authentication allows him to access the network using only his user name and password. Let's see how VIP Intelligent Authentication helps protect him under a number of different circumstances.

Scenario 1: User Logs on From Home Using Work Laptop

Work doesn't always happen at the office, and so John occasionally needs to work from his home office in the evening. To catch up on a project, John decides to logon from home using his work laptop. When he attempts to log on to the VPN, VIP Intelligent Authentication notices that the logon attempt:

- Is coming from a known device, and the device profile hasn't changed
- Is from a physical location near prior successful logons
- Is not originating from within a "risky country"
- Is not coming from an IP address known to be associated with malicious activity

For this logon attempt, the authentication experience is simple. John enters his user name and password, VIP Intelligent Authentication deems the logon to be low risk, and John is granted access to the VPN without further authentication.

Scenario 2: Under Attack from China

What John doesn't know is that his company is currently being targeted by malicious attackers located overseas. These attackers have compromised John's social networking account to steal his account password, and they're hoping that John uses that same password for his enterprise logon. If so, they plan to access to John's organization's corporate network, and steal its sensitive intellectual property for sale on the black market. It's just one of many lines of business for these attackers, along with sending spam through a botnet they control, and using malware to steal personal information.

Shortly after John logs off for the evening, a remote hacker in China attempts to log into John's account using the stolen password. When the hacker attempts to logon to the VPN, VIP Intelligent Authentication notices that the logon attempt:

- Is coming from an unknown device
- Is from a physical location situated an improbable distance from John's prior successful logon
- Is coming from an IP address known to be associated with malicious activity

These inputs elevate the risk score calculated by VIP Intelligent Authentication to the point that it exceeds the risk threshold set by the administrator. As a result, VIP Intelligent Authentication issues an authentication challenge and sends a security code to either John's phone or email address. As the attacker is unable to receive the security code sent to John's phone or email, they are unable to complete the challenge, and John's company easily deflects the attempt to compromise the network.

Scenario 3: Under Attack from Cuba

With a project deadline looming, John spends another evening working late from home. Several hours after John logs out and heads for bed, the attacker's associates make another attempt to compromise the corporate network using the stolen password. When the hackers, this time located in Cuba, attempt to logon to the VPN, VIP Intelligent Authentication notices that the logon attempt:

- Is coming from an unknown device
- Is from a physical location located a plausible distance from John's last successful logon
- Is from a physical location that John's organization has designated as source of elevated risk

When John's organization installed VIP Intelligent Authentication, they identified a list of countries where they operate and configured VIP Intelligent Authentication to treat logons from other countries as suspicious. Although the attackers have allowed enough time to elapse to avoid triggering the "difficult travel" rule, John's company has designated Cuba as a potential source of risky logons. These inputs elevate the risk score calculated by VIP Intelligent Authentication to the point that it exceeds the risk threshold set by the administrator. As a result, VIP Intelligent Authentication issues an authentication challenge and sends a security code to either John's phone or email address. Again, the attackers are unable to complete the authentication process, and are deflected from gaining access to the network.

Scenario 4: User Travels to India with Work Laptop

John's project has been approved, and so he's off to the office in India to manage the local team assigned to the project. Exhausted from the flight, John attempts to log into the VPN to check his email before heading to bed. When John attempts to logon to the VPN, VIP Intelligent Authentication notices that the logon attempt:

- Is coming from a known device
- Is from a physical location John hasn't logged in from before
- Is from a physical location located a plausible distance from John's last successful logon
- Is not originating from within a "risky country"
- Is not coming from an IP address known to be associated with malicious activity

When John attempts to logon from that new location, the Behavior Engine will recognize that this new behavior doesn't correlate with past exhibited behavior. As a result, the Behavior Engine will increase the risk score output by the Rules Engine. Even though the device ID and device profile matches John's previous logons, the new and unexpected location may result in John being challenged, depending on the risk threshold set by the administrator.

In this case, John's new location is enough to put him over the risk threshold set by the VIP Intelligent Authentication administrator. He is challenged by VIP Intelligent Authentication, and completes the challenge by entering the security code sent to his phone via SMS. After successfully responding to the challenge, John is granted access to the corporate network. VIP Intelligent Authentication updates its profile of John to account for his new location.

The next morning, John wakes up and attempts to log into the VPN again. This time, VIP Intelligent Authentication recognizes that John is logging in from a known location, and grants him immediate access without further prompting.

Scenario 5: Hack Attack from Within the Hotel

Poor John – it turns out his hotel in India is a hotbed of malicious activity and the concierge is part of an international ring of online organized crime. Yet again, John is targeted, this time when the concierge shoulder-surfs John's password as he logs into the VPN while sitting in the hotel lobby one evening. After John heads to his room to go to bed, the concierge attempts to logon to John's VPN. VIP Intelligent Authentication notices that the logon attempt:

- Is coming from an unknown device
- Is coming from a device with a significantly different configuration from John's known device
- Is from a known physical and network location

Attempting to logon from a new location isn't the only indicator of suspicious behavior considered by VIP Intelligent Authentication. Another indicator is the state of the user's device. Over time, a user's device configuration may change; for example, a user may install new plugins in their web browser, or update their browser to the latest version. These are expected behaviors. On the other hand, a user is unlikely to downgrade the version of software they're using.

In this case, the attacker is using older web browser version than John's device, elevating the risk score calculated by VIP Intelligent Authentication to the point that it exceeds the risk threshold set by the administrator. As a result, VIP Intelligent Authentication issues an authentication challenge and sends a security code to either John's phone or email address. Again, the attackers are unable to complete the authentication process, and are deflected from gaining access to the network.

Scenario 6: Upgrading Device Configuration

While John is in India, his web browser's manufacturer issues a critical patch for a newly discovered security vulnerability. While on the VPN, John's IT organization pushes down an update to his machine to patch the issue, and update his web browser to the latest version. Later in the day, John attempts to logon to the VPN and VIP Intelligent Authentication notices that the logon attempt:

- Is coming from an known device
- Is coming from a device with a different configuration from John's known device
- Is from a known physical and network location

Of course, by the same token, we don't want to intervene every time the user updates a minor version on their browser. Hence, VIP Intelligent Authentication is smart enough to differentiate between expected and unexpected changes. In this case, VIP Intelligent Authentication recognizes that the differences in the web browser version represent a minor upgrade, a change that by itself won't be significant enough to trigger secondary authentication, unless the risk threshold is set extremely low.

In this case, the risk score doesn't exceed the threshold set by the administrator, and John is granted access to the VPN without further prompting. VIP Intelligent Authentication updates its profile of John to reflect his new device configuration for evaluating future logon attempts.

Deployment Scenarios

VIP Intelligent Authentication can be integrated with any web-based application or enterprise applications, such as SSL VPNs, webmail, single sign-on gateways, and web-based collaboration tools that support configuration of the application's HTML-based logon page.

Integrating with Enterprise Applications

Integration Components

VIP Intelligent Authentication integrates with any enterprise web-based application that permits the administrator to customize the application's HTML logon page to include arbitrary HTML and JavaScript.

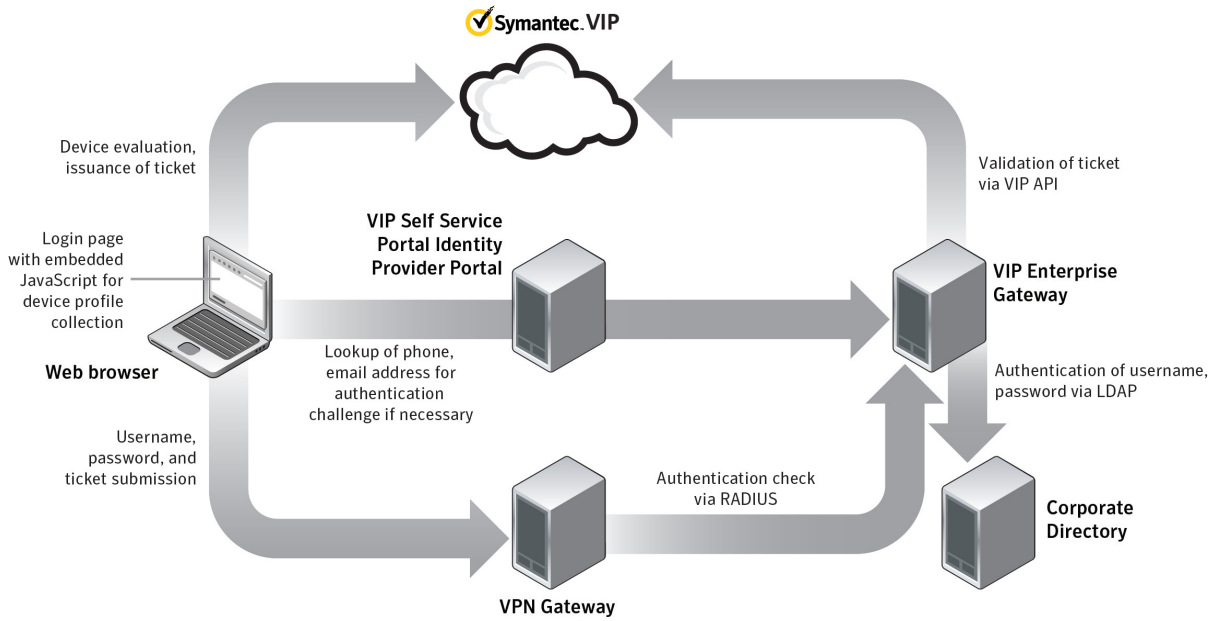

Figure 3: Enterprise Application Deployment of VIP Intelligent Authentication

VIP JavaScript Library

To enable VIP Intelligent Authentication to gather device information, the organization will need to incorporate the VIP JavaScript library and method calls into the HTML for their application's logon page. This JavaScript library and code allow VIP Intelligent Authentication to gather device information, as well as read the persistent device tag to identify the device.

Symantec™ VIP Enterprise Gateway

Symantec™ VIP Enterprise Gateway acts as a bridge between the organization's application and Symantec VIP's cloud-based infrastructure. Once VIP Intelligent Authentication determines that a logon attempt is not risky, it will generate and pass a ticket through the logon page's embedded JavaScript. The organization's application will authenticate this ticket by passing it to VIP Enterprise Gateway via RADIUS, which will authenticate the ticket against the Symantec VIP service. For those enterprise applications that don't support RADIUS natively, Symantec VIP provides plugins for a wide variety application plugins augment to enable such applications to connect to the VIP Enterprise Gateway.

VIP Self Service Portal Identity Provider Proxy

The VIP Self Service Portal Identity Provider Proxy provides VIP Intelligent Authentication with a mechanism to determine the phone number or email address to be used for out-of-band authentication challenges. The goal of this proxy is to provide the VIP JavaScript library with the ability to securely obtain this information from the organization's corporate directory directly at runtime.

Authentication Process

For a user logging on from a known device and exhibiting expected behavior, the authentication process is simple – using their web browser, the user navigates to the logon page of their enterprise application, enters their user name and password, and clicks "submit" as per usual (see Figure 4).

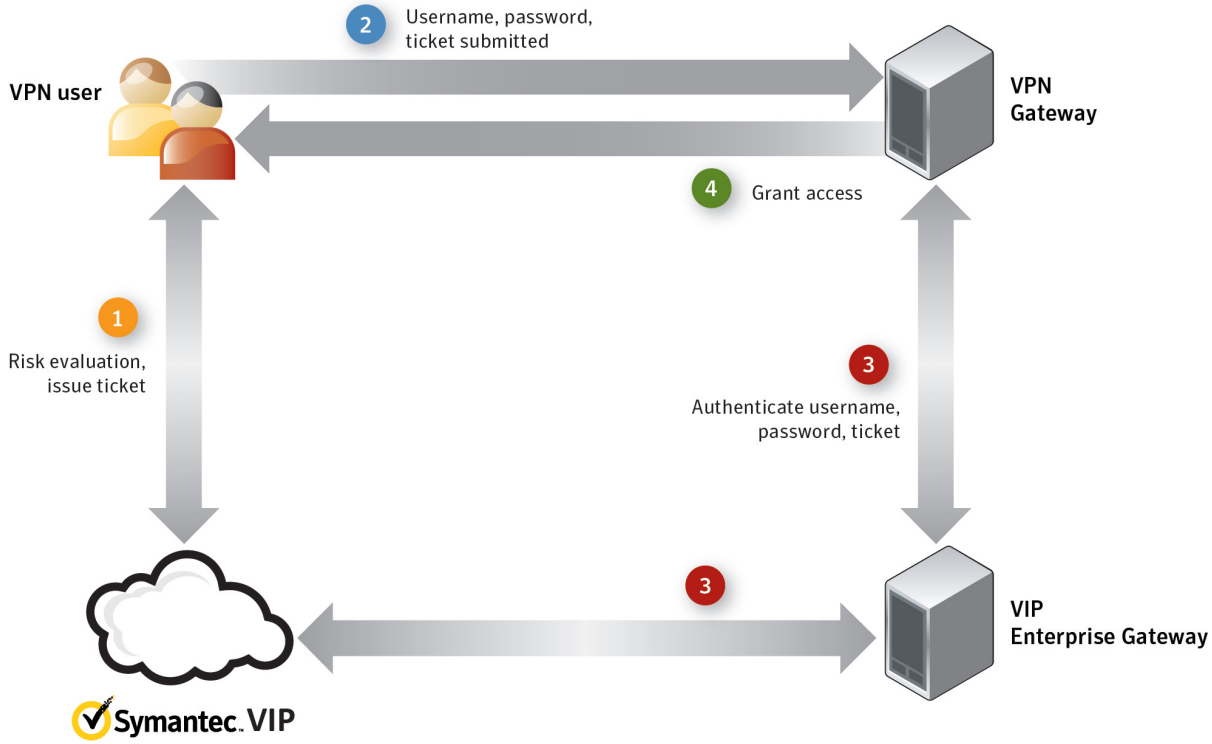

Figure 4: Enterprise Application Deployment, Authentication Process for Low Risk Logon

After the user submits their user name and password:

1. JavaScript embedded by the administrator into the enterprise application's logon page intercepts the form submission, and sends a request to Symantec VIP to perform risk analysis. If the device is known, based on the device ID or the device parameters, and the behavior is expected (based on prior logons, IP address/geographic location), then the logon is judged to be low risk. VIP issues a ticket back to the embedded JavaScript.
2. The browser now automatically submits the user name and the password (combined with the ticket returned from VIP) through the enterprise application logon form.

3. The enterprise application will authenticate the user by passing the user name and password and ticket to the VIP Enterprise Gateway via RADIUS. The VIP Enterprise Gateway will extract the ticket, authenticate the user name and password against the corporate directory via LDAP, and then authenticate the ticket using Symantec VIP. This is exactly the same as if the user had a OTP generator token or mobile credential, and used it to authenticate to the enterprise application. VIP will validate the ticket is correct, and signal if access should be granted to the user.
4. With the user successfully authenticated, they are granted access to the enterprise application.

For a logon attempt that is deemed too risky, possibly due to an unknown device or unexpected behavior, the authentication process involves the extra step of performing an out-of-band authentication of the user (see Figure 5).

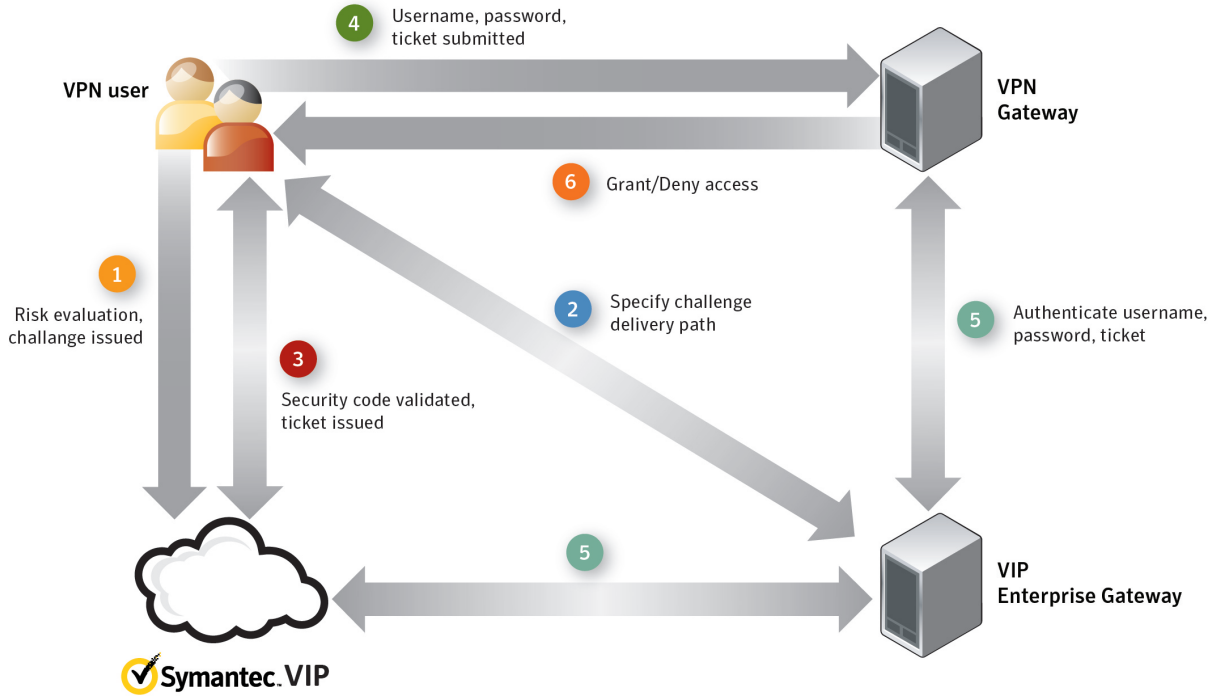

Figure 5: Enterprise Application Deployment, Authentication Process for High Risk Logon

In this case, the user navigates their web browser to the logon page of their enterprise application, enters their user name and password, and clicks “submit” as per usual. This kicks off an out-of-band authentication process:

1. JavaScript embedded by the administrator into the enterprise application’s logon page intercepts the submission, and instead sends a request to VIP containing details on the device for inspection. If the device is unknown, based on the device ID or the device parameters, or the behavior deviates from expected norms (based on prior logons, IP address/geographic location, or changes to the device configuration), then the logon is judged to be risky. VIP triggers an authentication challenge via the embedded JavaScript. The user is prompted to specify how they want to receive the security code required to respond to the out-of-band authentication challenge.
2. The user can choose to receive the security code by SMS text message, email, or a voice phone call; the details on where to contact a user for each of these options is configured by the administrator. A security code is sent to the user via that channel, and the user enters that security code into the prompt.
3. When the user submits the security code, the embedded JavaScript send the code to VIP, and VIP validates the security code. If it’s correct, VIP issues a ticket and returns it to the embedded JavaScript.

4. The embedded JavaScript silently submits the user name and the password (combined with the ticket returned from VIP) through the enterprise application's logon form. The enterprise application will authenticate the user by passing the user name and combined password/ticket to the VIP Enterprise Gateway via RADIUS. The VIP Enterprise Gateway will extract the ticket, authenticate the user name and password against the corporate directory via LDAP, and then authenticate the ticket against the VIP service. VIP will validate the ticket is correct, and signal if access should be granted to the user.With the user successfully authenticated, they are granted access to the enterprise application.

Integrating with Custom Web-Based Applications

VIP Intelligent Authentication can also be deployed to protect custom web-based applications in a similar fashion.

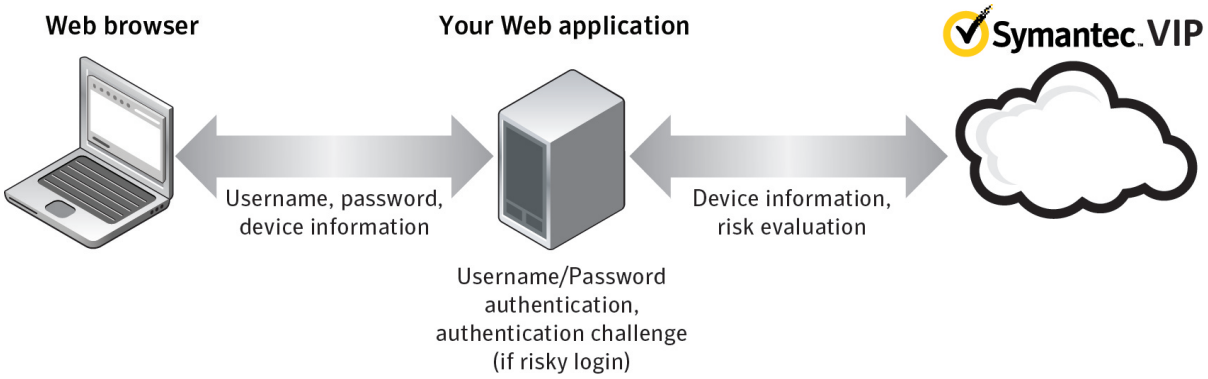

Figure 6: Web-based Application Deployment of VIP Intelligent Authentication

Key Differences versus Enterprise Application Integration

The integration of VIP Intelligent Authentication into a web-based application differs from a VPN integration in four key ways:

- **No VIP Enterprise Gateway:** The application will integrate directly with Symantec VIP using the VIP Intelligent Authentication APIs, eliminating the need to deploy the VIP Enterprise Gateway. This also means that the application is responsible for authenticating the first factor of authentication (i.e. the user name and password).
- **Requires programmamming resources to perform integration:** The application will be responsible for taking information gathered by the VIP JavaScript and interacting with Symantec VIP via the VIP Intelligent Authentication APIs to assess if a particular logon is risky. In addition, the application will also need to update VIP Intelligent Authentication with the results of the authentication challenge to allow VIP Intelligent Authentication to account for new behavior for future risk assessments.
- **Web application controls the challenge flow:** Unlike the enterprise application case, the application is solely responsible for how it implements the authentication challenge process. This provides organizations with the freedom to use existing information, such as pre-existing secret question/answers to implement their own authentication challenge process. Alternatively, the application may choose to use the VIP API to leverage one-time-password, SMS OTP, or voice-enabled OTP to implement a similar challenge to that provided in the enterprise application deployment.
- **No VIP Self Service Portal Identity Provider Proxy:** As the organization's web application is responsible for determining how to implement an authentication challenge, the VIP Self Service Portal Identity Provider Proxy is not required. It is the responsibility of the application to store and retrieve data used to perform the authentication challenge.

Authentication Process

For a user logging in from a known device and exhibiting expected behavior, the authentication process is simple - the user goes to the logon page of the web-based application, enters their user name and password, and clicks “submit” as per usual (see Figure 7).

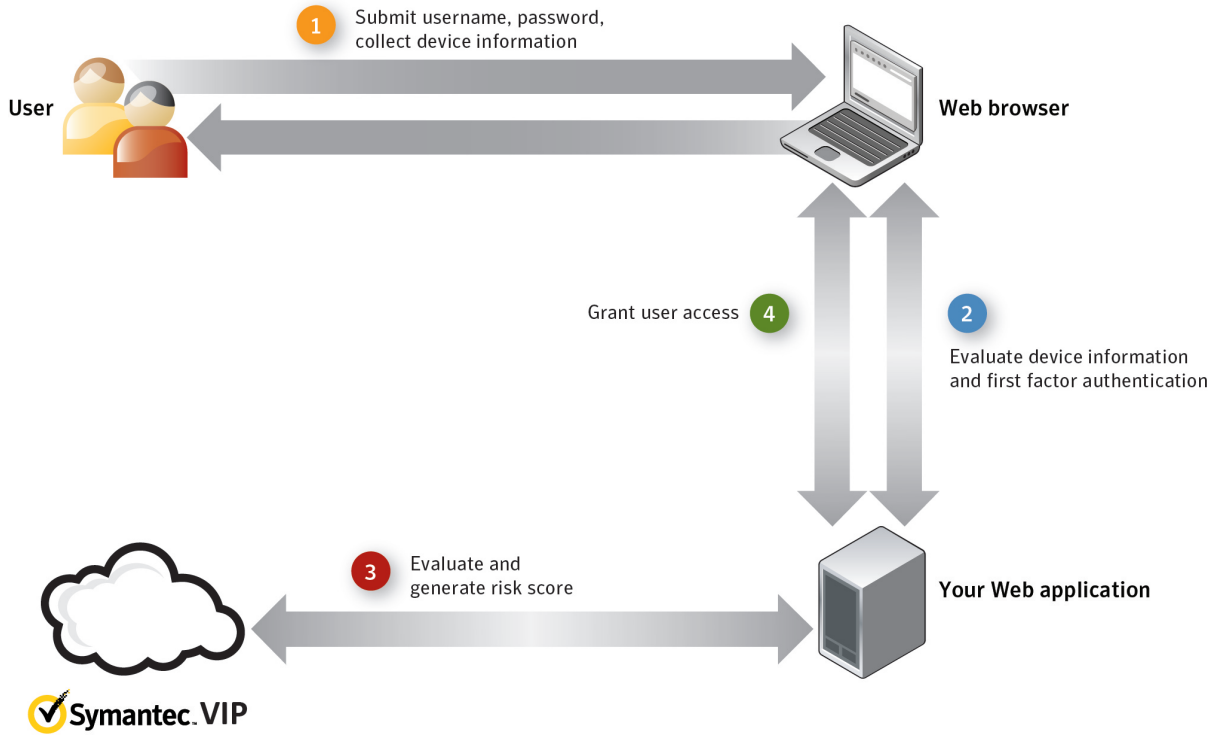

Figure 7: Custom Web-Based Application Deployment, Authentication Process for Low Risk Logon

After the user submits their user name and password:

1. JavaScript embedded by the administrator into the application’s logon page will collect information on the device for inspection. This device information, along with the user name and password, is submitted to the application.
2. The application validates the user name and password entered by the user. If these credentials validate, then the application passes the device information collected by the JavaScript to VIP using the VIP Intelligent Authentication API to determine risky represented by the logon attempt.
3. VIP Intelligent Authentication assesses the device and the logon behavior reflected in the information passed to it by the application, and generates a risk score. This risk score, along with information on the rules triggered by the logon attempt and the current risk threshold set by the administrator, will be passed back to the application.
4. In this scenario, the device is known and the behavior is expected (based on prior logons, IP address/geographic location), so the logon is judged to be low risk. The application evaluates the risk score and threshold returned by VIP Intelligent Authentication and, realizing that the risk score is less than the threshold, grants the user access to the protected application functionality.

For a logon attempt that is deemed too risky, possibly due to an unknown device or unexpected behavior, the authentication process involves the application performing supplemental authentication of the user (see Figure 8).

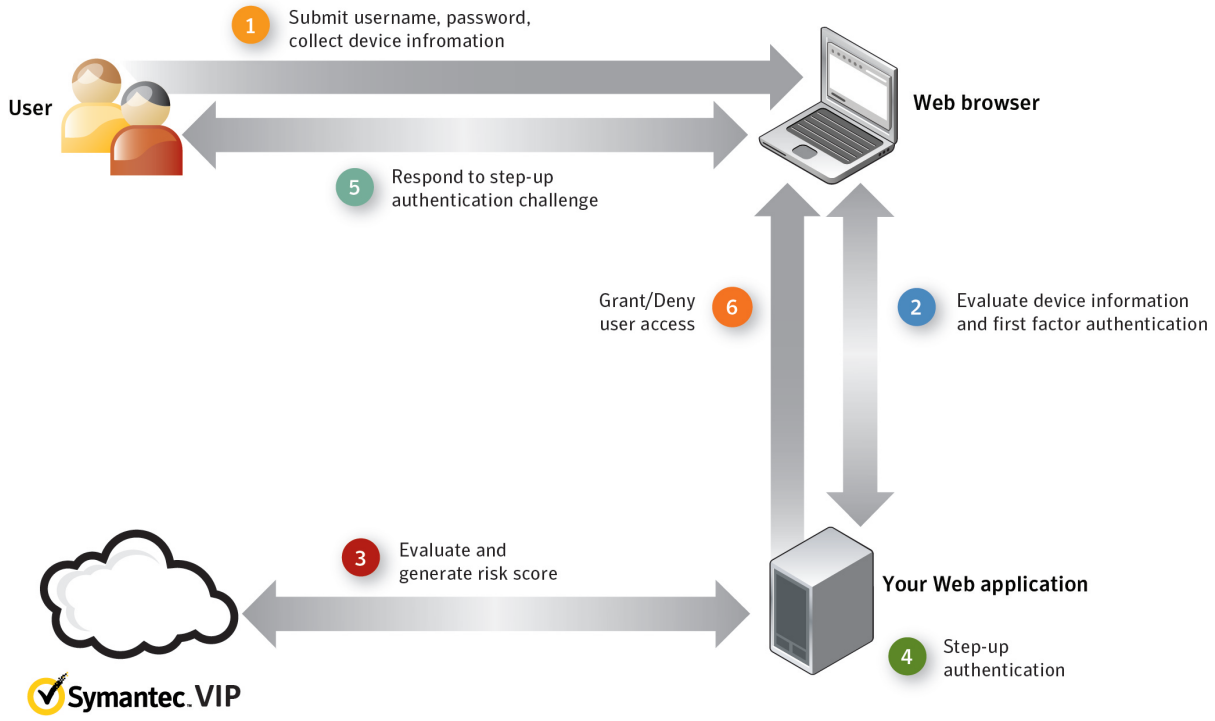

Figure 8: Custom Web-Based Application Deployment, Authentication Process for High Risk Logon

In this case, the user goes to the logon page of the application, enters their user name and password, and clicks "submit" as per usual. This kicks off a supplemental authentication process:

1. JavaScript embedded by the administrator into the application's logon page will collect information on the device for inspection. This device information, along with the user name and password, is submitted to the application.
2. The application validates the user name and password entered by the user. If these credentials validate, then the application passes the device information collected by the JavaScript to VIP using the VIP Intelligent Authentication API to determine risky represented by the logon attempt.
3. VIP Intelligent Authentication assesses the device and the logon behavior reflected in the information passed to it by the application, and generates a risk score. This risk score, along with information on the rules triggered by the logon attempt and the current risk threshold set by the administrator, will be passed back to the application.
4. In this scenario, the logon attempt is deemed to be risky; the application evaluates the risk score and threshold returned by VIP Intelligent Authentication and, realizing that the risk score is greater than the threshold, prompts the user to respond to an authentication challenge. Unlike the enterprise application deployment, in the customer application scenario it is the application's responsibility to implement this challenge mechanism.
5. The user responds to the authentication challenge, and the application determines if the user completed the authentication challenge successfully or not. The application notifies VIP Intelligent Authentication the result of the authentication challenge, allowing VIP Intelligent Authentication to learn new behavior.
6. If the user completed the authentication challenge, the application grants the user to protected application functionality; otherwise, the application can prompt the user to complete another challenge, or deny them access to protected application functionality.

For More Information

For more information on Symantec Validation and ID Protection, the components of the solution, and the process for integrating VIP Intelligent Authentication, see the following product documentation:

- Symantec™ VIP Enterprise Authentication Deployment Guide
- Symantec™ VIP Enterprise Gateway Installation and Configuration Guide
- Symantec™ VIP Intelligent Authentication Enterprise Integration Guide
- Symantec™ VIP Intelligent Authentication Member Site Integration Guide

Each of these documents is available for download from within VIP Manager (the web-based console for administering your Symantec™ VIP account), or on request from your Symantec sales representative.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.

3/2012 21225166