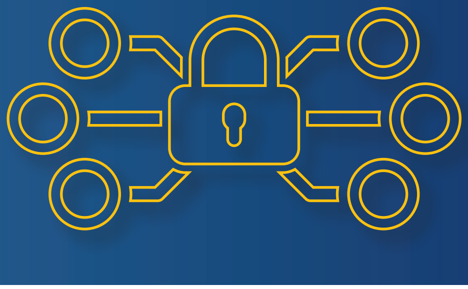
CUSTOMERONE

Symantec

VIP Access Manager–Our Key to Cloud Applications



Like most of you, Symantec has embraced the cloud. Our thousands of employees and contractors leverage some three dozen cloud applications in their daily work, from Anaqua for intellectual asset management to Workday for human resources. Symantec people live and work around the world, and many of us don't have conventional offices, so cloud applications help to empower everyone to work anywhere and anytime, using virtually any device.

Cloud applications enable Symantec to focus IT resources on business needs rather than on technology requirements. IT personnel can roll out new cloud-based services quickly, while cloud application providers build and manage infrastructure, keep software up to date, and respond to growing or shrinking user populations.

Because security is always top-of-mind at Symantec, cloud applications and Single Sign-On (SSO) technology go hand-in-hand here. SSO addresses the password sprawl that cloud applications can cause: Without SSO, users have to create a login and password for each application and more passwords means more chances to lose, forget, or recycle them.

With SSO, access to many different enterprise cloud applications is centrally controlled by Symantec. That's vital because some cloud applications hold business-critical information–customer and personnel data, financial records, intellectual property, planning documents and more–that requires tighter security controls to be in place. SSO is a true win-win technology: IT gets more control, and users get more convenience and productivity.

This paper describes Symantec's SSO journey and the lessons we've learned–many of which have helped to improve Symantec's SSO offering to our customers and ourselves. If you'd like to learn more about Symantec SSO or our overall security strategy, consider visiting one of our two Executive Briefing Centers. We'll walk you through our own blueprint for corporate security, and help you understand how to adapt our model to control access to cloud applications and keep your confidential information safe.

VIP Access Manager–Our Key to Cloud Applications is written to inform CIOs, CTOs, CISOs, and other senior managers about how cloud applications and Single Sign-On go hand-in-hand at Symantec. Leveraging Symantec VIP Access Manager, we've relieved people of the chore of maintaining multiple passwords, helped IT secure cloud application access based on user identities, and established a foundation for even better, more secure access. Another benefit: As the first customer to use VIP Access Manager, our experiences improved the product and related hosting services for everyone involved.

SSO From Scratch

Symantec's first SSO product, called O_3, was deployed for our employees in February 2012. O_3 worked as advertised: It let employees use a single login to access several cloud applications. But it had several shortcomings:

- An awkward user interface;
- A meager selection of cloud applications; and
- Limited mobile access.

So Symantec engineering set out to develop a new SSO solution from the ground up–one that would integrate SSO with strong authentication and Managed Public Key Infrastructure encryption, and eventually with Symantec Data Loss Prevention. Symantec IT volunteered to be the first customer to deploy the new product, called Symantec VIP Access Manager, when it became ready for general availability.

Hosting the Gateway

Symantec IT staffers began planning to implement the new VIP Access Manager in October 2014. One early decision was whether to host the VIP Access Manager gateway (the workhorse SSO engine) in our own IT data center, or let Symantec's Cloud Platform Engineering (CPE) team host it. (Both options are also available to VIP Access Manager customers.) CPE operates separately from Symantec IT, so we would be using our own colleagues like an outside hosting vendor, with service level agreements and other obligations we expect from every third party we work with.

"The gateway servers are the big animals that do all the work," explains Steve Broadbent, VIP Access Manager service owner in Symantec IT. "It's big-footprint, hard-to-manage infrastructure." Given Symantec IT's preference to leverage cloud solutions wherever possible, and its desire to focus IT resources on business needs rather than technology details, the team chose to have CPE host the gateway. Symantec IT would only need to host a lightweight ID Bridge server on-premises.

Letting CPE host the gateway offered two benefits: It relieved Symantec IT of the burden of running another server, and it gave CPE an opportunity to refine its service offering. "Having Symantec IT as our first customer gave us good experience creating the base setup," says Sean Xie, an infrastructure architect in CPE. "The first setup of a service always takes more time, and even though we prepared pretty well, some unexpected things happened." For example, the gateway administration console didn't perform as hoped, and session "stickiness" was a problem for some users.

Sean and infrastructure specialist Ari Nagarajan fine-tuned the service based on what they learned, and also suggested several improvements to the VIP Access Manager product. "We learned a lot from that first deployment, and the base setup for the gateway has been pretty stable after that," Sean says. CPE now hosts gateways for several other VIP Access Manager customers.

Configuring Applications, Implementing Policies

Because the cloud apps Symantec uses leverage the Security Assertion Markup Language standard, integrating them with VIP Access Manager is technically straightforward. Indeed, only two applications posed configuration problems and "Neither of those were showstoppers," according to application architect Arun Kumar.

Working with vendors and application owners to align timelines and exchange information was another story. "Configurations can be done in hours, but coordination is where the time goes," Arun explains. This sometimes required weeks of back-and forth communication; quality assurance, user acceptance testing and user education also consumed cycles.

Implementing and tuning application-specific policies also required considerable time–in part, because of VIP Access Manager's flexibility. We decided, for example, that the VIP Access Manager portal should only display applications appropriate for a user's role, geography, and other factors. This improves usability, because (for example) employees in North America don't see payroll applications for employees in Asia-Pacific, but requires configuration for each application to leverage information in Microsoft Active Directory, Symantec's identity provider.

We also decided that applications containing personnel or customer information or intellectual property would require step-up authentication. Step-up authentication is easiest understood using an example of how we set it up: A user on the public Internet can log into Symantec's instance of VIP Access Manager and immediately connect to Giving Station, our corporate responsibility application. However, to enter Workday or Salesforce, that person must also authenticate using Symantec's Validation and ID Protection (VIP) service.

Step-up authentication didn't require additional infrastructure investment, because VIP Access Manager at Symantec leverages the same VIP service as our virtual private network and source code protection program. (See the CustomerONE story, "Source Code Security the Symantec Way," to learn more about how Symantec protects its most valuable intellectual property.) Indeed, tight integration with VIP is a hallmark of VIP Access Manager–not simply a feature that enables two-factor authentication–blending convenience and security without sacrificing either.

Testing and Rollout

After months of configuration and internal testing, Symantec IT enlisted users for broader testing. Workday, which required step-up authentication, was the first application tested. After a successful test period, VIP Access Manager was launched to the company in March 2015, with VIP integration turned on soon afterward.

A total of 19 applications–16 existing applications and three new ones–were available in the VIP Access Manager portal on launch day. But there was a secret behind the screen: While users saw many applications in the new portal, many of them were still being authenticated using O_3. This was intentional; the IT team wanted to launch the portal, but couldn't make all of the company's cloud applications available at once, so it collaborated with the product team to make both O_3 and VIP Access Manager operate simultaneously while presenting all applications in the VIP Access Manager portal.

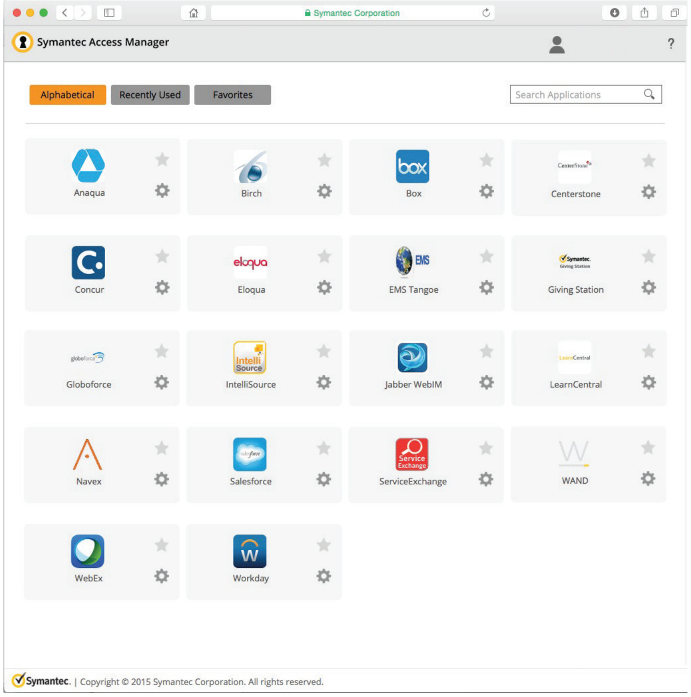
Here's the lesson for you: Changing from one SSO solution to another does not have to happen all at once. Indeed, it may be worthwhile to test a new SSO solution on lower-priority cloud applications first, then move up to the more business-critical applications when you're satisfied that everything is working properly.

"There are lots of challenges in coordinating and making all applications available on one day," explains Chandra Chezhian, the program manager who coordinated the VIP Access Manager project. "This gave us some room to work." With the seamless login feature in place, the rest of the applications were moved to VIP Access Manager over time, but the experience for the user did not change.

In total, three software engineers invested an estimated 2,000 hours over eight months to architect, configure, integrate, test, and ultimately deploy VIP Access Manager with our full set of cloud applications.

Improvements for Users and IT

Users liked VIP Access Manager's web user interface (shown at right), which included large, clear icons for applications and the ability to search for and sort applications and mark regularly used selections. This usability, personalization and customization hadn't been available with O_3. Mobile use blossomed, because VIP Access Manager authenticated many cloud vendors' mobile applications.



The Symantec VIP Access Manager portal, showing some of the cloud applications available to one user. The user can click the star next to an application to mark it as a favorite, and set preferences for each application by clicking its gear icon.

Application-based workflows also performed more smoothly. For example, Concur (Symantec's expense reporting application) sends out approval notification emails containing links; users who are already authenticated through VIP Access Manager can click those links to go straight to specific expense reports referenced in email. Users who aren't yet authenticated are sent to VIP Access Manager, then automatically forwarded to their expense reports upon signing in. Users don't need to authenticate before clicking a link, or worry that they'll be sent to the wrong place (such as an application's homepage) once they've authenticated.

This happens automatically because VIP Access Manager handles both service provider–initiated workflows and identity provider–initiated workflows. "That kind of functionality was missing in O_3, but is available out of the box with VIP Access Manager," Arun says.

Anecdotally, the IT team that owns VIP Access Manager believes that integrating new cloud applications is faster and easier with the new product. However, as noted earlier, the lion's share of time spent in application integration often goes toward coordinating activities, not technical tasks. Software can't make a vendor return your call or email.

While VIP Access Manager is a powerful tool, it is just one part of the comprehensive access solution we use at Symantec. Two examples: On-premises software (such as Oracle) continues to use its own authentication, and CyberArk is used for privileged account management.

Looking Ahead

Symantec IT's SSO strategy got a major endorsement with the sale of Veritas in October 2015. Given a clean slate to work with, Veritas IT chose to duplicate Symantec's SSO plan: "When we split with Veritas, they set up a separate instance of this exact same paradigm," Steve says. "Veritas has a clone of our environment, using Symantec as its SSO vendor."

The next evolution of SSO within Symantec will leverage Integrated Windows Authentication (IWA). Under IWA, the user needs only to log into his or her computer to gain SSO access to cloud applications. Steve will implement this capability, which requires another virtual server, when VIP Access Manager migrates to Symantec's Next Generation Secure Data Center.

And as Symantec deploys Microsoft Office 365, simple and secure access to cloud applications will become even more central to user productivity. VIP Access Manager can authenticate users for Office 365, paving the way for Symantec people to use these key cloud applications.

Learn More with an Executive Briefing

This brief was intended to give you a broad look at how we implemented single sign-on at Symantec. Your Symantec representative can show you how to adapt our blueprint to make it easier for your own users to use cloud-based applications.

For a more in-depth experience, visit our Executive Briefing Centers at our U.S. headquarters in Mountain View, California, or in Reading, U.K.

SYMANTEC SOLUTIONS AND PRODUCTS IN THIS PAPER

VIP Access Manager: Enables an access control platform for cloud applications that integrates Single Sign-On (SSO) with strong authentication, access control and user management

Validation and ID Protection: VIP delivers user-friendly authentication to protect networks, applications, and data through standards-based two-factor and risk-based token-less authentication

Managed PKI Service: MPKI ensures secure communications for users and connected devices, using a trusted, cloud-based infrastructure that monitors, manages, and scales encryption globally

Data Loss Prevention: DLP discovers where data is stored across your cloud, mobile, and on-premises environments; monitors how it's being used on and off your corporate network; and protects it from being leaked or stolen

Executive briefings provide you an exclusive opportunity to learn how Symantec solutions can protect your business and network environments. We'll customize the briefing to meet your specific goals, and we'll also give you a sneak peek at new technologies and challenges on the horizon.

Contact Symantec today.

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

Symantec's CustomerONE team can facilitate discussions between you and our IT security practitioners to help you address your security questions and concerns. Please contact us directly or through your Symantec sales team.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.