WHITE PAPER:
TWO-FACTOR AUTHENTICATION: A TCO VIEWPOINT

A Total Cost of Ownership Viewpoint for 1000 Users

Two-Factor Authentication

Who should read this paper

This whitepaper is directed at IT, Security, and Compliance workers who are responsible for recommending or evaluating security products; or running and managing two-factor authentication infrastructure.

Symantec™ Validation and ID Protection (VIP) Service provides you with an easier, more cost-effective way to protect your entire network and address topics such as expanding support to cloud applications, passwordless authentication, and usability and manageability issues. In fact, VIP Service reduces your total cost of ownership by 55 percent compared to RSA SecurID® - without getting locked into a proprietary system. Learn how strong authentication is being deployed today and understand the cost categories, including the hidden costs that must be considered.

Symantec

Content

Introduction

By the end of 2020 more than 72 percent of U.S. employees—and more than 1 billion workers worldwide—will routinely work outside of a traditional office environment.[1] Increasing numbers of employees will need to remotely access the corporate network. Even people working from the office will be using the Internet to do their jobs as organizations continue to adopt the software-as-a-service (SaaS) application delivery model.

Meanwhile, with the growing prominence of extranets and cross-organizational collaboration tools, non-employees—including customers, suppliers, and business partners—increasingly need access to corporate applications and data, sometimes through social media technologies. Extended networks can help organizations cut operational costs through greater process efficiencies; promote cross-organizational innovation; and eliminate the need to build costly and time-consuming point-to-point connections. Although there are tremendous benefits to this expansion of the corporate network, the need for strong security has never been more apparent.

Enterprises have traditionally used two-factor authentication (2FA) to secure access to corporate resources remotely. Due to their relative ease of use and familiar end-user paradigm, One-Time Password (OTP)-based solutions are the most widely used 2FA solution deployed by enterprises today. As 2FA vendors and enterprise IT professionals gain experience deploying these solutions, the true cost or total cost of ownership (TCO) becomes apparent and can be estimated quite accurately across different authentication solutions.

This white paper will focus specifically on various OTP-based authentication solutions and will help IT professionals identify the key components that contribute to their TCO. Furthermore, this white paper will draw a comparison between Symantec® Validation and ID Protection (VIP) Service and the RSA SecurID® strong authentication solution from a TCO perspective.

Defining TCO

TCO accounts for all of the costs associated with planning, procuring, deploying, and owning a two-factor authentication solution—not just the solution cost paid to a particular vendor. It should include:

One-time costs:

- Authentication software license fees for perpetual licenses
- Deployment costs should be considered, including both internal and outsourced resources to plan, install, and configure the solution, as well as costs to set up and train end users
- Up-front costs for an infrastructure that must be scalable, highly reliable, and protected in a secure facility (hardware costs)
- One-time costs for devices (such as tokens or mobile phone applications) that generate the OTP, as well as any token distribution costs
- Integration costs

Looking beyond TCO:

Simple, convenient strong authentication

- Consider token-less strong authentication instead of deploying tokens to partners
- The token-less alternative supports BYOD or unmanaged devices
- For the ultimate in convenience look to passwordless authentication as an option

Support for cloud applications

- Leverage your existing investment in strong authentication for web-based 3rd party applications (i.e. Salesforce) instead of relying solely on partner integrations
- Investigate solutions that provide Single Sign-On (SSO) that have tight integration with strong authentication solutions to easily extend your strong authentication to all cloud-based apps

Simplify administration

- Demand automated provisioning of tokens for users
- Mandate self-service alternatives

Maximum security and future-proof

- Require maximum security, annual 3rd party audits, and separation of factors to insure against the risk of a breach that obtains both factors of authentication
- Insist on timely delivery of new capabilities to stay ahead of emerging threats
- Utilize market-leading products and services (i.e. Symantec™ Global Intelligence Network, Norton™, or threat protection solutions) to provide advance warning of possible threats and more precise risk analysis

[1] IDC U.S Mobile Worker Forecast 2015-2020, May 2015

Recurring service costs:

- Authentication software license fees for annual subscriptions
- Annual software maintenance fees incurred for perpetually licensed products
- On-going administration costs include costs to maintain the OTP deployment, as well as support costs for end-users' help desk personnel
- Hardware token and device replacement costs (shelf decay is a factor that should also be considered, although it is not captured in this model)
- Token renewal costs
- Distribution costs for all replacement and token renewals

Symantec VIP vs. RSA SecurID

Scenario: Deployment of 1000 OTP credentials deployed to secure remote access to corporate resources.

Assumptions: Symantec and RSA both issue 75 percent software tokens and 25 percent hardware tokens (10 percent must be distributed to remote users). In addition, 10 percent of the hardware tokens require replacement annually. Furthermore, RSA renews all their tokens at the end of the 3-year renewal period (10 percent of which must be distributed to remote users).

The model uses list price for software license fees, infrastructure, and hardware and software token costs. It assumes the same unit cost per hardware token for shipping of both Symantec and RSA's tokens regardless of whether it is the initial purchase, a replacement, or renewal. It also assumes the unit cost at the time of the initial purchase is the same at the time of renewal for hardware and software tokens for RSA.

One-time costs

Software license/setup costs

Symantec VIP charges a flat per credential, per year subscription fee over the lifetime of the solution (three years in this example). For comparisons sake, the enterprise license will be used for RSA SecurID. It should be noted that SecurID does not include risk-based authentication, which is included with VIP. For this functionality RSA requires users to purchase a separate product, Adaptive Authentication.

IT Infrastructure costs

For validation, administration, and life-cycle management of OTP credentials, we assume one server on site as well as a single disaster-recovery server deployed at a different site. Symantec VIP deployment will also leverage the existing enterprise directory for the user's first factor (password). The ability to leverage the existing user store for the first factor is a cost benefit for the Symantec solution as it simplifies end-user onboarding and training, as well as administrative overhead. It is also important to note that the VIP Enterprise Gateway is lightweight and completely stateless as compared to RSA's servers which host a proprietary database engine. Therefore, the type of server required for Symantec VIP is less costly. Costs include both hardware and OS.

Credential costs

Symantec™ VIP Access for Mobile provides a FREE, downloadable mobile credential for 2FA that makes strong authentication more convenient for end users as well as more affordable and cost-effective 2FA for the enterprise. VIP Access for Mobile is free of charge to both the enterprise and end user, and is distributed directly by Symantec, further reducing administrative overhead for the enterprise. It supports over 900 different mobile phone models, including Blackberry®, iOS®, Android™, Windows® Phone and J2ME™. RSA also offers a mobile software credential, however it has associated token seed fees comparable to their hardware tokens, and is not supported on as many mobile

devices as VIP Access for Mobile. We find most end users prefer software tokens, therefore this model assumes 25 percent of end users use hardware tokens and 75 percent of end users use VIP Access for Mobile or software tokens with RSA SecurID.

The initial hardware token costs are a one-time fee in the first year of deployment. RSA leases their tokens typically over a three to five year period, and enforces token renewal as the lease expires. Symantec VIP hardware tokens do not expire and can be used for the life of the battery, typically 5-8 years. Estimated token costs are based on list pricing.

Hardware token distribution

Hardware tokens must be distributed to end users, and the model assumes that 25 percent of users utilizing hardware credentials are remote and must have tokens individually packaged and shipped to their location. This must be done each time that tokens are purchased or renewed, so in this model it occurs twice for 25 percent of remote hardware token users. Other hardware credential users will pick up their tokens from a central location, incurring minimal additional cost.

Recurring service costs

Software license fees

Symantec charges an annual subscription fee over the lifetime of the solution (three years in this example). Although RSA sells a perpetual license, the model assumes RSA is charging 20 percent of the software license fee as a recurring software maintenance fee.

Renewal and replacement costs

Symantec customers own their tokens, so are not required to renew them after the life of the subscription, providing further cost savings over a RSA SecurID that enforces token renewal as the lease expires. This typically occurs at least once during a three to five year period. This model assumes all of RSA's hardware and software tokens are renewed at the end the three year period. A cost is incurred for all tokens and for shipping of the hardware tokens.

Shelf decay is another factor to consider when there is an expiration date associated with a token; although it is not captured in this model. Shelf decay is the result of stocking tokens prior to deployment to the users. Enterprises typically order more tokens at a time than can be deployed immediately. A number of tokens remain un-deployed for a long period of time (as much as six months) and thus lose useful life. Although it is not a cost highlighted in this model, it should be noted that even for a deployment of a few hundred tokens over three years the customer could incur a hefty cost in shelf decay alone.

For replacement token costs, the model assumes that ten percent of issued tokens are lost or broken annually. The appropriate per unit shipping fee is associated with these tokens.

Administrator and staffing

Although it is not addressed in the model an enterprise administrator should be designated to support the deployment and for on-going management. With Symantec VIP, the administrator no longer needs to import token seed records for each batch of tokens, or distribute software token seeds to end users using mobile phone credentials. Based on past experience we have found that this reduces administrative costs for Symantec VIP by about 30 percent.

Product and token life-cycle management

- **Total number of credentials:** 1000
- **Total years of analysis:** 3

Product, token life-cycle management, and Symantec assumptions:
(Although VIP includes risk-based authentication, RSA SecurID does not. It should be noted that RSA's risk-based authentication solution, RSA® Adaptive Authentication, is not included in the calculations.)

One-Time Costs		
	Symantec	Competitor
Software license/setup	$2,000	$51,500
Hardware credential cost	$3,500	$15,500
Credential shipping	$750	$750
Software credential cost	$0	$34,125
Server costs	$3,000	$4,000
Total one-time costs	**$9,250**	**$105,875**
Token Renewal Costs (All tokens at 3 year point)		
Renewal fees for HW and SW tokens	$0	$49,625
Renewal pkg/ship for HW tokens	$0	$750
Total renewal costs for the period	**$0**	**$50,375**
Annual Recurring Service Costs		
Annual service fee	$24,890	$0
Software maintenance fee	$0	$10,300
Replacement HW tokens after 1st year	$350	$1,550
Replacement pkg/ship	$300	$300
Total recurring costs	**$25,540**	**$12,150**
Total Cost of Ownership		
Total one-time costs	$9,250	$105,875
Renewal Costs (All tokens)	$0	$50,375
Total recurring costs (over 3 years)	$75,970	$34,600
Total fees (over 3 years)	$85,220	$190,850
Annual total cost per credential	**$28.41**	**$63.62**
Estimated Symantec TCO Savings: 55%		

Competitor: RSA MSRP pricing based on publicly available information as of 07/15

Symantec assumptions

- Enterprise deploys VIP Access for Mobile for 75% of end users, eliminating the need to staff up for credential distribution for those users
- Two servers one on-site and a disaster-recovery server co-located (VIP Enterprise Gateway is lightweight and stateless requiring a less costly server)
- 10% of issued tokens are lost or broken annually

RSA assumptions

- Enterprise deploys mobile phone software tokens for 75% of end users (seed file management is still required)
- Two servers one on-site and a disaster-recovery server co-located (more costly servers required to guarantee performance of proprietary database engine)
- 10% of issued tokens are lost or broken annually
- All hardware and software tokens are renewed at the end of the 3 year period
- 20% of software license fees as recurring software maintenance fee

Conclusion

As seen in the example above, Symantec VIP delivers significantly lower TCO than RSA SecurID, by 55 percent. In addition, there are several key features of the Symantec VIP that will further enable the enterprise to adapt their deployment to the evolving business requirements, while at the same time minimizing TCO in the long run. These concepts are summarized below:

Better value with Symantec

- Lower costs
- Free, easy-to-use software credentials provide significant cost savings (ex. passwordless option)
- Cost-effective tokens—no token renewal fees and no shelf decay
- Single, integrated platform allows you to deploy multiple devices depending on user and application types
- Flexible models enable you to create a customized solution for your business—OTP with Push verification or passwordless, or token-less options
- Leverages existing technology investments (Directory, database, SSO servers, etc.)
- Fully scalable
- Open versus proprietary—more credential choices and no vendor lock
- Continuous innovation—innovative devices both in cost and functionality (secure storage, end-point security, etc.)
- Single platform can support changing authentication requirements (including risk-based authentication)
- Out-of-box self-service application—including token activation, token synchronization, etc.

At a glance

Reduce credential costs

- Free software credentials vs. paying up to 80% of the cost of a hardware token for an RSA software token
- Free token-less risk-based option vs. paying for an additional product (RSA Adaptive Authentication)
- Hardware token prices more than 50% lower than RSA's
- Own your own hardware credentials vs. renewing/repurchasing every 3-5 years

Reduce IT Costs

- Software license and one-time costs 59% below what RSA charges during the first year
- Server costs lower than RSA's
- IT Staffing - part time employee vs. one full time employee
- Eliminating the password with VIP reduces the IT burden associated with password related calls (further reduction in costs are possible if passwordless VIP authentication is utilized with Symantec Identity Access Manager SSO capabilities)

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

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