



The True Cost of Strong Authentication for SSL VPN Access

Cutting Costs with On-Demand VPN Authentication

Contents

Overview: Strong Authentication and the True Cost of SSL VPNs	1
Calculating the True Costs of Tokens	2
Upfront costs of tokens	2
Ongoing token costs	3
Other factors	4
myOneLogin Secure Single Sign-On: The On-Demand Alternative	4
How it works.....	4
Total costs.....	5
Comparing Tokens and myOneLogin Costs.....	6
Summary	8

Overview: Strong Authentication and the True Cost of SSL VPNs

As the global workforce becomes increasingly mobile and virtual, more employees are accessing corporate resources from remote locations. Companies need strategies to offer secure, remote access to support telecommuting, mobile employees, remote offices or external contractors.

For many companies, Secure Socket Layer (SSL) VPNs are the answer to the remote access dilemma. Businesses can easily deploy web-based clients for SSL VPNs, while limiting remote access to specific applications. Lacking complex client configuration, SSL VPN deployment is rapid and cost-effective.

However, the SSL VPN incurs an additional cost to the business: strong authentication for access. Because security is typically the driving factor for SSL adoption, access to the SSL VPN must itself be protected. Relying on a password alone to protect accounts has been proven to be ineffective, no matter how 'strong' you make your password policies. Most businesses that depend on SSL VPNs to secure access to critical resources also insist on strengthening authentication with a second factor.

The true price of an SSL VPN deployment includes the cost of the strong authentication solution deployed along with the VPN, both in upfront costs and operational costs over time.

Most organizations give their SSL VPN users a second authentication factor using One Time Password (OTP) tokens. OTP token solutions are available from a number of vendors. Most require enterprise software deployment and ongoing management. Physical device management adds another layer of complexity. The token deployment and management increases the real Total Cost of Ownership of the SSL VPN effort considerably.

TriCipher offers an alternative: strong authentication delivered as an on-demand service, without any enterprise software or token hardware to manage. myOneLogin Secure Single Sign-On is quick to deploy and incurs a low, fixed subscription fee. It is part of a complete cloud identity platform that includes web single sign-on, federation and roles-based access control.

If you are contemplating an SSL VPN deployment or looking for ways to expand SSL VPN usage and reduce token costs, you need to carefully consider your options. This paper examines the total cost of ownership for token solutions, using data from analysts, users and other public sources. It also discusses and compares the total cost of OTP token solutions with on-demand strong authentication using myOneLogin.

Calculating the True Costs of Tokens

In the sections that follow, we will analyze the total cost of ownership for OTP token deployments. The different tasks and costs are based on research from analysts and pricing information available from major token vendors. Your specific costs will vary based on a number of factors, including:

- The number of SSL VPN users
- The negotiated pricing you have arranged with a token vendor
- The behavior of your users
- Your help desk cost infrastructure

The final section of this paper points you to a TCO calculator that you can personalize with your business' actual costs. The information below simply explains and categorizes the various upfront and ongoing costs of tokens. For the example, we will use costs based on a 500-seat OTP token license.

Upfront costs of tokens

Upfront token costs include:

- Solution purchase costs
- On-boarding costs
- Token deployment

Purchase cost: The purchase cost of the various tokens can only be accurately defined by negotiations with the vendor, based on the number of seats you need. The following figures should serve as rough guidelines only, based on tokens for 500 users. The cost estimates include software, server hardware, token hardware, per-seat licensing and maintenance contracts.

ActivIdentity	Entrust	RSA Security
\$44,453	\$66,548	\$265,699

On-boarding: On-boarding is the process of registering and creating an account for a user for the token solution. You can either outsource the on-boarding process to a service provider, or handle the process internally through the Help Desk and manual efforts by an administrator. Typical costs are:

- Outsourced on-boarding: \$65 per user
- Internal on-boarding: \$85 per user

Token deployment: Deployment costs include storing the token hardware, managing the inventory, shipping or distributing the devices, and distributing PINs. Your costs may vary depending on the shipping requirements. (If overnight shipping is required, expenses can be high.)

- Typical cost: \$20 per user

Ongoing token costs

Once the solution is deployed, you're not done paying for tokens. Users come and go. They lose tokens, leave them at home, or run them through the washing machine.

Ongoing token management costs include token replacement, temporary access, and token synchronization issues.

Token replacement: The world being an imperfect place, some percentage of your tokens will need to be replaced on a regular basis. How often depends on a number of variables, including:

- How many tokens are lost each year
- How many tokens are damaged or have dead batteries
- Employee turnover and new hires
- Contractor usage and turnover
- Percentage of employees/contractors that return tokens

To determine your true token replacement costs, you need to estimate values for these variables.

Employee turnover deserves a discussion. Theoretically, when employees leave, they will return the token, which you can give to a new employee replacing them. In practice, we find departing employees rarely think to return tokens. Many businesses decide that recovering the token is more costly and difficult than simply replacing it.

In our sample cost case, we'll make the following assumptions:

- 5% total replacement (including loss, damage and battery problems)
- 10% turnover among token users (which may include contractors)
- 75% of those that leave neglect to return their tokens

Given our pricing examples, we found that our typical token installation for 500 users incurs a token replacement cost of \$1,250 per year, which grows as the installed base of token users grows.

Temporary access: Users need to gain temporary access to the SSL VPN when they do not have their OTP token devices with them, or are in a location where they cannot use external token hardware.

The variables in determining the costs of temporary access include:

- Number of temporary access requests per user per year
- Cost of temporary access calls

Using a conservative estimate of \$25 per help desk call for temporary access and 1.8 calls per user per year, the total temporary access cost for 500 users is \$22,500 per year. This number can vary widely based on users' habits.

Token synchronization: Occasionally, tokens will become out of synch with the OTP server and the user login fails. Time-synchronous tokens (such as RSA's OTP tokens) can experience synchronization problems due to temperature fluctuations (including being run through the laundry). Event-based OTP tokens can become out-of-synch if the event button is pushed too many times (a young child gets the token, or it presses up against something in a purse or pocket).

Unfortunately, troubleshooting and correcting a token synchronization typically requires two Help Desk calls: one to the general Help Desk about the login failure and another to an OTP specialist that resynchronizes the token.

The variables to determine your costs here include:

- Percentage of tokens with synchronization issues each year
- Total cost of Help Desk effort to troubleshoot and correct problem

Assuming a conservative 1% of tokens have synchronization problems and the two Help Desk calls together cost your organization \$45, then the yearly cost of synchronization issues for a 500-token installation is \$225.

Other factors

Relying on tokens has other costs that are not easily quantifiable. These are not included in our cost estimates, but may be relevant to your business:

- Token provisioning can delay the project start for contractors or new employees.
- The cost and inconvenience of provisioning a contractor with a token may tempt organizations to allow password-only access to SSL VPNs for short-term situations—introducing a security exposure to the business as a whole.
- The token deployment is difficult to scale rapidly should your needs change unexpectedly. For example, you may take on a large number of contractors for a one-time project, or give remote access to more employees during a flu epidemic.

myOneLogin Secure Single Sign-On: The On-Demand Alternative

myOneLogin Secure Single Sign-On is an on-demand service that adds a second authentication factor without the cost and inconvenience of traditional token deployments. Using myOneLogin minimizes the additional costs of strong authentication and speeds your SSL VPN deployment.

How it works

myOneLogin uses TriCipher's patented split-key authentication technology, which is battle-tested in the financial services industry protecting millions of transactions daily.

Using myOneLogin, businesses can map multiple credentials to a single identity. MyOneLogin currently supports the following authentication methods as part of the basic offering:

- Encrypted browser cookies
- Browser certificates (X.509 digital certificate)

One part of the credential resides on the user's computer, the other part securely in the myOneLogin service. Both parts are necessary for authentication. From the user's perspective, the experience of authenticating is as simple as providing a user ID and password. The secondary factor exchange occurs in the background.

A user connecting from another device without the secondary factor (such as a kiosk) can gain a one-time authorization by answering personalized security questions that they select during the self-provisioning process, or by having a security key sent to a phone number registered for that account.

TriCipher offers other strong authentication methods that can be used in addition to the methods described above. These include:

- One-time-passwords sent to mobile phones
- VIP Access for Mobile or other VeriSign VIP tokens

You can choose how to integrate your directory information. Using myOneLogin Enterprise Edition myOneLogin can validate passwords against your current corporate user store, while validating the secondary authentication factor on the myOneLogin service. Or, the myOneLogin service can maintain the user directory information and validate both factors.



myOneLogin offers tight integration with nearly every major SSL VPN on the market, including SSL VPNs from Juniper, Cisco, Citrix, F5 and SonicWall.

Total costs

The cost of myOneLogin is a simple and straightforward \$1 per user per month for SSL VPN authentication. For \$30 per user per year, you can access the complete cloud identity solution, with a single strong login for all of your web applications as well as SSL VPNs.

There are no upfront costs; deployment is quick and simple. You do not need to purchase hardware or manage tokens.

Comparing Tokens and myOneLogin Costs

The first section of this paper used a sample installation with 500 token users to illustrate the total cost of tokens. Given the assumptions established in that section, the total token costs for the various solutions are outlined in the table below.

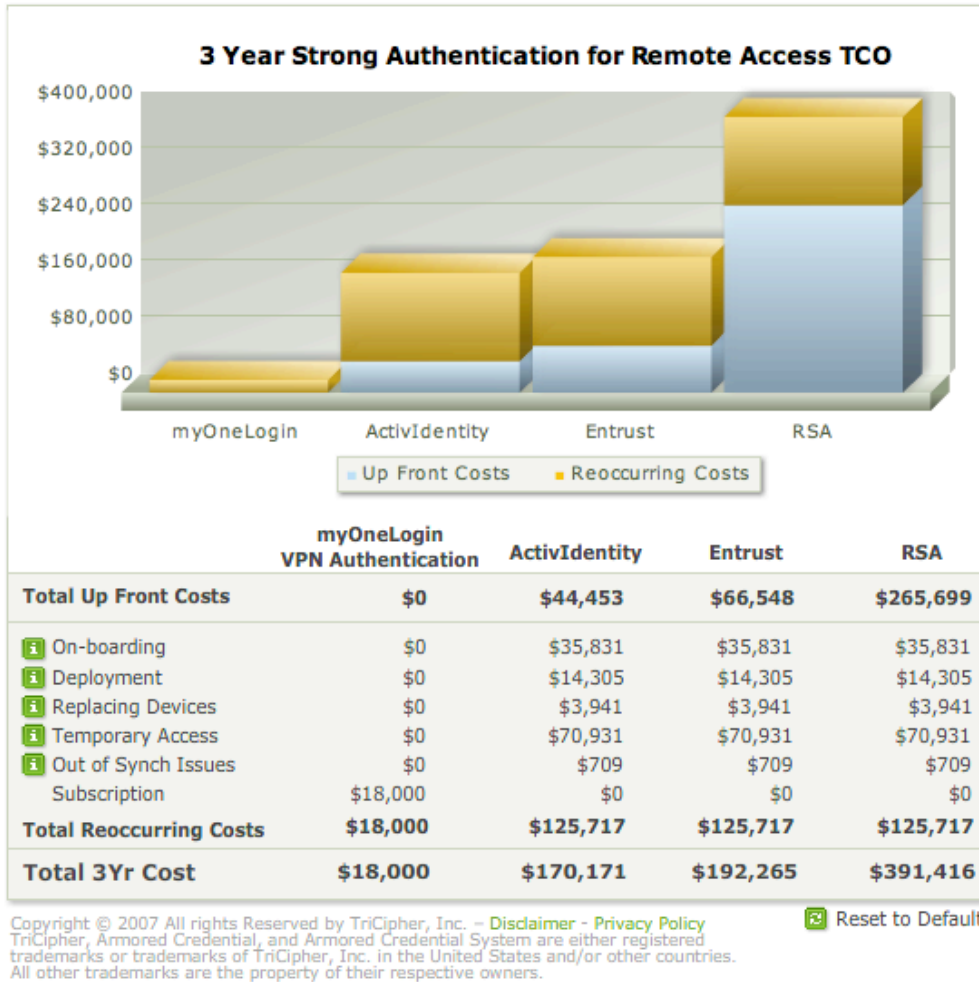
	ActivIdentity	Entrust	RSA Security
<i>Upfront costs</i>			
SW/HW purchase, license	\$44,453	\$66,548	\$265,699
On-boarding (internal)	\$32,500	\$32,500	\$32,500
Token deployment	\$10,000	\$10,000	\$10,000
Total upfront costs	\$86,953	\$109,048	\$308,199
<i>Ongoing yearly costs</i>			
Token replacement	\$3,941	\$3,941	\$3,941
Temporary access	\$1,250	\$1,250	\$1,250
Token synchronization	\$225	\$225	\$225
Total annual ongoing costs	\$5,416	\$5,416	\$5,416

In contrast, the cost of myOneLogin for 500 users for one year is a simple equation. For SSL VPN access alone, the cost is \$1 per user per month. \$12 per year for 500 users is \$6,000 per year. Or you can expand secure single sign-on to all web applications for \$30 per user per year.

If you have a different number of users or want to adjust the assumptions made about help desk costs or other factors, you can use an interactive calculator at:

http://www.myonelogin.com/vpn_authentication.html

- 1 Select number of users.
- 2 Customize the calculator & view your results.



Use the Customize button, or click on the green information buttons by the different fields, to examine the assumptions and adjust the values for your specific business environment. You can adjust most of the variables, including:

- Cost of token deployment
- Employee turnover
- Cost of help desk calls for temporary access

When you look at the calculator results, keep the following in mind:

- The total is based on the upfront costs and three years of ongoing costs.
- The ongoing costs include an assumption of 5% growth per year in the general costs of help desk and other expenses.

Summary

When calculating the true cost of an SSL VPN deployment for your business, you must include the strong authentication technology used to secure access through the SSL VPN. Traditional token solutions add cost and complexity to the SSL VPN deployment, and continue to incur costs over time for token management, replacement and support.

myOneLogin Secure Single Sign-On offers a cost-effective, on-demand alternative to OTP tokens, without the implementation and ongoing management costs of tokens. For a simple \$12 per user per year, myOneLogin is a fast and flexible way to provide strong authentication to the SSL VPN. Because it is an on-demand service, it is quick to implement and scale if your needs for secure remote access grow.

About myOneLogin and TriCipher

TriCipher offers the first "one and done" cloud identity services platform that manages and protects user identity in the cloud.

The myOneLogin Single Sign-On, Enterprise Edition offers a complete range of identity services, including multi-protocol federation, single sign-on, roles-based access control and strong authentication. This patented, proven technology platform supports a range of identity services, both in-the-cloud and on-premise, that manage and protect user identity in the cloud.

TriCipher's patented technology has been proven at over 10,000 financial institutions, protecting financial transactions for over six years. It uses a battle-tested infrastructure, with enterprise-caliber identity services and proven privacy walls securing data in the cloud.

myOneLogin Enterprise Edition integrates with enterprise directories, desktops and SSL VPNs through a lightweight Enterprise Connector, available from TriCipher. With this integration, myOneLogin can extend enterprise identity, authorization and roles-based access control to cloud-based applications.

For more information, visit www.myOneLogin.com, or contact sales@TriCipher.com.

TriCipher Headquarters:

750 University Avenue, Suite 260
Los Gatos, CA 95032
Phone: +1.650.372.1300
Fax: +1.650.376.8301

TriCipher Worldwide Sales:

Email: sales@tricipher.com
Phone: +1.650.376.8326
Fax: +1.650.376.8301

Copyright © 2010 TriCipher, Inc. The information in this document is subject to change without notice. TriCipher and myOneLogin are either registered trademarks or trademarks of TriCipher, Inc. All other business and product names mentioned are the property of their respective owners.