

Top five questions you should ask before purchasing a two-factor authentication solution



You've made the choice to implement two-factor authentication, but where do you go from there? With the multitude of solutions available in the market today, how do you know which is going to be right for your organization?

In this tech brief we will discuss the top five questions that you should ask before purchasing a two-factor authentication solution. We will also examine Defender, Dell's solution for two-factor authentication, and how it addresses each question.

1. How is the solution architected and how well will it scale?

Because architecture is the foundation of any solution, it is important that the architecture of your two-factor solution will blend well with your existing infrastructure. One of the first things to consider is where the solution will house all of the user and token information. Will it be stored in one of

your existing identity databases? Or will it be stored in a new database that will need to be supported and kept in sync with another identity store – and thus it's yet another place that a user will need to be provisioned to? If it is a new database, how will you manage load balancing and redundancy? Will you need two or three additional stores in order to scale? Finally, does it use industry standards for authentication? Will you be able to migrate to a different vendor with ease, or will you have to completely rip and replace the entire solution when you are ready to move on?

Defender bases all administration and identity management on an organization's existing investment in Active Directory, eliminating the cost and time involved in setting up and maintaining proprietary databases to support two-factor authentication. In addition, since Defender integrates directly with Active Directory it scales as you grow Active Directory

The most important question you need to ask around deployment is how tokens will be requested and assigned – a critical success factor and one of the most time-consuming tasks.

within your environment, making load balancing and redundancy a breeze. Defender is also based completely on industry standards such as RADIUS, OATH, LDAP and PAM. This enables easy and fast integration with more applications and devices, as well as the ability to quickly integrate with any other standards-based solution needed in case of a merger or acquisition.

2. Is the solution easy to administer?

Because administration is done on a regular basis it is likely the second most important factor when determining if a solution will be right for your organization. Two key things to consider when it comes to administration are availability and ease of use. Is Web-based administration available, and what types of tasks can be done via the Web? What about the admin interface? Is it easy to use? What type of help does it have, embedded, online or both?

Defender offers Web-based administration for token management, token deployment, real-time log viewing, help desk troubleshooting and reports. For the main console, Defender uses Active Directory's native administration tool, Active Directory Users and Computers (ADUC). Using ADUC for administration means no new console to learn, easing the heavy burden placed on admins when deploying new software. Defender also provides an embedded help desk troubleshooter, enabling administrators to troubleshoot, diagnose and resolve user-authentication-related problems with just a couple of mouse clicks from any browser.

3. How is the solution deployed? Is it user friendly?

A quick smooth deployment is vital to the success of any IT project. Any hiccups can cause both admins and user aversion, not only for the deployment but for ongoing use. The most important question you need to ask around deployment is how tokens will be requested and assigned – a critical

success factor and one of the most time-consuming tasks.

Defender enables users to securely request and/or receive a hard or soft token based upon pre-defined administrator policy. The user can then assign that token to their account through a unique secure mechanism, removing the entire administrative burden and associated costs of conventional manual token assignment.

4. What options are available for tokens, and how are they priced?

Token availability is also fundamental to the decision on which two-factor solution will be right for your organization; not all tokens are the same even when they look and function in the same manner. The first thing to consider is the overall selection of tokens. What type of hardware tokens do they offer? USB, credit card style, key fobs? And for software tokens, do they have one for all of the different phone operating systems? And what about SMS, email and Web-based?

The second question to ask is how tokens are priced. For hardware tokens, are they offered on a term basis, say for three, four or five years, or are they sold for the duration of their battery life, typically five to seven years? For software tokens the same question can be asked: Are they offered on a term basis, either two, three or four years, or are they perpetual licenses that never expire? If they are offered on a term basis, will a new token need to be provisioned to the end user after the term is up?

Finally for hardware tokens you will want to find out if they are OATH compliant. OATH is the open standard for authentication and ensures interoperability between authentication vendors using the standard. Choosing an OATH-compliant solution enables more choices of token devices as well as interoperability when it comes to interfacing with legacy systems or disparate agencies.

Defender supports any OATH-compliant hardware token and has relationships with several major token vendors, enabling you to choose the best token for your organization. Defender also offers a wide range of software tokens, including all the widely deployed mobile platforms, SMS, email, desktop and even Web-based tokens.

All Defender hardware tokens are sold for the duration of their battery life, and software tokens have a perpetual license that never expires. This reduces the cost, administrative burden and end-user disruption of re-deploying tokens after only two, three or four years. In addition, by offering a universal software token license, the administrator can easily reissue the appropriate device license when a user decides to switch mobile platforms.

5. What's included in the base cost of the solution?

Determining the total cost of ownership for some solutions is quite difficult as the solution providers hide the true costs beyond the most basic installations. To make sure you aren't nickel-and-dimed for every little feature, make sure you discuss the following topics. Agents are one of the more common hidden costs. For every device/server that you want to authenticate with using two-factor authentication, you need to ensure that they can use the authentication protocol of your solution's choice. In most cases this will be RADIUS authentication, but there are some solutions that use proprietary protocols.

In either case you will need an agent installed on each device/server that doesn't support the authentication protocol. Some solution providers will charge you for their agents in order to support these devices. There are also some solution providers that charge for features that make their product easier to deploy and manage. So make sure to ask if they charge for add-ons, like user self-registration and webmail.

Defender has a very simple pricing model. You pay for a user license and a token license, either hardware or software for each user. Everything else we offer with the solution – token self-registration, Web administration, webmail, all agents, etc. – is included. In addition first year's maintenance is included with the initial cost, and there are no maintenance fees on hardware or software tokens.

Defender software tokens never expire, and its hardware tokens are good for as long as the battery allows. Finally, users can be assigned multiple tokens without the need for additional user licenses, enabling you to provide token flexibility to the user in a cost-effective manner.

In the past, two-factor authentication solutions have been expensive, cumbersome to deploy and difficult to manage, but that doesn't have to be the case anymore. By asking at least these five questions of any potential vendor you will be able to make the most informed decision on what two-factor solution is best suited for your organization.

To learn more about Defender, visit www.quest.com/defender.

All Defender hardware tokens are sold for the duration of their battery life, and software tokens have a perpetual license that never expires. This reduces the cost, administrative burden and end-user disruption of re-deploying tokens after only two, three or four years.

For More Information:

© 2012 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT,

DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com

Refer to our Web site for regional and international office information.

