AuthAnvil

12 Questions You Need To Ask Your Multi-Factor Authentication Vendor

TWELVE QUESTIONS TO ASK YOUR MULTI-FACTOR AUTHENTICATION (MFA) VENDOR

Before selecting a multi-factor authentication solution, you'll want to make sure that the product you're considering is the right one for your company.

There are plenty of questions you should ask any potential vendor. Many of them will depend upon the unique infrastructure of your company and business processes.

Here are 12 questions that anyone considering a multi-factor authentication solution should be asking. The vendor should at least give you the foundational information needed to determine whether their given solution is right for your business.

1 WHAT OPTIONS DO YOU PROVIDE TO GENERATE ONE-TIME PASSWORDS (OTP)?

Before you put your trust in a vendor's product, be certain that they provide the options you need in terms of the software or hardware used to generate your OTPs.

Some solutions will require that the user have a hardware key-fob device to login, while others will allow you make use of company issued or personal cell phones and mobile devices. Take this into account when determining whether a vendor's offerings are appropriate for you and your users.

2 DO YOUR TOKENS EXPIRE AND NEED TO BE REPURCHASED AND REDEPLOYED?

Regardless of the number of employees in your company, it will get very expensive if you need to constantly replace expired tokens, or even worse the vendor requires you to replace tokens every few years even if they weren't used. This is also challenging for budgeting purposes since the costs are inconsistent. A better solution might be to consider a monthly billing or subscription based option where the cost is consistent and can be budgeted accurately.

Make certain the billing is clear and that you are only paying for tokens that have been activated. Some vendors will invoice based on the total number of tokens owned, whether they are in use or not.

3 WHICH ENDPOINTS ARE YOU ABLE TO PROTECT?

If the multi-factor authentication vendor cannot provide protection for the endpoints that you use, then you're not getting what you need out of the solution.

Do you need Office 365 or Salesforce protection? What about Windows servers, firewalls and networking gear? How about your remote management software? Make sure you have a good inventory of the endpoints you need to secure, and ask any potential vendors to provide a list of what they can protect. If you don't ask ahead of time, you might end up with a product that doesn't meet your current or future requirements.

4 HOW ARE USERS PROVISIONED? CAN YOU SYNC WITH ACTIVE DIRECTORY?

The ability to synchronize with Active Directory is one of the most powerful features a multi-factor authentication vendor can offer. This will streamline and accelerate setting up your secure environment by eliminating the need to provision users twice.

5 WHAT OPTIONS DO I HAVE IF A USER IS TEMPORARILY WITHOUT THEIR TOKEN?

If a user doesn't have access to their token and they cannot log into a necessary application or other resource, make sure the vendor you select has options to quickly remediate the situation.

A quick response will ensure users have confidence knowing they will never be locked out of the resources they need to get their work done.

6 CAN I STILL AUTHENTICATE IF I HAVE TEMPORARILY LOST NETWORK ACCESS?

Making sure that your multi-factor authentication still functions in the event you've lost network access is another consideration you should take into account.

With people consistently travelling for businesses it's vital the solution you select is able to offer solid security and usability in just about any situation, including one where access to the internet is lost. This can occur when someone is flying, or is on the road without access to a mobile network.

7 WHO HAS CONTROL OVER THE DATA AND INFRASTRUCTURE?

Employees, contractors and vendors come and go at just about every company. This means that you need a way to ensure your company's IT infrastructure and data are not under the control or accessible by the wrong people.

Remember that the entire point of a solid authentication solution is to provide access and identity management. If you have any doubts about where the data is stored, it might be time to consider another vendor.

8 DO YOU OFFER A WAY TO DELEGATE AUTH FROM ONE MFA SERVER TO ANOTHER?

The ability to delegate authentication to another multi-factor authentication server should be built into any system that your company considers. This allows you to manage multiple installations with one set of credentials and tokens.

For some infrastructure models, delegation is a critical feature and one that a company cannot do without. Make sure you ask your vendor about this, as it may have serious implications for deployment of your multi-factor authentication technology. No one wants to carry around a boat-anchor for a keychain with several hardware keyfobs or need to run dozens of software based apps… when one would do.

9 HOW ARE MULTIPLE USERS AUTHENTICATED AND DIFFERENTIATED WITH USING A SHARED ACCOUNT LIKE ADMINISTRATOR OR ROOT?

Most IT infrastructures will have multiple root or admin accounts to manage, but will need to have some way of differentiating who is logging into those accounts.

For instance, when logging in as a local administrator on a workstation, two technicians might use the same Windows credentials. With a good multi-factor auth system, the two technicians would then be differentiated by their individual PIN and OTP from their token.

10 CAN I MANUALLY OVERRIDE THE MFA REQUIREMENT IN AN EMERGENCY?

There may be times when you will need to override the authentication requirement and get access to an account. Being locked out of key resources in an emergency can be a nightmare for your IT staff and for your business processes.

Even though a multi-factor authentication solution should provide the highest levels of access control, be prepared for scenarios when some sort of an emergency situation calls for you to override the system.

11 IF I NEED TO REVOKE A USER'S ACCESS, HOW INVOLVED IS THE PROCESS?

What if someone leaves your company and you need to revoke their access to all of the company resources? What if the employee is still there, but you need to change their level of access? If this process is long, complex, or under-developed you might be setting your company up for a lot of extra risk, cost and work.

A good multi-factor authentication product should make it easy for administrators to immediately revoke access when needed.

12 DO ALL USERS HAVE TO USE MULTI-FACTOR AUTHENTICATION?

While multi-factor authentication is a great boon for your security, it doesn't follow that every single person who works at that business will necessarily benefit from the increased security. In fact, for some users, it may actually prove more of an inconvenience than anything else. And if that user has very low permissions levels, it may not be necessary at all.

No solution should be a one size fits all response. You should be able to customize and tailor the solution so that vital resources are protected, without inconveniencing users who really don't require multi-factor authentication. If you're interested in seeing a solution designed from the ground up with security and usability in mind, download the AuthAnvil Password Solutions Quick Peek. This brief eBook will introduce you to AuthAnvil.