



Questions the C-Suite Should Ask MFA Vendors

Multi-factor authentication (MFA) is an essential piece of security for any modern business. Whether you're trying to meet compliance requirements or trying to increase the security of your business, MFA can help. By implementing MFA, you can help secure your company's assets, confidential information, and accounts – especially if you have remote workers, privileged users, Cloud applications, and employees that access corporate resources on their laptops. Implementing MFA also minimizes the risk of a breach and the reputation damage, legal fees, and other consequences that come with that.

However, not all MFA is created equal. By asking these questions, you can better determine whether a potential MFA solution will provide the security you need or if you need to look elsewhere.

1

Does your MFA solution use SMS-based verification as the primary or default authentication option?

SMS-based verification is less secure than other methods because it is vulnerable to hijacking. It is acceptable as a back-up method since using multiple factors of authentication will always be stronger than using just one layer of protection. However, SMS-based authentication should not be the primary or default method used. If it is, look elsewhere.

2

How is the user experience for end users?

A good user experience is critical to ensure successful MFA adoption. If end users feel that the particular solution impedes productivity and prevents them from accessing the resources they need, it will not work. Ask the service provider to walk you through the user experience and question any parts that you predict will frustrate your employees (e.g. certain hardware tokens that are easily lost or forgotten). Ask the service provider if there are features that help with end-user adoption or if they have any recommendation on gaining end-user adoption.

3

Does it support offline authentication?

If you have employees that travel for work and that need to access their laptops while on the airplane, you'll need to ensure that your chosen MFA solution supports offline authentication. There are other instances, such as when you are connecting to hotel Wi-Fi or public Wi-Fi or when an Internet connection is spotty, in which offline authentication is required. Ask the service provider about offline authentication options and be sure that their solution is easy, secure, and doesn't require helpdesk connections.

4

Does the solution support secure Web Single Sign-On (SSO)?

Web single sign-on not only makes the solution easier for the end user, but also makes it more secure. It's essential that Web SSO into Cloud applications is supported by any MFA solution you are considering. If your company uses many different Cloud applications and each of those apps require users to sign in and create passwords, then the user experience becomes very complex. It also means employees will need to reset their passwords more often and may require helpdesk support more often. This can be avoided with single sign-on, which enables users to sign on just once to access all their Cloud applications. This ultimately provides a better user experience and is an important motivation for user adoption.

5

What is the MFA vendor's business model?

When purchasing MFA, it's not just important to make sure the solution meets your needs, but that the solution provider is the right fit for you as well. Ask the solution provider about their business model to get a feel for how much they'll be able to support you beyond just the purchase. Will they be able to support all your needs during deployment? Do they have local partners to provide support if there are ever issues? Does their pricing model accommodate how and when you want to allocate license?

6

Is the solution localized for end users?

End-user facing applications should be localized. While the management interface does not need to be localized, the language of the UI should be appropriate for all applicable regions. This is critical for end-user adoption of any MFA solution. Remember that an MFA end user is most of the time not a cyber security expert.

7

Is the solution easy to manage?

Management and token allocation should be simple, quick, intuitive, and web-based, even for non-experienced operators. How easy is it to set up and start using the solution? How fast can you add a resource to be protected by the MFA solution? How fast and easy can you provision authenticators for the users? Is the admin interface easy to understand and use? Seek solutions that provide a comprehensive interface for what you need without requiring you to be an expert.

8

How much does the solution cost?

Asking about pricing is a given, but we wanted to bring it up because MFA pricing can be unclear and sometimes there are hidden costs. How is it sold: per user, per authenticator, or even per protected application? Is support included – both technical support and subscription management support? Are there any other hidden costs that may apply, such as extra software you will need to license? Pricing for MFA is often done in bands or ranges with bulk discounts. If you fall below a certain range, work with the solution provider to see how you can be creative to meet the bulk requirements of the next pricing band.

THE WATCHGUARD SECURITY PORTFOLIO



Network Security



Secure Wi-Fi



Multi-Factor Authentication

Find out more

For additional details, talk to your authorized WatchGuard reseller or visit <https://www.watchguard.com/authpoint>

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.