The potential hidden costs of deploying multi-factor authentication in your business

With a sharp rise in cybercrime, it's a growing concern that irrelevant of size, geography, or industry, your business could be at risk, if you have not taken precautionary measures to protect it.

Protecting your business with an authentication solution requires considerable investment. However, ensuring you have full visibility of both the initial and the ongoing costs is paramount. This article explores ALL of the potential cost considerations.

With technology constantly evolving, many organisations are choosing to deploy a multi-factor authentication (MFA) solution, over a two-factor authentication (2FA) solution because of the increased protection it provides the business.

2FA utilises two factors to successfully authenticate users and is a subset of MFA. Full MFA requires the user to authenticate with knowledge, possession and inference. For example, if your organisation has data that is perceived as critical, such as intellectual property like patents, protecting access to it with MFA ensures that the users accessing that information are legitimate. Proving their identity with something that they have (app on a mobile device), something that they know (PIN or one-time code) and something that they are (fingerprint).

This could be utilised dynamically in the business, so users authenticate with methods appropriate to the application or data they are trying to access. If the data is perceived to be of great value or high risk, administrators can request users accessing it to provide full MFA.

It also ensures efficiency is optimised without compromising security. But how much does a business have to compromise when it comes to the investment?

Upfront investment considerations

There are initial upfront costs such as licenses (management, hardware and for end-users) and hardware requirements, including high availability. Professional Services might also be a necessity, depending on change control requirements, reducing the burden on internal IT professionals.

Help desk costs during deployment for end-users, and the shipping of the tokens, (if hardware tokens are required) also need to be factored in.

Other upfront costs could be less tangible and include training, and a price attributed to the increased productivity for enrolling users to authenticate using the platform.

However, whether the costs are tangible or not, the total cost of ownership (TCO) is sometimes overlooked with the initial enthusiasm to minimise disruption of network restructure.

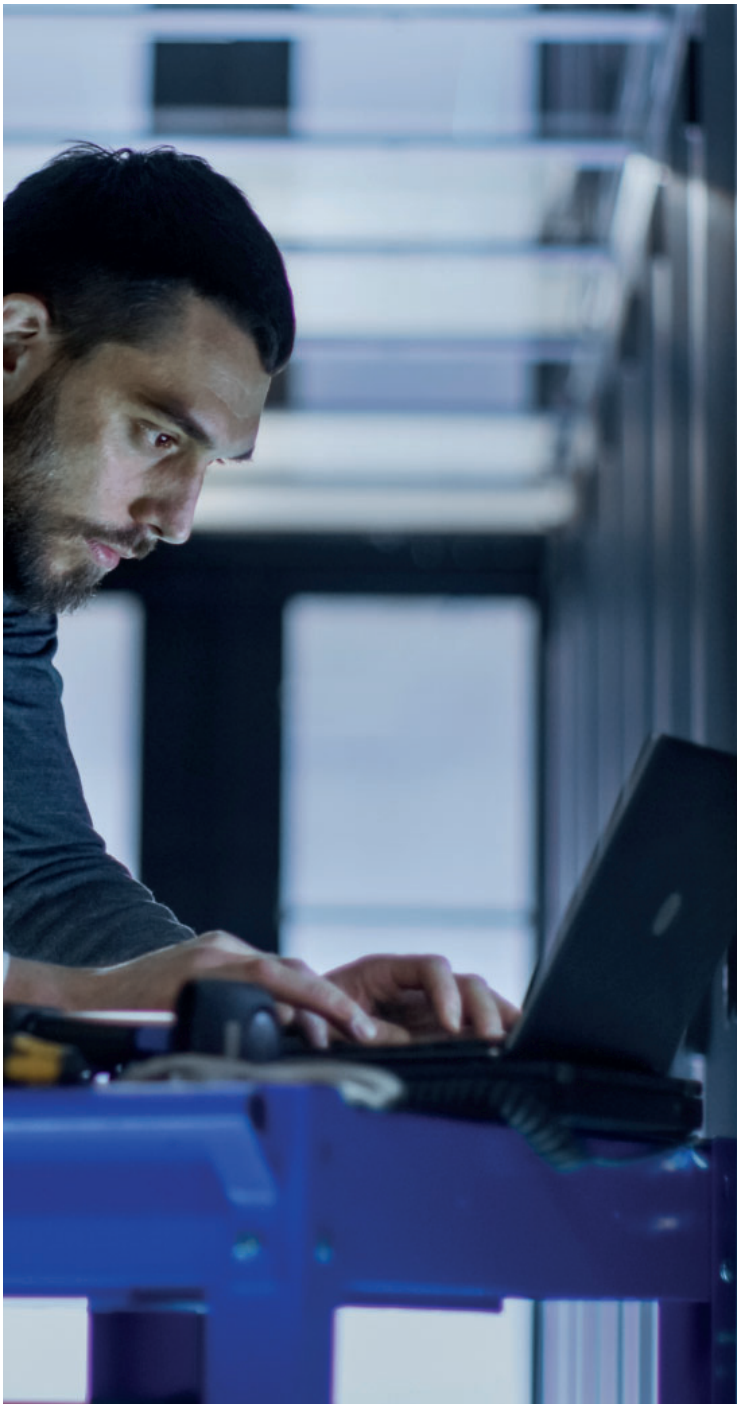
Considering total cost of ownership of your new solution

Once you have deployed your solution and the training has started to pay dividends, including a decrease in calls for assistance, you receive your invoice for your maintenance renewal.

Maintenance renewals can be very expensive, and the costs are not always transparent during initial discussions. With the focus on proof of concept (POC) and ease of deployment, it is easy to see why ongoing total costs are not always discussed or explored. Ultimately, it's a mistake to ignore costs of the solution in the medium term (years three and four), even in the early stages of your exploration.

Ongoing maintenance costs can include help desk costs for end-users, IT admin time for administrators. Some suppliers will also charge for patches and upgrades, new connectors / integrations, and even data centre charges such as utility costs.

Implementing a solution like MFA is no mean feat and not surprisingly, some suppliers will rely on you stomaching the large ongoing maintenance costs because the thought of going through the whole exercise again is just too much to bear.



Due Diligence

Ensuring you perform due diligence before signing on the dotted line is essential, if you don't want any nasty surprises after you have completed the first twelve months. Everybody seeks an easy life, especially when it comes to deploying something like MFA within their organisation, but it's easy to get wrapped up in the 'plug and play' selling point, without realising the hefty invoices that can follow.

To help you ask the right questions when you start exploring MFA solutions, we have listed some points below that should be considered at the outset.

Costs associated with productivity

Ongoing maintenance costs for administrators:

- Are there any costs associated with the support for hardware and software?
- What are the costs for patches and upgrades?
- Is there a cost for additional connections / integrations?
- Are there any data centre charges?
- What is the charge for IT admin time?

Ongoing maintenance costs for users

- Is there a cost for lost or damaged tokens?
- What are the costs for token license renewals?
- Are there any shipping costs involved?
- What are the costs for help desk for users?

As well as ongoing maintenance costs, other costs such as those associated with productivity continue to grow in importance. It is easy to see why the costs associated with productivity is a big advantage, with the senior management team keen to ensure both the implementation of the MFA solution, and the continued authentication of users does not cause major disruption to the business.

Time per authentication can be a big selling point, but ensuring your chosen solution incorporates features such as risk-based authentication (RBA) at no extra cost, means the user will only ever have to authenticate with the appropriate level or method. For instance, if they are working in the office and logging into Office 365, they may just require one method or factor.

If the same user is trying to access their customer relationship management (CRM) database remotely, using a personal device, they may require full multi-factor authentication. However, they may be denied access, depending on the configurations.

A dynamic solution can provide the appropriate level of authentication per user, per application basis, ensuring productivity is maximised, without compromising security.

A minority of MFA providers automatically include the RBA feature as standard, but most will add a surcharge to the license. Or it might only be included if you purchase the 'premium option'.

Single sign-on (SSO) can also carry a surcharge or it's only available as a premium option. As some of these features are now well established and often on the wish-list of administrators, it is worth considering how all of these costs accumulate to a potentially hefty total.

swivelsecure

Full functionality, accessibility and configurability as standard

Each organisation has different architecture, and this will impact the requirements. However, some features are universal and designed to provide:

- Efficiency - such as SSO where users only need to authenticate once to access all their applications

- Flexibility - such as RBA and the ability to protect all architecture variations

- Productivity - user portals which allow users to reset their PINs and provision their mobile device autonomously

Other surcharges can be added for each additional method (factor) of authentication. Using a solution with RBA might provide both increased flexibility and productivity, but if you get charged for utilising more than one authentication method, then it will counterbalance the advantages. Ensuring users have accessibility to all available methods of authentication as standard, will ensure you benefit from features such as RBA without the added cost of using more than one factor.

Final word

Once you have made all your decisions and found the right solution, ensure you question the likelihood of any requirement to amend the configuration, software or connections in the future. This is likely to cost your organisation considerable investment, so ensuring you understand the configurability and adaptability of the solution is paramount.

Documenting the differences between suppliers is never going to be easy. However, considering the full offering including features, factors and on-going maintenance costs (for both administrators and end-users), should help to illustrate the full investment of implementing the solution.